

Valódi vs. látszólagos adatvédelem: a kérdések, amelyeket érdemes feltenni

A 2. ciklus operatív összegzése: a kérdések, amelyek megkülönböztetik az architektúrális adatvédelmű szolgáltatást a deklaratív adatvédelmútől. Kérdőív az európai szakember számára, mielőtt bármilyen digitális eszközt használatba venne érzékeny adatokhoz.

Hogy értsük egymást: Két szolgáltatás ugyanazzal a jogi nyilatkozattal nagyon eltérően viselkedhet. Az egyik technikai tervezéssel véd. A másik szerződéses ígérettel véd. A különbség nem olvasható ki a nyilatkozatból — a konkrét kérdések feltevésével derül ki. A válaszok minősége annyit elárul a termékről, mint a saját tartalmuk.

A különbség az architektúrális és a deklaratív adatvédelem között

E ciklus hét előző cikke során ugyanannak a témának különböző rétegein haladtunk át. A nemzetközi adattovábbítások joga a Schrems II-vel. A kriptográfiai hash matematikai eszméje, amely minden Cuadernót lepecsétel. A kill switch architektúrális választása és az intézményi kisajátítás, amely szinte mindig kíséri. A végpontok közötti titkosítás mechanizmusa és az operatív kérdés arról, hol található a kulcsok. Az ösztönzők igazodása az üzleti modell szerint. Az önszuverén kriptográfiai identitás. A self-hosting mint arányos stratégia. Minden cikk egy-egy szögletet tárgyalt. Ez, a ciklus utolsó darabja, egy kérdőívben egyesíti őket.

A megkülönböztetés, amelyet érdemes megjegyezni, egyszerű: vannak szolgáltatások, amelyek adatvédelme *architektúrális*, és vannak szolgáltatások, amelyek adatvédelme *deklaratív*. Az első a technikai tervezésbe van beágyazva: az adatvédelmi kötelezettségvállalás bizonyos megsértései technikailag nehezek vagy lehetetlenek, mert az architektúra nem engedi meg őket. A második a jogi nyilatkozat szövegében van letétbe helyezve: bizonyos jogsértések szerződésileg szankcionálhatók lennének, ha bekövetkeznek, de technikailag semmi sem akadályozza meg őket. Mindkét modell megfelelhet a GDPR-nak; de az egyik konstrukció révén véd, a másik ígéret révén, és a különbség operatív szempontból óriási.

A következő kérdéseket úgy tervezték, hogy megkülönböztessék az egyik esetet a másiktól. Nem haladó technikai kérdések. Olyan kérdések, amelyekre bármely becsületes szolgáltató válaszolni tud a nyilvános dokumentációjában. A válasz minősége és pontossága annyit elárul a termékről, mint maga a válasz. A kérdések hat rétegbe csoportosulnak; mindegyiket érdemes feltenni, mielőtt a szolgáltatást érzékeny adatokhoz használatba vennénk, nem csak azokat, amelyeket az első ösztön azonosít.

1. réteg: architektúra

Rögzítsünk egy fogalmat, mielőtt továbbmennénk. *Üzemeltető* alatt a szolgáltatást nyújtó vállalatot értjük: a szervereket és a szoftvert irányító entitást, nem pedig egy konkrét személyt. Ezt tisztázva az alapvető architektúrális kérdés ez: mit tesz az üzemeltető a feladó és a címzett közötti tartalommal? Három lehetséges válasz van, és érdemes megtanulni megkülönböztetni őket, mert mindhárom olykor hasonló szókinccsel hirdetik.

- Az első: a tartalom nyíltan halad át az üzemeltető szerverén, ahol az üzemeltető elolvashatja, még ha ígéri is, hogy nem teszi.
- A második: a tartalom titkosítva halad át az üzemeltető szerverén, ahol az üzemeltető nem tudja elolvasni, ha a kulcsok kizárólag a felhasználók eszközein találhatóak.
- A harmadik: a tartalom egyetlen üzemeltetői szerveren sem halad át, mert abban a konkrét folyamatban nincs üzemeltetői szerver.

