Analyse · 18 mei 2026

← Vorige·Volgende →

Schrems II, vijf jaar later

Het vonnis dat het recht op internationale doorgifte van persoonsgegevens veranderde. Vijf jaar later werkt een aanzienlijk deel van de Europese professionele kantoren nog steeds alsof er niets is gebeurd.

Het vonnis dat er drie uur over deed om de regels te veranderen

Op 16 juli 2020, rond kwart over tien 's ochtends tijd in Luxemburg, maakte het Hof van Justitie van de Europese Unie (TJUE) het arrest bekend in zaak C-311/18. In de drie daaropvolgende uren hield het juridische regime dat de dagelijkse doorgifte van persoonsgegevens van Europa naar de Verenigde Staten ondersteunde — het zogenaamde Privacy Shield — op te bestaan. Tegen de tijd dat de Europese functionarissen voor gegevensbescherming die dag hun lunch op hadden, was het kader waarbinnen hun bedrijven en administraties werkten niet langer bruikbaar.

Het vonnis staat tegenwoordig bekend als Schrems II, naar Maximilian Schrems, de Oostenrijkse activist wiens klacht tegen Facebook Ireland de zaak in gang zette. De klacht had specifiek betrekking op de doorgifte tussen Facebook Ierland en Facebook Verenigde Staten. Het vonnis gaat in het algemeen veel verder: het schrijft voor hoe en onder welke voorwaarden persoonsgegevens die op Europees grondgebied zijn verzameld naar de Verenigde Staten mogen gaan.

Bijna zes jaar later is er het vervangende kader — het EU-US Data Privacy Framework, aangenomen in juli 2023 — en dit staat ook onder juridische druk. Een nieuwe Schrems-ronde wordt voorbereid. Ondertussen blijven Europese kleine en middelgrote ondernemingen Amerikaanse clouddiensten gebruiken voor dagelijkse taken, grotendeels zonder te weten dat de juridische kwestie waarop die diensten rusten nog steeds openstaat.

Wat Schrems II precies zei

Het vonnis rust op drie pijlers. De eerste is het Handvest van de grondrechten van de Europese Unie, in het bijzonder de artikelen 7 (privéleven en familie- en gezinsleven), 8 (bescherming van persoonsgegevens) en 47 (recht op een doeltreffende voorziening in rechte). De tweede is de Algemene Verordening Gegevensbescherming — de RGPD die veel Europeanen zich alleen herinneren door de cookie-waarschuwingen —, specifiek Hoofdstuk V, de artikelen 44 tot en met 50, over internationale doorgiften. De derde is de Amerikaanse inlichtingenwetgeving: sectie 702 van de Foreign Intelligence Surveillance Act, FISA 702 in juridisch jargon, en de presidentiële Executive Order 12333.

Het hof ging te werk via contrast. Het Handvest van de grondrechten vereist dat de persoonsgegevens van Europese burgers, wanneer zij de Unie verlaten, een beschermingsniveau genieten dat in essentie gelijkwaardig is aan het niveau dat door de RGPD wordt gegarandeerd. De vraag was bijgevolg of de Verenigde Staten dat essentieel gelijkwaardige niveau bieden.

Het antwoord was negatief, en niet door nuances. FISA 702 stelt de Amerikaanse overheid in staat om communicatie van niet-Amerikanen buiten het nationale grondgebied te verzamelen zonder voorafgaande individuele rechterlijke machtiging, zonder kennisgeving aan de betrokkene en zonder een doeltreffend rechtsmiddel dat vergelijkbaar is met het Europese. Executive Order 12333 breidt die capaciteit op analoge wijze

uit buiten het nationale grondgebied. Het hof concludeerde dat de Europese burger tegenover het Amerikaanse rechtssysteem niet beschikt over de essentieel gelijkwaardige bescherming die het Handvest vereist. Gelijkwaardigheid bestaat dus niet.

Vandaar het directe gevolg: Besluit 2016/1250 van de Europese Commissie, dat het Privacy Shield als adequaat kader voor doorgiften had gevalideerd, werd ongeldig verklaard. Elke doorgifte die uitsluitend op dat kader was gebaseerd, bleef vanaf dat moment zonder rechtsgrondslag.

