Dr. Domokos N. Márton:

Az EU új adatvédelmi szabályozása – avagy *„keep bangin' on the wall of Fortress Europe”*

I. AZ EU ADATVÉDELMI JOGÁNAK TELJES KÖRŰ REFORMJA

„People get ready it's time to wake up, tear down the walls of Fortress Europe” – szólít fel az Asian Dub Foundation zenekar. Ugyan az angol banda „*Enemy of the Enemy*” című albumának nyitószámában nem feltétlenül a hatályos európai adatvédelmi szabályozás hiányosságaira akarta felhívni a figyelmet, hanem a kontinens menekültügyi politikáját kritizálta, végső soron a „*Fortress Europe*” hozzáállás az, ami mostanra jóformán működésképtelenné tette az EU adatvédelmi szabályrendszerét is. A keményen politikus szövegű dal így remek háttérzene lehet, jogalkotóknak az EU új adatvédelmi jogszabályának véglegesítéséhez, adatkezelőknek pedig az új szabályokkal való megismerkedéshez és a megfelelésre való felkészülés megkezdéséhez – a jelen írás célja, hogy segítséget nyújtson ebben.

Az Európai Bizottság ugyanis 2012. január 25-én közzétette a jelenleg hatályos adatvédelmi irányelv (a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK Irányelv – a „**Hatályos Irányelv**”) helyébe lépő általános adatvédelmi rendeletének tervezetét (a „**Rendelettervezet**”). A Rendelettervezet radikális váltás az adatvédelem eddigi európai szabályozási irányában. Közzétételekor az adatvédelmi szakértők közül még kevesen fogadtak volna arra, hogy az új jogszabály nem csak adatvédelmi konferenciákon elemzett jogtörténeti érdekesség lesz, hanem érdemben megvitatásra kerül majd a tagországok és az egyéb érdekeltek (adatkezelők, jogalkalmazók, egyéb szakértők) között. Pedig 2012 folyamán pont az utóbbi történt: úgy tűnik, szabályozói, adatkezelői és fogyasztói oldalról egyaránt komoly igény van az EU adatvédelmi jogának reformjára.

Mi is a gond a Hatályos Irányelvvel?

- A jogszabály még az úgynevezett „második technológiai platformra” (PC és ügyfél/szerver struktúra) épült. Ma a komplex, digitalizált környezetben működő „harmadik platform” korát éljük[1] - a „*personal computer*” fogalmát felváltotta a „*personal computing*”: a személyes adatok kezelése *mobile computing* (mobil eszközök, okostelefonok, tárolóeszközök) és *cloud computing* (számítási felhő) technológiák alkalmazásával történik, nagyrészt virtuálisan, illetve a közösségi oldalak által biztosított nyilvános fórumokon, és az így kezelt, a felhasználók által folyamatosan megosztott, csak „*big data*”-ként emlegetett adatösszesség folyamatos elemzések tárgyát képezi.

- Ezzel egyidejűleg megjelentek az új adatbiztonsági fenyegetések: a *cybercrime* a Világgazdasági Fórum (*World Economic Forum*) szerint az 5 legnagyobb globális kockázat egyike[2], és csak az Egyesült Királyságban évente 27 milliárd angol font költséget okoz a gazdasági szereplőknek.[3] Új bűncselekménytípusok jelentek meg (*malware*, *phishing*, személyiséglopás (*identity theft*), *social engineering*), és ennek következtében szigorodtak a személyes adatokat tároló eszközök védelmére

[1] A platformváltás részletes elemzését lásd: **Dave Waterson: Security Challenges on the Third Platform**, http://dwaterson.com/2012/12/13/Security-Challenges-On-The-Third-Platform/

[2] **Global Risks 2012 Seventh Edition**, http://reports.weforum.org/global-risks-2012/

[3] **UK cyber crime costs £27bn a year - government report**, http://www.bbc.co.uk/news/uk-politics-12492309

vonatkozó gyakorlatok is: a munkahelyeken egyre elterjedtebbek a „*Bring Your Own Device – BYOD*", a „*Bring your Own Application – BYOA*", valamint a közösségi oldalak használatára irányadó szabályzatok. Specifikus hozzáférési technikák jelentek meg a *cloud computing*-gal összefüggésben, és egyéb innovatív azonosítási módszerek (pl. arcfelismerés, genetikai adatok felhasználása, biometrikus azonosítás) is mindennapossá válnak. (Az adatvédelmi kérdések trendjére egyébként jól lehet következtetni például a Facebook befektetései alapján: nemrég a Face.com nevű arcfelismerő technológiával foglalkozó céget vásárolták meg.) A *cybercrime* tekintetében különösen veszélyeztetettek az adatbiztonsági intézkedésekre kevesebbet költő kis- és középvállalkozások.

- További adatvédelmi jogi kihívásokat vet fel a különböző adatkezelők által kezelt adatok összekapcsolása: a mobiltelefon és a közösségi oldalak együttes használatával összefüggésben például helymeghatározási adatok kezelése, vagy a közösségi oldalon használt azonosítóknak az egyéb platformokon való – azonosítási célból történő használata. A legtöbb jelenlegi, innovatív üzleti modell is személyes adatok megosztásán, illetve személyre szabott tartalmak kínálatán alapul (pl. zenemegosztás közösségi oldalakon, a személyes adatnak minősülő felhasználói preferenciák jelzésével) – akár gyerekek számára is, mint a Disney „Magicbands" nevű, Disneylandbe látogatók számára kínált RFID-alapú megoldása[4].

- Új fogyasztóvédelmi kérdések is megjelentek: a célzott, az adatgazdák viselkedésén alapuló hirdetések jogi szabályozása, különösen az online azonosítók elhelyezésével és az azt blokkoló technológiákkal kapcsolatos viták (pl. a böngészők „*Do Not Track*" funkciójának alapértelmezésével, vagy a Robinson-listákhoz hasonló „*Tracking Protection List*" dokumentálási kötelezettséggel összefüggő viták).

- Az USA tagállamaiban, és ezáltal a globális piaci gyakorlatban alapvető fontosságúak lettek az adatbiztonsági értesítésekkel (*data security breach notification*) kapcsolatos jogszabályok és eljárások.[5]

- Külön adatvédelmi kérdéseket vetnek fel az új technológiák, például a mobilalkalmazások és elektronikus fizetési rendszerek adatgyűjtése, a közműcégek által kínált új megoldásokkal járó adatkezelés (*smart metering, smart grid*), valamint a személyre szabott egészségügyi és az *e-health* megoldások és általánosságban az egészségügyi adatok mindennapos kezelése[6].

- Új jelenség az „*Internet of Things*" (emberi beavatkozás nélküli adatmegosztás vezeték nélkül összekapcsolt eszközök között – 2015-re mintegy 25 milliárd ilyen eszköz lesz világszerte), melynek adatvédelmi és adatbiztonsági vonatkozásaival kapcsolatban az EU Bizottság 2012. április 12-én indított nyilvános konzultációt, és "*Machine-to-Machine Communication: Connecting Billions of Devices*" címmel hasonló kutatást végzett a Gazdasági Együttműködési és Fejlesztési Szervezet (*Organisation for Economic and Co-operative Development - OECD*) is. Ennek a jelenségnek már egy specifikusabb változata lesz a jövőben például az „*Internet of Cars*", ahol kiemelt szerepet kap a helymeghatározási személyes

[4] **Mickey Mouse Isn't Planning To Invade Kids' Privacy, Says Disney's Offended CEO,**
http://www.forbes.com/sites/kashmirhill/2013/01/29/mickey-mouse-isnt-planning-to-invade-kids-privacy-says-disneys-offended-ceo/

[5] Lásd még a Ponemon Institute elemzését: **Ponemon Study Shows the Cost of a Data Breach Continues to Increase**, http://www.ponemon.org/news-2/23

[6] Az USA-ban ezt részletes szektorspecifikus törvényekkel szabályozzák – HIPAA, HITECH Act

adatok kezelése[7], valamint a „pervasive computing", ahol maga az alkalmazás találja meg az adatgazdát.[8]

- Fontos azt is látni, hogy a hatályos jogszabályok alapján nincsenek „*one size fits all*" adatvédelmi megoldások – egyre gyakoribb, hogy az adatkezelők egyedi adatvédelmi hatásvizsgálatot (*privacy impact assessment)* végeznek a specifikusabb adatkezeléseik tekintetében.

- A nemzetközi szintű adattovábbítások, kormányzati adatkérések[9] szintén mindennapossá váltak, és ezáltal az adattovábbítással kapcsolatos jogszabályok is egyre inkább extraterritoriális jellegűek: az utóbbi idők legjellemzőbb példája az amerikai *Foreign Account Tax Compliance Act* (*FATCA*) elnevezésű új adójogi szabályozás. A FATCA szabályainak elviekben a Magyarországon működő pénzügyi intézményeknek is meg kell felelniük. A FATCA segítségével az amerikai adóhatóság (*Internal Revenue Service – IRS*) ellenőrizni tudja a nem amerikai pénzügyi szervezeteknél vezetett számlák amerikai tulajdonosait, annak érdekében, hogy az USA területén kívül szerzett, de az USA-ban be nem jelentett jövedelmeik után is megfizessék az USA-ban esedékes adóterhet. A FATCA hatálya nem csak az USA területére terjed ki, hanem közvetlen adatkezelési- és továbbítási kötelezettségeket határoz meg az USA-beli személyek számláit, szerződéseit kezelő pénzügyi intézmények számára is.

Az adatvédelmi kérdések tehát egyre összetettebbek, így mind az adatkezelők, mind az adatgazdák számára fontos, hogy megfelelő szabályozás alapján működhessenek. Ennek alapján egyértelmű, hogy az EU-ban az adatvédelmi jog reformjára hatékonyabb szabályozási forma a tagállamokban automatikusan, közvetlenül alkalmazható rendelet, mint a különböző nemzeti jogszabályokat harmonizáló, de végső soron nem egységesen átültetett irányelv. A Rendelettervezet elfogadása így nagyobb jogbiztonságot jelent az érintettek számára – és még így is biztosan lesznek eltérő tagállami értelmezések az alkalmazásával kapcsolatban. A Rendelettervezet elfogadásával megvalósuló egységes EU-szintű szabályozás célja az adatkezelési eljárások, a nyilvántartási kötelezettségek, és a határon átnyúló tevékenységet folytató adatkezelők tevékenységének egyszerűsítése, valamint az érintett személyek és a felügyelő hatóságok jogainak erősítése. A Hatályos Irányelv által bevezetett koncepciók és alapelvek nagyrészt hatályban maradnak, ugyanakkor több, jelenleg használt definíció is pontosításra, illetve szigorításra kerül (különös tekintettel a hozzájárulás fogalmára), új meghatározások jelennek meg (például profilozás), részletezésre kerülnek a harmadik országokba történő adattovábbítás feltételei, valamint új kötelezettségek terhelik majd az adatkezelőket és adatfeldolgozókat (pl. adatvédelmi felelős kötelező kinevezése, adatbiztonsági értesítések, széles körű dokumentációs kötelezettségek). Jelentősen növekednek az adatvédelmi hatóságok szankcionálási jogai. Ami a legfontosabb: ha a Rendelettervezet megközelítőleg a jelenlegi formájában elfogadásra kerül, az adatkezelőknek jelentős szervezeti és dokumentációs változásokat kell bevezetni, és az adatvédelmi hatóságok működési módja is lényeges módosulásokon eshet át.

A jelen írás célja, hogy bemutassa a Rendelettervezet legfontosabb rendelkezéseit és az egyes pontok végén a Rendelettervezet javasolt szövegének elfogadása esetén az érintettek

[7] **Forget the Internet of Things: Here Comes the Internet of Cars**, http://www.wired.com/opinion/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars/

[8] http://www.pwc.com/us/whatisyourdigitaliq

[9] Egy statisztika erről: **U.S. leads the world in requests for users' Google data** http://news.cnet.com/8301-1009_3-57565385-83/u.s-leads-the-world-in-requests-for-users-google-data/

számára várható gyakorlati következményeket.[10] Fontos megemlíteni, hogy az Európai Bizottság mellett működő független európai adatvédelmi tanácsadó szerv, a 29-es Munkacsoport már két alkalommal: 2012. március 23-án (*A 29-es Munkacsoport 2012/1. sz. véleménye az adatvédelmi reformjavaslatokról*), valamint 2012. október 5-én véleményezte a Rendelettervezetet. A jelen írásban főleg az első véleményre hivatkozunk, a „**29-es Munkacsoport Véleménye**" megnevezéssel. Szintén hasznos észrevételeket tartalmaz az angol adatvédelmi hatóságnak (*Information Commissioner's Office* – „**ICO**") a Rendelettervezettel kapcsolatos véleménye (a jelen írásban: „**ICO Vélemény**") is.[11] Legújabb fejlemény, hogy a Rendelettervezetet az Európai Parlament – állampolgári jogok, bel- és igazságügy (*LIBE*), rapportőr: Jan Philipp Albrecht - is észrevételezte, és az előzetes várakozásokra rácáfolva módosítási javaslataival („**EP Javaslat**") nemhogy „felhígította", hanem még szigorítaná rendelkezéseit.[12]

II. FŐBB ÚJDONSÁGOK A RENDELETTERVEZETBEN

1. Kiterjesztett területi hatály, uniós képviselő

1.1 Kiterjesztett területi hatály

A Rendelettervezetet alapvetően az EU-ban letelepedett adatkezelők és adatfeldolgozók tevékenységére kell alkalmazni, viszont fontos, a Hatályos Irányelven túlmutató célkitűzése a Rendelettervezetnek, hogy hatálya kiterjed „*a nem az EU-ban letelepedett adatkezelő által végzett adatkezelési tevékenységekre, feltéve, ha az termékeknek vagy szolgáltatásoknak az EU-ban lakóhellyel rendelkező érintett személyek számára való nyújtásához, vagy viselkedésük nyomon követéséhez kapcsolódik*".[13]

A kiterjesztett területi hatály kifejezett célja, hogy kötelezze a nem az EU-ban letelepedett adatkezelőket – tipikusan ilyenek a közösségi oldalak vagy az e-kereskedelemmel foglalkozó szolgáltatók – az EU-s szabályoknak való megfelelésre. Kérdés azonban, hogy a gyakorlatban hogyan valósítható meg a jogszabály rendelkezéseinek kikényszerítése a nem az EU-ban letelepedett adatkezelőkkel szemben - ehhez részletesen kidolgozott szabályrendszeren alapuló, határon átnyúló együttműködés szükséges a felügyelő hatóságok között, jelentős emberi és anyagi erőforrások bevonásával. Ennek hiányában az EU-s jogszabályoknak való megfelelés a nem az EU-ban letelepedett adatkezelők számára csak ajánlás, „legjobb gyakorlat" marad. Az ICO Vélemény a rendelkezés végrehajtásával kapcsolatos problémát az adatgazdák szemszögéből vizsgálja: eszerint a Rendelettervezet nem ígérhet olyan jogi védelmet az EU-ban lakóhellyel rendelkező érintett személyek számára, amit a valóságban nem tud biztosítani.

A Rendelettervezet véglegesítése során a szabályok megfelelő értelmezése és végrehajtása érdekében pontosan definiálni szükséges a „*termékek vagy szolgáltatások nyújtása*" és a „*viselkedés nyomon követése*" fogalmakat – ide tartozik-e például egy EU-n kívülről üzemeltetett egyszerű weboldal? Az EP Javaslata szerint a Rendelettervezet hatálya alá tartoznának majd az EU-n kívülről nyújtott ingyenes szolgáltatások (például

[10] A jelen írásban a Rendelettervezet nyilvánosan hozzáférhető magyar fordításának szövegezését idézzük – külön jeleztük, ha módosítottunk a fordításon. A „data processor" szó fordításaként viszont a Rendelettervezet fordításával ellentétben inkább a hatályos magyar szabályozás által használt „adatkezelő" fogalmat alkalmazzuk. Még ha a magyar definíció nem is felel meg a Hatályos Irányelv fogalomrendszerének, a gyakorlatban ez terjedt el, míg a „data processor" pontosabb, „adatfeldolgozó" elnevezése a magyar jogban egy szűkebb, a Hatályos Irányelv által nem ismert (és ésszerűtlen) fogalmat jelent. Ugyanígy, az „adatvédelmi tisztviselőt" is „adatvédelmi felelősnek" nevezzük.

[11] Az ICO szerepéről és a jogszabályalkotás folyamatáról: ICO blog: EU data protection reforms: how the process works, and what the ICO is doing http://www.ico.gov.uk/news/blog/2013/eu-data-protection-reforms-how-the-process-works-and-what-the-ICO-is-doing.aspx?goback=.gde_3204418_member_209486720

[12] **Draft Report**, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[13] Rendelettervezet 3. cikk

keresőprogramok), valamint nem csak a felhasználók viselkedésének nyomon követése, hanem az adataikkal kapcsolatos általános, EU-n kívül végzett adatkezelési tevékenységek is. A definíciók pontosítását, valamint a Rendelettervezet hatályának a viselkedés nyomon követéséhez kapcsolódó egyes adatfeldolgozási tevékenységekre való kiterjesztését szorgalmazza a 29-es Munkacsoport Véleménye is.

Várható következmény: széles körű hatály, és megfelelési kötelezettség az EU-n kívüli adatkezelőknek – jelentős *compliance* költségek az ilyen adatkezelők számára, ugyanakkor az EU-s jogszabályok hatékonyabb végrehajtása velük szemben.

1.2 Uniós képviselő kijelölése[14]

A nem az Unió területén letelepedett adatkezelők kötelesek uniós képviselőt kijelölni. E kötelezettséget nem kell alkalmazni a következő esetekben:

„*a) ha a Bizottság úgy határozott, hogy a harmadik ország „megfelelő védelmi szintet" biztosít; vagy*

b) a 250 főnél kevesebb főt foglalkoztató vállalkozásra; vagy

c) állami hatóságra vagy szervre; vagy

d) az Unióban lakóhellyel rendelkező érintetteknek csak alkalmi jelleggel termékeket és szolgáltatásokat kínáló adatkezelőre."

Az uniós képviselő kijelölésével kapcsolatban a Rendelettervezet további két fontos rendelkezést tartalmaz:

- „*A képviselőnek azon tagállamok egyikében kell székhellyel/lakóhellyel rendelkeznie, ahol azon érintettek lakóhelye található, akiknek a személyes adatait a termékek vagy szolgáltatások nyújtása keretében kezelik, vagy akiknek a viselkedését nyomon követik.*"

- „*A képviselő adatkezelő általi kijelölése nem érinti a magával az adatkezelővel szembeni keresetindításhoz való jogot.*"

A Rendelettervezet a képviselő funkciójával kapcsolatban nem tartalmaz további részletes rendelkezéseket, ugyanakkor a képviselő kijelölésének elmulasztása a legmagasabb bírság kiszabását vonhatja maga után, illetve ha az adatkezelő rendelkezik képviselővel, a szankciókat a képviselővel szemben kell alkalmazni (az adatkezelővel szemben alkalmazható szankciók sérelme nélkül).[15] A 29-es Munkacsoport Véleménye erre tekintettel kiemeli, hogy jobban kell tisztázni a képviselő szerepét, feladatkörét, kötelezettségeit és felelősségét, a 29-es Munkacsoport továbbá nem tartja indokoltnak a megfelelő szintű védelmet biztosító harmadik országbeli adatkezelő kijelölési kötelezettség alóli mentesítését. A 29-es Munkacsoport bírálta továbbá a „*csak alkalmi jelleggel termékeket és szolgáltatásokat kínáló adatkezelők"* meghatározásának bizonytalanságát, valamint a foglalkoztatottak létszámára tekintettel való mentesülést, mert kisméretű szervezetek is végezhetnek az egyének számára kockázatokat jelentő adatkezelést (ez az úgynevezett „kockázatalapú megközelítés" (*risk-based approach*). Az utóbbi megközelítést osztja az EP Javaslat is, amely 500-nál kevesebb személy (évi szinten történő) személyes adatának kezelése esetén adna mentesülést a kinevezési kötelezettség alól.

[14] Rendelettervezet 25. cikk

[15] Rendelettervezet 78. cikk (2)

Várható következmény: mint az előbb - jelentős *compliance* költségek az EU-n kívüli adatkezelők számára, ugyanakkor az EU-s jogszabályok hatékonyabb végrehajtása velük szemben.