A három közötti különbség nem fokozati: típusbeli.

A kiegészítő kérdés —amelyet már a titkosításról szóló Cuadernóban megfogalmaztunk— ez: kinél vannak a kriptográfiai kulcsok, amelyek lehetővé teszik a tartalom elolvasását? Ha a felhasználónál és csakis a felhasználónál vannak, a titkosítás valódi. Ha emellett az üzemeltetőnél is vannak bármilyen formában —akár »fiókhelyreállítás» vagy »eszközök közötti szinkronizálás» néven is—, a titkosítás névleges. A kérdés nem tűr becsületes köztes választ.

2. réteg: üzleti modell

Az üzleti modellről szóló kérdés ugyanolyan fontos, mint az architektúrális kérdés, és ugyanabból a lényegi okból: az ösztönzők idővel rendszeresen eltérő termékeket állítanak elő, még azonos kinyilvánított célok mellett is. Hogyan keres ma pénzt az üzemeltető? Egyetlen forrásból, kettőből, keverékből? Ha a finanszírozás reklámot vagy az adatok pénzzé tételét is magában foglalja, milyen adatokat tesznek pénzzé, és a GDPR melyik jogalapján teszik? A jogi nyilatkozatban kinyilvánított cél lefedi-e a harmadik felek azon adatait, amelyeket a szakember a szolgáltatásra kíván bízni?

És a másodrendű kérdés, amelyet nem mindig fogalmaznak meg: milyen az üzemeltető pénzügyi helyzete három-öt éves távlatban? Egy kockázati tőke szakaszában lévő vállalat más nyomások alatt működik, mint egy stabilan nyereséges vállalat. A finanszírozási modell változása ismételten az a pillanat, amikor a felhasználókkal kötött hallgatolagos szerződést tárgyalás nélkül újraírják.

3. réteg: joghatóság

Az európai szakember számára a joghatóság kérdése nem retorikai. Melyik joghatóságban van bejegyezve az üzemeltető? Melyik országban vannak fizikailag az adatokat feldolgozó szerverek? Az előző két kérdésre adott válasz azonos vagy eltérő, és ha eltér, melyik jogszabály vonatkozik rá? Egy amerikai vállalat által üzemeltetett európai régió a Schrems II szempontjából nem európai válasz: a vállalat a FISA 702 hatálya alá tartozik függetlenül attól, hol vannak a szerverek.

A kiegészítő operatív kérdés ez: ha holnap megérkezne egy, az üzemeltető joghatóságában érvényes hírszerzési utasítás, amely az én vagy az ügyfeleim adatainak kiadását kérné, mi történne? Ha a becsületes válasz azzal kezdődik, hogy »a vállalat köteles lenne kiadni azokat«, a szolgáltatás nem véd ezzel az utasítással szemben, akármennyire is az ellenkezőjét sugallja a reklám. Ha a becsületes válasz azzal kezdődik, hogy »a vállalat nem tudná kiadni azokat, mert nem birtokolja őket nyílt formában«, a szolgáltatás véd; és a különbség szinte teljes egészében az első két rétegtől függ, nem az adatvédelmi szabályzat minőségétől.

4. réteg: üzemeltető és kill switch

Milyen technikai képességet tart fenn az üzemeltető a szolgáltatás távoli felfüggesztésére, letiltására, megszüntetésére vagy leromlásztására? A kérdés nem paranoiás: operatív. A digitális platformok az elmúlt években ismételten gyakorolták ezt a képességet, néha saját kezdeményezésre, máskor kormányok utasítására, máskor tulajdonosi vagy szabályzati változások után. Ha a képesség létezik, érdemes tudni, milyen szerződésileg kinyilvánított feltételek mellett gyakorolják, és tartalékokat képezni a ki nem nyilvánított feltételekre, amelyeket az

elmúlt évek gyakorlata ugyanolyan relevánsnak mutatott: váratlan bírósági végzés, nemzetközi szankció, vállalatirányítási változás, más szabályzatú entitás általi felvásárlás.