Wat wel overleefde (en onder welke voorwaarden)

Schrems II heeft niet alle instrumenten geëlimineerd. De standaardcontractbepalingen — de SCC in internationaal jargon, van Standard Contractual Clauses — bleven bestaan. Dit zijn modelcontracten die zijn goedgekeurd door de Europese Commissie: een Europese exporteur en een importeur uit het land van bestemming ondertekenen deze en verbinden zich ertoe de gegevens te verwerken volgens de Europese norm. Het bedrijf dat dacht het probleem op 17 juli 2020 te hebben opgelost, ondertekende SCC met zijn provider en was tevreden.

Het ongemak kwam bij het aandachtig lezen van het vonnis. Het hof maakte duidelijk dat de SCC geldig blijven, maar hun geldigheid hangt af van een voorwaarde die onderstreept moet worden: dat de importeur van de gegevens ze in de praktijk kan naleven. Als de nationale wetgeving van het land van bestemming hem verhindert de clausules na te leven — omdat bijvoorbeeld een bevel onder FISA 702 hem verplicht de gegevens te overhandigen zonder zijn Europese tegenpartij hiervan op de hoogte te stellen — beschermen de clausules in werkelijkheid niet. En dan, zegt het hof, moet de Europese exporteur de doorgifte opschorten.

Dit introduceerde een nieuw element in de Europese praktijk van gegevensbescherming: de Transfer Impact Assessment, of impactanalyse van de doorgifte, bekend onder de Engelse afkorting TIA. Telkens wanneer een Europees bedrijf gegevens wil doorgeven naar de Verenigde Staten op basis van SCC, moet het formeel beoordelen of de ontvanger de clausules kan naleven, gezien de wetgeving die op hem van toepassing is. Het Europees Comité voor gegevensbescherming (EDPB) publiceerde gedetailleerde richtlijnen over hoe de TIA moet worden uitgevoerd. De eerlijke praktijk geeft meestal hetzelfde resultaat: als de importeur een Amerikaanse dochteronderneming van een grote cloudprovider is, is het oprechte antwoord op de TIA dat de clausules niet kunnen worden nageleefd zoals ze zijn opgeschreven.

Het Privacy Framework en het hangende Schrems III

Op 10 juli 2023 nam de Europese Commissie een nieuw adequaatheidsbesluit aan: 2023/1795. Het vervangt het ter ziele gegane Privacy Shield en werkt onder de naam EU-US Data Privacy Framework. De Verenigde Staten wijzigden eerder hun interne regime via Executive Order 14086, die de reikwijdte van signal intelligence beperkt tot wat «noodzakelijk en proportioneel» is — terminologie die bekend is voor de Europese lezer, maar minder voor de Amerikaanse administratieve praktijk — en creëert een herzieningsorgaan genaamd Data Protection Review Court (DPRC). De Commissie was van mening dat deze wijzigingen voldoende waren om het essentieel gelijkwaardige niveau te herstellen.

De organisatie noyb, opgericht door Schrems, diende op 7 september 2023 een klacht in tegen het nieuwe besluit. De argumenten zijn zoals verwacht: de DPRC is geen onafhankelijke rechtbank in de zin van artikel 47 van het Handvest; de begrippen «noodzakelijk en proportioneel» vertalen de Europese normen niet mechanisch; en tot slot kan een bescherming die rust op een Executive Order worden herroepen door de volgende Executive Order. Een uitspraak van het TJUE over het nieuwe besluit — die velen al met enige gelatenheid Schrems III noemen — wordt in de komende jaren verwacht. Het resultaat kan niet worden voorspeld. De structuur van het argument doet in ieder geval sterk denken aan die van 2020.

Wat de Europese KMO niet hoort

Terwijl de grote kamer van het TJUE beraadslaagt, blijft het middelgrote advocatenkantoor correspondentie uitwisselen met zijn cliënten via Microsoft 365, gehost in Europese regio's maar eigendom van een Amerikaans bedrijf dat onderworpen is aan FISA 702. De particuliere medische praktijk synchroniseert agenda's via Google Workspace. De belastingadviseur verstuurt ondertekende verklaringen via DocuSign. De psycholoog factureert vanuit een spreadsheet in Notion. Het arbeidsrechtkantoor archiveert dossiers in Dropbox. En vrijwel allemaal bedienen ze bovendien hun klanten via WhatsApp. Dit alles kan volgens de providers werken onder de bescherming van het adequaatheidsbesluit 2023/1795. Op de dag dat dit besluit in Schrems III sneuvelt, staan al die relaties in dezelfde seconde in de kou.

