AZ ÚJ ADATVÉDELMI RENDELET ÉS ALKALMAZÁSÁNAK KÉRDÉSEI

Baki József

2018. május 25-től új adatvédelmi normák kerülnek bevezetésre az Európai Unió tagállamaiban. Ezen időponttól alkalmazandó *Az Európai Parlament és a Tanács (EU) 2016/679 számú rendelete 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* (General Data Protection Regulation, továbbiakban: GDPR vagy Rendelet).

Amennyiben a hitelintézetek vezetőinek nagyjából egy oldalban kellene összefoglalniuk a GDPR változásait és azoknak a hitelintézetekre gyakorolt hatását, akkor az alábbi tíz pontban kísérelnék meg teljesíteni e feladatot:

- 2018. május 25-től az adatvédelmi normáknak való meg nem felelés esetén kiszabható bírság növekedéséből következően a jelenlegihez képest mintegy háromszázszoros működési kockázattal kell majd számolni (20 millió forint helyett 20 millió euró, illetve az adatkezelő, adatfeldolgozó éves világpiaci forgalmának 4%-a).
- A GDPR előírja, hogy az alkalmazásának időpontja előtt megkezdett adatkezeléseket is összhangba kell hozni a Rendelettel. Ezen kötelezettség a hitelintézet valamennyi személyes adatkezelést érintő folyamatának, személyes adatkezelésének teljes körű felülvizsgálatát jelenti, amely szinte minden szervezeti egységre jelentős feladatot ró majd.
- Az adatvédelmi incidenseket fő szabályként be kell majd jelenteni az adatvédelmi hatóságnál, és ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságaira, akkor az érintettet, érintetteket is tájékoztatni kell, ami számos további következménnyel járhat (esetleges hatósági eljárás, bírság, ügyfélpanasz, ügyfélkárigény, jó hírnév sérelme stb.).
- Jelentős feladattal és többletadminisztrációval jár, hogy az elszámoltathatóság elve alapján az adatkezelőknek 2018. májusától az adatkezelés megtervezésétől kezdve a megkezdésén át egészen a kezelt személyes adatok törléséig, valamennyi adatkezelési műveletet úgy kell megvalósítaniuk, hogy bármelyik pillanatban bizonyítani tudják, hogyan feleltek meg az adatvédelmi előírásoknak.
- A GDPR egyes magas kockázatúnak ítélhető esetekben bevezeti az adatvédelmi hatásvizsgálat intézményét, és ennek eredményétől függően egyes esetekben előzetes adatvédelmi hatósági konzultációt is előír, aminek az idővonzatát

is számításba kell venni a jövőben az egyes új eljárások bevezethetősége tekintetében.

- A GDPR szerinti egyes új jogalapok (pl. a jogos érdek) alkalmazása rugalmasabb, „piacosabb" adatkezelési lehetőségeket biztosít majd a jelenleginél, azonban az egyes adatkezelések új jogalapokba sorolása több bizonytalansággal és magasabb megfelelési kockázattal járhat a jövőben.
- A Rendelet a jelenlegi szabályozásnál részletesebb szabályokat tartalmaz az adatfeldolgozókra, ami valamennyi kiszervezett tevékenységet végzővel, valamint egyéb adatfeldolgozóval (pl. függő ügynök) kötött minden egyes korábbi együttműködésnek és szerződésnek a GDPR szempontjai szerinti felülvizsgálatát és módosítását teszi szükségessé.
- A GDPR-nak való megfelelésre való felkészülés informatikai fejlesztéseket is igényel (adattörlések, adathordozhatóság, álnevesítés, profilozás szabályai stb.), ami jelentős idő- és forrásigényekkel jár.
- A jelenlegi adatvédelmi felelősi tevékenységet a GDPR alapján „adatvédelmi tisztviselő" látja majd el, akinek a foglalkoztatása a jelenleginél szélesebb körben lesz kötelező, és a Rendelet számos garanciális elemmel, az eddiginél hangsúlyozottabban biztosítja függetlenségét, valamint tevékenységének szervezeti, működési feltételeit.
- A GDPR alkalmazására történő felkészülés során az új adatvédelmi intézményekre, eljárásokra figyelemmel új adatvédelmi szabályzat készítése szükséges; módosítandók az egyéb személyes adatkezelést is érintő eljárásrendek, személyes adatkezeléseket érintő dokumentumok is, ami a teljes belső szabályozási struktúra felülvizsgálatát és számos belső utasítás módosítását igényli.

Összességében tekintve, a GDPR alkalmazására való felkészülés összetett, számos szakterület tevékenységét érintő feladat, a felkészülés eredményessége pedig nagymértékben befolyásolja majd a hitelintézet jövőbeni működési kockázatait, az adatvagyon jogszerű hasznosíthatóságának lehetőségeit, valamint az esetleges meg nem felelésből eredő következmények hatással lehetnek a hitelintézet megítélésére, akár piaci versenyhelyzetére is.

A GDPR-ra való felkészülés ugyanakkor lehetőséget is kínál az üzleti szempontból kiemelkedő jelentőségű adatvagyon teljes körű áttekintésére az adatvagyon minél biztonságosabb, minél alacsonyabb működési kockázattal történő kezelése, a hitelintézet tevékenységi körével összefüggő, minél optimálisabb hasznosíthatósága céljából.

JEL- kódok: G2, K23
Kulcsszavak: adatvédelem, személyes adatok kezelése, pénzügyi intézmények

1. A GDPR ALKALMAZÁSÁVAL ÖSSZEFÜGGŐ, FŐBB VÁLTOZÁSOK

A GDPR-ral a jelenlegi uniós 95/46/EK irányelv helyett az egyes tagállamokra közvetlen hatályú uniós rendelettel történik meg a szabályozás, amelyet az EU-s határokon átnyúló hatósági jogkör, „egyablakos kiszolgálás" jellemez. E szabályok alapján tehát egyes, a GDPR-ban meghatározott esetekben akár külföldi adatvédelmi hatóság is eljárhat Magyarországon, illetve a magyar adatvédelmi hatóság külföldön. Ezek az intézmények közös műveleteket is végezhetnek, egyes esetekben hatáskört ruházhatnak át egymásra, egységességi mechanizmus céljából együttműködnek, stb. Kapcsolódó gyakorlat hiányában a határokon átnyúló hatósági jogkörnek a piaci szereplőkre gyakorolt hatása még nem ítélhető meg, de számos kérdést már jelenleg is felvet, amelyek egy része túlnyúlik a szűkebb értelemben vett személyes adatvédelmen.

Már az alapelvek körében is változásokat tartalmaz a Rendelet azzal, hogy megfogalmazza a *beépített és alapértelmezett adatvédelem követelményét*. Ennek célja egyrészt az adatvédelmi elvek hatékony megvalósítása, másrészt a Rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. A beépített és alapértelmezett adatvédelem meghatározó, kiemelt fontosságú követelmény a személyes adatok kezelése, védelme körében.

Szabályozza a GDPR az *elszámoltathatóság elvét*. Ennek alapján a tagállamoknak, a felügyeleti hatóságoknak egyrészt ösztönözniük kell olyan adatvédelmi tanúsítási mechanizmusok létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a Rendelet előírásainak; másrészt teljes körűen dokumentálni kell tudniuk az adatkezelések jogszerűségét. Mindig bizonyítani kell tudni, milyen jogalap alapján, milyen célból és csak a szükséges mértékben kezelnek-e adatokat. Mindez az adatvédelmi nyilvántartások összetett rendszerének kialakítását és belső szabályozását is igényeli.

Változásokat hoz a Rendelet az adatkezelésben meghatározó szerepet játszó *jogalapok tekintetében is*. A jelenlegi fő szabályként az érintett hozzájárulásán vagy a törvény rendelkezésén („kötelező" adatkezelésen) alapuló adatkezelési jogalap helyett hat jogalap áll majd rendelkezésre, és az eddiginél szűkebb körben lesz szükség az érintettek hozzájárulásának a beszerzésére. Önálló jogalapon alapul majd a szerződés teljesítéséhez szükséges adatkezelés, az adatkezelőre vonatkozó jogi kötelezettség teljesítése és az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés. Az új rendelkezések szerinti jogalapok alkalmazásának megkezdése, megfelelő kiválasztása – tekintettel a GDPR-hoz kapcsolódó hatósági és bírósági gyakorlat hiányára is – megfelelési kockázattal járhat.

