KATHOLIEKE UNIVERSITEIT LEUVEN
FACULTEIT RECHTSGELEERDHEID EN CRIMINOLOGISCHE WETENSCHAPPEN
Academiejaar 2024 – 2025

DE INTERNATIONALE DOORGIFTE VAN PERSOONSGEGEVENS VAN DE EUROPESE UNIE NAAR CHINA IN DE WETGEVING EN DE PRAKTIJK

Promotor: prof. Laura DRECHSLER
Co-promotor: Pauline HELLEMANS
Corrector: Frank VERBRUGGEN

Masterscriptie, ingediend door
Arne VINCKEN
bij het eindexamen voor de graad van
MASTER IN DE RECHTEN

KATHOLIEKE UNIVERSITEIT LEUVEN
FACULTEIT RECHTSGELEERDHEID EN CRIMINOLOGISCHE WETENSCHAPPEN
Academiejaar 2024 – 2025

DE INTERNATIONALE DOORGIFTE VAN PERSOONSGEGEVENS VAN DE EUROPESE UNIE NAAR CHINA IN DE WETGEVING EN DE PRAKTIJK

Promotor: prof. Laura DRECHSLER
Co-promotor: Pauline HELLEMANS
Corrector: Frank VERBRUGGEN

Masterscriptie, ingediend door
Arne VINCKEN
bij het eindexamen voor de graad van
MASTER IN DE RECHTEN

Arne VINCKEN

bij het eindexamen voor de graad van
MASTER IN DE RECHTEN

KU LEUVEN

Samenvatting

Sinds 2016 delen miljarden gebruikers op TikTok korte video's waarin ze aspecten van hun dagelijks leven tonen. De applicatie zorgde echter niet alleen voor een expansie aan creativiteit maar ook voor een enorme verzameling van persoonsgegevens. Zo verzamelt het Chinese moederbedrijf, ByteDance, onder andere locatiegegevens, apparaatgegevens en surfgedrag om de beste video's aan te bieden.[1] Er rees al snel de vraag of de gegevens van gebruikers op het EU-grondgebied wel voldoende beschermd worden wanneer ze naar China worden doorgegeven. Daarnaast overwoog de Verenigde Staten een verbod op TikTok vanwege mogelijke bedreigingen voor de nationale veiligheid.[2] Binnen Europa groeit de bezorgdheid dat data die naar China wordt geëxporteerd, kan worden ingezet voor de training van kunstmatige intelligentie, mogelijk met steun van de Chinese overheid.[3]

Deze masterscriptie onderzoekt de overdracht van persoonsgegevens van de EU naar China, met TikTok als praktijkvoorbeeld. Wanneer data de EU verlaat, is het cruciaal te bepalen of de rechten van EU-inwoners gewaarborgd blijven onder het wetgevingskader en de praktijk van het derde land. Het EU-recht, zoals vastgelegd in de AVG en ondersteund door de arresten *Schrems* I en *Schrems* II, vereist namelijk dat deze rechten worden beschermd. Aangezien China niet geniet van een adequaatheidsbesluit, ligt de focus op standaardcontractbepalingen en het beschermingsniveau onder het Chinese wetgevingskader, waaronder de PIPL. Daarnaast wordt onderzocht hoe TikTok meent een gelijkwaardig beschermingsniveau te bieden, onder meer via hun privacybeleid en standaardcontractbepalingen. Ook wordt nagegaan of de gegevens voldoende beschermd zijn tegen bijvoorbeeld overheidsinmenging.

De scriptie toont aan dat juridische en praktische problemen bij gegevensdoorgiften blijven bestaan, mede door gebreken in de Chinese wetgeving en TikToks beperkte transparantie en onvoldoende waarborgen in hun standaardcontractbepalingen.

---

[1] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, Welke gegevens we verzamelen, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 27 september 2024).

[2] VERHEYDEN T. en VANMELDERT D., 'Laatste kans voor TikTok in VS? Hooggerechtshof buigt zich vandaag over mogelijk verbod', *VRT NWS* 10 januari 2025, https://www.vrt.be/vrtnws/nl/2025/01/08/laatste-kans-voor-tiktok-in-vs/ (geraadpleegd op 20 januari 2025).

[3] VAN HORENBEEK J., 'Militaire geheime dienst waarschuwt voor AI', *De Morgen* 2 april 2025, https://www.demorgen.be/snelnieuws/militaire-geheime-dienst-waarschuwt-voor-ai~b3bbd0bc/ (geraadpleegd op 8 april 2025).

Dankwoord

Het schrijven van deze masterscriptie is een laatste stap in mijn academische traject, een avontuur dat zowel uitdagend als waardevol is geweest. Gedurende deze periode heb ik enorm veel steun gekregen van de mensen om mij heen en daarom wil ik graag mijn oprechte dankbaarheid uiten.

Eerst en vooral wil ik mijn promotor, prof. Laura Drechsler bedanken voor het interessante onderzoeksonderwerp. Haar begeleiding, steun en inzichtelijke feedback hebben een grote rol gespeeld bij het tot stand komen van deze scriptie. Samen met mijn co-promotor, Pauline Hellemans heeft ze me voortdurend aangemoedigd om mijn werk te verbeteren en mijn argumenten te verfijnen. Hun expertise was onmisbaar gedurende dit proces en ik ben hen dan ook zeer dankbaar voor hun hulp.

Daarnaast wil ik mijn familie bedanken voor hun voortdurende steun. Mijn bijzondere dank gaat uit naar mijn ouders, die met hun onvoorwaardelijke steun voortdurend een bron van motivatie zijn geweest. Dankzij hun aanmoediging, geduld en de ontelbare heerlijke maaltijden die ze bereidden, kon ik me op mijn onderzoek concentreren zonder kostbare tijd te verliezen.

Verder ben ik mijn vriendin ongelooflijk dankbaar voor haar trouwe steun. Ze stond altijd klaar om me aan te moedigen wanneer ik dat het meest nodig had. Ze zorgde daarnaast voor de nodige afleiding na lange dagen werken. Ze herinnerde me eraan om een stapje terug te zetten en nieuwe energie te vinden.

Het voltooien van deze masterscriptie zou niet mogelijk zijn geweest zonder deze mensen. Ik wil jullie allemaal bedanken voor jullie geduld, motivatie en geloof in mij. Jullie betekenden heel veel voor mij.

Inhoudsopgave

Lijst van afkortingen

APPI	Act on the Protection of Personal Information (Wet op de bescherming van persoonsgegevens)
AVG	Algemene Verordening Gegevensbescherming
BCR	Binding Corporate Rules (Bindende bedrijfsvoorschriften)
BCR-Lead	Binding Corporate Rules-Lead (Verantwoordelijke voor Bindende Bedrijfsvoorschriften)
CAC	Cyberspace Administration of China (Cyberspace Administratie van China)
CSL	Cybersecurity Law (Wet op de Cyberbeveiliging)
DSL	Data Security Law (Wet op de Gegevensbeveiliging)
EDPB	European Data Protection Board (Europees Comité voor gegevensbescherming)
EDPS	European Data Protection Supervisor (Europese Toezichthouder Gegevensbescherming)
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
HvJ-EU	Hof van Justitie van de Europese Unie
PIHBO	Bedrijfsexploitant die persoonsinformatie verwerkt
PIPL	Personal Information Protection Law (Wet op de Bescherming van Persoonsinformatie)

PISS	Personal Information Security Specification (Specificatie voor de Beveiliging van Persoonsinformatie)
SCC	Standard Contractual Clauses (Standaardcontractbepalingen)
DTIA	Data Transfer Impact Assessment (Beoordeling van de Gevolgen van de Overdracht)
UVRM	Universele Verklaring van de Rechten van de Mens

Lijst van bijlagen

Inleiding

Afdeling 1. Situering van het onderwerp

Dankzij de groeiende digitalisering en de steeds grotere afhankelijkheid van datagedreven technologieën, maken ondernemingen steeds vaker gebruik van grensoverschrijdende gegevensstromen. Een voorbeeld is het Amerikaanse technologiebedrijf Meta, dat persoonsgegevens van Europese gebruikers doorstuurt naar servers in de Verenigde Staten voor advertentiedoeleinden.[4] Volgens het Data Privacy Framework van de Europese Commissie hebben zulke gegevensstromen een aanzienlijke economische waarde, omdat ze innovatie en internationale handel ondersteunen.[5] Deze ontwikkeling gaat hand in hand met uitdagingen op het vlak van gegevensbescherming. Zo moet er gewaakt worden over de adequate bescherming van persoonsgegevens van EU-inwoners bij elke doorgifte ervan buiten de Europese Unie.[6] Voorgaande vloeit voort uit de Algemene Verordening Gegevensbescherming (AVG) die de Europese Unie in 2016 aannam. Met de AVG wil men alle personen die zich op het grondgebied van de Europese Unie bevinden, beschermen tegen het onrechtmatig verzamelen, gebruiken en opslaan van persoonlijk identificeerbare informatie door ondernemingen die zakendoen op het grondgebied van de EU.[7]

China, een van de grootste handelspartners van de EU, heeft zijn eigen gegevensbeschermingsregeling ontwikkeld met onder andere de Personal Information Protection Law (PIPL), die in 2021 in werking is getreden.[8] Gezien de grote aanwezigheid van Chinese producten en technologieën in de Europese Unie, worden er steeds meer gegevens uitgewisseld met China. Daarom is het voor ondernemingen en beleidsmakers van cruciaal belang om te

[4] META, 'How Meta Uses Legal Bases for Processing Ads in the EU', *Meta Newsroom,* 4 januari 2023, https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/ (geraadpleegd op 8 oktober 2024).
[5] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2023/1795 van de Commissie van 10 juli 2023 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, *Oj.L.* 20 september 2023, 198, http://data.europa.eu/eli/dec_impl/2023/1795/oj.
[6] Overw. 101, Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Hierna: AVG), *Pb.L.* 4 mei 2016, http://data.europa.eu/eli/reg/2016/679/oj.
[7] Art. 1 AVG.
[8] ACCESSIBLE LAW, 'Personal Information Protection Law of the People's Republic of China', *Personalinformationprotectionlaw,* 2021, https://personalinformationprotectionlaw.com (geraadpleegd op 14 oktober 2014).

begrijpen of China een niveau van gegevensbescherming te bieden heeft, dat in wezen gelijkwaardig is aan dat binnen de EU.

Een Chinese applicatie die gebruikmaakt van grensoverschrijdende gegevensstromen is TikTok. Dit is een socialmediaplatform waarop gebruikers korte video's met muziek, dans, komedie en andere genres kunnen maken en delen. Begin 2025 had TikTok wereldwijd ongeveer 1,5 miljard maandelijks actieve gebruikers, waarvan 159 miljoen in de Europese Unie, waarmee het een hoge positie inneemt tussen andere socialemediaplatformen.[9]

Voor doorgiften van persoonsgegevens naar landen buiten de EU is op grond van de AVG altijd een van de drie doorgiftemechanismen vereist: een adequaatheidsbesluit, passende waarborgen of een afwijking voor specifieke situaties.[10] Deze Chinese ondernemingen kunnen hoe dan ook niet terugvallen op een adequaatheidsbesluit voor hun gegevensoverdrachten, aangezien de Europese Commissie geen adequaatheidsbesluit heeft vastgesteld ten aanzien van China. Zij moeten hun toevlucht nemen tot de passende waarborgen voor de doorgifte van persoonsgegevens vanuit de EU, zoals standaardcontractbepalingen (SCC's) of bindende bedrijfsvoorschriften (BCR's). Hierbij rijst de vraag of de persoonsgegevens van EU-inwoners in de praktijk werkelijk beschermd zijn wanneer ze naar China worden doorgegeven. Hoewel SCC's en BCR's wettelijke middelen zijn, hangt de effectiviteit af van de aanvullende maatregelen die ondernemingen nemen om bescherming te bieden.[11] Daarom is het essentieel om te onderzoeken welke aanvullende maatregelen deze ondernemingen nemen, zoals versleuteling of pseudonimisering.

Afdeling 2. Onderzoeksvragen

In dit kader rijst de hoofdonderzoeksvraag: "*Hoe wordt het recht op gegevensbescherming van alle personen binnen de Europese Unie gewaarborgd bij de doorgifte van persoonsgegevens van de EU naar China door een Chinese onderneming zoals TikTok?*" Om de hoofdonderzoeksvraag te

[9] DIXON S.J., 'Most popular social networks worldwide as of February 2025, by number of monthly active users', *Statista* 26 maart 2025, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (geraadpleegd op 15 april 2025); TIKTOK, 'Digital Services Act: Our fourth transparency report on content moderation in Europe', *TikTok Newsroom* 28 ferbuari 2025, https://newsroom.tiktok.com/en-eu/digital-services-act-our-fourth-transparency-report-on-content-moderation-in-europe (geraadpleegd op 15 april 2025).
[10] Art. 45-49 AVG.
[11] HvJ 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, 'Data Protection Commissioner/Facebook Ireland en Schrems', §133; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §50, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

beantwoorden, moeten er een aantal subonderzoeksvragen beantwoord worden. De subonderzoeksvragen zijn de volgende:

1. Wat zijn de vereisten of beperkingen voor de doorgifte van persoonsgegevens naar derde landen volgens de Algemene Verordening Gegevensbescherming (AVG)?
2. Voldoet het Chinese raamwerk aan een passend beschermingsniveau dat in wezen gelijkwaardig is aan het niveau dat binnen de Unie wordt gewaarborgd?
3. Welke technieken gebruiken de Chinese ondernemingen om toch persoonsgegevens door te geven en zijn er problemen te identificeren?

Afdeling 3. Onderzoeksmethodologie

In dit onderzoek wordt het Chinese juridische kader inzake gegevensoverdracht geanalyseerd en getoetst aan de Europese vereisten. Hiervoor worden de AVG en de PIPL bestudeerd. De PIPL uit China wordt onderzocht op basis van de Engelse vertaling die beschikbaar is op de officiële website van het Nationale Volkscongres van de Volksrepubliek China.[12] De keuze om te vertrekken van een officiële vertaling is bewust gemaakt om de nauwkeurigheid van de wettekst te garanderen. In deze masterscriptie wordt er een officieuze letterlijke vertaling gebruikt, die gegenereerd is met behulp van de vertaalsoftware *DeepL*. Ondanks dat deze aanpak het lezen vergemakkelijkt, is het belangrijk om rekening te houden met mogelijke problemen. Juridische termen worden namelijk niet altijd accuraat weergegeven door machinevertalingen. Daarnaast kunnen kleine verschillen in formulering de juridische betekenis van specifieke bepalingen beïnvloeden.[13] Om deze risico's te beperken, werd de vertaalde tekst getoetst aan mijn eigen kennis van het Engels.

Het onderzoek zal zowel beschrijvend als evaluerend zijn. Het zal eerst een grondige beschrijving geven van de relevante wet- en regelgeving in elk rechtsgebied, en vervolgens kritisch beoordelen of het gegevensbeschermingsregime van China kan voldoen aan de bescherming die de EU vereist voor internationale gegevensoverdrachten. Uiteindelijk zal er een beschrijvende en evaluatieve analyse worden uitgevoerd op het privacybeleid en het doorgifte-instrument die wordt gebruikt

[12] THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA, 'Personal Information Protection Law of the People's Republic of China', *NPC GOV* 29 december 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (geraadpleegd op 10 oktober 2024).
[13] PIETERS D. en DEMARSIN B., *Rechtsvergelijking: de uitdagende wereld van het recht*, Acco, 2023, 63-65.

door TikTok. Vervolgens wordt er geëvalueerd of deze maatregelen de persoonsgegevens effectief beschermen.

Afdeling 4. Structuur

In het eerste deel van het onderzoek wordt het wettelijke kader voor gegevensoverdracht binnen de Europese Unie onderzocht, met speciale aandacht voor de vereisten van de AVG voor een adequaat niveau van gegevensbescherming in derde landen. Vervolgens worden de Chinese wetten op het gebied van gegevensbescherming in kaart gebracht, in het bijzonder de PIPL, om te beoordelen of de bepalingen ervan gelijken op deze van de AVG. De analyse onderzoekt ook in welke mate het Chinese wetgevingskader tekortkomingen vertoont vergeleken met de Europese vereisten voor gegevensbescherming. Tot slot wordt onderzocht hoe de Chinese onderneming, ByteDance (TikTok), omgaat met grensoverschrijdende gegevensoverdrachten.

Hoofdstuk: 1 Wettelijk kader Europese Unie

Afdeling 1. Inleiding

Gegevensbescherming is in de Europese Unie erkend als een fundamenteel recht en wordt specifiek beschermd door artikel 8 van het Handvest van de grondrechten van de Europese Unie.[14] In 2016 introduceerde de EU de AVG, de opvolger van de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Uit artikel 1 van de AVG blijkt dat de verordening onder andere tot doel heeft de veilige doorgifte van persoonsgegevens binnen de EU te garanderen.[15] Maar dankzij de digitalisering worden persoonsgegevens ook vaker naar derde landen getransporteerd. Ook in deze gevallen waarborgt de AVG het fundamentele recht op gegevensbescherming.[16] In dit hoofdstuk wordt eerst de definitie van een gegevensoverdracht afgebakend. Vervolgens worden de verschillende trajecten voor een grensoverschrijdende overdracht besproken. Tot slot wordt het beschermingsniveau en de vereisten om een gelijkwaardig niveau te bereiken onderzocht.

Afdeling 2. Definiëring gegevensoverdracht

Om te bepalen wanneer artikel 44 AVG (en de andere bepalingen van hoofdstuk V AVG) van toepassing zijn, is het belangrijk om te weten wanneer er sprake is van een "doorgifte van persoonsgegevens naar een derde land".[17] De meest voor de hand liggende plaats om een definitie te vinden is de AVG, maar daar wordt geen enkele definitie aangereikt. Ook in de rechtspraak is er nog geen definitieve uitspraak gedaan. Evenwel heeft het Hof van Justitie van de EU (HvJ-EU) de kwestie reeds besproken in de zaken *Lindqvist*, *Schrems I*, *Schrems II* en *Bindl*.

In de zaak *Lindqvist* suggereert het Hof van Justitie dat een gegevensdoorgifte een actieve handeling moet zijn waarbij gegevens worden verzonden, en niet alleen passief toegankelijk

[14] Art. 8 Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj.
[15] Art. 1 AVG.
[16] Art. 44 AVG.
[17] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG, 14 februari 2023, 05/2021, 3, https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_nl.pdf.

worden gemaakt.[18] Maar de vraag rijst of dit wel relevant is aangezien er kan worden geconcludeerd dat dit beïnvloed is door de specifieke omstandigheden van de zaak.[19] In de zaak *Bindl* tegen Europese Commissie van januari 2025 heeft het Gerecht van de Europese Unie een duidelijke definitie gegeven. Het hof benadrukte dat een doorgifte drie cumulatieve elementen vereist die sterk gelijken op de definitie van de EDPB.[20] Wat opmerkelijk is, is dat opnieuw wordt verduidelijkt dat het loutere risico van toegang tot persoonsgegevens door instanties in een derde land op zichzelf nog geen doorgifte vormt.[21] Het is dus noodzakelijk dat er een daadwerkelijke handeling heeft plaatsgevonden waarbij de gegevens beschikbaar zijn gesteld aan een ontvanger in een derde land. Deze interpretatie sluit uit dat hypothetische of potentiële toegang onder de wettelijke definitie van een doorgifte valt.

Het Europees Comité voor gegevensbescherming (EDPB) heeft ook een definitie aangereikt in de Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG.[22] Zo zijn er drie cumulatieve criteria om de reikwijdte te definiëren:

1) Een verwerkingsverantwoordelijke of een verwerker ("exporteur") valt voor de bepaalde verwerkingsactiviteit onder de AVG.
2) Persoonsgegevens die het voorwerp van deze verwerking zijn, worden door de exporteur door middel van doorzending verstrekt of op andere wijze ter beschikking gesteld aan een andere verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke of verwerker ("importeur").
3) De importeur bevindt zich in een derde land (ongeacht of deze importeur al dan niet voor de bepaalde verwerkingsactiviteit overeenkomstig artikel 3 onder de AVG valt) of is een internationale organisatie.

De definitie van de EDPB beperkt op deze manier de reikwijdte van wat een doorgifte vormt door zich specifiek te richten op verwerkingsverantwoordelijken of verwerkers buiten de EU. In deze

[18] HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, 'Bodil Lindqvist', §71.
[19] KUNER C., BYGRAVE L.A., DOCKSEY C. en DRECHSLER L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, 762-763.
[20] Ger.EU 8 januari 2025, T-354/22, 'Thomas Bindl/Europese Commissie', §95.
[21] Ibid, §135.
[22] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG, 14 februari 2023, 05/2021, 8, https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_nl.pdf.

richtsnoeren wordt er niet aangegeven of de gegevensexporteur de intentie moet hebben om persoonsgegevens door te geven.

De EDPB speelt een cruciale rol bij het interpreteren van de AVG. Het heeft de bevoegdheid om op eigen initiatief of op verzoek van de Europese Commissie richtlijnen en aanbevelingen uit te vaardigen.[23] Ondanks dat deze richtlijnen invloedrijk zijn, zijn ze niet wettelijk bindend.[24] Het HvJ-EU heeft de uiteindelijke bevoegdheid om EU-wetgeving te interpreteren en is dus niet verplicht om de interpretaties van de EDPB te volgen.[25]

De masterscriptie zal zich baseren op de definitie van de EDPB, aangevuld met de vereiste die uit de *Lindqvist* en de *Bindl* zaak voortvloeit. Namelijk dat een daadwerkelijke handeling van het beschikbaar stellen van de gegevens aan een ontvanger in een derde land moet plaatsvinden, waardoor hypothetische of potentiële toegang niet onder de juridische definitie van een gegevensdoorgifte valt.

Afdeling 3. Trajecten grensoverschrijdende gegevensoverdracht

Onderafdeling 1. Algemeen

In hoofdstuk V AVG zijn er drie trajecten terug te vinden om rechtmatig persoonsgegevens over te dragen aan derde landen en tegelijkertijd de gegevensbescherming te handhaven. Allereerst kan het zijn dat de Europese Commissie een adequaatheidsbesluit heeft uitgevaardigd voor het land waarnaar de gegevensexporteur persoonsgegevens wil overdragen.[26] Met dit besluit bevestigt de Europese Commissie dat een land een adequaat niveau van gegevensbescherming biedt, waardoor doorgiftes zonder aanvullende waarborgen kunnen plaatsvinden. Ten tweede, indien er geen adequaatheidsbesluit bestaat voor het derde land, kunnen de persoonsgegevens nog steeds worden doorgegeven indien de gegevensbescherming op een andere manier kan worden gegarandeerd. Dit kan met passende waarborgen zoals onder andere een standaardcontractbepaling (SCC's) of bindende bedrijfsvoorschriften (BCR's).[27] Tot slot zijn er afwijkingen, namelijk de uitzonderlijke

[23] VOIGT P., VON DEM BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide,* Springer, 2024, 271.
[24] DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 12.
[25] Art. 267 Verdrag betreffende de werking van de Europese Unie*, Pb.C.* 7 juni 2016.
[26] Art. 45 AVG.
[27] Art. 46-47 AVG.

gevallen die gegevensdoorgiften toestaan op basis van specifieke omstandigheden, zoals de uitdrukkelijke toestemming van de betrokkene.[28] Hierna zal elk traject nader onderzocht worden.

Figuur 1: De drie rechtmatigheidsgronden voor internationale gegevensdoorgiften

[28] Art. 49 AVG.

Onderafdeling 2. Doorgiften op basis van adequaatheidsbesluiten (Artikel 45 AVG)

Een adequaatheidsbesluit is een instrument dat uitgevaardigd moet worden door de Europese Commissie na een analyse van de regelgeving die van toepassing is op de importeurs en de rechtsregels die overheidsinstanties toegang geven tot deze gegevens.[29] Zodra er een besluit bestaat voor een land moeten exporteurs geen aanvullende waarborgen of voorwaarden meer opnemen om persoonsgegevens door te geven aan dit derde land.[30]

De EDPB heeft in dit scenario de rol van adviesorgaan en dient zo de Europese Commissie te voorzien van een onafhankelijk advies over het gegevensbeschermingsniveau van het betreffende derde land.[31] De Commissie zal daarna stemmen over het ontwerpadequaatheidsbesluit op basis van diens adviezen en de adviezen van het Europees Parlement.[32] Maar deze is niet verplicht de adviezen te volgen.[33] Zo heeft de Commissie niet ten volle rekening gehouden met hun bezwaren bij het *Privacy Shield*, maar ook andere adequaatheidsbesluiten zoals deze van Japan.[34] Wat het *Privacy Shield* betreft, heeft politieke druk van de Amerikaanse regering de Commissie ertoe bewogen het besluit snel goed te keuren, ook al hadden de voorganger van de EDPB, het Europees Parlement en de Europese Toezichthouder voor gegevensbescherming bedenkingen bij de geschiktheid van de Amerikaanse beschermingsmaatregelen.[35] Ook in het geval van Japan heeft de Commissie, ondanks zorgen over de doeltreffendheid van de toezichtsmaatregelen en het

[29] Art. 45, tweede en derde lid AVG.
[30] PHILLIPS M., 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)', *Hum Genet* 2018, (575) 579; ROTH P., 'Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation', *Journal of Law, Information and Science* 2017, (49) 56.
[31] Art. 70(1)(s) AVG.; VAN DEN BULCK P., 'Transfers of personal data to third countries', *ERA Forum* 2017, (229) 236.
[32] Art. 5 Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren, *Pb.L.* 28 februari 2011, http://data.europa.eu/eli/reg/2011/182/oj.
[33] DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 12.
[34] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Advies 5/2023 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, 28 februari 2023, 5/2023, https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_nl.pdf; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan, 18 juli 2023, 1/2023, 3, https://www.edpb.europa.eu/system/files/2023-07/edpb_statement_202301_statement_on_japan_adequacy_review_en.pdf.
[35] ROTH P., 'Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation', Journal of Law, *Information and Science* 2017, (49) 61-62.

Japanse handhavingsregime, toch het besluit inzake adequaatheid genomen, deels onder invloed van handelsbesprekingen.[36]

De adequaatheidsbesluiten die uitgevaardigd zijn, zijn onderworpen aan een periodieke beoordeling.[37] Meer bepaald zal de Europese Commissie minimum om de vier jaar een onderzoek moeten voeren of het adequaatheidsbesluit nog gerechtvaardigd is en zal hierbij kijken naar alle relevante ontwikkelingen in het derde land.[38] Indien bij deze beoordeling blijkt dat het derde land niet meer in staat is een voldoende beschermingsniveau te garanderen, moet de Europese Commissie verplicht het besluit intrekken, wijzigen of opschorten.[39] Daarna zal een overlegprocedure gestart worden om de situatie proberen te verhelpen.[40] Het HvJ heeft al twee adequaatheidsbesluiten voor de VS vernietigd: eenmaal na het *Schrems* I-arrest, waarbij de *Safe Harbor* tussen de EU en de VS ongeldig werd verklaard, en later na het *Schrems* II-arrest, waarbij het *Privacy Shield* tussen de EU en de VS ongeldig werd verklaard.[41] Daarnaast heeft de Commissie reeds zes rapporten gepubliceerd met betrekking tot de periodieke beoordeling. Namelijk een rapport over het adequaatheidsbesluit van Japan[42], de elf adequaatheidsbesluiten[43], drie rapporten die het *Privacy Shield* evalueren[44] en één rapport die het nieuwe EU-VS adequaatheidsbesluit evalueert[45].

---

[36] VOSS W., 'Cross-border data flows, the GDPR, and data governance', *Wash. Int'l L.J.* 2020, (485) 516-517.
[37] Art. 45, derde lid AVG.
[38] Art. 45, derde lid AVG; VAN DEN BULCK P., 'Transfers of personal data to third countries', *ERA Forum* 2017, (229) 236.
[39] Art. 45, vijfde lid AVG.
[40] Art 45, zesde lid AVG.
[41] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §106; HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §201.
[42] EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste evaluatie van de werking van het adequaatheidsbesluit voor Japan, 3 april 2023, COM(2023) 275, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52023DC0275.
[43] EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste evaluatie van de adequaatheidsbesluiten die zijn vastgesteld op grond van artikel 25, lid 6, van Richtlijn 95/46/EG, 15 januari 2024, COM(2024) 7, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52024DC0007.
[44] EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste jaarlijkse evaluatie van de werking van het EU-VS-privacyschild, 18 oktober, 2017, COM(2017) 611, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017DC0611; EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de tweede evaluatie van de werking van het EU-VS-privacyschild, 19 december, 2018, COM(2018) 860, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0860; EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de derde jaarlijkse evaluatie van de werking van het EU-VS-privacyschild, 23 oktober, 2019, COM(2019) 495, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52019DC0495.
[45] EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste periodieke evaluatie van de werking van het adequaatheidsbesluit inzake het kader voor gegevensbescherming EU-VS, 9 oktober 2024, COM(2024) 451, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52024DC0451.

Momenteel zijn er vijftien adequaatheidsbesluiten.[46] De betrokken landen zijn: Andorra, Argentinië, Canada, Faeröer Eilanden, Guernsey, Isle of Man, Israël, Japan, Jersey, Nieuw-Zeeland, Uruguay, Verenigd Koninkrijk, Verenigde Staten, Zwitserland en Zuid-Korea. Er bestaat tot op de dag van vandaag nog geen adequaatheidsbesluit voor China, waardoor ondernemingen die gegevens willen exporteren vanuit de EU naar China de zes stappen van de DTIA (infra: Afdeling 4) moeten doorlopen om te verzekeren dat hun doorgifte-instrument effectief zal zijn in het bieden van het adequate beschermingsniveau. In hoofdstuk 2, afdeling 6 wordt ingegaan op de vraag of China in aanmerking zou kunnen komen voor een adequaatheidsbesluit. Hierbij zal worden onderzocht of China voldoet aan de eisen die de EU stelt op het gebied van gegevensbescherming.

