Analys · 18 maj 2026

← Föregående·Nästa →

Schrems II, fem år senare

Domen som förändrade rätten för internationella överföringar av personuppgifter. Fem år senare fortsätter en betydande del av det dagliga europeiska kontorsarbetet som om ingenting hänt.

Domen som tog tre timmar att ändra reglerna

Den 16 juli 2020, vid kvart över tio på morgonen luxemburgsk tid, offentliggjorde Europeiska unionens domstol domen i mål C-311/18. Under de följande tre timmarna upphörde den rättsliga ordning som stödde den dagliga överföringen av personuppgifter från Europa till USA —det så kallade Privacy Shield— att existera. När europeiska dataskyddsombud hade ätit klart sin lunch den dagen, var det ramverk under vilket deras företag och myndigheter opererade inte längre giltigt.

Domen är idag känd som Schrems II, efter Maximilian Schrems, den österrikiske aktivisten vars klagomål mot Facebook Ireland utlöste den. Klagomålet rörde specifikt överföringarna mellan Facebook Irland och Facebook USA. Domen går i allmänhet mycket längre: den dikterar hur och under vilka villkor personuppgifter som samlats in på europeiskt territorium får överföras till USA.

Nästan sex år senare finns ersättningsramverket —EU-US Data Privacy Framework, antaget i juli 2023— och det är också under juridiskt tryck. En ny Schrems-runda förbereds. Under tiden fortsätter små och medelstora europeiska företag att använda amerikanska molntjänster för vardagliga uppgifter, för det mesta utan att veta att den juridiska frågan som dessa tjänster vilar på fortfarande är öppen.

Vad Schrems II exakt sa

Domen vilar på tre delar. Den första är Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artiklarna 7 (privat- och familjeliv), 8 (skydd av personuppgifter) och 47 (rätt till ett effektivt rättsmedel). Den andra är den allmänna dataskyddsförordningen —GDPR som många europeer bara kommer ihåg på grund av cookiemeddelanden— specifikt kapitel V, artiklarna 44 till 50, om internationella överföringar. Den tredje är den amerikanska lagstiftningen om underrättelseverksamhet: sektion 702 i Foreign Intelligence Surveillance Act, FISA 702 på juridiskt fackspråk, och presidentens Executive Order 12333.

Domstolen gick till väga genom kontrast. Stadgan om de grundläggande rättigheterna kräver att europeiska medborgares personuppgifter åtnjuter en skyddsnivå vid utförsel från unionen som i allt väsentligt motsvarar den som garanteras genom GDPR. Frågan var följaktligen om USA erbjuder denna väsentligen likvärdiga nivå.

Svaret var negativt, och inte på grund av nyanser. FISA 702 tillåter den amerikanska regeringen att samla in kommunikation från icke-amerikaner utanför det nationella territoriet utan föregående individuell rättslig prövning, utan underrättelse till den berörda och utan ett effektivt rättsmedel som är jämförbart med det europeiska. Executive Order 12333 utökar denna förmåga på liknande sätt utanför det nationella territoriet. Domstolen slog fast att den europeiska medborgaren inför det amerikanska rättssystemet inte har det väsentligen likvärdiga skydd som stadgan kräver. Likvärdighet existerar därför inte.

Därav den direkta konsekvensen: Europeiska kommissionens beslut 2016/1250, som hade validerat Privacy Shield som ett adekvat ramverk för överföringar, förklarades ogiltigt. Varje överföring som enbart stöddes på det ramverket saknade rättslig grund från och med det ögonblicket.

Det som faktiskt överlevde (och under vilka villkor)

Schrems II tog inte bort alla instrument. Standardavtalsklausuler —SCC på internationellt fackspråk, efter den engelska förkortningen Standard Contractual Clauses— överlevde. De är modellkontrakt godkända av Europeiska kommissionen: en europeisk exportör och en importör i mottagarlandet undertecknar dem och förbinder sig att behandla data enligt europeisk standard. Det företag som trodde sig ha löst problemet den 17 juli 2020 undertecknade SCC med sin leverantör och var nöjt med det.

Obehaget kom när man läste domen långsamt. Domstolen klargjorde att SCC fortfarande är giltiga, men deras giltighet beror på ett villkor som bör understrykas: att importören av data kan uppfylla dem i praktiken. Om mottagarlandets nationella lagstiftning hindrar dem från att uppfylla klausulerna —eftersom till exempel en order under FISA 702 tvingar dem att lämna ut data utan att meddela sin europeiska motpart— skyddar klausulerna inte i verkligheten. Och då, säger domstolen, måste den europeiska exportören avbryta överföringen.