Szabályozza a Rendelet az *adatgyűjtés céljától eltérő célra történő adatkezelést*. Jelenleg a meglévő adatoknak az eredeti céltól (eredeti hozzájárulástól, tájékoztatástól stb.) eltérő használata új adatkezelésnek minősül, és csak az annak való megfelelés (pl. újabb hozzájárulás és tájékoztatás) esetén kerülhet rá sor. A GDPR ennél rugalmasabb szabályokat állapít meg, mivel szempontrendszert határoz meg az eltérő adatkezelésnek az eredeti céllal történő összeegyeztetéséhez.

Bevezeti a Rendelet a „*Tanúsítás*" intézményét, amely alapján a tagállamoknak, a felügyeleti hatóságoknak ösztönözni kell olyan adatvédelmi tanúsítási mechanizmusok létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a Rendelet előírásainak. A tanúsítás vélelmezhetően bizalomerősítő, jó hírnevet növelő hatással járhat, és ezáltal akár üzleti előnye is jelentkezhet.

Előírja a Rendelet, hogy a tagállamoknak, a felügyeleti hatóságoknak ösztönözniük kell *ágazati magatartási kódexek* kidolgozását. A jelenlegi szabályozásnál részletesebben szabályozza a GDPR a tájékoztatási kötelezettségeket, és kitér olyan esetekre is, hogy melyek a rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg. A tájékoztatás szerepe a jogalapoknak és az adatvédelmi elveknek való megfelelőség mellett kiemelt fontosságú az adatkezelés érvényessége tekintetében.

Lényeges új rendelkezés, hogy új technológiák bevezetése esetén *hatásvizsgálat, hatástanulmány készítésének kötelezettségét* írja elő a GDPR, egyes esetekben adatvédelmi hatósági egyeztetést is előírva. A hatásvizsgálat módszertanának, eljárási szabályainak kialakítása fontos feladat lesz, amelyhez az adatvédelmi hatóság (NAIH) szempontrendszereket fog közzétenni.

Szabályozza a Rendelet a *belső adatvédelmi nyilvántartások követelményét* a kezelt adatok, adattovábbítások tekintetében. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), bár jelenleg is tartalmaz rendelkezéseket az adattovábbítási nyilvántartásról, tartalmát azonban nem határozza meg részletesen. A GDPR a jelenlegi, Infotv. szerinti definíciónál szűkebben határozza meg az adatvédelmi incidens fogalmát, ugyanakkor kötelezően előírja az adatvédelmi hatóság tájékoztatását, sőt, egyes esetekben az érintett(ek) tájékoztatását is. Mindez jelentős következményekkel járhat (hatósági eljárás, bírság, érintetti panasz, sérelemdíjigény stb.).

A GDPR az *adatfeldolgozókat* érintő, új rendelkezéseket is tartalmaz. Meghatározza az adatfeldolgozókra vonatkozó kötelezettségeket egyes szerződésbeli kikötések, adatvédelmi tisztviselő alkalmazása stb. tekintetében. Szabályozza a Rendelet a közös adatkezelést, a kapcsolódó, kötelező szerződési tartalmat és a közös adatkezelők felelősségét is, ennek alapján többek között a bankcsoportok adatkezelésének kereteit is újra kell gondolni. Közös adatkezelésnek az tekinthe-

tő, amikor az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg. Bár az Infotv. sem zárta ki a közös adatkezelést, a GDPR közvetlenül szabályozza azt, meghatározva a szerződési tartalmat és a felelősségre vonatkozó szabályokat is.

Rendezi a GDPR a *kötelező erejű vállalati szabályok (BCR)* alkalmazhatóságának feltételeit is.

A rendelkezés különösen azon adatkezelők számára bír kiemelt jelentőséggel, akik vállalkozáscsoportban működnek, és az Európai Unióból továbbítanak személyes adatokat az unión kívüli csoporttagnak.

Az érintettek jogai egy új joggal, az *adathordozhatósághoz való joggal* bővülnek. Az adathordozhatóság az érintetteknek az a joga, hogy a rá vonatkozó adatokat megkapja és továbbítsa; ha ez technikailag megvalósítható, kérje azoknak az adatkezelők közötti közvetlen továbbítását. A megvalósításhoz informatikai fejlesztési, információbiztonsági stb. kérdések is kapcsolódnak.

Az Infotv.-nek a jelenlegi, az automatizált adatfeldolgozással hozott döntésre vonatkozó rendelkezéseinél jóval részletesebben szabályozza a GDPR *az automatizált döntéshozatalt és a profilalkotást*. Az érintett joga, hogy ne legyen tárgya ilyen döntéshozatali eljárásnak. Biztosítani kell az érintettnek, hogy kifejtse a véleményét, illetve kifogást emeljen a döntés ellen, valamint kérje az emberi beavatkozást az adatkezelőtől. Automatizált adatfeldolgozással történő döntéshozatalra sor kerülhet továbbá tagállami jogszabályi felhatalmazás alapján is, ezen jogszabálynak azonban megfelelő garanciákat is kell biztosítania. Különleges adatokat érintő automatizált döntések meghozatala csak további feltételekkel megengedett.

Biztonsági célokból bevezeti a Rendelet az *„álnevesítés" intézményét*. A GDPR fogalommeghatározása szerint az „álnevesítés" a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni. Az álnevesítés alkalmazásának jelentősége a beépített és alapértelmezett adatvédelemnek való megfelelés körében is felvetődik.

A *törléshez való jog* („az elfeledtetéshez való jog") hangsúlyos követelménye a Rendeletnek. Az Infotv. eddig is tartalmazta a személyes adatok törlésének kötelezettségét, ha az adatkezelési cél megszűnt, és egyéb törvényi indokokból nem állt fenn további megőrzés lehetősége, illetve kötelezettsége. A GDPR az Infotv.-nél részletesebben szabályozza a törléshez való jogot, és az érintetti jogok körében jelentős hangsúllyal szerepel „az elfeledtetéshez való jog".

Az *adattovábbítások kérdéskörét* tekintve a GDPR az Infotv. rendelkezéseinél nagyobb terjedelemben, részletesebben szabályozza az adattovábbítások szabályait, feltételeül szabva, hogy az adatkezelő és az adatfeldolgozó teljesítse a GDPR-nak az adattovábbításokra vonatkozó feltételeit, külön szabályozva a megfelelő garanciák alapján történő adattovábbításokat.

Szélesíti a GDPR az *adatvédelmi tisztviselő* (az Infotv. szerinti jelenlegi adatvédelmi felelős) kötelező alkalmazásának körét, erősíti jogállását és fokozza e megfelelési kontrollfunkció védelmét, ennek alapján újragondoltatja e feladatkörnek a hitelintézeteknél betöltött szerepét.

2. SZÉP ÚJ VILÁG: AZ ÚJ JOGALAPOK

Megfelelő adatkezelési jogalap hiányában nem lehet jogszerű az adatkezelés. Ezért a GDPR szerinti új jogalapok alkalmazásának egyes kérdéseinek a tisztázása kiemelten fontos részét jelenti a felkészülésnek. A belső adatvédelmi szabályozást alkalmazóknak megfelelő iránymutatással kell rendelkezniük a jogalapok megállapíthatóságára vonatkozóan.

Lényeges különbség a GDPR és az Infotv. jogalapokra vonatkozó rendelkezéseinek alkalmazása között, hogy amíg az Infotv. rendelkezései alapján jelenleg két fő jogalap, az önkéntes hozzájárulás és a törvény kötelező rendelkezése szolgál az adatkezelések jogalapjául a hitelintézeteknél is, addig 2018. május 25-től több jogalap szolgál majd az adatkezelések alapjául. Így – egyéb jogalapok mellett – a szerződésen, jogos érdeken alapuló és az adatkezelőre vonatkozó jogi kötelezettség teljesítésére vonatkozó adatkezelésekkel bővíti, szélesíti a jogalkotó az adatkezelések jogalapját.

