

Data Transfer Impact Assessment (DTIA)

AI-intake-assistent Defence Advocaten

Doorgiften naar derde landen (hoofdstuk V AVG) – versie 1.0 – vastgesteld 5 september 2026

I. Inleiding en toetsingskader

1. Bij het gebruik van de AI-intake-assistent van Defence Advocaten worden persoonsgegevens doorgegeven aan technologieleveranciers in de Verenigde Staten. Naar aanleiding van het Schrems II-arrest (HvJ EU 16 juli 2020, C-311/18) en de aanbevelingen 01/2020 van het Europees Comité voor gegevensbescherming (EDPB) beoordeelt Defence Advocaten in deze Data Transfer Impact Assessment of bij deze doorgiften een beschermingsniveau is gewaarborgd dat in grote lijnen overeenkomt met dat binnen de Europese Economische Ruimte. Deze DTIA vormt een aanvulling op de gegevensbeschermingseffectbeoordeling (DPIA) van 5 september 2026 en volgt het stappenplan van het EDPB: het in kaart brengen van de doorgiften, de vaststelling van het doorgiftemechanisme, de beoordeling van het recht en de praktijk van het derde land, de aanvullende maatregelen, en de conclusie met periodieke herbeoordeling. Dit document wordt op verzoek gedeeld met betrokkenen en andere belanghebbenden.

II. Stap 1 – De doorgiften in kaart

2. De verwerkingsketen van de intake-assistent is beschreven in de DPIA. Defence Advocaten heeft twee verwerkers rechtstreeks gecontracteerd: het gespreksplatform Vapi en de spraaksynthesedienst ElevenLabs. Vapi schakelt voor de spraakherkenning en het taalmodel twee subverwerkers in (Deepgram en OpenAI), die op grond van artikel 28, vierde lid, AVG via de verwerkersovereenkomst met Vapi aan dezelfde verplichtingen zijn gebonden. Onderstaande tabel brengt per partij in kaart welke gegevens worden doorgegeven, in welke rol, naar welk land en met welke bewaartermijn, telkens zoals geborgd via de verwerkersovereenkomsten met Vapi en ElevenLabs. Het taalmodel van Anthropic (Claude) dat in het klantenportaal statusupdates genereert, blijft hier buiten beschouwing: die toepassing heeft geen toegang tot persoonsgegevens, zodat van doorgifte van persoonsgegevens geen sprake is.

Leverancier	Rol	Doorgegeven gegevens	Verwerkingsland	Bewaartermijn (cf. verwerkersovereenkomst)
-------------	-----	----------------------	-----------------	--

Jericholaan 44b 3061 HG Rotterdam
info@defence-advocaten.com - (+31) 10 32 20 005

De maatschap Defence Advocaten KvK86881310 is een samenwerkingsverband van BCKR KvK77179153, BPJH Advocaat KvK86009966, Vermaat strafrechtadvocatuur KvK91793335 en Janse Strafrechtadvocatuur KvK91800153. Alle diensten worden verleend op basis van een overeenkomst van opdracht met de betreffende advocaat, waarop de algemene voorwaarden van toepassing zijn, welke te raadplegen zijn via de website en op verzoek kunnen worden toegestuurd. Iedere aansprakelijkheid is beperkt tot het bedrag dat in het betreffende geval door beroepsaansprakelijkheidsverzekering van de betreffende advocaat wordt uitgekeerd.



DEFENCE ADVOCATEN

				st)
Vapi	Verwerker – gespreksplatform en orkestratie	Geluidsopname, transcript, gespreksmetadata (nummerherkenning, datum, tijdstip, duur), logbestanden	Verenigde Staten	Veertien dagen, daarna automatische verwijdering
Deepgram	Subverwerker van Vapi – spraakherkenning	Audiostream van het gesprek (realtime)	Verenigde Staten	Geen opslag na de omzetting in tekst
OpenAI	Subverwerker van Vapi – taalmodel	Transcript van de gespreksbeurten, systeem instructies, gegenereerde samenvatting	Ierland en Verenigde Staten	Maximaal dertig dagen (misbruikdetectie), daarna verwijdering
ElevenLabs	Verwerker – spraaksynthese	Tekstreacties van de assistent	Verenigde Staten	Maximaal dertig dagen, daarna verwijdering

- De doorgegeven gegevens omvatten mede persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 10 AVG, gedeeld in het kader van (mogelijke) rechtsbijstand en daarmee rakend aan de geheimhoudingsplicht en het verschoningsrecht van de advocaat (artikel 11a Advocatenwet). Defence Advocaten hanteert bij deze beoordeling daarom een strenge maatstaf.

III. Stap 2 – Het doorgiftemechanisme

- Op 10 juli 2023 heeft de Europese Commissie een adequaatheidsbesluit vastgesteld voor het EU-VS Data Privacy Framework (DPF). Doorgiften aan Amerikaanse organisaties die onder het DPF zijn gecertificeerd, berusten op artikel 45 AVG. Blijkens raadpleging van het openbare DPF-register (dataprivacyframework.gov) op 5 september 2026 is van de rechtstreeks gecontracteerde verwerkers ElevenLabs onder het DPF gecertificeerd; de doorgifte aan deze verwerker berust op het adequaatheidsbesluit. De doorgifte aan Vapi berust op de door de Europese Commissie vastgestelde standaardcontractbepalingen (Uitvoeringsbesluit (EU) 2021/914, module twee: verwerkingsverantwoordelijke naar verwerker), die deel uitmaken van de met Vapi gesloten verwerkersovereenkomst. De verdere doorgifte door Vapi aan zijn subverwerkers Deepgram en OpenAI is geborgd doordat Vapi hun op grond van artikel 28, vierde lid, AVG dezelfde verplichtingen oplegt; Defence Advocaten controleert dit via de verwerkersovereenkomst en de subverwerkersvoorwaarden van Vapi. Defence Advocaten controleert het DPF-register bovendien periodiek: verkrijgt een partij alsnog certificering, dan geldt vanaf dat moment het adequaatheidsbesluit als grondslag; vervalt een certificering, dan zijn de standaardcontractbepalingen als grondslag geborgd.

