A SCHREMS II ÍTÉLET HATÁSA AZ ADATVEZÉRELT MARKETING SZEKTORBAN

avagy mi a teendő a nem európai tárhely- és egyéb szolgáltatókkal, az EGT-én kívül tárolt, illetve az EGT-én kívülire történő adattovábbításokkal

HALÁSZ BÁLINT, ÜGYVÉD, PARTNER, BIRD & BIRD
NAGY JUDIT, ÜGYVÉDJELÖLT, BIRD & BIRD
2020. DECEMBER 4.

A közelmúltban számos fejlemény történt a nemzetközi adattovábbítások területén. A Schrems II ítélet atombombaként teljesen romba döntötte a Privacy Shield-et, de megrogyasztotta az SCC-ket is. Ezt követően egyes tagállamok adatvédelmi hatóságai gyakorlati útmutatókat adtak ki, amelyek alapján tűzoltás-szerű intézkedéseket lehetett tenni, de ami a helyzet hosszabb távú kezelését illeti, mindenki két helyre figyelt: az Európai Adatvédelmi Testületre (EDPB) és az EU Bizottságra. A közelmúltban előbbi ajánlásokat bocsátott ki, míg utóbbi új SCC-tervezeteket tett közzé. Az ezekben található elvárásoknak való megfelelés azonban jelentősen több erőforrást igényel, mint korábban.

A TÉNYEK

- 2020. július 16-án az az Európai Unió Bírósága (EUB) érvénytelennek mondta ki a Privacy Shield-ről szóló Bizottsági határozatot, amely az EU és az USA közötti adattovábbítások esetén az egyik olyan eszköz volt, amely biztosította az értintettek számára a személyes adatok megfelelő szintű védelmét az USÁ-ban.
- Az EUB szerint az USA nemzetbiztonsági szervei hozzáférhetnek az európai állampolgárok USÁ-ba továbbított adataihoz, ezért ténylegesen nem biztosított a megfelelő szintű védelem.
- Az EUB a személyes adatok megfelelő szintű védelmét biztosító másik eszközről, az EU modellklauzulák (Standard Contractual Clauses, SCCs) vonatkozásában is leszögezte, hogy az egyes adatátadásokat esetről-esetre kell megvizsgálni és ha a nem biztosított a megfelelő védelem ezen harmadik ország hatóságainak és bíróságainak az adatokhoz való hozzáféréseivel szemben, akkor a feleknek *további, hatékony biztosítékokat* kell nyújtaniuk, vagy fel kell függeszteniük a szóban forgó adattovábbítást.
- Az ítélet ugyanakkor nem adott további iránymutatást arra, hogy melyek ezek a *további, hatékony biztosítékok.*
- Egyes EU tagállami adatvédelmi hatóságok korábban adtak ki javaslatokat, amelyek tartalmaznak kézzelfogható iránymutatásokat.
- Az Európai Adatvédelmi Testület (European Data Protection Board, „EDPB") a nemzeti adatvédelmi hatóságok jóváhagyásával két ajánlást adott ki 2020 november 11-én: (i) az

adattovábbításokhoz szükséges *további hatékony biztosítékokról* és a (ii) lehallgatásokkal kapcsolatos alapvető európai garanciákról, melyek a Schrems II ítélet értelmezésén alapulnak. Az előbbi nyilvános konzultáció tárgyát képezi, míg az utóbbi végleges.

- Az Európai Bizottság 2020. november 12-én nyilvánosságra hozta az új, GDPR-nak megfelelő SCC-kről szóló végrehajtási határozattervezetet. Ennek mellékletében megtalálhatóak az új SCC minták, melyek a GDPR követelményein túl figyelembe veszik a Schrems II ítélet követelményeit is. A végrehajtási határozattervezet december 10-ig bárki számára észrevételezhető.
- Max Schrems, illetve mögötte álló NOYB, 2020. augusztus 17-én tette közzé, hogy panaszokat nyújtott be 101 olyan weboldal ellen, amelyek egy hónappal a Schrems II ítélet kihirdetését követően továbbra is továbbítanak adatokat a Facebook vagy a Google számára az USÁ-ba a Google Analytics vagy a Facebook Connect szolgáltatás keretében. A bepanaszolt weboldalak között a három magyar portál is van.
- A NAIH – nem hivatalos források szerint – kérdőíveket küldött ki bizonyos magyarországi adatkezelők részére a külföldi adattovábbításokkal kapcsolatban, melyre 30 nap válaszadási határidőt tűzött.
- A jelen cikk összefoglalja azt, hogy milyen lépéseket érdemes megtenni a Schrems II ítélet eredményeképpen előállít bizonytalan helyzetből adódó kockázatok mérséklése érdekében.