Mivel az Infotv. alkalmazásának jelenlegi gyakorlatához képest több jogalap jellemzi majd a személyes adatkezeléseket, mint jelenleg, alkalmazásukkal kapcsolatban még sok a nyitott kérdés. Alkalmazásuk, elhatárolásaik tekintetében a következő évek szakmai elméleti vitái, a hatósági és bírósági gyakorlat fog letisztultabb gyakorlatot eredményezni. Az egyes adatkezelési célok teljes körű áttekintése és a GDPR szerinti, megfelelő jogalapba történő, jövőbeni besorolási szempontjainak megállapítása, szabályozása kiemelkedő feladat lesz az adatkezelőknél mindazon szakterületek bevonásával, ahol a személyes adatok kezelése, illetve az adatkezelési célok meghatározása történik.

Ugyanakkor a GDPR 2018. május 25-i alkalmazásának megkezdésekor lesz egy jelentős ügyfélállomány, amelyik esetében az adatkezelés jogalapja önkéntes hozzájárulás volt. Bár már a jelenleg hatályos uniós adatvédelmi irányelv 7. cikke alapján – a GDPR-hoz hasonlóan – eredetileg is többféle jogalap lett volna indokolt, az Infotv. szűkítő rendelkezései alapján az adatkezelők önkéntes hozzájárulásban

kényszerültek megjelölni a jogalapot. Jelenlegi tudásunk szerint a már most folyamatban lévő adatkezelések tekintetében – értelemszerűen, ha a kiinduláskor megfelelő volt a jogalap – nem szükséges változtatás, új hozzájárulás kérése. Természetesen, ha az adatkezelések körében a felülvizsgálat során felmerül, hogy az adatkezelés nem jogszerű, az jogszerűvé csak akkor tehető, ha harmonizálják a jogszabályi feltételekkel, így adott esetben szükségessé válhat az érintettek újra nyilatkoztatása is.

A GDPR alapján, annak hat jogalapjából a pénzügyi szervezetek esetében a jövőbeni gyakorlati alkalmazás szempontjából *négy jogalap* érdemel különösen figyelmet:

- 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.
- Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.
- Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.
- Az érintett hozzájárulása.

Ezen jogalapokon túl, a fennmaradt két GDPR-jogalapot (közérdek, valamint az érintett létfontosságú érdeke) vizsgálva, azok a pénzügyi szervezetek tevékenységi körében a napi gyakorlatban kevésbé tipikusan merülnek fel. Az önkéntes hozzájárulás mint jogalap vélelmezhetően szűkebb körben marad fenn, mint jelenleg az Infotv. rendelkezései alapján, mivel a szerződéshez kapcsolódó jogalap és a jogos érdek alkalmazhatósága részben felváltja majd a jelenlegi önkéntes hozzájárulás alkalmazásának jelentős részét.

Az önkéntes hozzájárulás törvényi kritériumait az Infotv.-nél részletesebben munkálja ki a GDPR; ezekre a követelményekre alkalmazásának körében fokozottan kell majd figyelni. A hozzájárulásnak szabad elhatározásból adottnak, specifikusnak, megfelelő tájékoztatáson alapulónak és tevőlegesnek kell lennie. Nem tevőleges magatartás pl. a hallgatás, az előre kipipált checkbox (jelölőnégyzet). Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ha az érintett hozzájárulását olyan írásbeli nyilatkozatban adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájáru-

lását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti a Rendeletet, kötelező erővel nem bír. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. Az érdekmérlegelésen alapuló jogos érdeket mint jogalapot tekintve, a jelenleg hatályos Infotv. annak alkalmazására csak rendkívül szűk körben nyújt lehetőséget. A GDPR a jelenleg hatályos törvényi rendelkezéseknél jóval szélesebb utat nyit e jogalap alkalmazásához.

3. A JOGOS ÉRDEK. EGY ÚJ „CSODAFEGYVER" ÉS ALKALMAZÁSÁNAK KÉRDÉSEI

A GDPR alapján alkalmazásra kerülő jogalapok tekintetében a jövőben várhatóan az érdekmérlegelésen alapuló „jogos érdek" lesz a jogalap számos olyan esetben, ahol jelenleg önkéntes hozzájárulás beszerzésére kényszerültek az adatkezelők. Ilyen esetek lehetnek például, amikor valamely jogszabályból levezethető a hitelintézet jogos érdeke, azonban ezt direkt módon nem határozza meg majd jogi kötelezettségként a jogalkotó. A munkaügyi adatkezelések esetében szinte kizárólag ez lesz majd a jogalap, de felvetődik még a direkt marketingnél is egyes esetekben (pl. hírlevélküldés).

Jelenleg a hatályos Infotv. a jogos érdek alkalmazhatóságát szűk körben teszi csak lehetővé. Így jelenleg ott is az önkéntes hozzájárulás a jogalap, ahol egyébként a jelenleg hatályos uniós adatvédelmi irányelv 7. cikke szerint lehetne jogos érdek is, azonban a hatályos magyar törvényi szabályozás szűkítőbb jellegű az irányelv rendelkezéseinél.

A NAIH több ajánlásában és határozatában már jelenleg is elfogadja az irányelv 7. cikk f) pontja szerinti jogos érdek közvetlen alkalmazását, egyes esetekben pedig (a munkavállalói jogviszony esetében) e jogalapot tekinti fő szabályként alkalmazandónak.

A NAIH/2015/515/3/H. /NAIH-1116/2014/H/ ügyben hozott határozatában a NAIH az irányelv 7. cikkének f) pontja tekintetében hivatkozik az Európai Unió Bírósága előzetes döntéshozatali eljárás során hozott azon döntésére, hogy az irányelv ezen pontjának közvetlen hatálya van, tehát arra a tagállami bíróság előtt bárki hivatkozhat. A hatóság arra is utalt ezen határozatában: tekintettel arra, hogy az Infotv. nem megfelelően ültette át az irányelv 7. cikk f) pontját, ezért a hatóság a 29-es adatvédelmi munkacsoport 6/2014. számú véleményében részletesen tárgyalt érdekmérlegelési tesztet az irányelv 7. cikk f) pontja alapján végezte el.

A Nemzeti Adatvédelmi és Információszabadság Hatóságnak a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről szóló, 2013. 01. 23-i ajánlása hivatkozik arra, hogy az adatvédelmi irányelv 29. cikke

szerint létrehozott adatvédelmi munkacsoport több állásfoglalásában is kifejtette: a munkavállaló-munkáltató viszonyában megkérdőjelezhető az önkéntes hozzájárulás lehetősége, ezért a munkajog világában az adatvédelmi irányelvben szereplő, más jogalapok alkalmazása indokolt. Az adatvédelmi munkacsoport a „hozzájárulás" fogalom meghatározásáról szóló 15/2011. számú véleményében pedig azt is kifejtette, hogy a jogszerű adatkezelésnek nemcsak a hozzájárulás lehet az egyetlen jogalapja, hanem az adatvédelmi irányelv 7. cikkében szereplő, többi jogalapot is alkalmazhatják az adatkezelők.

Mindezek ellenére, az adatkezelők jelenleg még az Infotv. hatályos rendelkezéseire tekintettel, óvatosak a jogos érdek mint jogalap alkalmazása tekintetében.

A GDPR közvetlen hatálya alapján egyértelműen megnyílik majd az út a hitelintézet *jogos érdekére alapított adatkezelésre* megfelelő érdekmérlegelés alapján. E jogalap alkalmazása ugyanakkor vékony jégre lépést is jelent, hiszen alkalmazásának esetei nem határozhatók meg taxatív módon, az érdekmérlegelés eredményét vitathatja az ügyfél is, és megalapozatlannak tekintheti a hatóság is.

Az uniós adatvédelmi, ún. 29-es munkacsoport is foglalkozott a jogos érdek alkalmazásának kérdéseivel. A munkacsoport által alkalmazott „érdek" fogalma az adatkezelés céljánál tágabb kategória, ahol a tételes anyagi jogi szabályok mellett akár általános alapelvek is figyelembe veendők. A NAIH a Google Street GSV-szolgáltatásával kapcsolatosan elfogadta, hogy a Google-nak a GSV-szolgáltatás bevezetéséhez olyan jogos érdeke fűződik, amelynek érvényesítéséhez szükséges lehet az érintettek adatainak kezelése. Úgy tűnik, az értelmezés megnyitotta az utat a széles értelemben vett gazdasági érdek mint jogos érdek elismerése felé.

