USA CLOUD Act érthetően

- lényege és hatásai -

Október 10, 2026

CLOUD Act



- **C**larifying **L**awful **O**verseas **U**se of **D**ata Act
- 2018-ban elfogadott amerikai szövetségi törvény
- Felhatalmazza az amerikai hatóságokat (pl. FBI)
  - bírósági végzéssel
  - adatszolgáltatásra kötelezzék
  - az amerikai joghatóság alá tartozó IT- és felhőszolgáltatókat ,
  - függetlenül attól, hogy az adatokat fizikailag hol tárolják a világon
- Például: Ha a **Microsoft**, a Google vagy az Amazon egy európai adatközpontjában tárolod az adataidat, az amerikai bűnüldöző szervek (például az FBI) súlyos bűncselekmények nyomozása során legálisan kikérhetik azokat az amerikai anyacégen keresztül.

Mi az a CLOUD Act?

- **Hivatalos név**: Clarifying Lawful Overseas Use of Data Act (2018).
- **Amerikai törvény**: alapjaiban változtatta meg a digitális szuverenitást
- **A név csalóka**: Nem csak a felhőszolgáltatókra, hanem minden olyan tech szoftverre/vállalatra vonatkozik, amely amerikai joghatóság alá tartozik.
- **Alapelv:** A joghatóság nem a szerver fizikai helyén, hanem a szolgáltató tulajdonjogán és ellenőrzési körén alapul:
  - A szolgáltató tulajdonosa amerikai / részben amerikai
  - A szolgáltató központi székhelye Amerikában van

Miért jött létre? (Az előzmény)

- **A Microsoft-Írország ügy:**
  - Az FBI kábítószer-kereskedelmi nyomozás során adatokat kért a Microsofttól
  - A gyanúsított levelezése egy írországi szerveren (adatközpont) volt.
  - A Microsoft megtagadta az átadást, mondván, az USA törvényei nem érvényesek Írország szuverén területén.
  - Az FBI-nak a hivatalos nemzetközi jogsegélyen (MLAT) keresztül kellett volna eljárnia, ami hónapokig tart.
    https://www.kiteworks.com/risk-compliance-glossary/us-cloud-act/
    https://sovereignsky.no/laws/cloud-act/
- **A joghézag lezárása:**
  - Az amerikai kongresszus megunta a évekig tartó bírósági csatározást, és elfogadta a CLOUD Act-et.
  - A CLOUD Act kimondta, hogy ha egy cég amerikai (vagy ott működik), köteles kiadni az adatot, bárhol is tárolja azt a világon.
    https://proton.me/business/blog/cloud-act
    https://en.wikipedia.org/wiki/CLOUD_Act

A CLOUD Act két fő pillére

1. **Egyoldalú adatkiadási kötelezettség**:
   - Az USA bűnüldöző szervei bírói végzéssel kötelezhetik a szolgáltatókat adatszolgáltatásra külföldi szerverekről is súlyos bűncselekmények (pl. terrorizmus, kiberbűnözés, gyermekbántalmazás)
2. **Kétoldalú megállapodások (Executive Agreements)**:
   - Lehetővé teszi, hogy az USA szövetséges partnereivel (pl. az Egyesült Királyság) kölcsönös adatmegosztási egyezményeket kössön és azok közvetlenül kérhessenek le adatokat amerikai tech óriásoktól a saját nyomozásaikhoz.
   - Ha egy külföldi ország megfelel az amerikai kiberbiztonsági és emberi jogi feltételeknek, közvetlenül kérhet le adatokat az amerikai tech óriásoktól a saját nyomozásaihoz, megkerülve a lassú diplomáciai utakat.

https://www.eurojust.europa.eu/publication/cloud-act
https://www.congress.gov/crs-product/R45173

A nagy konfliktus: CLOUD Act vs. GDPR

- **Jogi csapdahelyzet (Catch-22)**:
  - A CLOUD Act kötelezi az amerikai felhőszolgáltatót az európai adatok átadására.
  - Az európai GDPR (48. cikk) szigorúan tiltja a személyes adatok harmadik országba (USA) történő továbbítását megfelelő uniós jóváhagyás nélkül
  - Kivéve, ha azt nemzetközi jogsegélyegyezmény (MLAT) szabályozza.
    https://www.exoscale.com/blog/cloudact-vs-gdpr/
    https://www.cyberthreat.report/p/az-europai-unio-digitalis-szuverenitasanak

