Analyysi · 18. toukokuuta 2026

← Edellinen·Seuraava →

Schrems II, viisi vuotta myöhemmin

Tuomio, joka muutti kansainvälisiä henkilötietojen siirtoja koskevaa oikeutta. Viisi vuotta myöhemmin huomattava osa eurooppalaisista toimistoista toimii edelleen ikään kuin mitään ei olisi tapahtunut.

Tuomio, joka muutti säännöt kolmessa tunnissa

16. heinäkuuta 2020 kello kymmenen ja neljäntoista välillä aamulla Luxemburgin aikaa Euroopan unionin tuomioistuin (TJUE) julkisti tuomion asiassa C-311/18. Seuraavien kolmen tunnin aikana oikeusjärjestelmä, joka tuki päivittäistä henkilötietojen siirtoa Euroopasta Yhdysvaltoihin — niin kutsuttu Privacy Shield (tietosuojakilpi) — lakkasi olemasta. Kun eurooppalaiset tietosuojavastaavat lopettivat lounaansa sinä päivänä, kehys, jonka puitteissa heidän yrityksensä ja hallintonsa toimivat, ei enää palvellut.

Tuomio tunnetaan nykyään nimellä Schrems II Maximilian Schremsin mukaan, joka on itävaltalainen aktivisti ja jonka valitus Facebook Irelandia vastaan pani sen alulle. Valitus koski nimenomaan Facebook Irlannin ja Facebook Yhdysvaltojen välistä tietojen siirtoa. Tuomio menee yleisesti paljon pidemmälle: siinä määrätään, miten ja millä ehdoilla kaikki Euroopan alueella kerätyt henkilötiedot voidaan siirtää Yhdysvaltoihin.

Lähes kuusi vuotta myöhemmin korvaava kehys on olemassa — heinäkuussa 2023 hyväksytty EU-US Data Privacy Framework — ja se on myös oikeudellisen paineen alaisena. Uusi Schrems-kierros on valmistelussa. Sillä välin eurooppalaiset pienet ja keskisuuret yritykset jatkavat yhdysvaltalaisten pilvipalvelujen käyttöä päivittäisissä tehtävissä, suurimmaksi osaksi tietämättä, että oikeudellinen kysymys, jonka varaan nuo palvelut perustuvat, on edelleen avoin.

Mitä Schrems II tarkalleen ottaen sanoi

Tuomio perustuu kolmeen osaan. Ensimmäinen on Euroopan unionin perusoikeuskirja, erityisesti sen 7 artikla (yksityis- ja perhe-elämä), 8 artikla (henkilötietojen suoja) ja 47 artikla (oikeus tehokkaisiin oikeussuojakeinoihin). Toinen on yleinen tietosuoja-asetus — GDPR, jonka monet eurooppalaiset muistavat vain evästeilmoituksista — erityisesti sen V luku, 44–50 artiklat kansainvälisistä siirroista. Kolmas on Yhdysvaltain tiedustelulainsäädäntö: Foreign Intelligence Surveillance Act -lain 702 pykälä (FISA 702 oikeuskielellä) ja presidentin Executive Order 12333.

Tuomioistuin eteni vertailun kautta. Perusoikeuskirja edellyttää, että Euroopan kansalaisten henkilötiedoilla on unionista poistuttaessa tietosuojan taso, joka on asiallisesti vastaava kuin GDPR:n takaama taso. Kysymys oli näin ollen siitä, tarjoaako Yhdysvallat tuon asiallisesti vastaavan tason.

Vastaus oli kielteinen, eikä kyse ollut vivahteista. FISA 702 antaa Yhdysvaltain hallitukselle mahdollisuuden kerätä muiden kuin kansallisen alueen ulkopuolella sijaitsevien yhdysvaltalaisten viestintää ilman edeltävää yksilöllistä oikeudellista lupaa, ilman ilmoitusta asianosaiselle ja ilman tehokasta oikeussuojakeinoa, joka olisi verrattavissa eurooppalaiseen. Executive Order 12333 laajentaa tuota kykyä vastaavalla tavalla kansallisen alueen ulkopuolella. Tuomioistuin totesi, ettei Euroopan kansalaisella ole Yhdysvaltain oikeusjärjestelmän edessä perusoikeuskirjan edellyttämää asiallisesti vastaavaa suojaa. Vastaavuutta ei siis ole.

Tästä seurasi suora seuraus: Euroopan komission päätös 2016/1250, joka oli vahvistanut Privacy Shieldin asianmukaiseksi kehykseksi siirroille, julistettiin pätemättömäksi. Kaikki siirrot, jotka perustuivat ainoastaan tuohon kehykseen, jäivät ilman oikeusperustaa sillä samalla hetkellä.