2. Az „érintett személy" és a „személyes adat" meghatározása

A Rendelettervezet az „érintett személy" fogalmát a következőképpen határozza meg: „*azonosított vagy közvetlen vagy közvetett módon az adatkezelő vagy más természetes vagy jogi személy által ésszerű módon – különösen egy azonosító számra, tartózkodási információra, online azonosító jelekre vagy a személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén – azonosítható természetes személy*"[16]. „Személyes adat" pedig „*az érintettre vonatkozó valamely információ*".[17]

A Hatályos Irányelvhez hasonlóan a Rendelettervezet sem tartalmazza a személyes adatok részletes meghatározását. A „személyes adatok" definiálása általános szinten történik, és csak az egyes adatvédelmi hatóságok iránymutatása segíthet eldönteni, hogy egy bizonyos információ személyes adatnak minősül-e. Ezzel szemben az USA-ban majdnem minden tagállam jogszabálya tartalmaz példákat, vagy kifejezett felsorolást a személyes adatok tekintetében. Ez a megközelítés több segítséget nyújthat az adatkezelők számára – a személyes adatokat kezelő nem-jogász munkatársaik ugyanis nem biztos, hogy esetről-esetre értelmezni tudják az adatvédelmi jogszabályok általános meghatározásait. A jogszabályokkal és gyakorlati alkalmazásukkal kapcsolatos részletes oktatás hiányában így nem tudják megállapítani azt sem, hogy valamely információ a jogszabály által védett személyes adatnak minősül-e.

Fontos lenne például tisztázni a Rendelettervezet véglegesítése során, hogy mit jelent pontosan az „online azonosító jelek" fogalma. Jelenleg nincs EU-s szinten egységes jogi szabályozás – csak az egyes tagállami hatóságok, valamint a 29-es Munkacsoport ajánlásai - arra nézve, hogy például az IP címek, online azonosítók vagy a cookie-k személyes adatnak minősülnek-e[18], illetve milyen kiegészítő feltételek (pl. egyéb azonosító információk) szükségesek ahhoz, hogy személyes adatnak minősüljenek. Ez jelentős nehézséget okoz a több EU országban működő adatkezelők számára, és egyelőre a Rendelettervezet sem ad megfelelő választ erre a létező problémára. A Rendelettervezetet észrevételező fórumok sem adnak ezzel kapcsolatban konkrét, gyakorlatias javaslatot, és az EP Javaslat is csak szélesíti a „személyes adat" fogalmának meghatározását. A ICO Véleménye szerint a definíciót esetleg oly módon kellene módosítani, hogy személyes adatnak minősül az online azonosító jel, ha kezelésének célja valamely tartalom célzott eljuttatása az adatgazda számára, vagy az adatgazdák egymástól való megkülönböztetése (bár véleményünk szerint az utóbbi feltétel is elég tág, a gyakorlatban nehezen értelmezhető fogalom). Ennél szigorúbb megközelítést javasol viszont a 29-es Munkacsoport Véleménye, amely módosítaná a Rendelettervezet (24)-es preambulumbekezdésének azt a megállapítását, miszerint „*az azonosítószámokat, tartózkodási helyre utaló adatokat, online azonosítókat vagy egyéb sajátos tényezőket nem szükségképpen kell minden körülmények között személyes adatnak tekinteni*".

Az USA egyes tagállamaiban nem illeti meg a személyes adatoknak járó védelem a „széles körben terjesztett" személyes adatokat. Az EU-ban egy hasonló megközelítés az egyes

[16] Rendelettervezet 4. cikk (1)

[17] Rendelettervezet 4. cikk (3)

[18] Érdemes arra is figyelni, hogy a cookie-k mellett más, és egyre hatékonyabb online nyomkövető eszközök léteznek. Hasznos tanulmány a témában: **Behavioral Advertising: The Offer You Cannot Refuse**, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601

országok kulturális sajátosságaitól és gyakorlatától függhet. Mindazonáltal a „széles körben terjesztett" személyes adatoknak az általánostól eltérő kezelése az egyes európai tagállamok számára megfontolandó lehet (különös tekintettel egyes személyes adatok széles körű hozzáférhetőségére, pl. a médiában vagy közösségi oldalakon). A kérdés már csak azért is érdekes, mert 2010 júliusában[19] a Skull Security biztonságtechnikai cég egyik munkatársa a nyilvánosan hozzáférhető Facebook profilokból (és a kapcsolódó személyes adatokból) összeállított adatbázist tett hozzáférhetővé az interneten, rávilágítva ezzel, hogy a felhasználók milyen könnyelműen osztják meg személyes adataikat a nyilvánossággal. Nemrég pedig a British Airways jelentette be, hogy a személyre szabott szolgáltatások nyújtása érdekében az utasokkal kapcsolatban végzett internetes kereséseket használna fel.[20] Magyarországon sem kell megtéríteni a kárt a személyes adatok jogellenes kezelésével kapcsolatban, ha az a károsult súlyosan gondatlan magatartásából származott - az Adatvédelmi Biztos is kiemelte többek között a magyar (új) adatvédelmi törvény előzetes észrevételezése során, hogy ez esetleg a közösségi oldalakon adataikat meggondolatlanul nyilvánosságra hozó felhasználóira is vonatkoztatható.[21] Álláspontunk szerint is indokolt lehet, hogy az adatkezelőnek lehetősége legyen mentesülnie felelőssége alól, ha az adatgazda maga hozta nyilvánosságra korábban azt az adatot, amivel kapcsolatban később visszaélés történt. Az internethasználat, különösen a közösségi oldalak elterjedtségére tekintettel ma már a felhasználóktól is elvárható lehet egy bizonyos minimális adatbiztonsági és adatvédelmi ismeret, különös tekintettel arra, hogy ne hozzák nyilvánosságra, ne osszák meg indokolatlanul személyes adataikat – ha mégis így döntenek, akkor viszont csak indokolt esetben háríthassák a felelősséget harmadik személyre.

Várható következmény: az adatgazdák fokozottabb ellenőrzési joga az adataik tekintetében, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára, mivel a korábbinál szélesebb körű adat tekintetében kell biztosítaniuk a jogszabályi megfelelőséget.

3. A „biometrikus adatok" fogalma

Új elem a Hatályos Irányelvhez képest a „biometrikus adat" fogalmának meghatározása, amely „*az egyén olyan fizikai, pszichológiai vagy viselkedési jellemzőjére vonatkozó adat, amely lehetővé teszi az egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat*"[22]. A 29-es Munkacsoport Véleménye szigorítaná a definíciót, mert a biometrikus adatokat nem csak azonosítás, hanem például tényleges azonosítás nélkül, a személyazonosság hitelesítése céljából is felhasználásra kerülhetnek.

A biometrikus adatok gyűjtésével kapcsolatos adatvédelmi kérdések vizsgálata egyébként világszerte aktuális: az USA-ban közös „fehér könyvet" bocsátott ki az *Immigration Policy Center* és az *Electronic Frontier Foundation* (*EFF*) (felmerült kérdések: ujjlenyomat-vételi és arcfelismerési technológiák, mobileszközök használata, bűnüldözési, bevándorlási és nemzetbiztonsági adatbázisok összekapcsolása, az adatbázisok kibővítése retinaszkenneléssel, DNS profilozással, tenyérlenyomatokkal)[23], de az arcfelismerési technológiák adatvédelmi vonatkozásairól bocsátott ki ajánlást az amerikai *Federal Trade Commission* (*FTC*) [24] is, a Facebook vonatkozó gyakorlatát pedig az ír adatvédelmi hatóság és német bíróságok is vizsgálták – és az EU hatályos adatvédelmi szabályaival ellentétesnek

[19] **Facebook Hacking, Security, and Privacy Concerns**, https://www.infosecisland.com/blogview/9361-Facebook-Hacking-Security-and-Privacy-Concerns.html; **Százmillió Facebook-felhasználó adatai kerültek ki a netre**, http://index.hu/tech/net/2010/07/29/100_millio_facebook-felhasznalo_adatai_kerultek_ki_a_netre/

[20] **British Airways to Google Passengers**, http://news.cnet.com/8301-17852_3-57467878-71/british-airways-to-google-passengers/

[21] Ügyszám: ABI-1788-2/2011/J, http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2011&dok=1788_J_2011-2

[22] Rendelettervezet 4. cikk (11)

[23] **From Finger Prints to DNA**, http://www.immigrationpolicy.org/sites/default/files/docs/Lynch%20-%20Executive%20Summary.pdf

[24] **FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies**, http://www.ftc.gov/opa/2012/10/facialrecognition.shtm

találták, így a szolgáltatónak módosítani kellett az alkalmazás európai megvalósítási módján.

4. Az „érintett hozzájárulásának" meghatározása

A Rendelettervezet a Hatályos Irányelv hozzájárulás-fogalmát a következők szerint szigorítja: hozzájárulás „*az érintett akaratának önkéntes, tájékozott és kifejezett kinyilvánítása nyilatkozat vagy egyértelmű megerősítő cselekedet alapján, amellyel az érintett beleegyezését adja az őt érintő személyes adatok kezeléséhez*". A legfontosabb újítás, hogy a hozzájárulásnak „*kifejezettnek*" kell lennie. Ez a megközelítés az európai adatvédelmi gyakorlatban folyamatos viták tárgya, különösen az online környezetben végzett adatkezelések során kért, illetve a cookie-k elhelyezéséhez a 2002. július 12-i 2002/58/EK Irányelv („**e-Privacy Irányelv**") 5. (3) alapján szükséges hozzájárulások módjával kapcsolatban. A kérdés a Rendelettervezettel kapcsolatban is változatlan: milyen megoldásokkal lehet biztosítani a „kifejezett" hozzájárulás beszerzését, úgy, hogy a jogszabályi megfelelés is biztosítva legyen, de az érintett személyek számára is könnyen használható, felhasználói élményüket nem romboló lehetőség álljon rendelkezésre?

A Hatályos Irányelvhez hasonlóan a bizonyítási terhet a Rendelettervezet is az adatkezelőre telepíti: rá hárul annak bizonyítása, hogy „*az érintett hozzájárult személyes adatainak konkrét célokból történő kezeléséhez*".[25] Ugyanígy megmarad az érintett személy joga, hogy hozzájárulását bármikor visszavonja; ez nem érinti azonban a visszavonás előtti hozzájáruláson alapuló adatkezelés jogszerűségét.[26]

A Rendelettervezet előírja továbbá, hogy ha a hozzájárulást valamely más ügyre is vonatkozó írásos nyilatkozattal összefüggésben kell megadni, „*a hozzájárulás kérésének megjelenésében megkülönböztethetőnek kell lennie ettől a más ügytől*"[27] – ez főleg az általános adatkezelési feltételek elfogadásába „rejtett" direkt marketing célú adatkezeléshez való hozzájárulások jogszerűségét érintheti, de az új rendelkezés alapján érdemes lehet az általános szerződési feltételekben szereplő adatvédelmi rendelkezéseket is külön hangsúlyozni.

A hozzájárulás feltételeivel kapcsolatban a Rendelettervezet rögzíti, hogy a hozzájárulás nem teremt jogalapot az adatkezelésre, ha „*jelentős egyenlőtlenség*"[28] áll fenn az érintett és az adatkezelő helyzete között. A gyakorlatban vélhetően ilyen lehet például a munkáltató-munkavállaló közötti viszony, vagy a vállalkozás-fogyasztó viszony, viszont megfelelően részletezni kellene a Rendelettervezet véglegesítése során, hogy pontosan milyen esetkörökben alkalmazandó ez a kivétel. Az egyes tagállamok eltérő adatvédelmi kultúrája miatt ugyanis fennáll a veszélye, hogy a különböző tagállami értelmezések jogbizonytalansághoz, és ezzel végső soron a Rendelettervezet céljának meghiúsulásához vezetnek.

Várható következmény: az adatgazdák fokozottabb ellenőrzési joga az adatkezeléssel kapcsolatban, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára, mivel a korábbinál szélesebb körben kell kifejezett hozzájárulást beszerezni és archiválni, valamint sokszor esetről-esetre kell vizsgálni a hozzájárulás jogszerűségét.

[25] Rendelettervezet 7. cikk (1)
[26] Rendelettervezet 7. cikk (3)
[27] Rendelettervezet 7. cikk (2)
[28] Rendelettervezet 7. cikk (4)

5. A „fő szervezet" fogalma - „*one-stop-shop*"

Fontos újítása a Rendelettervezetnek a Hatályos Irányelvhez képest a „fő szervezet" fogalmának bevezetése, mely a következőt jelenti: „*az adatkezelő vonatkozásában a letelepedés azon helye az Unióban, ahol a személyes adatok kezelésének céljaira, feltételeire és módjaira vonatkozó fő döntéseket meghozzák; amennyiben a személyes adatok kezelésének céljaira, feltételeire és módjaira vonatkozó fő döntéseket nem az Unióban hozzák meg, a fő szervezet az a hely, ahol az Unióban létrehozott adatkezelő tevékenységeivel összefüggésben a fő adatkezelési tevékenységeket végzik. A feldolgozó vonatkozásában a „fő szervezet" a központi ügyvezetés helye az Unióban*".

A Rendelettervezet szerint a „fő szervezet" azonosítása a több tagállamban működő adatkezelők esetében illetékes adatvédelmi hatóság megállapítása céljából elsődleges. Eszerint „*ha a személyes adatok kezelésére az EU-ban létrehozott adatkezelő vagy - feldolgozó tevékenységeivel összefüggésben kerül sor, és az adatkezelő vagy - feldolgozó egynél több tagállamban telepedett le, az adatkezelő vagy -feldolgozó minden tagállamban végzett tevékenységének felügyeletére az adatkezelő vagy -feldolgozó fő szervezete szerinti felügyelő hatóság lesz illetékes*.[29]

A cél tehát, hogy egy adatkezelő tevékenységével kapcsolatban alapvetően egy EU ország adatvédelmi hatósága legyen illetékes („*one-stop-shop*"). A szabályozási irány előremutató, a gyakorlatban azonban számos adatkezelő akad majd, akiknél nehéz lesz megállapítani a „fő szervezet" helyét a Rendelettervezet szövegezése alapján. A „*fő döntések*" meghozatalára, illetve a „*fő adakezelési tevékenységek*" elvégzésére ugyanis nemzetközi cégcsoportok esetén nem feltétlenül csak egy országban kerül sor. A 29-es Munkacsoport Véleménye is azt javasolja, hogy a Rendelettervezet véglegesítése során kerüljön jobban tisztázásra a „*fő szervezet*" fogalma és a többi adatvédelmi hatóság illetékességére gyakorolt hatása. Rögzíti továbbá a 29-es Munkacsoport Véleménye, hogy a „*one-stop-shop*" alapelve ne legyen alkalmazható a nem az EU-ban letelepedett adatkezelő által végzett adatkezelési tevékenységekre, ha az termékeknek vagy szolgáltatásoknak az EU-ban lakóhellyel rendelkező érintett személyek számára való nyújtásához, vagy viselkedésük nyomon követéséhez kapcsolódik – ebben az esetben bármely adatvédelmi hatóság járhasson el, amelynek tagállama érintett. A Rendelettervezet ugyanakkor nem szabályozza, hogy ilyen esetekben melyik a „vezető hatóság".

A „*one-stop-shop*" által elért adminisztrációs előnyök mellett azonban még mindig hiányzik a Rendelettervezetből, hogy támogassa azt a koncepciót, miszerint cégcsoport is minősülhet egy adatkezelőnek („*the missing group privilige*" - ahogy Cornelia Sasse és Brad Bryant, az Aon Group adatvédelmi szakértői nevezték egy konferencián) – a multinacionális vállalatok működését és jogszabályi megfelelőségét pedig jelentősen megkönnyítené egy ilyen megközelítés.

Várható következmény: a jogszabályok hatékonyabb végrehajtása európai szinten, ugyanakkor gyakorlati nehézségek a több országban működő adatkezelők számára a „fő szervezet" helyének megállapításával kapcsolatban.

[29] Rendelettervezet 51. cikk (2)

6. Új adatkezelési alapelv - adatminimalizáció

A Rendelettervezet egyrészről megismétli és pontosítja a Hatályos Irányelv által meghatározott adatkezelési alapelveket: az adatkezelésnek jogszerűnek, tisztességesnek, és az érintett számára átláthatónak kell lennie, továbbá adatkezelésre csak meghatározott, egyértelmű és törvényes célból kerülhet sor, pontos és naprakész adatok igénybevételével.

Ezen túlmenően új megközelítés az „adatminimalizációval" kapcsolatos alapelvek bevezetése. Ennek értelmében a személyes adatok „*megfelelőek, relevánsak, és nem haladják meg a kezelés céljához szükséges legkisebb mértéket, és csak akkor és addig dolgozhatók fel, amikor és ameddig e célok nem érhetők el olyan információ kezelésével, amely nem vonatkozik személyes adatokra*, valamint „*tárolásuknak olyan formában kell történnie, amely az érintettek azonosítását csak az adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé*"[30].

A 29-es Munkacsoport Véleménye tovább szigorítaná az adatkezelési alapelveket: a fentieken túlmenően olyan általános kötelezettség bevezetését javasolja, amely szerint ha az adatkezelés céljára figyelemmel megvalósítható és arányos, a személyes adatokat névtelenné vagy személytelenné kell tenni. Ugyan a gyakorlatban számos cég alkalmaz ilyen anonimizációs eljárást, véleményünk szerint ésszerűtlenül hátrányos kötelezettség lenne ezt jogszabályi szinten kötelezővé tenni.

Specifikus adatmegőrzési időket a Hatályos Irányelvhez hasonlóan a Rendelettervezet sem tartalmaz. Az egyes tagállamok eltérő adatvédelmi szabályozása miatt a több tagállamban működő cégek számára eltérő adatmegőrzési kötelezettségek irányadók – ez már a Hatályos Irányelv alapján sem túl ésszerű sajátosság, és hátráltathatja az egységes Uniós adatvédelmi szabályozás megvalósítását, és növeli a több tagállamban működő cégek adminisztrációs terheit. Célszerű lehet tehát az adatmegőrzési idők EU-s szintű egységesítése, bár a Rendelettervezetnek sajnos úgy tűnik ez nem volt célja.

Várható következmény: az adatgazdák fokozottabb védelme a kezelt adatmennyiség csökkentésével, ugyanakkor jelentős IT költség az adatkezelők számára az adatminimalizációhoz szükséges technikai intézkedések során.

7. Az adatkezelés jogszerűsége hozzájárulás nélkül

A „hozzájárulás" fogalmának megerősítése mellett bevezetésre kerülnek egyéb, hozzájárulás nélkül történő adatkezelést lehetővé tevő jogalapok is. A Hatályos Irányelv rendelkezéseinek nagy részét megtartva a Rendelettervezet tételesen felsorolja azokat az eseteket, amikor az adatkezelés jogszerű. Ezek az esetek a következők:[31]

(a) „*az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;*

(b) *az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;*

(c) *az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;*

(d) *az adatkezelés az érintett létfontosságú érdekének védelme miatt szükséges;*

[30] Rendelettervezet 5. cikk. Specifikus rendelkezések irányadók a kizárólag történelmi, statisztikai vagy tudományos kutatási célból kezelt adatokra.

[31] Rendelettervezet 6. cikk (1)

(e) *az adatkezelés közérdekű feladat végrehajtásához vagy az adatkezelőre ruházott hivatali hatáskör gyakorlásához szükséges;*

(f) *az adatkezelés az adatkezelő jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.*"

A Rendelettervezet szerint[32] a jogi kötelezettség teljesítéséhez, illetve a közérdekű feladat végrehajtásához és hivatali hatáskör gyakorlásához szükséges adatkezelés jogalapjáról uniós vagy tagállami jogszabályban kell rendelkezni. Ennek alapján várható, hogy a hatályos tagállami jogszabályokat széles körben módosítani kell a vonatkozó adatvédelmi szabályokkal – például számos jogszabály Magyarországon sem tartalmaz ilyen rendelkezéseket.

A fenti kivételek ugyanakkor nem elég specifikusak - megfelelően részletezni kellene a Rendelettervezet véglegesítése során, hogy pontosan milyen esetkörökben nem szükséges hozzájárulás. Nem egyértelmű, hogy ide tartoznak-e például a *compliance* jellegű, visszaélés-bejelentési vagy –felderítési, és pénzmosás-megelőzési (*AML*) célú adattovábbítások. Az egyes tagállamok eltérő adatvédelmi kultúrája miatt ugyanis fennáll a veszélye, hogy a különböző tagállami értelmezések jogbizonytalansághoz, és ezzel végső soron a Rendelettervezet céljának meghiúsulásához vezetnek. Szintén problémákat okozhat a gyakorlatban az EP Javaslat azon megoldása, amely a hozzájárulás nélkül történő adatkezelést egyébként kivételes esetekre korlátozná, és ezen túlmenően előírná az érintett személyek külön tájékoztatását, és az adatkezelés hozzájárulás alóli mentesülésének indokolását.

Várható következmény: az adatgazdák fokozottabb ellenőrzési joga az adatkezeléssel kapcsolatban, ugyanakkor jelentős *compliance* költség az adatkezelők számára, mivel esetről-esetre kell vizsgálni a hozzájárulás nélküli adatkezelés jogszerűségét.