A testvérkérdés a folytonossági terv kérdése: ha az üzemeltető a szakemberrel szemben gyakorolná a képességet —bármilyen okból, jogosan vagy sem—, mennyi működési idő maradna elérhető, milyen adatexportálási eljárás létezik, és melyik alternatív szolgáltatóhoz lehetne átállni? Ha a válasz azzal kezdődik, hogy »ennek nem szabadna megtörténnie«, az nem operatív válasz; az ígéret.

5. réteg: identitás és hozzáférés

Ki ellenőrzi a szolgáltatáshoz való hozzáférés hitelesítő adatait? Ha az üzemeltető vissza tudja állítani a felhasználó hozzáférését a felhasználó közreműködése nélkül —ezt az eljárást jellemzően »fiókhelyreállításnak« nevezik—, akkor az üzemeltető technikailag a fiók letéteményese, és át is adhatja annak, aki a megfelelő eljárás útján kéri. Ha az üzemeltető nem tudja visszaállítani a hozzáférést, mert az identitás kriptográfiailag a felhasználó eszközén található, akkor az üzemeltető át sem adhatja, még utasításra sem. Mindkét mód jogszerű a kontextustól függően; de ismét, ezek különbözőek, és érdemes tudni, melyiket veszi az ember használatba.

Mi történik a szakember adataival, ha a szakember elveszíti a hozzáférést? Léteznek-e helyreállítási mechanizmusok —fiók, archívum, munkamenet—, amelyek az üzemeltetőtől függenek? Összeegyeztethetők-e ezek a mechanizmusok az ágazat szakmai deontológiájával, ha az üzemeltetőt kényszerítik a használatukra?

6. réteg: jövő

Ezt az utolsó réteget gyakran elhanyagolják, mert előrelátást igényel. Mi történne, ha a szolgáltatást egy másik cég vásárolná fel? Szinte minden felvásárlás a szolgáltatási feltételek felülvizsgálatát vonja maga után a következő hónapokban. Mi történne, ha a szabályozási követelmények megváltoznának? Az európai jog 2022 óta növelte az eltávolítási és letiltási kötelezettségeket, nem csökkentette azokat. Mi történne, ha az üzemeltető eltűnne? A felhőszolgáltatások jelentős részének nincs dokumentált kilépési terve az üzemeltető megszűnésének forgatókönyvére; a szakember akkor fedezi fel a problémát, amikor már nincs idő felkészülni rá.

Van egy megfogalmazás, amelyet érdemes megjegyezni ehhez a réteghez: azok az architektúrák, amelyek kevésbé függenek az üzemeltetőtől, ellenállóbbak az üzemeltető változásaival szemben. A self-hosting bármely formájában, az önszuverén kriptográfiai identitás, a közbeiktatott szerver nélküli kommunikáció, mindezek csökkentik a jövőbeli kockázati felületet azáltal, hogy csökkentik a jelenlegi függőségi felületet. Nem szüntetik meg; csökkentik.

A különbség a struktúra és az ígéret között

Ha a ciklust egyetlen mondatba kellene desztillálnunk, ez lenne az: a strukturális válaszok fennmaradnak, még ha az üzemeltető, a közigazgatás vagy a jogszabály változik is; az ígéreten alapuló válaszok addig maradnak fenn, amíg az ígérő képes és hajlandó betartani őket. Mindkettő helyes lehet az elfogadás pillanatában. De csak az egyik áll meg az idő múlásától és a körülmények változásától függetlenül.

Ez nem azt jelenti, hogy minden szakembernek strukturális válaszokat kell követelnie minden szolgáltatástól, amelyet használatba vesz. Az arányosság jogszerű marad: egy belső könyvelési táblázatnak nincs szüksége ugyanarra a válaszra, mint egy beteg klinikai kórlapjának. Azt jelenti viszont, hogy a szakmaiság abban áll, hogy az ember tudja, milyen jellegű választ fogadott el az egyes esetekben, és hogy tudatosan eldöntötte: az adott jellegű válasz arányos a konkrét adattal.