Mikä selvisi (ja millä ehdoilla)

Schrems II ei poistanut kaikkia välineitä. Vakiosopimuslausekkeet — SCC-lausekkeet — säilyivät. Ne ovat Euroopan komission hyväksymiä mallisopimuksia: eurooppalainen viejä ja kohdemaan tuoja allekirjoittavat ne sitoutuen käsittelemään tietoja eurooppalaisen standardin mukaisesti. Yritys, joka luuli ratkaisseensa ongelman 17. heinäkuuta 2020, allekirjoitti SCC-lausekkeet palveluntarjoajansa kanssa ja oli tyytyväinen.

Epämukavuus syntyi luettaessa tuomiota hitaasti. Tuomioistuin teki selväksi, että SCC-lausekkeet ovat edelleen päteviä, mutta niiden pätevyys riippuu ehdosta, jota on syytä korostaa: että tietojen tuoja pystyy noudattamaan niitä käytännössä. Jos kohdemaan kansallinen lainsäädäntö estää häntä noudattamasta lausekkeita — esimerkiksi siksi, että FISA 702 -määräys velvoittaa hänet luovuttamaan tiedot ilmoittamatta siitä eurooppalaiselle osapuolelleen — lausekkeet eivät todellisuudessa suojaa. Ja silloin tuomioistuin sanoo, että eurooppalaisen viejän on keskeytettävä siirto.

Tämä toi uuden asian eurooppalaiseen tietosuojakäytäntöön: Transfer Impact Assessment eli siirtoa koskeva vaikutustenarviointi, joka tunnetaan lyhenteellä TIA. Joka kerta kun eurooppalainen yritys haluaa siirtää tietoja Yhdysvaltoihin SCC-sopimuslausekkeiden nojalla, sen on virallisesti arvioitava, pystyykö vastaanottaja noudattamaan lausekkeita häneen sovellettavan lainsäädännön perusteella. Euroopan tietosuojaneuvosto (EDPB) julkaisi yksityiskohtaiset ohjeet TIA:n suorittamisesta. Rehellinen käytäntö johtaa yleensä samaan tulokseen: jos tietojen tuoja on suuren pilvipalvelun yhdysvaltalainen tytäryhtiö, rehellinen vastaus TIA:han on, että lausekkeita ei voida noudattaa siinä muodossa kuin ne on kirjoitettu.

Privacy Framework ja odottava Schrems III

10. heinäkuuta 2023 Euroopan komissio hyväksyi uuden tietosuojan tason riittävyyttä koskevan päätöksen: 2023/1795. Se korvaa edesmenneen Privacy Shieldin ja toimii nimellä EU-US Data Privacy Framework. Yhdysvallat muutti aiemmin sisäistä järjestelmäänsä Executive Order 14086:lla, joka rajoittaa signaalitiedustelun kattavuuden "välttämättömään ja oikeasuhtaiseen" — terminologia on tuttua eurooppalaiselle lukijalle, mutta ei niinkään yhdysvaltalaiselle hallintokäytännölle — ja perustaa Data Protection Review Court (DPRC) -nimisen tarkastuselimen. Komissio katsoi näiden muutosten riittävän palauttamaan tietosuojan tasolle, joka on asiallisesti vastaava.

Schremsin perustama noyb-järjestö teki 7. syyskuuta 2023 valituksen uudesta päätöksestä. Argumentit ovat odotettuja: DPRC ei ole perusoikeuskirjan 47 artiklan tarkoittama riippumaton tuomioistuin; käsitteet "välttämätön ja oikeasuhtainen" eivät käänny mekaanisesti eurooppalaisiksi standardeiksi; ja lopuksi, Executive Orderiin perustuva suoja voidaan peruuttaa seuraavalla Executive Orderilla. TJUE:n tuomiota uudesta päätöksestä — jota monet kutsuvat jo tietyllä luovuttamisella nimellä Schrems III — odotetaan lähivuosina. Tulosta ei voida ennakoida. Argumentin rakenne muistuttaa joka tapauksessa suuresti vuoden 2020 rakennetta.

Mitä eurooppalainen pk-yritys ei kuule

TJUE:n suuren jaoston neuvotellessa keskikokoinen asianajotoimisto jatkaa kirjeenvaihtoa asiakkaidensa kanssa Microsoft 365:n kautta, jota isännöidään eurooppalaisilla alueilla mutta jonka omistaa FISA 702 -säännösten alainen yhdysvaltalainen yritys. Yksityinen lääkäriasema synkronoi kalentereita Google Workspacen kautta. Veroasiantuntija lähettää allekirjoitettuja ilmoituksia DocuSignin kautta. Psykologi laskuttaa Notion-taulukosta. Työoikeuteen erikoistunut asianajotoimisto arkistoi tiedostoja Dropboxiin. Ja käytännössä kaikki heistä palvelevat asiakkaitaan myös WhatsAppin kautta. Palveluntarjoajien mukaan tämä kaikki voi toimia tietosuojan

tason riittävyyttä koskevan päätöksen 2023/1795 nojalla. Sinä päivänä, jona tuo päätös kaatuu Schrems III:ssa, kaikki nuo suhteet jäävät suojaamattomiksi samalla sekunnilla.