8. Gyermekek személyes adatainak kezelése

A Rendelettervezet szerint „*a közvetlenül gyermekeknek nyújtott információs társadalommal összefüggő szolgáltatásokkal összefüggésben a 13 év alatti gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a gyermek szülője vagy gyámja ahhoz hozzájárult vagy engedélyezte. Az adatkezelő ésszerű erőfeszítéseket tesz, hogy ellenőrizhető hozzájárulást szerezzen be, figyelemmel az elérhető technológiára.*"[33]

A gyermekek személyes adatainak védelme kifejezetten előremutató, nem biztos azonban, hogy a különböző tagállami szabályozások (eltérő korhatárok a polgári jogi jogviszonyokban) megléte mellett kellően hatékonyan működhet-e ez a rendelkezés. Kérdés továbbá, hogy általánosságban lehet-e korlátozni a 13 év alatti gyermekek személyes adatainak átadását – az ICO Véleményében például a különböző segélykérő fórumok használatát, vagy nonprofit online tevékenységek végzését említi példaként. Nem tisztázott továbbá, hogy a gyakorlatban hogyan ellenőrizhető a szülő / gyám hozzájárulásának, engedélyének érvényessége, valamint a szülő / gyám ezzel kapcsolatban szükségszerűen átadott személyes adatainak összekapcsolása a gyermek adataival.

[32] Rendelettervezet 6. cikk (3)

[33] Rendelettervezet 8. cikk

Várható következmény: a gyermekek fokozottabb védelme, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára a gyermekek adatai kezelésével kapcsolatos eljárások finomhangolása miatt.

9. Különleges személyes adatok

A Hatályos Irányelvhez hasonlóan – az adatkör tekintetében némileg kibővítve – a Rendelettervezet szerint is „*tilos a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, az egészségügyi adatok vagy a szexuális életre, büntetőítéletekre, illetve az ezekhez kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok kezelése.*”[34] A Rendelettervezet felsorolja a kivételeket az általános tilalom alól, például ha az érintett személy hozzájárult az adatkezeléshez, illetve az foglalkoztatási jogszabályok alapján történik, vagy az érintett létfontosságú érdekeinek védelméhez szükséges, vagy olyan személyes adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott.

Érdekes módon az ICO kritikusan viszonyul a „személyes adatok” és a „különleges adatok” megkülönböztetéséhez. Az ICO Vélemény kiemeli, hogy az adatok jogszabályban történő éles elkülönítése nem túl életszerű, és az adatok megkülönböztetését érdemes lenne mindig az adott szituációra figyelemmel végezni, és megengedni a különleges adatok kezelését is, ha az az érintett személyek magánszférához való jogát nem érinti hátrányosan. A szexuális életre vonatkozó adat például bizonyos helyzetekben lehet valóban „különleges” védelmet igényel (pl. állásinterjún), más összefüggésben viszont kevésbé (pl. internetes társkereső oldal használata során). Szintén fontos lehet egészségügyi adatok kezelése például biztosítók számára, olyan napi szintű tevékenységek keretében, mint például kockázatfelmérés vagy valamilyen juttatásra való jogosultság megállapítása. Külön bírálja az ICO Vélemény a szakszervezeti tagságra utaló személyes adatok különleges státuszát. Az is előfordulhat, hogy az érintett személy valamely, a Rendelettervezet által különlegesnek nem minősített adatát (például pénzügyi helyzetre vonatkozó adatot) tekinti a saját szempontjából „különlegesnek”. Egy angol jogesetre hivatkozva – igényel-e külön védelmet egy munkavállalónak a klímaváltozással kapcsolatos véleménye? – az ICO Véleménye javasolja tisztázni, hogy a „*vallási vagy világnézeti meggyőződés*” mint különleges adat Hatályos Irányelv által használt fogalma (*religion or philosophical belief*) helyett bevezetésre kerülő „vallás vagy meggyőződés”[35] (*religion or belief*) mennyiben jelent szűkítést a korábbi értelmezéshez képest – az ICO itt a „vallási vagy egyéb meggyőződés” (*religion or similar belief*) fogalmát javasolja használni.

Várható következmény: az adatgazdák különleges adatainak változatlanul kiemelt védelme, ugyanakkor jelentős *compliance* költség az adatkezelők számára a különleges adatatok jogszerű kezelésének folyamatos vizsgálata során.

10. Az azonosítást lehetővé nem tévő adatkezelés

A Rendelettervezet szerint „*amennyiben az adatkezelő által kezelt adatok nem teszik lehetővé az adatkezelő számára, hogy azonosítson egy természetes személyt, az adatkezelő nem köteles kiegészítő információkat beszerezni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen e rendelet valamelyik rendelkezésének*„.[36]

[34] Rendelettervezet 9. cikk

[35] A Rendelettervezet magyar fordítása itt pontatlan.

[36] Rendelettervezet 10. cikk

A szokatlan rendelkezés célja vélhetően, hogy az érintett személyek hozzáférési jogának (információkérés az adatkezelés feltételeiről) teljesítéséhez – ha a rendelkezésre álló adatok önmagukban nem teszik lehetővé az érintett személy azonosítását, pl. kizárólag IP cím kezelése esetén – az adatkezelő ne legyen köteles további információkat beszerezni. Az ICO Véleménye kifejezetten üdvözli ezt a rendelkezést, mindazonáltal javasolja a pszeudonimizáció (*pseudonymisation* – erre javasol külön definíciót az EP Javaslat is*)* bátorítását, valamint a Hatályos Irányelv bevezetése 26. pontjának megismétlését, miszerint a védelem elvei nem alkalmazhatók az olyan módon anonimmé tett adatokra, ahol az érintett a továbbiakban nem azonosítható - mivel a tagállamok által elfogadott nemzeti rendelkezések helyes végrehajtásának elősegítésére szánt eljárási szabályzatok hasznos eszközök lehetnek útmutatásként ahhoz, hogy hogyan kell az adatokat anonimmé tenni, és olyan formában megőrizni, amelyben a szóban forgó adatok azonosítása a továbbiakban már nem lehetséges. Az ICO maga is bocsátott ki ilyen útmutatást, valamint 15.000 angol fontot különített el egy, az anonimizációval kapcsolatos technikák megosztását lehetővé tevő szakmai hálózat kialakítása céljából.[37]

Várható következmény: az anonimizációs gyakorlatok szélesebb körű elterjedése.

11. Átlátható tájékoztatás és kommunikáció és az érintett tájékoztatása[38]

A Rendelettervezet szerint az érintettre vonatkozó személyes adatok gyűjtése során az adatkezelőnek legalább az alábbiakról tájékoztatnia kell az érintettet:

a) az adatkezelő és képviselőjének (ha van) és az adatvédelmi felelősnek a személyazonossága és részletes elérhetősége;
b) az adatkezelés céljai (ideértve a szerződési feltételeket és az általános feltételeket, ha az adatkezelés szerződés megkötéséhez / teljesítéséhez, illetve jogi kötelezettség teljesítéséhez szükséges);
c) a személyes adatok tárolásának időtartama;
d) az érintett joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokba való betekintést, azok helyesbítését vagy törlését, vagy kifogásolhatja az ilyen személyes adatok kezelését;
e) a felügyelő hatósághoz címzett panasz benyújtásának joga és a felügyelő hatóság elérhetősége;
f) a személyes adatok címzettjei, illetve a címzettek kategóriái;
g) az adatkezelő harmadik országba vagy nemzetközi szervezet részére történő adattovábbítási szándéka esetén a harmadik ország vagy nemzetközi szervezet által biztosított védelem szintje, a Bizottság megfelelőségi határozatára való hivatkozás mellett;
h) az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükséges minden további tájékoztatás, tekintettel a személyes adatok gyűjtésének specifikus körülményeire;
i) ha az adatokat az érintettől gyűjtik, az adatok rendelkezésre bocsátásának kötelező vagy önkéntes jellege, valamint az adatszolgáltatás elmaradásának esetleges következményei; és
j) ha az adatokat nem az érintettől gyűjtik, milyen forrásból származnak a személyes adatok.

Az adatkezelő a fentiek szerinti tájékoztatást akkor nyújtja:

[37] **Draft Anonymisation code of practice**, http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/anonymisation_cop_draft_consultation.ashx

[38] Rendelettervezet 14. cikk

a) amikor a személyes adatot az érintettől beszerzi; vagy

b) ha a személyes adatot nem az érintettől szerezte be, a rögzítés időpontjában, vagy az adatgyűjtés vagy -kezelés különös körülményeire tekintettel az adatgyűjtést követő ésszerű időtartamon belül, illetve, ha az adatokat más címzetthez kívánják továbbítani, legkésőbb az adatok első közlésekor. Ebben esetben az adatkezelő megteszi a megfelelő intézkedéseket az érintett jogos érdekeinek védelme érdekében.

A fent ismertetett tájékoztatási kötelezettség nem alkalmazható, ha:

a) az érintett már rendelkezik a fenti információkkal; vagy

b) az adatot nem az érintettől szerezték be, és a kérdéses információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel; vagy

c) az adatot nem az érintettől szerezték be, és a rögzítést vagy a közlést jogszabály kifejezetten előírja; vagy

d) az adatot nem az érintettől szerezték be, és az ilyen tájékoztatás nyújtása sérti másoknak az uniós jogban vagy a tagállam jogában meghatározott jogait és szabadságait.

A Rendelettervezet az érintettek irányába történő átlátható tájékoztatás és kommunikáció megvalósítása céljából a következőket írja elő: „*Az adatkezelőnek a személyes adatok kezelése tekintetében és az érintettek jogainak gyakorlása érdekében átlátható és könnyen hozzáférhető szabályzatokkal kell rendelkeznie. Az adatkezelő a személyes adatok kezelésére vonatkozó tájékoztatást és értesítést, különösen a kifejezetten gyermekeknek szóló tájékoztatást, az érintett részére érthető formában, az érintett befogadóképességének megfelelő, világos és közérthető nyelven nyújtja.*”

A Hatályos Irányelv alapján nem állapítható meg egyértelműen, hogy miként lehet biztosítani a tájékoztatást, ha a személyes adatokra nem várt esetben van szükség (például *compliance* vizsgálat), vagy ha a tájékoztatás késleltetése szükséges – erre a kérdésre sajnos egyelőre a Rendelettervezet sem ad választ. Az ICO Véleménye az adatok rendelkezésre bocsátásának „kötelező” jellegét javasolja tovább részletezni: kötelező jogszabályon alapuló adatkezelést ért ezalatt a jogalkotó, vagy ha az adatok rendelkezésre bocsátása gyakorlati szempontból „kötelező”, például egy szolgáltatás igénybevételéhez. További kérdés, hogy a harmadik országban biztosított adatvédelmi szintről pontosan milyen mértékben kell tájékoztatni az érintett személyt – a tagállamok nemzeti előírásai ebben a tekintetben nem egységesek.

<u>Várható következmény: az adatgazdák szélesebb körű tájékoztatása az adatkezelésről, ugyanakkor jelentős és nem mindig ésszerű dokumentációs kötelezettség az adatkezelők számára.</u>

12. Az érintett jogai

A Rendelettervezet a Hatályos Irányelvhez képest jelentősen ki bővítené az érintett személyeknek az adatkezeléssel kapcsolatos jogait, az alábbiak szerint:

12.1 Hozzáférési jog

A Rendelettervezet a „hozzáférési jogot" (információkérés az adatkezelés feltételeiről) az alábbiak szerint szabályozza[39]:

„*Az érintett erre irányuló kérelem benyújtásával jogosult az adatkezelőtől bármikor megerősítést kérni arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. Az ilyen személyes adatok kezelése esetén az adatkezelő az alábbiakról nyújt tájékoztatást:*

a) az adatkezelés céljai;

b) az érintett személyesadat-kategóriák;

c) a címzettek vagy a címzettek kategóriái, akik számára az adatokat ki kívánják adni vagy kiadták, ideértve különösen a harmadik országbeli címzetteket;

d) a személyes adatok tárolásának időtartama;

e) azon jog megléte, hogy az érintett kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését vagy törlését, vagy kifogásolhatja az ilyen személyes adatok kezelését;

f) a felügyelő hatósághoz címzett panasz benyújtásának joga és a felügyelő hatóság elérhetősége;

g) értesítés az adatkezelés alatt álló személyes adatokról és az azok forrásával kapcsolatos minden rendelkezésre álló információról;

h) az ilyen adatkezelés jelentősége és várható következményei, legalább a profilalkotáson alapuló intézkedések esetében.

Az érintettnek joga van az adatkezelőtől a kezelt személyes adatok közlését kérni. Amennyiben az érintett a kérést elektronikus formában terjeszti elő, az információt elektronikus formában kell megadni, kivéve, ha az érintett eltérően igényli."

Várható következmény: az adatgazdák fokozottabb védelme az átláthatóbb adatkezelési gyakorlat megvalósításával, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára a szükséges eljárási szabályzatok bevezetése és gyakorlati alkalmazása során.

12.2 A helyesbítési jog

A Hatályos Irányelvhez hasonlóan a Rendelettervezet a „helyesbítési jogot" az alábbiak szerint szabályozza: „*Az érintett jogosult az adatkezelőtől a rá vonatkozó pontatlan személyes adatok helyesbítését kérni. Az érintett jogosult a hiányos személyes adatok kiegészítését kérni, ideértve a helyesbítő nyilatkozat igénybevételét.*".[40]

[39] Rendelettervezet 15. cikk

[40] Rendelettervezet 16. cikk

12.3 A személyes adatok tárolásának megszüntetéséhez és a törléshez való jog – valamint a „*felejtéshez való jog - right to be forgotten*”

A Rendelettervezet a személyes adatok tárolásának megszüntetéséhez és a törléshez való jogot az alábbiak szerint szabályozza[41]:

- „*Az érintett kérheti az adatkezelőtől a rá vonatkozó személyes adatok törlését, valamint az ilyen adatok további terjesztésétől való tartózkodást, különösen az érintett által gyermekkorában elérhetővé tett személyes adatok vonatkozásában, ha:*

  a) az adatokra már nincs szükség az adatgyűjtés vagy más módon történő kezelés céljából; vagy

  b) az érintett visszavonta hozzájárulását, vagy lejárt az engedélyezett adattárolási időtartam, vagy a személyes adatok kezelésének nincs más jogalapja; vagy

  c) az érintett kifogásolja a személyes adatok kezelését; vagy

  d) az adatkezelés egyéb okokból nem áll összhangban a rendelettel.”

A Rendelettervezet bevezeti az úgynevezett „felejtéshez való jogot” („*right to be forgotten*”), amely a Hatályos Irányelvhez képest jóval több kötelezettséget telepít az adatkezelőkre:

- „*Amennyiben az adatkezelő nyilvánosságra hozza a személyes adatokat, a technikai intézkedéseket is beleértve megtesz minden ésszerű lépést, hogy – azon adatok vonatkozásában, amelyek nyilvánosságra hozatala az adatkezelő felelősségi körébe tartozik – értesítse az ilyen adatokat kezelő harmadik felet arról, hogy az érintett kérte a személyes adat bármely nyilvános internetes linkjének, másolatának vagy másodpéldányának törlését. Amennyiben az adatkezelő harmadik felet hatalmazott fel a személyes adatok nyilvánosságra hozatalára, az adatkezelő felelősséggel tartozik e nyilvánosságra hozatalért.”*

- „*Az adatkezelő késedelem nélkül elvégzi a törlést, kivéve, ha a személyes adatok megőrzése a következő okokból szükséges: (i) a véleménynyilvánítás gyakorlásának szabadsága, (ii) a népegészség területén közérdekből, (iii) történelmi, statisztikai vagy tudományos célú kutatási célok, (iv) az adatkezelőre vonatkozó, uniós vagy nemzeti jogszabályba foglalt, a személyes adat megőrzésére vonatkozó jogi kötelezettség, illetve (v) ha az adatkezelés korlátozásának van helye.*”

A „felejtéshez való jog” a Rendelettervezet egyik legvitatottabb rendelkezése - a George Washington University professzora, Jeffrey Rosen szerint „*a legnagyobb veszély az internetes szólásszabadságra az elkövetkező évtizedben*”[42].

A Rendelettervezet gyakorlati megvalósításával kapcsolatban az egyik legnagyobb kérdés, hogy a „*felejtéshez való jog*” érvényesítésével kapcsolatos kérések teljesítése hogyan érhető el, különösen online környezetben. Nincs megfelelő szabályozás a Rendelettervezetben

[41] Rendelettervezet 17. cikk

[42] **The Right to be Forgotten**, http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

például azzal kapcsolatban, ha a „felejtéshez való jogot" visszaélésszerűen gyakorolják, például egy közszereplő a róla megjelent hátrányos információkat különböző nyilvános adatbázisokból töröltetni akarja. A 29-es Munkacsoport is bírálta a rendelkezés életszerűségét, megállapítva, hogy az internet gyakorlati működése jelentősen korlátozhatja annak hatékonyságát. Kiemelte továbbá a 29-es Munkacsoport, hogy a Rendelettervezet nem szabályozza azt az esetet, ha az adatkezelő már megszűnt, eltűnt vagy nem azonosítható, illetve nem lehet kapcsolatba lépni vele, valamint semmi sem teszi kötelezővé harmadik felek számára (ha nem terjed ki rájuk a Rendelet hatálya), hogy teljesítsék az adatkezelőnek a személyes adat bármely nyilvános internetes linkjének, másolatának vagy másodpéldányának törlésével kapcsolatos kérését.

A „felejtéshez való jog" megvalósításának technikai lehetőségeit vizsgálta Európai Hálózatbiztonsági Ügynökség (*European Network and Information Security Agency - ENISA*) is. 2012. november 20-án kiadott jelentésében az ENISA felhívta a figyelmet, hogy a fenti jog végrehajtásában segítséget nyújtó technikai megoldás a személyes adatok és a jogosultságot gyakorló személyi kör, valamint a véleménynyilvánítás gyakorlásának szabadsága által biztosított kivételi kör egységes meghatározásán kell alapuljon – és a Rendelettervezet jelenlegi szövege egyelőre nem felel meg ennek a feltételnek, mert nem definiálja például a „véleményszabadság" pontos tartalmát. Az ENISA is hangsúlyozza, hogy a „felejtéshez való jog" teljes megvalósítása az interneten gyakorlatilag lehetetlen. Az adatok szabadon másolhatók, terjeszthetők, és a másolatok utólagos azonosítása és törlése nem lehetséges. Elméletileg megfelelő megoldás lehet a digitális jogkezelési (*digital rights management* - DRM) technológiák alkalmazása (de még ezek is megkerülhetők), vagy a Rendelettervezet területi hatálya alá eső keresőmotorok szűrésre való kötelezése. Keresőmotorok esetében a kérdéses adat eltávolítása egyszerűbb lehet, egy Wikipedia szócikk esetén azonban már kevésbé. (Érdekes azonban a Bizottságnak az a megközelítése, miszerint a közösségi oldalak által végzett adatkezelés – ha az adatvédelmi beállításaik engedik, hogy csak „ismerősöknek" legyenek hozzáférhetők fényképek – a „természetes személy által haszonszerzési cél nélkül, kizárólag saját személyes célú vagy háztartási tevékenység során végzett adatkezelés" (*household exeption*) alá eshet, így a „felejtéshez való jog" elméletileg nem is vonatkozik az ilyen típusú adatkezelésre.) Óvatosan, de az EP Javaslat is bírálja a felejtéshez való jog életszerűségét – a módosítás-tervezet szerint a jog csak azokra az adatokra vonatkozna, amik jogosulatlanul kerültek nyilvánosságra.

Az adatok törléséhez való jog jelenlegi szabályozását az Európai Bíróság is vizsgálta, a spanyol legfelsőbb bíróság, az *Audiencia Nacional* előterjesztésére. Az ügyben érintettek panasszal éltek a spanyol adatvédelmi hatóságnál, mert a Google negatív színben feltüntető találatokat adott ki róluk (például egy, korábban műhibával vádolt plasztikai sebész, aki töröltetni szerette volna az erre vonatkozó utalásokat). Az illetékes hatóságok utasították a Google-t, hogy körülbelül 100 találatot töröljön, a szolgáltató azonban jogorvoslathoz folyamodott. Az Európai Bíróság azt vizsgálja, hogy köteles-e a Google eltávolítani a tartalmakat abban az esetben is, ha nem jogellenesek, és nem a Google szolgáltatja őket, kérdés továbbá, hogy az USA-ban letelepedett Google esetében jogosultak-e európai bíróságok eljárni. A Google állítása szerint csak akkor áll módjában eltávolítani a tartalmat, ha az érintett oldalak üzemeltetői kérik, hogy ne szerepeljen az oldal tartalma a Google keresési eredményei között. A Bizottság álláspontja szerint azonban az érintett személyeknek joguk van az adatok törlését kérni, és a Google köteles ennek eleget tenni, mert módjában áll meghatározni az adatok kezelésének módját, feltételeit és tartalmát. Érdekes párhuzam, hogy a SABAM vs. Netlog (C-360/10) ügyben 2012. február 16-én hozott ítéletében az Európai Bíróság megállapította, a közösségi oldalak és internetes platformok nem kötelezhetők a felhasználók által egymás között cserélt, de szerzői jogot sértő fájlok általános szűrőrendszer bevezetésére, a személyes adatok védelméhez való jog korlátozása ugyanis nem áll arányban a szerzői jogok védelméhez fűződő érdekkel.

