DIMSZ adatvédelmi webinár: Adattovábbítás a felhőbe és cookie megfelelés

Miről lesz szó?

1. **EGT-n kívüli adattovábbítások és felhőszolgáltatások igénybevételének értékelése.** Az Európai Adatvédelmi Testület (EDPB) két ajánlást tett közzé, amelyek az Európai Unió Bíróságának Schrems II ítélete nyomán útmutatást nyújthatnak a szervezeteknek az Európai Gazdasági Térségen kívüli adattovábbításaik megfelelőségének biztosításával kapcsolatban. Hogyan kell értékelni és dokumentálni azoknak a feltételeknek a megvalósulását, amelyek mellett a GDPR-nak megfelelő módon továbbíthatók személyes adatok az EGT-n kívülre?

2. **Cookiek használata és a kapcsolódó tájékoztatók felülvizsgálata.** Az elmúlt időszakban az európai adatvédelmi hatóságok több ajánlást is tettek, és bírságokat is kiszabtak a vállalatok weboldalain használt cookiek és egyéb online nyomkövetők használatával kapcsolatban. Hogyan érdemes felülvizsgálni a cookie tájékoztatókat és hozzájáruló nyilatkozatokat?

A legfontosabb adatvédelmi fejlemény 2020-ban

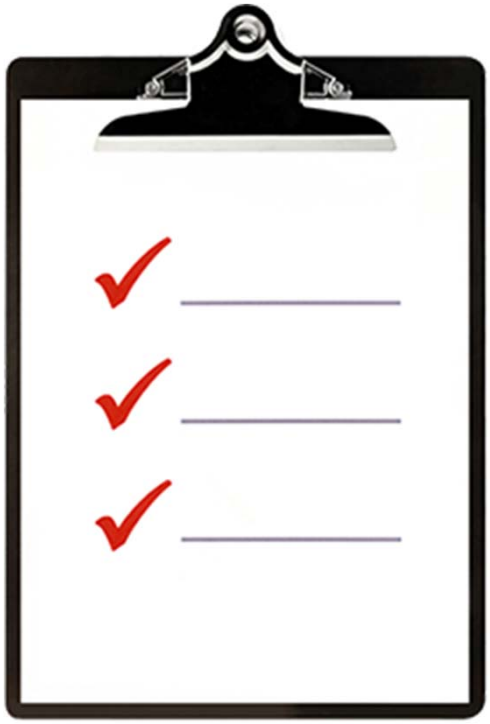
Mi a Supplemental Measures Recommendations (SMR) Ajánlás célja?

Hogyan kell a szervezeteknek értékelniük és dokumentálniuk azoknak a feltételeknek a megvalósulását, amelyek mellett a GDPR-nak megfelelő módon továbbíthatnak adatokat az EGT-n kívülre, a Schrems II ítélet megállapításait is figyelembe véve?

Az SMR Ajánlás 6 lépésben határozza meg, mit kell tenni az értékelés során.

Az értékelés részét képezi a European Essential Guarantees (EEG) Ajánlásban meghatározott szempontok vizsgálata is – fókusz: a célországban a bűnüldözési és nemzetbiztonsági célú megfigyelések (*surveillance*) során megfelelően biztosított-e a személyes adatok védelme?

SMR Ajánlás - feladatok



1. lépés:
Adattérkép készítése (*data mapping*)

2. lépés:
Az adattovábbítási eszközök (*transfer tools*) azonosítása

3. lépés:
A célország vizsgálata

4. lépés:
Kiegészítő védelmi intézkedések elfogadása

5. lépés:
Az SCC vagy a BCR kiegészítése

6. lépés:
A megfelelőség nyomonkövetése

1. lépés: Adattérkép készítése (*data mapping*)

Az adatexportőr nyilvántartja, milyen adatokat továbbít az EGT-n kívülre.

Ez tulajdonképpen a GDPR 30. cikkében előírt kötelezettség megismétlése.

Specifikus esetek:

- „újbóli továbbítások” (*onward transfer*, például al-adatfeldolgozók számára)
- távoli hozzáférés biztosítása (pl: támogatás nyújtásakor)
- EGT-n kívüli felhőben történő adattárolás

Ennek a felmérésére nem biztos, hogy korábban megfelelő figyelmet fordítottak.

2. lépés: Az adattovábbítási eszközök azonosítása

Az adatexportőrnek minden egyes EGT-n kívüli adattovábbítás esetében meg kell határoznia a megfelelő adattovábbítási eszközt (*transfer tool* - a GDPR V. fejezet alapján).

- Ha az adatokat „megfelelőnek” minősített országba továbbítják, vagy a GDPR 49. cikke szerint nem ismétlődő, korlátozott számú érintettre vonatkozó, „kivételes” adattovábbítás történik, akkor nincs szükség további teendőre.

- Ha az adatokat *Standard Contractual Clauses* (*SCC)* vagy *Binding Corporate Rules* (*BCR)* segítségével továbbítják, biztosítani kell, hogy a célországban az EU szabályozásával „lényegében megegyező” (*essentially equivalent*) védelmet kapjanak.

