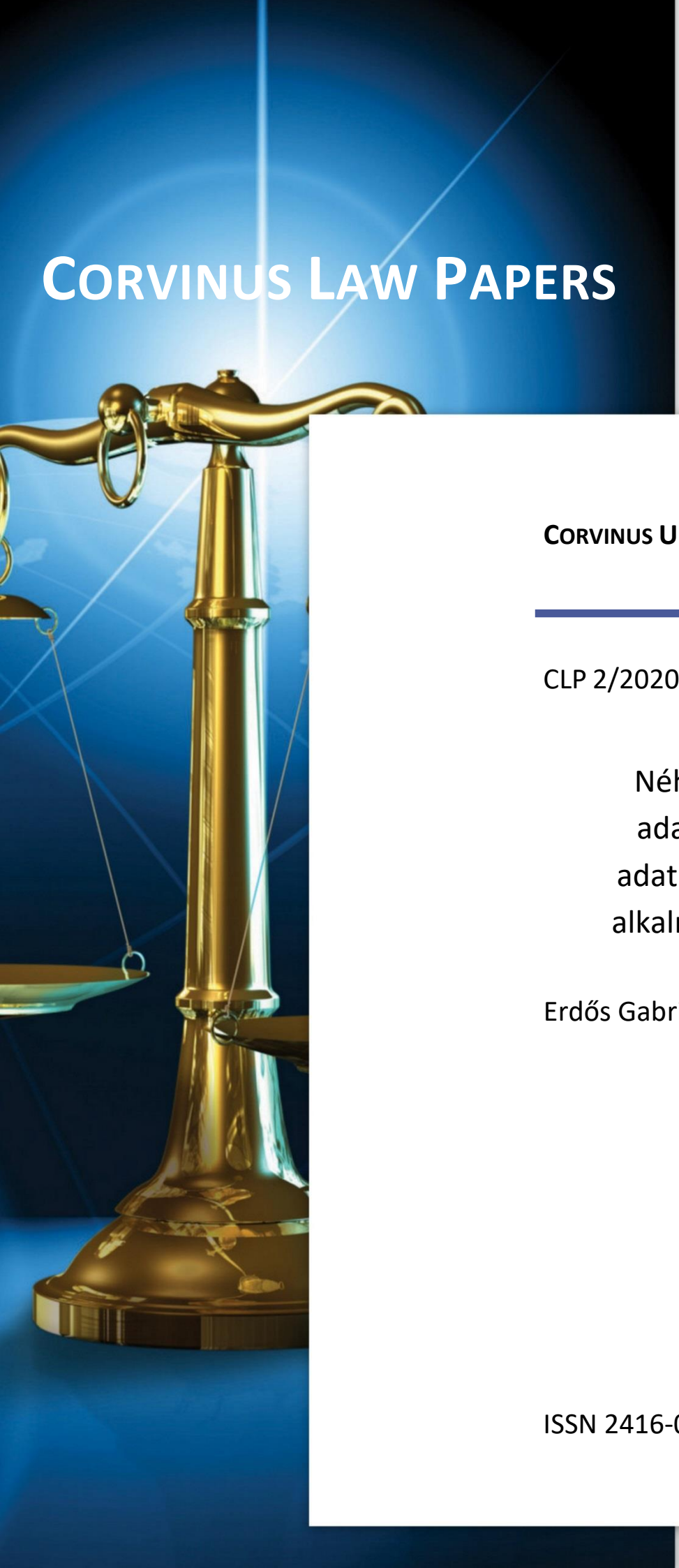

CORVINUS LAW PAPERS

Corvinus

CORVINUS UNIVERSITY OF BUDAPEST

CLP 2/2020

Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén

Erdős Gabriella

ISSN 2416-0415

Corvinus Law Papers

CLP 2/2020

The primary purpose of the Corvinus Law Papers (CLP) is to publish the results of research projects performed by those connected to the Department of Business Law as research reports, working papers, essays and academic papers. The CLP also publishes supplementary texts to be used for practical and theoretical training of students.

Address of the Editorial Board:

Corvinus Law Papers
1093 Budapest, Fővám tér 8. III. emelet 321/A

Publisher:

Corvinus University of Budapest
H-1093 Budapest, Fővám tér 8.