Onderafdeling 3. Doorgiften op basis van passende waarborgen (Artikel 46 AVG)

Indien er geen adequaatheidsbesluit voorhanden is, kunnen de ondernemingen teruggevallen op de zes verschillende instrumenten uit artikel 46 AVG.[47] Ook hier moet worden verzekerd dat er een passend beschermingsniveau wordt geleverd door de importeurs.[48] Partijen moeten passende waarborgen, afdwingbare rechten en doeltreffende rechtsmiddelen voor betrokkenen kunnen waarborgen.[49] Hieronder worden de instrumenten besproken die het meest gebruikt worden in de praktijk.

a) Bindende bedrijfsvoorschriften (BCR's) (Artikel 47 AVG)

De bindende bedrijfsvoorschriften (hierna: BCR's), geïntroduceerd door de Artikel 29 Werkgroep[50] en bevestigd in de AVG, zijn zoals artikel 4, 20) AVG beschrijft een beleid dat moet worden nageleefd door in de EU gevestigde ondernemingen, voor overdrachten van persoonsgegevens buiten de EU binnen een groep ondernemingen of een groep ondernemingen

[46] EUROPESE COMMISSIE, 'Adequacy decisions', https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=nl (geraadpleegd op 8 oktober 2024).
[47] Art. 46 AVG.
[48] Art. 44 AVG.
[49] BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 18.
[50] GROEP GEGEVENSBESCHERMING ARTIKEL 29,, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74, 3 juni 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf.

die gezamenlijk een economische activiteit verrichten.[51] De EU heeft dit instrument ontwikkeld om ondernemingen die in meerdere landen actief zijn de mogelijkheid te geven om tussen hun organisaties persoonsgegevens door te geven.[52]

b) Standaardcontractbepalingen (SCC's)

Standaardcontractbepalingen (hierna SCC's) zijn gestandaardiseerde modelovereenkomsten die vooraf goedgekeurd zijn door de Europese Commissie waarmee ondernemingen gegevens kunnen overdragen naar landen buiten de EU.[53] In zulke overeenkomsten worden verplichtingen opgenomen voor enerzijds de gegevensexporteur en anderzijds de gegevensimporteur.[54] Daarnaast zijn er ook aansprakelijkheden voorzien, indien men de verplichtingen niet zou nakomen.[55] Partijen mogen dus niet afwijken van de standaardcontractbepalingen, evenwel kunnen ze nadere invulling geven via bijlagen in het contract.[56]

Onderafdeling 4. Doorgiften op basis van afwijkingen (Artikel 49 AVG)

Tot slot moet er nog vermeld worden dat een gegevensoverdracht ook kan plaatsvinden zonder een adequaatheidsbesluit of passende waarboven als men zich in een van de situaties bevindt, opgesomd in artikel 49 AVG.[57] Deze uitzonderingen zijn voorzien indien bijvoorbeeld het publieke belang de bovenhand neemt op het recht op privacy. In de Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679 wordt wel benadrukt dat deze afwijkingen restrictief geïnterpreteerd moeten worden, beperkt zijn tot sommige gevallen en een niet-repetitief karakter mogen hebben.[58] Het voortdurend doorgeven van persoonsgegevens aan een derde land kan dus niet worden geplaatst onder de strikte uitzonderingen.

---

[51] Art. 4(20) AVG.
[52] PHILLIPS M., International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR*). Hum Genet* 2018, (575) 580.
[53] VOIGT P., VD BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing, 2017, 119.
[54] DE BOER D.S., 'Internationale doorgifte van persoonsgegevens: aandachtspunten bij het gebruik van modelcontracten', *Contracteren* 2021, (105) 109.
[55] Ibid.
[56] VOIGT P., VON DEM BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide,* Springer, 2024, 120.
[57] Art. 49 AVG.
[58] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 2/2018, 25 mei 2018, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_nl.pdf.

Afdeling 4. Gelijkwaardig beschermingsniveau

Wanneer persoonsgegevens vanuit de Europese Unie worden doorgegeven naar derde landen stelt de AVG duidelijke eisen. De kern van deze vereisten is dat persoonsgegevens ook buiten de EU moeten worden beschermd volgens een niveau dat "in wezen gelijkwaardig" is aan het beschermingsniveau binnen de EU.[59] De fundamentele rechten en vrijheden van betrokkenen mogen dus niet in gedrang komen bij deze gegevensdoorgifte. Om deze gelijkwaardige bescherming te waarborgen, voorziet de AVG in verschillende trajecten die in afdeling 3 toegelicht werden. Zo kan bij het ontbreken van een adequaatheidsbesluit gebruik worden gemaakt van passende waarborgen, zoals SCC's.

Het belang van dergelijke passende waarborgen kwam scherp naar voren in het *Schrems II* arrest. Dit arrest had namelijk niet enkel gevolgen voor het *Privacy Shield* en de Verenigde Staten, maar wierp ook bredere vragen op over de doorgifte van persoonsgegevens naar derde landen in het algemeen.[60] In deze zaak heeft het HvJ-EU de geldigheid van de SCC's beoordeeld. Het Hof is tot de conclusie gekomen dat de SCC's een rechtmatig mechanisme blijven voor de doorgifte van gegevens buiten de Europese Unie. Het benadrukte echter dat er aanvullende maatregelen moeten worden geïmplementeerd om de gegevensbescherming te verzekeren wanneer gegevens worden doorgegeven op basis van SCC's.[61]

Uit deze zaak vloeit voort dat gegevensexporteurs vanaf nu de opdracht hebben om het niveau van gegevensbescherming in het ontvangende land te evalueren.[62] Het Hof oordeelde dat het rechtsgebied waarnaar de gegevens worden doorgegeven een beschermingsniveau moet bieden dat "in wezen gelijkwaardig" is aan het niveau dat in de EU wordt gewaarborgd.[63] Dit vereist dus geen identiek beschermingsniveau.[64] Het Hof heeft verschillende factoren opgesomd waarmee een

[59] Art. 45 en overw. 104 AVG.; HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94.
[60] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §201.
[61] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §133; BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 22.
[62] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §134.
[63] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94.
[64] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94.

gegevensexporteur rekening moet houden zoals de contractuele verplichtingen van de gegevensimporteur, het rechtssysteem van het derde land (met inbegrip van zijn wetgeving inzake privacy, gegevensbescherming en mogelijke praktijken van overheidstoezicht die de rechten van de betrokkenen kunnen aantasten) en de factoren die zijn opgesomd in artikel 45, lid 2, van de GDPR (zoals de rechtsstaat, gerechtelijke verhaalmechanismen en het bestaan van onafhankelijke toezichthoudende autoriteiten die verantwoordelijk zijn voor de handhaving van gegevensbescherming).[65]

Aangezien overheidsinstanties geen partij zijn bij de SCC's tussen de gegevensimporteur en de gegevensexporteur, kunnen de SCC's de overheidsinstanties niet binden.[66] Daarom heeft het HvJ-EU uitdrukkelijk verklaard dat de verantwoordelijkheid bij de exporteur ligt om na te gaan of het rechtskader van het ontvangende land een passend beschermingsniveau biedt.[67] Als de exporteur vaststelt dat de SCC's alleen onvoldoende bescherming bieden, moet hij aanvullende maatregelen nemen om naleving te waarborgen. Als noch de SCC's noch de aanvullende maatregelen het vereiste beschermingsniveau kunnen garanderen, moet de doorgifte van persoonsgegevens worden opgeschort of beëindigd.[68]

Na het *Schrems* II-arrest heeft de EDPB aanbevelingen gepubliceerd om organisaties te begeleiden bij het bepalen van de juiste bescherming voor gegevensoverdrachten.[69] Het heeft onder andere aanvullende maatregelen voorgesteld zoals technische waarborgen, contractuele waarborgen en organisatorische waarborgen.

Volgend op dit arrest heeft de Europese Commissie op 4 juni 2021 gemoderniseerde SCC's uitgevaardigd voor overdrachten van verwerkingsverantwoordelijken of verwerkers in de EU aan verwerkingsverantwoordelijken of verwerkers buiten de EU.[70] Dit bracht een aantal

[65] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §105.
[66] BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 19.
[67] NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 184.
[68] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §135.
[69] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §22, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.
[70] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening

vernieuwingen met zich mee. Een eerste belangrijk verschil is dat de SCC's nu vier verschillende doorgiftescenario's dekken, wat de toepasbaarheid ervan aanzienlijk verruimt.[71] Daarnaast krijgen betrokkenen een versterkte positie doordat zij als derde-begunstigden rechtstreeks rechten uit de SCC's kunnen afdwingen en schadevergoeding kunnen eisen van zowel de gegevensimporteur- als exporteur.[72] Ook nieuw is dat gegevensimporteurs in derde landen bijkomende verplichtingen hebben wanneer overheidsinstanties toegang tot persoonsgegevens eisen.[73] In dat geval moeten ze een risicoanalyse uitvoeren en aantonen dat zij aan de SCC's kunnen voldoen, ondanks de lokale wetgeving. Tot slot is er een versterkte verantwoordingsplicht ingevoerd, waarbij partijen moeten kunnen aantonen dat de doorgifte plaatsvindt in overeenstemming met de contractuele bepalingen en met voldoende waarborgen.[74]

Onderafdeling 1. Stappenplan EDPB

De vraag rijst nu hoe ondernemingen kunnen achterhalen welke soort passende waarborgen ze moeten nemen en welke aanvullende maatregelen nodig zijn. Er wordt dus gezocht naar criteria die leiden tot de juiste passende waarborgen.

Het Hof van Justitie heeft geoordeeld dat alle beschermingsmechanismes die ondernemingen zouden kiezen, moeten verzekeren dat de gegevens die overgedragen worden een gelijkwaardige adequate bescherming zouden genieten.[75] Het Hof wijst hiervoor de verwerkers en de verwerkingsverantwoordelijken aan die optreden als gegevensexporteurs om te onderzoeken of de wetgeving en de praktijk van het derde land adequate bescherming biedt die "in wezen gelijkwaardig" is aan de EU-wetgeving.[76] De EDPB vaardigde een richtlijn uit voor het uitvoeren

(EU) 2016/679 van het Europees Parlement en de Raad, *Pb.L.* 7 juni 2021, http://data.europa.eu/eli/dec_impl/2021/914/oj.

[71] DE BOER D.S., 'Internationale doorgifte van persoonsgegevens: aandachtspunten bij het gebruik van modelcontracten', *Contracteren* 2021, (105) 108.

[72] Ibid., 109.

[73] Ibid., 112.

[74] Ibid, 111.

[75] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §22, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[76] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §134.

van een beoordeling, die in de praktijk onder advocaten en ondernemingen al snel de naam "*Data Transfer Impact Assessment*" (DTIA) kreeg.[77]

Met een DTIA zal dus beoordeeld worden of een gegevensimporteur in staat zal zijn om te voldoen aan de verplichtingen die voortvloeien uit het overdrachtsinstrument, in het licht van de wetgeving en praktijken van het derde land.[78] Indien er risico's geïdentificeerd zouden worden, moeten deze gecompenseerd worden door aanvullende maatregelen te nemen.[79] Volgens de Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, zijn er zes fases om deze beoordeling te doorlopen.[80] In figuur 2 worden deze stappen gevisualiseerd.

In de eerste fase geeft de EDPB de aanbeveling aan gegevensexporteurs om op de hoogte te zijn van wat er precies doorgegeven wordt. Men moet de doorgiften van de persoonsgegevens in kaart brengen en weten waar de gegevens terechtkomen.[81] Daarbij moet men erover waken dat de gegevens die doorgegeven worden passend, relevant en tot het noodzakelijke beperkt zijn voor het doel waarvoor ze worden verwerkt.[82]

In de tweede fase moet men het doorgifte-instrument controleren dat men gebruikt voor de doorgiften aan de hand van de lijst in hoofdstuk V van de AVG.[83]

---

[77] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §134; DE BOER D.S., 'Internationale doorgifte van persoonsgegevens: aandachtspunten bij het gebruik van modelcontracten', *Contracteren* 2021, (105) 112; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[78] SANFUCHS B., 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II', *GRUR International* 2021, (245) 247.

[79] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §133.

[80] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[81] DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 14.

[82] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §8, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[83] Ibid., §14.

Ten derde moet men het recht en/of de geldende praktijken van het derde land beoordelen en zo achterhalen of deze elementen omvatten die afbreuk doen aan de doeltreffendheid van de passende waarborgen van de gebruikte doorgifte-instrumenten.[84] Dit betekent dus dat de desbetreffende gegevensexporteurs op zoek moeten gaan naar rechtsbronnen van de EU, nationale rechtsbronnen, adequaatheidsbesluiten, om zo de wetgeving en de praktijk te onderzoeken.[85] Dit kan veel tijd en kosten met zich meebrengen.

Ten vierde moet men kiezen of en welke aanvullende maatregelen nodig zijn om te voldoen aan het in wezen gelijkwaardig beschermingsniveau.[86] Bijlage 2 geeft een exemplatieve lijst met aanvullende maatregelen en de voorwaarden om deze toe te passen. Indien er geen enkele aanvullende maatregel geschikt lijkt, moet overwogen worden om de gegevens niet door te geven.

In de vijfde stap neemt men de formele procedurele stappen voor het toepassen van de aanvullende maatregel.[87]

Ten slotte moet het beschermingsniveau periodiek worden beoordeeld.[88] Zo moeten de ontwikkelingen in het derde land nauwgezet in de gaten worden gehouden om de aanvullende maatregelen te evalueren.[89]

Onderafdeling 2. Soorten aanvullende maatregelen

Aanvullende maatregelen zijn extra waarborgen die ondernemingen moeten nemen wanneer ze persoonsgegevens doorgeven naar derde landen indien de bestaande doorgifte-instrumenten uit artikel 46 van de AVG, zoals SCC's, alleen niet voldoende bescherming bieden.[90] Deze

[84] Ibid., §30.
[85] Ibid., §144; DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 14.
[86] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §50, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.
[87] Ibid., §59.
[88] Ibid., §67-68.
[89] DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 16.
[90] Ibid., 15.

maatregelen moeten ervoor zorgen dat het beschermingsniveau van de gegevens in het derde land in grote lijnen overeenkomt met het niveau dat binnen de EU is gegarandeerd.[91]

Er bestaan drie soorten aanvullende maatregelen: technische, contractuele en organisatorische.

a) Technische maatregelen

Technische maatregelen zijn maatregelen die de gegevens zelf beschermen door middel van technologie, ongeacht wie toegang probeert te verkrijgen.[92] Het gaat hier bijvoorbeeld om versleuteling (een techniek waarbij persoonsgegevens worden omgezet zodat ze zonder een speciale sleutel of code niet meer leesbaar zijn[93]), pseudonimisering (een techniek waarbij persoonsgegevens worden bewerkt zodat ze niet meer direct aan een specifieke persoon kunnen worden gekoppeld[94]) of het splitsen van gegevens over meerdere verwerkers (een techniek zodat niemand zelfstandig toegang heeft tot het geheel[95]).[96] Deze maatregelen zijn noodzakelijk wanneer het risico bestaat dat overheidsinstanties in het derde land op basis van nationale wetgeving toegang kunnen krijgen tot gegevens, zonder dat dit noodzakelijk en evenredig is in een democratische rechtstaat. In zulke gevallen zijn technische maatregelen in staat om effectieve bescherming te bieden, want noch contractuele afspraken noch organisatorische maatregelen kunnen wettelijk bindend zijn voor buitenlandse autoriteiten.[97]

---

[91] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §96.

[92] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, §72-74, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[93] LI N.., OZSU M. en LIU L., *Encyclopedia of Database Systems,* Springer, 2018, 751.

[94] Art. 4(5) AVG; LI N.., OZSU M. en LIU L., *Encyclopedia of Database Systems,* Springer, 2018, 2932.

[95] FARRAS O., RIBES-GONZ´ALEZ J. en RICCI S., 'Privacy-preserving Data Splitting: A Combinatorial Approach', *Designs, Codes and Cryptography* 2018, (1) 1.

[96] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, §77-92, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 15.

[97] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §132; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §48 en 95, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 25.

b) Contractuele maatregelen

Contractuele maatregelen zijn afspraken die schriftelijk worden vastgelegd tussen de gegevensexporteur in de EU en de gegevensimporteur in het derde land.[98] Deze leggen verantwoordelijkheden en gedragingen vast die van de importeur worden verlangd.[99] Voorbeelden hiervan zijn verplichtingen tot transparantie over verzoeken van overheden, garanties dat er geen alternatieve toegang tot gegevens is ingebouwd, verplichtingen om gegevensverzoeken aan te vechten voor de rechter, en bepalingen om gegevens terug te zenden of te vernietigen als het beschermingsniveau niet meer kan worden gewaarborgd.[100] Contractuele maatregelen zijn vooral relevant wanneer het rechtskader van het derde land op zich niet problematisch is, maar er onzekerheid bestaat over hoe dat in de praktijk wordt toegepast. Ze zijn nuttig als aanvulling op technische maatregelen, maar kunnen zelden als enige maatregel volstaan omdat overheden niet gebonden zijn aan private contracten.[101]

a) Organisatorische maatregelen

Organisatorische maatregelen zijn beleidsmatige en procedurele waarborgen binnen de organisatie van de exporteur en/of importeur.[102] Bijvoorbeeld een intern beleid rond gegevensdoorgiften, duidelijke procedures bij toegangsvragen, beperking van toegang binnen de organisatie, periodieke audits, training van personeel, of het beperken van gegevensdoorgiften tot wat strikt noodzakelijk

[98] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §92, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.
[99] Ibid.
[100] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, §98-127, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 15.
[101] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §132; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §48 en 95, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 25.
[102] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §122, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

is.[103] Deze maatregelen zorgen ervoor dat afspraken in de praktijk correct worden uitgevoerd. Organisatorische maatregelen zijn met name relevant wanneer doorgiften plaatsvinden binnen een groep ondernemingen die gezamenlijk bij een economische activiteit zijn betrokken.[104] Ze kunnen de andere maatregelen ondersteunen en concreet maken.

De effectiviteit van de aanvullende maatregelen moet steeds worden beoordeeld in het licht van de specifieke context waarin een doorgifte plaatsvindt.[105] Daarbij spelen het rechtskader van het derde land, de aard van de persoonsgegevens en het doel van de verwerking een belangrijk rol.[106] Alleen wanneer deze maatregelen een beschermingsniveau kunnen garanderen dat in grote lijnen overeenkomt met het niveau binnen de EU, mag de doorgifte worden uitgevoerd.[107] Indien echter uit de beoordeling blijkt dat geen enkele maatregel of combinatie van maatregelen voldoende bescherming biedt, dan is het niet toegestaan om met de doorgifte te starten, en moet een lopende doorgifte onmiddellijk worden beëindigd.[108]

Aanvullende maatregelen hoeven in principe niet vooraf afzonderlijk te worden goedgekeurd door de bevoegde toezichthoudende autoriteit, op voorwaarde dat zij niet in strijd zijn met de bepalingen van het gebruikte doorgifte-instrument en het niveau van gegevensbescherming dat deze proberen te bieden.[109] Wel geldt dat deze maatregelen aantoonbaar doeltreffend moeten zijn. Zo moeten ze helder en ondubbelzinnig zijn geformuleerd.

---

[103] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, §128-143, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 15.

[104] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §124, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[105] Ibid., §46.

[106] Ibid., §49.

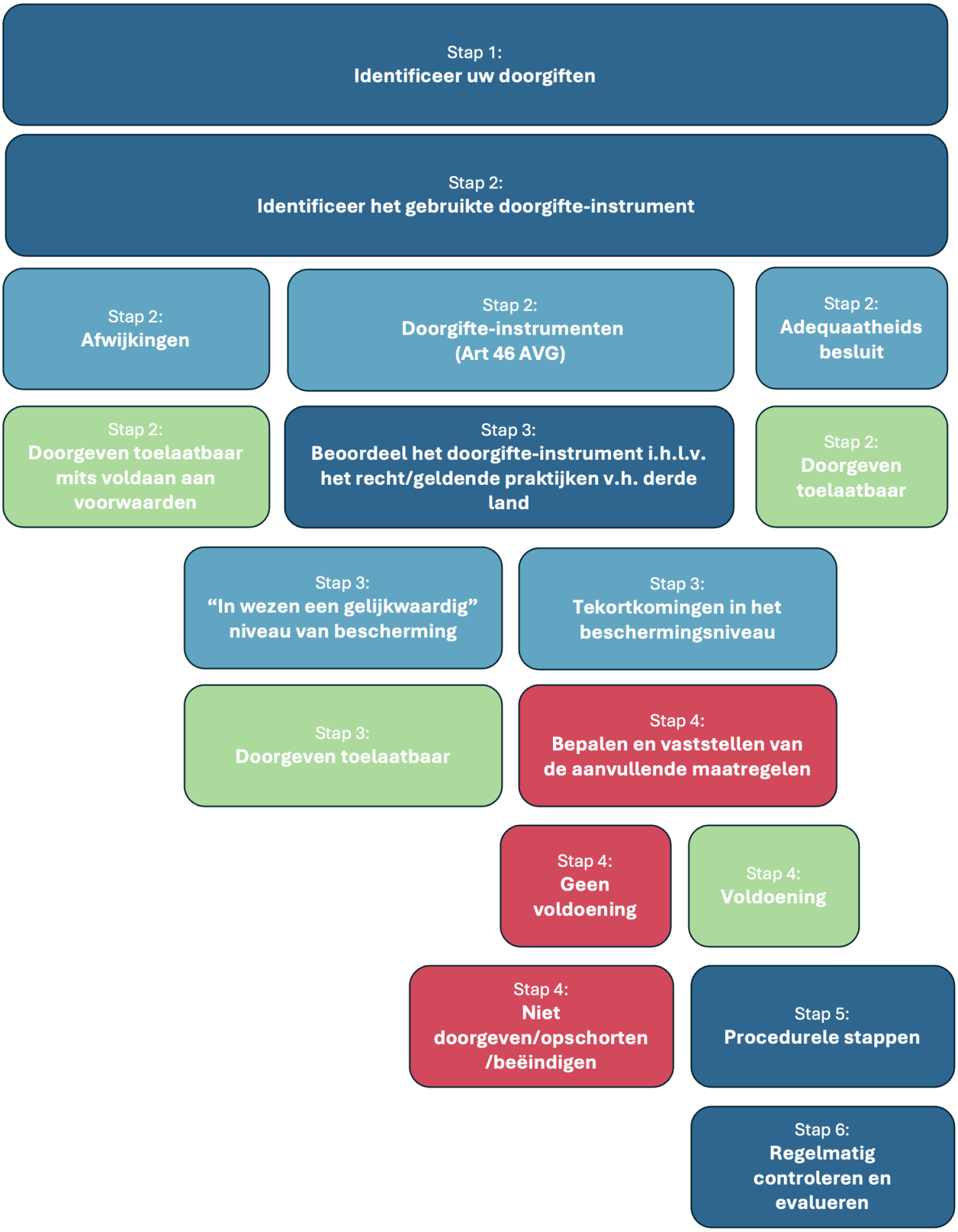
[107] Ibid., §51.

[108] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §135; EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §52, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

[109] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §56, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

In de nieuwe standaardcontractbepalingen van 4 juni 2021 is bovendien expliciet vereist dat de technische en organisatorische maatregelen die worden genomen om aanvullende bescherming te bieden, concreet en gedetailleerd worden beschreven in bijlage II bij de SCC's.[110] Het is niet voldoende om deze maatregelen op generieke of abstracte wijze te vermelden. Er moet duidelijk worden aangegeven welke specifieke maatregelen op welke doorgifte of reeks van doorgiften van toepassing zijn.

[110] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad, *Pb.L.* 7 juni 2021, 60 http://data.europa.eu/eli/dec_impl/2021/914/oj.

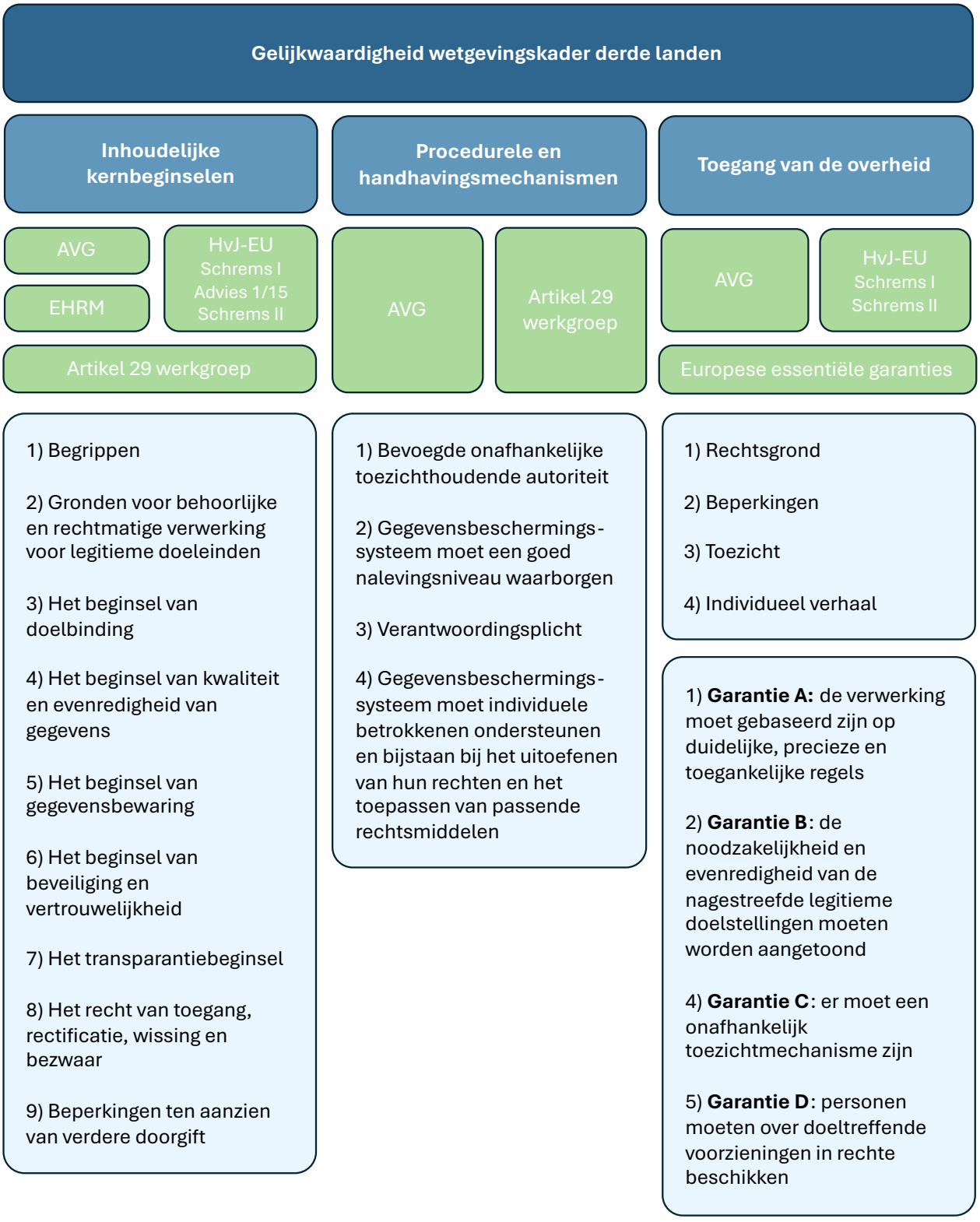


Figuur 2: Overzicht van de stappen van het EDPB over de maatregelen ter aanvulling op doorgifte-instrumenten

Afdeling 5. Vereisten voor een gelijkwaardig beschermingsniveau

Zoals uit afdeling 4 blijkt staat bij gegevensoverdrachten één concept centraal, namelijk de "in wezen gelijkwaardigheid". Het derde land moet een niveau van bescherming garanderen dat "in wezen gelijkwaardig" is aan de garanties die de wet in de Europese Unie biedt.[111] Hieronder zal toegelicht worden met welke elementen rekening dient gehouden te worden bij de beoordeling van een gegevensbeschermingsregime van een derde land. Dit kan achterhaald worden uit de bewoordingen in de AVG, de rechtspraak van het HvJ-EU en het EHRM, richtsnoeren van de Artikel 29 Werkgroep en de adequaatheidsbesluiten zelf. In deze masterscriptie wordt de structuur gevolgd die door de Artikel 29 Werkgroep wordt gehanteerd.[112] Telkens worden volgende drie elementen behandeld: 1) inhoudelijke kernbeginselen,[113] 2) procedurele en handhavingsmechanismen,[114] 3) toegang van de overheid.[115] Hieronder wordt voor een beter begrip van deze afdeling reeds een overzicht gegeven van de resultaten die volgen uit de analyse.

[111] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94.
[112] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie, 28 november 2017, WP 254 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54200.
[113] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 55; ROTH P., "Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation." *Journal of Law, Information and Science* 2017, (49) 52.
[114] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 62; ROTH P., "Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation." *Journal of Law, Information and Science* 2017, (49) 53.
[115] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 58; WAGNER J., 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?', *International Data Privacy Law* 2018, (318) 332.