A bírói gyakorlatban ugyanakkor a jogos érdeket „mindig valamely jogszabályban nevesített módon megjelenő érdekhez kell kötni, ellenkező esetben a »jogos« érdek helyére a »méltánylást érdemlő érdek« kerülne." E jogalap alkalmazása tehát nagyfokú óvatosságot, önmérsékletet követel, hiszen amennyiben a jogalap nem bizonyulna megalapozottnak, az érvénytelen adatkezelést eredményezhetne, amelynek beláthatatlan következményei lehetnének a tömegszerű adatkezelések tekintetében.

Tehát jelenleg is vannak a jogos érdek alkalmazásával kapcsolatban adatvédelmi hatósági esetek, vélemények, összességében azonban vélelmezhetően csak több év adatvédelmi hatósági és bírósági gyakorlata után lesz nagyobb biztonsággal alkalmazható ezen jogalap. Külön vizsgálat tárgyát kell annak képeznie, hogy a hitelintézeti tevékenységben hol jelentkezhetnek olyan adatkezelési célok, ahol e jogalap megalapozottan válthatja majd ki az eddigi önkéntes hozzájárulások szükségességét. A jogszerű adatkezeléshez e jogalap mellett is értelemszerűen meg kell felelni az adatkezelés elveinek és a tájékoztatási feltételeknek is. A jogos érdek tehát nem üzleti csodafegyver, de érdekmérlegelésen alapuló, gondos alkalmazása egyszerűbbé, életszerűbbé teszi a hitelintézeti gyakorlatot az érintettek jogainak sérelme nélkül.

4. A GDPR ALKALMAZÁSA ÉS AZ EGYÉB KAPCSOLÓDÓ TÖRVÉNYI SZABÁLYOZÁSOK

Jelenleg számos törvény tartalmaz olyan rendelkezéseket hazai jogunkban, amelyek személyes adatkezelést keletkeztetnek a hitelintézetek tevékenységében. A GDPR alkalmazásával összefüggésben elkerülhetetlenül szükséges ezen törvények áttekintése, továbbá a nem törvényszintű, de személyes adatkezelést érintő, egyéb normák vizsgálata is a tekintetben, hogy hogyan harmonizálnak a GDPR rendelkezéseivel, illetve hogyan érintik az új jogalapok az ezen normákkal összefüggésben kezelt személyes adatok 2018. május 25-ét követő kezelését.

A törvények vizsgálata jelentős különbségeket mutat az adatkezelések meghatározásának módja tekintetében, ami determinálja a jogalap-meghatározásokat. Ezek egy része direkt módon kötelező adatkezeléseket ír elő, taxatíve meghatározva a kezelendő adatokat is, illetve azok továbbításának feltételeit is (pl. Pmt., KHR stb.). Ezek esetében jelenleg egyértelmű, hogy az adatkezelés jogalapja a törvény kötelező rendelkezése.

Más esetekben a törvényi rendelkezések közvetve személyes adatkezeléseket generálnak, azonban a kezelendő személyes adatokat nem határozza meg a törvény. E kettő között is találhatók olyan törvényi rendelkezések, ahol a személyes adatkezelés behatárolhatóbb követelmény, de körülírásuk nem harmonizál teljesen az Infotv. kötelező adatkezelésekre vonatkozó, az adatok kezelését taxatíve történő meghatározásának követelményével. A törvényeken túl kormányrendeletek és miniszteri rendeletek is érintenek személyes adatkezeléseket; ezek esetében – törvényi felhatalmazás hiányában – jelenleg önkéntes hozzájárulás az adatkezelés jogalapja. A GDPR alkalmazása után a jogi kötelezettség teljesítése, illetve a jogos érdek alapján kezelhetőbbnek tűnik majd ezen adatkezelések megfelelő jogalapba történő besorolása.

Lényeges kérdés a GDPR rendelkezéseinek jövőbeni hatálybalépése szempontjából, hogy alkalmazásáig módosulnak-e egyes jogszabályok. Például amennyiben a Hpt., Bszt. bank- és értékpapírtitok továbbítására vonatkozó, jelenlegi szabályozása nem módosul a jogos érdeken, egyéb jogi kötelezettségen alapuló jogalappal, akkor ezek a „piacosabb" rendelkezések nem lennének alkalmazhatók, noha ez egyébként több lehetőséget jelenthetne a csoport-tagok közötti adatátadások, esetleges egyéb szerződéses jogviszonyok tekintetében.

A reklámszakma képviselői, DM-szakemberek is nagy várakozással tekintenek a GDPR-ra, lehetőséget látva pl. a jogos érdek egyes esetekben történő alkalmazására (pl. hírlevélküldés esetében). Amennyiben viszont nem kerülne módosításra a reklámtörvénynek (Rktv.) a reklámüzenetek küldésére vonatkozó, szűk kivételtől eltekintve, előzetes hozzájáruláson alapuló fő szabálya, úgy érdemi változást aligha jelenthetne e területen a GDPR, amennyiben a reklámtörvény minősülne

lex specialisnak. Más kérdés, hogyan járjon el az adatkezelő, ha értelmezése szerint olyan, a GDPR rendelkezéseivel nem harmonizáló törvényi rendelkezéssel találkozna, amely területen a GDPR nem biztosít tagállami hatáskörben eltérő szabályozási lehetőséget.

5. AZ ADATVÉDELMI ÁGAZATI KÓDEX MEGALKOTÁSÁNAK KÉRDÉSEI. BIZTONSÁGI ÖV VAGY A SZABADSÁG KORLÁTOZÁSA?

A GDPR előírja, hogy a tagállamoknak, a felügyeleti hatóságoknak ösztönözni kell az ágazati magatartási kódexek kidolgozását. Előnye lenne egy ilyen kódexnek, hogy ha elfogadná a hatóság a kódex egyes rendelkezéseit (pl. a jogalapok alkalmazásának, így pl. különösen a jogos érdek megállapításának szempontjai tekintetében), ez csökkentené a megfelelési, működési kockázatokat és biztonsági övként működhetne. Tudjuk ugyanakkor, hogy a biztonsági öv egyúttal korlátozza is a szabad mozgást, és nem mindenki híve az alkalmazásának, még ha ez kockázattal is jár. A hitelintézet jó hírnevének növeléséhez ugyanakkor bizonyosan hozzájárulna egy ilyen, az adatvédelmi hatóság által elfogadott kódex.

Egy ágazati kódex tartalmi kimunkálásának, hatóság általi elfogadásának folyamata akár több évig is elhúzódhat, és jelenleg nem ismert (előzetes felmérést igényelne), hogy a hitelintézetek milyen köre igényelné, vetné magát alá annak. A kódex ágazati szintű előkészítő munkái ugyanakkor már önmagukban is segíthetnék a hitelintézetek egységes jogértelmezési gyakorlatának kialakulását a GDPR alkalmazásához. Felvetődhetne a kódexen kívül akár más megoldások keresése is a GDPR alkalmazásával kapcsolatos biztonságosabb, egységesebb gyakorlat kialakításához. Így pl. a jogalap-alkalmazások valamely ágazati módszertanának kimunkálása és esetleges hatósági auditáltatása, vagy egy adatvédelmi ágazati szabályzat tartalmi követelményeinek meghatározása, auditáltatása a hatósággal, stb.

6. ADATVÉDELMI FELELŐSBŐL ADATVÉDELMI TISZTVISELŐ. NÉVCSERE VAGY SZEREPVÁLTÁS?

A GDPR alkalmazásával eltűnik jogunkból az Infotv. nem túl szerencsésnek tűnő „adatvédelmi felelős" fogalma, és helyébe az adatvédelmi tisztviselő kerül. A data protection officer „adatvédelmi felelősként" való jelenlegi meghatározása akár félrevezető is lehet a feladatát illetően az e tisztség törvényi feladatait kevésbé ismerők számára. Az a gyakorlat, hogy ezen adatvédelmi „felelős" feladatkört leggyakrabban a jogi szakterülethez kapcsolódó jogtanácsosok látják el, szintén azt

látszik alátámasztani, mintha egy meghatározott jogterületre specializált jogtanácsosként operatív feladatok ellátására, ügyintézői szintű kiszolgálásra lennének predesztinálva.