A HÁTTÉR: AZ EGT-ÉN KÍVÜLI ADATTOVÁBBÍTÁSOK

A GDPR (és elődje, az EU Adatvédelmi Irányelv) megközelítése az, hogy a személyes adatok az Európai Gazdasági Térségen (EGT, ami az EU tagállamokat és Izlandot, Liechtensteint és Norvégiát foglalja magában) belül biztonságban vannak abból a szempontból, hogy az érintettek számára a jogszabályi háttér megfelelő jogokat biztosít arra, hogy rendelkezhessenek adataikról, tájékoztatást kérhessenek és egyéb jogaikkal élhessenek, valamint, hogy ha úgy gondolják, hogy jogaik sérültek, akkor jogorvoslati lehetőségek álljanak rendelkezésükre. A személyes adatokat az EGT-n kívülre azonban csak akkor lehet továbbítani ha valamilyen módon biztosított az adatok megfelelő szintű védelme az adatokat megkapó félnél, azaz az adatimportőrnél.

A megfelelő szintű védelmet többféle jogi eszközzel lehet biztosítani, ezek közül a leggyakoribbak:

- **Megfelelőnek elismert országok**: vannak olyan országok, amelyet az EU Bizottság megfelelőnek ismert el, így ezekbe lehet továbbítani adatokat (ilyen pl. Izrael, Kanada, Svájc, a teljes lista a Bizottság honlapján található).
- **SCCs**: a gyakorlatban sokkal gyakrabban használt megoldás az SCC-k alkalmazása volt. Ezek tulajdonképpen EU Bizottsági határozat formájában megjelenő modellszerződések, amelyek úgy biztosítják az érintettek számára az előbb említett jogokat, hogy az adatimportőr szerződéses úton vállal kötelezettségeket, amelyek egyébként a saját nemzeti jogán túlmennek, és többek között az érintettek számára biztosítják azon jogokat, amelyek egyébként az EU-ban őket a GDPR alapján megilletik. Az SCC-knek eddig két típusa volt: adatkezelő-adatkezelő (C2C) és adatkezelő-adatfeldolgozó (C2P). Az új bizottsági határozat ezeket a változatokat tovább bővíti, például ezek után lesz az amúgy régóta várt adatfeldolgozó-adatfeldolgozó (P2P) SCC is.

- **BCRs:** kötelező erejű vállalati szabályok, amelyek egy cégcsoporton belül biztosítják a személyes adatok továbbításával kapcsolatos megfelelő védelmet. A BCR-t az adatvédelmi hatóságok a GDPR szerinti egységességi mechanizmus alapján hagyják jóvá egy hosszadalmas eljárás keretén belül. A BCR-ok cégcsoporton kívüli adattovábbítás érdekében nem használhatóak.
- **Magatartási szabályok / tanúsítványok:** elméletben a GDPR lehetőséget ad magatartási szabályok vagy tanúsítványok alapján történő adattovábbításokra is. A gyakorlatban azonban ilyen eszközök még nem állnak rendelkezésre.
- **Privacy Shield**: az USA-ba történő adattovábbítások esetén ez volt egy további lehetőség, amely tulajdonképpen egy, az Egyesült Államok Kereskedelmi Minisztériuma által működtetett éves önértékelésen alapuló rendszer volt: ha valaki megszerezte és fenntartotta a Privacy Shield tanúsítványt, akkor ez önmagában biztosította az USA-ban a megfelelő szintű védelmet.