Figuur 3: Overzicht analyse gelijkwaardigheidsniveau derde land

Onderafdeling 1. Inhoudelijke kernbeginselen

a) Algemene verordening gegevensbescherming (AVG)

In overweging 104 van de AVG wordt het passend beschermingsniveau beschreven als "*overeenkomend met het niveau dat in de Unie wordt verzekerd".*[116] Daarnaast specifieert artikel 45, lid 2 AVG een aantal aspecten waarmee rekening dient gehouden worden bij de beoordeling van de adequaatheid van het beschermingsniveau.[117] Zo moet de commissie bij het uitvaardigen van een adequaatheidsbesluit letten op:

> *a) de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke algemene en sectorale wetgeving, onder meer inzake openbare veiligheid, defensie, nationale veiligheid en strafrecht en de toegang van overheidsinstanties tot persoonsgegevens, evenals de tenuitvoerlegging van die wetgeving, gegevensbeschermingsregels, beroepsregels en veiligheidsmaatregelen, met inbegrip van regels voor de verdere doorgifte van persoonsgegevens aan een ander derde land of een andere internationale organisatie die in dat land of die internationale organisatie worden nageleefd, precedenten in de rechtspraak, alsmede het bestaan van effectieve en afdwingbare rechten van betrokkenen en effectieve mogelijkheden om administratief beroep of beroep in rechte in te stellen voor betrokkenen wier persoonsgegevens worden doorgegeven;*
>
> *b) het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten in het derde land of waaraan een internationale organisatie is onderworpen, welke tot taak heeft of hebben de naleving van de gegevensbeschermingsregels te verzekeren en deze onder meer met passende handhavingsbevoegdheden te handhaven, betrokkenen bij de uitoefening van hun rechten bij te staan en te adviseren en met de toezichthoudende autoriteiten van de lidstaten samen te werken; en*
>
> *c) de internationale toezeggingen die het derde land of de internationale organisatie in kwestie heeft gedaan, of andere verplichtingen die voortvloeien uit juridisch bindende*

[116] Overw. 104 AVG.
[117] Art. 45, tweede lid AVG.

overeenkomsten of instrumenten, alsmede uit de deelname van dat derde land of die internationale organisatie aan multilaterale of regionale regelingen, in het bijzonder met betrekking tot de bescherming van persoonsgegevens.

b) Hof van Justitie (HvJ-EU)

De bewoordingen in de AVG zijn niet helemaal duidelijk waardoor de rechtspraak van het Hof van Justitie bestudeerd dient te worden.

I. Schrems I (2015)

Voor de gegevensuitwisseling tussen de EU en Amerikaanse ondernemingen werd er gebruikgemaakt van de *Safe Harbor* (voorganger van *Privacy Shield*).[118] Hiermee werd vastgesteld dat het beschermingsniveau door de ondernemingen in de VS adequaat was. In 2015 viel Max Schrems de *Safe Harbor* aan omdat hij meende dat Amerikaanse wetgeving vergaande rechten verleende aan Amerikaanse inlichtingendiensten om persoonsgegevens te monitoren en te analyseren.[119] Uiteindelijke verklaarde het Hof van Justitie het *Safe Harbor* systeem ongeldig.[120]

Het Hof oordeelde meer bepaald dat zowel het recht op eerbiediging van het privéleven en het familie- en gezinsleven krachtens artikel 7 van het Handvest van de grondrechten van de Europese Unie als het recht op bescherming van persoonsgegevens krachtens artikel 8 van het Handvest van de grondrechten van de Europese Unie in het gedrang kwamen, aangezien de Amerikaanse wetgeving overheidsinstanties op algemene basis toegang verleende tot de inhoud van elektronische communicatie.[121] Zo was het *Safe Harbor Framework* alleen van toepassing op zelfgecertificeerde ondernemingen, met uitzondering van Amerikaanse overheidsinstanties.[122] De gegevensverwerkingsactiviteiten door overheidsinstanties vielen bijgevolg niet onder het wetgevend kader, wat het risico met zich meebracht op een verwerking van persoonsgegevens die

[118] COMPAGNUCCI M.C., ABOY M., MINSSEN T. en NAEF T., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs),* SSRN, 2021, 39; NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 56.
[119] BU-PASHA S., 'Cross-border issues under EU data protection law with regards to personal data protection.' *Information & Communications Technology Law* 2017, (213) 220.
[120] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §196; VOSS W., 'Cross-border data flows, the GDPR, and data governance', *Wash. Int'l L.J.* 2020, (485) 513.
[121] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §94.
[122] Ibid., §82.

in strijd was met de wettelijke vereisten van de EU.[123] Bovendien stipuleerde het *Safe Harbor Framework* dat het recht van de VS voorrang zou hebben in geval van conflicten tussen het *Framework* en het Amerikaans recht, zoals op het gebied van nationale veiligheid of openbaar belang.[124] Het Hof oordeelde dat een dergelijke algemene afwijking in strijd is met het beginsel van "strikt noodzakelijkheid".[125] Tot slot werd het recht op een doeltreffende voorziening in rechte krachtens artikel 47 van het EVRM geschonden, aangezien de Amerikaanse wetgeving personen geen rechtsmiddelen bood met betrekking tot de toegang tot en rectificatie of wissing van hun persoonsgegevens.[126]

Het Hof van Justitie heeft tevens verklaard dat de voorwaarde van een gelijkwaardige bescherming tot doel heeft het "*hoge niveau van deze bescherming te continueren bij doorgifte van persoonsgegevens naar een derde land*".[127] Daarnaast wordt het passend beschermingsniveau *"zo opgevat dat die vereist dat het derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat in grote lijnen overeenkomt met het niveau dat binnen de Unie wordt gewaarborgd op grond van richtlijn 95/46, gelezen in samenhang met het Handvest".*[128] Het benadrukt echter in paragraaf 74 dat het geen exacte kopie moet zijn van de regels zoals ze gelden in de EU, maar dat het ook via andere middelen kan bereikt worden.[129]

II. Advies 1/15 HvJ-EU (2017)

In het advies 1/15 heeft het Hof van Justitie bevestigd dat persoonsgegevens slechts van de Europese Unie naar een derde land mogen worden doorgegeven, indien in dit land *"een niveau van bescherming van vrijheden en grondrechten wordt geboden dat in wezen gelijkwaardig is aan het binnen de Unie gewaarborgde niveau"… "teneinde de continuïteit van het door het Unierecht geboden beschermingsniveau te garanderen".*[130] In deze zaak ging het over het feit dat de EU passagiersgegevens wou doorgeven aan Canada door middel van een PNR-overeenkomst

[123] NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 56-58.
[124] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §86.
[125] Ibid., §93-94.
[126] Ibid., §95.
[127] Ibid., §72.
[128] Ibid., §73.
[129] Ibid., §74.
[130] HvJ 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592, §214.

(*Passenger Name Record*).[131] Het Hof heeft geoordeeld dat deze overeenkomst in haar voorgenomen vorm niet mag worden afgesloten, omdat het een inbreuk vormt op het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, zoals gewaarborgd in de artikelen 7 en 8 van het Handvest van de grondrechten van de EU.[132] Het Hof merkt evenwel op dat dit desalniettemin zou kunnen worden gerechtvaardigd op basis van doelstellingen van het algemeen belang zoals de openbare veiligheid (denk aan terroristische aanslagen).[133] Echter gingen de bepalingen van de overeenkomst op dat moment verder dan noodzakelijk.[134]

III. Schrems II (2020)

Ook de opvolger van het *Safe Harbor* systeem, namelijk het *Privacy Shield* werd aangevallen door Max Schrems in 2020. De reden hiervoor was dezelfde als in de *Schrems* I zaak. De Amerikaanse inlichtingendiensten hadden namelijk de mogelijkheid op basis van verschillende wetten, zoals de Foreign Intelligence Surveillance Act of Executive Order 12333 of de Presidential Policy Directive, data te analyseren en te monitoren uit correspondentie.[135] Verder vloeit voort uit deze zaak dat de bescherming die in de EU aan persoonsgegevens wordt geboden, moet meereizen met de gegevens.[136] Het Hof benadrukt daarnaast dat er niet vereist wordt dat exact hetzelfde niveau van bescherming moet worden geboden, maar dat er minimaal een "in wezen gelijkwaardig" niveau van bescherming voorhanden dient te zijn.[137]

Het Hof van Justitie oordeelde daarnaast dat er een gebrek was aan effectieve rechtsmiddelen.[138] Er waren, in tegenstelling tot onder het *Safe Harbor* systeem, wel rechtsmiddelen aanwezig. Maar deze waren niet effectief tegen Amerikaanse autoriteiten.[139] Tevens werd de ombudsman benoemd door de minister en moest hij aan deze rapporteren, wat erop wijst dat hij niet volledig

---

[131] NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 58-60.
[132] HvJ 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592, §232.
[133] HvJ 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592, §151; NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 59.
[134] Ibid., §151.
[135] BEUDELS M., 'Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest' *Tijdschrift Privacy en Persoonsgegevens* 2021, (18) 23.
[136] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §93.
[137] Ibid., §94.
[138] Ibid., §192.
[139] Ibid., §190-197.

onafhankelijk was.[140] Daarenboven was de Ombudsman geen tribunaal in de zin van artikel 47 van het Handvest en kon het niet in de plaats treden van een gerechtelijk verhaalmechanisme.[141] Het *Privacy Shield*-kader, voorzag eveneens in voorrang van het Amerikaanse recht indien de regels van het wettelijk kader in strijd waren met de vereisten van het Amerikaanse recht op het gebied van nationale veiligheid, openbaar belang of wetshandhaving.[142]

In het *Schrems* II arrest verwees het Hof dus opnieuw naar de "in wezen gelijkwaardigheid". In deze zaak werd het gebruikt om de geldigheid van de SCC's te beoordelen, maar afgezien daarvan verzekert het Hof in paragraaf 92 dat het beschermingsniveau moet worden gewaarborgd *"ongeacht de bepaling van dat hoofdstuk op basis waarvan persoonsgegevens naar een derde land worden doorgegeven".*[143] Ook het EDPB bevestigt dit in haar Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen.[144]

c) Europees Hof voor de Rechten van de Mens (EHRM)

In de *Schrems II* zaak heeft het HvJ-EU duidelijk gemaakt dat bij de beoordeling of een derde land een passend niveau van gegevensbescherming biedt, moet worden uitgegaan van het beschermingsniveau dat binnen de Europese Unie vereist is.[145] De verplichtingen vloeien voort uit de AVG en het EU-Handvest van de grondrechten, maar ook uit het EVRM.[146] Hoewel de EU nog geen partij is bij het EVRM, maken de daarin gewaarborgde grondrechten wél deel uit van het Unie-recht in de vorm van algemene beginselen.[147] Het EVRM speelt dus onrechtstreeks een belangrijke rol in deze evaluatie omdat alle EU-lidstaten het hebben ondertekend, waardoor het een gemeenschappelijke noemer vormt voor de grondrechten in de hele Unie.

---

[140] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §195; DRECHSLER L., "What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights." *Jusletter IT* 2019*,* (1) 7.
[141] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §65.
[142] Ibid., §164-165.
[143] Ibid., §92.
[144] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf, §62.
[145] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94.
[146] Ibid., §97.
[147] Ibid., §98.

Artikel 8 van het EVRM, dat het recht op eerbiediging van het privéleven beschermt, komt nauw overeen met artikel 7 van het Handvest. Ook artikel 13 van het EVRM, dat het recht op een doeltreffende voorziening in rechte waarborgt, komt overeen met artikel 47 van het Handvest. Deze bepalingen worden gebruikt om te beoordelen of een derde land voldoende rechtsbescherming en rechtsmiddelen biedt in de context van toezichtpraktijken. Als een derde land niet voldoet aan bovenstaande normen van het EVRM, zal het waarschijnlijk ook niet voldoen aan de vereisten van het Handvest. In die zin wordt de jurisprudentie van het EHRM een praktisch instrument voor het beoordelen van adequaatheid. De advocaat-generaal in *Schrems II* verwees ook naar belangrijke jurisprudentie van het EHRM, waaronder *Big Brother Watch* en *Centrum för Rättvisa*, die betrekking hebben op grootschalige surveillance.[148] Deze zaken worden relevant geacht om te beoordelen of derde landen zorgen voor toezicht en rechtsmiddelen die voldoen aan de Europese mensenrechtennormen.

d) Artikel 29 Werkgroep

In vorige onderafdelingen werd achterhaald welke elementen de AVG, het HvJ-EU en het EHRM noodzakelijk achtten wat betreft de inhoudelijke kernbeginselen voor een passend beschermingsniveau. De Artikel 29 Werkgroep heeft op 28 november 2017 een adequaatheidsreferentie uitgevaardigd waarin ze een lijst heeft uiteengezet met haar interpretatie van de adequaatheidscriteria uit de AVG.[149] Het werd opgesteld met het achterliggende idee dat de Europese Commissie deze als leidraad zou kunnen gebruiken bij de beoordeling van het beschermingsniveau van derde landen.

1) **Begrippen[150]:** Er moeten basisbegrippen en/of -beginselen voor gegevensbescherming worden geformuleerd die een afspiegeling vormen van de begrippen in de EU-wetgeving en daarmee consistent zijn. Zoals “persoonsgegevens", "verwerking van persoonsgegevens", "verwerkingsverantwoordelijke, "verwerker", "ontvanger" en "gevoelige gegevens".
2) **Gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden[151]:** Gegevens moeten worden verwerkt op een behoorlijke, rechtmatige en

[148] BOBEK M., Conclusie bij HvJ 16 juli 2020, C-498/16, ECLI:EU:C:2017:863.
[149] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie WP 254 rev.01, 28 november 2017, WP 253 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54200.
[150] Ibid., 7.
[151] Ibid.

legitieme wijze. De gerechtvaardigde grondslagen moeten duidelijk worden uiteengezet. Bijvoorbeeld de toestemming van de betrokkene.

3) **Het beginsel van doelbinding[152]:** De verwerking van de gegevens moet gebeuren voor een specifiek doeleinde.
4) **Het beginsel van kwaliteit en evenredigheid van gegevens[153]:** De nauwkeurigheid van de gegevens zijn belangrijk en daarom moeten ze soms bijgewerkt worden. Daarnaast moeten ze toereikend zijn en kunnen dienen voor de beoogde doeleinden.
5) **Het beginsel van gegevensbewaring[154]:** De gegevens mogen niet langer worden bewaard dan noodzakelijk voor de doeleinden.
6) **Het beginsel van beveiliging en vertrouwelijkheid[155]:** De verwerking moet passende beveiliging van de gegevens verzekeren. Ze moeten bijvoorbeeld beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit kan volbracht worden aan de hand van technische of organisatorische maatregelen.
7) **Het transparantiebeginsel[156]:** Iedere betrokkene moet op een transparante, duidelijke manier worden geïnformeerd over alle belangrijke elementen van de verwerking van zijn of haar persoonsgegevens. Deze informatie bevat het doel, de identiteit van de verwerkingsverantwoordelijke, de rechten. Hier kunnen uitzonderingen op worden gemaakt om bijvoorbeeld onderzoeken naar strafbare feiten veilig te stellen.
8) **Het recht van toegang, rectificatie, wissing en bezwaar[157]:** De betrokkene heeft het recht om uitsluitsel te verkrijgen en een kopie te verkrijgen. De betrokkene heeft recht op rectificatie van zijn of haar gegevens om specifieke redenen, bijvoorbeeld wanneer deze gegevens onjuist of onvolledig blijken te zijn. De betrokkene heeft recht op wissing van zijn of haar persoonsgegevens wanneer de verwerking ervan bijvoorbeeld onrechtmatig of niet langer noodzakelijk is. De betrokkene heeft ook te allen tijde het recht om bezwaar te maken tegen de verwerking van zijn of haar gegevens onder bepaalde voorwaarden die zijn vastgelegd in het rechtskader van het derde land.

[152] Ibid.
[153] Ibid.
[154] Ibid.
[155] Ibid., 7-8.
[156] Ibid., 8.
[157] Ibid.

9) **Beperkingen ten aanzien van verdere doorgifte[158]:** Verdere doorgifte van de persoonsgegevens door de eerste ontvanger van de oorspronkelijke gegevensdoorgifte mag alleen worden toegestaan wanneer a) de latere ontvanger eveneens is onderworpen aan voorschriften b) deze ontvanger de relevante instructies opvolgt. Het beschermingsniveau van natuurlijke personen mag niet worden ondermijnd door de verdere doorgifte. Indien nodig moet de eerste ontvanger, bij ontstentenis van een adequaatheidsbesluit, passende waarborgen aannemen voor verdere doorgifte van gegevens.

Wat opvalt is dat sommige rechten van betrokkenen uit de AVG ook rechtstreeks deel uitmaken van de grondrechten in het Handvest. Zo zijn bijvoorbeeld het recht van toegang en rectificatie ook rechtstreeks opgenomen in de beschrijving van het grondrecht op bescherming van persoonsgegevens van het Handvest.[159]

Tussenconclusie inhoudelijke kernbeginselen

De Europese Commissie onderzoekt inhoudelijke kernbeginselen voor gegevensbescherming om te beoordelen of het gegevensbeschermingskader van een derde land kan worden beschouwd als wezenlijk gelijkwaardig aan dat van de Europese Unie.[160] Deze beginselen vinden hun oorsprong in de AVG, de jurisprudentie van het HvJ-EU en het EHRM, evenals de richtsnoeren van de voormalige Artikel 29-werkgroep.[161] Dankzij bovenstaande analyse kan er een lijst van deze beginselen opgesteld worden. De beginselen bestaan uit: rechtmatige verwerking (artikel 6 AVG), doelbinding (artikelen 5 lid 1, b AVG), gegevenskwaliteit en evenredigheid (artikelen 5, lid 1, c en 16 AVG), gegevensbewaring (artikel 5, lid 1, e AVG), beveiliging en vertrouwelijkheid (artikelen 5, lid 1, f en 32 AVG), transparantie (artikelen 5 en 13 AVG), het recht van inzage, rectificatie, gegevenswissing (artikelen 15, 16 en 17 AVG), beperkingen op verdere doorgifte (artikel 44 AVG), bescherming van bijzondere categorieën van persoonsgegevens (artikelen 9 en 10 AVG), het recht

[158] Ibid.
[159] Art. 8 Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj; DRECHSLER L., "Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation.", *Review of European Administrative Law* 2023, (35) 41.
[160] Overw. 104 AVG, ROTH P., 'Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation', Journal of Law, *Information and Science* 2017, (49) 54.
[161] Art. 45, tweede lid AVG; HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner'; HvJ 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592; HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems; GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie WP 254 rev.01, 28 november 2017, WP 254 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54200.

om bezwaar te maken tegen direct marketing (artikel 21 AVG) en geautomatiseerde individuele besluitvorming, waaronder profilering aan te vechten (artikelen 22 AVG).

In de praktijk past de Commissie deze beginselen echter zeer flexibel toe.[162] Zij eist niet altijd dat elk van de bovengenoemde beginselen uitdrukkelijk en volledig wordt weerspiegeld in het rechtskader van het betrokken derde land.[163] De rechtmatigheid van de verwerking of het recht om bezwaar te maken tegen direct marketing kan bijvoorbeeld slechts in beperkte mate aan de orde komen of er kan indirect naar worden verwezen, maar toch kan de Commissie de algemene regeling toereikend achten.[164] Uit de bestaande adequaatheidsbesluiten blijkt ook dat de Europese Commissie autonoom kiest welke criteria worden gehanteerd bij de beoordeling.[165] Zo is het criterium uit artikel 45, lid 2, a) AVG in geen enkel adequaatheidsbesluit opgenomen. Dit criterium houdt in dat er rekening dient gehouden te worden met de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, etc.[166] Nochtans zijn enkele rechtsgeleerden van mening dat een gebrek aan bescherming van de mensenrechten en de rechtsstaat een derde land van tevoren moet uitsluiten van de mogelijkheid een adequaatheidsbesluit te kunnen verkrijgen.[167]

Naar mijn mening moet de drempel voor adequaatheid strikt worden geïnterpreteerd. Hoewel de juridische diversiteit tussen derde landen een zekere mate van flexibiliteit vereist, moet de bescherming van de grondrechten het centrale criterium blijven. De "in wezen gelijkwaardigheid" mag niet alleen worden beoordeeld op basis van wetteksten, maar ook de daadwerkelijke afdwingbaarheid van deze rechten zijn essentiële onderdelen van een systeem dat bescherming kan bieden.

[162] BYGRAVE L.A., *Data Privacy Law*, Oxford University Press, 2014, 193.
[163] HvJ 16 juli 2020, nr. C-11/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §94; BYGRAVE L.A., *Data Privacy Law*, Oxford University Press, 2014, 193.
[164] EUROPESE COMMISSIE, Uitvoeringsbesluit van de Commissie (EU) 2019/419 van 23 januari 2019 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door Japan krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 19 maart 2019, 15, http://data.europa.eu/eli/dec_impl/2019/419/oj.
[165] NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 298-300.
[166] Art. 45, tweede lid AVG.
[167] DRECHSLER L., KAMARA I., 'Essential equivalence as a benchmark for international data transfers after Schrems II', in KOSTA E., LEENES R., *Essential equivalence as a benchmark for international data transfers after Schrems II*, Edward Elgar Publishing, 2022, (314) 341.

Onderafdeling 2. Procedurele en handhavingsmechanismen

Naast de inhoudelijke kernbeginselen wordt er ook onderzocht of het beschermingsniveau adequaat is op het vlak van de procedurele en handhavingsmechanismen.[168] Hieronder zal opnieuw onderzocht worden welke elementen de AVG en de Artikel 29 Werkgroep vereisen.

a) Algemene verordening gegevensbescherming (AVG)

Uit artikel 45, lid 2, b) AVG vloeit voort dat er voor een passend beschermingsniveau te kunnen bieden er een of meer onafhankelijke toezichthoudende autoriteiten in het derde land moeten worden opgericht om de gegevensbeschermingsregels te kunnen handhaven.[169]

b) Artikel 29 Werkgroep

Om te weten te komen wat er volstaat om te voldoen aan de vereiste uit artikel 45, lid 2, b), kan er opnieuw gekeken worden naar dezelfde adequaatheidsreferentie van de Artikel 29 Werkgroep. In hoofdstuk 3, onderdeel C, worden diverse criteria uiteengezet waaraan voldaan moet zijn teneinde een adequaat handhavingsmechanisme tot stand te brengen:[170]

1) **Bevoegde onafhankelijke toezichthoudende autoriteit[171]:** Zij krijgen de taak toebedeeld om de naleving van de bepalingen omtrent de gegevensbescherming en bescherming van de persoonlijke levenssfeer te controleren, te waarborgen en te handhaven. De toezichthoudende autoriteit moet hierbij volledig onafhankelijk en onpartijdig handelen. De onafhankelijkheid houdt in:
    - **a.** beschikken over alle noodzakelijke en beschikbare bevoegdheden en missies
    - **b.** de personeelsbezetting en de begroting
    - **c.** op eigen initiatief onderzoeken kunnen verrichten.

[168] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie WP 254 rev.01, 28 november 2017, WP 254 rev.01, 9, https://ec.europa.eu/newsroom/article29/redirection/document/54200; DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, vol. 5, nr 1, (54) 62; ROTH P., "Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation." *Journal of Law, Information and Science* 2017, (49) 53.
[169] Art. 45, lid 2, b) AVG.
[170] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheidsreferentie, 28 november 2017, WP 254 rev.01, hoofdstuk 3,C, https://ec.europa.eu/newsroom/article29/redirection/document/54200.
[171] Ibid., 9.

2) **Het gegevensbeschermingssysteem moet een goed nalevingsniveau waarborgen[172]:** De verwerkingsverantwoordelijken moeten zich bewust kunnen zijn van hun verplichtingen, taken en bevoegdheden, en de betrokkenen moeten zich bewust kunnen zijn van hun rechten en de wijze waarop ze deze kunnen uitoefenen. Afschrikkende sancties kunnen hierbij een rol spelen.
3) **Verantwoordingsplicht[173]:** Verwerkingsverantwoordelijken moeten verplicht worden om zich aan het gegevensbeschermingskader te houden en worden dan ook verwacht om hun naleving te kunnen aantonen. Bijvoorbeeld door middel van effectbeoordelingen.
4) **Het gegevensbeschermingssysteem moet individuele betrokkenen ondersteunen en bijstaan bij het uitoefenen van hun rechten en het toepassen van passende rechtsmiddelen[174]:** De betrokkene moet de mogelijkheid hebben om terug te vallen op rechtsmiddelen waarmee hij of zij snel en effectief, zijn of haar rechten kan uitoefenen en naleving van de regelgeving kan afdwingen. Zo moet het derde land beschikken over een toezichtsmechanisme die het mogelijk maakt klachten onafhankelijk te onderzoeken, inbreuken vast te stellen en deze te bestraffen.

Tussenconclusie procedurele en handhavingsmechanismen

Wanneer persoonsgegevens van EU-ingezetenen worden doorgegeven aan een derde land, moet niet alleen worden gekeken naar de materiële kernbeginselen, maar ook naar de kernbeginselen met betrekking tot handhavingsmechanismen.[175] De volgende elementen moeten bijvoorbeeld worden geëvalueerd: het bestaan van een bevoegde onafhankelijke toezichthoudende autoriteit, een goed niveau van naleving, verantwoordingsplicht en verhaalsmogelijkheden voor personen.[176]

De Europese Commissie heeft de neiging om bij de beoordeling van de "in wezen gelijkwaardigheid" flexibel te zijn ten aanzien van procedurele en handhavingsmechanismen.[177]

[172] Ibid., 10.
[173] Ibid.
[174] Ibid.
[175] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 62; ROTH P., "Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation." *Journal of Law, Information and Science* 2017, (49) 53.
[176] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheidsreferentie, 28 november 2017, WP 254 rev.01, hoofdstuk 3,C,.https://ec.europa.eu/newsroom/article29/redirection/document/54200.
[177] WOLF C., 'Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers', *Washington University Journal of Law & Policy* 2013, (227) 239-242.

De onafhankelijkheid van toezichthoudende autoriteiten wordt bijvoorbeeld niet altijd strikt gemeten aan de hand van eerder vastgestelde criteria, en de evaluatie van de naleving omvat vaak een onderzoek naar de mogelijke handhavingsmaatregelen en sancties die zijn vastgelegd in het wetgevingskader van het derde land.[178] In sommige gevallen neemt de Commissie zelfs statistische gegevens op over hoe vaak dergelijke sancties worden toegepast.[179] De verantwoordingsplicht en rechtsmiddelen worden over het algemeen vanuit een breed perspectief onderzocht, waarbij aandacht wordt besteed aan de vraag of de organisatie beschikt over functionarissen voor gegevensbescherming of effectbeoordelingen.[180]

Naar mijn mening is het essentieel dat er een onafhankelijke toezichthoudende autoriteit en verantwoordingsplicht bestaan, aangezien dit zorgt voor een effectief toezicht op het beschermingsniveau en de handhaving van gegevensbeschermingsmaatregelen. Alleen een onafhankelijke autoriteit en een verantwoordingsplicht kunnen ervoor zorgen dat de naleving van de gegevensbeschermingsregels daadwerkelijk wordt gecontroleerd en gehandhaafd. Verder is het zeer belangrijk dat betrokkenen de mogelijkheid hebben om rechtsmiddelen in te zetten vooral wanneer er sprake is van een inbreuk. Dit zorgt ervoor dat ze hun rechten effectief kunnen uitoefenen.

[178] EUROPESE COMMISSIE, Uitvoeringsbesluit van de Commissie (EU) 2019/419 van 23 januari 2019 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door Japan krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 19 maart 2019, 16-19, http://data.europa.eu/eli/dec_impl/2019/419/oj; EUROPESE COMMISSIE, Uitvoeringsverordening (EU) 2021/1772 van de Commissie van 28 juni 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk, *Oj.L.* 11 oktober 2021, 17-21, http://data.europa.eu/eli/dec_impl/2021/1772/oj; EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2022/254 van de Commissie van 17 december 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door de Republiek Korea krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 24 februari 2022, 25-31, http://data.europa.eu/eli/dec_impl/2022/254/oj.

[179] EUROPESE COMMISSIE, Uitvoeringsverordening (EU) 2021/1772 van de Commissie van 28 juni 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk, *Oj.L.* 11 oktober 2021, 20, http://data.europa.eu/eli/dec_impl/2021/1772/oj.

[180] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheidsreferentie, 28 november 2017, WP 254 rev.01, 10, https://ec.europa.eu/newsroom/article29/redirection/document/54200.