Az adatvédelmi felelős Infotv. szerinti, törvényben meghatározott feladatait tekintve ugyanakkor egyértelmű, hogy az adatvédelmi normák megtartásának szervezeten belüli független, legfőbb ellenőrző szerve, aki ellenőrzési kötelezettségén túl közreműködik, segítséget nyújt az adatkezelésekkel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában. Utóbbi hatáskörei egyfajta tanácsadói, valamint az ügyfelek, munkavállalók mint érintettek tekintetében valamiféle belső szervezeti ombudsman jellegű tevékenységként lennének definiálhatók. Törvényi feladataival és azzal, hogy az adatvédelmi felelős a törvény kogens rendelkezése alapján közvetlenül a szerv vezetőjének felügyelete alá tartozik, a többi megfelelési kontrollal azonos szinten helyezkedik el a törvény alapján azzal, hogy ellenőrzésének tárgyát a személyes adatvédelemre vonatkozó jogszabályok és az adatvédelmi szabályzatban foglaltak betartásának ellenőrzése képezi.

Mivel a hitelintézetek esetében szinte alig fordul elő olyan folyamat, szervezeti egység, ahol ne történne személyes adatkezelés, aligha túlzás azt állítani, hogy az adatvédelmi felelős, illetve majd az adatvédelmi tisztviselő megfelelőségi kontrollterülete szinte a hitelintézet teljes tevékenységét lefedi.

A GDPR szélesíti az adatvédelmi tisztviselő kötelező alkalmazásának körét, erősíti jogállását, és fokozza e megfelelési kontrollfunkció védelmét. A GDPR a jelenleg hatályos szabályozásunktól eltérően nem meghatározott (jogi, informatikai) iskolai végzettséget követel meg az adatvédelmi tisztviselői feladat ellátásához, hanem elsődlegesen a „szakmai rátermettséget és különösen az adatvédelmi jog és gyakorlat szakmai szintű ismeretét", illetve a Rendeletben meghatározott feladatok ellátására való alkalmasságot tekinti a kiválasztás szempontjainak.

A GDPR rendelkezései szerint az adatvédelmi tisztviselő számára biztosítani kell a Rendelet szerint feladat ellátásához, szakértői szintű ismereteinek fenntartásához szükséges forrásokat, hogy időben bekapcsolódjon a személyes adatok védelmével kapcsolatos ügyekbe; biztosítani kell, hogy feladatai ellátásával kapcsolatban senkitől ne fogadjon el utasítást, közvetlenül a „legfelső vezetésnek" tartozzon felelősséggel, „feladatai ellátásaival összefüggésben nem bocsáthatja el és szankcióval nem sújthatja" az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt.

A Rendelet alapján az érintettek közvetlenül az adatvédelmi tisztviselőhöz fordulhatnak. Az adatvédelmi tisztviselő tevékenységében a függetlenség biztosítása mellett kiemelt figyelmet érdemel az összeférhetetlenség vizsgálata is. Aligha összeférhető az a megoldás, ahol olyan munkakörrel kerül összekapcsolásra, amelynek körében személyes adatkezelések meghatározása, konkrét kezelése történik. Ilyen pl. a compliance szakterület, amelynek körében jellemzően olyan adatkeze-

lésekre kerül sor, amelyek az adatvédelmi tisztviselő személyes megfelelési kontrolltevékenységébe esnek (bennfentes kereskedelemmel, saját számlás ügyletekkel, összeférhetetlenséggel stb. kapcsolatban kezelt személyes adatok).

Példa egy kontrollfunkció függetlenségének meghatározására a Magyar Nemzeti Banknak az informatikai rendszer védelméről szóló 7/2017. (VII.5.) számú ajánlása, amely kimondja: „*Függetlenség alatt az értendő, hogy az ellenőrzési terület nem vonható be az ellenőrzendő kontrollintézkedések megtervezésébe, kiválasztásába, implementálásába vagy azok működtetésébe, és nincs alárendelt viszonyban az ellenőrzött területtel.*" (13.1.2. pont)

Az adatvédelmi tisztviselő új szerepkörét vizsgálva, az hangsúlyosabban mutat egy független megfelelési kontrollfunkció, illetve az azzal kapcsolatos vezetői feladatkör irányába. Önmagában külön tanulmányt érdemel az adatvédelmi megfelelési kontroll új szervezeti és személyi feltételeinek vizsgálata, a kontrollfunkciók egymáshoz való viszonya, figyelemmel a kockázat alapú belső ellenőrzési szemléletre is.

7. MÚLT ÉS JÖVŐ TALÁLKOZÁSA. HOGYAN KÉSZÜLJÜNK A GDPR ALKALMAZÁSÁRA?

A GDPR-t 2018. május 25-től kell alkalmazni, de az alkalmazásának időpontja előtt megkezdett adatkezeléseket a Rendelet hatálybalépésétől (2016. május 24.) számított két éven belül – gyakorlatilag a Rendelet alkalmazásáig – „összhangba kell hozni" a GDPR-al. Így kettős feladat hárul az adatkezelőkre:

– egyrészt 2018. május 25-re „ugrásra készen" kell állni az új adatvédelmi normák alkalmazására a belső szabályozással és az egyéb szervezeti, személyi és informatikai feltételek biztosításával az ezen időponttól alkalmazandó rendelkezések végrehajtására,
– másrészt ezen időpontig felül kell vizsgálni a személyes adatkezeléssel járó valamennyi folyamatot, és ezen adatkezeléseket is harmonizálni kell a GDPR rendelkezéseivel.

A felkészülés folyamata több szakaszra, feladatra osztható:

a) a folyamatban lévő adatkezelések felmérése;

b) a folyamatban lévő adatkezelések jogszerűségének felülvizsgálata, az adatkezelés jogszerűségével kapcsolatos megállapítások;

c) az esetleges törvényi meg nem felelés esetén a szükséges intézkedések meghatározása és végrehajtása;

d) az adatkezelések GDPR-al való harmonizálási feltételeinek vizsgálata, a szükséges intézkedések meghatározása és végrehajtása;

e) a folyamatok, adatkezelések áttekintésére is figyelemmel, a GDPR alkalmazásához a belső adatvédelmi szabályzat és kapcsolódó egyéb belső szabályozás megalkotása;

f) a GDPR alkalmazásáig a megfelelőség biztosításához szükséges szervezeti, személyi, informatikai, egyéb technikai feltételek megvalósítása;

g) külön is kiemelten az oktatási feladatok elvégzése;

h) a GDPR alkalmazására való felkészülés folyamatainak, az adatkezelés szabályozásának, tényleges jogszerűségének az értékelése, meghatározott körben kvázi belső auditja, illetve esetlegesen külső audit.

A felkészülés szakaszaihoz kapcsoló feladatok végrehajtása azok részletes kimunkálását és ahhoz kapcsolódóan külön szempontrendszerek, valamint egyéb dokumentumok kimunkálását igénylik.

7.1. A folyamatban lévő adatkezelések felmérése

A folyamatban lévő adatkezelések eredményes felmérése kulcsfontosságú, mert ez szolgál majd kiindulási alapul az adatkezelések jogszerűségének vizsgálatához, a GDPR-ral történő harmonizációhoz, az adatvédelmi nyilvántartások kialakításához és az elszámoltathatóság elvének való megfeleléshez is. Amely adatkezelés felülvizsgálata ebből a felmérésből esetlegesen kimarad, az lappangó megfelelési kockázatként élhet tovább.

Ehhez segítséget nyújthatnak a korábbi belső adatvédelmi nyilvántartások és az adatleltár, de a felülvizsgálathoz adatkezelési célonként át kell tekinteni valamennyi adatkezelést minden személyes adatkezeléssel járó folyamatban. Így a termékfejlesztés, hitelnyújtás, hitelgondozás, követeléskezelés, pénzforgalmi szolgáltatások, befektetési szolgáltatási tevékenység, DM (direkt marketing), compliance, HR, munkaügy, bankbiztonság stb. folyamatait, az adattovábbítások, nyilvántartások, informatikai rendszerekben történő rögzítések, rendszerek közötti átjárások, rendszerekből történő adattörlések, iratselejtezések stb. körében minden adatkezelést felül kell vizsgálni. Az adatkezelési célonként történő felülvizsgálat a termékek, szolgáltatások körében gyakorlatilag termékszintű felülvizsgálatot igényel.

A folyamatban lévő adatkezelések áttekintése összetett szempontrendszer kialakítását igényli.