Responsible for the edition:

Dániel Bán

ISSN 2416-0415

Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén*

Erdős Gabriella
egyetemi adjunktus
e-mail: gabriella.erdos@uni-corvinus.hu

Absztrakt: A cikk a mobil alkalmazások adatvédelmi megoldásait elemzi és vizsgálja azok összhangját az adatvédelmi rendelettel, különös tekintettel az adatfelhasználáshoz való aktív hozzájárulás, az álnevesítés, és törléshez való jog gyakorlásának megvalósítására. Az elemzés kitér az adatvédelem és más olyan alapvető uniós elvek, mint a közös piac, a csalások lehetőségének minimalizálása és a magánélethez való jog összehangolásának szükségességére és eddig megvalósított lépéseire is.

Kulcsszavak: adatvédelem, GDPR, adatbiztonság, magánélethez való jog

1. Sebezhetőség

Az ImmuniWeb[1] 2019 közepén saját fejlesztésű AI platformja segítségével tesztelte a világ 100 legnagyobb bankjának weboldalait és applikációit az adatbiztonság szempontjából, és mindössze 3 bankot talált adatbiztonsági szempontból megfelelőnek.
A kutatás az összes megvizsgált mobil banki applikációban talált legalább alacsony kockázatú sebezhetőségeket, és szerintük minden ötödik súlyos hibákkal működik. A felmérés szerint „a mobil banki alkalmazások 55 százaléka fér hozzá különösen érzékeny adatokhoz, ezek az alkalmazások összesen 298 féle backend API-val kommunikálnak, hogy ilyen adatokat küldjenek vagy fogadjanak a megfelelő bankok rendszereiből.”Ez a megállapítás azt is jelenti, hogy az érzékeny adatok a mobil applikációkon keresztül könnyedén eljuthatnak bárkihez, hiszen a backend API többek között éppen a felhő alapú tárolási módokhoz való hozzáférést biztosítja.
A banki ügyfelek jelentős része az internetes, mobil telefonon keresztül elérhető banki szolgáltatásokat részesíti előnyben, ezzel is kihívások elé állítva az adatvédelmi szakembereket. A mobil telefonok rengeteg érzékeny adatot tartalmaznak, és a letöltött alkalmazás általában sokkal egyszerűbb védelmi rendszerekkel rendelkezik, mint a központi banki rendszerek. Hogy csak néhány, mindenki által ismert, személyes adatnak minősülő adathozzáférést említsünk: a mobiltelefonon tárolt fényképek elérése, bejelentkezési adatok megszerzése, vagy akár a személy lokációja. Ma már az sem ritka, hogy valaki különösen érzékenynek minősülő egészségügyi adatokat tároljon az okos telefonján, például az edzés eredményeit, pulzusszámot, stb. A mobil telefonok más oldalról is lehetnek adatvédelmi veszélygócok. A banki alkalmazottak sok esetben telefonon tartják a kapcsolatot ügyfeleikkel, így azok adatai szerepelnek majd az alkalmazott saját privát mobiltelefonjában is, ahol végképpen nem védi az adatokat komoly adatvédelmi program. Ebben az esetben tehát a bank anélkül is megvalósíthatja az adatvédelmi rendelkezések megszegését, hogy tudomása lenne róla.

*A cikk aGINOP-2.2.1-18-2018-00010 „*Automatizált, élethelyzet alapú, valós idejű döntéstámogató keretrendszer*” program keretében készült.
[1] https://www.immuniweb.com/blog/SP-100-banks-application-security.html#7

Amennyiben a mobil applikáció vagy a felhő szolgáltatás adatbiztonsága nem megfelelő, akkor a személyes adatok védelme nem tud megvalósulni, holott a megfelelő adatvédelem biztosítása az adatkezelők és adatszolgáltatók feladata. Az adatvédelmet az Európai Unióban a 2016/679-es Tanácsi rendelet[2](a következőkben: Rendelet) szabályozza, amelyet a tagországoknak 2018 májusáig kellett bevezetniük.