Peter Fleischer, a Google adatvédelmi jogásza a társaság blogjában bírálta a „felejtéshez való jog" előírását.[43] Írásának fő gondolata, hogy a hagyományos definíciók alapján besorolható-e a Google, a Facebook vagy a Youtube az e-kereskedelemről szóló jogszabályok által meghatározott kategóriákba, és felelősségi körbe (a probléma ugyanaz, mint a cloud computing esetében). Nem szabad továbbá „túlvédeni" az adatgazdákat, és elhanyagolni felelősségüket a közösségi oldalak megfelelő használata során – fontos angol példa a Nominet „Know the Net"felvilágosító kampánya az ezzel kapcsolatos adatvédelmi kockázatokról. Nincs egységes szabályozás egyelőre az adatmegsemmisítés pontos módjáról sem – az ICO 2012. november 20-án bocsátott ki ezzel kapcsolatos iránymutatást.[44]

A fenti aggályok alapján az biztosan megállapítható, hogy a Rendelettervezet elfogadása esetén a „felejtéshez való jog" biztosításával kapcsolatban számos gyakorlati nehézség várható.

Várható következmény: az adatgazdák fokozottabb védelme az adattörlési jog kiterjesztésével, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára a szükséges eljárási szabályzatok bevezetése és gyakorlati alkalmazása során, valamint jogviták felmerülésének veszélye a „felejtéshez való jog" tartalmának gyakorlati interpretációjával kapcsolatban.

12.4 Az adatkezelés korlátozása

A Rendelettervezet előírja az adatkezelő számára, hogy minden olyan címzettet tájékoztasson a Rendelettervezet 16. és 17. cikke értelmében végzett valamennyi törlésről vagy zárolásról, akivel/amellyel az adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

A Rendelettervezet szerint „*az adatkezelő a személyes adatok törlése helyett korlátozza azok kezelését, ha:*

a) az érintett vitatja az adatok pontosságát, arra az időtartamra, amely alatt az adatkezelő felülvizsgálhatja az adatok pontosságát;

b) az adatkezelőnek feladata ellátásához már nincs szüksége a személyes adatokra, de bizonyítási célból meg kell tartania az adatokat;

c) a kezelés jogellenes, és az érintett kifogásolja a törlést, és inkább az adatok felhasználásának korlátozását kéri;

d) az érintett az „adathordozhatósághoz való jog" alapján kéri a személyes adatok más automatizált feldolgozó rendszerbe történő továbbítását."[45]

A fentiek szerinti „korlátozott" felhasználású személyes adatok a tárolás kivételével csak bizonyítás céljára vagy az érintett hozzájárulásával vagy más természetes vagy jogi személy jogainak védelme, illetve közérdekű cél érdekében dolgozhatók fel. Ha a személyes adatok kezelése a fentiek értelmében korlátozott, az adatkezelő az adatkezelés korlátozásának feloldása előtt tájékoztatja az érintettet. A Rendelettervezet előírja az adatkezelő számára,

[43] **Our thoughts on the right to be forgotten**, http://googlepolicyeurope.blogspot.hu/2012/02/our-thoughts-on-right-to-be-forgotten.html

[44] **IT asset disposal for organizations**, http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/it_asset_disposal_for_organisations_20121_pdf.ashx

[45] Rendelettervezet 17. cikk (4)

hogy olyan mechanizmusokat vezessen be, amelyek biztosítják a személyes adatok törlésére és/vagy az adattárolás szükségességének időszakos felülvizsgálatára meghatározott határidő tiszteletben tartását.[46]

12.5 Az adathordozhatósághoz való jog[47]

Az „adathordozhatósághoz való jog" (*data portability*) rögzítésével a Rendelettervezet új alapelvet vezet be, a következők szerint:

„*A személyes adatok strukturált és széles körben használt formátumban történő elektronikus kezelése esetén az érintettnek joga van arra, hogy kérje az adatkezelőtől az adatkezelés alatt álló adatok széles körben használt elektronikus és strukturált formátumú másolatát, amely lehetővé teszi az érintett általi további használatot. Amennyiben a személyes adatokat az érintett bocsátotta rendelkezésre, és az adatkezelés hozzájáruláson vagy szerződésen alapul, az érintett jogosult arra, hogy ezeket a személyes adatokat és az érintett által rendelkezésre bocsátott, automatizált feldolgozó rendszerben tárolt bármely egyéb információt széles körben használt elektronikus formátumban egy másik rendszerbe továbbítson, anélkül hogy akadályozná a személyes adatok visszavonásával érintett adatkezelőt.*"

Az „adathordozhatósághoz való jog" elfogadása esetén az adatkezelőknek jelentősen kell kialakítani az adatkezelés technikai feltételeit és belső eljárásaikat, hogy meg tudjanak felelni az új rendelkezéseknek.

Az ICO aggálya az új alapelv gyakorlati megvalósításával kapcsolatban, hogy az adatkezelők „nem széles körben használt" formátumban fogják majd tárolni az adatokat, ezzel próbálva kikerülni a rendelkezésnek való megfelelést – emiatt javasolja, hogy a Rendelettervezet tartalmazzon az adatkezelők számára egy ezzel kapcsolatos „konvertálási" kötelezettséget is.

Várható következmény: a „felejtéshez való joghoz" hasonlóan az adatgazdák fokozottabb védelme az adatok feletti ellenőrzési jog kiterjesztésével, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára a szükséges eljárási szabályzatok bevezetése és gyakorlati alkalmazása során, valamint jogviták felmerülésének veszélye az „adathordozhatósághoz való jog" tartalmának gyakorlati interpretációjával kapcsolatban.

12.6 A kifogásoláshoz való jog[48]

A Rendelettervezet lehetővé teszi, hogy az érintett egyedi helyzetével kapcsolatos indokok alapján bármikor kifogásolhatja személyes adatainak a kezelését a következő esetekben:

(a) *az adatkezelés az érintett létfontosságú érdekének védelme miatt szükséges;*
(b) *az adatkezelés közérdekű feladat végrehajtásához vagy az adatkezelőre ruházott hivatali hatáskör gyakorlásához szükséges;*
(c) *az adatkezelés az adatkezelő jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek*".

Kivétel a fentiek alól, ha az adatkezelő igazolja, hogy az adatkezelést olyan kényszerítő erejű, jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel vagy

[46] Rendelettervezet 17. cikk (5) – (7)
[47] Rendelettervezet 18. cikk
[48] Rendelettervezet 19. cikk

alapvető jogaival és szabadságaival szemben. A bizonyítási tehernek az adatkezelőre való telepítésével a rendelkezés az érintett személyek javára előrelépést jelent a Hatályos Irányelvhez képest.

A Rendelettervezet külön kifogásolási jogot határoz meg arra az esetre, ha a személyes adatokat közvetlen üzletszerzés érdekében kezelik, és előírja, hogy e jogra kifejezetten, érthető módon fel kell hívni az érintett figyelmét, és a felhívásnak egyértelműen megkülönböztethetőnek kell lennie minden más információtól.[49] A közvetlen üzletszerzés céljából történő adatgyűjtésre ettől függetlenül irányadók a tagállami jogszabályok, különös tekintettel az *opt-in* vagy *opt-out* szabályaira a direkt marketing kommunikációk esetén.

12.7 Az érintett jogainak gyakorlására vonatkozó eljárások és mechanizmusok

A Rendelettervezet előírja[50] az adatkezelő számára, hogy alakítsa ki a tájékoztatáshoz, valamint az érintettek jogainak gyakorlásához szükséges eljárásokat.

Amennyiben a személyes adatokat automatizált módon kezelik, az adatkezelő biztosítja a kérelmek elektronikus úton történő benyújtásának lehetőségét is. Az adatkezelő késedelem nélkül és legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet arról, hogy történt-e az érintett jogainak gyakorlásával kapcsolatos intézkedés, valamint szolgáltatja a kért információt. E határidő egy hónappal meghosszabbítható, ha több érintett gyakorolja jogait, és együttműködésük ésszerű mértékben szükséges az adatkezelő szükségtelen és aránytalan törekvésének megakadályozása szempontjából. Ezt a tájékoztatást írásban kell nyújtani.

Amennyiben az érintett elektronikus formában nyújtotta be a kérelmet, az értesítést elektronikus formában kell közölni, kivéve, ha az érintett eltérően igényli. Amennyiben az adatkezelő megtagadja, hogy az érintett kérelme nyomán intézkedést hozzon, tájékoztatja az érintettet az elutasítás okairól, valamint a felügyelő hatósághoz címzett panasz és a bírósági jogorvoslati kérelem lehetőségéről.

A fenti tájékoztatás és a kérelemre tett intézkedések térítésmentesek. Amennyiben a kérelmek egyértelműen túlzóak, különösen ismétlődő jellegük miatt, az adatkezelő díjat számíthat fel a tájékoztatásért vagy a kért intézkedés megtételéért, vagy visszautasíthatja a kért intézkedés megtételét. Ebben az esetben az adatkezelőt terheli a kérelem egyértelműen túlzó jellegének bizonyítása.

Az ICO bizonyos esetekben – például ha a személyes adatok az érintett személy számára már elektronikus formában rendelkezésre állnak – rövidebb határidőt javasol. Hangsúlyozza ugyanakkor, hogy több érintett joggyakorlása esetén a két hónapos válaszadási határidő viszont rövid lehet – az ICO itt nem javasol konkrét határidőt meghatározni, csak a kérés „lehető legrövidebb időn belül" történő teljesítését. A „több érintett" fogalmát is érdemes lehet számszerűsíteni a Rendelettervezet végső szövegében.

Várható következmény: az adatgazdák fokozottabb védelme az átláthatóbb adatkezelési gyakorlat megvalósításával, ugyanakkor jelentős *compliance* és IT költség az adatkezelők számára a szükséges mechanizmusok bevezetése és gyakorlati alkalmazása során.

[49] Rendelettervezet 19. cikk (2)

[50] Rendelettervezet 12. cikk

13. Profilalkotáson alapuló intézkedések

A Rendelettervezet – előrelépésként a Hatályos Irányelvhez képest – kifejezetten nevesíti a profilalkotással kapcsolatos adatvédelmi kötelezettségeket. Eszerint:

- „*Minden természetes személynek joga van ahhoz, hogy ne terjedhessen ki rá olyan intézkedés hatálya, amely e természetes személyre nézve jogi hatással járna, vagy őt jelentős mértékben érintené, és amely kizárólag automatizált adatkezelésen alapul, és amelynek célja a természetes személyre vonatkozó egyes személyes szempontok értékelése, vagy különösen a természetes személy munkahelyi teljesítményének, gazdasági helyzetének, tartózkodási helyének, egészségének, személyes igényeinek, megbízhatóságának vagy viselkedésének elemzése vagy előrejelzése.*"

- „*Valamely személyre csak abban az esetben vonatkozhat a fentiek szerinti intézkedés, ha az adatkezelést:*

  a) valamely szerződés megkötése vagy teljesítése során végzik, ha a szerződés érintett kérelmére történő megkötése vagy teljesítése teljesül, vagy ha biztosítják az érintett jogos érdekeinek biztosítására alkalmas intézkedéseket, például az emberi beavatkozás kérésére vonatkozó jogot; vagy

  b) olyan uniós vagy nemzeti jogszabály írja elő kifejezetten, amely rendelkezik az érintett jogos érdekeinek biztosítására alkalmas intézkedésekről is; vagy

  c) az érintett hozzájárulása alapján végzik, a hozzájárulás feltételeivel kapcsolatban megállapított rendelkezések és a megfelelő biztosítékok mellett."[51]

- „*A valamely természetes személlyel kapcsolatos egyes személyes szempontok értékelését célzó automatizált személyesadat-feldolgozás nem alapulhat kizárólag különleges személyes adatokon.*"

- „*Az adatkezelő által nyújtandó adatvédelmi tájékoztatás felöleli a profilalkotáson alapuló intézkedés céljából történő adatkezelés megvalósulására, és az ilyen adatkezelésnek az érintett tekintetében várható hatásaira vonatkozó információkat.*"

Az ICO Vélemény szerint a rendelkezésből nem vezethető le egyértelműen, hogy a profilalkotáson alapuló intézkedésekkel kapcsolatos kötelezettségek vonatkoznak-e az online viselkedésalapú, célzott reklámokra – a szövegezés alapján a válasz inkább nem, mivel az ilyen típusú reklámok vélhetően nem járnak jogi hatással, vagy érintenék jelentős mértékben az adott személyt. A 29-es Munkacsoport Véleménye kifejezetten nevesíti a webes elemző eszközöket, a felhasználó viselkedésének elemzési célú nyomon követését, a mobil alkalmazások által alkotott helyváltoztatási profilokat, és a közösségi oldalak által végzett személyes profilalkotást, jelezve, hogy tisztázni kell, vajon kiterjednek-e ezekre a Rendelettervezet fenti rendelkezései. A 29-es Munkacsoport Véleménye szerint továbbá a rendelkezés nem korlátozható kizárólag az automatizált adatkezelésre, hanem a részben automatizált adatkezelési módszerekre is ki kell terjedjen. Az EP Javaslat még ennél is messzebb megy: kifejezetten az adatgazda előzetes hozzájárulásához, vagy jogszabályi

[51] Rendelettervezet 20. cikk

felhatalmazáshoz kötné a profilozást. Kérdés, hogy mennyire életszerű a tilalom az online környezetben, ahol a profilozás elengedhetetlen a személyre szabott szolgáltatások, tartalmak előállításához, valamint a pénzügyi szervezetek és biztosítók gyakorlatában, ahol szintén fontos az ügyfél-profilok kialakítása.

Várható következmény: az adatgazdák fokozottabb védelme a profilozás szigorításával, ugyanakkor jelentős *compliance* az adatkezelők számára a profilozás jogszerűségének esetről-esetre történő vizsgálata során.

14. Az adatkezelő általános kötelezettsége – „elszámoltathatóság"[52]

A Rendelettervezet által bevezetett „elszámoltathatóság" (*accountability*) értelmében „*az adatkezelő elfogadja azokat a szabályzatokat és végrehajtja azokat a megfelelő intézkedéseket, amelyekkel biztosítja és igazolni tudja azt, hogy a személyes adatok kezelése a rendelettel összhangban történik*".

- Ezek az intézkedések különösen a következőket tartalmazzák:

  a) a Rendelettervezet szerinti, az adatkezelési műveleteket dokumentáló dokumentáció vezetése (lásd részletesen a 16. pontot);

  b) a Rendelettervezetben rögzített adatbiztonsági követelmények érvényesítése;

  c) a Rendelettervezet szerinti adatvédelmi hatásvizsgálat lefolytatása;

  d) a Rendelettervezet értelmében a felügyelő hatóság előzetes engedélyezéséhez vagy előzetes konzultációhoz szükséges feltételek teljesítése;

  e) a Rendelettervezet szerinti adatvédelmi felelős kijelölése.

- „*Az adatkezelő végrehajtja a fent említett intézkedések hatékonyságának felülvizsgálatához szükséges mechanizmusokat. Amennyiben ez arányos, a felülvizsgálatot független belső vagy külső ellenőr végzi*."

Tény, hogy az „elszámoltathatóság" koncepciója egyre inkább terjed az adatvédelmi gyakorlatban. A szabályozási háttér különösen Kanadában előremutató: az illetékes adatvédelmi biztosok (*Canadian Federal, British Columbia and Alberta Privacy Commissioners*) 2012. április 27-én „*Getting Accountability Right with a Privacy Management Program*" elnevezésű iránymutatást bocsátottak ki. Az „elszámoltathatóság" elvének jogszabályi szintre emelésével kapcsolatban ugyanakkor a legnagyobb aggály, hogy nem vezet-e az adatkezelő szervezetén belül „túldokumentáltsághoz". Ismét érdekes módon az ICO Vélemény tartja problémásnak a rendelkezés dokumentáció-központúságát; kiemeli például, hogy nem kellene szankcionálni azt az adatkezelőt, aki egyébként a jogszabályoknak megfelelően, az érintett személyek magánszféráját nem veszélyeztetve végzi tevékenységét, de nem rendelkezik a megfelelő „papírokkal". Az adatkezelők és az adatfeldolgozók párhuzamos dokumentációs kötelezettsége is további ésszerűtlen adminisztrációhoz vezethet. A jogszabálynak az ICO szerint inkább azt kellene általánosságban rögzítenie, hogy az adatkezelőnek megfelelően tudnia kell bizonyítani: megtette a szükséges lépéseket a jogszabályoknak való megfelelés érdekében. Ennek elmulasztását a hatóság pedig figyelembe veszi akkor, ha egyébként szankció kiszabására

[52] Rendelettervezet 22. cikk

kerülne sor. Az ICO Véleménye felhívja a figyelmet arra is, hogy az elszámoltathatóság elvének érvényesíthetősége során lehetővé kell tenni az adatkezelő méretének és az adatkezelési tevékenység jellegének figyelembevételét.

Több kutatás is vizsgálta, mennyire ésszerű elvárás az adatkezelőkkel szemben az adatkezelési műveletek teljes körű dokumentálása, és valóban növeli-e ez az adatkezelés átláthatóságát, az adatgazdák tájékoztatását - egy átlagember több száz, saját adatvédelmi tájékoztatóval rendelkező weboldalt keres fel évente. A Microsoft-ot képviselő Brad Smith példája szerint „az átlagos fogyasztónak évente 1462 adatvédelmi szabályzatot kellene elolvasnia."[53] Egy másik példa: a legnagyobb 75 weboldal adatvédelmi szabályzatának átlagos terjedelme 2514 szó, elolvasásuk 10 perc, a potenciálisan erre fordított idő évente 25 nap. Kiesett munkaórák alapján az elvesztett összeg nagyobb, mint Florida állam (az USA negyedik legnagyobb gazdasága) GDP-je.[54] Egy másik becslés szerint az USA-ban például 781 milliárd amerikai dollár bevételkiesést jelentene, ha mindenki elolvasná az általa egy évben felkeresett weboldalak adatvédelmi szabályzatát.[55]

A fenti aggályok kivédése érdekében az FTC-t képviselő Jon Leibowitz szerint az adatvédelmi szabályzatoknak a „müzlisdobozokon található tájékoztatásokhoz"-hoz hasonló hosszúságúnak kellene lenniük.[56] Mostanában számos EU tagállam szabályozása a „dereguláció", az adatkezelési dokumentáció minimalizálása irányába mozdul: Olaszországban egy jogszabály-módosítás következtében például a „Documento Programmatico sulla Sicurezza – DPS" elnevezésű adatbiztonsági dokumentáció vezetése nem kötelező már. Megoldás lehet a Rendelettervezet által biztosított tanúsítási lehetőség, miszerint „*a tagállamok, valamint a Bizottság – különösen európai szinten – ösztönzik olyan adatvédelmi tanúsítási mechanizmusok és adatvédelmi címkék és jelzők létrehozását, amelyek segítségével az érintettek gyorsan fel tudják mérni az adatkezelő és az adatfeldolgozó által biztosított adatvédelem szintjét. Az adatvédelmi tanúsítási mechanizmusok hozzájárulnak e rendelet helyes alkalmazásához, figyelembe véve a különböző ágazatok és a különböző adatkezelési műveletek sajátos jellemzőit*".[57] Hasonló megközelítést alkalmaz az EP Javaslat is, amikor az adatvédelmi szabályzatok főbb rendelkezéseit elektronikus ikonok formájában is elérhetővé tenné az adatgazdák számára.

Várható következmény: a korábbinál jóval szélesebb körű, és nem mindig ésszerű dokumentálási kötelezettség és adminisztrációs teher az adatgazdák számára.

15. „Beépített és alapértelmezett adatvédelem" (*Privacy by Design*)

A nemzetközi adatvédelmi gyakorlatban már a Rendelettervezet közzététele előtt is megjelent, és egyre inkább piaci gyakorlattá válik a „beépített és alapértelmezett adatvédelem (*Privacy by Design*)" fogalma. A Global System for Mobile Communications Association (GSMA) például 2012. február 27-én kibocsátotta a „*Privacy Design Guidelines for Mobile Application Development*" című iránymutatást, melynek célja, hogy a felhasználók nagyobb átláthatósággal, választási lehetőséggel és ellenőrzési jogkörrel rendelkezzenek arról, hogy az egyes alkalmazások hogyan használják fel személyes adataikat.