Így egységes adatfelmérő lapok, kitöltési útmutatók létrehozása indokolt az adatkezelések, adattovábbítások felméréséhez, szempontrendszer a jogszerűség megállapításához, az adattisztításokhoz, a GDPR harmonizációs feladatokhoz, külön is figyelemmel az elszámoltathatóság elvére, a GDPR szerinti nyilvántartások kimunkálására.

Ilyen szempontok a folyamatban lévő adatkezelések felméréséhez: az adatkezelés megnevezése, az érintettek kategóriái, kezelt adatok, az adatok kezelésének célja, jogalapja, az adatok forrása, gyűjtésük módja, hol rögzítik, tárolják azokat, kik az adatfeldolgozók, bankon kívülre, külföldre történik-e adattovábbítás, alkalmaznak-e automatikus adatfeldolgozást, profilozás történik-e az adatokkal, meddig őrzik meg azokat, stb. Fontos felmérni, megvizsgálni azt is, hogy jelenleg milyen adatkezelési tájékoztatások kapcsolódnak az egyes adatkezelésekhez.

A GDPR 2018. május 25-i alkalmazásához valamennyi adatkezelési tájékoztató átdolgozandó (honlapos általános, cookie, egyes termékek, szolgáltatások igénybevételéhez kapcsolódó tájékoztatók, szerződésekben szereplő adatkezelési tájékoztatók, rögzített hang- és képfelvételekhez, beléptetőrendszerekhez, direkt marketinghez, álláspályázatokhoz, munkaügyi adatkezelésekhez stb. kapcsolódó tájékoztatók).

Az adatkezelő pénzügyi szervezeteken belül – az egyes szervezeti egységek tevékenységéből eredően – jelentős eltérések mutatkoznak az általuk történő, szélesebb értelemben vett „adatkezelések" tekintetében. Így pl. vannak szervezeti egységek, amelyek tevékenységük során személyes adatok kezelésének körét határozzák meg, de konkrét személyes adatokat akár nem is „kezelnek". Ilyen a termékfejlesztési-szabályozási tevékenység, amikor új termékek esetében kialakítják a termékre, a szolgáltatást igénylő hitelkérelemre stb. vonatkozó nyomtatványokat a kapcsolódó tájékoztatókkal és nyilatkozatokkal. A preventív megfelelési kontroll az e területek által meghatározott adatkezelések, kapcsolódó belső szabályzatok, eljárásrendek tekintetében kiemelkedő fontosságú.

Más szervezeti egységek tevékenysége körében konkrétan merül fel személyes adatok kezelése (hitelezési, kockázatkezelési szakterület, követeléskezelés stb.). Vannak adattovábbításra szakosodott szervezeti egységek (pl. az MNB, MÁK stb. részére rendszeres adatszolgáltatást végző szakterület vagy a hatósági megkeresésekre válaszadással foglalkozó szakterület, szervezeti egység). Szintén eltérő módon jelennek meg az adatkezelések pl. a marketing szakterületen, ahol a vonatkozó speciális törvények (pl. a reklámtörvény, az Rktv.) alapján kerülnek meghatározásra, gyűjtésre, nyilvántartásra és kezelésre személyes adatok.

Máshol jellemzően ügyfeleknek nem minősülő, harmadik személyek adatainak kezelésére kerül sor (pl. a társasági titkárságokon a Hpt. szerinti bizottságok külső tagjainak személyes adatai, külsős felügyelőbizottsági-igazgatósági tagok, részvényesek stb.)

Más vizsgálati szempontrendszert igényel az informatikai szakterület, ahol egyrészt azt kell áttekinteni, hogy egyáltalán milyen rendszerekben, milyen célból, milyen személyes adatok kezelése történik, illetve ezekből milyen adattovábbítások történnek, valamint az informatikai rendszerek mennyiben felelnek meg a

törvényi követelményeknek, mind a jelenlegi Infotv., mind majdan a GDPR követelményeinek. Ilyen követelmények pl. az adattörlések, megjelölések, zárolások technikai feltételei vagy az automatikus adatfeldolgozás, profilozás, álnevesítés, adathordozhatóság szempontjai.

De érinti a felülvizsgálat, a GDPR-harmonizáció az információbiztonság teljes területét is, ez pedig saját vizsgálati, harmonizálási szempontrendszer kimunkálását, alkalmazását igényli.

Az információbiztonságot, illetve informatikai biztonságot érintő felkészülés olyan terület, amely önálló szempontrendszert követel meg. Az alkalmazott fogalmak, a szakterületet érintő, különböző jogszabályoknak való megfelelés kérdései, a szakterület és különösen a kapcsolódó kontrollfunkció vizsgálata önálló tanulmányt is érdemel.

De külön vizsgálat tárgyát képezi valamennyi adatfeldolgozó tevékenységének a GDPR-követelmény szempontjából történő felülvizsgálata, majd a szerződések módosítása, amely ugyancsak saját szempontrendszert igényel, és megkívánja valamennyi adatfeldolgozói tevékenység felülvizsgálatát, valamennyi kapcsolódó szerződés módosítását. Nem elhanyagolandó kérdés, hogy a GDPR-változások vélelmezhetően számos informatikai fejlesztést generálnak, amelyek kiszervezett tevékenységhez kapcsolódnak, és az adatfeldolgozóknál realizálódnak. Ennek pedig fejlesztési idő- és költségvonzata merül fel, ami egyéb, a hitelintézetek és a kiszervezett tevékenységet végzők közötti szerződéses jogviszonyok tartalmát is érinti.

Ugyanakkor a felkészüléshez kapcsolódó, valamennyi szempontrendszer végső céljának harmonizálnia is kell. A felülvizsgálat szempontrendszerét úgy szükséges kialakítani, hogy az adatfelmérő lapok, táblázatok tartalma alapján megítélhető legyen az adatkezelés jogszerűsége, meghatározhatók legyenek a a harmonizáció érdekében teendő, további intézkedések. A szempoontrendszernek – az elszámoltathatóság elvére is figyelemmel – biztosítania kell az adatkezelések átláthatóságát, és alapul kell szolgálnia a Rendelet elvárásainak megfelelő, belső adatvédelmi nyilvántartások kialakításához.

Fontos kérdés az egyes szakterületek tevékenységét is szabályozó, kapcsolódó személyes adatkezelésekről is rendelkező jogszabályok, belső szabályzatok, eljárásrendek hálójának feltérképezése, illetve kontrollja mind az Infotv., mind a GDPR-harmonizáció (illetve a szükséges módosítások) szempontjából.

7.2. A folyamatban lévő adatkezelések felmérését követő feladatok

Az adatfelméréseket követő, egyik fő feladat az adatkezelések jogszerűségének vizsgálata, amelyet adatkezelési célonként szükséges végrehajtani. Jogszerű adatkezelésről csak akkor beszélhetünk, ha megfelelő az adatkezelés jogalapja, az adatkezelés megfelel az adatkezelés elveinek, és az érintett a jogszabályi követelményeknek megfelelő tájékoztatást kapott. A jogszerűség vizsgálatához ezen követelmények figyelembevételével kimunkált szempontrendszer kidolgozása indokolt. A vizsgálatot egyrészt a hatályos Infotv. rendelkezéseinek figyelembevételével szükséges elvégezni az esetlegesen nem jogszerűnek minősülő adatkezelések megszüntetése érdekében, másrészt ki kell alakítani a jövőre nézve, hogy az ugyanezen célokból 2018. május 25-től megkezdett adatkezelések esetében melyek lesznek az új jogalapok.

A GDPR szerint, amennyiben az adatkezelések a jelenleg hatályos 95/46/EK irányelv szerinti hozzájáruláson alapultak, és az érintettek a Rendeletben foglalt feltételekkel összhangban adták meg hozzájárulásukat, akkor nem kell ismételt hozzájárulást kérni. Problematikusabb, ha a jogszerűségi vizsgálat esetlegesen olyan hiányosságot tárna fel, ahol a jogszerűség valamelyik eleme nem felelne meg teljes körűen. Itt az lehet a kérdés, hogy pótolható-e (pl. tájékoztatással) a hiányosság, vagy az érvénytelenség egyéb okból nem küszöbölhető ki (pl. valamely adatkezelés tekintetében nem felel meg az adattakarékosság elvének).