Onderafdeling 3. De toegang van de overheid tot persoonsgegevens

Tot slot wordt er eveneens rekening gehouden met nationale wetgeving die toegang zou verlenen aan de overheid tot de persoonsgegevens.[181] Ook hier zijn er een aantal vereisten vastgelegd.

a) Algemene verordening gegevensbescherming

Volgens artikel 45, lid 2, a) AVG moet er rekening gehouden worden met *"de toepasselijke algemene en sectorale wetgeving, onder meer inzake openbare veiligheid, defensie, nationale veiligheid en strafrecht en de toegang van overheidsinstanties tot persoonsgegevens".*[182] De AVG verduidelijkt hier niet welke specifieke wetgeving zo'n passend beschermingsniveau met zich meebrengt. Hiervoor moeten de *Schrems* arresten van het Hof van Justitie bestudeerd worden.

b) Hof van Justitie (HvJ-EU)

In *Schrems* I paragraaf 87 stelt het Hof dat er geen passend beschermingsniveau voorhanden kan zijn indien wetgeving van het derde land het mogelijk maakt, op grond van bijvoorbeeld eisen van de nationale veiligheid en het algemeen belang, een inmenging te veroorzaken in de grondrechten van de personen van wie de persoonsgegevens vanuit de Unie naar de Verenigde Staten zijn of zouden kunnen worden doorgegeven.[183]

Het *Schrems* II arrest verklaarde het adequaatheidsbesluit op basis van het *Privacy Shield* ongeldig voor de redenen genoemd in paragraaf 164, 168, 176 en 197.[184] Meer bepaald 1) het feit dat de vereisten van de VS op het gebied van nationale veiligheid of wetshandhaving voorrang kunnen hebben op de beschermingsbeginselen uit het *Privacy Shield*, 2) de beperkingen van de bevoegdheden van de Amerikaanse overheidsinstanties niet kunnen voldoen aan de noodzakelijkheids- en evenredigheidstoets van de EU-wetgeving, 3) de Amerikaanse wetgeving betrokkenen geen rechtsmiddel biedt tegen de Amerikaanse overheidsinstanties en 4) het

[181] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 58; WAGNER J., 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?', *International Data Privacy Law* 2018, (318) 332.
[182] Art. 45, lid 2, a) AVG.
[183] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §87.
[184] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §164, 168, 176 en 197.

ombudsmechanisme uit het *Privacy Shield*-kader, geen doeltreffende bescherming biedt voor de rechten van betrokkenen.

c) Europese essentiële garanties

De Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen voorzien vier garanties die nageleefd moeten worden indien de overheid toegang krijgt tot de persoonsgegevens en deze eventueel zou verwerken.[185] De garanties bestaan uit:

1) **Garantie A: de verwerking moet gebaseerd zijn op duidelijke, precieze en toegankelijke regels[186]**

   Artikel 8, lid 2 en artikel 52, lid 1 van het Handvest bepalen dat persoonsgegevens verwerkt kunnen worden op basis van een gerechtvaardigde grondslag waarin de wet voorziet.[187] De rechtsgrond moet duidelijke, nauwkeurige en toegankelijke regels bevatten die de reikwijdte en de toepassing van de betrokken maatregel bepalen en minimale eisen opleggen. Daarnaast moet de betrokkenen deze rechten kunnen afdwingen. Bovendien moet de rechtsgrond aangeven in welke omstandigheden en onder welke voorwaarden deze verwerking kan gebeuren. Het Hof stelt ook dat deze rechtsgrondslag zelf de reikwijdte van de beperking van de uitoefening van dit recht moet definiëren en dat de rechtsgrond minstens volgende elementen moet bevatten:

   a. een definitie van de categorieën mensen op wie toezicht kan worden gehouden;
   b. een beperking van de duur van de maatregel;
   c. te volgen procedure voor de beoordeling;
   d. het gebruik en de opslag van de verkregen gegevens;
   e. de voorzorgsmaatregelen die moeten worden getroffen als de gegevens aan andere partijen worden doorgegeven.

[185] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.
[186] Ibid., 9.
[187] Art. 8, tweede lid en Art. 52, eerste lid Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj.

2) Garantie B: de noodzakelijkheid en evenredigheid van de nagestreefde legitieme doelstellingen moeten worden aangetoond[188]

Artikel 52, lid 1 van het Handvest bepaalt dat de beperkingen die gesteld worden aan rechten uit het Handvest, moeten voldoen aan een noodzakelijkheidstoets en daadwerkelijk moeten beantwoorden aan erkende doelstellingen van algemeen belang of eisen van de bescherming van de rechten en vrijheden van anderen die werden opgesteld door de Unie.[189]

Wat betreft de evenredigheidstoets moet er enerzijds worden nagegaan wat de ernst van de inmenging betreft en anderzijds moet er gecontroleerd worden of het belang dat wordt nagestreefd met de doelstelling van algemeen belang, evenredig is met die ernst.

Wat betreft de noodzakelijkheidstoets moeten de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan strikt noodzakelijk blijven. Dit wil meer bepaald zeggen dat er objectieve criteria moeten bestaan voor de verplichting van toegang of verwerking van de gegevens. Hierbij vereist het Hof dan ook dat de regeling enerzijds duidelijke en nauwkeurige regels bevat over de reikwijdte en de toepassing van de maatregel en anderzijds dat de regeling ook minimale eisen oplegt.

3) Garantie C: er moet een onafhankelijk toezichtmechanisme zijn[190]

Zodra er een inmenging is met het recht op privacy of het recht op gegevensbescherming, moeten deze inmengingen onderworpen kunnen worden aan een doeltreffend, onafhankelijk en onpartijdig toezichtsysteem dat moet worden verschaft door een rechter of een andere onafhankelijke instantie.

---

[188] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 10, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

[189] Art. 52, eerste lid Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj.

[190] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 13, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

Wat betreft de onafhankelijkheid verduidelijkt de aanbeveling dat het EHRM heeft bepaald dat er rekening moeten worden gehouden met:

a. de onafhankelijkheid van de uitvoerende macht en van de autoriteiten die de surveillance uitvoeren;
b. de wijze waarop de leden van het toezichtorgaan zijn benoemd en hun juridische status;
c. toegang heeft tot alle relevante documenten;
d. door het publiek kunnen worden gecontroleerd.

4) Garantie D: personen moeten over doeltreffende voorzieningen in rechte beschikken[191]

Artikel 47 van het Handvest en het Hof in de *Schrems I en II*-zaak vereisen dat eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, recht moet hebben op een effectief rechtsmiddel om aan zijn of haar rechten te voldoen.[192] Het Hof brengt deze garantie in verband met een kennisgeving die verricht zou moeten worden indien er een inmenging plaatsvindt, maar enkel en alleen indien dit de taken waarvoor deze autoriteiten verantwoordelijk zijn niet in gevaar brengt. Ook het EHRM brengt het in verband met de kennisgeving. Dit keer bij een surveillancemaatregel zodra de surveillance is beëindigd.

Tussenconclusie toegang van de overheid tot persoonsgegevens

Indien men de gegevensbescherming van een derde land onderzoekt, moet men naast de inhoudelijke kernbeginselen en de procedurele handhavingsbeginselen ook kijken naar de toegang van de overheid tot de persoonsgegevens.[193] Het gaat hier niet alleen over de centrale overheid,

[191] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 14, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

[192] Art. 47 Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj; HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §95; HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §194.

[193] DE CARVALHO D., LEONOR S., 'Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.', *European Data Protection Law Review* 2019, (54) 58; WAGNER J., 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?', *International Data Privacy Law* 2018, (318) 332.

maar ook een breed scala aan overheidsinstanties die bevoegd zijn om persoonsgegevens in te zien of te verwerken.[194] Dit omvat onder andere inlichtingendiensten, strafrechtelijke opsporingsdiensten, belastingdiensten of immigratiediensten.[195] Allereerst is het vereist dat indien nationale wetgeving voorziet in beperkingen op de gegevensbescherming op grond van bijvoorbeeld het algemeen belang of het naleven van dwingende wetten, deze regels een noodzakelijkheids- en evenredigheidstoets moeten doorstaan.[196] Daarnaast is het vereist dat er beperkingen worden opgelegd aan de toegang van de overheid tot de persoonsgegevens.[197] Tot slot moet er ook rekening gehouden worden met de vier Europese essentiële garanties die ontwikkeld zijn door de EDPB. Deze garanties omvatten: duidelijke, precieze en toegankelijke regels; noodzakelijkheid en evenredigheid; onafhankelijk toezichtsmechanisme en tot slot effectieve rechtsmiddelen.[198]

Naar mijn mening zijn onafhankelijk toezicht, doeltreffende rechtsmiddelen en transparantie met betrekking tot de surveillancepraktijken van de overheid cruciale indicatoren om te weten of een wetgeving van een derde land in wezen gelijkwaardig is. Uiteindelijk wordt een hoog beschermingsniveau bereikt wanneer de grondrechten van individuen niet worden ondermijnd door onevenredige of ongecontroleerde toegang tot hun persoonsgegevens door overheidsinstanties.

[194] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 5, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.
[195] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Guidelines 02/2024 on Article 48 GDPR, 2 december 2024, 02/2024, 5, https://www.edpb.europa.eu/system/files/2024-12/edpb_guidelines_202402_article48_en.pdf.
[196] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 10, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.
[197] HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §180.
[198] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

Hoofdstuk: 2 Wettelijk kader China

Afdeling 1. Inleiding

In dit hoofdstuk wordt de Chinese wetgeving geanalyseerd met het oog op doorgifte van persoonsgegevens vanuit de EU. Deze analyse is relevant in het kader van stap 3 van de *Data Transfer Impact Assessment (DTIA),* waarin het doorgifte-instrument moet worden beoordeeld in het licht van de wetgeving en praktijken van het derde land.

Eerst wordt onderzocht in hoeverre de Chinese wetgeving voldoet aan de drie vereisten die in hoofdstuk 1 zijn afgeleid als noodzakelijk voor een gelijkwaardig beschermingsniveau: (1) inhoudelijke kernbeginselen van gegevensbescherming, (2) procedurele en handhavingsmechanismen, en (3) beperkingen op overheidstoegang tot persoonsgegevens. Aansluitend wordt het bredere Chinese wetgevingskader geëvalueerd.

Afdeling 2. Wetgevingskader van China

De Chinese grondwet bevat geen specifieke bepaling voor de bescherming van de privacy of gegevensbescherming in vergelijking met het Handvest van de Europese Unie. De Volksrepubliek China heeft wel de Universele Verklaring van de Rechten van de Mens geratificeerd. De implementaties van artikel 12 UVRM zijn dan ook terug te vinden in de artikelen 39 en 40 van de Chinese grondwet. Artikel 39 van de Chinese grondwet beschrijft de onschendbaarheid van de woning van de Chinese burgers en artikel 40 van de Chinese grondwet is een bepaling die de vrijheid en vertrouwelijkheid van correspondentie van burgers van de Volksrepubliek China beschermt.[199] In dit artikel worden wel uitzonderingen ingebed in functie van de nationale veiligheid of een strafrechtelijk onderzoek of wettelijk voorgeschreven procedures.

De creatie van regelgeving over gegevensbescherming begon pas echt in 2012 met het besluit van het Nationaal Volkscongres van de Volksrepubliek China betreffende het versterken van de bescherming van netwerkinformatie.[200] Na de Cybersecurity Law (CSL) in 2017 en de Personal

[199] Art. 39 en 40 中华人民共和国宪法 [Grondwet van de Volksrepubliek China], 4 december 1982, https://www.gov.cn/guoqing/2018-03/22/content_5276318.htm.

[200] 全国人民代表大会常务委员会关于加强网络信息保护的决定 [Besluit van het Permanent Comité van het Nationale Volkscongres over het versterken van de bescherming van netwerkinformatie], 28 December 2012,

Information Security Specification (PISS) in 2020 werd dan uiteindelijk in 2021 de Data Security Law (DSL) en de Personal Information Protection Law (PIPL) uitgevaardigd.[201] Vooral deze laatste zal belangrijk zijn voor deze masterscriptie.

De PIPL vormt een aanvulling op alle voorgaande instrumenten, en bevat de regels betreffende de toegang en gebruik van persoonsgegevens.[202] Zoals artikel 1 van de PIPL ook aangeeft, is de PIPL gecreëerd *"om de rechten en belangen van persoonsgegevens te beschermen, de verwerking van persoonsgegevens te reguleren en het redelijke gebruik van persoonsgegevens te bevorderen."*.[203]

De volgende hoofdstukken zullen hetzelfde stramien volgen als "hoofdstuk 1, afdeling 5: Vereisten voor een gelijkwaardig beschermingsniveau." Doordat de omvang van deze masterproef het niet toelaat, zullen de gelijkenissen tussen de AVG en de PIPL minder uitgebreid besproken worden. Onder elke afdeling zal telkens een paragraaf toegewijd worden aan de gelijkenissen, terwijl de focus in het verdere verloop voornamelijk op de verschillen zal liggen. Voor een meer gedetailleerd overzicht kan verwezen worden naar de tabellen aan het einde van elke afdeling.

Afdeling 3. Inhoudelijke kernbeginselen

Beide wetgevingen hanteren gelijkaardige kernbegrippen zoals 'persoonsgegevens[204]' en 'verwerking van persoonsgegevens[205]', en delen fundamentele beginselen zoals 'legaliteit[206]',

https://www.gov.cn/jrzg/2012-12/28/content_2301231.htm; ZHAO Y., *Chinese Legal Reform and the Global Legal Order*, Cambridge University Press, 2017, 169.

[201] 中华人民共和国数据安全法 [Wet op gegevensbeveiliging van de Volksrepubliek China], 10 juni 2021, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm; 中华人民共和国个人信息保护法 [wet op de bescherming van persoonlijke informatie van de Volksrepubliek China], 20 augstus 2021, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm; LIU J., 'Towards a Global Regulatory Framework for Cross-Border Data Flows—Fundamental Concerns and the China's Approach.' *Frontiers of Law in China* 2022, (412) 427.

[202] KE X., LIU V., LUO Yen YU Z., 'Analyzing China's PIPL and how it compares to the EU's GDPR', *Iapp* 24 augustus 2021, https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr (geraadpleegd op 8 december 2024).

[203] Art. 1 中华人民共和国个人信息保护法 [wet op de bescherming van persoonlijke informatie van de Volksrepubliek China], 20 augstus 2021, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm (hierna: PIPL).

[204] Art. 4, lid 1 PIPL; Art. 4(1) AVG.

[205] Art. 4, lid 2 PIPL; Art. 4(2) AVG.

[206] Art. 5 PIPL; Art. 5 AVG.

'doelbinding[207]', 'gegevenskwaliteit[208]', 'opslagbeperking[209]', 'beveiliging[210]', 'transparantie[211]' evenals het 'recht op inzage[212]'. Toch zijn er enkele kleine verschillen. Zo bijvoorbeeld vereist de PIPL net als de AVG dat gegevens nauwkeurig zijn, maar legt ze daarbij iets meer nadruk op het voorkomen van schade.[213] Ook kent de PIPL een transparantieverplichting, al maakt ze – in tegenstelling tot de AVG – geen expliciet onderscheid tussen rechtstreekse en onrechtstreekse gegevensverzameling. Dergelijke kleine nuanceverschillen worden verder verduidelijkt in de bijhorende tabel.

1) Begrippen:

I. Verwerkingsverantwoordelijke (Art. 73, lid 1 PIPL vgl. Art. 4(7) AVG)

Een persoonlijke informatieverwerker wat te vergelijken valt met onze verwerkingsverantwoordelijke verwijst naar elke organisatie of persoon die onafhankelijk het doel en de methode van verwerking bij verwerkingsactiviteiten voor persoonsgegevens bepaalt.[214] Wat opvalt is dat er geen onderscheid wordt gemaakt in de PIPL tussen een verwerkingsverantwoordelijke en een verwerker. Dit kan een invloed hebben op de beoordeling van een adequaat beschermingsniveau, omdat het onderscheid in de AVG essentieel is voor het toekennen van verantwoordelijkheden, aansprakelijkheid en toezicht op de verwerking. Zo heeft een verwerkingsverantwoordelijke onder de AVG een reeks specifieke verplichtingen (zoals het afsluiten van verwerkersovereenkomsten en het naleven van transparantieverplichtingen), terwijl een verwerker vooral onder instructie werkt.[215] Als deze rollen in een ander juridisch kader niet worden onderscheiden, kan dat leiden tot lacunes in toezicht en rechten van betrokkenen. Echter moet erop gewezen worden dat de EU niet van het derde land verlangt dat het identieke wettelijke grondslagen heeft voor de verwerking van persoonsgegevens als de AVG.[216]

[207] Art. 6 PIPL; Art. 5, lid 1, b) AVG.
[208] Art. 8 PIPL; Art. 5, lid 1, d) AVG.
[209] Art. 19 PIPL; Art. 5, lid 1, e) AVG.
[210] Art. 9 PIPL; Art. 5, lid 1, e) AVG.
[211] Art. 17 PIPL; Art. 13(1) AVG.
[212] Art. 45 PIPL; Art. 15 AVG
[213] Art. 8 PIPL
[214] Art. 73, eerste lid PIPL.
[215] Art. 24 en 28 AVG.
[216] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §74.

2) Gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden:

I. Rechtmatigheid/Legitimiteit (Art. 13, lid 1 PIPL vgl. Art. 6 AVG)

Daarnaast vereist de PIPL dat de verwerking van persoonsgegevens rechtmatig is.[217] Artikel 13 PIPL noemt gronden die grotendeels overeenkomen met artikel 6 van de AVG, zoals het verkrijgen van toestemming, de noodzaak voor het sluiten of uitvoeren van een overeenkomst, het voldoen aan een wettelijke verplichting, bescherming van vitale belangen, het vervullen van taken van het algemeen belang.[218] Meteen valt op dat er geen variant bestaat voor artikel 6, lid 1, f) AVG, namelijk voor de "*behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde*".[219] Daarnaast bestaat er in de AVG geen variant voor de grond uit artikel 13, VI PIPL, namelijk "*het verwerken van openbaar gemaakte gegevens*". Het verschil tussen de PIPL en de AVG betekent dat sommige verwerkingen die onder de AVG als rechtmatig zouden worden beschouwd, onder de PIPL mogelijk onrechtmatig zijn of omgekeerd. Dit verschil maakt het moeilijker om te beoordelen of persoonsgegevens bij doorgifte naar China onder vergelijkbare omstandigheden even goed worden beschermd. Echter moet er opnieuw gewezen worden op het feit dat de Europese Commissie niet van het derde land verlangt dat het identieke wettelijke grondslagen heeft voor de verwerking van persoonsgegevens als de AVG.[220] Uit het onderzoek van het adequaatheidsbesluit van Japan bleek zelfs dat de legitieme doeleinden enkel in de voetnoten vermeld werden.[221]

3) Het recht op inzage, rectificatie, wissing en bezwaar:

I. Recht op rectificatie (Art. 46 PIPL vgl. Art. 16 AVG):

Artikel 46 PIPL geeft het recht aan de betrokkene om wanneer deze vaststelt dat zijn of haar gegevens onnauwkeurig of onvolledig is, ze te laten corrigeren of aan te vullen.[222] Zoals gezien

[217] Art. 13, lid 1 PIPL.
[218] Art. 13 lid 1 PIPL.
[219] Art. 6, lid 1, f) AVG.
[220] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §74.
[221] EUROPESE COMMISSIE, Uitvoeringsbesluit van de Commissie (EU) 2019/419 van 23 januari 2019 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door Japan krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 19 maart 2019, §47, http://data.europa.eu/eli/dec_impl/2019/419/oj.
[222] Art. 46 PIPL.

in artikel 8 PIPL is nauwkeurigheid en volledigheid zeer belangrijk.[223] In de AVG heeft de betrokkene een onverwijld recht op de correctie van de gegevens, terwijl volgens de PIPL de correctie pas plaatsvindt na verzoek en verificatie.

II. Recht op gegevenswissing (Art. 47 PIPL vgl. Art. 17 AVG):

Op grond van artikel 47 PIPL krijgen betrokkenen het recht om hun persoonsgegevens te laten verwijderen.[224] Dit kan vergeleken worden met het recht om vergeten te worden in de AVG.[225] Evenwel geeft de AVG meer informatie over de termijnen en de wijze waarmee men rekening moet houden bij het reageren op dergelijke verzoeken. Bovendien eist de AVG dat de verwerkingsverantwoordelijken andere partijen waarmee de informatie is gedeeld, op de hoogte stellen van het verzoek. Verder reikt het artikel een aantal situaties aan waarin de betrokkene het recht kan vragen. Om volledig transparant te zijn, krijgt de betrokkene bovendien een recht op uitleg toebedeeld onder artikel 48 PIPL.[226] Dit is niet voorzien in de AVG. De betrokkene ontvangt een toelichting over de regels voor de verwerking van zijn of haar persoonsgegevens. Bovendien is dit recht relatief aangezien in artikel 47, lid 2 PIPL aangegeven staat dat indien de verwijdering bijvoorbeeld technisch moeilijk te realiseren valt, de verwerkingsverantwoordelijke moet stoppen met het verwerken en enkel nodige beveiligingsmaatregelen moet nemen voor de tot dan toe opgeslagen informatie.[227]

4) Beperkingen ten aanzien van verdere doorgifte (Art. 38 PIPL vgl. Art. 46 (1) AVG):

Het Chinese kader vertoont overeenkomsten met de trajecten voor een grensoverschrijdende gegevensoverdracht uit de AVG, zoals besproken in hoofdstuk 1, afdeling 3 – namelijk adequaatheidsbesluiten, passende waarborgen en afwijkingen voor specifieke situaties. De trajecten voor de doorgifte van persoonsgegevens van China naar derde landen bevinden zich in artikel 38 van de PIPL. Gegevens kunnen worden doorgegeven na een geslaagde veiligheidsbeoordeling door de cyberspace-administratie (vergelijkbaar met een adequaatheidsbesluit), certificering door een specialist (vergelijkbaar met een certificeringsmechanisme), het sluiten van een contract met een overzeese ontvanger op basis

[223] Art. 8 PIPL.
[224] Art. 47 PIPL.
[225] Art 17 AVG.
[226] Art. 48 PIPL.
[227] Art. 47, tweede lid PIPL.

van het standaardcontract van de cyberspace-administratie (vergelijkbaar met de SCC's inzake gegevensbescherming) of het voldoen aan andere voorwaarden die zijn voorgeschreven door wet- of regelgeving.[228]

Daarnaast vereist de doorgifte van persoonsgegevens aan een derde land een aantal bijzondere informatieverplichtingen en bijkomend ook de toestemming van de betrokkene volgens artikel 39 PIPL.[229] Uit artikel 40 PIPL volgt nog dat indien de doorgifte betrekking heeft op persoonsgegevens uit kritieke informatie-infrastructuur of verwerkers van persoonsgegevens waarvan de verwerking van persoonsgegevens het aantal bereikt dat is voorgeschreven door de cyberspace-administratie van de staat, de doorgifte hoe dan ook een veiligheidsbeoordeling moet doorstaan.[230]

Zowel de PIPL als de AVG vereisen dus dat de ontvanger een adequaat beschermingsniveau biedt dat gelijkwaardig is aan de eisen van de PIPL of de AVG. De "beveiligingsbeoordeling" van de PIPL zou vergeleken kunnen worden met het adequaatheidsbesluit van de AVG en "het contract met een overzeese ontvanger" met de SCC's.

[228] Art. 38 PIPL.
[229] Art. 39 PIPL.
[230] Art. 40 PIPL.

Inhoudelijke kernbeginselen	PIPL Artikel	AVG Artikel	Belangrijkste Verschillen
1) Begrippen			
Persoonsgegevens	Art. 4(1)	Art. 4(1)	PIPL beperkt zich tot "elektronisch of anders geregistreerd"; AVG is ruimer in formulering.
Verwerking van persoonsgegevens	Art. 4(2)	Art. 4(2)	AVG specifieker: noemt o.a. ordenen, structureren, combineren.
Verwerkingsverantwoordelijke	Art. 73(1)	Art. 4(7)	PIPL kent geen onderscheid tussen verwerker en verwerkingsverantwoordelijke.
2) Gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden:			
Legaliteitsbeginsel	Art. 5	Art. 5	PIPL vermeldt ook expliciet 'goede trouw' en verbiedt misleiding, dwang.
Rechtsgrond voor verwerking	Art. 13(1)	Art. 6	PIPL bevat geen variant van gerechtvaardigd belang (Art. 6(1)(f) AVG), en voegt wel extra gronden toe.
3) Doelbinding	Art. 6	Art. 5(1)(b)	PIPL is beknopter en mist uitzonderingen voor archivering/wetenschappelijk/statistisch gebruik.
4) Gegevenskwaliteit & evenredigheid	Art. 8	Art. 5(1)(d)	PIPL focust op voorkomen van schade, minder gedetailleerd.
5) Opslagbeperking	Art. 19 & Art. 6(2)	Art. 5(1)(e)	PIPL noemt geen uitzonderingen voor archivering/onderzoek.
6) Beveiliging & vertrouwelijkheid	Art. 9 & 51	Art. 5(1)(f)	AVG specifieker in risico's zoals verlies, ongeoorloofde toegang.
7) Transparantie	Art. 17 & 48	Art. 13(1)	AVG maakt onderscheid tussen directe en indirecte gegevensverzameling;

			PIPL kent recht op toelichting (niet in AVG).
8) Het recht van toegang, rectificatie, wissing en bezwaar			
Recht op inzage	Art. 45	Art. 15	PIPL bevat beperking op basis van vertrouwelijkheid; AVG specifieker over verstrekte informatie.
Recht op rectificatie	Art. 46	Art. 16	PIPL vereist verzoek en verificatie; AVG voorziet recht op onverwijlde correctie.
Recht op gegevenswissing	Art. 47	Art. 17	AVG noemt meer gronden en verplicht mededeling aan derden; PIPL bevat uitzondering bij technische moeilijkheid.
9) Beperkingen ten aanzien van verdere doorgifte	Art. 38-40	Art. 46(1)	PIPL vereist veiligheidsbeoordeling (bijv. door staatsinstantie); AVG werkt met adequaatheidsbesluiten/SCC's.

Tabel 1: Vergelijking inhoudelijke kernbeginselen AVG en PIPL

Afdeling 4. Procedurele en handhavingsmechanismen

Zowel de PIPL als de AVG hebben als doel de bescherming van persoonsgegevens te waarborgen en stellen beide dat een toezichthoudende autoriteit verantwoordelijk is voor het toezicht op naleving van de wetgeving.[231] Beide wetgevingen voorzien in mechanismen die bedrijven verplichten om te voldoen aan de regelgeving, zoals administratieve sancties en boetes voor inbreuken op de bescherming van persoonsgegevens.[232] Zowel de PIPL als de AVG leggen de verantwoordelijkheid bij de verwerkingsverantwoordelijke en bieden individuen de mogelijkheid om hun rechten uit te oefenen, zoals het recht op rectificatie en het recht om klachten in te dienen.[233] Beide wetgevingen voorzien ook in het mechanisme voor rechtsmiddelen voor betrokkenen, zoals de mogelijkheid om een rechtszaak aan te spannen bij een volksrechtbank.[234]

1) **Bevoegde onafhankelijke toezichthoudende autoriteit (Art. 60 PIPL vgl. Art. 51 AVG):**
   Artikel 60 van de PIPL identificeert drie afdelingen die belast worden met het toezicht op de handhaving van de regels over de gegevensbescherming uit de PIPL.[235] Deze bevatten namelijk
   i. De cyberspace-administratie van de staat
   ii. Relevante afdelingen onder de Chinese Staatsraad
   iii. Relevante afdelingen op provinciaal niveau en hogere volksregeringen

   Het lijkt er dus op dat het Chinese raamwerk niet één onafhankelijke toezichthoudende autoriteit heeft aangesteld voor het toezicht. Deze drie bovenstaande afdelingen kunnen niet beschouwd worden als onafhankelijk, aangezien ze verbonden zijn aan de Chinese Staatsraad. In tegenstelling tot de PIPL waarbij meer dan één toezichthoudende autoriteit optreedt, moet volgens de AVG elke EU-lidstaat zijn eigen bevoegde toezichthoudende autoriteit oprichten.[236] De bevoegde onafhankelijke toezichthoudende autoriteit in Europa voor de AVG is de EDPB.[237] Daarnaast heeft elk EU-land zijn eigen nationale toezichthoudende autoriteit, die verantwoordelijk is voor de handhaving van de AVG binnen dat land.[238]

[231] Art. 60 PIPL; Art. 51 AVG.
[232] Art. 66 PIPL; Art. 83(5) AVG.
[233] Art. 64 PIPL; Art. 58(2) AVG.
[234] Art. 50 PIPL; Art. 79 AVG.
[235] Art. 60 PIPL.
[236] Art. 51 AVG.
[237] NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023, 271.
[238] DE BOEL L. en BRODAHL L., 'Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes', *Tijdschrift Privacy en Persoonsgegevens* 2021, (12) 12.

2) **Het gegevensbeschermingssysteem moet een goed nalevingsniveau waarborgen (Art. 66 PIPL vgl. Art. 83(5) AVG):**

Op basis van artikel 63 PIPL worden verschillende maatregelen ter beschikking gesteld om de naleving van de regels van de gegevensbescherming af te dwingen.[239] Daarnaast voorziet artikel 66 PIPL in de mogelijke administratieve sancties die kunnen worden opgelegd, zoals rectificatie, waarschuwingen en het in beslag nemen van illegale winsten of het opschorten van diensten.[240] Indien rectificatie wordt geweigerd, kunnen er boetes worden opgelegd aan de verwerker en de direct verantwoordelijke personen. De hoogte van de boetes varieert van RMB 10.000 (ongeveer 1.300 euro) tot maximaal RMB 1 miljoen (ongeveer 130.000 euro) voor minder ernstige gevallen. In ernstige gevallen kan de boete oplopen tot RMB 50 miljoen (ongeveer 6,5 miljoen euro) of 5% van de jaarlijkse omzet van de verwerker, en boetes van tot RMB 1 miljoen (ongeveer 130.000 euro) voor direct verantwoordelijke personen.[241]

In tegenstelling tot in de AVG is het niet duidelijk of de jaarlijkse omzet die gebruikt wordt voor de berekening, verwijst naar de wereldwijde omzet of naar de omzet gegenereerd in China.[242] Daarnaast kan elke inbreuk van de PIPL geregistreerd worden in China's kredietwaardigheidsdossiers wat de reputatie van een bedrijf ernstig kan schaden.[243]

3) **Verantwoordingsplicht (Art. 64 PIPL vgl. Art. 58(2) AVG):**

In artikel 64 PIPL zijn er een aantal mogelijkheden gegeven aan de toezichthoudende instanties om bijvoorbeeld de wettelijke vertegenwoordiger (of de persoon die voornamelijk verantwoordelijk is voor de persoonsgegevensverwerker) te ondervragen door de voorgeschreven autoriteit en volgens de procedures.[244] Daarnaast kunnen ze de persoonsgegevensverwerker verplichten om professionele instanties toe te laten om nalevingsaudits uit te voeren. In de AVG wordt er eerder een expliciete opsomming voorzien van bevoegdheden, terwijl de PIPL een procedurele aanpak beschrijft zonder een vaste lijst van sancties.[245]

---

[239] Art. 63 PIPL.
[240] Art. 66 PIPL.
[241] Art. 66 PIPL.
[242] KE X., LIU V., LUO Yen YU Z., 'Analyzing China's PIPL and how it compares to the EU's GDPR', *Iapp* 24 augustus 2021, https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr (geraadpleegd op 8 december 2024).
[243] Art 67 PIPL.
[244] Art. 64 PIPL.
[245] Art. 58, tweede lid AVG.