IV. Stap 3 – Recht en praktijk van de Verenigde Staten

- De relevante Amerikaanse wetgeving omvat in het bijzonder Section 702 van de Foreign Intelligence Surveillance Act (FISA), Executive Order 12333 en de CLOUD Act. Aanbieders van clouddiensten kunnen kwalificeren als 'electronic communications service provider' en in dat



DEFENCE ADVOCATEN

geval onder omstandigheden worden verplicht gegevens te verstrekken aan Amerikaanse autoriteiten. Dit is het risico dat in het Schrems II-arrest centraal stond.

6. Sinds Executive Order 14086 (2022) gelden voor toegang door Amerikaanse inlichtingendiensten aanvullende waarborgen: toegang is beperkt tot wat noodzakelijk en proportioneel is voor vastgestelde inlichtingendoelen, en betrokkenen uit de EER beschikken over een rechtsgang via het Civil Liberties Protection Officer-mechanisme en het Data Protection Review Court. Deze waarborgen vormen de grondslag van het adequaatheidsbesluit voor het DPF.
7. Voor de praktische beoordeling van het risico is van belang dat de doorgegeven gegevens betrekking hebben op Nederlandse strafrechtelijke intakegesprekken van particulieren, een categorie die buiten de kenbare prioriteiten van Amerikaanse inlichtingenvergaring valt; dat de betrokken leveranciers transparantierapportages publiceren en geen gevallen bekend zijn van verstrekking van dit type klantgegevens aan Amerikaanse autoriteiten; dat de gegevens versleuteld zijn opgeslagen en slechts kort worden bewaard, zodat het tijdvenster voor een eventueel verzoek beperkt is; en dat de omvang van de gegevens per beller gering is. Defence Advocaten beoordeelt de kans dat de doorgegeven gegevens daadwerkelijk voorwerp worden van een verzoek van Amerikaanse autoriteiten als laag. Gelet op het verschoningsrecht wordt aan dit restrisico niettemin principieel gewicht toegekend, hetgeen de hierna beschreven aanvullende maatregelen rechtvaardigt.

V. Stap 4 – Aanvullende maatregelen

8. In aanvulling op het doorgiftemechanisme treft Defence Advocaten de volgende maatregelen. Technisch: versleuteling van de gegevens tijdens verzending (TLS) en bij opslag (AES), de in hoofdstuk II vermelde korte bewaartermijnen, en dataminimalisatie in het gespreksscript (geen burgerservicenummer, geen uitvraag die voor de eerste beoordeling niet noodzakelijk is, beperkte uitvraag in spoedsituaties en bij slachtoffers zonder vervolgingsbeslissing). Volledige versleuteling waarbij de leverancier geen toegang heeft tot de inhoud (end-to-end) is bij een spraakassistent naar haar aard niet mogelijk, omdat de leveranciers de inhoud moeten verwerken om het gesprek te kunnen voeren; dit is onderkend en verdisconteerd in de korte bewaartermijnen en de contractuele waarborgen.
9. Contractueel: de verwerkersovereenkomsten met Vapi en ElevenLabs verplichten deze verwerkers om verzoeken van autoriteiten op rechtmatigheid te toetsen en waar mogelijk aan te vechten, om Defence Advocaten over een verzoek te informeren voor zover dat wettelijk is toegestaan, om niet meer te verstrekken dan strikt noodzakelijk, en om de gegevens niet te



DEFENCE ADVOCATEN

gebruiken voor het trainen van AI-modellen of voor eigen doeleinden. Voor de subverwerkers gelden deze verplichtingen via de contractuele keten van artikel 28, vierde lid, AVG.

10. Organisatorisch: periodieke controle van de DPF-certificeringen en van de naleving van de verwerkersovereenkomsten, documentatie van eventuele verzoeken van autoriteiten, en onderzoek naar het afnemen van het taalmodel via een verwerkingslocatie binnen de EER, waarmee de omvang van de doorgifte verder wordt beperkt.

VI. Stap 5 en 6 – Conclusie en herbeoordeling

11. Op grond van het voorgaande concludeert Defence Advocaten dat het adequaatheidsbesluit voor het EU-VS Data Privacy Framework respectievelijk de standaardcontractbepalingen, in samenhang met de getroffen aanvullende technische, contractuele en organisatorische maatregelen en de lage kans op daadwerkelijke toegang door Amerikaanse autoriteiten, voor deze doorgiften een beschermingsniveau waarborgen dat in grote lijnen overeenkomt met dat binnen de EER. De doorgiften kunnen worden voortgezet; het restrisico is laag en aanvaardbaar.
12. Deze DTIA wordt herbeoordeeld bij iedere wezenlijke wijziging van de verwerkingsketen of van de betrokken leveranciers, bij relevante ontwikkelingen in het Amerikaanse recht of in de geldigheid van het adequaatheidsbesluit voor het DPF, en in ieder geval jaarlijks, gelijktijdig met de herziening van de DPIA. Vastgesteld door de maatschap Defence Advocaten op 5 september 2026.