AZ EUB ATOMBOMBÁJA: A PRIVACY SHIELD ROMBA DŐLT, AZ SCC-K MEGROGGYANTAK

Az EUB a Schrems II ítéletben azonnali hatállyal érvénytelenítette a személyes adatok továbbításáról szóló 2016/1250 EU Bizottsági határozatot az Egyesült Államokba történő adattovábbításról (Privacy Shield). Ennek a döntésnek az alapja lényegében az Egyesült Államok titkosszolgálatokra vonatkozó jogi előírásai, különösen a Foreign Intelligence Surveillance Act (külföldi hírszerzési felügyeletről szóló törvény, „FISA") 702. §-a és az Executive Order 12333, amely nem biztosít olyan védelmet a személyes adatok tekintetében, amely egyenértékű az EU-ban érvényes előírásokkal (hiányoznak a GDPR szerinti megfelelő biztosítékok, a jogok végrehajthatósága és a hatékony jogorvoslatok).

Mindez azt jelenti, hogy azon európai adatkezelők/adatexportőrök, akik eddig olyan USA-beli partnereknek, szolgáltatókkal dolgoztak együtt (pl. felhőben tárolt adatok, hírlevél küldés, analitika stb.), amelyeknél a Privacy Shield biztosította a megfelelő szintű védelmet, légüres térbe kerültek, elvesztették azt a jogi eszközt, amely eddig a megfelelő szintű védelmet biztosította.

Az első logikus reakció természetesen az lett volna, hogy nézünk egy alternatív jogi eszközt, amelyre át lehet térni, és nem kell lekapcsolni az USA-ba történő adattovábbítást, az USA-ban lévő szolgáltatók igénybevételét. Az egyetlen ilyen szóba jöhető alternatíva az SCC-k voltak, azonban az EUB az ítéletében jelezte, hogy önmagában az ezekre való áttérés kevés, mert országonként meg kell vizsgálni, hogy gyakorlati szempontból valóban biztosítanak-e megfelelő szintű védelmet, és ha nem, akkor a *további, hatékony biztosítékokat* kell nyújtani vagy fel kell függeszteni a szóban forgó adattovábbítást. Ilyen kiegészítő biztosítékok magukban foglalhatják a technikai intézkedéseket, például az adatok titkosítását, szerződéses biztosítékokat vagy egyéb technikai vagy szervezeti intézkedéseket. Az EUB azonban az ítéletben nem részletezi ezeket a kiegészítő biztosítékokat, így nem volt teljesen egyértelmű, hogy az adatkezelőknek/adatexportőröknek e tekintetben milyen elvárásoknak kéne megfelelniük.

Az USA részéről természetesen jött reakció: a Kereskedelmi Minisztérium közzétett egy fehér könyvet, amelyben többek között azzal érvelnek, hogy az USA-ban tárolt európai személyes adatok többsége nem olyan, amelyek érdekesek lehetnének az USA nemzetbiztonsági szerveinek, továbbá hogy a terrorizmus elleni harcban együttműködnek az EU-val, illetve az EU tagállamokkal, amelyek kérnek adatokat az USA-ból e célra. Továbbá az USA Kereskedelmi Minisztériuma és az Európai

Bizottság közös sajtónyilatkozatban bejelentette, hogy tárgyalásokat kezdtek egy olyan megerősített Privacy Shield keretrendszerrel kapcsolatban, amely az EUB által támasztott követelményeknek is megfelel.

HOGYAN TOVÁBB: MI VAN AZ EDPB AJÁNLÁSAIBAN ÉS AZ ÚJ SCC-KBEN?

Az EDPB ajánlásai és az Európai Bizottság által megjelentett új SCC-k egymással szoros összefüggésben állnak, és beépíthetőek az EDPB adattovábbításokhoz szükséges *további hatékony biztosítékokról* szóló ajánlásа által javasolt az ún. roadmap-szerű hatásvizsgálatba, amelyeket az adat exportőröknek a Schrems II ítéletet követően kötelezően el kell végezniük minden adattovábbítás esetén. Az ún. „roadmap" alapján az adatexportőröknek az alábbi lépéseket kell megtenniük:

#01 Az első lépés – nem meglepő módon – az adattovábbítások feltérképezése. Amennyiben az adatexportőrnek van adatkezelési nyilvántartása, ez a dokumentum jó kiindulópont lehet. Adattovábbítások feltérképezése során azt is figyelembe kell venni, ha az EGT-n kívüli adatfeldolgozó egy másik EGT-n kívüli országba továbbítja az adatokat. Az adatexportőrnek már itt kötelessége, hogy az adattakarékosság elvét figyelembe véve az adattovábbítást csak a szükséges adatokra korlátozza.