4) **Het gegevensbeschermingssysteem moet individuele betrokkenen ondersteunen en bijstaan bij het uitoefenen van hun rechten en het toepassen van passende rechtsmiddelen (Art. 50 PIPL vgl. Art. 79 AVG):**

Allereerst moet er gewezen worden op de verplichting uit artikel 50 PIPL die oplegt aan de persoonsgegevensverwerker om een mechanisme uit te werken voor het accepteren en verwerken van verzoeken voor de uitoefening van de verhaalsrechten van de betrokkenen over verwerking van hun persoonsgegevens.[246] Volgens Artikel 50, lid 2 PIPL moet bij weigering van het verzoek door de persoonsgegevensverwerker de betrokkene in de mogelijkheid gesteld worden om een rechtszaak aan te spannen bij een volksrechtbank.[247]

Daarnaast hebben personen volgens artikel 65 PIPL ook de mogelijkheid een klacht in te dienen bij de afdelingen die hierboven vermeld zijn en die zich bezighouden met de taken met betrekking tot de naleving op het gebied van de bescherming van persoonsgegevens.[248] Verder moeten deze afdelingen de klagers op de hoogte stellen over het resultaat van hun klacht.

Ten derde blijkt uit artikel 69 PIPL dat de betrokkene een klacht kan indienen bij de volksrechtbank waar hij een schadevergoeding kan eisen ten aanzien van de persoonsgegevensverwerker op grond van een onrechtmatige daad.[249]

Tot slot vermeldt artikel 70 PIPL nog een laatste mogelijkheid in geval van een inbreuk op de regels met betrekking tot de verwerking van de persoonsgegevens die een groot aantal individuen treft.[250] Zo kunnen het volksprocuraat, de consumentenorganisaties die bij wet zijn gespecificeerd en de organisatie die door de cyberspace-administratie van de staat wordt bepaald, een rechtszaak aanspannen bij de volksrechtbank.

De Chinese PIPL volgt een vergelijkbare aanpak als de AVG. Zo wordt er een strikte burgerrechtelijke aansprakelijkheid opgelegd aan de verwerkingsverantwoordelijken en verwerkers op grond van artikel 82, lid 1 AVG.[251] De PIPL voorziet geen rechtstreeks rechtsmiddel tegen toezichthoudende instanties voor gegevensbescherming.

[246] Art. 50 PIPL.
[247] Art. 50, tweede lid PIPL.
[248] Art. 65 PIPL.
[249] Art. 69 PIPL.
[250] Art. 70 PIPL.
[251] Art. 81, eerste lid AVG.

Procedurele en handhavingsmechanismen	**PIPL**	**AVG**	**Belangrijkste verschillen**
Onafhankelijke toezichthoudende autoriteit	**(Art. 60 PIPL)** Geen onafhankelijke toezichthouder Meerdere afdelingen: • Cyberspace-administratie van de staat • Afdelingen onder de Staatsraad • Provinciale afdelingen	**(Art. 51 AVG)** - Elke lidstaat moet een onafhankelijke toezichthouder aanstellen. - EDPB op EU-niveau	PIPL mist onafhankelijkheid, terwijl dit een kernvereiste is onder de AVG
Goed nalevingsniveau	**(Art. 66 PIPL)** - Boetes tot 50 miljoen RMB of 5% van omzet - Geen duidelijkheid over reikwijdte omzet (nationaal/globaal) - Registratie in kredietwaardigheidssysteem	**(Art. 83(5) AVG)** - Boetes tot 20 miljoen euro of 4% van wereldwijde jaaromzet - Transparante omzetbasis	PIPL voegt reputatieschade toe via kredietsysteem; omzetbasis minder duidelijk

Verantwoordingsplicht	**(Art. 64 PIPL)** - Geen uitputtende lijst, maar procedurele bevoegdheden: - Onderzoek, audits, ondervraging	**(Art. 58(2) AVG)** - Uitgebreide lijst bevoegdheden in wet vastgelegd	AVG specifieker en transparanter in bevoegdheden
Rechtsmiddelen voor betrokkenen	**(Art. 50, 65, 69 & 70 PIPL)** - Verzetsmechanisme verplicht - Recht op klacht bij toezichthouder - Recht op gerechtelijke procedure - Collectieve acties mogelijk via procureur of erkende organisaties	**(Art. 79 AVG)** - Recht op klacht en effectieve rechtsmiddelen via toezichthouder en gerecht - Collectieve acties mogelijk via vertegenwoordigende entiteiten	Andere actoren voor collectieve acties in PIPL (overheidsgestuurd)

Tabel 2: Vergelijking procedurele en handhavingsmechanismen AVG en PIPL

Afdeling 5. De toegang van de overheid tot persoonsgegevens

Onderafdeling 1. Strafrechtelijke handhavingsdoeleinden

a) Rechtsgrond

De regels met betrekking tot het gebruik van persoonsgegevens voor strafrechtelijke handhavingsdoeleinden, kan gevonden worden in de Criminal Procedure Law of the People's Republic of China (hierna: CPL). Artikel 50 CPL bepaalt dat elektronische gegevens deel uitmaken van bewijsmateriaal dat gebruikt kan worden om de feiten van een zaak te bewijzen.[252] In artikel 54 CPL luidt de rechtsgrondslag: *"Volksrechtbanken, volksprocureurs en openbare veiligheidsinstanties het recht hebben om bij relevante werkplekken en personen bewijsmateriaal te verzamelen in overeenstemming met de wet."*[253]. Bewijsmateriaal kan ten eerste worden verzameld bij huiszoekingen. De burgers hebben de plicht om bij huiszoekingen te voldoen aan verzoeken van de volksprocureur om bewijsmateriaal te overhandigen dat de schuld of onschuld van de verdachte zou kunnen bewijzen.[254] Ten tweede kunnen ook technische onderzoeksmaatregelen ingezet worden om bewijs te verzamelen. Dit kan enkel *"in gevallen van misdaden die de nationale veiligheid in gevaar brengen, terroristische activiteiten, maffia-achtige organisatiemisdrijven, grote drugsmisdrijven of andere misdaden die de samenleving ernstig in gevaar brengen, na het voltooien van strikte goedkeuringsprocedures."*[255]

b) Beperkingen

De rechten van de onderzoeksinstanties worden beperkt. Zo stipuleert artikel 54 CPL dat bewijsmateriaal dat betrekking heeft op persoonlijke privacy vertrouwelijk behandeld dient te worden.[256] Dit geldt ook voor de verzameling met behulp van technische onderzoeksmaatregelen.[257] Bovendien is gebruik van het bewijs enkel toegelaten voor strafrechtelijk onderzoek, vervolging en berechting, en kunnen ze niet voor andere doeleinden worden gebruikt.[258] Daarnaast kan een huiszoeking enkel plaatsvinden met een huiszoekingsbevel

---

[252] Art. 50 中华人民共和国刑事诉讼法 [De wet op de strafvordering van de Volksrepubliek China], 1 juli 1979, https://www.gov.cn/flfg/2012-03/17/content_2094354.htm (Hierna: CPL).
[253] Art. 54 CPL.
[254] Art. 137 CPL.
[255] Art. 150 CPL.
[256] Art. 54 CPL.
[257] Art. 152 CPL.
[258] Art. 152 CPL.

tenzij in noodsituaties.[259] Wat betreft de technische onderzoeksmaatregelen zijn deze slechts toegelaten na een strikte goedkeuringsprocedure.[260]

c) Toezicht

Wat betreft de toezichtsmechanismen is er een intern toezicht. Dit houdt toezicht op de goedkeuringen van de huiszoekingsbevelen en de interne goedkeuringsprocedures voor de technische onderzoeksmaatregelen.[261] Er ontbreekt dus een onafhankelijk extern systeem, wat zorgwekkend is gebleken in het *Safe Harbor* systeem en het *Privacy Shield* systeem van de Verenigde Staten.[262]

d) Individueel verhaal

Het Chinees strafproces recht bevat geen rechtsmiddel die individuen kunnen aanwenden tegen de strafrechtelijke onderzoeksinstanties. Inbreuken op het recht op privacy en gegevensbescherming door onderzoeksinstanties kunnen niet voor de nationale rechter gebracht worden volgens het wetgevingskader.

Onderafdeling 2. Nationale veiligheidsdoeleinden

a) Rechtsgrond

I. Anti-spionagewet van de Volksrepubliek China

Om spionage te bestrijden kunnen nationale veiligheidsorganen dankzij de contraspionagewet toegang krijgen tot persoonsgegevens die in het bezit zijn van individuen en organisaties.[263] Deze wet heeft toepassing op instellingen en individuen binnen en buiten het grondgebied.[264] Zo zullen ook dochterondernemingen die in China zijn opgericht door buitenlandse moederondernemingen, als ook buitenlanders die in China wonen onder het toepassingsgebied vallen.

---

[259] Art. 138 CPL.
[260] Art. 150 CPL.
[261] Art. 138 en 150 CPL.
[262] HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, 'Schrems/Data Protection Commissioner', §41; HvJ 16 juli 2020, nr. C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner/Facebook Ireland en Schrems, §195.
[263] 中华人民共和国反间谍法 [Anti-spionagewet van de Volksrepubliek China], 26 april 2023, https://www.gov.cn/yaowen/2023-04/27/content_5753385.htm (Hierna: CEL).
[264] Art. 6 CEL.

II. Anti-terrorismewet van de Volksrepubliek China

Exploitanten van telecommunicatieondernemingen en internetaanbieders zijn verplicht volgens de Antiterrorismewet een aantal zaken ter beschikking te stellen zoals een technische interface, hulp bij decryptie en andere technische ondersteuning voor het voorkomen en onderzoeken van terroristische activiteiten.[265]

III. Nationale veiligheidswet van de Volksrepubliek China

Volgens artikel 52 van de Nationale veiligheidswet zijn staatsorganen, waaronder staatsveiligheidsorganen, openbare veiligheidsorganen en militaire organen bevoegd om op wettige wijze inlichtingen te verzamelen met betrekking tot de nationale veiligheid.[266] Burgers en organisaties zijn hierbij verplicht om bewijsmateriaal te leveren met betrekking tot activiteiten die de nationale veiligheid in gevaar brengen.[267]

IV. Nationale inlichtingenwet van de Volksrepubliek China

De Nationale inlichtingenwet verduidelijkt de middelen voor het uitvoeren van bovenstaande onderzoeksactiviteiten. Zo krijgen ze de bevoegdheid om werkplekken en faciliteiten te betreden; relevante instellingen en individuen te ondervragen en relevante bestanden, materialen of items te verzamelen.[268]

b) Beperkingen

In de Nationale inlichtingenwet wordt de veiligheid van de vrijheid en eigendommen van burgers en andere wetten gerechten en belangen gewaarborgd.[269] Daarnaast wordt bepaald dat de staatsorganen en hun personeel hun gezag niet mogen overschrijden of misbruiken en dat hier een sanctie op staat indien dit wel gebeurt.[270] Daarnaast moet de toegang tot informatie in

---

[265] Art. 18 中华人民共和国反恐怖主义法 [Anti-terrorismewet van de Volksrepubliek China], 27 december 2015, http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm (Hierna: ATL).

[266] Art. 52 中华人民共和国国家安全法 [Nationale veiligheidswet van de Volksrepubliek China], 1 juli 2015, https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm (Hierna: NSL).

[267] Art. 77 NSL.

[268] Art. 16 中华人民共和国国家情报法 [Nationale inlichtingenwet van de Volksrepubliek China], 27 juni 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm (Hierna: NIL).

[269] Art. 16 NIL.

[270] Art. 43 NIL.

overeenstemming zijn met de wet en beperkt worden tot de werkelijke behoeften.[271] Bovendien mogen de overheidsinstanties geen staatsgeheimen, commerciële geheimen en persoonsgegevens lekken.[272]

De bevoegdheden in de Anti-spionagewet mogen enkel worden aangewend bij contra spionagewerk op basis van nationale bepalingen en op voorwaarde dat er voldaan is aan de strikte formaliteiten voor de goedkeuring.[273]

c) Toezicht

Bovengenoemde rechtsgronden voorzien niet in gedetailleerde handhavings- en toezichtsmechanismen. Het toezicht bestaat opnieuw uit een interne toezichtprocedure.[274] Zo zijn de onderzoeksactiviteiten enkel toelaatbaar na goedkeuring of andere strikte formaliteiten. Bijgevolg is er opnieuw geen onafhankelijk extern systeem voorhanden.

d) Individueel verhaal

De Nationale inlichtingenwet voorziet met artikel 82 het recht om kritiek te uiten en aanbevelingen te doen aan staatsorganen, en het recht om klachten en beschuldigingen in te dienen om onwettige activiteiten te melden.[275]

Daarnaast kunnen burgers en organisaties een schadevergoeding eisen indien hun vermogen geschaad is omwille van de hulp die ze geboden hebben aan de nationale veiligheidsdiensten.[276]

Bovendien hebben burgers en organisaties ook het recht om aangifte te doen of beschuldigingen te uiten bij het overschrijden of misbruiken van het gezag of een ander onwettig gedrag van de veiligheidsdiensten.[277]

[271] Art. 83 NIL.
[272] Art. 31 NIL.
[273] Art. 12 en 17 CEL.
[274] Art. 16 en 31 NIL; Art. 12 en 16 CEL.
[275] Art. 82 NIL.
[276] Art. 78 ATL; Art. 81 NIL.
[277] Art. 27 NIL; Art. 26 CEL.

Onderafdeling 3. Personal Information Protection Law

a) Beginselen

Er gelden ook regels voor de overheidsinstanties volgens artikel 33 PIPL.[278] Deze regels zijn terug te vinden zijn in artikel 34, 35 en 36 PIPL.

I. Artikel 34 PIPL

Artikel 34 PIPL bevat een soort van dataminimalisatie voor de overheidsinstanties. De verwerking van persoonsgegevens door een staatsorgaan mag namelijk niet verder gaan dan nodig voor de uitoefening van de wettelijke taken.[279]

II. Artikel 35 PIPL

Overheidsinstanties moeten daarnaast ook de betrokkenen in kennisstellen dat hun persoonsgegevens worden verwerkt.[280] Echter zijn er in dit artikel ook een aantal beperkingsgronden ingebouwd. Bijvoorbeeld de vertrouwelijkheid zoals voorgeschreven in artikel 18, lid 1 PIPL of indien de kennisgeving de uitvoering van de wettelijke taken verhindert.[281]

III. Artikel 36 PIPL

Indien een overheidsinstantie persoonsgegevens verwerkt wordt er vereist dat deze gegevens worden opgeslagen op het grondgebied van de Volksrepubliek China.[282] Indien een doorgifte naar een derde land toch noodzakelijk is, moet er eerst een veiligheidsbeoordeling worden uitgevoerd.

De AVG heeft geen specifieke artikelen die uitsluitend gewijd zijn aan overheidsinstanties, zoals de artikelen 33-36 van de PIPL. In plaats daarvan zijn de regels voor overheidsinstanties doorheen heel de AVG geïntegreerd.

b) Toezicht

[278] Art. 33 PIPL.
[279] Art. 34 PIPL.
[280] Art. 35 PIPL.
[281] Art. 18, eerste lid PIPL.
[282] Art. 36 PIPL.

Zoals hierboven werd besproken, bestaan er drie afdelingen die belast worden met het toezicht op de naleving van de regels over de gegevensbescherming uit de PIPL.[283] Deze bevatten namelijk

i. de cyberspace-administratie van de staat
ii. relevante afdelingen onder de Chinese Staatsraad
iii. relevante afdelingen op provinciaal niveau en hogere volksregeringen

Deze afdelingen zijn ondergeschikt aan de centrale overheid. Daarenboven duidt de PIPL geen ander onafhankelijk toezichthoudend orgaan aan die toezicht zou houden op de overheidsinstanties.

[283] Art. 60 PIPL; LI Y., 'Cross-Border Data Transfer Regulation in China.' *Rivista Italiana Di Informatica e Diritto* 2021, (67) 73.

Categorie	Rechtsgrond	Beperkingen	Toezicht	Individueel verhaal
Strafrechtelijke handhavingsdoeleinden	Criminal Procedure Law (CPL): - Art. 50: elektronische gegevens als bewijs - Art. 54: recht op bewijsverzameling (incl. technische onderzoeksmaatregelen)	- Privacy moet vertrouwelijk blijven (art. 54) - Technische maatregelen enkel bij ernstige misdrijven + strikte goedkeuring - Huiszoeking enkel met bevel (tenzij noodsituatie) - Gebruik enkel voor strafzaken	Intern toezicht op: - Huiszoekingsbevelen - Goedkeuring technische maatregelen **Geen extern toezicht**	Geen rechtsmiddel voor individuen Geen toegang tot rechter bij privacyschendingen door onderzoeksinstanties
Nationale veiligheidsdoeleinden	- **Anti-spionagewet**: toegang tot data van individuen/organisaties, ook buitenlandse vestigingen - **Anti-terrorismewet**: verplichtingen voor telecom- en internetproviders - **Nationale veiligheidswet**: recht op informatievergaring door staatsorganen - **Nationale inlichtingenwet**: uitvoering via betreding, ondervraging, verzamelen	- Verbod op machtsmisbruik, sancties voorzien - Alleen toegang bij wettelijke noodzaak + formele goedkeuring - Bescherming van persoonlijke info, staats- en handelsgeheimen - Anti-spionage: enkel bij legitieme contraspionagezaken	Interne goedkeuringsprocedures vereist **Geen onafhankelijk extern toezicht**	Art. 82 Inlichtingenwet: - Recht op klacht, kritiek en aanbevelingen - Recht op schadevergoeding bij geleden schade - Recht op melding bij machtsmisbruik

Algemene bescherming via PIPL	PIPL art. 33-36 gelden ook voor overheid: - Art. 34: dataminimalisatie - Art. 35: kennisgeving (tenzij uitzondering) - Art. 36: opslag op Chinees grondgebied + veiligheidsbeoordeling bij doorgifte	- Enkel verwerking voor wettelijke taken - Beperkingen op kennisgeving indien vertrouwelijk of taakverstorend - Gegevens moeten in China blijven tenzij veiligheidsbeoordeling	Toezicht door: i. Cyberspace Administration ii. Staatsraad-afdelingen iii. Provinciale overheden **Geen onafhankelijk toezichthouder**	Geen expliciet individueel rechtsmiddel voorzien tegen overheidsinstanties onder de PIPL

Tabel 3: Overzicht toegang van de overheid tot persoonsgegevens

Afdeling 6. Evaluatie wetgevingskader

In deze afdeling wordt er onderzocht waarom China op dit moment niet in aanmerking zou kunnen komen voor een adequaatheidsbesluit. Hierbij worden de gelijkwaardigheden en tekortkomingen van de Chinese wetgeving geïdentificeerd.

Onderafdeling 1. Gelijkwaardigheid (supra: afdeling 3)

Ondanks een aantal structurele en terminologische verschillen, vertonen de kernbeginselen voor gegevensbescherming in het Chinese rechtskader een opmerkelijke mate van gelijkenis met die in de EU-wetgeving. Begrippen als transparantie[284], doelbinding[285] en gegevensminimalisatie[286] zijn duidelijk opgenomen in beide systemen. Hoewel deze plichten in het Chinese kader beknopter of minder gedetailleerd zijn geformuleerd, weerspiegelt de inhoud van de verplichtingen een vergelijkbaar voornemen om de rechten van individuen te waarborgen. In die zin kunnen de basisbeginselen van de Chinese gegevensbeschermingsregeling op veel gebieden als functioneel gelijkwaardig worden beschouwd aan die van de GDPR.

Onderafdeling 2. Tekortkomingen

a) Mensenrechten

Wat betreft artikel 45, lid 2, a) AVG, dat bepaalt dat er rekening dient gehouden te worden met de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, kan meteen opgemerkt worden dat China al verschillende keren mensenrechten heeft geschonden. Zo werd in 1989 het Tiananmenprotest op een gewelddadige manier onderdrukt, wat gepaard ging met duizenden doden.[287] Het bespreken of onderzoeken van deze gebeurtenis werd daarna verboden in China. Indien men dit verbod schond, riskeerde men een zware vervolging.[288] Daarnaast doen er zich nog een aantal schendingen voor van willekeurige detenties tot gedwongen arbeid zoals in de Culturele Revolutie van 1966.[289] China schuilt zich achter de nationale veiligheid

[284] Art. 17 PIPL; Art. 13(1) AVG.
[285] Art. 6 PIPL; Art. 5, lid 1, b) AVG
[286] Art. 19 PIPL; Art. 5, lid 1, e) AVG.
[287] O'BRIEN M., 'Classifying Cultural and Physical Destruction: Are Modern Historical and Current Human Rights Violations in China Violations of International Criminal Law?', *Criminal Law Forum* 2015, (533) 550-554.
[288] GÜNTHER HILPERT H., KRUMBEIN F., en STANZEL V., '*China's Guided Memory. How Historical Events Are Remembered, Glorified, Reinterpreted, and Kept Quiet'*, Stiftung Wissenschaft und Politik (SWP), 2020, 6.
[289] O'BRIEN M., 'Classifying Cultural and Physical Destruction: Are Modern Historical and Current Human Rights Violations in China Violations of International Criminal Law?', *Criminal Law Forum* 2015, (533) 536.

en terrorismebestrijding om deze schendingen te rechtvaardigen.[290] Volgens enkele rechtsgeleerden zou China dan ook uitgesloten moeten worden van de mogelijkheid een adequaatheidsbesluit te kunnen verkrijgen.[291] Maar het criterium uit artikel 45, lid 2, a) AVG werd in nog geen enkel adequaatheidsbesluit opgenomen, en daarom gaat de analyse hieronder verder met de andere tekortkomingen.

b) Overheid als verwerkingsverantwoordelijke (supra: afdeling 3)

Ten tweede wordt in artikel 4, 7) AVG benadrukt dat overheidsinstanties ook beschouwd kunnen worden als verwerkingsverantwoordelijke indien ze de doeleinden en middelen van de gegevensverwerking bepalen.[292] In de Personal Information Protection Law (PIPL) daarentegen worden overheidsinstanties niet opgenomen in artikel 73, lid 1 PIPL.[293] Dit zorgt ervoor dat Chinese overheidsinstanties niet dezelfde normen voor gegevensbescherming moeten handhaven als particuliere verwerkingsverantwoordelijken.[294] Deze lacune zorgt ervoor dat de overheid toezicht kan houden of toegang kan krijgen tot persoonlijke gegevens zonder hiervoor gegevensbeschermingsplichten en verantwoordingsplichten na te leven. Dit vermindert het beschermingsniveau van de persoonsgegevens.

c) Transparantie en rechtszekerheid

Ten derde zijn er ook problemen met de transparantie van het Chinese raamwerk. Zo is de privacywetgeving verspreid over meerdere wetten.[295] Namelijk de Cybersecurity Law (CSL), de Data Security Law (DSL) en de Personal Information Protection Law (PIPL). Waarvan de eerste gericht is op netwerk- en infrastructuurbeveiliging, de tweede op dataveiligheid in brede zin, met nadruk op nationale veiligheid en controle over gevoelige data en de laatste op de bescherming van persoonsgegevens.[296] De Chinese wetgever heeft zich niet uitgesproken over de specifieke reikwijdte en hiërarchie van deze overlappende wetten. Hierdoor kan het moeilijk zijn voor personen om hun verantwoordelijkheden en rechten te kennen. Dit kan op zijn beurt tot gevolg

[290] LOUISA L., *The people's republic of amnesia: Tiananmen revisited,* Oxford University Press, 2014, 72.
[291] DRECHSLER L., KAMARA I., 'Essential equivalence as a benchmark for international data transfers after Schrems II', in KOSTA E., LEENES R., *Essential equivalence as a benchmark for international data transfers after Schrems II*, Edward Elgar Publishing, 2022, (314) 341.
[292] Art. 4 7) AVG.
[293] Art. 73, eerste lid PIPL.
[294] GOLD A., 'China's new privacy law leaves U.S. behind', *Axios* 23 november 2021, https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind (geraadpleegd op 13 februari 2024).
[295] X, *Data Protection laws of the World,* DLA Piper 2022, 2-3.
[296] Ibid.

hebben dat er geen effectieve bescherming van de persoonsgegevens voorhanden is, zonder dat de betrokkenen hiervan op de hoogte zijn.

d) Onafhankelijke toezichthoudende autoriteit (supra: afdeling 4)

Ten vierde beschikt China niet over één onafhankelijke gegevensbeschermingsautoriteit. China delegeert deze bevoegdheid aan meerdere overheidsinstanties.[297] Deze instanties bestaan uit de Cyberspace Administration of China (CAC), het Ministerie van Openbare Veiligheid, het Ministerie van Industrie en Informatietechnologie.[298] Daarnaast hebben deze instanties meerdere taken waaronder een van deze taken het toezicht op de bescherming van persoonsgegevens is.[299] De Cyberspace Administration of China (CAC) wordt veelal gezien als de belangrijkste toezichthoudende instantie.[300] Deze instantie voldoet niet aan de voorwaarden onder de AVG. Zo is deze niet onafhankelijk door de nauwe banden met de staat.[301] Bovendien is het niet alleen verantwoordelijk voor de bescherming van persoonsgegevens, maar ook voor netwerk- en cyberbeveiliging.[302] Dit kan resulteren in tegenstrijdige belangen en het opgeven van de gegevensbescherming om bedreigingen te voorkomen en de nationale veiligheid te dienen.

e) Rechtsmiddel tegen handhavingsinstanties (supra: afdeling 4)

Een van de belangrijkste resterende tekortkomingen van het Chinese gegevensbeschermingsregime is dat er geen volledig ontwikkeld gerechtelijk beroepsmechanisme is waarmee personen besluiten of het niet-handelen door handhavingsinstanties op het gebied van gegevensbescherming rechtstreeks kunnen aanvechten. Deze institutionele zwakte beperkt de afdwingbaarheid van individuele rechten en doet vragen rijzen over de verantwoordingsplicht.[303]

---

[297] Art. 60 PIPL; LI Y., 'Cross-Border Data Transfer Regulation in China.' *Rivista Italiana Di Informatica e Diritto* 2021, (67) 73.
[298] X, *Data Protection Laws of the World*, DLA Piper 2022, 240.
[299] Art. 61 PIPL.
[300] LI Y., 'Cross-Border Data Transfer Regulation in China.' *Rivista Italiana Di Informatica e Diritto* 2021, (67) 73.
[301] YANG F., 'Personal Data Protection at the Crossroad in China: Legal Framework, Practical Problems and Suggested Reforms'. *Asia Pacific Law Review* 2019, (62) 75; GELLER A., 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective', *GRUR International* 2020, (1191) 1200; PALMIERI N., 'Data Protection in an Increasingly Globalized World', *Indiana Law Journal* 2019, (297) 321.
[302] Art. 37 中华人民共和国网络安全法 [Cyberbeveiligingswet van de Volksrepubliek China], 7 november 2016, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.
[303] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheidsreferentie, 28 november 2017, WP 254 rev.01, 10, https://ec.europa.eu/newsroom/article29/redirection/document/54200.

Hoewel er tot nu toe geen rechtszaak is geweest tegen de eerder genoemde Chinese handhavingsautoriteiten zelf, is er wel een opmerkelijke zaak geweest tegen een Frans bedrijf in China.[304] In de zaak van de Guangzhou Internet Court spande een betrokkene met succes een rechtszaak aan onder de PIPL, waarbij hij de manier waarop een platform omging met persoonsgegevens aanvocht.[305] Dit was de allereerste zaak in China gebaseerd op de nieuwe PIPL. Deze zaak toont aan dat personen niet geheel zonder verhaal zijn bij Chinese rechtbanken binnen het nieuwe wettelijke kader.

Om deze leemte op te vullen, kunnen mechanismen die vergelijkbaar zijn met die welke in andere adequaatheidsbesluiten worden gebruikt, als model dienen. In het EU-VS-kader voor gegevensprivacy werd namelijk een Hof voor gegevensbescherming opgericht dat individuele klachten behandelt.[306] Soortgelijke mechanismen kunnen in theorie worden ingevoerd om de gegevensstromen tussen de EU en China te faciliteren.

f) Nationale veiligheidsdiensten (supra: afdeling 5)

Het wettelijke kader van China omvat verschillende specifieke wetten die de nationale veiligheidsdiensten ruime toegang geven tot persoonsgegevens.[307] Deze wetten, zoals de nationale veiligheidswet, de nationale inlichtingenwet en de contraspionagewet, verplichten organisaties en personen om inlichtingenactiviteiten te ondersteunen. Het brede en algemene karakter van de toegang van de overheid geeft aanleiding tot bezorgdheid over mogelijke surveillance.[308] Dit kan in strijd zijn met de EU-normen van "noodzakelijkheid en evenredigheid" voor overheidstoezicht,

[304] 广州市互联网法院 25 december 2022, （2022）粤0192民初648号,'左某诉某酒店公司侵犯个人信息权益纠纷案.