A kérdőív, rendszerezve

Tizenkét konkrét kérdés, amely összegzi a ciklust, úgy rendezve, hogy mindegyikre adott válasz tájékoztassa a következőt:

1. Áthalad a tartalom az üzemeltető szerverén? Ha igen: nyíltan, az üzemeltető kulcsaival titkosítva, vagy kizárólag a felhasználó kulcsaival titkosítva?
2. Ha végpontok közötti titkosításra hivatkoznak, hol találhatóak a kriptográfiai kulcsok? Ismeri vagy megőrzi-e az üzemeltető ezeknek bármely részét bármilyen formában, beleértve a »helyreállítást« is?
3. Milyen metaadatokat hoz létre és őriz meg a szolgáltatás? Mennyi ideig? Kik számára láthatók?
4. Hogyan finanszírozza magát az üzemeltető? Ha a finanszírozás reklámot vagy az adatok pénzzé tételét is magában foglalja, lefedi-e a kinyilvánított cél a szakember által rábízott harmadik felek adatait?
5. Milyen az üzemeltető pénzügyi helyzete három-öt éves távlatban? Vannak-e olyan tényezők, amelyek a modell közelgő változására utalnak (függőben lévő tőzsdei bevezetés, kifutó finanszírozási kör, valószínű felvásárlás)?
6. Melyik joghatóságban van bejegyezve az üzemeltető? Melyik országban vannak fizikailag a szerverek? Ha eltérnek, melyik nemzeti jogszabály vonatkozik az adatkezelésre?
7. Mi történne, ha az üzemeltető joghatóságában érvényes hírszerzési utasítás kérné az adataim kiadását? Teljesíthetné-e ezt a vállalat technikailag?
8. Milyen technikai képességet tart fenn az üzemeltető a szolgáltatás felfüggesztésére, letiltására vagy megszüntetésére? Milyen szerződéses feltételek mellett? Milyen, történetileg dokumentált, szerződésen kívüli feltételek mellett?
9. Milyen kilépési terv létezik, ha az üzemeltető velem szemben gyakorolná ezt a képességet, jogosan vagy jogtalanul? Van-e dokumentált eljárás az adatok egy alternatív szolgáltatóhoz történő exportálására?
10. Ki ellenőrzi a hozzáférési hitelesítő adatokat? Vissza tudja-e állítani azokat az üzemeltető az én közreműködésem nélkül? Ez véd engem, vagy kiszolgáltat?
11. Létezik-e európai, önállóan üzemeltetett vagy közbeiktatott szerver nélküli alternatíva erre a konkrét funkcióra? Mennyi a tényleges költsége a felmért kockázathoz képest?
12. Ha a mai döntést öt év múlva egy ellenőr, egy auditor vagy egy adatszivárgás által érintett ügyfél vizsgálná meg, a jelenlegi választás védhető volna-e a ma rendelkezésre álló érvekkel, vagy bocsánatkérést igényelne azért, hogy nem tett fel ésszerű kérdéseket?

A kérdések nem tökéletes válaszokat várnak. Őszinte válaszokat várnak, amelyeket a becsületes üzemeltető tud adni, a kevésbé becsületes üzemeltető pedig kerüli, hogy pontosan megfogalmazza. A két üzemeltetőtípus közötti operatív különbség, ezt drámaiság nélkül mondjuk, általában úgy érzékelhető, hogy lassan elolvassuk a válaszokat, amelyeket önként kínálnak, még mielőtt többet kellene kérnünk.