#02 A második lépés annak meghatározása, hogy az adatexportőr melyik jogi eszközt kívánja használni a megfelelő védelem biztosítása érdekében (lásd korábbi felsorolás).

Amennyiben ez a jogi eszköz az Európai Bizottság megfelelőségi döntése, az adatexportőrnek nincs egyéb feladata a „roadmap" alapján.

A választott jogi eszköz lehet például az Európai Bizottság által a végrehajtási határozattervezetben közzétett új SCC is. Mivel azonban ennek a szövege még nem tekinthető véglegesnek a folyamatban lévő nyilvános konzultációra tekintettel, ennek használata (még) nem javasolt. A véglegessé válás, azaz új SCC határozat hatályba lépése reálisan 2021 első felében várható. A régi SCC-ket az adatexportőr a hatályba lépéstől számított egy éves átmeneti időben használhatja jogszerűen. Ez azt jelenti, hogy előreláthatólag 2022 első feléig lesz idő az átállásra a régi SCC-kről az új SCC-kre. Ugyanakkor ezt véletlenül sem szabad úgy értelmezni, hogy annak az adatexportőrnek, aki régi SCC-ket használt, ne lenne teendője (lásd következő lépés).

#03 A harmadik lépés az, ami a gyakorlatban a legnagyobb kihívás elé állítja az adatexportőröket, ez ugyanis annak meghatározásáról szól, hogy a választott jogi eszköz, például az SCC-k hatékonyak-e az adattovábbítás körülményeinek tekintetében. Ehhez a vizsgálathoz az adatexportőrnek figyelembe kell vennie, hogy a harmadik ország **releváns jogi szabályozása** (pl. adatvédelmi jogszabályok, lehallgatási jogszabályok amennyiben ezek az adott adattovábbításra alkalmazandóak, egyéb, az adott adattovábbításra alkalmazandó jogszabályok) akadályozza-e az adatimportőrt, hogy pl. az SCC-kben vállalt kötelezettségeinek eleget tegyen. Az EDPB szerint a releváns jogi szabályozásról elsősorban az adatimportőrtől lehet kérni tájékoztatást, vagy a EDPB adattovábbításokhoz szükséges további hatékony biztosítékokról szóló ajánlásа 3. mellékletében felsorolt forrásokból is lehet tájékozódni (pl. a strasbourgi emberi jogi bíróság ítéletei, az Európa Tanács állásfoglalásai, civil szervezetek jelentései). Amennyiben nincsen releváns jogi szabályozás akkor figyelembe kell venni az adatok kezelésével kapcsolatos általános gyakorlatot, ideértve a harmadik országbeli hatóságok adatokhoz való tényleges hozzáférésének lehetőségét.

A Schrems II ítélet alapján a lehallgatási jogszabályoknak különös jelentőséget kell tulajdonítani a fenti értékelés során. Az adott ország lehallgatási jogszabályainak értékeléséhez az EDPB lehallgatásokkal kapcsolatos alapvető európai garanciákról szóló ajánlása ad iránymutatást.

Amennyiben az adatexportőr nem azonosít olyan jogszabályt vagy gyakorlatot, amely akadályozza az adatimportőrt abban, hogy a vállalt kötelezettségeinek eleget tegyen, akkor az adattovábbításhoz a választott jogi eszköz minden további nélkül használható.

Azt fontos megjegyezni, hogy a Schrems II döntés alapján az USA releváns jogszabályai, különösen a lehallgatási jogszabályok akadályozzák az adatimportőrt, hogy az SCC-k szerinti kötelezettségét teljesítse, mivel nem felelnek meg az EDPB lehallgatásokkal kapcsolatos alapvető európai garanciákról szóló ajánlásában foglaltaknak. Így az USA-ba történő adattovábbítás esetén az adatexportőr az értékelés ezen harmadik lépésnél – szűk kivételek mellett – nem állhat meg.

#04 A negyedik lépés a megfelelő kiegészítő biztosítékok azonosítása. Az EDPB ajánlás három kategóriát azonosít: (i) technikai biztosítékok (például titkosítás, álnevesítés); (ii) szerződéses biztosítékok (például szerződéses többletkötelezettségek telepítése az adatimportőrre); (iii) szervezeti biztosítékok (például belső szabályzatok, mechanizmusok kialakítása). Ezeket a lehetséges intézkedéseket az EDPB az adattovábbításokhoz szükséges további hatékony biztosítékokról szóló ajánlása második melléklete részletesen ismerteti különböző gyakorlati példákon keresztül.

