# Schrems II, viis aastat hiljem

Kohtuotsus, mis muutis isikuandmete rahvusvahelise edastamise õigust. Viis aastat hiljem jätkab suur osa Euroopa igapäevasest bürootööst nii, nagu poleks midagi juhtunud.

## Kohtuotsus, mis muutis reegleid kolme tunniga

16. juulil 2020 kella veerand üheteistkümne ajal hommikul Luksemburgi aja järgi avalikustas Euroopa Liidu Kohus kohtuotsuse asjas C-311/18. Järgmise kolme tunni jooksul lakkas olemast õiguskord, mis toetas igapäevast isikuandmete edastamist Euroopast Ameerika Ühendriikidesse — niinimetatud andmekaitsekilp ehk Privacy Shield. Selleks ajaks, kui Euroopa andmekaitseametnikud sel päeval lõunasöögi lõpetasid, ei olnud raamistik, mille alusel nende ettevõtted ja administratsioonid tegutsesid, enam kehtiv.

Kohtuotsus on täna tuntud kui Schrems II Maximilian Schremsi järgi, Austria aktivisti, kelle kaebus Facebook Irelandi vastu selle algatas. Kaebus puudutas konkreetselt andmete edastamist Facebook Iirimaa ja Facebook USA vahel. Kohtuotsus läheb üldiselt palju kaugemale: see määrab, kuidas ja millistel tingimustel võivad Euroopa territooriumil kogutud isikuandmed USA-sse liikuda.

Peaaegu kuus aastat hiljem on asendusraamistik olemas — 2023. aasta juulis vastu võetud EU-US Data Privacy Framework — ja see on samuti juriidilise surve all. Ettevalmistamisel on uus Schremsi voor. Vahepeal jätkavad Euroopa väikesed ja keskmise suurusega ettevõtted USA pilveteenuste kasutamist igapäevasteks ülesanneteks, enamasti teadmata, et juriidiline küsimus, millel need teenused põhinevad, on endiselt lahtine.

## Mida Schrems II täpselt ütles

Kohtuotsus toetub kolmele osale. Esimene on Euroopa Liidu põhiõiguste harta, eriti selle artiklid 7 (era- ja perekonnaelu austamine), 8 (isikuandmete kaitse) ja 47 (õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele). Teine on isikuandmete kaitse üldmäärus ehk RGPD, mida paljud eurooplased mäletavad vaid küpsisehoiatuste järgi, täpsemalt selle V peatükk, artiklid 44–50, mis käsitlevad rahvusvahelist edastamist. Kolmas on USA luureseadused: Foreign Intelligence Surveillance Acti jagu 702 (juriidilises žargoonis FISA 702) ja presidendi korraldus 12333.

Kohus lähtus kontrastist. Põhiõiguste harta nõuab, et Euroopa kodanike isikuandmed peavad Liidust lahkudes nautima kaitsetaset, mis on sisuliselt samaväärne RGPD-ga tagatuga. Küsimus oli järelikult selles, kas USA pakub seda sisuliselt samaväärset taset.

Vastus oli negatiivne ja seda mitte ainult detailide tõttu. FISA 702 võimaldab USA valitsusel koguda väljaspool riigi territooriumi asuvate mitte-ameeriklaste sidet ilma eelneva individuaalse kohtuliku loata, ilma asjaomast isikut teavitamata ja ilma Euroopa omaga võrreldava tõhusa õiguskaitsevahendita. Presidendi korraldus 12333 laiendab seda võimekust analoogselt väljaspool riigi territooriumi. Kohus järeldas, et Euroopa kodanikul ei ole USA õigussüsteemi ees sisuliselt samaväärset kaitset, mida harta nõuab. Samaväärsust seega ei eksisteeri.

Sellest tulenes otsene tagajärg: Euroopa Komisjoni otsus 2016/1250, mis oli kinnitanud Privacy Shieldi sobivaks raamistikuks edastamisteks, kuulutati kehtetuks. Kõik edastamised, mis põhinesid üksnes sellel raamistikul, jäid

sellest hetkest ilma õigusliku aluseta.