De kwestie is niet retorisch. Tussen 2022 en 2024 hebben verschillende Europese autoriteiten zaken afgehandeld tegen verwerkingsverantwoordelijken voor het gebruik van Google Analytics zonder adequaat doorgifte-instrument, in letterlijke toepassing van de redenering van het TJUE, zelfs voordat het Privacy Framework in werking trad. De Franse autoriteit, de CNIL, was de eerste die het criterium in 2022 formaliseerde; de Oostenrijkse, Italiaanse en andere autoriteiten volgden kort daarna. De niet-naleving, onder de huidige operationele opzet van de Europese KMO, wordt in real-time gedocumenteerd voor wie weet waar hij moet kijken.

De TIA als instrument, niet als ritueel

Een aanzienlijk deel van de TIA's die door Europese kantoren circuleren, zijn bij nader inzien formele oefeningen. Ze vermelden de contractuele instrumenten, sommen de certificeringen van de provider op, citeren de technische garanties en vinken het vakje aan. Weinigen vragen zich serieus af of een FISA 702-bevel de provider zou dwingen de gegevens te overhandigen. Nog minder vragen zich af wat er met die doorgifte zou gebeuren onder een hypothetische herziening van het Privacy Framework. Artikel 5 van de RGPD vereist dat de verwerkingsverantwoordelijke in staat is de naleving aan te tonen. Een TIA die niet serieus wordt uitgevoerd, bewijst niets; wat het aantoont is de bereidheid om op papier na te leven terwijl in de praktijk het tegenovergestelde wordt gedaan.

De eerlijke versie van de TIA begint met een eenvoudige vraag: wat zou er gebeuren als er morgen een FISA 702-bevel bij deze provider zou binnenkomen over deze specifieke gegevens? Als het eerlijke antwoord «hij zou ze moeten overhandigen zonder ons te waarschuwen» is, lossen de contractuele clausules het probleem niet op. Wat het wel oplost, in de gevallen waarin de vraag er echt toe doet, is de gegevens niet in handen van die provider te hebben gegeven.

Politieke verandering als structureel risico

Er is een extra laag, politiek, die zonder dramatiek benoemd moet worden. Het adequaatheidsbesluit 2023/1795 rust uiteindelijk op Executive Order 14086, ondertekend door president Biden in oktober 2022. Een Executive Order wordt ondertekend door een president en kan door de volgende president worden herroepen, gewijzigd of van inhoud worden ontdaan. De bescherming van Europese gegevens in de Verenigde Staten hangt dus af van een administratieve beslissing die noch het Amerikaanse Congres garandeert, noch het Amerikaanse rechtssysteem met dezelfde soliditeit beschermt als andere interne aangelegenheden. Sinds januari 2025 bestuurt een nieuwe regering de Verenigde Staten, en de vraag naar de praktische continuïteit van de EO 14086 is niet langer een hypothese maar actueel geworden. Elk scenario waarin de regering besluit de Order in te trekken of te verzwakken, zou het Europese besluit achterlaten zonder het stuk waarop het is gebouwd.

Het is geen complotargument. Het is de nuchtere lezing van het juridische ontwerp. De transatlantische kaders voor gegevensbescherming zijn al twee keer gesneuveld: de Safe Harbor in 2015 (Schrems I-arrest), het Privacy Shield in 2020 (Schrems II). De derde rust op een kwetsbaarder stuk dan zijn twee voorgangers. Een Europees bedrijf dat vandaag zijn gegevensverwerking op dat stuk inzet, neemt een risicobeheersingsbeslissing, geen beslissing van louter naleving van de regelgeving.