Fontos megjegyezni, hogy az EDPB álláspontja szerint, amennyiben a harmadik ország lehallgatási jogszabályai nem felelnek meg az EDPB lehallgatásokkal kapcsolatos alapvető európai garanciákról szóló ajánlásában foglalt követelményeknek, akkor pusztán szerződéses vagy szervezeti biztosítékokkal nem lehet biztosítani a jogszerű adattovábbítás lehetőségét.

Ide tartozik, hogy az EDPB álláspontja szerint önmagában az, hogy a továbbított adatok az adatexportőr szerint valószínűleg nem érdekesek az importőr országának nemzetbiztonsági szolgálatai részére (pl. csak emailcímek kerülnek továbbításra egy hírlevél-küldő rendszerbe), nem mentesíti az adatexportőrt a fenti kötelezettségek alól. Máshogy fogalmazva: még egyszerű, banális adatok továbbítása esetén is ugyanazt a tesztet kell elvégezni, mert az EDBP szerint szubjektív faktorokat nem, csak objektív faktorokat lehet figyelembe venni a vizsgálat során.

#05 Az ötödik lépés a megfelelő kiegészítő biztosítékok alkalmazása. Az EDPB kiemeli, hogy amennyiben olyan szerződéses biztosítékot alkalmaz az adatexportőr, amely az SCC-k szövegének ellentmond, akkor az ilyen módosításhoz az adatvédelmi hatóság engedélyét kell kérni. Egyebekben az adatexportőr nem köteles tájékoztatni az adatvédelmi hatóságot arról, hogy kiegészítő biztosítékokat alkalmaz.

#06 A hatodik lépés, hogy az adatexportőr megfelelő időközönként felülvizsgálja a fenti értékelést.

A fentiekből látható, hogy vége van a Schrems II előtti „boldog békeidőknek", amikor is elég volt a fenti lépések közül az első hármat megtenni, ami az USA-ba történő adattovábbítás esetén a legtöbb esetben kimerült a Privacy Shield regisztráció ellenőrzésében vagy az adatimportőr szerződéses csomagjának részét képező SCC-k elfogadásában. Schrems II után ennél jóval több és összetettebb feladat hárul az adatexportőrökre, hiszen az EDPB szerint minden egyes esetben egyedileg kell

mérlegelniük olyan szempontokat, amelyekre nem biztos, hogy van rálátásuk, illetve erőforrásuk (lásd a fenti harmadik lépésben említett, a harmadik ország releváns jogi szabályozásának megvizsgálása), továbbá az SCC-ken túl megfelelő kiegészítő biztosítékokat is kell alkalmazniuk (lásd a fenti negyedik lépésben említett technikai, szerződéses és szervezeti biztosítékok).

A gyakorlati problémát az jelenti, hogy az esetek többségében ezek vonatkozásban az adatexportőr az adatimportőrre van utalva, azaz ha az utóbbi nyújt ilyen megoldásokat, akkor ezeknek meg tud felelni az exportőr, míg ha nem vagy egyébként nem hajlandó együttműködni, akkor az exportőr egyedül valószínűleg nem fogja tudni ezeket a kiegészítő biztosítékokat megvalósítani. Előbb-utóbb azért az valószínű, hogy az adatimportőrök is alkalmazkodnak a helyzethez, és előbb-utóbb szolgáltatásuk részéve teszik ezeket a kiegészítő biztosítékokat. Mindez azt jelenti, hogy az adatexportőröknek egyenként kell monitorozniuk az általuk használt adatimportőröket és egyedileg kell értékelniük a kockázatokat.

VAN BÁRMI MÁS MEGOLDÁS A JOGSZERŰ ADATTOVÁBBÍTÁSRA?

Jelenleg a fenti „roadmap" szerinti vizsgálat elvégzése az egyetlen a jogszerű módja az adattovábbításnak. Azok az adat exportőrök, akik ezt mellőzik, potenciálisan adatvédelmi hatósági eljárás alá kerülhetnek – amennyiben a hatóság erről a gyakorlatról tudomást szerez.

VAN EGYÁLTALÁN JELENLEG JOGSZERŰ MEGOLDÁS AZ USA-BA TÖRTÉNŐ ADATTOVÁBBÍTÁSOKRA?