Kysymys ei ole retorinen. Vuosina 2022–2024 useat eurooppalaiset viranomaiset ratkaisivat asioita rekisterinpitäjiä vastaan Google Analyticsin käytöstä ilman asianmukaista siirtovälinettä soveltaen kirjaimellisesti TJUE:n päättelyä jo ennen Privacy Frameworkin voimaantuloa. Ranskan viranomainen CNIL oli ensimmäinen, joka virallisti kriteerin vuonna 2022; Itävallan, Italian ja muiden maiden viranomaiset seurasivat pian perässä. Noudattamatta jättäminen eurooppalaisen pk-yrityksen nykyisessä toimintamallissa dokumentoidaan reaaliajassa niille, jotka osaavat katsoa.

TIA työkaluna, ei rituaalina

Huomattava osa eurooppalaisissa toimistoissa liikkuvista TIA:ista on tarkemmin luettuna muodollisia harjoituksia. Niissä luetellaan sopimusvälineet, luetellaan palveluntarjoajan sertifioinnit, mainitaan tekniset takuut ja rastitetaan ruutu. Harva kysyy vakavasti, velvoittaisiko FISA 702 -määräys palveluntarjoajaa luovuttamaan tiedot. Vielä harvempi kysyy, mitä tuolle siirrolle tapahtuisi Privacy Frameworkin hypoteettisessa tarkistuksessa. GDPR:n 5 artikla edellyttää, että rekisterinpitäjä pystyy osoittamaan noudattamisen. TIA, jota ei tehdä vakavasti, ei osoita mitään; se osoittaa halua noudattaa sääntöjä paperilla, kun taas käytännössä toimitaan päinvastoin.

TIA:n rehellinen versio alkaa yksinkertaisella kysymyksellä: mitä tapahtuisi, jos tälle palveluntarjoajalle tulisi huomenna FISA 702 -määräys näistä nimenomaisista tiedoista? Jos rehellinen vastaus on "hänen olisi luovutettava ne ilmoittamatta meille", sopimuslausekkeet eivät ratkaise ongelmaa. Ongelman ratkaisee niissä tapauksissa, joissa kysymyksellä on todella merkitystä, se, ettei tietoja ole annettu kyseisen palveluntarjoajan käsiin.

Poliittinen muutos rakenteellisena riskinä

On olemassa poliittinen lisäkerros, joka on syytä nimetä ilman dramatiikkaa. Tietosuojan tason riittävyyttä koskeva päätös 2023/1795 perustuu viime kädessä Executive Order 14086:een, jonka presidentti Biden allekirjoitti lokakuussa 2022. Executive Orderin allekirjoittaa presidentti, ja seuraava voi peruuttaa sen, muuttaa sitä tai tyhjentää sen sisällöstä. Eurooppalaisten tietojen suoja Yhdysvalloissa riippuu siis hallinnollisesta päätöksestä, jota Amerikan kongressi ei takaa eikä Amerikan oikeusjärjestelmä suojaa samalla vankkuudella kuin se suojaa muita sisäisiä asioita. Tammikuusta 2025 lähtien Yhdysvaltoja on johtanut uusi hallinto, ja kysymys EO 14086:n käytännön jatkuvuudesta on lakannut olemasta hypoteesi ja tullut nykypäiväksi. Mikä tahansa skenaario, jossa hallinto päättää peruuttaa tai heikentää määräystä, jättäisi eurooppalaisen päätöksen ilman sitä osaa, jonka varaan se rakennettiin.

Tämä ei ole salaliittoargumentti. Se on oikeudellisen suunnittelun selväsanainen tulkinta. Transatlanttiset tietosuojakehykset ovat kaatuneet jo kahdesti: Safe Harbor vuonna 2015 (Schrems I -tuomio) ja Privacy Shield vuonna 2020 (Schrems II). Kolmas perustuu hauraampaan osaan kuin kaksi edeltäjäänsä. Eurooppalainen yritys, joka laskee tietojenkäsittelynsä tänään tuon osan varaan, tekee riskinhallintapäätöksen, ei pelkkää säännösten noudattamista koskevaa päätöstä.