Detta införde ett nytt objekt i den europeiska dataskyddspraxis: Transfer Impact Assessment, eller konsekvensbedömning av överföring, känd under sin engelska förkortning TIA. Varje gång ett europeiskt företag vill överföra data till USA med stöd av SCC, måste de formellt utvärdera om mottagaren kan uppfylla klausulerna med hänsyn till den lagstiftning som tillämpas på dem. Europeiska dataskyddsstyrelsen (EDPB) publicerade detaljerade vägledningar om hur man genomför en TIA. Den ärliga praxisen ger vanligtvis samma resultat: om importören är ett amerikanskt dotterbolag till en molnjätte, är det uppriktiga svaret på TIA att klausulerna inte kan uppfyllas som de är skrivna.

Privacy Framework och det väntande Schrems III

Den 10 juli 2023 antog Europeiska kommissionen ett nytt adekvansbeslut: 2023/1795. Det ersätter det nedlagda Privacy Shield och verkar under namnet EU-US Data Privacy Framework. USA ändrade tidigare sitt interna system genom Executive Order 14086, som begränsar omfattningen av signalspaning till vad som är «nödvändigt och proportionerligt» —en terminologi som är bekant för den europeiska läsaren, men inte lika vanlig i amerikansk administrativ praxis— och skapar ett kontrollorgan kallat Data Protection Review Court (DPRC). Kommissionen ansåg att dessa ändringar var tillräckliga för att återställa en väsentligen likvärdig skyddsnivå.

Organisationen noyb, grundad av Schrems, lämnade in ett klagomål den 7 september 2023 mot det nya beslutet. Argumenten är de förväntade: DPRC är inte en oberoende domstol i den mening som avses i artikel 47 i stadgan; begreppen «nödvändigt och proportionerligt» översätter inte mekaniskt europeiska standarder; och slutligen kan ett skydd som vilar på en Executive Order återkallas av nästa Executive Order. En dom från CJEU om det nya beslutet —som många redan kallar Schrems III med viss resignation— väntas under de kommande åren. Resultatet kan inte förutses. Argumentationens struktur påminner i vilket fall mycket om den från 2020.

Det som europeiska småföretag inte hör

Medan CJEU:s stora avdelning överlägger, fortsätter den medelstora advokatbyrån att utbyta korrespondens med sina klienter via Microsoft 365, som huseras i europeiska regioner men ägs av ett amerikanskt företag som lyder under FISA 702. Den privata läkarmottagningen synkroniserar kalendrar via Google Workspace. Skatterådgivaren skickar signerade deklarationer via DocuSign. Psykologen fakturerar från ett kalkylblad i Notion. Arbetsrättsbyrån arkiverar ärenden i Dropbox. Och praktiskt taget alla kommunicerar dessutom med sina klienter via WhatsApp. Allt detta kan ske med stöd av adekvansbeslut 2023/1795 enligt leverantörerna. Den dag då det beslutet faller i Schrems III, lämnas alla dessa relationer oskyddade i samma sekund.

Frågan är inte retorisk. Mellan 2022 och 2024 avgjorde flera europeiska myndigheter ärenden mot personuppgiftsansvariga för att de använt Google Analytics utan ett lämpligt överföringsinstrument, genom en bokstavlig tillämpning av CJEU:s resonemang även innan Privacy Framework trädde i kraft. Den franska myndigheten CNIL var först med att formalisera kriteriet 2022; österrikiska, italienska och andra myndigheter följde kort därefter. Bristande efterlevnad, under den nuvarande operativa designen hos europeiska småföretag, dokumenteras i realtid för den som vet var man ska titta.

TIA som ett instrument, inte som en ritual

En betydande del av de TIA som cirkulerar på europeiska kontor är, vid en närmare granskning, formella övningar. De listar avtalsinstrument, räknar upp leverantörens certifieringar, citerar tekniska garantier och kryssar i rutan. Få frågar sig på allvar om en order enligt FISA 702 skulle tvinga leverantören att lämna ut uppgifterna. Ännu färre frågar sig vad som skulle hända med den överföringen under en hypotetisk översyn av Privacy Framework. Artikel 5 i GDPR kräver att den personuppgiftsansvarige ska kunna visa efterlevnad. En TIA som inte görs på allvar visar ingenting; vad den visar är viljan att uppfylla kraven på papperet medan man gör motsatsen i praktiken.

Den uppriktiga versionen av en TIA börjar med en enkel fråga: vad skulle hända om detta företag i morgon fick en order enligt FISA 702 gällande just dessa data? Om det ärliga svaret är «de skulle bli tvungna att lämna ut dem utan att meddela oss», löser inte avtalsklausulerna problemet. Det som löser det, i de fall där frågan verkligen betyder något, är att inte ha lagt data i händerna på den leverantören.