Meg kell vizsgálni, hogy a célország jogszabályai vagy gyakorlata hatással lehet-e az SCC vagy a BCR alkalmazására. Ezt a követelményt a GDPR nem tartalmazza!

3. lépés: A célország vizsgálata

Az EGT-n kívüli célország vonatkozásában négy fő alapelv teljesülését kell vizsgálni, és megfelelően dokumentálni az EEG Ajánlás alapján:

(i) Az adatkezelésnek világos, pontos és hozzáférhető szabályokon kell alapulnia

(ii) Bizonyítani kell az elérni kívánt jogszerű célok szükségességét és arányosságát.

(iii) A megfigyelési intézkedések megfelelőségét független fórum kell felügyelje.

(iv) Az érintettek hatékony jogorvoslati lehetőségekkel kell rendelkezzenek.

Kiknek a feladata ez tulajdonképpen?

4. lépés: kiegészítő védelmi intézkedések

- Ha az EEG Ajánlás alapján az adatexportőr megállapítja, hogy az adatokat nem illeti meg az EU szabályozásával „lényegében megegyező” védelem, kiegészítő védelmi intézkedésekben kell megállapodni az adatimportőrrel.

- Ezek szerződéses, technikai vagy szervezési jellegű intézkedések.

- Lehet, hogy a technikai intézkedések önmagukban elengendők (pl. titkosítás, álnevesítés, megosztott vagy több fél által végzett adatkezelés), hogy megakadályozzák az adatokhoz való hozzáférést az EGT-n kívüli célországban, különösen hatóságok részéről, illetve megfigyelési céllal.

A szerződéses vagy szervezési intézkedések jellege

Kiegészíthetik a technikai intézkedéseket - például előírhatják:

- konkrét technikai intézkedések alkalmazását
- a hatóságok általi adatokhoz való hozzáférés átláthatóságát
- „hátsó ajtók” és a titkosító kulcs átadásával kapcsolatos kötelezettségek tilalmát
- megerősített audit jogokat és érintetti jogokat
- haladéktalan tájékoztatási kötelezettséget az adathozzáférés megadása előtt
- un. "*warrant canary*" módszer alkalmazását
- kötelezettségvállalást az adatátadást elrendelő határozatok megtámadására

Csak kiegészítik a technikai intézkedéseket - fő szempont a titkosítás.

Vezetői összefoglaló az EDPB-től…

„Ha nem sikerül megfelelő kiegészítő intézkedést találni, például azért, mert az EGT-n kívüli célország tiltja vagy akadályozza az adott intézkedés alkalmazását, vagy az adatimportőr nem tudja az adott intézkedést alkalmazni, fel kell függeszteni, vagy le kell állítani az adattovábbítást.”

Vezetői összefoglaló egy adatvédelmes kollégától…

„Amúgy hogy a pékbe fogjuk / fogják ezt a cégek a gyakorlatban alkalmazni? Ez kvázi egy vagyoni census lesz: aki ki tudja fizetni az USA ügyvédet, aki mindezeket kideríti neki, az üzletelhet a Facebookkal, a Google-lel, a többi pedig lemarad, kimarad, nem tud USA szolgáltatást jogszerűen igénybe venni. Szerintem ez egyszerűen nem fair. Lehet, hogy én nem vagyok most eléggé érzékenyítve a személyes adataim védelmére, de ez nekem már túlzásnak tűnik és nem igazán forgolódok álmatlanul amiatt, hogy a Facebook milyen adatokat hol tárol rólam és hogy azokhoz hozzáfér-e az USA hírszerzés vagy sem.”

5. lépés: az SCC vagy a BCR kiegészítése

Az SCC és a BCR lényege: követhető, strukturált, egységes szöveg és szabályrendszer. Változás esetén egyszerű szerződésmódosítás elég volt - adminisztrációs teher?

Egyedi szerződések váltják fel az SCC rendelkezéseit.
Egyedileg kell megvizsgálni a célországot és az adatfeldolgozót.
Az SCC elveszíti „standard” jellegét.
„Country assessment” adatbázisok – milyen felelősségvállalás van mögötte?

Egy közepes méretű magyar cégnél hány szerződéses partner van?

6. lépés - az adattovábbítás megfelelőségi szintjének nyomonkövetése

Az adatexportőröknek folyamatosan és megfelelő időközönként (vagy jelentős változások esetén) ellenőriznünk kell, és újra kell értékelnünk az EGT-n kívüli országokba továbbított adatok védelmi szintjét, a fenti lépéseken keresztül.

Cookie megfelelés - hatósági gyakorlat az EU-ban

- A felhasználók hozzájárulása nélkül telepítettek hirdetési sütiket.
- Nem adtak egyértelmű tájékoztatást arról, hogyan használják a sütiket, és a felhasználók hogyan utasíthatják el azokat.
- Nem kérték a felhasználók hozzájárulását nem alapvető sütik telepítéséhez (Google Analytics)

A francia CNIL cookie iránymutatása (1)

Tájékoztatás: az adatkezelő(k) személye (saját és harmadik fél – link az adatkezelési tájékoztatójukra!) a sütik céljai (kétszintű tájékoztatás), a felhasználók hogyan járulhatnak hozzá vagy utasíthatják el a sütiket, a hozzájárulás visszavonásának joga, valamint a hozzájárulás vagy elutasítás következményei.