Ammattilukijalle

Toiminnalliset kysymykset, jotka on syytä esittää ennen pilvipalvelun valitsemista ammattikäyttöön — sillä tarkkuudella, jolla tietosuojatarkastaja ne esittäisi — ovat seuraavat:

1. Missä tiedot fyysisesti säilytetään? Eurooppalainen alue ei ole riittävä vastaus, jos operaattori on yhdysvaltalainen.

2. Kuka palvelua operoi, mihin lainkäyttöalueeseen se on rekisteröity ja millaisten oikeudellisten määräysten alainen se voi olla?
3. Mihin siirtovälineeseen vedotaan: tietosuojan tason riittävyyttä koskeva päätös 2023/1795, SCC ja TIA, GDPR:n 49 artiklan mukainen poikkeus? Onko valinta puolustettavissa tarkastuksessa?
4. Jos tietosuojan tason riittävyyttä koskeva päätös kaatuisi huomenna, mikä on toimintasuunnitelma toiminnan jatkamiseksi?
5. Onko kyseiselle toiminnolle eurooppalaista tai itseisännöityä vaihtoehtoa ja mitkä olisivat siirtymisen todelliset kustannukset?

Kaikki päivittäiset toimistotoiminnot eivät vaadi samaa vastausta. Sisäiseen kirjanpitoon tarkoitettu taulukkolaskenta ei todennäköisesti nosta kysymystä tälle tasolle. Asiakkaan rikosrekisteri, sairaushistoria tai työntekijöiden palkkalista sen sijaan nostavat. Oikeasuhtaisuus on perusteltua; se kollektiivinen inertia, jolla eurooppalainen pk-yritys on jäänyt yhdysvaltalaisten palveluntarjoajien käyttäjäksi kaikessa — jopa kaikkein herkimmissä asioissa — ei ole.

Schrems II täyttää tänä heinäkuuna kuusi vuotta. Tuomio ei ole muuttanut useimpien eurooppalaisten yritysten päivittäisiä tapoja. Se on kuitenkin muuttanut riskikarttaa, jolle nämä yritykset altistuvat. Kun Yhdysvaltain hallinnollinen päätös asettuu eurooppalaisen säädöksen ja pk-yrityksen todellisen toiminnan väliin, on hyvä ainakin tietää, että päätös on olemassa ja että se on hauras. Me, jotka olemme valinneet arkkitehtuurin ilman välissä olevaa operaattoria — Cuadernos Lacre -sarjaa kulkeva lanka — toivoisimme, ettei meidän tarvitsisi kirjoittaa tällaista analyysia joka kerta, kun joku Schrems istuu tekemään valitusta. Mutta jatkamme niiden tekemistä.

Lähteet ja lisälukemista

- Euroopan unionin tuomioistuin — tuomio 16. heinäkuuta 2020, asia C-311/18, *Data Protection Commissioner vastaan Facebook Ireland Ltd ja Maximillian Schrems*.
- Asetus (UE) 2016/679, V luku, 44–50 artiklat — henkilötietojen kansainväliset siirrot.
- Komission täytäntöönpanopäätös (UE) 2023/1795, annettu 10 päivänä heinäkuuta 2023, henkilötietojen suojan riittävästä tasosta EU-US Data Privacy Framework -järjestelyssä.
- Euroopan tietosuojaneuvosto — *Suositukset 01/2020 toimenpiteistä, joilla täydennetään siirtovälineitä Euroopan unionin henkilötietojen suojan tason noudattamisen varmistamiseksi*, hyväksytty 18. kesäkuuta 2021.
- noyb.eu — 7. syyskuuta 2023 tehty valitus päätöksestä (UE) 2023/1795 Euroopan tietosuojaviranomaisille.
- *Foreign Intelligence Surveillance Act*, 702 pykälä (koodattu 50 U.S.C. § 1881a) ja Executive Order 12333 Yhdysvaltain tiedustelutoiminnasta kansallisen alueen ulkopuolella.

← EdellinenKun välissä ei ole ketäänSeuraava →CUADERNOS_LIST_SHA256_TITLE

Viimeaikaiset lukemiset

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ota tämä artikkeli mukaasi minne tarvitset.

↓ Markdown ↓ Pelkkä teksti ↓ PDF

Tiedosto ladataan laitteellesi. Voit tallentaa sen, tuoda sen Solo2-sovellukseen tai jakaa sen haluamallasi tavalla. Cuadernos ei päätä tiedoston kohtaloa puolestasi.

Sinetti · SHA-256 5ae9affc8029090cd3b546960f9c3836dfe0dd14fa16fd562b7c12daf45a1946

Cuadernos Lacre · Menzuri Gestión S.L. -julkaisu ·
kirjoittanut R.Eugenio · toimittanut Solo2-tiimi.