

Schrems II, fem år etter

Dommen som endret retten for internasjonale overføringer av personopplysninger. Fem år senere opererer en betydelig del av europeiske profesjonelle kontorer som om ingenting har skjedd.

Dommen som brukte tre timer på å endre reglene

Den 16. juli 2020, rundt kvart over ti om morgenen i Luxembourg, offentliggjorde EU-domstolen (TJUE) dommen i sak C-311/18. I løpet av de neste tre timene opphørte det juridiske regimet som støttet den daglige overføringen av personopplysninger fra Europa til USA — det såkalte Privacy Shield — å eksistere. Da europeiske personvernombud var ferdige med lunsjen den dagen, fungerte ikke lenger rammeverket deres selskaper og administrasjoner opererte under.

Dommen er i dag kjent som Schrems II, etter Maximilian Schrems, den østerrikske aktivisten hvis klage mot Facebook Ireland utløste den. Klagen handlet konkret om overføringer mellom Facebook Irland og Facebook USA. Dommen går generelt mye lenger: den dikterer hvordan og under hvilke betingelser alle personopplysninger som samles inn på europeisk territorium kan overføres til USA.

Nesten seks år senere eksisterer erstatningsrammeverket — EU-US Data Privacy Framework, vedtatt i juli 2023 — og det er også under juridisk press. En ny Schrems-runde forberedes. I mellomtiden fortsetter små og mellomstore europeiske bedrifter å bruke amerikanske skytjenester til daglige oppgaver, for det meste uten å vite at det juridiske spørsmålet disse tjenestene hviler på, fortsatt er uavklart.

Hva Schrems II nøyaktig sa

Dommen hviler på tre deler. Den første er Den europeiske unions pakt om grunnleggende rettigheter, særlig artikkel 7 (privatliv og familieliv), 8 (personvern) og 47 (retten til en effektiv prøvingsrett). Den andre er personvernforordningen — RGPD som mange europeere bare husker på grunn av cookie-varsler —, spesielt kapittel V, artikkel 44 til 50, om internasjonale overføringer. Den tredje er amerikansk etterretningslovgivning: seksjon 702 i Foreign Intelligence Surveillance Act, FISA 702 på juridisk fagspråk, og presidentens Executive Order 12333.

Domstolen gikk frem ved sammenligning. Pakten om grunnleggende rettigheter krever at personopplysningene til europeiske borgere, når de forlater unionen, nyter et beskyttelsesnivå som i det vesentlige tilsvarende det som garanteres av RGPD. Spørsmålet var følgelig om USA tilbyr dette vesentlig tilsvarende nivået.

Svaret var negativt, og ikke på grunn av nyanser. FISA 702 tillater den amerikanske regjeringen å samle inn kommunikasjon fra ikke-amerikanere utenfor nasjonalt territorium uten forhåndsautorisasjon fra domstolen, uten varsel til de berørte, og uten et effektivt rettsmiddel sammenlignbart med det europeiske. Executive Order 12333 utvider denne kapasiteten på tilsvarende måte utenfor nasjonalt territorium. Domstolen konkluderte med at den europeiske borgeren, overfor det amerikanske rettssystemet, ikke har den vesentlig tilsvarende beskyttelsen som pakten krever. Tilsvarende eksisterer derfor ikke.

Derav den direkte konsekvensen: EU-kommisjonens beslutning 2016/1250, som hadde validert Privacy Shield som et tilstrekkelig rammeverk for overføringer, ble erklært ugyldig. Enhver overføring som kun var basert på dette rammeverket, sto uten rettslig grunnlag fra det øyeblikket.

Det som overlevde (og under hvilke betingelser)

Schrems II fjernet ikke alle instrumenter. Standardkontraktsklausuler — SCC på internasjonalt fagspråk, for Standard Contractual Clauses — overlevde. Dette er modellkontrakter godkjent av EU-kommisjonen: en europeisk eksportør og en importør i mottakerlandet signerer disse og forplikter seg til å behandle dataene i henhold til den europeiske standarden. Selskapet som trodde de hadde løst problemet 17. juli 2020, signerte SCC med sin leverandør og sa seg fornøyd.

Ubehaget kom da man leste dommen nøye. Domstolen gjorde det klart at SCC fortsatt er gyldige, men deres gyldighet avhenger av en betingelse som bør understrekes: at importøren av dataene faktisk kan overholde dem. Hvis mottakerlandets nasjonale lovgivning hindrer dem i å overholde klausulene — for eksempel fordi et pålegg under FISA 702 tvinger dem til å utlevere dataene uten å varsle sin europeiske motpart — beskytter ikke klausulene i realiteten. Og da, sier domstolen, må den europeiske eksportøren stanse overføringen.