2. GDPR rendelet

A Rendelet a személyes adatok kezelésére, védelmére és áramlására vonatkozóan tartalmaz általános elveket és szabályokat. Személyes adatnak minősül minden, ami természetes személy azonosítására akár részben is alkalmas. Adatkezelésnek minősül a személyes adatokkal végzett bármilyen művelet. Az adatok kezelését jogszerűen, tisztességesen és az érintett számára átlátható módon kell végezni. Az adatok gyűjtésének célhoz kötöttnek kell lennie, biztosítani kell az adatok biztonságát, és az adatkezelőnek elszámoltathatónak kell lennie arról, hogy adatkezelése megfelelt-e a fenti követelményeknek. Adatkezelőnek minősül bárki, aki a személyes adatok kezelésének a célját meghatározhatja, azzal kapcsolatban érdemi döntéseket hozhat, tehát egy bank minden esetben adatkezelőnek minősül. Adatfeldolgozó az a személy, aki más adatkezelő nevében kezel személyes adatokat. Adatfeldolgozónak minősülhetnek például a middle-office funkciókat ellátó banki egységek.
A korábbi gyakorlatot, amely lehetővé tette az adatgyűjtést és felhasználást az adattulajdonos hallgatólagos beleegyezésével is, az új rendelet bevezetésével felváltotta az aktív hozzájárulás követelménye[3]. Ez azt jelenti, hogy az adatkezelésnek az érintett adattulajdonos aktív hozzájárulásán kell alapulnia, az adatkezelőnek a hozzájárulást bármikor be kell tudni mutatnia. Az adat magánszemély tulajdonosa jogosult arra is, hogy a hozzájárulását bármikor visszavonja, a rá vonatkozó személyes adatokat töröltesse. Az adatkezelőnek önmagáról és az adatkezelés céljáról, jogalapjáról és még sok másról is kötelezően tájékoztatnia kell az érintettet. Az adatkezelőnek meg kell teremtenie és folyamatosan biztosítania kell a rendeletnek megfelelő és az érintettek jogainak védelméhez szükséges adatvédelmi folyamatokat. Az adatkezelők az adatkezelési tevékenységről részletes nyilvántartást vezetnek, biztosítják az adatok biztonságát és 72 órán belül jelentik a hatóságnak, ha adatvédelmi incidens történik. A belső nyilvántartás vezetése az adatfeldolgozók számára is kötelező. A Rendelet részletes szabályokat ír elő az érzékeny adatatok kezelésére vonatkozóan, illetve kemény büntetést szab ki abban az esetben, ha a rendelet előírásai az adatkezelőnél nem valósulnak meg maradéktalanul.

3. Aktív hozzájárulás

Az adatkezelésnek jogszerűnek kell lennie[4]. A jogszerűség biztosításának egyik módja éppen az adatkezeléshez való hozzájárulás megszerzése[5]. A hozzájárulásnak nemcsak aktívnak kell lennie, hanem célhoz kötöttnek is, vagyis az applikáció nem kérhet az adatfelhasználáshoz való általános hozzájárulást, hanem meg kell mondania az adatkezelés konkrét célját. Azonban a Rendelet nem szól arról, hogy hogyan kell a célok konkrétságát értelmezni, ezt

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), L119/1,
[3] Rendelet, 7.cikk
[4] Rendelet 6. cikk
[5] Más indokokkal is lehet az adatkezelés jogszerű: amennyiben olyan szerződés teljesítéséhez szükséges, amelyet az érintett már aláírt, vagy jogszabályon alapul, vagy létfontosságú érdekek védelme miatt van rá szükség, vagy pedig közhatalmi szervnek van rá szüksége a feladata elvégzéséhez.