Ezzel a cikkel lezárjuk a Cuadernos Lacre második ciklusát. A Schrems II-től örökölt szerkesztői adóssággal kezdtük, és egy operatív kérdőívvel fejezzük be. Útközben fogalmakon haladtunk át —hash, titkosítás, identitás— és alkalmazott elemzéseken —kill switch, üzleti modell, self-hosting—. A kiadvány kinyilvánított szerkesztői szándéka nem az volt, hogy eláraszsa az olvasót a problémák kimerítő listájával, hanem hogy eszközöket adjon a kezébe, amelyekkel bármely új szolgáltatás előtt meg tudja különböztetni, milyen jellegű választ fogad el. Ez a megkülönböztetés —az architektúra és az ígéret között— maga az eszköz. A többit minden szakember azon adatok szolgálatába állítja, amelyeket a gyakorlatában a kérdésre érdemesnek ítélt.

Források és további olvasnivalók

- Ez a kiadvány, 2. ciklus (2026. május) — *Schrems II, öt évvel később, Mi is valójában a SHA-256, Kill switch és az intézményi kisajátítás, Végpontok közötti titkosítás, igazából elmagyarázva, Az üzleti modell mint a bizalom jele, A 24 szó: mi az a kriptográfiai identitás, Self-hosting mint szakmai gyakorlat.* A hét cikk, amelyen ez a kérdőív nyugszik.
- (EU) 2016/679 rendelet — Általános Adatvédelmi Rendelet. Hivatkozási jogi keret a kérdőív által felvetett minden kérdéshez, különösen az 5., 6., 25., 28., 32., 33. cikk és az V. fejezet.
- Európai Adatvédelmi Testület — operatív iránymutatások és vélemények a Schrems II-ről, a nemzetközi adattovábbításokról, a hatásvizsgálatokról és a proaktív elszámoltathatóságról (2020–2024-es

kiadványok).

- Spanyol Adatvédelmi Ügynökség — 2022–2024 között közzétett szankciók adatkezelőkkel szemben nem megfelelő adattovábbítási eszközökért vagy érdemi tartalom nélküli formális hatásvizsgálatokért.
- noyb.eu — Európai Digitális Jogok Központja, amelyet Maximilian Schrems vezet. Nyilvános adattár az európai adatvédelmi szabályok valós, nem látszólagos betartásáról szóló panaszokról, jogorvoslatokról és elemzésekről.

[← Előző Self-hosting mint szakmai gyakorlat](#) [Következő → Amit egy aláírás nem tud megoldani](#)

Legutóbbi olvasmányok

- [Reflexió · 2026. június 29. Nem vagy névtelen](#)
- [Reflexió · 2026. május 27. Amit egy aláírás nem tud megoldani](#)
- [Elemzés · 2026. május 25. Self-hosting mint szakmai gyakorlat](#)

Vigye magával ezt a cikket, ahová csak szüksége van rá.

[↓ Markdown](#) [↓ Egyszerű szöveg](#) [↓ PDF](#)

A fájl letöltődik az Ön eszközére. Onnan elmentheti, importálhatja a Solo2-be, vagy megoszthatja bárhol. A Cuadernos nem dönt Ön helyett a fájl sorsáról.

Viaszpecsét · SHA-256 9c45663505da8baed2264b32a033262144a993caa8974153c385895b36f8f089

[Funkciók](#) [Újdonságok](#) [Blog](#) [Súgó](#) [Rólunk](#) [Kapcsolat](#)
[Átláthatóság](#) [Ellenőrzés](#) [Adatvédelem](#) [Feltételek](#) [Sütik](#)

Cuadernos Lacre · A [Menzuri Gestión S.L.](#) kiadványa ·
írta R.Eugenio · szerkesztette a [Solo2](#) csapata.

Ez a weboldal nem használ sütiket. Mindazt, amit a böngésződ betölt, mi írtuk vagy mi felügyeljük, és a saját európai szervereinken van tárolva: a névtelen látogatásszámláló (Umami, saját tárolású) és a nyelvválasztóhoz, valamint a világos vagy sötét témára vonatkozó beállításodhoz szükséges minimális JavaScript, amely a saját eszközödön tárolódik. Nincsenek külső cégektől származó erőforrások, nincsenek nyomkövetők, nincs profilalkotás, nincs adatmegosztás. Ha követni szeretne minket: [RSS](#).