[305] KENNEDY G., LAI J. en WONG J., 'Guangzhou internet court issues the first decision on cross-border transfer of personal data under PIPL', *Mayer Brown* 19 december 2024, https://1npdf11.onenorth.com/pdfrenderer.svc/v1/ABCpdf11/GetRenderedPdfByUrl/guangzhou-internet-court-issues-the-first-decision-on-cross-border-transfer-of-personal-data-under-pipl.pdf/?url=https://www.mayerbrown.com/en/pdf/insights/publications/2024/12/guangzhou-internet-court-issues-the-first-decision-on-cross-border-transfer-of-personal-data-under-pipl?pdf-options=countrycode%3ABE (geraadpleegd op 10 januari 2025)

[306] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2023/1795 van de Commissie van 10 juli 2023 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, *Oj.L.* 20 september 2023, 118, http://data.europa.eu/eli/dec_impl/2023/1795/oj.

[307] Art. 138 CPL; Art. 18 ATL; Art. 52 NSL; Art. 16 NIL.

[308] FENG Y., 'The future of China's personal data protection law: challenges and prospects', *Asia Pacific Law Review* 2019, (62) 74.

zoals gedefinieerd in de Europese Essentiële Garanties.[309] Het gebrek aan onafhankelijk toezicht en de beperkte individuele rechtsmiddelen vormen verdere obstakels voor de Chinese gegevensbeschermingsregeling om als "in wezen gelijkwaardig" aan die van de EU te worden beschouwd.

[309] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 10, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

Hoofdstuk: 3 Praktijkonderzoek TikTok

Afdeling 1. Inleiding

Zoals reeds in de inleiding werd toegelicht, is TikTok een applicatie waarmee gebruikers korte video's kunnen creëren en delen, vaak met muziek, dans of komische inhoud. De applicatie, gelanceerd in 2016 door het Chinese bedrijf ByteDance, kent sindsdien een wereldwijde groei aan gebruikers.[310] De werking van TikTok is sterk afhankelijk van algoritmes die gebruikersgedrag analyseren om gepersonaliseerde videocontent aan te bieden.[311] Deze verregaande personalisering, gebaseerd op het verzamelen en verwerken van grote hoeveelheden persoonsgegevens, heeft echter geleid tot juridische en maatschappelijke bezorgdheden.[312] TikTok is zelfs geconfronteerd met verschillende rechtszaken en verboden in diverse landen.[313] De bezorgdheid ligt bij de privacy van gegevens en de veiligheid van jonge gebruikers.[314] Volgens critici zouden Chinese autoriteiten toegang krijgen tot de gegevens van gebruikers omdat ByteDance in China is gevestigd.[315] Het hoofdkantoor van TikTok bevindt zich in Peking, maar het bedrijf heeft ook verschillende Europese vestigingen, waaronder TikTok Technology Limited in Dublin, TikTok Information Technologies UK Limited in Londen, en kantoren in Parijs, Berlijn en Amsterdam.[316]

---

[310] DIXON S.J., 'Most popular social networks worldwide as of February 2025, by number of monthly active users', *Statista* 26 maart 2025, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (geraadpleegd op 8 april 2025); TIKTOK, 'Digital Services Act: Our fourth transparency report on content moderation in Europe', *TikTok Newsroom* 28 ferbuari 2025, https://newsroom.tiktok.com/en-eu/digital-services-act-our-fourth-transparency-report-on-content-moderation-in-europe (geraadpleegd op 8 april 2025).

[311] VOMBATKERE K., MOUSAVI S., ZANNETTOU S. e.a., TikTok and the Art of Personalization: Investigating Exploration and Exploitation on Social Media Feeds, *WWW '24* 2024, (1) 1.

[312] VAN HORENBEEK J., 'Militaire geheime dienst waarschuwt voor AI', *De Morgen* 2 april 2025, https://www.demorgen.be/snelnieuws/militaire-geheime-dienst-waarschuwt-voor-ai~b3bbd0bc/ (geraadpleegd op 8 april 2025); VERHEYDEN T. en VANMELDERT D., 'Laatste kans voor TikTok in VS? Hooggerechtshof buigt zich vandaag over mogelijk verbod', *VRT NWS* 10 januari 2025, https://www.vrt.be/vrtnws/nl/2025/01/08/laatste-kans-voor-tiktok-in-vs/ (geraadpleegd op 20 januari 2025).

[313] Omzendbrief nr. 716 van 17 maart 2023 betreffende het tijdelijk verbod op het gebruik van de TikTok-applicatie, 17 maart 2024, https://www.ejustice.just.fgov.be/mopdf/2024/03/26_1.pdf#page=723; EURONEWS, 'Which countries have banned TikTok and why?', *Euronews* 14 maart 2024, https://www.euronews.com/next/2025/01/17/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears (geraadpleegd op 20 januari 2025).

[314] GOUJARD C., 'TikTok hit with €345M fine for violating children's privacy', *Politico* 15 september 2023, https://www.politico.eu/article/tiktok-fine-social-media-china-violate-children-privacy/ (geraadpleegd op 10 maart 2024).

[315] SINGLETON C., 'It's not just a theory. TikTok's ties to Chinese government are dangerous', *FDD* 18 maart 2024, https://www.fdd.org/analysis/2024/03/18/its-not-just-a-theory-tiktoks-ties-to-chinese-government-are-dangerous/ (geraadpleegd op 20 januari 2025).

[316] BYTEDANCE, 'Over TikTok' *TikTok* s.d., https://www.tiktok.com/about?lang=nl (geraadpleegd op 21 januari 2025).

Afdeling 2. Analyse privacybeleid

Het privacybeleid van 19 november 2023 zal in dit onderzoek uitsluitend worden geraadpleegd om de eerste twee stappen van de EDPB-aanbevelingen te controleren, die noodzakelijk zijn voor een verdere analyse van het beschermingsniveau bij gegevensdoorgifte. De eerste stap bestaat erin op de hoogte te zijn van wat er wordt doorgegeven.[317] Hiervoor wordt nagegaan welke categorieën van persoonsgegevens worden verwerkt, wat de bestemming is van deze gegevens en welke doeleinden daarbij worden vermeld, om zo te kunnen beoordelen of voldaan is aan het beginsel van gegevensminimalisatie. De tweede stap betreft de controle van het doorgifte-instrument dat voor de doorgiften wordt gebruikt.[318] Voor deze stap zal worden onderzocht of het privacybeleid specificeert op welke doorgifte-instrumenten men zich baseert. Het privacybeleid wordt gebruikt omdat artikel 13 en 14 van de AVG ondernemingen verplichten om transparant te zijn over de manier waarop ze persoonsgegevens verzamelen, verwerken, bewaren en doorgeven.[319] Het beleid heeft als voordeel dat het publiek toegankelijk is en specifiek opgesteld is om de betrokkenen te informeren, wat het een goede bron maakt voor eerste inzichten in de gegevensverwerkingen van een organisatie.[320] Een belangrijk nadeel is echter dat deze in de praktijk te algemene formuleringen bevatten die onvoldoende transparantie bieden. Bovendien is het privacybeleid vaak opgesteld vanuit een commercieel oogpunt, waardoor het mogelijk niet strookt met de werkelijkheid.[321]

Onderafdeling 1. Categorieën van persoonsgegevens

Uit het privacybeleid volgt dat TikTok op basis van drie verschillende bronnen informatie verzamelt en verwerkt. Namelijk informatie die de gebruikers verstrekken, informatie die automatisch verzameld wordt en informatie uit andere bronnen.[322]

---

[317] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §8, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.
[318] Ibid., §14.
[319] Art. 13-14 AVG.
[320] HELSEN E., 'Privacybeleid: Waarom heb je het nodig als ondernemer?', *Digitale jurist* 19 juli 2024, https://digitalejurist.be/privacybeleid-waarom-heb-je-het-nodig-als-ondernemer/ (geraadpleegd op 12 april 2024).
[321] SEYEN K., 'Transparantievereiste zet advocaten en marketeers in hun blootje', *DeJuristen* 22 april 2021, https://dejuristen.be/privacy/transparantievereiste-zet-advocaten-en-marketeers-in-hun-blootje/ (geraadpleegd op 12 april 2024).
[322] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).

a) Informatie die de gebruikers verstrekken

Gebruikers van TikTok verstrekken zelf veel persoonlijke gegevens aan het platform. Deze gegevens worden allemaal opgesomd onder de rubriek "informatie die u verstrekt".[323] Onder deze informatie wordt verstaan:

- Profielinformatie
- Gebruikersinhoud
- Directe Berichten
- Uw contacten
- Aankoopinformatie
- Enquêtes, onderzoek en promoties
- Informatie wanneer u contact met ons opneemt.
- Informatie uit formulieren en functies die u gebruikt

Het privacybeleid vermeldt bovendien dat TikTok ook gegevens kan verwerken en verzamelen van niet-gebruikers van het platform. Dit is namelijk mogelijk wanneer informatie over u verschijnt in inhoud gecreëerd of gepubliceerd door gebruikers die wel over een account op TikTok beschikken.

b) Informatie die automatisch verzameld wordt

Daarnaast verzamelt TikTok automatisch gegevens van gebruikers zonder dat ze deze actief verstrekken.[324] Deze informatie wordt veelal verzameld om de gebruiksvriendelijkheid van de applicatie te verbeteren, inhoud te personaliseren of specifieke functies mogelijk te maken. TikTok verzamelt om deze redenen:

- Technische informatie
- Locatie-informatie
- Informatie over het gebruik
- Kenmerken en eigenschappen van de inhoud
- Afgeleide informatie
- Cookies

c) Informatie uit andere bronnen

Tot slot ontvangt TikTok persoonlijke gegevens van derden.[325] Deze externe dienstverlener worden ingezet om onder andere de functionaliteit en de beveiliging te verbeteren. Zo overhandigen ze onder meer gegevens over de effectiviteit van advertenties en transactieverwerkingen. De bronnen waaruit deze informatie voortkomen, zijn:

[323] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, informatie die u verstrekt, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).
[324] Ibid., Informatie die automatisch verzameld wordt.
[325] Ibid., Informatie uit andere bronnen.

- Reclame-, meet- en andere partners
- Handelaren, aanbieders voor de uitvoering van betalingen en transacties.
- Platforms van derden en partners
- Aanvullende bronnen

Onderafdeling 2. Bestemming van gegevens

a) Landen

Daarna moet er onderzocht worden aan welke landen TikTok persoonsgegevens doorgeeft. In het beleid onder de rubriek "Onze wereldwijde activiteiten en gegevensdoorgifte" staat heel algemeen beschreven dat bepaalde entiteiten in de ondernemingsgroep van TikTok "die zich buiten het land waar u woont" beperkte toegang krijgen op afstand.[326] Daarnaast deelt de onderneming informatie met dienstverleners, partners en andere derden die "gevestigd kunnen zijn buiten het land waar u woont".[327] In plaats van een specifieke lijst te voorzien van zo'n landen in het beleid zelf, verwijst TikTok echter naar een aparte pagina met de titel "Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep".[328] Deze pagina verduidelijkt de betrokken landen. Het specifieert meer bepaald dat ze standaardcontracten gebruiken om gegevens over te dragen naar Australië, Brazilië, China, Maleisië, de Filipijnen, Singapore en de Verenigde Staten.[329] Echter wordt nergens verduidelijkt welke specifieke categorieën persoonsgegevens naar welke specifieke derde landen uit deze lijst en voor welke specifieke doeleinden worden doorgegeven. TikTok vermeldt enkel dat de gegevens worden gedeeld om "belangrijke functies uit te voeren".

Om hier meer over te weten te komen, werd voor deze masterproef op 14 oktober 2024 een aanvraag ingediend via het online webformulier van TikTok genaamd "Contact the Data Protection Officer".[330] Reeds drie dagen later werd een uitgebreid antwoord toegestuurd (Bijlage 1). Wat

[326] Ibid., Onze wereldwijde activiteiten en gegevensdoorgifte.
[327] Ibid.
[328] BYTEDANCE, 'Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep', *TikTok* s.d., https://www.tiktok.com/legal/page/eea/transferee-countries/nl (geraadpleegd op 12 oktober 2024).
[329] Ibid.
[330] BYTEDANCE, 'Contact the Data Protection Officer', *TikTok* s.d., https://www.tiktok.com/legal/report/dpo (geraadpleegd op 14 oktober 2024).

meteen opvalt, is dat het op geen enkele wijze naar China verwijst, hoewel de vraag daar expliciet op gericht was.

Volgens de gegevensbeschermingsadviseur hebben TikTok Ierland en het VK standaardcontracten afgesloten met andere groepsentiteiten en externe dienstverleners om wereldwijde activiteiten te ondersteunen. Gegevens worden opgeslagen in de VS, Maleisië en Singapore, met beperkte toegang voor andere onderdelen. Externe partners in onder andere Brazilië, India, Marokko, Maleisië, de Filipijnen, Singapore en de VS ondersteunen functies zoals *cloudservices*, beveiliging, R&D, statistieken, betalingen, klantenondersteuning, moderatie en reclame. Daarnaast gebruikt TikTok SCC's en aanvullende beveiligingsmaatregelen zoals toegangscontrole, versleuteling en netwerkbeveiliging. De gegevensbeschermingsadviseur bezorgde ook de ingevulde SCC's voor doorgiften naar China, maar verder bood deze correspondentie geen extra informatie. De verkregen informatie komt grotendeels overeen met hetgeen in TikToks privacybeleid is opgenomen onder "Hoe we je gegevens delen". Opvallend blijft dat, ondanks de melding op de site over toegang voor Chinese entiteiten, ze enkel de andere landen noemen.

b) Categorieën van ontvangers

Bovendien kunnen ook de categorieën van ontvangers worden geïdentificeerd. Zo deelt TikTok gegevens met dienstverleners, partners, entiteiten binnen hun ondernemingsgroep en anderen. De partners bestaan uit platforms van derden en partners, adverteerders, meet- en gegevenspartners, handelaren voor de uitvoering van betalingen en transacties.[331] Echter wordt er nergens verduidelijkt welke concrete ontvangers in een derde land persoonsgegevens ontvangen.

Onderafdeling 3. Doelbinding

Artikel 13, lid 1, c) AVG vereist dat de verwerkingsverantwoordelijke verwerkingsdoeleinden moet verstrekken.[332] TikTok voldoet aan deze verplichting door twaalf doeleinden op te sommen onder de rubriek "Hoe wij informatie over u gebruiken".[333] Deze omvatten

[331] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, hoe we je gegvens delen, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).
[332] Art. 13, eerste lid, c) AVG.
[333] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, Hoe wij informatie over u gebruiken, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).

- Het platform aan te bieden en te beheren
- Winkelfuncties aan te bieden
- Functies en inhoud te personaliseren en aan te passen
- Handhaving van de voorwaarden, richtlijnen en ander beleid
- Aanbieden van interactieve functies
- Aanbieden en verbeteren van advertentiediensten
- Handhaven en verbeteren van de veiligheid
- Delen van uw informatie met platforms van derden om u functies te bieden
- Faciliteren van onderzoek door onafhankelijke onderzoekers
- Promoten van het platform of diensten van derden
- Voldoen aan wettelijke verplichtingen

Deze doeleinden en nog vele anderen zijn ook terug te vinden onder de rubriek "Onze rechtsgronden en hoe we je gegevens verwerken",[334] waarin het beleid aangeeft op welke rechtsgrond uit artikel 6 AVG TikTok steunt voor de bepaalde verwerkingsdoeleinden.

Onderafdeling 4. Doorgifte-instrument

Volgens stap 2 van de aanbeveling van de EDPB moet er een doorgifte-instrument gekozen worden.[335] Onder de rubriek "Onze wereldwijde activiteiten en gegevensoverdracht" informeert TikTok duidelijk welke doorgifte-instrumenten ze gebruiken voor een adequaat niveau van gegevensbescherming te waarborgen.[336] Zo maken ze enkel gebruik van bestaande adequaatheidsbesluiten en standaardcontracten. Om te weten te komen welk instrument voor welk land gebruikt wordt, wordt er opnieuw verwezen naar de aparte pagina die hierboven reeds aan bod kwam.[337] Voor de landen Canada, Verenigd Koninkrijk, Israël, Japan en Zuid-Korea maakt TikTok gebruik van de adequaatheidsbesluiten die voor deze landen bestaan.[338] Verder worden er

[334] Ibid., Onze rechtsgronden en hoe we je gegevens verwerken.
[335] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, §14, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.
[336] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, Onze wereldwijde activiteiten en gegevensoverdracht, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).
[337] BYTEDANCE, 'Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep', *TikTok* s.d., https://www.tiktok.com/legal/page/eea/transferee-countries/nl (geraadpleegd op 12 oktober 2024).
[338] Ibid.

standaardcontracten opgesteld met Australië, Brazilië, China, Maleisië, de Filipijnen, Singapore en de Verenigde Staten.[339]

Tussenconclusie privacybeleid TikTok

Op basis van de definitie die in deze masterscriptie wordt gehanteerd, kan worden vastgesteld dat TikTok persoonsgegevens doorgeeft aan China. Uit het privacybeleid blijkt dat TikTok verschillende categorieën persoonsgegevens verzamelt en verwerkt. Deze gegevens zijn afkomstig uit drie bronnen: informatie die door gebruikers wordt verstrekt, gegevens die automatisch worden verzameld, en informatie afkomstig van derden.[340] TikTok vermeldt nergens dat bepaalde gegevenscategorieën uitgesloten zijn van toegang door entiteiten in derde landen. Hierdoor kan worden aangenomen dat alle genoemde persoonsgegevens in beginsel in aanmerking komen voor doorgifte. Concreet stelt TikTok dat entiteiten binnen de eigen ondernemingsgroep, waaronder in China, toegang op afstand kunnen krijgen tot persoonsgegevens van gebruikers.[341] Deze toegang vindt plaats op basis van standaardcontracten en wordt verleend met het oog op het uitvoeren van "belangrijke functies".[342] Deze toegang betreft geen louter hypothetische of passieve mogelijkheid, maar een actieve vorm van gegevensbeschikbaarheid. Daarmee is sprake van een daadwerkelijke handeling waarbij persoonsgegevens ter beschikking worden gesteld aan een ontvanger in een derde land.[343]

Het privacybeleid van TikTok maakt het moeilijk of zelfs onmogelijk voor betrokkenen om te bepalen welke categorieën van hun persoonsgegevens worden doorgegeven naar welke landen, voor welke doeleinden en via welke verwerkingsactiviteiten. De AVG vereist nochtans transparantie en verantwoording.[344] Zonder concreet te specifiëren welke persoonsgegevens naar het buitenland worden doorgegeven en met welk doel, kunnen betrokkenen niet beoordelen of dergelijke doorgiften rechtmatig, noodzakelijk en evenredig zijn. Dit gebrek aan specificiteit

---

[339] Ibid.
[340] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, Welke gegevens we verzamelen, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).
[340] Art. 13, eerste lid, c) AVG.
[341] BYTEDANCE, 'Privacybeleid', *TikTok* 19 november 2023, Hoe we je gegevens delen, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).
[342] BYTEDANCE, 'Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep', *TikTok* s.d., https://www.tiktok.com/legal/page/eea/transferee-countries/nl (geraadpleegd op 12 oktober 2024).
[343] HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, 'Bodil Lindqvist', §7; Ger.EU 8 januari 2025, T-354/22, 'Thomas Bindl/Europese Commissie', §135.
[344] Art. 13-14 AVG.

ondermijnt bovendien de effectiviteit van de rechten van betrokkenen. Doordat gebruikers namelijk niet voldoende informatie hebben met betrekking tot deze gegevensdoorgiften, is het beduidend moeilijker om de verwerking van hun gegevens aan te vechten en hun rechten af te dwingen, zoals het recht op bezwaar, het recht op gegevensoverdraagbaarheid, het recht op wissing. Daarnaast brengt de ruime bewoording van de informatie beschreven in "Welke informatie wij verzamelen" de vereiste van noodzakelijkheid en evenredigheid in gevaar.[345] Eveneens is de vage bewoording van “om belangrijke functies uit te voeren” in strijd is met het AVG-principe van doelbinding, aangezien het niet de specifieke doeleinden specifieert.[346]

Afdeling 3. Analyse standaardcontract

In deze afdeling wordt er dieper ingegaan op het standaardcontract waarvan TikTok gebruikmaakt, aangezien er geen adequaatheidsbesluit bestaat voor China.[347] Er wordt bestudeerd of dit document de inhoudelijke kernbeginselen respecteert en of ze de toegang van de overheid tot de persoonsgegevens inperkt. Deze contracten bevatten specifieke clausules die de verantwoordelijkheden schetsen tussen de gegevensexporteur en de gegevensimporteur. Daarnaast zijn er vaak bijlagen bijgevoegd, waarin onder andere de technische en organisatorische maatregelen worden beschreven. Op 14 oktober 2024 werd een aanvraag ingediend via het online webformulier van TikTok genaamd “Contact the Data Protection Officer”.[348] Op 17 oktober 2024 werd het standaardcontract toegestuurd.

Het valt meteen op dat TikTok zich gebaseerd heeft op de nieuwe standaardcontractbepalingen, die de Europese Commissie op 4 juni 2021 heeft uitgevaardigd.[349] Deze nieuwe SCC’s zijn ontworpen als reactie op het *Schrems* II-arrest.

---

[345] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, 10, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

[346] Art. 5, eerste lid, b) AVG; GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie WP 254 rev.01, 28 november 2017, WP 254 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54200.

[347] BYTEDANCE, ‘Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep’, *TikTok*, https://www.tiktok.com/legal/page/eea/transferee-countries/nl (geraadpleegd op 13 oktober 2024); BYTEDANCE, ‘Privacybeleid’, *TikTok* 19 november 2023, https://www.tiktok.com/legal/page/global/privacy-policy-eea-archive/nl.

[348] BYTEDANCE, ‘Contact the Data Protection Officer’, *TikTok* s.d., https://www.tiktok.com/legal/report/dpo (geraadpleegd op 14 oktober 2024).

[349] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening

Onderafdeling 1. Inhoudelijke kernbeginselen

a) Gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden

De SCC's verwijzen niet echt naar de gronden die de rechtmatigheid van de verwerking dienen. Er wordt meer gefocust op de waarborging van een passend beschermingsniveau bij de gegevensdoorgifte. Maar in de clausule 8.1 over doelbinding wordt er gespecifieerd dat er afgeweken kan worden van de oorspronkelijke doeleinden.[350] Hierbij verwijst TikTok naar 2 van de 6 rechtsgronden uit artikel 6 AVG, namelijk de toestemming en de vitale belangen.[351] Zo kan er een bijkomende verwerking plaatsvinden indien de betrokkenen hierom toestemming verleent. Daarnaast is het ook mogelijk indien dit noodzakelijk is om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen.

b) Het beginsel van doelbinding

Clausule 8.1 bepaalt dat de gegevensimporteur de persoonsgegevens enkel mag verwerken voor de specifieke doeleinden die zijn vastgelegd in bijlage 1.B.[352] De doeleinden zijn zeer algemeen beschreven en omvatten: cloud hosting, levering van inhoud, inhoudelijke moderatie, klant- en technische ondersteuning, marketing, analytics, gegevensbeveiliging, onderzoek en ontwikkeling; en online betalingen.[353] Deze lijst is minder uitgebreid dan de doelbinding uit het privacybeleid. Zo ontbreekt er een gelijkende vermelding naar: personalisatie, beleidshandhaving en voldoen aan wettelijke verplichtingen.

c) Het beginsel van kwaliteit en evenredigheid van gegevens

In clausule 8.4 van de SCC van TikTok wordt er verwezen naar het principe van gegevenskwaliteit. Zo rust er de verplichting op de gegevensimporteur, indien deze zich bewust wordt van onnauwkeurigheden of verouderde informatie, de gegevensexporteur op de hoogte te stellen en de gegevens zo snel mogelijk te verwijderen of te corrigeren.[354]

(EU) 2016/679 van het Europees Parlement en de Raad, *Pb.L.* 7 juni 2021, http://data.europa.eu/eli/dec_impl/2021/914/oj.

[350] BYTEDANCE, Standaardcontractbepaling, 8.1 Purpose limitation, 6.

[351] Art. 6, eerste lid a) en d) AVG.

[352] BYTEDANCE, Standaardcontractbepaling, 8.1 Purpose limitation, 6.

[353] BYTEDANCE, Standaardcontractbepaling, Annex I.B. Description of transfers, 16.

[354] BYTEDANCE, Standaardcontractbepaling, 8.4 Storage limitation, 4.

d) Het beginsel van gegevensbewaring

Wat betreft de duur van de gegevensbewaring heeft TikTok geen expliciete duur opgegeven in bijlage 1.B. De onderneming verklaart de gegevens te bewaren voor "de duur van de overeenkomst tussen TikTok en de gegevensimporteur".[355] Dit doet vragen rijzen over de naleving van de AVG-vereiste. Persoonsgegevens mogen namelijk niet langer worden bewaard dan noodzakelijk is voor de verwerking van deze gegevens.[356] Het feit dat de duur gekoppeld is aan de duur van de overeenkomst tussen TikTok en zijn gegevensimporteurs, kan ertoe leiden dat de bewaring langer duurt dan nodig is om de specifieke doeleinden te bereiken waarvoor de gegevens zijn verzameld en wat op zijn beurt de kans op ongeoorloofde openbaarmaking van persoonsgegevens vergroot.

e) Het beginsel van beveiliging en vertrouwelijkheid

Clausule 8.5 regelt de veiligheid van de verwerking. Deze verduidelijkt dat de gegevensimporteur en gegevensexporteur passende technische en organisatorische maatregelen moeten nemen om de veiligheid van de gegevens te waarborgen.[357] Deze maatregelen zijn opgesomd in bijlage 2.[358]

I. Technische en organisatorische maatregelen

Hieronder zal er nagegaan worden welke technische en organisatorische maatregelen de gegevensimporteur neemt bij het verwerken van gegevens. De maatregelen worden vergeleken met de technische en organisatorische maatregelen uit de Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen van de EDPB.[359] Zie tabel 4 en 5 voor een overzicht van de vergelijking.

Allereerst valt bij het onderzoeken van de aanvullende maatregelen van TikTok op dat deze maatregelen zeer algemeen zijn omschreven. Dit is opmerkelijk aangezien uit zowel de

[355] BYTEDANCE, Standaardcontractbepaling, Annex I.B. Description of transfers, 16.
[356] GROEP GEGEVENSBESCHERMING ARTIKEL 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, 29 november 2017, WP260 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54194.
[357] BYTEDANCE, Standaardcontractbepaling, 8.5 Security of processing, 4.
[358] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.
[359] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

aanbevelingen van de EDPB als de Q&A van de Europese Commissie blijkt dat een duidelijke beschrijving van deze aanvullende maatregelen vereist is.[360] De nieuwe SCC's vereisen zelfs expliciet een specifieke omschrijving en geen algemene bewoordingen.[361] Om meer duidelijkheid te krijgen over de reden van deze algemene formulering, werd er opnieuw contact opgenomen met de gegevensbeschermingsadviseur van TikTok. De correspondentie is opgenomen in bijlage 2 van deze masterscriptie. In hun reactie stellen ze dat de details van deze aanvullende technische en organisatorische maatregelen 'vertrouwelijk' zijn. Uit de Q&A van de Europese Commissie blijkt inderdaad dat informatie die beroepsgeheimen bevat, niet gedeeld moet worden.[362] Echter wordt in dat geval wel een verantwoording verwacht waarom informatie niet kan worden verstrekt.[363] Een dergelijke toelichting ontbreekt volledig in bijlage II van TikToks SCC. Het zou daarnaast ook zeer onwaarschijnlijk zijn dat al hun aanvullende maatregelen als bedrijfsgeheimen worden beschouwd.

TikTok heeft op het eerste gezicht wel een aantal algemene technische maatregelen genomen om persoonsgegevens te beschermen wanneer ze naar landen buiten Europa worden doorgestuurd. De onderneming maakt bijvoorbeeld gebruik van versleuteling, beperkt wie toegang heeft tot gegevens, en controleert wie toegang krijgt tot hun systemen.[364] Maar toch zijn er een aantal belangrijke tekortkomingen.

De EDPB zegt namelijk dat gewone beveiligingsmaatregelen niet steeds voldoende zijn als gegevens naar een land worden doorgegeven waar de overheid op grote schaal toegang kan eisen

[360] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 25-44, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; EUROPESE COMMISSIE, 'New Standard Contractual Clauses - Questions and Answers overview', *Europese Commissie* 25 mei 2022, 39. Are there any requirements for filling in the annexes? How detailed should the information be?, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (geraadpleegd op 11 april 2025).

[361] EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad, *Pb.L.* 7 juni 2021, 60 http://data.europa.eu/eli/dec_impl/2021/914/oj.

[362] EUROPESE COMMISSIE, 'New Standard Contractual Clauses - Questions and Answers overview', *Europese Commissie* 25 mei 2022, 39. Are there any requirements for filling in the annexes? How detailed should the information be?, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.

[363] Ibid.

[364] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.

tot die gegevens.[365] Om dit risico in te perken, kan versleuteling van de gegevens als technische maatregel worden ingezet.[366] Hierbij maakt het bedrijf de gegevens onleesbaar voor iedereen die niet de juiste sleutel heeft.[367] Maar het spreekt voor zich dat deze sleutels dan niet in handen mogen zijn van het bedrijf in het derde land. Indien dit wel zo zou zijn, kunnen overheidsinstanties alsnog toegang krijgen tot de gegevens. TikTok geeft aan in bijlage II van hun standaardcontract dat ze versleuteling gebruiken en ook een systeem hebben om deze sleutels te beheren.[368] Echter zeggen ze er niet bij wie die sleutels beheert of waar ze precies bewaard worden. Hierdoor blijft het onduidelijk of overheidsinstanties alsnog toegang kunnen krijgen tot de gegevens.

Ook tijdens het verzenden van gegevens moeten deze worden beschermd tegen onderschepping. De EDPB vereist dat bedrijven sterke vormen van versleuteling en beveiliging moeten gebruiken, zoals de nieuwste versies van beveiligingsprotocollen.[369] TikTok geeft aan dat ze versleutelde verbindingen gebruiken.[370] Zo maken ze gebruik van een VPN, waarmee ze de gegevens versleutelen en hun IP-adressen maskeren. Evenwel wordt er geen informatie verstrekt over hoe sterk die beveiliging precies is. Zonder deze details kan er niet nagegaan worden of deze maatregel voldoende is.