Politisk förändring som en strukturell risk

Det finns ett ytterligare politiskt lager som bör nämnas utan dramatik. Adekvansbeslut 2023/1795 vilar i sista hand på Executive Order 14086, undertecknad av president Biden i oktober 2022. En Executive Order undertecknas av en president och kan återkallas, ändras eller tömmas på innehåll av nästa. Skyddet av europeiska data i USA beror således på ett administrativt beslut som varken den amerikanska kongressen garanterar eller det amerikanska rättssystemet skyddar med samma soliditet som det skyddar andra interna angelägenheter. Sedan januari 2025 styr en ny administration i USA, och frågan om den praktiska kontinuiteten för EO 14086 har upphört att vara en hypotes för att bli samtida. Varje scenario där administrationen beslutar att dra tillbaka eller dämpa ordern skulle lämna det europeiska beslutet utan den del som det byggdes på.

Det är inget konspiratoriskt argument. Det är en nykter läsning av den juridiska designen. De transatlantiska dataskyddsramverken har redan fallit två gånger: Safe Harbor 2015 (domen Schrems I), Privacy Shield 2020 (Schrems II). Det tredje vilar på en mer bräcklig del än sina två föregångare. Ett europeiskt företag som idag satsar sin databehandling på den delen fattar ett beslut om riskhantering, inte bara om regelefterlevnad.

För den professionella läsaren

De operativa frågor som bör ställas innan man väljer en molntjänst för professionella data —med den stringens som en dataskyddsinspektör skulle ställa dem— är följande:

1. Var lagras data fysiskt? En europeisk region är inte ett tillräckligt svar om operatören är amerikansk.
2. Vem driver tjänsten, i vilken jurisdiktion är den inkorporerad och vilka rättsliga order kan den underställas?
3. Vilket överföringsinstrument åberopas: Adekvansbeslut 2023/1795, SCC med TIA, undantag enligt artikel 49 i GDPR? Är det valet försvarbart vid en inspektion?
4. Om adekvansbeslutet skulle falla i morgon, vilken operativ plan finns för att upprätthålla verksamheten?
5. Finns det ett europeiskt eller självbetjänt alternativ för den funktionen, och vad skulle den faktiska kostnaden vara att migrera?

Alla funktioner på det dagliga kontoret kräver inte samma svar. Ett kalkylblad för intern bokföring lyfter troligen inte frågan till denna nivå. En klients brottmålsakt, en sjukjournal, anställdas lönebesked, gör det. Proportionalitet är legitim; den kollektiva tröghet med vilken europeiska småföretag har stannat hos amerikanska leverantörer för allt —även för det mest känsliga— är det inte.

Schrems II fyller sex år i juli. Domen har inte förändrat de dagliga vanorna för de flesta europeiska företag. Den har däremot förändrat riskkartan som dessa företag är exponerade för. När ett amerikanskt administrativt beslut hamnar mellan den europeiska förordningen och den faktiska driften av ett småföretag, är det åtminstone klokt att veta att beslutet finns där, och att det är bräckligt. Vi som har valt en arkitektur utan operatör i mitten — tråden som löper genom Cuadernos Lacre— skulle föredra att inte behöva skriva denna typ av analyser varje gång en Schrems sätter sig ner för att lämna in ett överklagande. Men vi kommer att fortsätta göra dem.

Källor och vidare läsning

- Europeiska unionens domstol — dom av den 16 juli 2020, mål C-311/18, *Data Protection Commissioner mot Facebook Ireland Ltd och Maximillian Schrems*.
- Förordning (EU) 2016/679, kapitel V, artiklarna 44 till 50 — internationella överföringar av personuppgifter.
- Kommissionens genomförandebeslut (EU) 2023/1795 av den 10 juli 2023 om den adekvata skyddsnivån för personuppgifter inom ramen för EU-US Data Privacy Framework.
- Europeiska dataskyddsstyrelsen — *Rekommendationer 01/2020 om åtgärder som kompletterar överföringsinstrument för att säkerställa efterlevnad av EU:s skyddsnivå för personuppgifter*, antagna den 18 juni 2021.
- noyb.eu — klagomål ingivet den 7 september 2023 mot beslut (EU) 2023/1795 till de europeiska dataskyddsmyndigheterna.
- *Foreign Intelligence Surveillance Act*, sektion 702 (kodifierad i 50 U.S.C. § 1881a), och Executive Order 12333 om amerikansk underrättelseverksamhet utanför det nationella territoriet.

← FöregåendeNär ingen är emellanNästa → Vad SHA-256 egentligen är

Senaste läsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 812c639eec6bc7193d7ef56643c4d2eabf690aef3a9cd6a1b00d0495693b4b85

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.