Az EDPB ajánlás természetesen nem mondja ki egyértelműen, hogy az EU-USA adattovábbítás jogellenes. Azonban a jogszerű adattovábbításra az USA esetében – a korábbihoz képest – igen magas feltétel-küszöb vonatkozik, mivel az EUB már a Schrems II ítéletben megállapította, hogy az USA lehallgatásokkal kapcsolatos jogszabályi környezete nem felel meg az lényeges európai követelményeknek. Emiatt kiegészítő biztosítékok alkalmazása EU-USA adattovábbítások esetén csak akkor kerülhető el, ha az adott amerikai szolgáltató nem esik a lehallgatási jogszabályok hatálya alá. Ennek hiányában az USA-ba történő adattovábbítás akkor lehet jogszerű az EDPB ajánlás szerint, ha az adatimportőr nem fér hozzá az adatokhoz azok titkosítás nélküli formájában, vagy pedig akkor, ha az adatexportőr más olyan technikai kiegészítő biztosítékot alkalmaz, amely az amerikai hatóságok személyes adatokhoz való hozzáférését lehetetlenné teszi.

E körben megjegyzendő, hogy az EDPB ajánlás nem rendelkezik kötelező erővel, hanem az ún. puha jog eszköze. Azonban az EDPB ajánlások megállapításai szorosan követik a Schrems II ítéletet, melynek EUB által meghozott ítéletként kötelező ereje van, valamint az ajánlást minden tagállami adatvédelmi hatóság elfogadta (lásd lent).

MIK A KILÁTÁSOK ÉS AZ ALTERNATÍVÁK?

Ami a hosszabb távú kilátásokat illeti, trendként az rajzolódik ki, hogy az EGT-én kívüli adattovábbítások inherens kockázatot, illetve jelentős adminisztratív többletterhet fognak jelenti, ha olyan országba történnek, amelyek nem szerepelnek a Bizottság megfelelőségi listáján. A jogilag legbiztonságosabb megoldásnak az látszik, hogy ha az európai természetes személyek adatai el sem hagyják el az EGT területét. Jogilag szintén biztonságos megoldás olyan országokban található szolgáltatókat használni, ahol van érvényben megfelelőségi döntés. Ezen EGT-n kívüli országok listája itt található. Jelenleg 13 ország van a listán: Andorra, Argentína, Kanada, Feröer-szigetek,

Guernsey, Izrael, Man-sziget, Japán, Jersey, Új-Zéland, Svájc, Uruguay. Dél-Korában folyamatban vannak a tárgyalások az elismerésről.

Amennyiben az adatok EGT-én belüli vagy fenti országokba történő továbbítására nincs lehetőség, akkor az EDPB által meghatározott „roadmap"-et követve minél pontosabban érdemes dokumentálni azt, hogy az amerikai (vagy más harmadik ország-beli) szolgáltató használata miért felel meg az európai követelményeknek. E tekintetben érdemes kockázat alapú megközelítést alkalmazni, azaz a legkockázatosabb adattovábbításokat érdemes az első körben ilyen vizsgálatnak alávetni.

Végül, mivel mind az EDPB adattovábbításokhoz szükséges további hatékony biztosítékokról szóló ajánlása, valamint az Európai Bizottság SCC-kről szóló végrehajtási határozattervezete jelenleg nyilvános konzultáció tárgyát képezi, az érintett szereplők jelenleg még kifejezhetik a véleményüket a kialakult helyzettel kapcsolatban, amelyet az EDPB és az Európai Bizottság figyelembe vehet a dokumentumok véglegesítése során.

Az EU-USA adattovábbításokkal kapcsolatban kedvező kilátást jelenthet, hogy mind az USA mind az Európai Bizottság elkötelezettnek tűnik az adattovábbítások fenntartása iránt, így várható, hogy belátható időn belül valamilyen intézményesített megoldás születik majd ezen adattovábbítások „legalizálására", akár a megerősített Privacy Shield keretrendszer formájában. Azonban az, hogy ez a belátható idő pontosan hány hónapot vagy rosszabb esetben esetleg évet jelent, jelenleg megjósolhatatlan.