## Mis jäi ellu (ja millistel tingimustel)

Schrems II ei kaotanud kõiki instrumente. Lepingu tüüptingimused — rahvusvahelises žargoonis SCC (Standard Contractual Clauses) — jäid ellu. Need on Euroopa Komisjoni poolt heaks kiidetud tüüplepingud: Euroopa eksportija ja sihtkoha importija allkirjastavad need, kohustudes töötlema andmeid vastavalt Euroopa standardile. Ettevõte, kes arvas, et lahendas probleemi 17. juulil 2020, allkirjastas oma pakkujaga SCC-d ja jäi rahule.

Ebamugavustunne tekkis kohtuotsust aeglaselt lugedes. Kohus tegi selgeks, et SCC-d on endiselt kehtivad, kuid nende kehtivus sõltub tingimusest, mida tasub alla kriipsutada: andmete importija peab suutma neid praktikas täita. Kui sihtkoha riigisisene seadus takistab tal tingimusi täitmast — näiteks seetõttu, et FISA 702 korraldus kohustab teda andmeid üle andma ilma oma Euroopa partnerit teavitamata —, siis tingimused tegelikult ei kaitse. Ja siis, ütleb kohus, peab Euroopa eksportija edastamise peatama.

See tõi Euroopa andmekaitsepraktikasse uue objekti: Transfer Impact Assessment ehk edastamise mõjuhinnang, tuntud lühendi TIA all. Iga kord, kui Euroopa ettevõte soovib SCC alusel andmeid USA-sse edastada, peab ta ametlikult hindama, kas saaja suudab tingimusi täita, arvestades talle kohalduvaid seadusi. Euroopa Andmekaitsenõukogu (EDPB) avaldas üksikasjalikud suunised TIA läbiviimiseks. Aus praktika annab tavaliselt sama tulemuse: kui importija on USA pilvehiiglase tütarettevõte, siis on siiras vastus TIA-le, et tingimusi ei ole võimalik täita nii, nagu need on kirja pandud.

## Andmekaitseraamistik ja ootel olev Schrems III

10. juulil 2023 võttis Euroopa Komisjon vastu uue kaitse piisavuse otsuse: 2023/1795. See asendab kadunud Privacy Shieldi ja tegutseb nime all EU-US Data Privacy Framework. USA muutis eelnevalt oma sisemist režiimi presidendi korraldusega 14086, mis piirab signaaliluure ulatust „vajaliku ja proportsionaalsega“ — see on Euroopa lugejale tuttav terminoloogia, kuid mitte niivõrd USA administratiivse praktika jaoks — ning loob läbivaatamisorgani nimega Data Protection Review Court (DPRC). Komisjon leidis, et need muudatused on piisavad, et taastada sisuliselt samaväärne kaitsetase.

Schremsi asutatud organisatsioon noyb esitas 7. septembril 2023 kaebuse uue otsuse vastu. Argumendid on ootuspärased: DPRC ei ole sõltumatu kohus harta artikli 47 tähenduses; mõisted „vajalik ja proportsionaalne“ ei kattu mehaaniliselt Euroopa standarditega; ja lõpuks saab presidendi korraldusel põhineva kaitse tühistada järgmise presidendi korraldusega. Euroopa Kohtu otsust uue otsuse kohta — mida paljud nimetavad juba teatud resignationiga Schrems III-ks — on oodata lähiaastatel. Tulemust ei ole võimalik ette ennustada. Argumendi struktuur meenutab igal juhul väga 2020. aasta oma.