---

[53] **Uruguay: Soundbites from the 34th Annual Privacy Conference,** http://dataguidance.com/news.asp?id=1887

[54] **Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days**, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

[55] **The Cost of Reading Privacy Policies**, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf

[56] **FTC chair Leibowitz: Apps need simpler privacy statements**, http://news.cnet.com/8301-1023_3-57444602-93/ftc-chair-leibowitz-apps-need-simpler-privacy-statements/

[57] Rendelettervezet 39. cikk

A Rendelettervezet fogalomrendszerében[58] „beépített és alapértelmezett adatvédelem" két általános kötelezettséget jelent az adatkezelő számára:

- „*a technika állására és végrehajtás költségeire tekintettel mind az adatkezelés módjának meghatározása, mind az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre oly módon, hogy az adatkezelés megfeleljen e rendelet követelményeinek, és biztosítsa az érintettek jogainak védelmét*"
- „*olyan mechanizmusokat kell végrehajtania, amelyek alapértelmezett módon biztosítják azt, hogy kizárólag az adatkezelés egyes konkrét céljaihoz szükséges személyes adatok kerülnek kezelésre, és különösen azt, hogy az adatgyűjtés vagy -tárolás során az adatok mennyisége és az adattárolási időtartam tekintetében sem lépik túl az e célokhoz szükséges legkisebb mértéket. Ezeknek a mechanizmusoknak különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezett módon ne váljanak határozatlan számú egyén számára hozzáférhetővé*."

A 29-es Munkacsoport Véleménye javasolja, hogy a Rendelettervezet végső szövege külön rögzítse, hogy a gyártóknak, adatkezelőknek automatikusan aktiválniuk kell a „beépített és alapértelmezett adatvédelmet".

Várható következmény: az adatgazdák fokozottabb védelme, ugyanakkor jelentős technikai és fejlesztési kiadások az adatgazdák számára.

16. Az adatkezelési műveletek dokumentálása

A már említett „elszámoltathatóság" keretében a Rendelettervezet a következő dokumentáció-vezetési kötelezettségeket írja elő az adatkezelők és adatfeldolgozók számára[59]:

„*Valamennyi adatkezelő és –feldolgozó, valamint – ha van ilyen – az adatkezelő képviselője dokumentálja a feladatkörébe tartozó összes adatkezelési műveletet. A dokumentáció legalább az alábbi információt tartalmazza:*

a) *az adatkezelő vagy a közös adatkezelő, illetve az adatfeldolgozó és – ha van ilyen – a képviselő neve és elérhetősége;*

b) *az adatvédelmi felelős neve és elérhetősége, ha van ilyen;*

c) *az adatkezelés céljai, beleértve az adatkezelő jogos érdekeit, amennyiben az adatkezelés az adatkezelő jogszerű érdekeinek érvényesítéséhez szükséges;*

d) *az érintettek kategóriáinak, valamint a rájuk vonatkozó személyes adatok kategóriáinak ismertetése;*

e) *a személyes adatok címzettjei vagy címzetti kategóriái, beleértve a jogos érdekre hivatkozással a személyes adatokat megszerző adatkezelőket;*

f) *adott esetben az adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország és a*

[58] Rendelettervezet 23. cikk
[59] Rendelettervezet 28. cikk

nemzetközi szervezet azonosítását, valamint szükség esetén a megfelelő adatvédelmi biztosítékok (részletesen lásd a 22. pontot) *igazolását;*

g) a különböző adatkategóriák törlésére vonatkozó határidők általános meghatározása;

h) az „elszámoltathatósággal" kapcsolatos intézkedések hatékony felülvizsgálata mechanizmusainak leírása.

E kötelezettségek nem vonatkoznak az alábbi adatkezelőkre és adatfeldolgozókra:

a) kereskedelmi érdek nélkül személyes adatokat kezelő természetes személyek; vagy

b) a 250 főnél kevesebb főt foglalkoztató vállalkozás vagy szervezet, amely személyes adatokat csak a főtevékenységét kiegészítő tevékenységként kezel."

Az ICO Vélemény az „elszámoltathatóság" bírálatához hasonlóan ezzel a rendelkezéssel kapcsolatban is kétségeit fejezi ki a kiterjedt dokumentálási kötelezettség hatékonyságával kapcsolatban.

Várható következmény: mint az „elszámoltathatóság" koncepciójánál - a korábbinál jóval szélesebb körű dokumentálási kötelezettség és adminisztrációs teher az adatgazdák számára.

17. Adatbiztonság

A Hatályos Irányelvhez hasonlóan a Rendelettervezet is csak általános kereteket biztosít az adatbiztonsági intézkedéseknek: nem határozza meg specifikusan azok végrehajtásának módját, az alkalmazandó eljárásokat, technológiákat. A Rendelettervezet szerint: „*Az adatkezelő és az adatfeldolgozó, a technika állására és a végrehajtás költségeire tekintettel, végrehajtja a megfelelő technikai és szervezési intézkedéseket az adatkezelés kockázatainak és a védendő személyes adatok jellegének megfelelő védelmi szint biztosítása érdekében. Az adatkezelő és az adatfeldolgozó a kockázatok értékelését követően végrehajtja az adatbiztonsági intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése vagy véletlen elvesztése elleni védelme, valamint az adatkezelés jogellenes formáinak, különösen a személyes adatok jogosulatlan nyilvánosságra hozatalának, terjesztésének vagy az azokhoz való hozzáférésnek vagy azok megváltoztatásának megelőzése érdekében.*"[60]

18. Adatbiztonsági értesítések

Összhangban a nemzetközi adatvédelmi trendekkel, a Rendelettervezet általánosságban kötelezővé teszi az adatbiztonsági értesítési kötelezettséget (*security breach notification*) valamennyi iparágban. Az EU-ban egyelőre csak az elektronikus hírközlési szektorban van egységes szabályozás az e-Privacy Irányelv alapján. Egyes tagállamok ugyanakkor szélesebb körben határozzák meg ezt a kötelezettséget: Németországban és Norvégiában például van értesítési kötelezettség mind a felügyelő hatóság, mind az érintett személyek számára. Ausztriában csak az érintett személyeket kell értesíteni, más országokban – Anglia, Dánia, Írország – önkéntes értesítési rendszer van. Az USA-ban egyre jelentősebb bírói gyakorlata alakul ki az adatbiztonsági eseményekkel kapcsolatos pereknek, és a csoportos perindítások nagy médianyilvánosságot is kapnak. Nemrég a LinkedIn-től loptak 6,5 millió ügyféladatot, melynek eredményeképpen Kaliforniában csoportos per indult a

[60] Rendelettervezet 30. cikk

közösségi oldal ellen, bár a felhasználókat ért kárt nehéz bizonyítani [61] - a bíróságok viszont eddig következetesen csak a közvetlen károk megtérítését írták elő. (Az EP Javaslat előírná a közvetett károk megtérítését is.) Európában legutóbb az ICO büntetett adatbiztonsági esemény miatt – a Sony Computer Entertainment Europe Limited 250.000 angol font bírságot kapott, mert a megfelelő szoftverfrissítéssel és biztonságosabb jelszóvédelemmel megakadályozhatta volna a 2011. áprilisi hackertámadást, ahol több millió felhasználó személyes adata került veszélybe.[62] (A különböző fórumokon egyébként azóta is vitatják, hogy megfelelő nagyságú pénzbüntetés-e a fenti összeg egy ilyen mértékű adatbiztonsági hiba szankcionálására, különös tekintettel a Rendelettervezet által előirányzott büntetési tételek várható összegére.[63])

18.1 Adatbiztonsági értesítések a felügyelő hatóság számára[64]

A Rendelettervezet a felügyelő hatóságoknak küldendő adatbiztonsági értesítésekkel kapcsolatban a következő szabályokat állapítja meg:

- „*Az adatkezelő a személyes adatok megsértése esetén indokolatlan késedelem nélkül, amennyiben lehetséges a személyes adatok megsértéséről való tudomásszerzéstől számított 24 órán belül értesíti a felügyelő hatóságot a személyes adatok megsértéséről. A felügyelő hatóság értesítését írásbeli indokolással kell ellátni, amennyiben arra nem 24 órán belül került sor.*"

- „*Az adatfeldolgozó a személyes adatok megsértésének megállapítását követően azonnal figyelmezteti és tájékoztatja az adatkezelőt.*"

- Az adatbiztonsági értesítés legalább az alábbiakat tartalmazza:

  „*a) a személyes adatok megsértésének ismertetése, beleértve az érintettek kategóriáit és számát, valamint az érintett adatok kategóriáit és számát;*

  b) az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó személyének és elérhetőségének közlése;

  c) a személyes adatok megsértéséből eredő esetleges hátrányos következmények enyhítésére irányuló intézkedésekre vonatkozó javaslat;

  d) a személyes adatok megsértéséből fakadó következmények ismertetése;

  e) az adatkezelő által a személyes adatok megsértésének orvoslására javasolt vagy tett intézkedések ismertetése."

- „*Az adatkezelő dokumentál minden személyesadat-sértést a hozzá kapcsolódó tények, hatások és az orvoslására tett intézkedések feltüntetésével.*"

[61] **LinkedIn Passwords Hacked – UPDATE**, http://www.privacyandsecuritymatters.com/2012/06/linkedin-passwords-hacked/

[62] **Sony fined £250,000 after millions of UK gamers' details compromised**, http://www.ico.gov.uk/news/latest_news/2013/ico-news-release-2013.aspx?goback=.gde_42462_member_208337621

[63] **Playstation Punishment – Harsh Enough?**, http://cloud-data-news.postcodeanywhere.co.uk/index.php/2013/1/24/playstation-punishment/?goback=.gde_944557_member_208043501

[64] Rendelettervezet 31. cikk

18.2 Adatbiztonsági értesítések az érintett személyek számára[65]

A Rendelettervezet az érintett személyeknek küldendő adatbiztonsági értesítésekkel kapcsolatban a következő szabályokat állapítja meg:

- „*Amennyiben a személyes adatok megsértése várhatóan hátrányosan érinti az érintett személyes adatainak vagy magánéletének védelmét, az adatkezelő a felügyelő hatóságnak tett értesítést követően indokolatlan késedelem nélkül tájékoztatja az érintettet a személyes adatok megsértéséről.*"

- „*Az érintett értesítésének ismertetnie kell a személyes adat megsértésének jellegét, és tartalmaznia kell legalább az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó személyének és elérhetőségének közlését, valamint a személyes adatok megsértéséből eredő esetleges hátrányos következmények enyhítésére irányuló intézkedésekre vonatkozó javaslatokat.*"

- „*A személyes adatok megsértéséről nem szükséges értesíteni az érintettet, ha az adatkezelő a felügyelő hatóság által elfogadott módon igazolja, hogy a megfelelő technológiai védelmi intézkedéseket végrehajtotta, és az említett intézkedéseket alkalmazták az adatok megsértésével érintett adatokra. E technológiai védelmi intézkedéseknek értelmezhetetlenné kell tenniük az adatokat a hozzáférési joggal nem rendelkező személyek számára.*"

- „*Amennyiben az adatkezelő az érintettet még nem értesítette a személyes adatok megsértéséről, a felügyelő hatóság – az adatkezelő azon kötelezettségének sérelme nélkül, hogy az érintettet a személyes adatok megsértéséről értesítse – az adatsértés esetleges hátrányos hatásait mérlegelve felszólíthatja ennek megtételére.*"

Az utolsó ponttal kapcsolatban az ICO Vélemény bírálja, hogy a felügyelő hatóság számára a Rendelettervezet nem ír elő határidőt az értesítési kötelezettség előírására, valamint – a vonatkozó intézkedések megtételének sürgősségére tekintettel – célszerű lehet az érintett személyt az adatbiztonsági eseményről minél hamarabb értesíteni.

Az adatbiztonsági értesítésekkel kapcsolatos aggályokat az ICO Vélemény is megismétli. Fontos lenne meghatározni, hogy a csak néhány személyt érintő, vagy jelentős kockázatot nem hordozó adatbiztonsági eseményről nem feltétlenül szükséges értesíteni az illetékes hatóságokat, mert a relatíve kis jelentőségű eseményekről való túl sok értesítést a hatóságok rendelkezésre álló erőforrásokkal nem lehet kezelni, és az adatgazdák sem fogják komolyan venni a nagyszámú értesítések jelentőségét. „*Notification fatigue"* – ezt a szót használja az EP Javaslat is, ami példákkal határozza meg, mi minősül „hátrányos" eseménynek. Ilyen a személyiséglopás, a csalás, a testi épség veszélye, megaláztatás, vagy jóhírnév sérelme. Ezen az álláspontón van a 29-es Munkacsoport is. Az amerikai gyakorlat alapján ilyen eset lehet például, ha különleges adatok, jelentős számú adatgazda vagy kiskorúak érintettek, bűncselekmény veszélye áll fenn, ismétlődő eseményről van szó, vagy közvetlen, anyagi kár merülhet fel. Egyes adatkezelők – pl. egészségügyi adatok kezelői vagy hitelintézetek – természetesen kivonhatók a kivételek alól, az általuk kezelt speciális adatkörre tekintettel.

A gyakorlatban a 24 órás határidő nem kifejezetten reális – az EP Javaslat például 72 órában határozná meg ezt az időtartamot. Célszerű lehet a harmonizáció az e-Privacy Irányelv rendelkezésével, ami „késedelem nélküli" értesítést ír elő. A 29-es Munkacsoport Véleménye „kétlépcsős" bejelentést javasol: bejelentést 24 órán belül - ha nincsenek meg a

[65] Rendelettervezet 32. cikk

szükséges információk, akkor azok nélkül, majd egy második szakaszban teljes bejelentéstt. Javasolja továbbá a 29-es Munkacsoport Véleménye, hogy a bejelentési formanyomtatvány tartalmazza a személyes adatok megsértésének súlyosságára vonatkozó, objektív kritériumokon alapuló értékelést.

Az ICO Véleménye szerint a megfelelő technológiai intézkedések végrehajtását csak a felügyelő hatóság kérésére kelljen igazolni, ne automatikusan; ugyanakkor az értelmezhetetlenné tett adatok megsértése nem is feltétlenül jelent adatbiztonsági eseményt.

Várható következmény: szélesebb körű tájékoztatás az adatgazdák részére az adatbiztonsági eseményekkel kapcsolatban, de jelentős *compliance* és IT költségek az adatkezelők érdekkörében, mind az adatbiztonsági eljárások bevezetése, mind gyakorlati megvalósításuk során, és erőteljesen megnövekedett feladatkör az illetékes hatóságok számára.

19. Adatvédelmi hatásvizsgálat (*Data Protection Impact Assesment – „DPIA" / Privacy Impact Assesment*)

A Rendelettervezet a tervezett adatkezelési műveletek személyes adatok védelme tekintetében várható hatásának vizsgálatát írja elő az adatkezelő és az adatfeldolgozó számára, „*ha az adatkezelési műveletek jellegük, alkalmazási területük vagy céljaik tekintetében különleges kockázatot jelentenek az érintettek jogaira és szabadságaira nézve*".[66] Ez az úgynevezett „adatvédelmi hatásvizsgálat" – ismertebb angol nevén a *Data Protection Impact Assesment* – „*DPIA*" / *Privacy Impact Assesment*, amit a gyakorlatban már ma is sok adatkezelő elvégez egy-egy specifikusabb adatkezelési művelet megkezdése előtt.

A fentiek értelmében „különleges kockázatokat" különösen a következő adatkezelési műveletek jelentik a Rendelettervezet szerint:

- „*a természetes személyre vonatkozó egyes személyes szempontok olyan módszeres és átfogó értékelése vagy különösen a természetes személy gazdasági helyzetének, tartózkodási helyének, egészségének, személyes igényeinek, megbízhatóságának vagy viselkedésének olyan elemzése vagy előrejelzése, amelyre automatizált adatkezelésen alapul, és amelyre az érintett személy tekintetében joghatással bíró vagy az egyént jelentős mértékben érintő intézkedések épülnek*"

- „*a szexuális életre, egészségre, fajra vagy etnikai származásra vagy az egészségügyi ellátás nyújtására, járványügyi kutatásokra vagy mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó információk, amennyiben az adatok kezelésére meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor*"

- a „*nyilvánosság számára hozzáférhető területek nyomon követése, különösen optikai-elektronikus eszközök nagyarányú alkalmazásával (videomegfigyelés)*"

- „*a gyermekekre, genetikus vagy biometrikus adatokra vonatkozó széleskörű nyilvántartási rendszerekben tárolt személyes adatok*"

- „*egyéb olyan adatkezelési műveletek, amelyek vonatkozásában konzultálni kell a felügyelő hatósággal* (részletesen lásd a 20. pontot)"

[66] Rendelettervezet 33. cikk

A Rendelettervezet az adatvédelmi hatásvizsgálat elemeit a következőképpen határozza meg: „*a vizsgálat legalább a tervezett adatkezelési műveletek általános leírását, az érintettek jogaira és szabadságaira vonatkozó kockázatok vizsgálatát, a kockázatok kezelésére tervezett intézkedéseket, a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló biztosítékokat, biztonsági intézkedéseket és mechanizmusokat tartalmazza, figyelembe véve az érintettek és más személyek jogait és jogos érdekeit*".

A Rendelettervezet az adatkezelő konzultációs kötelezettségeként előírja továbbá, hogy „*az adatkezelő a kereskedelmi érdekek vagy a közérdek védelme vagy az adatkezelési műveletek biztonságának sérelme nélkül kikéri az érintettek vagy képviselőik véleményét a tervezett adatkezelésről*".

Az ICO Vélemény javasolja a DPIA eredménye összefoglalójának közzétételét, különös tekintettel arra az esetre, ha az adatkezelő közhatalmi szerv; a magánszektor esetében pedig az üzleti titkok és bizalmas információk megfelelő kitakarásával. A 29-es Munkacsoport Véleménye némileg szigorítani javasolja a rendelkezést: kötelezővé tenné a DPIA-t abban az esetben is, ha az adatkezelési műveletek „*valószínűsíthetően*" különleges kockázatot jelentenek. A 29-es Munkacsoport javasolja a DPIA lefolytatását minden típusú különleges adat kezelését megelőzően, a Rendelettervezet által meghatározott feltételek közül pedig törölni javasolja a „széleskörű", „széles körben" és „nagy arányban" megnevezésű feltételeket, mert a 29-es Munkacsoport Véleménye szerint az ilyen adatkezelési műveletek esetében még szűk körű adatkezelés esetén is hatásvizsgálatra van szükség (különös tekintettel a biometrikus adatokra).

A gyakorlatban fennáll ugyanakkor a veszélye, hogy a Rendelettervezet elfogadása esetén a hatóságokat és az érintetteket „elárasztják" a DPIA-k[67] –a Microsoft például 2.000 adatvédelmi hatásvizsgálatot végez évente.

Fontos annak a tisztázása is, hogy pontosan milyen adatkezelési műveletek tartozhatnak a DPIA alá – mi a helyzet például a csalás- és pénzmosás megelőzési, visszaélés-bejelentési rendszerek jogi megítélésével?

Várható következmény: hasonló az adatbiztonsági értesítésekhez - szélesebb körű tájékoztatás az adatgazdák részére az adatkezeléssel kapcsolatban, de jelentős *compliance* és IT költségek az adatkezelők érdekkörében, mind az adatvédelmi hatásvizsgálat lefolytatásához szükséges eljárások bevezetése, mind gyakorlati megvalósításuk során, és erőteljesen megnövekedett feladatkör az illetékes hatóságok számára.

20. Előzetes engedélyezés és konzultáció[68]

Az adatvédelmi nyilvántartásba való általános bejelentkezési kötelezettség eltörlése mellett a Rendelettervezet rögzít néhány olyan kérdést, ahol az illetékes felügyelő hatóságok előzetes engedélye / konzultáció szükséges:

- „*A tervezett adatkezelés e rendelettel való összhangjának biztosítása érdekében a személyes adatok kezelését megelőzően az adatkezelő vagy az adatfeldolgozó kéri a felügyelő hatóság engedélyét, különösen az érintettekre vonatkozó kockázatok csökkentése érdekében, ha az adatkezelő vagy az adatkezelő vagy -feldolgozó és az adat címzettje között létrejött, a felügyelő hatóság által engedélyezett szerződéses*

[67] **The EU's Proposed Data Protection Regulation: Microsoft's Position,**
http://www.microsoft.eu/Portals/0/Document/Technology%20Policy/Microsoft%20position%20on%20EU%20Privacy%20Regulation%20-%20February%202012.pdf

[68] Rendelettervezet 34. cikk

feltételek kerülnek alkalmazásra, vagy az adatkezelő / adatfeldolgozó nem nyújt megfelelő biztosítékokat egy jogilag kötelező eszközben a személyes adatok harmadik országokba vagy valamely nemzetközi szervezet részére történő továbbítása esetén."