Bovendien raadt de EDPB ook pseudonimisering aan.[371] Dit zorgt ervoor dat persoonsgegevens bewerkt worden, zodat ze niet meer direct naar een persoon herleidbaar zijn.[372] TikTok maakt geen gebruik van deze techniek terwijl het in veel gevallen net een sterke manier is om gegevens extra te beschermen vóór ze het land verlaten.

---

[365] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 18-19, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;
[366] Ibid., 29;
[367] LI N.., OZSU M. en LIU L., *Encyclopedia of Database Systems,* Springer, 2018, 751.
[368] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.
[369] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 29, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;
[370] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.
[371] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 27-28, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;
[372] Art. 4(5) AVG; LI N.., OZSU M. en LIU L., *Encyclopedia of Database Systems,* Springer, 2018, 2932.

Daarnaast neemt TikTok ook nog een aantal organisatorische maatregelen. Zo zijn er interne beleidslijnen, is er een beveiligingsteam, en beperken ze de toegang tot data via onder andere toegangsrechten en dubbele verificatie.[373] Verder wordt elk jaar hun beveiligingsbeleid herzien en zijn er externe audits.[374] Op het eerste gezicht lijken dit goede maatregelen, maar zodra deze maatregelen vergeleken worden met de doeltreffendheidsvereisten van de EDPB, blijken TikToks maatregelen niet voldoende.

De EDPB verwacht dat importbedrijven over interne procedures beschikken, zodat ze verzoeken van overheidsdiensten om toegang tot die gegevens afdoende kunnen behandelen.[375] Dit kan bijvoorbeeld een juridisch team zijn dat beoordeelt of het verzoek wettelijk is. TikTok heeft hier geen maatregel genomen. Ze hebben wel een intern audit- en beveiligingsteam en een algemeen incidentenproces, maar nergens wordt er gespecifieerd wat ze doen als een overheid persoonsgegevens opvraagt.[376] Er is bovendien ook geen mechanisme dat toelaat zich te verzetten tegen zulke verzoeken. Dit baart zorgen omdat uit hoofdstuk 2 blijkt dat China wetten heeft die bedrijven zoals TikTok kunnen verplichten om data af te staan aan de overheid. Bovendien zou een bedrijf ook moeten bijhouden wanneer en waarom een overheid toegang tot gegevens heeft gevraagd, en hoe daarop is gereageerd.[377] TikTok vermeldt nergens dat er een register wordt bijgehouden.

Tot slot geeft TikTok aan dat ze gebruikmaken van het "*need-to-know*"-principe, wat betekent dat werknemers enkel toegang krijgen tot gegevens als dat nodig is voor hun werkzaamheden.[378] Daarnaast voert het bedrijf jaarlijkse toegangscontroles uit en blokkeren ze toegang van medewerkers die het bedrijf verlaten.[379] Maar dit zou niet volstaan volgens de EDPB. Er moet namelijk vooraf worden onderzocht welke gegevens noodzakelijk zijn voor de dienst die geleverd

[373] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.
[374] Ibid.
[375] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 41-42, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;
[376] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.
[377] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 42, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;
[378] Ibid., 43; MAKHECHA J., HARKER D., 'Information Control and the "Need-to-Know" principle', *Deloitte* 1 augustus 2024, https://www.deloitte.com/uk/en/Industries/financial-services/blogs/information-control-and-the-need-to-know-principle.html (geraadpleegd op 13 april 2025).
[379] BYTEDANCE, Standaardcontractbepaling, Annex II Minimum Security Measures, 18-19.

wordt, zodat alleen die gegevens worden doorgestuurd.[380] Er wordt niets gespecifieerd over een analyse in bijlage II. Er is dus een gebrek aan garantie dat er niet te veel data naar het buitenland wordt gestuurd. Bovendien is er geen controle- of sanctiesysteem als blijkt dat het "*need-to-know*"-principe wordt overtreden.

[380] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, 43, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf;

EDPB voorbeeld	TikTok SCC	Beperkingen	Voldoet aan vereisten?
Technologische maatregelen			
Versleuteling bij opslag (back-up doeleinden)	"Encryption of data at rest as instructed by the Transferor" "Key management system"	Sleutelbeheer wordt niet afdoende toegelicht. Geen garantie dat sleutels enkel in EER worden beheerd, en dat de importeur geen toegang heeft tot de sleutels zodat de overheid TikTok niet kan verplichten sleutels af te staan.	Neen
Pseudonimisering voorafgaand aan doorgifte	Niet genoemd in TikToks SCC	Geen pseudonimisering vermeld. Volgens de EDPB een van de weinig doeltreffende maatregelen tegen structurele toegang door overheidsinstanties.	/
Versleuteling tijdens transport	"Remote access via VPN or encrypted connections"	Alleen algemene verwijzing naar VPN/versleuteling. Geen specificaties over sterkte/protocols/sleutelbeheer zoals vereist.	Neen
Gesplitste verwerking (multi-party computation)	Niet genoemd in TikToks SCC	TikToks functionele mogelijkheid tot reconstructie van persoonsgegevens kunnen verhinderen.	/

Tabel 4: Evaluatie technologische maatregelen TikTok

EDPB voorbeeld	TikTok SCC	Beperkingen	Voldoet aan vereisten?
Organisatorische maatregelen			
Interne beleidsmaatregelen bij overheidsverzoeken	"Incident management program" "Dedicated internal audit and security function",	Moet voorzien in een juridische beoordeling of verzetmechanisme.	Neen
Transparantie & logging van overheidsverzoeken	Niet genoemd in TikToks SCC	Exporteur moet geïnformeerd worden, logging vereist.	/
Gegevensminimalisering & toegangsbeperking	"Least privilege", "Need-to-know" beleid "Annual access reviews" MFA en tijdige toegangstermijn	Moet gepaard gaan met voorafgaande analyse welke gegevens noodzakelijk zijn. Handhaving vereist met monitoring, disciplinaire maatregelen.	Beperkt
Betrekken DPO/juridisch team bij doorgifte)	Niet genoemd in TikToks SCC	Een DPO/legal moet advies geven bij doorgiftebeslissingen; toegang tot risicobeoordeling, derde land wetgeving, garanties van importeur.	/
Internationale normen & jaarlijkse herziening	"Security policies aligned to highest industry standards", "Annual review of policies", audits (SOC2/ISO27001)	Moet gekoppeld zijn aan doorgiftecontext.	Beperkt
Geen verdere doorgifte of automatische opschorting bij risico	Niet genoemd in TikToks SCC	Importeur moet toezeggen doorgifte te staken als garanties niet langer houdbaar zijn; geen verdere verspreiding binnen of buiten derde land.	/

Tabel 5: Evaluatie organisatorische maatregelen TikTok

f) Het transparantiebeginsel

Wat betreft de transparantie, bepaalt clausule 8.2 dat de betrokkenen het recht krijgen om te begrijpen (i) wie de gegevens verwerkt, (ii) welke categorieën persoonsgegevens worden verwerkt, (iii) dat de betrokkene het recht heeft een afschrift van deze bepalingen te verkrijgen; iv), welke categorieën derden gegevens ontvangen en voor welke doeleinden.[381]

g) Het recht van toegang, rectificatie, wissing en bezwaar

De betrokkenen beschikken ook over een aantal rechten zoals de toegang, rectificatie en verwijdering van hun persoonsgegevens. Clausule 10 regelt deze rechten. Meerbepaald kan de betrokkene onjuiste of onvolledige gegevens laten rectificeren en persoonsgegevens laten wissen indien ze worden verwerkt in strijd met de bepalingen uit de SCC.[382] Daarnaast kan de betrokkene bezwaar maken tegen de geautomatiseerde besluitvorming.[383]

h) Beperkingen ten aanzien van verdere doorgifte

Tot slot heeft clausule 8.7 betrekking op de beperkingen op de verdere doorgifte van persoonsgegevens door de gegevensimporteur. Deze clausule voorziet strikte voorwaarden zodat het beschermingsniveau consistent blijft bij de verdere doorgifte. Zo mogen de gegevens enkel worden doorgegeven aan derden volgens de gedocumenteerde instructies van de gegevensexporteur.[384] Daarnaast mogen de gegevens enkel doorgegeven worden aan een andere entiteit die een gelijkwaardig passend beschermingsniveau biedt.[385] Dit kan (i) indien de verdere doorgifte plaatsvindt naar een land dat in aanmerking komt voor een adequaatheidsbesluit, (ii) indien de derde passende waarborgen biedt, (ii) indien de verdere doorgifte noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte in het kader van een specifieke administratieve, regelgevende of gerechtelijke procedure, (iv) indien de verdere doorgifte noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon.[386] Maar de gegevens kunnen ook doorgegeven worden indien de derde gebonden is of ermee instemt geboden te zijn door de relevante bepalingen uit de SCC.

[381] BYTEDANCE, Standaardcontractbepaling, 8.2 Transparency, 3.
[382] BYTEDANCE, Standaardcontractbepaling, 10 Data subject rights, 8-9.
[383] Ibid.
[384] BYTEDANCE, Standaardcontractbepaling, 8.7 Onward transfers, 5.
[385] Ibid.
[386] Ibid.

Onderafdeling 2. De toegang van de overheid tot persoonsgegevens

a) Het standaardcontract en de Data Transfer Impact Assessment

In deze onderafdeling wordt er onderzocht wat er in het standaardcontract van TikTok is bepaald over de toegang van de overheid tot deze persoonsgegevens. Deze analyse vloeit voort uit de aanbevelingen van de EDPB over Europese essentiële garanties.[387] TikTok heeft vermoedelijk een *Data Transfer Impact Assessment* uitgevoerd. In deze DTIA worden de wetten en praktijken met betrekking tot overheidstoegang in het land van bestemming geanalyseerd om mogelijke gevolgen voor de rechten van de betrokkenen te identificeren en te beperken.[388] Er werd een aanvraag gestuurd naar TikTok om een kopie te verkrijgen van het document waaruit hun analyse zou kunnen blijken. Helaas werd hier een negatief antwoord op ontvangen, waardoor deze elementen niet beoordeeld kunnen worden (bijlage 3). Dit gebrek aan toegang beperkt de mogelijkheid om TikToks aanpak voor het beheren van deze risico's volledig te onderzoeken en te beoordelen.

Evenwel bevat het standaardcontract van TikTok specifieke bepalingen over toegang tot persoonsgegevens door de overheid. Meerbepaald worden er beperkingen opgelegd aan de manier waarop gegevensimporteurs met verzoeken van de overheid moeten omgaan.[389] Deze bepalingen zijn terug te vinden onder sectie 3 "*Local laws and obligations in case of access by public authorities*".

Allereerst bepaalt clausule 14 dat de partijen verklaren dat ze geen reden hebben om aan te nemen dat de wetten en praktijken in het derde land, de gegevensimporteur verhinderen zijn verplichtingen na te komen.[390] Daarnaast vereist de clausule dat zowel TikTok als de gegevensimporteur de wetten en praktijken van het land van de importeur beoordelen om te

[387] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.
[388] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf; SANFUCHS B., 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II', *GRUR International* 2021, (245) 247.
[389] BYTEDANCE, Standaardcontractbepaling, Section iii – Local laws and obligations in case of access by public authorities, 11-13.
[390] BYTEDANCE, Standaardcontractbepaling, 14 Local laws and practices affecting compliance with the Clauses, 11-12.

bepalen of deze een invloed kunnen hebben op de naleving van de SCC's.[391] De partijen moeten bovendien deze beoordeling documenteren en op verzoek ter beschikking stellen van de bevoegde toezichthoudende autoriteit.[392] Tevens moet de gegevensimporteur de gegevensexporteur onmiddellijk in kennis stellen indien hij redenen heeft om aan te nemen dat hij onderworpen is of is geworden aan wetten of praktijken die vermoedelijk niet meer overeenstemmen met de clausules uit de SCC.[393]

Clausule 15 legt een aantal procedures en waarborgen vast in het geval van mogelijke verzoeken van de overheid om toegang tot persoonsgegevens. Zo wordt de gegevensimporteur verplicht om de gegevensexporteur in kennis te stellen indien hij ofwel een verzoek ontvangt van een overheidsinstantie voor de openbaarmaking van persoonsgegevens, ofwel indien hij kennis krijgt van de rechtstreekse toegang van overheidsinstanties tot de persoonsgegevens in overeenstemming met de wetgeving van het derde land.[394] Hierbij dient de gegevensimporteur informatie te verstrekken over de ontvangen verzoeken. Tot slot moet de gegevensimporteur ook elk verzoek om toegang beoordelen. Als het verzoek niet wettig zou zijn, moet de gegevensimporteur het verzoek aanvechten. Daarenboven mag de gegevensimporteur alleen een minimale hoeveelheid persoonsgegevens bekendmaken die nodig is om aan het verzoek te voldoen.

b) Information Requests Report

TikTok heeft daarnaast ook nog een transparantiecentrum opgericht die halfjaarlijks een rapport uitbrengt over de verzoeken die het ontvangen heeft van de wetshandhavingsinstanties.[395] Het vermeldt hierbij dat de verzoeken zorgvuldig worden beoordeeld.[396] TikTok garandeert hierbij dat gebruikersgegevens alleen openbaar gemaakt worden wanneer een juridische procedure is doorlopen door de aanvrager of in uitzonderlijke noodsituaties, zoals een dreiging van ernstig lichamelijk letsel of de dood van een persoon.[397]

---

[391] Ibid.
[392] Ibid.
[393] Ibid.
[394] BYTEDANCE, Standaardcontractbepaling, 15 Obligations of the data importer in case of access by public authorities, 12-13.
[395] BYTEDANCE, 'Rapport Informatieverzoeken', *Transparantiecentrum* 6 juni 2024, https://www.tiktok.com/transparency/nl-nl/information-requests-2023-2 (geraadpleegd op 2 februari 2025).
[396] Ibid.
[397] Ibid.

Het rapport vermeldt dat TikTok nog geen aanvragen van Chinese wetshandhavingsinstanties heeft ontvangen, maar het is onduidelijk of het bedrijf volledig vrij is om dergelijke informatie te publiceren. De landen met de meeste aanvragen zijn Amerika, Verenigd Koninkrijk, Duitsland en Frankrijk.[398]

Desondanks zijn er naast het rechtstreeks indienen van formele verzoeken bij TikTok nog steeds andere manieren waarop overheden toegang kunnen krijgen tot persoonlijke gegevens. Zo kan er bijvoorbeeld gebruikgemaakt worden van heimelijke surveillancemaatregelen door de Chinese overheid.

c) Project Clover

In het antwoord op de vragen betreffende het standaardcontract, duidde de gegevensbeschermingsadviseur van TikTok ook op hun project Clover.[399] Dit project houdt in dat alle data van Europese gebruikers eind 2024 dienen opgeslagen te worden in Europese datacenters, in Ierland en Noorwegen.[400] Daarnaast gaat TikTok ook samenwerken met het beveiligingsbedrijf NCC Group, dat toezicht zal houden op de data.[401] Het project zou er bovendien voor moeten zorgen dat Chinese werknemers geen toegang meer krijgen tot persoonsgegevens zoals een *e-mailadres*, een telefoonnummer of financiële informatie.[402] Evenwel blijven ze toegang krijgen tot de andere publieke data.[403]

Tussenconclusie TikTok

Het privacybeleid van TikTok schiet ernstig tekort in transparantie, waardoor gebruikers nauwelijks kunnen achterhalen welke categorieën persoonsgegevens worden doorgegeven, naar welke landen, met welk doel en via welke verwerkingsactiviteiten. Deze gebrekkigheid schendt de vereisten van de AVG, die transparantie en verantwoording voorschrijft.[404] Hierdoor kunnen

[398] Ibid.
[399] Zie bijlage 1 en 2.
[400] BYTEDANCE, 'Setting a new standard in European data security with Project Clover', *TikTok Newsroom* 8 maart 2023, https://newsroom.tiktok.com/en-ie/project-clover-ireland (geraadpleegd op 12 maart 2025); BYTEDANCE, 'Progress update on Project Clover', *TikTok Newsroom* 12 juli 2024, https://newsroom.tiktok.com/en-eu/progress-update-on-project-clover-measures (geraadpleegd op 12 maart 2025).
[401] Ibid.
[402] KASTELEIJN N., 'Experts kritisch op plan TikTok om China buiten de deur te houden', *NOS* 11 september 2023, https://nos.nl/artikel/2490070-experts-kritisch-op-plan-tiktok-om-china-buiten-de-deur-te-houden (geraadpleegd op 12 maart 2025).
[403] Ibid.
[404] Art. 13-14 AVG.

betrokkenen niet beoordelen of de doorgiften naar China rechtmatig, noodzakelijk en evenredig zijn. Ook tast dit hun mogelijkheid aan om hun fundamentele rechten uit te oefenen.

Daarnaast is TikTok ook niet transparant in haar SCC's. Zo zijn de technische en organisatorische maatregelen die het zegt te nemen bij internationale doorgiften te algemeen geformuleerd. Deze informatie is nochtans cruciaal om vast te stellen of een gelijkwaardig beschermingsniveau kan worden gegarandeerd. In mijn ogen heeft TikTok dan ook gefaald en zouden doorgiften naar China moeten worden stopgezet. Indien details over de aanvullende maatregelen werkelijk om vertrouwelijke redenen zijn achtergehouden, zou dit op zijn minst duidelijk aangegeven dienen te worden. Transparantie is namelijk essentieel om de waarborgen te kunnen controleren. Mijn bezorgdheid weerklinkt ook in de media. Zo blijkt uit verscheidene nieuwsartikelen dat TikTok dreigt een boete van meer dan 500 miljoen euro te krijgen van de Ierse gegevensbeschermingsautoriteit omdat het Europese gebruikersgegevens illegaal naar China heeft doorgestuurd.[405] De gegevens zouden daar toegankelijk geweest zijn voor ingenieurs van het moederbedrijf.[406]. De Ierse Data Protection Commission bevestigt deze boete. Het ontdekte dat TikTok niet voldoende waarborgen had getroffen om te garanderen dat de gegevensbescherming in China gelijkwaardig is aan die in de EU.[407] Bovendien werd vastgesteld dat TikTok gebruikers onvoldoende informeerde over deze gegevensoverdrachten en onjuiste informatie verstrekte tijdens het onderzoek. TikTok moet binnen zes maanden zijn gegevensverwerking in overeenstemming brengen met de AVG, of het overdragen van gegevens naar China opschorten. Ook privacy-organisatie *Noyb* sluit zich hierbij aan. Zij stelt dat bedrijven zoals TikTok persoonsgegevens uit Europa overdragen aan autoritaire regimes zoals China, zonder afdoende waarborgen.[408]

---

[405] STOLTON S., 'TikTok faces fine over €500 million for EU-China data export', *Bloomberg* 3 april 2025, https://www.bloomberg.com/news/articles/2025-04-03/tiktok-faces-fine-over-500-million-for-eu-data-sent-to-china? (geraadpleegd op 9 april 2025); AUSSEMS M., 'EU plant 500 miljoen euro boete voor TikTok, overweegt dubbele voor X', *ITdaily* 4 april 2025, https://itdaily.be/nieuws/business/eu-boete-tiktok-x/ (geraadpleegd op 9 april 2025).

[406] DAVIES P., 'TikTok faces €500 million fine for illegally shipping European user data to China – report', *Euronews* 3 april 2025, https://www.euronews.com/next/2025/04/03/tiktok-faces-500-million-fine-for-illegally-shipping-european-user-data-to-china-report (geraadpleegd op 9 april 2025).

[407] DPC, 'Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China', *An Coimisiún um Chosaint Sonrai Data Protection Commission* 2 mei 2025, https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following (geraadpleegd op 2 mei 2025).

[408] POIREAULT K., 'Noyb Files GDPR Complaints Against TikTok and Five Chinese Tech Giants', *Infosecurity Magazine* 17 januari 2025, https://www.infosecurity-magazine.com/news/noyb-gdpr-complaints-tiktok-temu/ (geraadpleegd op 9 april 2025); X, 'TikTok, AliExpress, SHEIN & Co surrender Europeans' data to authoritarian

Besluit

Deze masterscriptie onderzoekt de hoofdonderzoeksvraag: “Hoe wordt het recht op gegevensbescherming van alle personen binnen de Europese Unie gewaarborgd bij de doorgifte van persoonsgegevens van de EU naar China door een Chinese onderneming zoals TikTok?”. Om deze hoofdvraag te beantwoorden werden drie deelonderzoeksvragen geformuleerd.

De eerste subonderzoeksvraag luidt: “Wat zijn de vereisten of beperkingen voor de doorgifte van persoonsgegevens naar derde landen volgens de Algemene Verordening Gegevensbescherming (AVG)?”. Deze vraag werd behandeld in hoofdstuk 1. In dit hoofdstuk werd de AVG geanalyseerd, met name hoofdstuk V AVG, waarin de drie juridische mechanismen voor gegevensdoorgiften worden beschreven: adequaatheidsbesluiten, passende waarborgen (zoals SCC's en BCR's) en afwijkingen voor specifieke situaties. De beginselen uit de AVG benadrukken dat het beschermingsniveau voor persoonsgegevens niet mag afnemen wanneer deze de EU verlaten. De uitspraken van het Hof van Justitie van de Europese Unie in de zaken *Schrems* en *Schrems* II hebben verduidelijkt dat alle doorgiftemechanismen een beschermingsniveau moeten garanderen dat in wezen gelijkwaardig is aan het niveau dat binnen de EU wordt gegarandeerd. Daarnaast werd er ingegaan op de inhoudelijke criteria waarmee rekening moet worden gehouden bij de beoordeling van de bescherming van derde landen. Dit is belangrijk aangezien het Hof in *Schrems* II heeft beoordeeld dat gegevensexporteurs die standaardcontractbepalingen willen gebruiken, bijkomend moeten analyseren of het derde land een passend beschermingsniveau garandeert. Er zijn inconsistenties gevonden tussen de EU-instellingen bij de interpretatie van deze inhoudelijke criteria, waarbij de Commissie flexibeler is en het HvJ-EU een strengere aanpak hanteert. Voor het beoordelen van het gegevensbeschermingsniveau van derde landen werd een consistente aanpak gebruikt. Zo werd er voor de volgende subonderzoeksvragen gekeken naar de inhoudelijke kernbeginselen, de procedurele en handhavingsmechanismen en de toegang van de overheid tot persoonsgegevens.

De tweede subonderzoeksvraag luidt: “Voldoet het Chinese raamwerk aan een passend beschermingsniveau dat in wezen gelijkwaardig is aan het niveau dat binnen de Unie wordt

China’, *Noyb* 16 januari 2025, https://noyb.eu/en/tiktok-aliexpress-shein-co-surrender-europeans-data-authoritarian-china (geraadpleegd op 9 april 2025).

gewaarborgd?". Hoofdstuk 3 tracht hier een antwoord op te formuleren. Er wordt een diepgaande analyse uitgevoerd op de Chinese wetgeving inzake gegevensbescherming, namelijk de Personal Information Protection Law (PIPL). Hoewel het Chinese rechtskader duidelijk is gebaseerd op de principes uit de AVG, bleken er nog belangrijke verschillen te bestaan. Deze omvatten het ontbreken van een onafhankelijke toezichthoudende autoriteit, onvoldoende rechtsmiddelen en te algemeen omschreven beperkingen van de bevoegdheden van de overheid op het gebied van toezicht. Wat vooral zorgen baart, is de toegang die aan Chinese overheidsinstanties wordt verleend voor nationale veiligheids- en wetshandhavingsdoeleinden. China voldoet in mijn ogen momenteel niet aan de "in wezen gelijkwaardige" norm die vereist is voor de doorgifte van persoonsgegevens op grond van de AVG, dus bedrijven zouden gebruik kunnen maken van SCC's als passende waarborg bij doorgiften. De verwerkingsverantwoordelijke is hierbij verplicht om een *Data Transfer Impact Assessment* uit te voeren. Het Chinese recht is daarbij van doorslaggevend belang, aangezien het bedrijf moet nagaan of, gelet op de omstandigheden van de doorgifte en de wetgeving in het derde land, de SCC's daadwerkelijk kunnen worden nageleefd en of de bescherming van persoonsgegevens kan worden gewaarborgd. Als uit de DTIA blijkt dat het Chinese rechtskader afbreuk doet aan de werking van de SCC's en er geen aanvullende technische of organisatorische maatregelen getroffen kunnen worden die dit compenseren, dan is doorgifte van persoonsgegevens naar China niet toegestaan onder de AVG. Voor Chinese bedrijven betekent dit dat ze ofwel structurele maatregelen moeten treffen om aan het EU-niveau van gegevensbescherming te voldoen, ofwel EU-persoonsgegevens enkel binnen de EU of in landen met een adequaatheidsbesluit zouden moeten verwerken.

De derde subonderzoeksvraag luidt: "Welke technieken gebruiken de Chinese techondernemingen om toch persoonsgegevens door te geven en zijn er problemen te identificeren?". Dit werd in hoofdstuk 4 onderzocht aan de hand van een studie van het sociaal media platform TikTok. De analyse van het privacybeleid en de standaardcontractbepalingen onthulde een paar problemen. TikTok is namelijk niet voldoende transparant over welke gegevens worden doorgegeven, voor welke doeleinden en op basis van welke rechtsgrondslag. Daarnaast is er weinig bewijs dat ondernemingen beoordelingen van doorgiften uitvoeren of effectieve aanvullende maatregelen nemen. Bovendien ontwijkt de onderneming de vraag hoe ze omgaan met het risico van toegang tot persoonsgegevens door Chinese autoriteiten. We kunnen concluderen dat TikTok op de goede weg is, maar dat ze hun naleving nog steeds moeten verbeteren op het vlak van transparantie, opslagbeperking en doelbinding.

Concluderend toont deze masterscriptie dat er nog steeds een aantal juridische problemen zijn bij gegevensdoorgiften ondanks dat de EU de uitgebreide Algemene Verordening Gegevensbescherming heeft uitgevaardigd. Daarnaast kan er bezorgdheid worden geuit op de Chinese wetgeving met name wat betreft toegang door de overheid en afdwingbaarheid. Bovendien ontbreekt het bij TikTok aan transparantie en hebben ze moeite om in de praktijk aan de AVG-vereisten te voldoen, waardoor er onrust ontstaat over de doeltreffendheid van de huidige waarborgen voor de bescherming van de gegevens van EU-inwoners bij doorgifte naar China.

Aangezien de omvang van deze masterscriptie beperkt was, is bijkomend onderzoek aanbevolen naar hoe andere Chinese bedrijven zoals AliExpress en Huawei omgaan met hun verantwoordelijkheden. Hoewel aanvankelijk beoogd werd om ook AliExpress te onderzoeken en hiervoor een SCC-verzoek werd verstuurd, bleef een reactie uit. Dergelijk vervolgonderzoek kan helpen bepalen of TikTok een uitzondering vormt binnen de Chinese ondernemingen.

Bibliografie

WETGEVING

Handvest van de grondrechten van de Europese Unie, *Pb.C.* 7 juni 2016, http://data.europa.eu/eli/treaty/char_2016/oj.

Verdrag betreffende de werking van de Europese Unie*, Pb.C.* 7 juni 2016.

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Hierna: AVG), *Pb.L.* 4 mei 2016, http://data.europa.eu/eli/reg/2016/679/oj.

Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren, *Pb.L.* 28 februari 2011, http://data.europa.eu/eli/reg/2011/182/oj.

Omzendbrief nr. 716 van 17 maart 2023 betreffende het tijdelijk verbod op het gebruik van de TikTok-applicatie, 17 maart 2024, https://www.ejustice.just.fgov.be/mopdf/2024/03/26_1.pdf#page=723.

中华人民共和国个人信息保护法 [wet op de bescherming van persoonlijke informatie van de Volksrepubliek China], 20 augstus 2021, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.

中华人民共和国刑事诉讼法 [De wet op de strafvordering van de Volksrepubliek China], 1 juli 1979, https://www.gov.cn/flfg/2012-03/17/content_2094354.htm.

中华人民共和国反恐怖主义法 [Anti-terrorismewet van de Volksrepubliek China], 27 december 2015, http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm.

中华人民共和国反间谍法 [Anti-spionagewet van de Volksrepubliek China], 26 april 2023, https://www.gov.cn/yaowen/2023-04/27/content_5753385.htm.

中华人民共和国国家安全法 [Nationale veiligheidswet van de Volksrepubliek China], 1 juli 2015, https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm.

中华人民共和国国家情报法 [Nationale inlichtingenwet van de Volksrepubliek China], 27 juni 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm.

中华人民共和国宪法 [Grondwet van de Volksrepubliek China], 4 december 1982, https://www.gov.cn/guoqing/2018-03/22/content_5276318.htm.

中华人民共和国数据安全法 [Wet op gegevensbeveiliging van de Volksrepubliek China], 10 juni 2021, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm.

中华人民共和国网络安全法 [Cyberbeveiligingswet van de Volksrepubliek China], 7 november 2016, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

全国人民代表大会常务委员会关于加强网络信息保护的决定 [Besluit van het Permanent Comité van het Nationale Volkscongres over het versterken van de bescherming van netwerkinformatie], 28 December 2012, https://www.gov.cn/jrzg/2012-12/28/content_2301231.htm.

RECHTSPRAAK

HvJ 6 november 2003, nr. C-101/01, ECLI:EU:C:2003:596, ‘Bodil Lindqvist’.

HvJ 23 september 2015, nr. C-362/14, ECLI:EU:C:2015:650, ‘Schrems/Data Protection Commissioner’.