## Mida Euroopa väikeettevõte ei kuule

Samal ajal kui Euroopa Kohtu suurkoda arutab, jätkab keskmise suurusega advokaadibüroo klientidega kirjavahetust Microsoft 365 kaudu, mida majutatakse Euroopa piirkondades, kuid mis kuulub USA ettevõttele, millele kohaldub FISA 702. Eraarstipraksis sünkroonib kalendreid Google Workspace'i kaudu. Maksunõustaja saadab allkirjastatud deklaratsioone DocuSigni kaudu. Psühholoog esitab arveid Notioni tabeli kaudu. Tööõigusbüroo arhiveerib toimikuid Dropboxis. Ja peaaegu kõik nad suhtlevad klientidega lisaks ka WhatsAppi kaudu. Pakkujate sõnul võib see kõik toimuda kaitse piisavuse otsuse 2023/1795 alusel. Päeval, mil see otsus Schrems III käigus kehtetuks muutub, jäävad kõik need suhted samal sekundil kaitseta.

Küsimus ei ole retooriline. Aastatel 2022–2024 lahendasid mitmed Euroopa asutused asju vastutavate töötlejate vastu Google Analyticsi kasutamise pärast ilma asjakohase edastusvahendita, kohaldades Euroopa Kohtu põhjendusi sõna-sõnalt juba enne andmekaitseraamistiku jõustumist. Prantsuse asutus CNIL oli esimene, kes

kriteeriumi 2022. aastal vormistas; Austria, Itaalia ja teised asutused järgnesid peagi. Mittevastavus Euroopa väikeettevõtte praeguse tegevusmudeli juures on reaalajas dokumenteeritud kõigile, kes oskavad vaadata.

## TIA kui tööriist, mitte kui rituaal

Suur osa Euroopa büroodes ringlevatest TIA-dest on tähelepanelikul lugemisel vaid formaalsed harjutused. Need loetlevad lepingulised instrumendid, loetlevad pakkuja sertifikaadid, viitavad tehnilistele garantiidele ja märgivad kasti. Vähesed küsivad tõsiselt, kas FISA 702 korraldus kohustaks pakkujat andmeid üle andma. Veelgi vähem küsitakse, mis saaks sellest edastamisest andmekaitseraamistiku hüpoteetilise läbivaatamise korral. RGPD artikkel 5 nõuab vastutavalt töötlejalt suutlikkust tõendada nõuete täitmist. TIA, mida ei tehta tõsiselt, ei tõenda midagi; see tõendab vaid tahet täita nõudeid paberil, tehes samal ajal praktikas vastupidist.

TIA siiras versioon algab lihtsa küsimusega: mis saaks, kui homme saabuks sellele pakkujale FISA 702 korraldus nende konkreetsete andmete kohta? Kui aus vastus on „ta peaks need üle andma ilma meid teavitamata“, siis lepingutingimused probleemi ei lahenda. Probleemi lahendab neil juhtudel, kus küsimus on tõesti oluline, andmete mitteandmine selle pakkuja kätte.

## Poliitiline muutus kui struktuurne risk

On veel täiendav poliitiline kiht, mida tasub nimetada ilma dramatismita. Kaitse piisavuse otsus 2023/1795 toetub viimases instantsis presidendi korraldusele 14086, mille president Biden allkirjastas 2022. aasta oktoobris. Presidendi korralduse allkirjastab üks president ja järgmine võib selle tühistada, muuta või sisust tühjaks teha. Euroopa andmete kaitse USA-s sõltub seega administratiivsest otsusest, mida ei garanteeri Ameerika Kongress ega kaitse Ameerika õigussüsteem sellise kindlusega, nagu see kaitseb muid siseküsimusi. Alates 2025. aasta jaanuarist juhib USA-d uus administratsioon ja küsimus EO 14086 praktilise jätkumise kohta ei ole enam hüpotees, vaid kaasaeg. Iga stsenaarium, kus administratsioon otsustab korralduse tagasi võtta või seda leevendada, jätaks Euroopa otsuse ilma osata, millele see ehitati.