- „*Az adatkezelő vagy az adatkezelő nevében eljáró adatfeldolgozó a tervezett adatkezelés és a rendelet közötti összhang biztosítása, valamint különösen az érintettekre vonatkozó kockázatok csökkentése érdekében a személyes adatok kezelését megelőzően konzultál a felügyelő hatósággal, amennyiben:*

  a) az adatvédelmi hatásvizsgálat azt jelzi, hogy az adatkezelési műveletek jellegüknél, alkalmazási területüknél vagy céljaiknál fogva várhatóan magas szintű különleges kockázatot jelentenek; vagy

  b) a felügyelő hatóság szükségesnek tartja az olyan – a hatóság által meghatározott – adatkezelési műveletekről szóló előzetes konzultációt, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva valószínűleg különleges kockázatot jelentenek az érintettek jogai és szabadságai tekintetében."

- „*Amennyiben a felügyelő hatóság véleménye szerint a tervezett adatkezelés nem áll összhangban a rendelettel, különösen, ha a kockázatokat elégtelen módon azonosították vagy csökkentették, megtiltja a tervezett adatkezelést, és megfelelő javaslatot tesz az összhang helyreállítására."*

Az ICO Véleménye szerint a harmadik országokba történő adattovábbítás ma már mindennapos, és az ICO gyakorlatában nem merültek fel ezzel kapcsolatban eddig jelentős jogsértések. Az előzetes engedélyezés kötelezettsége ezért ebben a tekintetben csak túlzott bürokráciát jelenthet – az adatkezelőknek maguk kellene biztosítaniuk az „elszámoltathatóságon" keresztül a jogi megfelelőséget.

Várható következmény: szélesebb körű tájékoztatás az adatgazdák részére az adatkezeléssel kapcsolatban, jelentős *compliance* és IT költségek az adatkezelők számára az engedélyezési eljárások során.

21. Az adatvédelmi felelős[69]

Az EU-ban a Hatályos Irányelv alapján egyelőre nincs egységes követelményrendszer az adatvédelmi felelős kötelező kinevezésére. Németországban például tíz munkavállaló esetén kötelező, míg máshol – például Magyarországon – csak bizonyos iparágakban a belső adatvédelmi felelős kinevezése.

A Rendelettervezet a Hatályos Irányelvnél jóval szigorúbban jelöli meg az adatvédelmi felelős kötelező kijelölésének körét, mely a következő esetekben szükséges:

„*a) az adatkezelést hatóság vagy állami szerv végzi; vagy*

b) az adatkezelést legalább 250 alkalmazottat foglalkoztató vállalkozás végzi - a vállalkozások társulásai egy adatvédelmi felelőst jelölhetnek ki (könnyítés, hogy vállalkozások csoportja egy adatvédelmi felelőst nevezhet ki); vagy

[69] Rendelettervezet 35. cikk

c) az adatkezelő vagy -feldolgozó fő tevékenységei olyan adatkezelési eljárásokat foglalnak magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű nyomon követését igénylik."

A Rendelettervezet általános jelleggel határozza meg az adatvédelmi felelőstől elvárt képesítést: „*a szakértői ismeretek szükséges szintjét kifejezetten az adatkezelő vagy -feldolgozó által végzett adatfeldolgozás, valamint az általuk feldolgozott személyes adatok tekintetében megkövetelt védelem határozza meg*".

Az adatvédelmi felelős az adatkezelő vagy -feldolgozó alkalmazásában állhat, vagy szolgáltatási szerződés keretében láthatja el feladatait. Az adatvédelmi felelős feladata többek között az adatkezelési műveletek dokumentációjának biztosítása, az adatbiztonsági értesítésekkel kapcsolatos dokumentáció, értesítés és tájékoztatás ellenőrzése, valamint az adatvédelmi hatásvizsgálat és az előzetes hatósági engedélyezés vagy előzetes konzultáció alkalmazásának ellenőrzése.

Fontos az adatvédelmi felelős függetlensége: „*az adatkezelő vagy -feldolgozó biztosítja, hogy az adatvédelmi felelős minden egyéb szakmai kötelezettsége összeegyeztethető legyen az adott személy adatvédelmi felelősként ellátandó feladataival és kötelezettségeivel, és nem eredményez összeférhetetlenséget. Az adatkezelő vagy -feldolgozó az adatvédelmi felelőst legalább 2 éves időtartamra jelöli ki. Az adatvédelmi felelős további időtartamra ismételten kijelölhető. Az adatvédelmi felelőst hivatali ideje alatt csak akkor lehet felmenteni, ha már nem felel meg a feladatai ellátásához szükséges feltételeknek. Az adatkezelő vagy -feldolgozó biztosítja, hogy az adatvédelmi felelős a feladatokat és kötelezettségeket függetlenül látja el, és azok ellátásával kapcsolatosan senkitől nem fogad el utasításokat. Az adatvédelmi felelős közvetlenül az adatkezelő vagy -feldolgozó vezetésének tesz jelentést. Az adatkezelő vagy -feldolgozó az adatvédelmi felelőst támogatja feladatai ellátásában, és biztosítja számára feladatai és kötelezettségei végrehajtásához szükséges személyzetet, helyiségeket, felszerelést és egyéb forrásokat.*"[70]

Az ICO Véleménye szerint nem feltétlenül szükséges kötelezővé tenni az adatvédelmi felelős kinevezését, ha az adatvédelmi megfelelőség egyéb megfelelő módon biztosítható. Az adatvédelmi felelős kinevezésének hiánya viszont jogsértés esetén súlyosbító körülmény lehet a szankció kiszabásakor. Az adatvédelmi felelős feladatai – az adott adatkezelő szervezeti felépítésétől függően – akár több pozícióhoz, területhez is tartozhatnak. Az sem feltétlenül indokolt, hogy az adatvédelmi felelős kinevezése a munkavállalók számához kötődjön – előfordulhat, hogy nagyszámú személyzettel rendelkező adatkezelő csak alacsony kockázatú adatkezelési tevékenységet folytat. Internetes cégek ugyanakkor kevés munkavállalóval is működnek, viszont jelentős mennyiségű adatot kezelnek. Célszerűbb lehet tehát a kezelt adatok mennyiségéhez / természetéhez kötni az adatvédelmi felelős kinevezésének kötelezettségét. Ebbe az irányba mozdul el az EP Javaslat is, amely 500-nál kevesebb személy (évi szinten történő) személyes adatának kezelése esetén adna mentesülést az adatvédelmi felelős kötelező kinevezése alól – a kinevezés időtartamát ugyanakkor 4 évre növelné. A bírálatokra válaszul Viviane Reding 2012. november 29-én sajtótájékoztatón elismerte, hogy a fokozottabb kockázattal járó adatkezelési tevékenységek KKV-k esetén is indokolhatják az adatvédelmi felelős kötelező kinevezését.[71]

További kérdés, hogy hogyan vizsgálják a felügyelő hatóságok az adatvédelmi felelős képzettségét, valamint, hogy megvalósítható a „függetlenség" egy munkaszervezeten belül

[70] Rendelettevezet, 36. cikk (2)-(3)

[71] **EU: Commissioner Reding: risky activities could justify DPO appointment for SMEs**, http://www.dataguidance.com/news.asp?id=1915

– az ICO Véleménye elképzelhetőnek tartja, hogy az adatvédelmi felelős szerepét egy, a felsővezetésbe tartozó „*Chief Privacy Officer*” tölti be, aki a döntéshozatalra is nagyobb hatással lehet, mint egy alacsonyabb pozícióban levő, de kvázi független munkavállaló.

Várható következmény: átláthatóbb adatkezelés és nagyobb adatvédelmi megfelelőség a szervezeten belül, ugyanakkor a feladat ellátásával kapcsolatos költségek növekedése.

22. Adattovábbítás harmadik országokba

A Rendelettervezet kifejezett célja, hogy gyakorlatiasabbá és átláthatóbbá tegye a nemzetközi (EGT-n kívüli, az EGT-vel megegyező megfelelő szintű adatvédelmet nem biztosító országokba történő) adattovábbításokat. Új elem a Hatályos Irányelvhez képest a kötelező erejű vállalati szabályok kifejezett nevesítése és kötelező elemeik meghatározása és vélhetően ez váltja fel az EU/USA Safe Harbor rendszert is, ami már nem kerül nevesítésre a Rendelettervezetben.

Ilyen jellegű adattovábbítás a Rendelettervezet szerint az alábbiak szerint történhet:

22.1 Adattovábbítás „megfelelőségi határozat” alapján[72]

Ebben az esetben „*akkor kerülhet sor adattovábbításra, ha a Bizottság megállapítja, hogy a harmadik ország, annak régiója vagy adatfeldolgozó ágazata, illetve a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges további engedély*.” Erre várhatóan nem sok ország esetében lehet hivatkozni – a Hatályos Irányelv alapján a Bizottság eddig is csak néhány országot minősített „megfelelőnek” (Argentína, Kanada, Guernsey, Isle of Man, Izrael, Svájc és Uruguay).

22.2 Adattovábbítás megfelelő biztosítékok alapján[73]

Ha nem áll rendelkezésre megfelelőségi határozat, a Rendelettervezet szerint „*az adatkezelő vagy -feldolgozó csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha a személyes adatok védelme tekintetében az adatkezelő vagy -feldolgozó megfelelő biztosítékokat nyújt jogilag kötelező eszköz útján*.”

A „*megfelelő biztosítékok*” a Rendelettervezet értelmében különösen az alábbiak:

a) az illetékes adatvédelmi hatóság által jóváhagyott, a rendeletben felsorolt kötelező elemeket tartalmazó kötelező erejű vállalati szabályok (*Binding Corporate Rules – BCR*); vagy

b) a Bizottság által elfogadott, úgynevezett általános adatvédelmi előírások (*standard data protection clauses*); vagy

c) valamely tagállami hatóság által elfogadott, úgynevezett általános adatvédelmi előírások (*standard data protection clauses*)[74]; ha azokat a Bizottság általánosan érvényesnek nyilvánítja; vagy

d) az adatkezelő vagy -feldolgozó és az adat címzettje között létrejött, az illetékes adatvédelmi hatóság által engedélyezett szerződéses feltételek.

[72] Rendelettervezet 41. cikk

[73] Rendelettervezet 42. cikk

[74] A Rendelettervezet magyar fordítása itt némileg pontatlan.

A kötelező erejű vállalati szabályokon vagy a b) és c) pontokban említett egységes adatvédelmi feltételeken alapuló adattovábbítás esetében nincs szükség további engedélyre. Ha a személyes adatok védelmére jogilag kötelező eszközben nem nyújtanak megfelelő biztosítékokat, az adatkezelőnek vagy -feldolgozónak előzetes engedélyt kell szerezni az adattovábbításra a felügyelő hatóságtól.

22.3 Adattovábbítás egyéb módon[75]

Megfelelőségi határozat, illetve megfelelő biztosítékok hiányában a személyes adatok harmadik országba történő továbbítására a következő esetekben kerülhet sor:

„*a) az érintett hozzájárulását adta a tervezett továbbításhoz, miután tájékoztatták az ilyen továbbításnak a megfelelőségről szóló határozat és a megfelelő biztosítékok hiányából fakadó kockázatairól; vagy*

b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy

c) a továbbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy

d) a továbbítás fontos közérdekből szükséges; vagy

e) a továbbítás jogi követelések létrejötte, érvényesítése vagy védelme miatt szükséges; vagy

f) a továbbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására; vagy

g) a továbbítást olyan nyilvántartásból végzik, amely az uniós vagy nemzeti jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben az uniós vagy nemzeti jog által a betekintésre megállapított feltételek az adott esetben teljesülnek; vagy

h) a továbbítás az adatkezelő vagy -feldolgozó jogos érdekében szükséges, amely nem minősíthető gyakorinak vagy tömegesnek, amennyiben az adatkezelő vagy -feldolgozó az adattovábbítás vagy az adattovábbítás-sorozat minden körülményét megvizsgálta, és e vizsgálat alapján szükség szerint megfelelő biztosítékokat hozott létre a személyes adatokra tekintettel. Az adatkezelő vagy - feldolgozó különös figyelmet fordít az adatok jellegére, a tervezett feldolgozási művelet vagy műveletek céljára és időtartamára, valamint a kiindulási ország, a harmadik ország és a célország szerinti helyzetre, valamint szükség szerint a személyes adatok védelme tekintetében biztosított megfelelő biztosítékokra. Az adatkezelő vagy -feldolgozó a 16. pont szerinti dokumentációban dokumentálja a vizsgálatot és a megfelelő biztosítékokat, ezen túlmenően a továbbításról értesíti a felügyelő hatóságot.”

[75] A magyar fordítás ismét pontatlan: a feltételek érvényességéhez az angol szövegben nem szereplő „tagállami előírások” meglétére utal.

A 29-es Munkacsoport Véleményében az adatkezelő vagy -feldolgozó jogos érdekében szükséges adattovábbításokkal kapcsolatban javasolja, hogy kerüljön rögzítésre: kétoldalú, kölcsönös jogsegély-egyezmény vagy egyéb nemzetközi megállapodás hiányában ne legyen lehetőség peres eljárások során tömeges, gyakori és strukturális jellegű adattovábbításokra. Ez érintheti az USA-ba történő elektronikus adattovábbításokat, az ottani peres eljárások során történő bizonyítási célból (*discovery*, illetve *e-discovery* – az ezzel kapcsolatos gyakorlatot lásd még a III.3 pontban*)*. Az ICO Véleménye itt a Hatályos Irányelv rendelkezéseihez való visszatérést javasolja, és az EP Javaslat is hasonló megközelítést alkalmaz.

Nem tartja továbbá szükségesnek az ICO a BCR-ok felügyelő hatóságok általi előzetes jóváhagyását – a javaslat szerint a hatóságoknak ehelyett iránymutatásokat kellene adniuk a BCR-ok megfelelő elkészítéséhez. Az ICO Véleménye külön bírálja a rendkívül széles körben értelmezhető „nem gyakori vagy tömeges" kivételi kör bevezetését.

Várható következmény: a harmadik országokba történő adattovábbítás dokumentálásával és engedélyeztetésével kapcsolatos megnövekedett feladatmennyiség az adatkezelők és az illetékes hatóságok számára, valamint gyakorlati nehézségek a „legjobb gyakorlatok" kidolgozása során.

23. A Rendelettervezet végrehajtása

A Rendelettervezet a Hatályos Irányelvhez képest jelentősen megváltozott struktúrában határozza meg az adatvédelmi jogszabályok végrehajtását. Régi elvárás, hogy az adatvédelmi felügyelő hatóságoknak a mostani eszközrendszerükhöz képest sokkal hatékonyabban kell érvényesíteniük az adatvédelmi jogszabályoknak való megfelelést. A Rendelettervezet értelmében a végrehajtásnak három fő eleme van: (i) egy bizonyos ügyben egy hatóság illetékes és jár el; (ii) a többi tagállam felügyelő hatósága ezzel összefüggésben közreműködik; és (iii) fontos szerep jut a 29-es Munkacsoportnak is. A Rendelettervezet által bevezetett új rendelkezésekkel és a végrehajtásukat felügyelő szervekkel kapcsolatban ugyanakkor a fő kérdés, hogy lesznek-e megfelelő anyagi és személyi erőforrások akár közösségi, akár tagállami szinten az elfogadásra kerülő szabályok megfelelő végrehajtására?

23.1 Az Európai Adatvédelmi Testület

A Rendelettervezet szerint a 29-es Munkacsoport utódaként létrejön az Európai Adatvédelmi Testület (*European Data Protection Board*), amely minden tagállam egy felügyelő hatóságának vezetőjéből és az európai adatvédelmi biztosból áll.[76] Az Európai Adatvédelmi Testület saját titkársággal rendelkezik, melyet az európai adatvédelmi biztos biztosít.

Az Európai Adatvédelmi Testület feladatai alapvetően a következők:

- adatvédelmi tanáccsal látja el a Bizottságot
- a rendelet következetes alkalmazásának elősegítése érdekében iránymutatásokat, ajánlásokat és bevált módszereket dolgoz ki, és vizsgálja gyakorlati alkalmazásukat;
- véleményezi az egységességi mechanizmus értelmében a felügyelő hatóságok határozattervezeteit; és
- előmozdítja a felügyelő hatóságok közötti együttműködést, információcserét, közös képzési programokat.

[76] Rendelettervezet 64. cikk

Az Európai Adatvédelmi Testület működése ugyanakkor további részletszabályok elfogadását igényli: a Rendelettervezet nem szabályozza például az Európai Adatvédelmi Testület elszámoltathatóságát, vagyis milyen jogorvoslat kereshető abban az esetben, ha nem az érdekelt felek érdekeivel ellentétes gyakorlatot folytat.

23.2 Az adatvédelmi hatóságok

A Hatályos Irányelvhez hasonlóan a Rendelettervezet is meghatározza a tagállami adatvédelmi hatóságok kinevezésének alapvető feltételeit, különös tekintettel azok függetlenségére. (A Bíróság két esetben is vizsgálta már a tagállami adatvédelmi hatóságok függetlenségét: a C-614/10. számú ügyben (Ausztria) és a C–518/07. számú ügyben (Németország), mindkét alkalommal elmarasztalva az érintett tagállamot. Jelenleg Magyarország ellen folyik eljárás ugyanebben a tárgyban.)

A Rendelettervezet szerint[77] a tagállami adatvédelmi hatóságok alapvető feladatai a következők:

- ellenőrzik és biztosítják a rendelet alkalmazását;
- foglalkoznak az adatvédelmi panaszokkal;
- információmegosztás és kölcsönös segítségnyújtás más felügyelő hatóságokkal;
- vizsgálatot folytatnak le;
- figyelemmel kísérik a személyes adatok védelmére kiható jelentősebb fejleményeket, különösen az információtechnológia és a hírközlési technológia, valamint a kereskedelmi gyakorlatok fejlődését;
- egyeztetnek a tagállami intézményekkel és szervekkel a jogalkotási és közigazgatási intézkedésekről;
- engedélyezik a rendelet értelmében engedélyköteles adatkezelési műveleteket (lásd részletesen a fenti 20. pontot);
- jóváhagyják a kötelező erejű vállalati szabályokat.

Valamennyi felügyelő hatóság vizsgálati hatáskörrel rendelkezik a következők szerint:

- betekintés a feladatainak teljesítéséhez szükséges valamennyi személyes adatba és információba;
- belépés az adatkezelő vagy -feldolgozó bármely helyiségébe, hozzáférés az adatfeldolgozó eszközökhöz, ha alapos indokok alapján feltételezhető, hogy a rendelet megsértésével járó tevékenység zajlik.

A 29-es Munkacsoport Véleménye felhívja a figyelmet, hogy a fenti rendelkezés pontosításra szorul: a felügyelő hatóságoknak vizsgálati jogkörük mellett kifejezetten lehetőséget kell adni ellenőrzések elvégzésére is.

A Rendelettervezet szerint a felügyelő hatóságok hatáskörüket tagállamuk területén gyakorolják. A különböző tagállami hatóságok közös vizsgálati feladatokat, közös végrehajtási intézkedéseket és közös műveleteket hajthatnak végre.[78] Határon átnyúló együttműködésre már most is van példa a felügyelő hatóságok között: az észt és a litván adatvédelmi hatóság együttesen vizsgálta például a Stockmann Group munkavállalói- és ügyféladatok kezelésével kapcsolatos gyakorlatát. Hasonló ügy volt a Google módosított adatvédelmi szabályainak a francia adatvédelmi hatóság (*Commission nationale de*

[77] Rendelettervezet 52. cikk

[78] Rendelettervezet 55. cikk

l'informatique et des libertés - CNIL) vezetésével végzett vizsgálata is.[79] Sőt, transzatlanti együttműködésre is sor került: a WhatsApp nevű adatkezelő mobil üzenetküldő platformjának adatvédelmi vizsgálatát (felhasználói kontaktlisták felhasználása és megőrzése, megfelelő adatbiztonsági intézkedések – az üzenetek titkosításának – hiánya, valamint könnyen visszafejthető jelszavak generálása) a holland (*College Bescherming Persoonsgegevens - CBP*) és a kanadai (*Office of the Privacy Commissioner of Canada – OPC*) adatvédelmi hatóság közösen végezte.[80]

A Hatályos Irányelvhez hasonlóan a Rendelettervezet is biztosítja az adatvédelmi hatósággal szembeni bírósági jogorvoslathoz való jogot.