majd a kialakuló esetjog fogja megmondani. Például elfogadható-e konkrét adatkezelési hozzájárulásként az adatvédelmi szabályzat elfogadása. Véleményem szerint egy ilyen megoldás már nem valósítja meg a rendelet szellemét, ennek ellenére számtalan olyan alkalmazás létezik, amely csak az általános feltételek között határoz meg általános felhasználási célokat. Ráadásul az általános feltételek, illetve az adatvédelmi szabályzatok nagyon sok esetben hosszúak, szakkifejezésekkel teletűzdelt jogi nyelven vannak megfogalmazva, így nem igazán felelnek meg az áttekinthetőség követelményének sem. Konkrét cél esetén is felmerülhet, hogy a cél mennyire legyen konkrét, például elegendő-e azt mondani, hogy az adatgyűjtés a személy vásárlói szokásainak felmérése céljából történik vagy meg kell nevezni a projektet? Vannak olyan applikációk, amelyek több célt határoznak meg, azonban minden célhoz külön kérnek hozzájárulást. Például külön kérdés lehet a mobiltulajdonos lokációjához való hozzáférés, a szükséges, illetve kényelmi sütik használata, a reklámcélú adatgyűjtés, illetve a személyre szabott reklám küldése, a szolgáltatások személyre szabása, és még hosszan lehetne sorolni a célokat. Ezek az alkalmazások teljesen megvalósítják a rendelet célját, azonban így a felhasználónak lehetősége van arra, hogy az adatgyűjtést a lehető legszűkebb területre szorítsa vissza, ami az alkalmazás tulajdonosának nem feltétlenül érdeke. A másik végletet azok az alkalmazások képviselik, amely egyszerű, bináris megközelítést alkalmaznak: a felhasználónak összesen annyi a lehetősége, hogy vagy elfogadja a személyes adatainak az összes konkrét célra történő alkalmazását, vagy nem kap az alkalmazáshoz hozzáférést. A fenti példánál maradva ezt úgy lehet megvalósítani, hogy az applikáció ugyan felsorolja az összes fent említett célt, azonban azokra nem egyenként, hanem csak egyben lehet elfogadó nyilatkozatot tenni.

Azt a kérdést is a bíróságnak kell majd eldöntenie a konkrét ügyekben, hogy ténylegesen megvalósul-e a hozzájárulás szabadsága olyan esetben, amikor a kapcsolt célokhoz (reklám, marketing) történő hozzájárulás nélkül az alapszolgáltatás nem vehető igénybe. A Rendelet ugyanis kimondja, hogy „annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.”[6]A Rendelet azonban nem ad útmutatást abban a tekintetben, hogy mi történjék akkor, ha a szerződés teljesítéséhez is szükséges adatoknakmás célokra történő kezeléséhez való hozzájárulás a szolgáltatás igénybevehetőségének a feltétele. Azok az applikációk, amelyek a reklámcélokhoz való hozzájárulást nem külön elfogadandó célként jelölik meg, valószínűleg nem tekinthetőek a rendelettel teljesen összhangban lévőnek, de ez a törvény szövegezéséből nem vezethető le egyértelműen.

Jogi kötőerővel nem rendelkező iránymutatásokat azért lehet a témában találni. A legfontosabbak ezek közül a 29. cikk Munkacsoport (Art29.WP), illetve a munkacsoportot felváltó EDPB (European Data Protection Board) ajánlásai.[7] Az ajánlások a hozzájárulás szabadságával kapcsolatosan[8] kifejtik, hogy a választási lehetőségnek ténylegesnek kell lennie. Nem kapcsolhatók hozzá meg nem változtatható feltételek, illetve az elutasítás nem járhat hátrányos következménnyel a magánszemély részére. A hozzájárulás szabadságának része az is, hogy a szolgáltatás elérése nem függhet olyan adatkezeléshez való hozzájárulástól, amely nem szükséges az adott szolgáltatáshoz. A hozzájárulásnak szabadnak kell lennie abban az értelemben is, hogy az érintett választhasson több cél esetén a célok között, és eldönthesse melyikhez kapcsolódó adatkezeléshez járul hozzá.

Fontos, és a rendelet által nem kellően szabályozott kérdés az is, hogy az érintett adattulajdonos hozzájárulása kiterjed-e harmadik személyekre, más szoftverre. Nagyon sok

[6] Rendelet 7. cikk (4) pont.