HvJ 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, ‘Data Protection Commissioner/Facebook Ireland en Schrems’.

HvJ 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592.

Ger.EU 8 januari 2025, T-354/22, ‘Thomas Bindl/Europese Commissie’.

广州市互联网法院 25 december 2022, (2022）粤0192民初648号, ‘左某诉某酒店公司侵犯个人信息权益纠纷案.

RECHTSLEER

BEUDELS M., ‘Duiding bij rechtspraak: internationale gegevensdoorgiften na het Schrems II–arrest’ *Tijdschrift Privacy en Persoonsgegevens* 2021, 18.

BOBEK M., Conclusie bij HvJ 16 juli 2020, C-498/16, ECLI:EU:C:2017:863.

BU-PASHA S., ‘Cross-border issues under EU data protection law with regards to personal data protection.’ *Information & Communications Technology Law* 2017, 213.

BYGRAVE L.A., Data Privacy Law, Oxford University Press, 2014.

BYTEDANCE, Standaardcontractbepaling.

COMPAGNUCCI M.C., ABOY M., MINSSEN T. en NAEF T., *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs),* SSRN, 2021.

DE BOEL L. en BRODAHL L., ‘Schrems II: biedt de EDPB raad?: Toelichting bij de aanbevelingen van de EDPB met betrekking tot internationale gegevensdoorgiftes’, *Tijdschrift Privacy en Persoonsgegevens* 2021, 12.

DE BOER D.S., ‘Internationale doorgifte van persoonsgegevens: aandachtspunten bij het gebruik van modelcontracten’, *Contracteren* 2021, 105.

DE CARVALHO D., LEONOR S., ‘Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108.’, *European Data Protection Law Review* 2019, 54.

DRECHSLER L., “Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation.”, *Review of European Administrative Law* 2023, 35.

DRECHSLER L., “What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights.” *Jusletter IT* 2019, 1.

DRECHSLER L., KAMARA I., ‘Essential equivalence as a benchmark for international data transfers after Schrems II’, in KOSTA E., LEENES R., *Essential equivalence as a benchmark for international data transfers after Schrems II*, Edward Elgar Publishing, 2022.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2021, 01/2020, §50, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_nl.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, 10 november 2020, 02/2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Advies 5/2023 betreffende het ontwerp van uitvoeringsbesluit van de Europese Commissie inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, 28 februari 2023, 5/2023, https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_nl.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Guidelines 02/2024 on Article 48 GDPR, 2 december 2024, 02/2024, https://www.edpb.europa.eu/system/files/2024-12/edpb_guidelines_202402_article48_en.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen inzake internationale doorgiften overeenkomstig hoofdstuk V van de AVG, 14 februari 2023, 05/2021, 3, https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_nl.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 2/2018, 25 mei 2018, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_nl.pdf.

EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan, 18 juli 2023, 1/2023, https://www.edpb.europa.eu/system/files/2023-07/edpb_statement_202301_statement_on_japan_adequacy_review_en.pdf.

EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad, *Pb.L.* 7 juni 2021, http://data.europa.eu/eli/dec_impl/2021/914/oj.

EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2022/254 van de Commissie van 17 december 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door de Republiek Korea krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 24 februari 2022, http://data.europa.eu/eli/dec_impl/2022/254/oj.

EUROPESE COMMISSIE, Uitvoeringsbesluit (EU) 2023/1795 van de Commissie van 10 juli 2023 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad inzake het passende niveau van bescherming van persoonsgegevens krachtens het EU-VS-kader voor gegevensbescherming, *Oj.L.* 20 september 2023, http://data.europa.eu/eli/dec_impl/2023/1795/oj.

EUROPESE COMMISSIE, Uitvoeringsbesluit van de Commissie (EU) 2019/419 van 23 januari 2019 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad over de passende bescherming van persoonsgegevens door Japan krachtens de Wet bescherming persoonsinformatie, *Oj.L.* 19 maart 2019, http://data.europa.eu/eli/dec_impl/2019/419/oj.

EUROPESE COMMISSIE, Uitvoeringsverordening (EU) 2021/1772 van de Commissie van 28 juni 2021 overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad betreffende de passende bescherming van persoonsgegevens door het Verenigd Koninkrijk, *Oj.L.* 11 oktober 2021, http://data.europa.eu/eli/dec_impl/2021/1772/oj.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste evaluatie van de werking van het adequaatheidsbesluit voor Japan, 3 april 2023, COM(2023) 275, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52023DC0275.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste evaluatie van de adequaatheidsbesluiten die zijn vastgesteld op grond van artikel 25, lid 6, van Richtlijn 95/46/EG, 15 januari 2024, COM(2024) 7, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52024DC0007.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste jaarlijkse evaluatie van de werking van het EU-VS-privacyschild, 18 oktober, 2017, COM(2017) 611, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017DC0611.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de tweede evaluatie van de werking van het EU-VS-privacyschild, 19 december, 2018, COM(2018) 860, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018DC0860.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de derde jaarlijkse evaluatie van de werking van het EU-VS-privacyschild, 23 oktober, 2019, COM(2019) 495, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52019DC0495.

EUROPESE COMMISSIE, Verslag van de Commissie aan het Europees Parlement en de Raad over de eerste periodieke evaluatie van de werking van het adequaatheidsbesluit inzake het kader voor gegevensbescherming EU-VS, 9 oktober 2024, COM(2024) 451, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52024DC0451.

FARRAS O., RIBES-GONZ´ALEZ J. en RICCI S., 'Privacy-preserving Data Splitting: A Combinatorial Approach', *Designs, Codes and Cryptography* 2018, 1.

FENG Y., 'The future of China's personal data protection law: challenges and prospects', *Asia Pacific Law Review* 2019, 62.

GELLER A., 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective', *GRUR International* 2020, 1191.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, Adequaatheisreferentie, 28 november 2017, WP 254 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54200.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, 29 november 2017, WP260 rev.01, https://ec.europa.eu/newsroom/article29/redirection/document/54194.

GROEP GEGEVENSBESCHERMING ARTIKEL 29,, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74, 3 juni 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf.

GÜNTHER HILPERT H., KRUMBEIN F., en STANZEL V., '*China's Guided Memory. How Historical Events Are Remembered, Glorified, Reinterpreted, and Kept Quiet'*, Stiftung Wissenschaft und Politik (SWP), 2020.

KUNER C., BYGRAVE L.A., DOCKSEY C. en DRECHSLER L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020.

LI N.., OZSU M. en LIU L., *Encyclopedia of Database Systems,* Springer, 2018.

LI Y., 'Cross-Border Data Transfer Regulation in China.' *Rivista Italiana Di Informatica e Diritto* 2021, 67.

LIU J., 'Towards a Global Regulatory Framework for Cross-Border Data Flows—Fundamental Concerns and the China's Approach.' *Frontiers of Law in China* 2022, 412.

LOUISA L., *The people's republic of amnesia: Tiananmen revisited,* Oxford University Press, 2014.

NAEF T., *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law,* Springer, 2023.

O'BRIEN M., 'Classifying Cultural and Physical Destruction: Are Modern Historical and Current Human Rights Violations in China Violations of International Criminal Law?', *Criminal Law Forum* 2015, 533.

PALMIERI N., 'Data Protection in an Increasingly Globalized World', *Indiana Law Journal* 2019, 297.

PHILLIPS M., 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR*)', Hum Genet* 2018, 575.

PIETERS D. en DEMARSIN B., *Rechtsvergelijking: de uitdagende wereld van het recht*, Acco, 2023.

ROTH P., 'Adequate Level of Data Protection' in Third Countries Post-Schrems and under the General Data Protection Regulation', *Journal of Law, Information and Science* 2017, 49.

SANFUCHS B., 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II', *GRUR International* 2021, 245.

VAN DEN BULCK P., 'Transfers of personal data to third countries', *ERA Forum* 2017, (229) 236.

VOIGT P., VD BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing, 2017.

VOMBATKERE K., MOUSAVI S., ZANNETTOU S. e.a., TikTok and the Art of Personalization: Investigating Exploration and Exploitation on Social Media Feeds, *WWW '24* 2024, 1.

VOSS W., 'Cross-border data flows, the GDPR, and data governance', *Wash. Int'l L.J.* 2020, 485.

WAGNER J., 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?', *International Data Privacy Law* 2018, 318.

WOLF C., 'Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers', *Washington University Journal of Law & Policy* 2013, 227.

X, *Data Protection Laws of the World*, DLA Piper 2022.

YANG F., 'Personal Data Protection at the Crossroad in China: Legal Framework, Practical Problems and Suggested Reforms'. *Asia Pacific Law Review* 2019, 62.

ZHAO Y., *Chinese Legal Reform and the Global Legal Order*, Cambridge University Press, 2017.

MEDIA

ACCESSIBLE LAW, 'Personal Information Protection Law of the People's Republic of China', *Personalinformationprotectionlaw,* 2021, https://personalinformationprotectionlaw.com (geraadpleegd op 14 oktober 2014).

AUSSEMS M., 'EU plant 500 miljoen euro boete voor TikTok, overweegt dubbele voor X', *ITdaily* 4 april 2025, https://itdaily.be/nieuws/business/eu-boete-tiktok-x/ (geraadpleegd op 9 april 2025).

BYTEDANCE, 'Contact the Data Protection Officer', *TikTok* s.d., https://www.tiktok.com/legal/report/dpo (geraadpleegd op 14 oktober 2024).

BYTEDANCE, 'Onze wereldwijde activiteiten en gegevensoverdracht: Opslag en beperkte toegang op afstand binnen onze Ondernemingsgroep', *TikTok* s.d., https://www.tiktok.com/legal/page/eea/transferee-countries/nl (geraadpleegd op 12 oktober 2024).

BYTEDANCE, ‘Over TikTok’ *TikTok* s.d., https://www.tiktok.com/about?lang=nl (geraadpleegd op 21 januari 2025).

BYTEDANCE, ‘Privacybeleid’, *TikTok* 19 november 2023, https://www.tiktok.com/legal/page/eea/privacy-policy/nl (geraadpleegd op 12 oktober 2024).

BYTEDANCE, ‘Progress update on Project Clover’, *TikTok Newsroom* 12 juli 2024, https://newsroom.tiktok.com/en-eu/progress-update-on-project-clover-measures (geraadpleegd op 12 maart 2025).

BYTEDANCE, ‘Rapport Informatieverzoeken’, *Transparantiecentrum* 6 juni 2024, https://www.tiktok.com/transparency/nl-nl/information-requests-2023-2 (geraadpleegd op 2 februari 2025).

BYTEDANCE, ‘Setting a new standard in European data security with Project Clover’, *TikTok Newsroom* 8 maart 2023, https://newsroom.tiktok.com/en-ie/project-clover-ireland (geraadpleegd op 12 maart 2025).

DAVIES P., ‘TikTok faces €500 million fine for illegally shipping European user data to China – report’, *Euronews* 3 april 2025, https://www.euronews.com/next/2025/04/03/tiktok-faces-500-million-fine-for-illegally-shipping-european-user-data-to-china-report (geraadpleegd op 9 april 2025).

DIXON S.J., ‘Most popular social networks worldwide as of February 2025, by number of monthly active users’, *Statista* 26 maart 2025, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (geraadpleegd op 8 april 2025).

DPC, ‘Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China’, *An Coimisiún um Chosaint Sonrai Data Protection Commission* 2 mei 2025, https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following (geraadpleegd op 2 mei 2025).

EURONEWS, ‘Which countries have banned TikTok and why?’, *Euronews* 14 maart 2024, https://www.euronews.com/next/2025/01/17/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears (geraadpleegd op 20 januari 2025).

EUROPESE COMMISSIE, ‘Adequacy decisions’, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=nl (geraadpleegd op 8 oktober 2024).

EUROPESE COMMISSIE, ‘New Standard Contractual Clauses - Questions and Answers overview’, *Europese Commissie* 25 mei 2022, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en (geraadpleegd op 11 april 2025).

GOLD A., ‘China’s new privacy law leaves U.S. behind’, *Axios* 23 november 2021, https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind (geraadpleegd op 13 februari 2024).

HELSEN E., ‘Privacybeleid: Waarom heb je het nodig als ondernemer?’, *Digitale jurist* 19 juli 2024, https://digitalejurist.be/privacybeleid-waarom-heb-je-het-nodig-als-ondernemer/ (geraadpleegd op 12 april 2024).

KASTELEIJN N., ‘Experts kritisch op plan TikTok om China buiten de deur te houden’, *NOS* 11 september 2023, https://nos.nl/artikel/2490070-experts-kritisch-op-plan-tiktok-om-china-buiten-de-deur-te-houden (geraadpleegd op 12 maart 2025).

KE X., LIU V., LUO Yen YU Z., ‘Analyzing China's PIPL and how it compares to the EU's GDPR’, *Iapp* 24 augustus 2021, https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr (geraadpleegd op 8 december 2024).

KENNEDY G., LAI J. en WONG J., ‘Guangzhou internet court issues the first decision on cross-border transfer of personal data under PIPL’, *Mayer Brown* 19 december 2024, https://1npdf11.onenorth.com/pdfrenderer.svc/v1/ABCpdf11/GetRenderedPdfByUrl/guangzhou-internet-court-issues-the-first-decision-on-cross-border-transfer-of-personal-data-under-pipl.pdf/?url=https://www.mayerbrown.com/en/pdf/insights/publications/2024/12/guangzhou-internet-court-issues-the-first-decision-on-cross-border-transfer-of-personal-data-under-pipl?pdf-options=countrycode%3ABE (geraadpleegd op 10 januari 2025).

MAKHECHA J., HARKER D., ‘Information Control and the “Need-to-Know” principle’, *Deloitte* 1 augustus

2024, https://www.deloitte.com/uk/en/Industries/financial-services/blogs/information-control-and-the-need-to-know-principle.html (geraadpleegd op 13 april 2025).

META, ‘How Meta Uses Legal Bases for Processing Ads in the EU’, *Meta Newsroom,* 4 januari 2023, https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/ (geraadpleegd op 8 oktober 2024).

POIREAULT K., ‘Noyb Files GDPR Complaints Against TikTok and Five Chinese Tech Giants’, *Infosecurity Magazine* 17 januari 2025, https://www.infosecurity-magazine.com/news/noyb-gdpr-complaints-tiktok-temu/ (geraadpleegd op 9 april 2025).

SINGLETON C., ‘It’s not just a theory. TikTok’s ties to Chinese government are dangerous’, *FDD* 18 maart 2024, https://www.fdd.org/analysis/2024/03/18/its-not-just-a-theory-tiktoks-ties-to-chinese-government-are-dangerous/ (geraadpleegd op 20 januari 2025).

SEYEN K., ‘Transparantievereiste zet advocaten en marketeers in hun blootje’, *DeJuristen* 22 april 2021, https://dejuristen.be/privacy/transparantievereiste-zet-advocaten-en-marketeers-in-hun-blootje/ (geraadpleegd op 12 april 2024).

STOLTON S., ‘TikTok faces fine over €500 million for EU-China data export’, *Bloomberg* 3 april 2025, https://www.bloomberg.com/news/articles/2025-04-03/tiktok-faces-fine-over-500-million-for-eu-data-sent-to-china? (geraadpleegd op 9 april 2025).

THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA, ‘Personal Information Protection Law of the People's Republic of China’, *NPC GOV* 29 december 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (geraadpleegd op 10 oktober 2024).

TIKTOK, ‘Digital Services Act: Our fourth transparency report on content moderation in Europe’, *TikTok Newsroom* 28 ferbuari 2025, https://newsroom.tiktok.com/en-eu/digital-services-act-our-fourth-transparency-report-on-content-moderation-in-europe (geraadpleegd op 15 april 2025).

VAN HORENBEEK J., ‘Militaire geheime dienst waarschuwt voor AI’, *De Morgen* 2 april 2025, https://www.demorgen.be/snelnieuws/militaire-geheime-dienst-waarschuwt-voor-ai~b3bbd0bc/ (geraadpleegd op 8 april 2025).

VERHEYDEN T. en VANMELDERT D., ‘Laatste kans voor TikTok in VS? Hooggerechtshof buigt zich vandaag over mogelijk verbod’, *VRT NWS* 10 januari 2025, https://www.vrt.be/vrtnws/nl/2025/01/08/laatste-kans-voor-tiktok-in-vs/ (geraadpleegd op 20 januari 2025).

X, ‘TikTok, AliExpress, SHEIN & Co surrender Europeans’ data to authoritarian China’, *Noyb* 16 januari 2025, https://noyb.eu/en/tiktok-aliexpress-shein-co-surrender-europeans-data-authoritarian-china (geraadpleegd op 9 april 2025).

Bijlagen

BIJLAGE 1: CORRESPONDENTIE TIKTOK ONDERSTEUNINGSAANVRAAG (16 OKTOBER 2024)

Hello,

Thank you for contacting TikTok.

We understand that you're interested in the Standard Contractual Clauses that TikTok Ireland and UK use to transfer personal information outside the European Economic Area (**EEA**), Switzerland, and United Kingdom (**UK**).

Transfer Subject to Appropriate Safeguards
Where EU/EEA/UK user personal data is transferred from the EU/EEA/UK to a third country (i.e., countries recognised as not having adequate data protection laws), the EU GDPR and UK GDPR require a lawful data transfer mechanism.

For transfers of personal data from the EU/EEA/UK subject to the GDPR and UK GDPR, TikTok relies on:

- Standard Contractual Clauses ("**EU SCCs**"), which are a standard-form contract issued by the European Commission with *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)
- the UK International Data Transfer Addendum (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) issued by the UK Information Commissioner under section 119A of the UK Data Protection Act 2018 (the "**UK SCCs"**; **UK SCCs** and **EU SCCs,** together **SCCs**).

TikTok also assesses the protections afforded to personal data under the legal framework of third countries where it transfers EU/EEA/UK user data to and adopts any supplementary measures

necessary to ensure an essentially equivalent level of protection. This assessment includes a review of the legal frameworks of these countries to determine the level of data protection in place for data subjects. Based on these assessments, the SCCs together with various supplementary measures ensure that personal data is afforded a level of protection essentially equivalent to that guaranteed within the EU/EEA/UK.

Project Clover

As announced under Project Clover, EU/EEA/UK user data will be migrated to servers in the EEA (Ireland and Norway). At present, TikTok stores this data by default in a designated "European Enclave", currently hosted in the United States. Our first data centre in Dublin, Ireland, is already operational and migration of EU/EEA/UK user data to this data centre has begun. Other two data centres in Norway and Ireland are under construction. For more information about Project Clover, please see the following resources: https://newsroom.tiktok.com/en-eu/tiktok-sets-new-standards-for-security-and-sustainability-through-12-bn-project-clover-programme and https://newsroom.tiktok.com/en-eu/progress-update-on-project-clover, along with our dedicated European Data Security microsite (https://www.tiktokeds.com/).

TikTok's use of SCCs

We understand that your request is to receive a copy of the SCCs as they are used by TikTok Technology Limited ("**TikTok Ireland**") and TikTok Technologies UK Limited ("**TikTok UK**") (together, "**TikTok**"). An example of the SCCs used by TikTok Ireland to transfer data outside the EU/EEA/UK is attached.

In order to support TikTok's global operations, TikTok Ireland and TikTok UK have entered into SCCs with other entities of TikTok's Corporate Group and 3rd party service providers. We did this in order to:

- store the information in secure servers located in the United States, Malaysia and Singapore.
- allow certain entities in our Corporate Group limited remote access.
- transfer data to enable the provision of services from 3rd party service providers.

These entities provide a variety of important functions which TikTok relies on for its daily operations, such as content delivery (cloud service providers), security, research and development, analytics, online payments, customer and technical support, content moderation, and advertisement, among others. These entities may be located globally in countries like Brazil, India, Morocco, Malaysia, Philippines, Singapore, and the United States. Along with SCCs, supplementary measures are used to ensure that user information continues to be appropriately protected. These measures include security controls such as system access controls, encryption and network security. For more information, please see the sections "How We Share Your Information" and "Our Global Operations and Data Transfers" of our Privacy Policy (https://www.tiktok.com/legal/page/eea/privacy-policy/en).

The Annexes

The information in the Annexes of the SCCs will vary depending on the relevant transfer. In particular, Annex I of the attached SCCs illustrates the transfers of EU/EEA/UK user data to various data importers. Annex II summarises the minimum security standards; however, TikTok and the importer may agree to adopt additional technical and organisational measures depending on the circumstances of the transfer.

Optional Clauses

The optional clauses are left to the negotiation between TikTok and the data importers and may vary depending on the circumstances of the transfer.

We hope this answers your query, but please let us know if we have misunderstood your request or if you have any further questions.

Regards,
TikTok Team

SCCs_with_Annexes.pdf

BIJLAGE 2: CORRESPONDENTIE TIKTOK ONDERSTEUNINGSAANVRAAG (11 APRIL 2025)

Hello,

Thanks for reaching out.

We understand that you are requesting information regarding the supplementary measures which TikTok has implemented to ensure that appropriate safeguards are in place where your data is transferred outside the EEA.

Supplementary Measures

At the outset, we wish to clarify that, before transferring EEA, Swiss and UK user data to countries outside the EEA/UK that are not recognised as having adequate data protection laws under GDPR, UK GDPR and Swiss Data Protection Laws, TikTok has implemented supplementary technical and organisational measures and assessed that, in the context of the specific transfer, the SCCs alongside TikTok robust supplementary measures afford an equivalent level of protection to EEA/UK/CH user data.

The details of these supplementary technical and organisational measures are confidential, but the following categories of measures are deployed:

- Information Security Policies: TikTok applies rigorous information security policies and requires importers to comply with them.
- Appropriate Organization of Information Security, including dedicated information security function, designated roles and a designated internal audit function.
- Human Resource Security. This includes confidentiality obligations, security awareness and education, disciplinary process for policy violations to the extent permitted by applicable law.
- Asset Management, including oversight of assets such as servers and user endpoints, assets handling and classification.
- Access Control: access controls include remote access via VPN, where appropriate, encryption, multi-factor authentication, password complexity. Cryptography, including encryption of data at

rest and in transit and security key management system
- Physical and Environmental Security, including physical entry controls, security of equipment and assets off-premises, secure disposal or reuse of equipment, visitor access and authorization program.
- Operations Security: a management process for changes to products and infrastructure, appropriate backup methodology, secure event log preservation, regular vulnerability scanning of systems and environment.
- Communications Security, such as security intrusion-detection-system, anti-malware software, firewalls deployed across the environment, segregation of networks into zones, network monitoring services.
- Secure software development process, separation of development and production environments, periodic review of open-source and third-party source code libraries, static and dynamic scanning of source code.
- Information security incident management, including incident management program, forensic capability for collecting incident data, a business continuity and disaster program and business impact analysis.

You can also find further details about our technical and organisational measures below.

Project Clover

TikTok has also implemented an industry leading initiative: Project Clover. EEA and UK user data will be stored by default in a designated "European Enclave", currently hosted in servers in EEA and the United States. For more information about Project Clover, please see our further details here (https://www.tiktokeds.com/eds-updates/) along with our dedicated European Data Security microsite (https://www.tiktokeds.com/).

Government Access

TikTok is committed to cooperating with law enforcement while respecting the privacy and other rights of our users. TikTok publishes online guidelines that describe its approach to managing law enforcement requests here (https://www.tiktok.com/legal/page/global/law-enforcement/en), as well as a set of law enforcement request FAQs here (https://www.tiktok.com/legal/page/global/law-enforcement/en#FAQ).

In addition to these guidelines and FAQs, TikTok has internal policies governing how TikTok handles and responds to law enforcement requests. These procedures are informed by legal and human rights standards and have been developed in a way that seeks to limit adverse human rights impacts, while enabling TikTok to comply with legitimate, valid legal requests from law enforcement to disclose user data.

All requests received undergo a case-by-case assessment by TikTok's dedicated law enforcement response team before any user data is disclosed to make sure they are legally valid and comply with our policies. This team is trained to evaluate requests from law enforcement authorities and frequently engages in outreach to communicate TikTok's requirements for disclosing user data to law enforcement authorities.

TikTok also believes transparency about our practices is an important part of building trust. We disclose transparency reports with information about the requests we receive from law enforcement authorities. These reports can be found in the TikTok Transparency Centre (https://www.tiktok.com/transparency/en-gb/information-requests-2024-1).

We trust this resolves your query. Should you have any further queries on this or another privacy matter, please do not hesitate to contact us.

Regards,
TikTok Team

BIJLAGE 3: CORRESPONDENTIE TIKTOK ONDERSTEUNINGSAANVRAAG (12 NOVEMBER 2024)

Hello,

Thank you for getting back to us.

TikTok evaluates the legal framework and data protection standards of 3rd countries before transferring EU/EEA/UK user data to said countries. Based on these assessments, TikTok implements any additional measures needed to provide and ensure a level of protection that is essentially equivalent to the standards within the EU/EEA/UK.

These assessments are legally privileged and confidential, so we are unable to share them.

Please note that a list of supplementary measures TikTok has taken is featured at pag. 18 and 19 of the attachment provided previously.

We hope this helps. Should you have any further privacy-related queries, please do not hesitate to contact us.

Regards,
TikTok Team

BIJLAGE 4: FORMULIER BETREFFENDE GEBRUIK VAN GENAI

Gebruik van GenAI bij een schrijfopdracht

Conform de afspraken gemaakt in de universiteit en faculteit, communiceren studenten transparant over het gebruik van GenAI. Ze voegen dit ingevulde formulier toe als bijlage aan hun schrijfopdracht. Alle aanvinkopties zijn toegelaten op voorwaarde dat studenten de gedragscode en de KU Leuven richtlijnen volgen.

Naam student: Arne Vincken

Studentnummer: 0839140

Geef met "X" aan:

☐ Ik heb **geen** AI Writing/Coding/Visualisation-assistent gebruikt.

☒ Ik heb **wel** een AI Writing/Coding/Visualisation-assistent gebruikt. Geef in dat geval aan welke (bijv. ChatGPT/GPT4/Grammarly...): ChatGPT

Geef met "X" aan (mogelijk meerdere keren) op welke manier je de AI Writing/Coding/Visualisation-assistent hebt gebruikt:

☒ Als hulp bij **de verwoording van de tekst**
Gedragscode: Deze toepassing is vergelijkbaar met het gebruik van spellingscontrolesoftware

☒ Als **zoekmachine** om meer te leren over een onderwerp of om **nieuwe ideeën** op te doen
Gedragscode: Deze toepassing is vergelijkbaar met een Google-zoekopdracht of het raadplegen van Wikipedia. Houd er rekening mee dat de output van GenAI evolueert en na verloop van tijd kan veranderen. Verifieer ook steeds of het idee nieuw is of niet. Het idee is waarschijnlijk gerelateerd aan bestaand werk, dat moet worden geciteerd.

☒ Voor **literatuuronderzoek**
Gedragscode: Deze toepassing is vergelijkbaar met een Google Scholar-zoekopdracht. Door GenAI gegenereerde tekst heeft mogelijk geen of verkeerde referenties. Het is jouw verantwoordelijkheid om de afwezigheid van referenties na te gaan of de correctheid te verifiëren.

☐ Om **programmeercode** te genereren
Gedragscode: Vermeld het gebruik van GenAI correct en citeer.

☐ Om **grafieken** te genereren
Gedragscode: Vermeld het gebruik van GenAI correct en citeer.

☐ Om **tekstblokken** te genereren
Gedragscode: **Het invoegen van tekstblokken zonder aanhalingstekens van tekst die gegenereerd is via GenAI in je werk is niet toegestaan.** Artikel 84 van het examenreglement bepaalt dat je werk moet worden beoordeeld op basis van je eigen kennis. Als het echt nodig is om een tekstblok geproduceerd door GenAI in te voegen, vermeld je dit als citaat met aanhalingstekens. Beperk ook dit echter tot een minimum.

☐ **Andere**

Gedragscode: Neem contact op met je promotor. Leg uit hoe je voldoet aan artikel 84 van de examenregeling. Leg uit wat het nut of de toegevoegde waarde van het gebruik van de AI-tool is: Klik of tik om tekst in te voeren.

Bijkomende richtlijnen en opmerkingen:

- GenAI kan niet worden gebruikt met betrekking tot gegevens of onderwerpen die onder een **geheimhoudingsovereenkomst** vallen.
- GenAI kan niet worden gebruikt met betrekking tot gevoelige of persoonlijke gegevens vanwege **privacykwesties.**
- Neem een **wetenschappelijke en kritische houding** aan bij interactie met GenAI en het interpreteren van de output ervan.
- Als student ben je verantwoordelijk voor naleving van **artikel 84 van het OER**: je werk moet je eigen kennis weerspiegelen. Hou er rekening mee dat plagiaatregels ook van toepassing zijn op het gebruik van AI-tools.
    - Examenreglement artikel 84: " Elk gedrag van individuele studenten waardoor zij een juist oordeel omtrent de kennis, het inzicht en/of de vaardigheden van henzelf of van andere studenten geheel of gedeeltelijk onmogelijk maken of onmogelijk pogen te maken, wordt als een onregelmatigheid beschouwd die aanleiding kan geven tot een aangepaste sanctie. Een bijzondere vorm van een dergelijke onregelmatigheid is plagiaat, namelijk de overname zonder adequate bronvermelding van het werk (ideeën, teksten, structuren, ontwerpen, beelden, plannen, codes, ...) van anderen of van eerder werk van zichzelf, op identieke wijze of onder licht gewijzigde vorm. Elk bezit tijdens een examen van een niet-toegestaan hulpmiddel (zie artikel 65) wordt als een onregelmatigheid beschouwd."
- **KU Leuven richtlijnen voor het citeren en refereren van GenAI tools, en andere informatie:** https://www.kuleuven.be/onderwijs/student/onderwijstools/artificiele-intelligentie