Lényeges kérdés annak a meghatározása, hogy a GDPR rendelkezéseiből melyeket kell alkalmazni a folyamatban lévő adatkezelésekre, és melyeket kizárólag a 2018. május 25-e után megkezdett adatkezelésekre. Így pl. az adatvédelmi hatásvizsgálat elvégzésének kötelezettsége nem terjed ki a korábban megkezdett, már folyamatban lévő adatkezelésekre.

Az adatkezelés olyan új elvének, mint az elszámoltathatóság elvének való megfelelés viszont már minden 2018. május 25-én fennálló adatkezelés esetén követelményként értelmezhető. Azaz bármikor dokumentálni kell tudni az adatkezelés jogszerűségét. Ez már a jelenleg hatályos Infotv.-ben is megjelenik annyiban, hogy a bíróság előtti eljárásban jelenleg is az adatkezelőnek kell bizonyítania jogszerű adatkezelését, ami már körvonalazza e tekintetben ezen elvet.

A GDP szerinti belső adatvédelmi nyilvántartásoknak is nyilvánvalóan meg kell felelni mind a GDPR alkalmazása előtt, mind az utána megkezdett adatkezelések tekintetében. Jelenleg is követelmény a belső adatvédelmi nyilvántartás, bár annak tartalmát nem határozza meg az Infotv. A GDPR e tekintetben már tartalmaz rendelkezéseket.

A GDPR alkalmazásáig felül kell vizsgálni és a GDPR-nak való megfelelőség céljából szükség szerint át kell dolgozni valamennyi adatkezelési tájékoztatót (termék-

tájékoztatók, marketingtájékoztatók, honlapos tájékoztató, hangrögzítéssel, kamerás megfigyeléssel kapcsolatos tájékoztatók stb.), és ahol szükséges, az ügyfelek nyilatkozati formáit is. A többes adatkezelőkre, adatfeldolgozókra vonatkozó új rendelkezések alapján át kell tekinteni és módosítani kell a szerződéses jogviszonyokat. Gyakorlatilag minden adatfeldolgozóra (így a kiszervezett tevékenységet végzőkre, független közvetítőkre, ügynökökre, egyéb adatfeldolgozókra) vonatkozó szerződés felülvizsgálandó és módosítandó a Rendelet szempontrendszerének figyelembevételével. Fontos szempont a beépített és alapértelmezett adatvédelem elvének megfelelő feltételrendszer, folyamatok kiépítése, szabályozása.

A felülvizsgálat eredményéhez kapcsolód(hat)nak adattisztítások és a szükséges informatikai fejlesztések is (pl. az adattörlések informatikai, technikai megvalósítása, az adatok kezelésével, továbbításával kapcsolatos nyilvántartások az adathordozhatóság új jogával vagy a profilozás új szabályaival kapcsolatban). A törlés megfelelő időn belül történő biztosításának hiányában intézkedni kell a kapcsolódó kockázatok mérsékléséről (zárolás, hozzáférések korlátozása stb.).

Célszerű a felkészüléshez kapcsolni a működési kockázatok feltérképezésének, az ellenőrzési pontok meghatározásának, általában a folyamatba épített vezetői ellenőrzés kialakításának, szabályozásának kérdéskörét is. Kapcsolódó feladatként a folyamatban lévő adatkezelések felülvizsgálatát követően indokolt az adatkezelés elveinek figyelembevételével a jogosultságkezelések felülvizsgálata, annak áttekintése, szükség szerinti újraszabályozása, kik milyen célból, milyen mértékben férhetnek hozzá személyes adatokhoz.

Indokolt az adatvédelmi tisztviselő feladatkör betöltésének vizsgálata, a feladatok ellátásához szükséges feltételek vizsgálata, szükség szerinti intézkedések a Rendelettel való összhang érdekében. A GDPR-ben foglalt „elszámoltathatóság elve" alapján teljes körűen dokumentálni kell tudni az adatkezelések jogszerűségét, és ennek figyelembevételével ki kell alakítani az adatkezelések rendjét és a GDPR szerinti kötelező nyilvántartásokat, az azt alátámasztó dokumentálási rendet.

7.3. Az adatvédelmi szabályzat és kapcsolódó egyéb belső szabályozás

A GDPR 2018. május 25-től történő alkalmazásához el kell készíteni az új adatvédelmi szabályzatot. Az adatvédelmi hatóság korábbi elvárásai szerint az adatvédelmi szabályzattal szembeni követelmény, hogy egyfajta kézikönyvként szolgáljon. Ebből is következik, hogy nem felel meg az adatvédelmi szabályzat tartalmi követelményeinek, ha az csak a normaszöveget tartalmazza. Más kérdés, hogy hitelintézetek esetében a szabályozás többszintű a gyakorlatban; még egy részletesebb követelményeket tartalmazó adatvédelmi szabályzat esetében is az egyes végrehajtási rendelkezések különböző szabályzatokban realizálódnak (pl. a tele-

fonos hangrögzítés a call center eljárásrendjében, vagy a követeléskezelés speciális adatkezelési szabályai annak eljárásrendjében, stb.). De érinthetik az egyes változások a hitelintézet szervezeti működési szabályzatának szabályozási szintjét is az egyes feladatok tekintetében, sőt az egyes munkaköri leírások szintjére történő lebontást is.

Az adatvédelmi szabályozásnak tehát az adatvédelmi szabályzaton túl figyelemmel kell lennie valamennyi személyes adatkezelést is érintő, egyéb belső szabályozásra, és le kell fednie ennek egész hálóját. A szabályozásnak gyakorlatcentrikusnak kell lennie. A folyamatokon túl a szabályozás a GDPR új jogintézményeinek kimunkálását igényli, ez informatikai fejlesztéseket és kapcsolódó, külön szabályozást is szükségessé tesz.

Az adatvédelmi szabályzat módosítása vagy inkább új adatvédelmi szabályzat készítése során az *alábbi tartalmi szempontokra célszerű felhívni a figyelmet:*

– Az alapfogalmakra, alapelvekre vonatkozó rendelkezések kiegészítendők, átdolgozandók a GDPR változásai szerint.
– Szabályozandó az új jogalapok alkalmazása, annak metodikája, különös tekintettel arra, hogy a jelenlegi adatkezelési célok esetében 2018. május 25-től a korábban alkalmazott jogalapoktól eltérően, több jogalapba kell majd sorolni az ezen időponttól megkezdett adatkezeléseket.
– Ki kell munkálni a szabályozásban az olyan új intézményeket és eljárási szabályaikat, mint a hatástanulmány kötelező esetei, a profilozás, adathordozhatóság, álnevesítés új, az adatvédelmi incidens módosuló szabályai.
– Fontos az érintettek jogaira vonatkozó szabályozás, külön is figyelemmel a „felejtés jogára", az adattörlések követelményeire.
– Nem elhanyagolható részterület az adatgyűjtés céljától eltérő adatkezelések szabályozása, a közös adatkezelések vonatkozásainak kimunkálása.

A fentieken túlmenően jelentős feladat az adatfeldolgozókkal szembeni új, személyes adatvédelmi követelményrendszer kialakítása. Továbbra is alapvető fontosságú az érintettek megfelelő tájékoztatási rendjének kimunkálása, szabályozása. Külön figyelmet érdemel az adatvédelmi tisztviselő szerepkörének átgondolása és független kontrollszerepének kimunkálása.

A szabályozásnak kiemelten szolgálnia kell az elszámoltathatóság elvének való megfelelést, hogy a belső adatkezelési, adattovábbítási nyilvántartások alapján végzett, szabályozott tevékenység kontrolljával bármikor alátámasztható legyen az adatkezelés jogszerűsége.

Számos, az adatvédelmi szabályzat mellékletét képező segédanyaggal is segíthető a jogszabályi megfelelőség, a munkavállalók személyes adatvédelmi tevékenysége

(pl. új adatkezelések meghatározására, adatvédelmi tisztviselő általi véleményezésére szolgáló adatlap, adatvédelmi incidens bejelentőlapja stb.).

Az információbiztonság a hitelintézeteknél jellemzően külön szabályozási terület, saját szabályozással, így ennek vizsgálati, szabályozási rendszerét nem vizsgáljuk a jelen keretek között.