MI ARRA AZ ESÉLY, HOGY A MAGYAR ADATVÉDELMI HATÓSÁG ELJÁRÁST INDÍT/BÍRSÁGOL A FENTI KÉRDÉSEKBEN?

Jelenleg nehéz előre látni, hogy a magyar adatvédelmi hatóság hogyan fog reagálni a fentiek alapján kialakulni látszó helyzetre. Az EDPB képviselői a november 17-én az IAPP által szervezett online beszélgetés keretében hangsúlyozták, hogy bár az ajánlást az EDPB titkársága készítette elő, a tagállami adatvédelmi hatóságok azt egyhangúlag jóváhagyták. Az EDPB úgy értelmezte ezt az egyhangúságot, hogy a nemzeti hatóságok készek az ajánlás kikényszerítése érdekében eljárni. Az EDPB szerint a nemzeti hatóságok az ajánlás jóváhagyásakor figyelembe vették azt is, hogy az ajánlás kikényszerítése nagyobb erőforrások bevonásával fog járni. Az ajánlás jóváhagyása az EDPB szerint azt jelzi, hogy a nemzeti hatóságok ezen erőforrásokkal rendelkeznek.

A Schrems II ítélettel kapcsolatban eddig mind az európai, mind az amerikai cégeknek főként a kivárás volt a taktikája, annak ellenére, hogy az EUB nem állapított meg átmeneti időszakot az ítéletének való megfelelésre. Ezt az attitűdöt a NOYB kérdőíve is megerősítette. Annak érdekében, hogy a Schrems II ítélet megállapításainak érvényt szerezzen a gyakorlatban is, a NOYB a panaszt nyújtott be 101 olyan weboldal ellen, amelyek egy hónappal a Schrems II Ítélet kihirdetését követően továbbra is továbbítanak adatokat a Facebook vagy a Google számára az USÁ-ba a Google Analytics vagy a Facebook Connect szolgáltatás keretében. A bepanaszolt weboldalak között a három magyar portál is van. A NOYB panaszok elbírálására az EDPB erre dedikált munkacsoportot hozott létre annak érdekében, hogy egységes reakció szülessen a nemzeti hatóságok részéről.

A fentiek alapján az várható, hogy NAIH is a munkacsoport által kialakított álláspont szerint fogja elbírálni az EU-USA adattovábbításokat. Az egyelőre kiszámíthatatlan, hogy a NOYB panaszok elbírálására mikor kerülhet sor.

Az szintén kérdéses, hogy a NAIH fog-e általános vizsgálatot indítani magyar adatkezelők és adatfeldolgozók ellen. Aggodalomra adhat okot, hogy a NAIH – nem hivatalos források szerint – kérdőíveket küldött ki bizonyos magyarországi adatkezelők részére a külföldi adattovábbításokkal kapcsolatban, melyre 30 nap válaszadási határidőt tűzött.

A BIG TECH VÁLLALATOKNAK VAN EU-S LEÁNYVÁLLALATA ÉS EU-BAN TALÁLHATÓ SZERVEREIK, EZ HASZNÁLATA AKKOR RENDBEN VAN?

Ami USA-beli techóriások európai nagyvállalatait illeti, egyelőre nem világos, hogy ezek milyen megítélés alá fognak esni. Egyik oldalról nézve ezek európai vállalatok, amelyek adott esetben európai szervereken tárolják az adatokat, másik oldalról nézve anyacégük az USA-ban található, és emiatt rájuk vonatkoznak az USA extraterritoriális jogszabályai, mint például a CLOUD Act. Ami utóbbit illeti, a Microsoft Corp. v. United States ügy végeredménye mutatja, hogy a CLOUD Act alapján a Microsoft is kiadja az EU-ban tárolt adatokat az amerikai kormányszerveknek. Egyes vélemények szerint azonban a CLOUD Act alapján történő adatkérések nem nagyszámú érintett megfigyelését jelentik, hanem egyes személyekre vonatkozó adatkéréseket, amely esetében biztosított valamilyen szintű jogorvoslati lehetőség, ezért nem lehet kijelenteni, hogy az USA-beli szolgáltatók EU-s leányvállalatainál nem áll fent a megfelelő szintű védelem. Mások azonban ezzel ellentétes vélemények vannak. Nem lenne meglepő, ha pár éven belül az EUB ebben a kérdésben is ítéletet hozna... Stílszerűen: stay tuned.