- **A szolgáltatók dilemmája**:
  - Ha átadja az adatot, súlyos GDPR bírságot kockáztat az EU-ban (akár a globális forgalom 4%-a).
  - Ha a szolgáltató megtagadja az átadást, Amerikai bírósági ítéletet és bírságot kockáztat (Contempt of Court).
- **Következmény**:
  - Az amerikai cégek európai leányvállalatai választani kényszerülnek, hogy az amerikai vagy az európai törvényeket szegjék-e meg.
  - Az európai ügyfelek adatai állandó jogi bizonytalanságban vannak.
    https://www.cyberthreat.report/p/az-europai-unio-digitalis-szuverenitasanak

Kit érint ez a probléma? (A kockázati kör)

- **Közvetlen érintettek köre**: Minden olyan európai cég és állampolgár, aki amerikai szolgáltatók (pl. AWS, Microsoft Azure, Google Cloud) infrastruktúráját használja.
  - Európai vállalatok és startupok, amelyek amerikai hiperskálarú szolgáltatók (AWS, Azure, GCP) infrastruktúrájára építi szoftvereit vagy AI-modelljeit.
  - Közszféra és egészségügy: Kórházak, klinikák, kutatóintézetek és állami szervek, amelyek állampolgárok érzékeny személyes és egészségügyi adatait kezelik.
  - Európai állampolgárok: Bárki, akinek a digitális lábnyoma (orvosi leletek, pénzügyi adatok, e-mailek) amerikai tulajdonú szervereken fut.
    https://www.nexthop.fr/en/cloud-act/

- **Tévhit**: "Az adataim biztonságban vannak, mert az EU-n belüli adatközpontot választottam."
- **A valóság**: Az anyacég amerikai mivolta miatt a CLOUD Act alá esik, törvény kötelezi őket az adatok átadására
  https://www.youtube.com/watch?v=QJgwA8tkJ-U&t=830

Hogyan lehet védekezni? (Megoldások)

- **Európai alternatívák**: Tisztán európai tulajdonú és joghatóságú felhőszolgáltatók választása.
- **Titkosítás (Client-side encryption)**: Olyan titkosítási kulcsok használata, amelyeket kizárólag az európai ügyfél kezel, így a szolgáltató technikailag sem tudja olvasható formában átadni az adatokat a hatóságoknak.
- **Zero-Knowledge architektúrák** bevezetése.

https://wire.com/en/blog/cloud-act-eu-data-sovereignty
https://aws.amazon.com/compliance/cloud-act/
https://www.exoscale.com/blog/cloudact-vs-gdpr/

Európa és Ázsia válasza

- Alapjaiban különböző, és még kontinenseken belül, sőt országonként is rendkívül eltérő
- Európa a szigorú adatvédelmi jogra és a digitális szuverenitásra épít
- Ázsia megosztott:
  - Egyes országok (mint Kína) totális adatlokalizációt írnak elő,
  - Mások kétoldalú megállapodásokkal inkább együttműködnek az USA-val.

Európa vs. Ázsia: Különböző megközelítések

Régió / Ország	Stratégia a CLOUD Actre	Jogi / Technológiai Válasz
Európai Unió	Jogvédelmi és szuverenitási fókusz	A GDPR szigorú korlátozásokat szab meg, a Gaia-X kezdeményezés pedig európai felhőalternatívákat épít.
Franciaország	Extrém szigor (SecNumCloud)	Betegadatok esetén kötelező a SecNumCloud minősítés. Az állami felhőből teljesen kizárják az amerikai tech óriásokat.
Németország	Szigorú lokalizáció	Különösen érzékeny a szövetségi adatokra és a betegadatokra (pl. C5 minősítési követelmények).
Kína	Totális állami kontroll és elzárkózás	Az Adatbiztonsági Törvény megtiltja az adatok külföldi hatóságoknak történő átadását állami jóváhagyás nélkül.
Japán & Szingapúr	Együttműködés és hibrid modellek	Megbízható adatátviteli megállapodásokat kötnek az USA-val, miközben hazai kormányzati felhőket is fenntartanak.

Miért használnak az európai AI startup-ok mégis amerikai infrastruktúrát?

- A hardverhiány és a brutális infrastruktúra-költségek
  - Azonnali elérhetőség
  - Rugalmas skálázhatóság
- Kész AI-ökoszisztéma és „Time-to-Market”
  - Menedzselt szolgáltatások
  - Gyorsaság
- Az alapmodellek (Foundation Models) kisajátítása
- A vevők (Kórházak, Gyógyszergyárak) bizalma és integrációja