23.3 Panasztétel a felügyelő hatóságnál

A Hatályos Irányelvhez hasonlóan jogellenes adatkezelés esetén az érintett személyek jogosultak panaszt emelni bármely tagállam adatvédelmi hatóságánál. Újdonság, hogy erre egyéb olyan szervek, szervezetek, egyesületek is jogosultak, akiknek célja a személyes adatok védelmére vonatkozó jogok védelme - akár az érintett nevében, akár önállóan.

23.4 A kártérítéshez való jog és a felelősség[81]

A Rendelettervezet nem csak az adatkezelők, hanem az adatfeldolgozók felelősségét is rögzíti. A Rendelettervezet szerint „*minden olyan személy, aki jogellenes adatfeldolgozási művelet vagy a rendelettel összeegyeztethetetlen cselekmény eredményeként kárt szenvedett, az elszenvedett károkért az adatkezelővel vagy -feldolgozóval szemben kártérítésre jogosult. Amennyiben az adatfeldolgozásban egynél több adatkezelő vagy -feldolgozó vesz részt, minden adatkezelő vagy -feldolgozó egyetemlegesen felel a kár teljes összegéért. Az adatkezelő vagy -feldolgozó részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős*."

A fentiek mellett – a Hatályos Irányelvhez hasonlóan - a Rendelettervezet is biztosítja az adatkezelővel vagy - feldolgozóval szembeni bírósági jogorvoslathoz való jogot az adatgazdák számára.

23.5 Közigazgatási szankciók

„*We like the idea of fines*." (*Françoise Le Bail,* Európai Bizottság Jogérvényesülési Főigazgatóság, az International Association of Privacy Professionals konferenciáján)

„*This is not about taking the scalp of a big company. It's about pushing them to come into conformity.*" (Isabelle Falque- Pierrotin, CNIL, a New York Times cikkében)[82]

A Rendelettervezet az adatvédelmi hatóságokat széles körű szankcionálási joggal ruházza fel. Jelenleg nincs egységes európai gyakorlata annak, hogy az egyes tagállami adatvédelmi hatóságok jogosultak-e pénzbírságot kiszabni – a Rendelettervezet ezt a jogosultságot emeli jogszabályi szintre. A bírság kiszabásának alapelveiként a Rendelettervezet az illetékesek fent idézett nyilatkozataival szemben némileg részletesebben rögzíti, hogy „*a szankcióknak*

---

[79] **Google's new privacy policy raises deep concerns about data protection and the respect of the European law**, http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/

[80] **News Release - WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities**, http://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp

[81] Rendelettervezet 77. cikk

[82] **Guarding a 'Fundamental Right' of Privacy in Europe** http://www.nytimes.com/2012/11/21/technology/guarding-a-fundamental-right-of-privacy-in-europe.html?_r=0

minden egyes esetben hatékonynak, arányosnak és visszatartó erejűnek kell lenniük. A bírság összegének meghatározása során kellő figyelmet kell fordítani a jogsértés jellegére, súlyosságára és időtartamára, a jogsértés szándékos vagy gondatlan jellegére, a természetes vagy jogi személy felelősségének szintjére és az e személy által korábban megvalósított jogsértésekre, a rendelet szerint alkalmazott technikai és szervezeti intézkedésekre és eljárásokra, valamint a felügyelő hatóságokkal a jogsértés orvoslása érdekében megvalósított együttműködés szintjére."[83]

A szankcionálás négy lépcsőben valósulhat meg, az alábbiak szerint:

(A) Első lépcső

„*A rendeletnek való első és nem szándékos meg nem felelés esetén írásbeli figyelmeztetést bocsátható ki és mellőzhető a szankció kiszabása, amennyiben:*

(a) a természetes személy kereskedelmi érdek nélkül kezel személyes adatokat; vagy

(b) a 250 főnél kevesebb főt foglalkoztató vállalkozás vagy szervezet, amely személyes adatokat csak a főtevékenységét kiegészítő melléktevékenységként kezel."[84]

(B) Második lépcső

„*A felügyelő hatóság **250.000 euróig terjedő bírságot** alkalmaz, vagy vállalkozás esetén az **éves világméretű forgalom legfeljebb 0,5%-át**, azzal szemben, aki szándékosan vagy gondatlanságból:*

a) nem hozza létre az érintettek kérelmeihez kapcsolódó mechanizmusokat, vagy az érintetteknek nem válaszol haladéktalanul, vagy nem a megfelelő formátumban, az érintettek jogainak gyakorlásával összefüggésben; vagy

b) a rendelet megsértésével díjat számít fel az érintettek tájékoztatásáért vagy a kérelmeik megválaszolásáért."[85]

(C) Harmadik lépcső

„*A felügyelő hatóság **500.000 euróig terjedő bírságot** alkalmaz, vagy vállalkozás esetén az **éves világméretű forgalom legfeljebb 1%-át**, azzal szemben, aki szándékosan vagy gondatlanságból:*

a) nem, vagy hiányosan, vagy nem megfelelően átlátható módon bocsátja az érintett rendelkezésére az adatkezeléssel kapcsolatos, a rendeletben előírt információt;

b) nem biztosítja az érintett számára hozzáférést vagy nem helyesbíti a személyes adatokat, vagy nem értesíti a címzettet a vonatkozó információkról valamennyi törlésről vagy zárolásról;

[83] Rendelettervezet 79. cikk (2)

[84] Rendelettervezet 79. cikk (3)

[85] Rendelettervezet 79. cikk (4)

c) nem tesz eleget a személyes adatok tárolásának megszüntetéséhez vagy a törléshez való jognak, vagy elmulasztja a határidők nyomon követésére szolgáló mechanizmusok létrehozását, vagy nem teszi meg a szükséges lépéseket annak érdekében, hogy tájékoztassa a harmadik feleket az érintetteknek link, másolat vagy másodpéldány törlésére irányuló kérelméről a felejtéshez való jog szerint;

d) az adathordozhatósághoz való jog megsértésével nem bocsátja elektronikus formában rendelkezésre a személyes adatok másolatát, vagy megakadályozza az érintettet a személyes adatok más alkalmazásba való továbbításában;

e) nem vagy nem kellőképpen határozza meg a közös adatkezelők vonatkozó kötelezettségeit;

f) nem vagy nem kellőképpen vezeti az elszámoltathatósággal kapcsolatos általános dokumentációt, az adatbiztonsági eseményekkel kapcsolatos, vagy a jogos érdeken alapuló adattovábbításokkal kapcsolatos dokumentációt;

g) az adatok különös kategóriáit nem érintő esetekben nem tesz eleget a véleménynyilvánítás szabadságához kapcsolódó szabályoknak, vagy a foglalkoztatással összefüggő adatkezeléshez kapcsolódó szabályoknak, vagy a történelmi, statisztikai vagy tudományos kutatási célú adatkezelés feltételeinek."[86]

(D) Negyedik lépcső

„*A felügyelő hatóság **1.000.000 euróig terjedő bírságot** alkalmaz, vagy vállalkozás esetén az **éves világméretű forgalom legfeljebb 2%-át**, azzal szemben, aki szándékosan vagy gondatlanságból:*

a) a személyes adatok kezelését az adatkezeléshez szükséges jogalap nélkül vagy megfelelő jogalap nélkül végzi, vagy nem tesz eleget a rendelet szerinti hozzájárulás feltételeinek;

b) a rendelet megsértésével dolgozza fel az adatok különös kategóriáit;

c) nem tesz eleget a kifogásolásnak vagy a kifogáshoz való jog érvényesítésével kapcsolatos követelményeknek;

d) nem tesz eleget a profilalkotáson alapuló mechanizmusok feltételeinek;

e) nem fogadja el azokat a belső szabályzatokat vagy nem alkalmazza azokat a megfelelő intézkedéseket, amelyek biztosítják és igazolják az adatkezelő felelősségét, a beépített és alapértelmezett adatvédelemre, valamint az adatkezelés biztonságára vonatkozó körülményekkel való összhangot;

f) a nem az Unió területén letelepedett adatkezelő nem jelöli ki az uniós képviselőt;

[86] Rendelettervezet 79. cikk (5)

g) az adatkezelő nevében végzett feldolgozáshoz kapcsolódó kötelezettségek megsértésével dolgozza fel a személyes adatokat vagy irányítja azok kezelését;

h) nem, vagy nem időben vagy nem teljes mértékben figyelmezteti vagy értesíti a felügyelő hatóságot vagy az érintettet a személyes adatok megsértéséről;

i) nem végez adatvédelmi hatásvizsgálatot, vagy a felügyelő hatóság előzetes engedélyezése vagy a vele való előzetes konzultáció nélkül kezel személyes adatot;

j) nem jelöl ki adatvédelmi felelőst, vagy nem biztosítja a feladatai ellátásához szükséges feltételeket;

k) visszaél az alkalmazott adatvédelmi szintet igazoló adatvédelmi címkével vagy jelzővel;

l) olyan harmadik országba vagy nemzetközi szervezet részére végez vagy irányít adattovábbítást, amelyet nem engedélyeztek megfelelőségi határozattal, vagy megfelelő biztosítékok, vagy eltérés alapján;

m) nem tesz eleget a felügyelő hatóság utasításának vagy az adatkezelés átmeneti vagy végleges tilalmára vagy az adatáramlás felfüggesztésére vonatkozó felszólításának;

n) nem tesz eleget azon kötelezettségének, hogy a felügyelő hatóságot támogassa, válaszoljon neki vagy rendelkezésére bocsássa a vonatkozó információkat, vagy belépést biztosítson a helyiségeibe;

o) nem tesz eleget a szakmai titoktartás biztosítására vonatkozó szabályoknak."[87]

Általánosságban megállapítható, hogy a Rendelettervezet szankcionálásra vonatkozó rendelkezései meglehetősen szigorúak. Becslések szerint[88] egy Microsoft méretű cégnek a 2 %-os büntetési tétel például 2008-ban 1,2 milliárd amerikai dollár összeget jelent. A szankciókra vonatkozó részből hiányzik a versenyjogi szabályozáshoz hasonló engedékenységi (*leniency*) politika. Az új rendelkezéseket a 29-es Munkacsoport Véleménye is szigorúnak tartja: javaslata szerint a felügyelő hatóságoknak mérlegelési jogkörrel kell rendelkezniük annak eldöntése tekintetében, hogy kiszabnak-e bírságot, mivel sok olyan tényező befolyásolja a jogsértés jellegét, amelyet figyelembe kell venni a bírság kiszabásakor. Több felügyelő hatóság hatásköre esetén felmerülhet a kétszeres büntetés (*non bis in idem*) tilalmának megsértése. Kérdés az is, hogy a gyakorlatban hogyan működik majd a tagállami jogszabályok értelmezése: például hogyan fogja értelmezni egy, az adatkezelő fő szervezete tekintetében illetékes hatóság valamely leányvállalat tevékenységével összefüggő helyi jogszabályokat?

Várható következmény: nagyobb adatvédelmi megfelelőség, a bírságok magas és elrettentő jellege miatt, ugyanakkor a potenciális bírságok bekalkulálása az adatkezelők árazásába.

[87] Rendelettervezet 79. cikk (5)

[88] **6 things you need to know about the new eu privacy framework**, http://www.donneespersonnelles.fr/6-things-you-need-to-know-about-the-new-eu-privacy-framework

23.6 Felhatalmazáson alapuló, valamint végrehajtási aktusok

Az EU működéséről szóló Szerződés 290. cikke alapján a Bizottság általános hatályú nem jogalkotási aktusokat (*delegated acts*) fogadhat el, amelyek a rendelet egyes nem alapvető rendelkezéseit kiegészítik, illetve módosítják. A tagállamok nemzeti jogukban elfogadják a kötelező erejű uniós jogi aktusok végrehajtásához szükséges intézkedéseket, illetve ha a végrehajtásnak egységes feltételek szerint kell történnie, a vonatkozó jogi aktus végrehajtási hatásköröket ruház a Bizottságra (*implementing acts*). A Rendelettervezetben szabályozott kérdések végrehajtásának részletes szabályai sok kérdésben a fent említett, úgynevezett „elhatalmazáson alapuló", valamint „végrehajtási" aktusokban kerülnek meghatározásra. A 29-es Munkacsoport 2012 októberében elfogadott 08/2012. számú véleményében elemezte részletesen a felhatalmazáson alapuló, valamint a végrehajtási aktusok szükségességét. Általánosságban megállapítható, hogy a Rendelettervezet nagyon sok kérdést utal ilyen szabályozási körbe, ami az egységes, európai szintű jogszabályi rendelkezések szétaprózódásához vezethet.

Várható következmény: számos részletszabály kibocsátása (és az ezzel járó politikai viták) a Rendelettervezet elfogadását követően.

III. VÁRHATÓ FEJLEMÉNYEK ÉS KITEKINTÉS AZ USA-RA

1. A tagállamok reakciói

A szabályozási cél, ahogyan a Rendelettervezet 2013 folyamán történő véglegesítéséért felelős Alan Shatter ír igazságügyi- és védelmi miniszter megfogalmazta: „*kemény és gyors jogi védelem, valamint a reklámipar jogszerű és gazdaságilag fontos érdekeinek összehangolása az adatvédelmi kérdésekkel*".[89] A Rendelettervezet ellenzői (például az Egyesült Királyság, ahol a Rendelettervezetet az érintettek egy, az Igazságügyi Minisztérium által indított, úgynevezett „*Call for Evidence*" eljárásban észrevételezhették egy hónapig) szerint ugyanakkor egy rendelet – mint szabályozási forma - nincs tekintettel a tagállami szabályozási és kulturális sajátosságokra. A Miniszterek Tanácsa legutóbbi ülésén[90] ezért az Egyesült Királyság, valamint Dánia, Szlovénia, Belgium, Svédország és Magyarország jelezte: rendelet helyett inkább irányelv formájában javasolják az új adatvédelmi szabályozást. Bulgária, Németország, Spanyolország, Hollandia, Luxemburg, Franciaország, Olaszország, Görögország és Írország viszont támogatja a rendeletet. A rendeletet ellenzők egyik legfőbb érve az irányelvi szinten történő szabályozás mellett, hogy a Rendelettervezet több helyen megengedőbb / szigorúbb adatvédelmi szabályokat tartalmaz, mint a hatályos tagállami szabályozások. A valódi ok azonban vélhetően a tagállami szuverenitás további feladásától való félelem, különös tekintettel a felhatalmazáson alapuló, valamint végrehajtási aktusok nagy számára, és a *one-stop-shop* bevezetésére. A Rendelettervezetet véleményező hatóságok közül a német Rhineland-Palatinate és Hesse szövetségi államok adatvédelmi hatóságai ugyanígy hangsúlyozták, hogy fontos meghagyni a tagállamok szabályozási jogosultságát is. A Rendelettervezet elfogadtatása mellett elkötelezett Viviane Reding uniós biztos felismerte a tagállamok aggályát, és nyilatkozatai szerint „*kész további rugalmasságra*"[91] – vagyis vélhetően a felhatalmazáson alapuló, valamint végrehajtási aktusok számának csökkentésére. A Rendelettervezet 21. cikke ráadásul további eltérési lehetőségeket biztosít a tagállamok

[89] **New Player in E.U. Data Privacy Battle**, http://www.nytimes.com/2012/11/21/technology/new-player-in-eu-data-privacy-battle.html?_r=0

[90] Beszámoló itt: **UK Government opposed to the Commission's Data Protection Regulation**, http://amberhawk.typepad.com/amberhawk/2012/11/uk-government-opposed-to-the-commissions-data-protection-regulation.html

[91] **Viviane Reding Vice-President of the European Commission, EU Justice Commissioner Justice Council: Making good progress on our Justice for Growth agenda Justice Council Press Conference /Luxembourg 26 October 2012**, http://europa.eu/rapid/press-release_SPEECH-12-764_en.htm

számára bizonyos rendelkezésektől közbiztonság, közérdek, illetve az érintett vagy mások jogainak és szabadságának védelme céljából, valamint egyéb, a fenti indokokhoz hasonlóan rugalmasan értelmezhető okokból, így a rendeleti szinten történő szabályozás mellett megmaradhat a tagállamok mozgástere is.

2. Az adatkezelők reakciói – adatvédelmi szint, költségek, hatály

Az előbb említett kritikus tagállami reakcióktól eltérően a Rendelettervezetet bíráló piaci szereplők, adatkezelők legfőbb aggálya, hogy a Rendelettervezet egyes tagállamok – például az Egyesült Királyság – „adatkezelő-barát" szabályainál szigorúbb rendelkezéseket vezet be, és ezzel fékezheti az internetes gazdaság, az elektronikus kereskedelem fejlődését, végső soron csökkentve ezzel a munkahelyek számát. „*Évek óta szorgalmazzuk az adatvédelmi jogszabályok harmonizációját, de aggódunk, hogy a javaslat túl korlátozó*." – nyilatkozta a Microsoft Europe-ot képviselő Ron Zink belső jogász.[92] Szintén ő emelte ki a rendelet végrehajtásával kapcsolatban az önszabályozás fontosságát: „*minél többet bízunk a technológiai cégekre, annál jobb*".[93]

Fontos a Rendelettervezet elfogadása esetén az adatkezelők számára felmerülő költségek figyelembevétele. A Bizottság szerint az új szabályok bevezetése összességében 2,3 milliárd EUR költségcsökkentést eredményezhet a Rendelettervezet hatálya alá eső adatkezelők számára[94], és csak az adatvédelmi nyilvántartásba való bejelentési kötelezettség megszüntetése évente összességében 130 millió euró spórolásához vezet.[95] Helen Grant angol igazságügyi miniszter becslése szerint ugyanakkor az angol cégek számára a kezdeti megfelelés költsége 100 millió angol font és 360 millió angol font közé tehető, csak az éves megfelelőségi költség pedig 10 millió angol font. A túl sok dokumentációs kötelezettséget és a hozzájárulás-centrikus megközelítésre fókuszáló, Rendelettervezet elfogadásának eredménye így „*extra bürokrácia és kattintós compliance*" („*extra red-tape and tick box compliance*") lehet, ráadásul a hozzájárulás pedig nem jelenti egyúttal automatikusan az adatgazda megfelelő tájékoztatáson alapuló döntését.[96] A Bizottság becslése ugyanis csak az adminisztratív költségek csökkentésével számolt, de nem vizsgálja például a felügyelő hatóság irányába teljesítendő befizetéseket, az adatvédelmi felelősök kötelező kinevezésének költségét és az adatvédelmi hatásvizsgálatok költségeit.[97] A UK Confederation of British Industry (CBI) elemzése szerint például a független belső adatvédelmi felelős két évre történő kinevezésének költsége évente 30.000 angol font és 75.000 angol font között mozog. A megfelelés költségvonzata különösen fontos lehet a sokszor kisebb jelentőségű, alacsony kockázatú, rutinszerű adatkezeléseket végző KKV-k számára.

A globális szinten működő adatkezelők különösen aggályosnak tartják a Rendelettervezet extraterritoriális hatályát: a Rendelettervezet bírálói szerint az EU-s szabályok betartása ésszerűtlenül nehézkes lehet egy EU-n kívül működő adatkezelőnek, különös tekintettel arra, hogy az EU adatvédelmi szabályai jelentősen és a gyakorlatban nem mindig indokolt mértékben eltérhetnek más országok – különösen az USA – szabályaitól, vagy az iparági

---

[92] **New EU privacy rules worry business**, http://www.ft.com/cms/s/2/e14f2f3e-44f3-11e1-be2b-00144feabdc0.html

[93] **EU: Industry reacts to the EU draft Regulation**, http://dataguidance.com/news.asp?id=1708

[94] **Commission proposes a comprehensive reform of the data protection rules**, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[95] **Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design Munich, 22 January 2012**, http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm?locale=en

[96] **UK Concerned about Economic Impact of European Data Protection Reform Proposals**, http://www.huntonprivacyblog.com/2012/11/articles/uk-concerned-about-economic-impact-of-european-data-protection-reform-proposals/

[97] **Written Ministerial Statement**, http://www.parliament.uk/documents/commons-vote-office/November_2012/22-11-12/7-Justice-DataProtection.pdf

„legjobb gyakorlattól". A legnagyobb adatkezelők – technológiai cégek, közösségi oldalak – mind az USA-ban, mind az EU-ban működnek, és jogosan várhatják el a jogalkotóktól az adatvédelmi szabályok közelítését. Egyre gyakoribb, hogy egy-egy világszerte hozzáférhető szolgáltatást az EU valamely tagállamának adatvédelmi hatósága jogellenesnek talál. Ilyen például a Google módosított adatvédelmi szabályainak a CNIL vezetésével végzett vizsgálata esetén. További példa: a Facebook „Friend Finder" – a felhasználó e-mail címlistáját felhasználó – funkcióját egy német bíróság tartotta a helyi adatvédelmi jogszabályokba ütközőnek, mert a felhasználókat nem tájékoztatták megfelelően erről a funkcióról. Szintén jogellenesnek minősült a Facebook azon felhasználási feltétele, miszerint tulajdonjogot szerez a Facebook-ra feltöltött személyes adatok felett, és egyéb célokra is felhasználhatja azokat. Egy súlyosabb eset: 2010. február 24-én az illetékes olasz bíróság megállapította a Google három tisztségviselőjének - Peter Fleischer *Global Privacy Counsel*, David Drummond *Chief Legal Officer* és George Reyes volt *Chief Financial Officer* – büntetőjogi felelősségét, mert Olaszországban a Google Video-n keresztük elérhető volt egy tinédzser bántalmazásáról készült videó. A szigorúbb európai szabályozásnak ugyanakkor nem csak elbizonytalanító, de konstruktív hatása is lehet, és emiatt előfordulhat, hogy egy szolgáltatás adatvédelmi feltételei más, adatvédelmi szempontból megengedőbb országokban is az európai szabványoknak megfelelően módosításra kerülnek.