[7] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

[8] Guidelinesonconsentunder Regulation 2016/679, WP259 rev01

applikáció maga is felhasznál ugyanis harmadik fél által birtokolt licenceket, amelyek adott esetben automatikusan hozzáférnek a személyes adathoz az applikációnak adott hozzájárulás alapján. Vannak olyan alkalmazások, amelyek felsorolják az általuk használt szoftvereket, de az ilyen lista önmagában nem mond semmit az adatáramlásról és a felhasználónak sem nyújt elég információt az elfogadáshoz vagy elutasításhoz. A legtöbb applikáció pedig egyáltalán nem tesz említést az általa használt egyéb szoftverekről. Ebből az applikáció tulajdonosa számára az a feladat következik, hogy amennyiben adatkezelőként jogszerűen akar eljárni, akkor a beépült szoftverek számára meg kell tiltania az adatgyűjtést, adatkezelést. Ez azonban a gyakorlatban nehezen megvalósítható. Még amennyiben szerződéses úton megvalósítható lenne, akkor is kétséges a kikényszeríthetősége és az ellenőrizhetősége. A másik megoldás az lehet, ha a beépült szoftvereket az adatfeldolgozókra vonatkozó szabályok szerint kezeli, és a szerződésbe is bekerülnek ezek a feltételek. Ez a megközelítés is ütközhet gyakorlati akadályokba, amennyiben kereskedelmi szoftvert épít be az adatkezelő az alkalmazásba.
Az adott applikáció számára a hozzájárulás kérés módja és a konkrét célok halmazának meghatározásaaz adatvédelmen és adatbiztonságon túl akár versenyelőnyt vagy versenyhátrányt is jelenthet, mivel a túlzottan agresszív applikációk elveszíthetik a potenciális felhasználók egy részét, a túlzottan megengedő applikációk pedig nem tudnak elég hatékony marketinget folytatni új felhasználók megnyerésére, illetve az alkalmazást eltartó reklámbevételeik csökkenhetnek.

4. Álnevesítés

A hozzájárulás megszerzése nem a GDPR kötelezettség végét, hanem a kezdetét jelenti az applikáció tulajdonosa számára[9]. Az információt ugyanis csak az adott célra, és csak addig lehet tárolni, ameddig a cél meg nem valósul. Ráadásul az adat magánszemély tulajdonosa bármikor visszavonhatja korábbi beleegyezését vagy kérheti a tárolt adatok törlését. Ameddig az adatkezelés fennáll, az adatokat megfelelően védeni kell, biztosítani kell azok integritását, pontosságát, naprakészségét.
Az adatkezelés fennállása alatti adatvédelem nem egyszerű feladat. Nagy bankcsoportok esetén például természetes, hogy az adatok a vállalatcsoporton belül átadásra kerülnek valamilyen részfeladat (pl. az ügyfél kockázati profiljának a meghatározása, ügyfél szegmentáció, stb.) elvégzése érdekében. Mivel a Rendelet az adatkezelőt jogi személyenként definiálja, ezért a vállalatcsoporton belüli adatátadáshoz ugyanúgy szükséges az érintett adattulajdonos aktív beleegyezése, ha változik a felhasználás célja. Amennyiben az adatfeldolgozás az eredeti cél érdekében megy végbe, akkor az adat adatfeldolgozónak történő továbbításáról beszélünk. Ebben az esetben nem szükséges a természetese személy adattulajdonos hozzájárulása, de az adatkezelésre vonatkozó követelményeket az adatfeldolgozóknak is teljesíteniük kell. Az adatkezelő és az adatfeldolgozó között létre jött írásos szerződésben rögzíteni kell azt, hogy miként kívánják a rendelet előírásait megvalósítani. Többek között arra is ki kell térni, hogy az adatfeldolgozó kizárólag az adatkezelő utasításai szerint jár el, al-adatfeldolgozót csak az adatkezelő beleegyezésével vesz igénybe, biztosítja a titoktartást, illetve a továbbított adatok feldolgozás utáni haladéktalan visszajuttatását vagy törlését. Az adatbiztonsági kockázat is növekszik a másodlagos felhasználással, hiszen ezek a felhasználások más szoftvereket, digitális alkalmazásokat vehetnek igénybe. A Rendelet az adatok védelmére az egyik legfontosabb általános eszközként az álnevesítést[10] javasolja.