A felhasználók hozzájárulását **honlaponként** kell beszerezni.

Ugyanolyan egyszerű kell legyen a sütik használatának elfogadása vagy visszautasítása. Nem jogszerű, ha a felület kizárólag az „*összes elfogadása*” és a „*beállítások testreszabása*” gombokat tartalmazza, vagyis a felhasználók egyetlen kattintással elfogadhatják az összes sütit, de csak több kattintással utasíthatják vissza azokat.

Ha használják az „*összes elfogadása*” gombot, akkor azonos méretű és azonos szintű **„*összes elutasítása*” gomb** is kell legyen, illetve egyenként is lehessen válogatni.

Alternatíva: „***folytatás hozzájárulás nélkül***” link. A lényeg: a felhasználók számára egyértelműnek kell lennie, hogyan utasíthatják el a sütiket.

A francia CNIL cookie iránymutatása (2)

A felhasználók **hallgatását** úgy kell értelmezni, hogy elutasítják a sütik telepítését.

A hozzájárulást **6 havonta** meg kell újítani.

Önmagukban a „**sütifalak**” nem tilosak, de esetről-esetre kell őket értékelni, és a felhasználókat egyértelműen tájékoztatni kell választásaik következményeiről.

Például: ha nem jutnak át a „sütifalon”, nem tudnak hozzáférni a weboldal, alkalmazás vagy szolgáltatás tartalmához.

A francia CNIL cookie iránymutatása (3)

Nem kell hozzájárulás:

- a felhasználó választását rögzítő sütik (hogy hozzájárul-e a sütik használatához)
- hitelesítési célokra használt sütik
- a bevásárlókosár tartalmát tároló sütik
- a felület személyre szabásához használt sütik, ha ez a szolgáltatáshoz elengedhetetlen és elvárható (pl. nyelvválasztás)
- a szolgáltatást támogató eszközök terheléskiegyenlítéséhez szükséges sütik
- ingyenes tartalomhoz való szabad hozzáférés korlátozását szabályozó sütik (előre meghatározott mennyiség / korlátozott idő mérése)

A francia CNIL cookie iránymutatása (4)

A közönségmérő sütik szintén mentesülhetnek a hozzájárulás alól, ha elengedhetetlenek a weboldal vagy az alkalmazás megfelelő működéséhez, és a szolgáltatás nyújtásához.

Például:

- kizárólag az üzemeltető használja, a weboldal vagy az alkalmazás közönségének mérésére
- nem teszi lehetővé a felhasználó nyomon követését más alkalmazásokban vagy webhelyeken
- kizárólag anonim statisztikai adatok előállítására használják, más adatkezelési tevékenységekkel nem kapcsolják össze, harmadik feleknek nem továbbítják

- Időtartama legfeljebb 13 hónap (ez elegendő időt hagy az elemzésre).
- A közönségmérő sütik által gyűjtött adatokat legfeljebb 25 hónapig lehet tárolni.

Adatvédelmi teendők a közösségi média modulok alkalmazásával kapcsolatban – NAIH állásfoglalás (1)

1. **A honlap-üzemeltető minden olyan személyes adat tekintetében adatkezelő, amelynek a gyűjtésére és továbbítására a honlapjának a használata során kerül sor.**

   - Ide tartozik minden általa alkalmazott közösségi modul által kezelt adat is. Például: „tracking-pixel” beágyazása.
   - Közös adatkezelés a közösségi média szolgáltatóval.

2. **A közösségi modul alkalmazásához be kell szerezni az érintettek hozzájárulását.**

   - Az érintettek egyesével kell eldönthessék, hogy az adott típusú süti működéséhez hozzájárulnak-e vagy sem.
   - A szolgáltatásokhoz és funkcionalitásokhoz történő hozzáférésnek nem képezheti feltételét a felhasználó hozzájárulása.

Adatvédelmi teendők a közösségi média modulok alkalmazásával kapcsolatban – NAIH állásfoglalás (2)

A honlap-üzemeltetőknek:

- meg kell vizsgálniuk, hogy pontosan milyen adatok rögzítésével és továbbításával jár együtt egy-egy közösségi modul alkalmazása
- megfelelő adatkezelési tájékoztatót kell készíteniük a közösségi modul alkalmazásával kapcsolatban
- érvényes hozzájárulási lehetőséget kell biztosítani az érintett felhasználók számára a közösségi modul használatával kapcsolatban
- a közös adatkezelői minőségre tekintettel ellenőrizniük kell a közösségi média szolgáltató adatvédelmi feltételeit
- figyelemmel kell lenniük az EDPB közösségi média felhasználók célzásával kapcsolatos 8/2020 számú iránymutatás-tervezetének rendelkezéseire is

Beszélgetés