Voor de professionele lezer

De operationele vragen die men zich moet stellen voordat men een clouddienst kiest voor professionele gegevens — met de strengheid waarmee een inspecteur gegevensbescherming ze zou stellen — zijn de volgende:

1. Waar worden de gegevens fysiek opgeslagen? Een Europese regio is geen voldoende antwoord als de operator Amerikaans is.
2. Wie exploiteert de dienst, in welk rechtsgebied is deze gevestigd en aan welke wettelijke bevelen kan deze worden onderworpen?
3. Welk overdrachtsinstrument wordt ingeroepen: Adequaatheidsbesluit 2023/1795, SCC met TIA, afwijking van artikel 49 van de RGPD? Is die keuze verdedigbaar bij een inspectie?
4. Als het adequaatheidsbesluit morgen zou vervallen, welk operationeel plan is er dan om de activiteit voort te zetten?
5. Is er een Europees of zelf-gehost alternatief voor die functie, en wat zouden de werkelijke kosten van migratie zijn?

Niet alle functies van de dagelijkse kantoorpraktijk vereisen hetzelfde antwoord. Een spreadsheet voor interne boekhouding tilt de vraag waarschijnlijk niet naar dit niveau. Het strafdossier van een cliënt, de medische geschiedenis, de loonstrook van werknemers wel. Proportionaliteit is legitiem; de collectieve traagheid waarmee de Europese KMO bij Amerikaanse providers is gebleven voor alles — zelfs voor het meest gevoelige — is dat niet.

Schrems II viert deze juli zijn zesde verjaardag. Het vonnis heeft de dagelijkse gewoonten van de meeste Europese bedrijven niet veranderd. Het heeft echter wel de risicokaart waaraan deze bedrijven zijn blootgesteld veranderd. Wanneer een Amerikaanse administratieve beslissing tussen de Europese verordening en de werkelijke werking van een KMO komt te staan, is het raadzaam om tenminste te weten dat de beslissing er is en dat deze kwetsbaar is. Degenen onder ons die gekozen hebben voor een architectuur zonder operator in het midden — de rode draad door Cuadernos Lacre — zouden liever niet dit soort analyses hoeven te schrijven telkens wanneer een Schrems een beroep instelt. Maar we zullen ze blijven maken.

Bronnen und verdere lectuur

- Hof van Justitie van de Europese Unie — arrest van 16 juli 2020, zaak C-311/18, *Data Protection Commissioner tegen Facebook Ireland Ltd en Maximillian Schrems*.
- Verordening (EU) 2016/679, Hoofdstuk V, artikelen 44 tot en met 50 — internationale doorgifte van persoonsgegevens.
- Uitvoeringsbesluit (EU) 2023/1795 van de Commissie van 10 juli 2023 over het adequate beschermingsniveau voor persoonsgegevens in het kader van het EU-US Data Privacy Framework.
- Europees Comité voor gegevensbescherming — *Aanbevelingen 01/2020 over de maatregelen ter aanvulling van doorgifte-instrumenten om de naleving van het EU-niveau van bescherming van persoonsgegevens te waarborgen*, aangenomen op 18 juni 2021.
- noyb.eu — klacht ingediend op 7 september 2023 tegen Besluit (EU) 2023/1795 bij de Europese gegevensbeschermingsautoriteiten.
- *Foreign Intelligence Surveillance Act*, sectie 702 (gecodificeerd in 50 U.S.C. § 1881a), en Executive Order 12333 over Amerikaanse inlichtingenactiviteiten buiten het nationale grondgebied.

← VorigeWanneer er niemand in het midden isVolgende →CUADERNOS_LIST_SHA256_TITLE

Recente artikelen

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE

- CUADERNOS_LIST_IDENTIDAD_TITLE

Neem dit artikel mee naar waar u het nodig heeft.

↓ Markdown ↓ Platte tekst ↓ PDF

Het bestand wordt gedownload naar uw apparaat. Van daaruit kunt u het opslaan, importeren in Solo2 of delen waar u maar wilt. Cuadernos beslist niet voor u over de bestemming.

Lakzegel · SHA-256 d6d3d0c4cdc370c21419c6d872445f4be154262f02282043f095800170e0dec4

Cuadernos Lacre · Een uitgave van Menzuri Gestión S.L. ·
geschreven door R.Eugenio · geredigeerd door het team van Solo2.