Dette introduserte et nytt element i europeisk personvernpraksis: Transfer Impact Assessment, eller konsekvensutredning av overføring, kjent under forkortelsen TIA. Hver gang et europeisk selskap ønsker å overføre data til USA under SCC, må det formelt vurdere om mottakeren kan overholde klausulene gitt lovgivningen som gjelder for dem. Det europeiske personvernrådet (EDPB) publiserte detaljerte retningslinjer for hvordan TIA skal gjennomføres. Ærlig praksis gir vanligvis samme resultat: hvis importøren er et amerikansk datterselskap av en stor skyleverandør, er det ærlige svaret på TIA-en at klausulene ikke kan overholdes slik de er skrevet.

Privacy Framework og den ventende Schrems III

Den 10. juli 2023 vedtok EU-kommisjonen en ny adekvansbeslutning: 2023/1795. Den erstatter det avdøde Privacy Shield og opererer under navnet EU-US Data Privacy Framework. USA endret tidligere sitt interne regime gjennom Executive Order 14086, som begrenser omfanget av signaletterretning til det «nødvendige og proporsjonale» — terminologi som er kjent for den europeiske leseren, men ikke så mye i amerikansk administrativ praksis — og oppretter et kontrollorgan kalt Data Protection Review Court (DPRC). Kommisjonen mente at disse endringene var tilstrekkelige til å gjenopprette et vesentlig tilsvarende beskyttelsesnivå.

Organisasjonen noyb, grunnlagt av Schrems, sendte inn en klage 7. september 2023 mot den nye beslutningen. Argumentene er som forventet: DPRC er ikke en uavhengig domstol i betydningen av artikkel 47 i pakten; begrepene «nødvendig og proporsjonalt» oversetter ikke automatisk europeiske standarder; og til slutt, en beskyttelse som hviler på en Executive Order kan tilbakekalles av den neste Executive Order. En dom fra TJUE om den nye beslutningen — som mange allerede kaller Schrems III med en viss resignasjon — ventes i løpet av de kommende årene. Resultatet kan ikke forutsies. Argumentasjonens struktur minner uansett mye om den fra 2020.

Det den europeiske SMB-en ikke hører

Mens TJUEs storkammer rådslår, fortsetter det mellomstore advokatkontoret å utveksle korrespondanse med sine klienter gjennom Microsoft 365 hostet i europeiske regioner, men eid av et amerikansk selskap underlagt FISA 702. Den private legepraksisen synkroniserer avtaler gjennom Google Workspace. Skatterådgiveren sender signerte erklæringer via DocuSign. Psykologen fakturerer fra et regneark i Notion. Arbeidsrettsadvokaten arkiverer saksmapper i Dropbox. Og praktisk talt alle sammen betjener dessuten sine kunder via WhatsApp. Alt dette kan, ifølge leverandørene, operere under adekvansbeslutningen 2023/1795. Den dagen den beslutningen faller i Schrems III, blir alle disse relasjonene stående uten beskyttelse i samme sekund.

Spørsmålet er ikke retorisk. Mellom 2022 og 2024 avgjorde flere europeiske myndigheter saker mot behandlingsansvarlige for bruk av Google Analytics uten egnet overføringsinstrument, i bokstavelig anvendelse av TJUEs resonnement selv før Privacy Framework trådte i kraft. Den franske myndigheten, CNIL, var den første til å formalisere kriteriet i 2022; østerrikske, italienske og andre myndigheter fulgte kort tid etter. Manglende overholdelse, under den nåværende operasjonelle utformingen av europeiske SMB-er, dokumenteres i sanntid for den som vet hvor man skal se.

TIA som instrument, ikke som ritual

En betydelig del av TIA-ene som sirkulerer i europeiske kontorer er, når de leses nøye, formelle øvelser. De lister opp kontraktsinstrumenter, ramser opp leverandørens sertifiseringer, siterer tekniske garantier og krysser av i boksen. Få spør seg seriøst om et FISA 702-pålegg ville tvinge leverandøren til å utlevere dataene. Enda færre spør seg hva som ville skje med den overføringen under en hypotetisk revisjon av Privacy Framework. Artikkel 5 i RGPD krever at den behandlingsansvarlige skal kunne dokumentere etterlevelse. En TIA som ikke gjøres seriøst, dokumenterer ingenting; det den dokumenterer er viljen til å etterleve på papiret mens man gjør det motsatte i praksis.

Den ærlige versjonen av TIA-en starter med et enkelt spørsmål: Hva ville skje hvis denne leverandøren i morgen fikk et FISA 702-pålegg om disse spesifikke dataene? Hvis det ærlige svaret er «de måtte utlevere dem uten å varsle oss», løser ikke kontraktsklausulene problemet. Det som derimot løser det, i de tilfellene hvor spørsmålet virkelig betyr noe, er å ikke ha lagt dataene i hendene på den leverandøren.

Politisk endring som strukturell risiko

Det er et ekstra lag, politisk, som bør nevnes uten dramatisering. Adekvansbeslutningen 2023/1795 hviler til syvende og sist på Executive Order 14086, signert av president Biden i oktober 2022. En Executive Order signeres av en president og kan tilbakekalles, endres eller tømmes for innhold av den neste. Beskyttelsen av europeiske data i USA avhenger dermed av en administrativ beslutning som verken den amerikanske kongressen garanterer eller det amerikanske rettssystemet beskytter med samme soliditet som det beskytter andre interne anliggender. Siden januar 2025 styrer en ny administrasjon USA, og spørsmålet om den praktiske kontinuiteten til EO 14086 har sluttet å være en hypotese og blitt dagsaktuelt. Ethvert scenario der administrasjonen bestemmer seg for å trekke tilbake eller svekke ordren, ville etterlate den europeiske beslutningen uten den delen den ble bygget på.