[9] Rendelet 5. cikk
[10] Rendelet, 4.Cikk (5) pont

Az álnevesítés lényege, hogy az álnevesítés elvégzése után további információk nélkül az eredeti adattulajdonos személye már nem állapítható meg. Az álnevesítésre vonatkozó információt külön kell tárolni és nem lehet a személyes adatokhoz kapcsolni. Az álnevesítést a Rendelet megfelelő garanciának tekinti a személyes adatok védelmére, a beépített, alapértelmezett adatvédelem[11] részeként fogja fel, amelyet az adatkezelőnek meg kell valósítania. Az álnevesítés maga technikailag jól megvalósítható, de azért lehetnek buktatói. Egyáltalán nem biztos például, hogy az applikáció által nyert adat feldolgozása az EU-ban, vagy EU adatfeldolgozó által történik. Ebben az esetben is biztosítani kell a GDPR megfelelőséget, azonban ilyenkor előfordulhatnak a jogrendszerek ütközéséből származó konfliktusok. Például az EU adattörlési kötelezettség ellentétben állhat, mondjuk a megfelelő USA törvény adatmegőrzési kötelezettségével. Általában is elmondható, hogy a bankok globális működési modellje komplexitást visz a GDPR megfelelőség megvalósításába. Az álnevesítés segít a problémát megoldani, azonban az álnevesítés koncepciója viszonylag új, ezért egyáltalán nem biztos, hogy azt a korábbi szoftver verziók is tartalmazták. Amennyiben nem, akkor a banki szoftverrendszert összességében át kell alakítani, nem elegendő csak az applikáció GDPR megfelelőségét biztosítani. A Rendelet nem ad útmutatást az álnevesítés, titkosítás mélységére, technikájára (algoritmusára), illetve architektúrájára vonatkozóan, de annak olyannak kell lennie, hogy megvalósítsa az eredeti célt, nevezetesen, hogy az adat ne legyen az eredeti tulajdonosához kapcsolható.
Az álnevesítés, titkosítás akkor is szükséges, ha az adatkezelő felhőszolgáltatást vesz igénybe az adatok tárolására. A titkosítás mélységét a Rendelet ebben az esetben sem határozza meg, így alkalmazhatók mind in-transit megoldások, amikor a felhő szolgáltató hozzáférhet az álnevesítés információhoz, illetve end-to-end megoldások, amikor kizárólag az adatkezelőnek van hozzáférési joga.

5. Törléshez való jog

Az adatok törléséhez való jogot is garantálja a GDPR, azonban nem tesz említést a konkrét megvalósítási módokról. Az érintettnek a törlési jog gyakorlásából nem szabad, hogy kára származzon, nem köthető a törlés például díjfizetéshez. A kár fogalmát azonban ennél sokkal általánosabban kell érteni, beleértve az erkölcsi károkat, vagy bármilyen más negatív következményt. Hátránynak számít az is, ha az adatkezeléshez való hozzájárulás visszavonása után az applikáció már csak korlátozottan, vagy egyáltalán nem működik a felhasználónál.
Ugyanakkor gyakori megoldás, hogy maga az applikáció nem biztosít egyszerű lehetőséget a törlési jog gyakorlására, hanem például azt külön levélben kell kérni, vagy csak a weboldal valamely eldugott részén található a törlési lehetőség. Az ajánlások szerint a jogok gyakorlása akkor egyszerű, ha maximum két kattintással megvalósítható. A törlés külön gondot okoz a keresők használata esetén. A keresők segítségével optimalizálják például a weboldalakon megjelenő reklámokat (például, ha valaki sok gyerekjátékot áruló weboldalra keres rá, akkor várhatóan több pelenka reklámot fog kapni a jövőben). Azonban ezekben az esetekben nem lehetséges az aktív hozzájárulás megszerzése (bár a keresők általános feltételei között természetesen megtalálható a reklám célú adatgyűjtés), és nincs kinek küldeni a hozzájárulás visszavonását sem. A kérdéskörrel kapcsolatban az EU jelenleg is konzultációt folytat és iránymutatás kiadását tervezi.
A törlésnek, módosításnak sokszor technikai akadályai is lehetnek. Az érintett magánszemélynek joga van bármikor kérni a személyes adat törlését, ez azonban feltételezi a szoftverek kompatibilitását a fejlesztések során, ami nem mindig valósul meg maradéktalanul.