3. Reakciók az USA-ból - transzatlanti adatvédelmi háború?

Az előbb említett, a Rendelettervezet hatályának kérdésével függ össze, hogy az USA-ból érkező reakciók meglehetősen hűvösek a Rendelettervezettel kapcsolatban, mind adatkezelői, mind szabályozói oldalról. (Vannak ugyanakkor csoportok - *Consumer Federation of America*, *Consumers Union, Electronic Privacy Information Center*, *Public Citizen* – akik támogatják az EU szigorúbb szabályozását.[98]) Az európai szabályozó hatóságok vizsgálataiban folyamatosan napirenden van az USA-ba a Patriot Act, a Foreign Intelligence and Surveillance Amendments Act (*FISAA*), és a már említett FATCA alapján történő adattovábbítás, valamint a bírósági eljárások során történő tömeges adattovábbítás jogszerűsége. Az „*e-discovery*" problémájával kapcsolatban az úgynevezett Working Group 6 (WG6) of the Sedona Conference fogalmazott meg ajánlásokat 2011. decemberében (International Principles on Discovery, Disclosure & Data Protection). Az EU-USA adattovábbítás jogszerűségének megfelelő szabályozást sürgeti az Amerikai Ügyvédi Kamara (*American Bar Association*) is, amely 2012. február 6-án kelt, 103. számú döntésében felhívja az USA-beli bíróságok figyelmét a külföldi adatvédelmi jogszabályok betartására. (Hasonló nehézségek merültek fel a *SWIFT* (pénzügyi tranzakciók) és a *PNR* (légiutas-adatok) rendszerekkel kapcsolatos adattovábbítási megállapodások tárgyalása során.) Az EU és az USA adatvédelmi jogának eltérését, és a Rendelettervezet várható amerikai hatását elemző újságcikkek transzatlanti adatvédelmi konvergencia helyett már transzatlanti adatvédelmi háborút emlegetnek – az EU-s válaszok pedig bírálják az USA-nak az EU-nál állítólagosan kevésbé szigorú adatvédelmi szabályozását. Egy jellemző megállapítás Isabelle Falque-Pierrotin (CNIL) részéről: „*a személyes (az USA-ban) adat nyersanyag az üzleti szférának*".[99]

Nem szabad azonban lebecsülni az USA adatvédelmi szabályozását, csak azért, mert az országnak nincs egységes, szövetségi szintű általános adatvédelmi jogszabálya. Az adatvédelmi jog reformja az USA-ban is folyamatban van, és mind a szektor-specifikus jogszabályok (pl. egészségügyi adatok védelmével kapcsolatos jogszabályok,

[98] **Re: European Commission General Data Protection Regulation**, http://www.consumerfed.org/pdfs/Comments.EUPrivacyRegulationLetter9.5.12.pdf

[99] **Guarding a 'Fundamental Right' of Privacy in Europe**, http://www.nytimes.com/2012/11/21/technology/guarding-a-fundamental-right-of-privacy-in-europe.html?_r=0

adatbiztonsági értesítési kötelezettségek), mind a hatósági gyakorlat figyelemre méltó és előremutató. Vannak egyébként kezdeményezések szövetségi szintű adatvédelmi jogszabály elfogadására is: ennek keretében 2012 során a kormányzat közzétette – a *Department of Commerce Internet Policy Task Force* által kibocsátott „*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*."[100] elnevezésű korábbi anyagon alapuló, adatvédelmi keretszabályzást előirányzó jelentését.[101]

Érdemes megfigyelni azt is, hogy az USA egyes tagállamai az EU-nál jóval gyorsabban reagálnak a technológiai változásokra, és az általuk felvetett adatvédelmi kérdésekre: nemzetközi szinten fontos megemlíteni a 2012 folyamán elfogadott kaliforniai *Online Privacy Protection Act* elnevezésű jogszabályt, ami a kereskedelmi honlapok vagy internetes szolgáltatások üzemeltetőin túl a mobilalkalmazások fejlesztői és platformszolgáltatói számára is kötelezővé teszi adatvédelmi szabályzat készítését és jól látható módon történő közzétételét. Az iparág külön megállapodás formájában támogatta a kezdeményezést - az Amazon, az Apple, a Google, a Microsoft, a HP és a Research in Motion vállalták az alkalmazásfejlesztők adatvédelmi oktatását is. Hasonló iránymutatásokat bocsátott ki például maga az FTC, a kaliforniai végrehajtó szerv,[102] külföldön az illetékes japán minisztérium, és a mobilalkalmazások adatvédelmi kérdéseivel kapcsolatos önszabályozást fogadott el a Payment Card Industry Security Standards Council (PCI SSC) is.[103] A Mobile Marketing Association (MMA) pedig 2012. január 25-én tette közzé a Mobile Application Privacy Policy elnevezésű, az első, mobil adatvédelmet szabályozó adatvédelmi szabályzatát.

Kaliforniában a szabályzat az európai gyakorlathoz hasonlóan tartalmazza a gyűjtött adatok részletes leírását, harmadik személyekkel való megosztásuk módját, valamint a fogyasztó információs / adatmódosítási jogait. A jogszabálynak nem megfelelő adatkezelőkre alkalmazásonként akár 500.000 amerikai dollár fogyasztóvédelmi bírság is kiszabható. A mobilalkalmazások jogellenes adatkezelési gyakorlata PR szempontból is aggályos, a szolgáltatók ezért jogszabályi kötelezettség hiányában is olyan gyorsan orvosolják, amint tudják. Nagy nyilvánosságot kapott például, amikor kiderült, hogy az Apple iOS alkalmazásai a felhasználó előzetes hozzájárulása nélkül gyűjtenek személyes adatokat.[104] A Delta Airlines ellen pedig már fel is lépett az illetékes kaliforniai hatóság, mert nem biztosította időben a jogszabályi megfelelést. Ezt követően a társaság közzétette az előírt adatvédelmi szabályzatot, az FTC egy korábbi adatbiztonsági szakértője azonban észrevette, hogy a társaság olyan adatokat is kezel (iPhone UDID), ami nem szerepel a szabályzatban – az ügy szintén nagy nyilvánosságot kapott, tehát az amerikaiak adatvédelmi tudatossága sem elhanyagolható.[105]

A mobilalkalmazások által felvetett kérdések szabályozása mellett érdemes megemlíteni a közösségi oldalak használatát szabályozó specifikus amerikai jogszabályokat is. Legutóbb - Maryland, Illinois, Kalifornia, és New Jersey államokhoz hasonlóan - Michigan államban fogadtak el törvényt, amely tiltja a munkáltatók és oktatási intézmények számára a munkavállalók, jelentkezők és diákok közösségi oldalakon használt felhasználói fiókjaival

[100] **Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework**, http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework

[101] **Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Global Innovation in the Global Digital Economy**, http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf

[102] **Atty. Gen. Kamala Harris issues mobile apps privacy guidelines**, http://www.latimes.com/business/technology/la-fi-tn-california-ag-kamala-harris-issues-mobile-apps-privacy-guidelines-20130110,0,3765367.story?goback=.gde_1961370_member_203161108

[103] **Marketing Your Mobile App: Get It Right from the Start**, http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

[104] **Apple: Apps using address data are in violation, fix to come**, http://news.cnet.com/8301-27076_3-57378551-248/apple-apps-using-address-data-are-in-violation-fix-to-come/

[105] **Delta Air Lines publishes privacy policy, but reseacher finds a fault**, http://www.computerworld.com/s/article/9234539/Delta_Air_Lines_publishes_privacy_policy_but_reseacher_finds_a_fault

kapcsolatos adatainak bekérését.[106] A Rendelettervezet nem tartalmaz hasonló, specifikus adatkezelési módokat szabályozó rendelkezéseket, pedig a gyakorlatban feltehetőleg hasznosabb lenne, mint az általános adatvédelmi rendelkezések minden egyes technológia, illetve szolgáltatástípus esetére való egyedi interpretációja.

A legutóbbi jogalkalmazási fejlemények közül érdemes kiemelni a *U.S. Securities and Exchange Commission* (SEC) iránymutatását arról, hogy milyen adatbiztonsági kockázatokat szükséges feltüntetetni a tőzsdei nyilvános jelentésekben[107] - a megfelelő adatbiztonság és adatvédelem így különösen releváns lehet a tőzsdei bevezetést tervező cégeknek, mint például a nemrég tőzsdére ment Facebook-nak. Itt az igazi – minden hatósági intézkedésnél visszatartóbb – szankció az árfolyamcsökkenés.

Az USA-ban kiemelt fontosságú a jogszabályok hatékony végrehajtása – e tekintetben is van mit tanulni az EU-s jogalkotóknak. Kaliforniában például 2012. július 20-án az illetékes végrehajtó szerven belül (*Office of the Attorney General*) „*Privacy Enforcement and Protection Unit*" létrehozatalát jelentették be, és hasonló kezdeményezést fogadott el Maryland is (*Internet Privacy Unit*).[108] Szövetségi szinten pedig az adatvédelmi megfelelőség – általában fogyasztóvédelmi rendelkezések, kötelezettségvállalások alapján - történő ellenőrzését az FTC végzi, többnyire a cégekkel kötött egyezségek (*settlement*) keretében. (Bírálói szerint ugyanakkor az FTC megegyezések problémásak lehetnek abból a szempontból, hogy az adatkezelők nem tesznek majd adatvédelmi vállalásokat a fogyasztók felé szerződéses feltételeikben, így megszegni sem tudják azokat.)[109]

Néhány példa az adatvédelmi szabályok végrehajtására az USA-ban:

- A Spokeo Inc. adatbróker a Fair Credit Reporting Act (FCRA) megszegése miatt 2012. június 6-án 800.000 amerikai dollár összeget fizetett az FTC számára. Az adatkezelő vállalta továbbá, hogy az általa gyűjtött és harmadik személy felhasználók (többnyire HR cégek) számára átadott személyes adatok, pl. név, cím, életkor, email, hobbi, származás, vallás, közösségi oldalakon való jelenlét, és a fentiek alapján alkotott profil – csak jogszabálynak megfelelő célból kerülnek további felhasználásra, valamint teljesíti a fogyasztók számára teljesítendő kötelező értesítési kötelezettségét abban az esetben, ha az adatokat felhasználó személy az adatok alapján hátrányos intézkedést tett a fogyasztóval kapcsolatban.

- A Google – legalább három reklámszolgáltatóval (Vibrant Media, WPP PLC's Media Innovation Group, és Gannett's PointRoll) együtt megkerülte az Apple Safari Web keresőjének a harmadik fél cookie-kat automatikusan blokkoló adatvédelmi beállításait, és cookie-t helyezett el az OS X és iOS eszközökön (pl. Safari-t használó iPhone). Az FTC-vel kötött egyezség keretében a Google szankcióként 22.5 millió amerikai dollár megfizetését vállalta.

- Az FTC felé 2012. október 22-én tett kötelezettségvállalást a Complete, Inc. nevű társaság, amely az adatvédelmi szabályzatában azt állította, hogy a felhasználó internethasználattal kapcsolatos viselkedési adatai anonimizálva, ésszerű

[106] **Michigan Enacts Social-Media Privacy Law**, http://www.delawareemploymentlawblog.com/2012/12/michigan-enacts-social-media-privacy-law.html?goback=.gde_1243587_member_200319229

[107] **CF Disclosure Guidance: Topic No. 2**, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[108] **Maryland Attorney General Doug Gansler Establishes Internet Privacy Unit**, http://www.stateagmonitor.com/2013/01/29/maryland-attorney-general-doug-gansler-establishes-internet-privacy-unit/?goback=.gde_3204418_member_209335767

[109] FTC Online Privacy Settlements Do More Harm Than Good?

adatbiztonsági intézkedésekkel kerülnek továbbításra a társaság számára. Valójában más személyes adatok gyűjtésére és nem biztonságos módon való továbbítására is sor került.

- Az FTC keményen szankcionálja azt is, ha a telemarketing cégek nem tesznek eleget az *opt-out* kötelezettségüknek (Dish Network – 5.991.000 amerikai dollár, DirecTV 5.335.000 amerikai dollár, Craftmatic 4.400.000 amerikai dollár), vagy ha az adatkezelők 13 év alatti gyermekek személyes adatait a vonatkozó jogszabály (*Children's Online Privacy Protection Act - COPPA*) előírásait megszegve szülői hozzájárulás nélkül gyűjtik (Playdom – 3.000.000 amerikai dollár, Sony BMG Music Entertainment 1.000.000 amerikai dollár), vagy elmulasztják megtenni a fogyasztók irányába vállalt adatbiztonsági intézkedéseket (LifeLock – 12.000.000 amerikai dollár). Várható egyébként, hogy a COPPA szabályai nem csak a weboldalak üzemeltetőire alkalmazandók majd, hanem egyéb, gyermekek személyes adatait gyűjtő harmadik személyekre is (például a mobilalkalmazás-fejlesztőkre), és az FTC azt is javasolja, hogy az IP címeket, valamint a helymeghatározási adatokat kifejezetten minősítse a jogalkotó személyes adatoknak.[110] Az FTC külön vizsgálta a mobilalkalmazások adatkezelési gyakorlatának gyermekvédelmi vonatkozásait is.[111]

- Az Equifax Information Services LLC hitelinformációs céget szintén bírságolta az FTC, a hitelüket késedelmesen törlesztő személyek személyes adatai jogellenes kezelése miatt.

- Az FTC végrehajtásával működő Safe Harbor működése is sikeresnek mondható: 3.000 amerikai cég vesz benne részt, probléma azonban a megfelelőség ellenőrzéséhez szükséges erőforrások hiánya. Pedig ez fontos lenne: a Google Buzz indulásakor a Gmail felhasználóinak személyes adatait a Google jogellenesen használta fel – az adatkezelőt az FTC a Safe Harbor alapján marasztalta el.

- Nincs lehetőség a hatósági vizsgálatok elhúzására sem: 2012. április 14-én a *Federal Communications Commission* (*FCC*) 25.000 amerikai dollár bírságot szabott ki a Google-re, mert a Google Street View adatvédelmi gyakorlatának vizsgálata során (adatgyűjtés jelszóval nem védett WiFi hálózatokról) kilenc hónapig nem tett eleget információszolgáltatási kötelezettségének.

Érdemes arra is figyelni, hogy az USA számára nem csak az EU felé, hanem az ázsiai-csendes óceáni térség irányában is fontos az adatvédelmi megfelelőség: az FTC 2012. július 26-án végrehajtó szervként bekapcsolódott az Asia-Pacific Economic Cooperation (APEC[112]) nevű szervezet Cross-Border Privacy Rules System (CPBR) elnevezésű rendszerébe. Nem egyértelmű azonban, hogy a térség országai milyen típusú adatvédelmi szabályozást valósítanak meg: európai típusú általános keretszabályozást, vagy amerikai típusú részlet- és önszabályozást. Japán, India, Thaiföld, Szingapúr és a Fülöp szigetek például az EU-hoz hasonló adatvédelmi szabályozást működtet.

[110] **Children's Online Privacy Protection Rule**, https://ftcpublic.commentworks.com/FTC/InitiativeDocFiles/330/2012copparulereview.pdf

[111] **FTC: Mobile apps for kids lack privacy disclosures**, http://news.cnet.com/8301-19518_3-57379469-238/ftc-mobile-apps-for-kids-lack-privacy-disclosures/

[112] Az USA mellett a 21 APEC tagország: Ausztrália, Brunei, Kanada, Chile, Kína, Hong Kong, Indonézia, Japán, Korea, Malajzia, Mexikó, Új Zéland, Pápua Új Guinea, Peru, Fülöp-szigetek, Oroszország, Szingapúr, Tajvan, Thaiföld, és Vietnam.

4. Mi történik 2013-ban, és mit tehetnek az adatkezelők?

Várható, hogy a Rendelettervezet az elkövetkező időszakban számos változtatáson esik át – a legkritikusabb pontok: extraterritoriális hatály, a személyes adatok bizonytalan meghatározása, a kifejezett hozzájárulás követelménye, a kiterjedt dokumentációs kötelezettség, a felejtéshez való jog, az adathordozáshoz való jog, a szigorú bírságolási kötelezettség, a felhatalmazáson alapuló, valamint végrehajtási aktusok nagy száma, valamint az adatbiztonsági értesítési eljárások gyakorlati megvalósítása. A Bizottság mindenesetre elszánt a Rendelettervezetben bevezetett koncepciók megvalósítása mellett, az elért előnyök ugyanis még a problémás rendelkezések felhígítása mellett is figyelemre méltóak: nagyobb jogharmonizáció, a *one-stop-shop*, az adatvédelmi nyilvántartásba való bejelentkezési kötelezettség eltörlése, az „elszámoltathatóság" és a „beépített és alapértelmezett adatvédelem" nevesítése, és a nemzetközi adattovábbítások részletesebb szabályozása.

Az adatkezelők számára tehát elengedhetetlen, hogy időben megkezdjék felkészülésüket a Rendelettervezetnek való megfelelésre, különös tekintettel a belső eljárások, dokumentációs kötelezettségek bevezetésére, a szükséges szervezeti, szerződéses és technológiai változtatások – pl. adatkezeléssel járó szerződések módosítása, a szigorúbb hozzájárulási követelmények miatt IT rendszerek cseréje - elvégzésére, az illetékes személyek kinevezésére, a munkavállalók oktatására és egyéb megfelelési (*compliance*) feladatok teljesítésére. Ennek előkészítését már most érdemes elkezdeni. Fontos a „*buy-in from the top*", vagyis a menedzsment támogatása az adatvédelmi intézkedések (adatvédelmi felelős kinevezése, dokumentációk elkészítése, belső eljárások megvalósítása) megvalósításában.

A lényeg: a Rendelettervezet – nemcsak elfogadása esetén, de már tervezet formájában is – jelentős hatást gyakorol majd az adatkezelők működésére, valamint más országok és régiók adatvédelmi szabályozására, így különös figyelemmel kell lenni, hogy a Rendelettervezet ne tartalmazzon ésszerűtlen feltételeket, hanem inkább mintául szolgáljon, és elősegítse a különböző szabályozások interoperabilitását, valamint az üzleti környezet egyszerűsítését, az adminisztratív terhek és *compliance* költségek csökkentését. Nagyon fontos elkerülni a szükségtelen adminisztratív terhek bevezetését. A Rendelettervezet véglegesítésével kapcsolatos vitáknak nyitottnak és transzparensnek kell lenniük - nem úgy, mint például a rossz emlékű ACTA esetében. A jogalkotási aktusok mellett támogatandók a magatartási kódexek, és egyéb, önszabályozási kezdeményezések is, valamint az EU Bizottság által meghatározott egységes gyakorlatok, adattárolási formátumok, formanyomtatványok. Az új, 503.7 millió adatgazdát érintő EU-s adatvédelmi szabályozás már a „Privacy 2.0" jegyében készül, 27 különböző szabályozási rendszert vált fel, így fontos, hogy ne gátolja az innovatív, személyes adatok kezelésén alapuló üzleti megoldásokat, hosszú távra kiszámítható (*future proof*), a technikai fejlődést lehetőség szerint szem előtt tartó szabályozási környezetet biztosítson, és megfelelő védelmet, tájékoztatást és ellenőrzési jogot biztosítson az adatgazdák számára is.

A szerző ügyvéd, a CMS Cameron McKenna LLP budapesti irodájának munkatársa. Munkája során folyamatosan figyelemmel kíséri az új EU-s adatvédelmi szabályozás alakulását, és tájékoztatást nyújt az adatkezelőknek az új rendelkezésekre való felkészülésben – különös tekintettel azok regionális vonatkozásaira. Az írással kapcsolatos kérdéseket, észrevételeket a marton.domokos@cms-cmck.com vagy a marton.domokos@gmail.com címre várja.