Det er ikke et konspiratorisk argument. Det er den edruelige lesningen av det juridiske designet. De transatlantiske rammeverkene for personvern har allerede falt to ganger: Safe Harbor i 2015 (Schrems I-dommen), Privacy Shield i 2020 (Schrems II). Den tredje hviler på en mer skjør del enn sine to forgjengere. Et europeisk selskap som i dag satser sin databehandling på denne delen, tar en beslutning om risikostyring, ikke bare om regelverkscompliance.

For den profesjonelle leseren

De operasjonelle spørsmålene man bør stille seg før man velger en skytjeneste for profesjonelle data — med den strengheten som en personverininspektør ville stilt dem — er følgende:

1. Hvor lagres dataene fysisk? En europeisk region er ikke et tilstrekkelig svar hvis operatøren er amerikansk.
2. Hvem driver tjenesten, i hvilken jurisdiksjon er den innlemmet, og hvilke juridiske pålegg kan den underlegges?
3. Hvilket overføringsinstrument påberopes: Adekvansbeslutning 2023/1795, SCC med TIA, unntak i artikkel 49 i RGPD? Er dette valget forsvarlig ved et tilsyn?
4. Hvis adekvansbeslutningen falt i morgen, hvilken operasjonell plan eksisterer for å opprettholde aktiviteten?

5. Finnes det et europeisk eller selvbetjent alternativ for den funksjonen, og hva ville den faktiske kostnaden for migrering være?

Ikke alle funksjoner i det daglige kontorarbeidet krever samme svar. Et regneark for intern regnskapsføring løfter sannsynligvis ikke spørsmålet til dette nivået. En klients straffesak, medisinsk historikk, ansattes lønsslipper, gjør det. Proporsjonalitet er legitimt; den kollektive tregheten som europeiske SMB-er har utvist ved å bli værende hos amerikanske leverandører for alt — selv for det mest sensitive — er ikke det.

Schrems II fyller seks år denne juli. Dommen har ikke endret de daglige vanene til de fleste europeiske selskaper. Den har imidlertid endret risikokartet som disse selskapene er eksponert for. Når en amerikansk administrativ beslutning stiller seg mellom den europeiske forordningen og den faktiske driften av en SMB, bør man i det minste vite at beslutningen er der, og at den er skjør. Vi som har valgt en arkitektur uten operatør i midten — den røde tråden i *Cuadernos Lacre* — ville foretrukket å slippe å skrive denne typen analyser hver gang en Schrems sender inn en anke. Men vi vil fortsette å gjøre det.

Kilder og videre lesing

- EU-domstolen — dom av 16. juli 2020, sak C-311/18, *Data Protection Commissioner mot Facebook Ireland Ltd. og Maximillian Schrems*.
- Forordning (EU) 2016/679, kapittel V, artikkel 44 til 50 — internasjonale overføringer av personopplysninger.
- Kommisjonens gjennomføringsbeslutning (EU) 2023/1795 av 10. juli 2023 om tilstrekkelig beskyttelsesnivå for personopplysninger i EU-US Data Privacy Framework.
- Det europeiske personvernrådet — *Anbefalinger 01/2020 om tiltak som utfyller overføringsinstrumenter for å sikre overholdelse av EUs personvernivå*, vedtatt 18. juni 2021.
- noyb.eu — klage inngitt 7. september 2023 mot beslutning (EU) 2023/1795 overfor europeiske personvernmyndigheter.
- *Foreign Intelligence Surveillance Act*, seksjon 702 (kodifisert i 50 U.S.C. § 1881a), og Executive Order 12333 om amerikansk etterretningsvirksomhet utenfor nasjonalt territorium.

[← Forrige](#)[Når ingen er i midten](#)[Neste](#) → [CUADERNOS LIST SHA256 TITLE](#)

Siste lesninger

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Ta med deg denne artikkelen dit du trenger den.

[↓ Markdown](#) [↓ Klartekst](#) [↓ PDF](#)

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 e26a561b58a0d468445326842e4fcce786974bbdc78e2757653088cccd3b6244

Cuadernos Lacre · En utgivelse fra [Menzuri Gestión S.L.](#) · skrevet av R.Eugenio · redigert av teamet bak [Solo2](#).

Dette nettstedet bruker ikke informasjonskapsler (cookies) og laster ikke inn ressurser fra tredjeparter. Det bruker en selvhostet anonym besøksteller (Umami på vår europeiske server) og det minimum av JavaScript som er

nødvendig for ditt valg av lyst/mørkt tema. Ingen trackere, ingen profilering, ingen datadeling. Hvis du vil følge oss: [RSS](#).