[11] Rendelet, 25. Cikk

6. GDPR, PSD2 és az e-Privacy irányelv viszonya

Végezetül álljon itt néhány gondolat a GDPR és más EU jogszabályok viszonyáról. Két olyan terület is van, amely szorosan összefügg, és látszólag akár ellentétben is állhat az adatvédelemmel. Az egyik a digitális közös piac[12] megteremtése, amely többek között a digitális tartalmakhoz való könnyebb hozzáférést, a geo-blokkolás megakadályozását tűzi ki célul. Ennek a stratégiának a részeként került elfogadásra a digitális fizetésekről szóló módosított irányelv (Payment Services Directive[13], a továbbiakban: PSD2), amely egyenlő versenyfeltételeket teremt a hagyományos bankok és innovatív fizetési módokat alkalmazó fintech vállalkozások számára, tiltja a különdíjak felszámolását, és még számos könnyítést hoz. Ezek közül kiemelendő, hogy a PSD2 lehetőséget teremt arra, hogy harmadik feles szolgáltatók (Számlainformációs Szolgáltatók (AISP), a Fizetés-Kezdeményezési Szolgáltatók (PISP) és a Kártyaalapú Fizetési Eszközt Kibocsátó Szolgáltatók (CISP)) hozzáférjenek API-n keresztül a bankok folyószámla vezető rendszeréhez és az abban tárolt adatokhoz annak érdekében, hogy új, innovatív pénzügyi szolgáltatásokat nyújthassanak lakossági és vállalati ügyfelek számára. A hozzáférés azonban csak a GDPR szabályok betartásával valósulhat meg, vagyis csak a magánszemély adattulajdonos aktív hozzájárulásával, és csak a szükséges mértékig és időtartamra lehetséges. Ugyanakkor össze kell hangolni az adatvédelem igényeit a csalás lehetőségének minimalizálásával. Erre szolgál az ún. erős ügyfél-hitelesítés[14] intézménye (strong customer identification, SCA). Az SCA a számlavezető rendszere szerint megy végbe, jellemzően hitelesítési kódokat, egyszeri jelszavakat alkalmaz, és minden esetben legalább két jellemző alapján azonosítja az ügyfelet mielőtt a fizetési utasítást végrehajtja.
A másik olyan terület, amely szorosan kapcsolódik az adatvédelemhez, a magánélet tiszteletben tartása. Ezzel kapcsolatosan létezik egy irányelv[15], de még nem született meg az új elektronikus hírközlési adatvédelmi rendelet; jelenleg a javaslat[16] a társadalmi vita fázisában van. A magánélet védelmével kapcsolatos szabályoknak az alkalmazásokra nézve érdekes része az aktív hozzájárulás követelménye és az adatbiztonság biztosítása. A magánszemély aktív hozzájárulása nélkül ma már nem küldhető például elektronikus reklám, és a sütik használatához is hozzá kell járulni. A titkosságot az online szolgáltatóknak ugyanolyan szinten kell biztosítaniuk, mint a hagyományos hírközlési szolgáltatóknak, mindkettejüknek a piacon elérhető legjobb technikai megoldással kell az adatbiztonságot biztosítaniuk. A meta-adatokat is ugyanolyan szabályok szerint kell kezelni, mint a tényleges tartalmat, és menet közben nem lehet a továbbított információfolyamba beavatkozni, azt lehallgatni. Bár az adatvédelmi és a magánélet védelmi szabályok más területet céloznak meg, a kettejük között jelentős átfedés található a kommunikáció területén. A GDPR szabályozása átfogó, ezért azokat a magánélethez való jog védelme során is alkalmazni kell. Ugyanakkor az EPD részletszabályokat is tartalmaz a fogyasztókat célzó online szolgáltatások vonatkozásában.

---

[12] Communication from the Commissiontothe European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategyfor Europe (COM/2015/0192 final)

[13]Az Európai Parlament és a Tanács (EU) 2015/2366 Irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről

[14] PSD2, 4. cikk (30) pont

[15] Az Európai Parlament és a Tanács 2009/136/Ek Irányelve(2009. November 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról (a továbbiakban: e-Privacy Directive, EPD)

[16] Az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), (COM(2017)10 final)

7. Összefoglalás

Összességében elmondható, hogy a digitális gazdaság gyors ütemű fejlődése jelentős kihívások elé állította az Európai Uniót és a szolgáltatókat egyaránt. Olyan alapvető uniós elveket kellett összehangolni, mint a közös piac és az adatvédelem, a csalások lehetőségének minimalizálása és a magánélethez való jog. Mindeközben pedig olyan új digitális megoldások szültettek és születnek, amelyekre a korábbi szabályozások nem voltak felkészülve. Az adatbiztonság és az adatvédelem jelentős pénzügyi terhet jelent a bankoknak, az alkalmazások működtetőinek, ugyanakkor a magas szintű védelem versenyelőnyhöz is juttathatja őket. Mindenesetre ma már semmilyen digitális megoldás nem képzelhető el, és nem is piacképes erős adatvédelmi és adatbiztonsági rendszerek, garanciák nélkül.