See ei ole vandenõuteooria. See on õigusliku disaini kaine lugemine. Transatlantilised andmekaitseraamistikud on juba kaks korda kokku kukkunud: Safe Harbor 2015. aastal (Schrems I otsus), Privacy Shield 2020. aastal (Schrems II). Kolmas toetub hapramale osale kui selle kaks eelkäijat. Euroopa ettevõte, kes täna panustab oma andmetöötluse sellele osale, teeb riskijuhtimise otsuse, mitte pelgalt normatiivse täitmise otsuse.

## Professionaalsele lugejale

Operatiivsed küsimused, mida tasub endalt küsida enne pilveteenuse valimist professionaalsete andmete jaoks — sellise rangusega, nagu andmekaitseinspektor neid esitaks —, on järgmised:

1. Kus andmeid füüsiliselt hoitakse? Euroopa piirkond ei ole piisav vastus, kui operaator on USA ettevõte.
2. Kes teenust opereerib, millises jurisdiktsioonis on see registreeritud ja millistele seaduslikele korraldustele see võib alluda?
3. Millist edastusvahendit kasutatakse: kaitse piisavuse otsus 2023/1795, SCC koos TIA-ga, erand vastavalt RGPD artiklile 49? Kas see valik on kontrolli käigus kaitstav?
4. Kui kaitse piisavuse otsus peaks homme kehtetuks muutuma, milline tegevuskava on olemas tegevuse jätkamiseks?
5. Kas selle funktsiooni jaoks on olemas Euroopa või isehostitav alternatiiv ja milline oleks ülemineku tegelik kulu?

Mitte kõik igapäevased büroofunktsioonid ei vaja sama vastust. Sise-raamatupidamise tabel tõenäoliselt ei tõsta küsimust sellele tasemele. Kliendi kriminaaltoimik, haiguslugu, töötajate palgaleht aga küll. Proportsionaalsus on leegitiimne; kollektiivne inerts, millega Euroopa väikeettevõtted on jäänud USA pakkujate juurde kõige jaoks — isegi kõige tundlikuma jaoks —, seda ei ole.

*Schrems II saab tänavu juulis kuueaastaseks. Kohtuotsus ei ole muutnud enamiku Euroopa ettevõtete igapäevaseid harjumusi. See on aga muutnud riskikaarti, millele need ettevõtted on avatud. Kui USA administratiivne otsus seisab Euroopa määruse ja väikeettevõtte tegeliku tegevuse vahel, tasub vähemalt teada, et see otsus on olemas ja et see on habras. Need meist, kes on valinud arhitektuuri ilma vahendajata — see on Cuadernos Lacre läbiv teema —, eelistaksid mitte kirjutada selliseid analüüse iga kord, kui mõni Schrems istub kaebust esitama. Kuid me jätkame nende koostamist.*

## Allikad ja täiendav lugemine


- Euroopa Liidu Kohus — 16. juuli 2020. aasta kohtuotsus asjas C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd ja Maximillian Schrems*.
- Määrus (EL) 2016/679, V peatükk, artiklid 44–50 — isikuandmete rahvusvaheline edastamine.
- Komisjoni rakendusotsus (EL) 2023/1795, 10. juuli 2023, isikuandmete piisava kaitse taseme kohta EU-US Data Privacy Frameworki raames.
- Euroopa Andmekaitsenõukogu — *Soovitused 01/2020 meetmete kohta, mis täiendavad edastusvahendeid, et tagada isikuandmete kaitse vastavus ELi tasemele*, vastu võetud 18. juunil 2021.
- noyb.eu — 7. septembril 2023 esitatud kaebus otsuse (EL) 2023/1795 vastu Euroopa andmekaitseasutustele.
- *Foreign Intelligence Surveillance Act*, jagu 702 (kodifitseeritud 50 U.S.C. § 1881a) ja presidendi korraldus 12333 USA luuretegevuse kohta väljaspool riigi territooriumi.



← EelmineKui kedagi ei ole vahelJärgmine →CUADERNOS_LIST_SHA256_TITLE


## Viimased lugemised


- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE


Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 bc2b006bf84a6e1bbb64d0d8556768a0e77e843c50468caac5bd7e8ca0b45bf0


Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.