7.4. A GDPR-felkészüléssel kapcsolatos egyéb feladatok

A GDPR alkalmazásáig garantálni kell a megfelelőség biztosításához szükséges szervezeti, személyi, informatikai és egyéb technikai feltételeket. Összetettebb tevékenységet végző hitelintézeteknél, bankcsoportoknál az adatvédelmi szabályozás minden személyes adatkezeléssel járó folyamat szabályozásának áttekintését, szükség szerinti módosítását is jelenti. Az új jogalapok alkalmazásának szempontrendszere alapján felül kell vizsgálni és át kell dolgozni az adatkezelési tájékoztatókat is. Ez érinti valamennyi terméktájékoztatót, de a honlapos egyéb tájékoztatókat, a rögzített kamerás felvételről, hangfelvételről stb. adott tájékoztatásokat is.

A többes adatkezelőkre, adatfeldolgozókra vonatkozó, új rendelkezések alapján át kell tekinteni és módosítani kell a szerződéses jogviszonyokat. Gyakorlatilag minden adatfeldolgozóra (így a kiszervezett tevékenységet végzőkre, független közvetítőkre, ügynökökre, egyéb adatfeldolgozókra) vonatkozó szerződés felülvizsgálandó és módosítandó a Rendelet szempontrendszerének figyelembevételével. Fontos szempont a beépített és alapértelmezett adatvédelem elvének megfelelő feltételrendszer, folyamatok kiépítése, szabályozása, ideértve a személyes adatvédelemmel kapcsolatos feladatok, felelősök meghatározását.

A jogszabályi megfelelés, a GDPR alkalmazására vonatkozó felkészülés körében indokolt legalább belső, illetve döntéstől függően külső audit elvégzése.

7.5. Oktatási feladatok

A felkészülésben kiemelt hangsúlyt kell kapnia a munkavállalók, adatfeldolgozók (kiszervezett tevékenységet végzők, adatfeldolgozónak minősülő ügynökök, egyéb adatfeldolgozók) oktatásának.

A mindenkire kiterjedő, az egyes eltérő szakterületi sajátosságokat nem kellően figyelembe vevő, általánosabb jellegű e-learning útján történő oktatás „biztos halál". Olyan adatvédelmi oktatás szükséges, amely (dokumentált módon) biztosítja az egyes szakterületi munkavállalók, ügynökök stb. részére, hogy napi feladataik ellátásával összefüggésben „testre szabottan", adatvédelmi tudatossággal járjanak el. Bár kétségtelenül szükségesek általános, mindenkire érvényes, általános ismeretek is, de pl. a termékszabályozásban azoknak, akik az új adatkezeléseket

meghatározzák, vagy a kifejezetten csak adattovábbításra szakosodott szervezeti egységek munkavállalóinak a napi munka adatvédelmi követelményeinek rutinos biztosításához specifikus ismeretek tudatos alkalmazására van szükségük. Ezekre a specifikumokra az oktatásnak figyelemmel kell lennie.

8. A GDPR HATÁSA A PIACI VERESENYRE

A jövőben várható, hogy a személyes adatvédelmi normák megsértésének okán a hitelintézetekre kiszabott, több száz millió forintos, esetleg milliárdos bírságok a GDPR alkalmazását követő időben nagyobb visszhangot keltenek majd a sajtó és a társadalom körében, mint a jelenlegi, néhány milliós összegben kiszabott hatósági bírság.

Másként ítélhetnek meg majd az ügyfelek egy olyan hitelintézetet, amelyet százmilliós nagyságrendű vagy akár többmilliárdos bírsággal sújtanak, függetlenül attól, hogy a jogsértés jellege hasonló lesz, mint amiért jelenleg néhány millió forintos bírságot szabnak ki. Ha esetleg már a honlapon lévő adatkezelési tájékoztatók, az ott megkezdett adatkezelések, a bárki által hozzáférhető terméknyomtatványok, direktmarketing-eljárások keretében jól érzékelhetően felmerülne, hogy azok valamely tekintetben nem felelnek meg a GDPR rendelkezéseinek, annak számos következménye lehet majd, attól függően is, ki milyen szándékkal vizsgálja. Ez lehet tudatos adatvédelmi hatósági kontroll, de felmerülhet más is. Egy magas összegű hatósági bírsággal szankcionált jogsértés a polgári jogi követelések étvágyát is megnövelheti abban a reményben, hogy a szankcionálások nagyságrendje esetleg a jelenlegihez képest más léptékbe helyezheti a polgári jogi igények összegszerűségének megítélését is.

A jogellenesség bekövetkeztéhez nem kell valami ördögtől való gonoszságra gondolni. A jogszerű adatkezelés feltétele a megfelelő jogalap, az adatkezelés elveinek (célhoz kötöttség, adatminimalizálás elve stb.) való megfelelés és az érintettek megfelelő tartalmú, előzetes tájékoztatása. Amennyiben ezek valamelyike sérül, az adatkezelés már nem jogszerű.

A GDPR új jogalapjai – különösen kapcsolódó hatósági és bírósági gyakorlat kialakulásáig – nem zárják ki a téves jogalap-megállapítás lehetőségét, mivel taxatív szabályozás nincs és nem is lehet e kérdésben. De az egyéb feltételek (pl. tájékoztatási kötelezettség) esetében sem zárható ki teljes mértékben a megfelelési kockázat, különösen az egyes adatvédelmi hatósági ajánlásokban, egyéb hatósági dokumentumokban megfogalmazott elvárásokra is figyelemmel. De vita tárgyát képezheti az alapelveknek való megfelelés is: az, hogy az adatkezelési cél eléréséhez valóban szükséges-e minden adat, és valóban a legenyhébb eszköz kerül-e igénybevételre – vagy jogos érdek alkalmazása esetén vitatható az érdekmérlegelés eredménye.

Az adatvédelmi normák alkalmazása a GDPR-ral nemcsak több lehetőséget, hanem jóval magasabb megfelelési kockázat lehetőségét is jelentheti, legalábbis a következő években, a kapcsolódó hatósági és bírói gyakorlat kialakulásáig. Minden egyes új adatkezelésnél kockázatot jelenthet a jogalapok megfelelő megállapítása, az adatvédelem valamennyi elvének való megfelelés és a megfelelő tájékoztatás megtörténte, később az adatok jogszerű felhasználása és az, hogy csak a szükséges ideig történjen a kezelésük.

A GDPR alapján majdan kiszabható bírság (20 millió euró, illetve az adatkezelő, adatfeldolgozó éves világpiaci forgalmának 4%-a) miatt kiemelt hangsúlyt kap a megfelelési kockázatok minél hatékonyabb kezelésére vonatkozó eljárások kidolgozása és az adatvédelmi tisztviselői megfelelési kontroll minél hatékonyabb működtetése. Az adatvédelmi hatósági bírságon túl egyéb esetleges következményekkel is számolni kell. A nem jogszerűnek tartott adatkezelés esetén a személyes adatok törlésére vonatkozó kötelezésnek is számos következménye lehet akár az adatvagyon működése, akár az informatikai rendszerbeli szerepe (pl. azonosítás) okán. A GDPR kártérítési jogot is biztosít az érintetteknek, de hatályos jogunk több büntetőjogi tényállást is tartalmaz. Sérülhet a jó hírnév is akár hatósági bírsággal, akár az adatvédelmi incidensekkel kapcsolatos ügyfélértesítési esetek kapcsán is.

A személyes adatvédelmi kontroll szerepének és hatékony működtetésének, szervezeti és személyi feltételeinek kialakítása így várhatóan jelentősebb szerepet kap a következő években.

Talán nem túlzás azon állítás, hogy a hitelintézet által végzett, személyes adatkezelések jogszerűsége, annak az ügyfelek általi átláthatósága, vagy éppen azok meg nem felelő volta, szankcionálása akár még az adott hitelintézet versenyhelyzetét is befolyásolhatja a bizalom vagy éppen bizalomvesztés okán. Mindezek a kockázatok is erősíthetik a jelenlegi gyakorlathoz képest egy új típusú adatvédelmi kontrollszervezet kialakításának vizsgálatát, megfontolását.

9. EGY ÚJ TÍPUSÚ ADATVÉDELMI KONTROLLSZERVEZET KIALAKÍTÁSÁNAK KÉRDÉSEI

A hatékony adatvédelmi ellenőrzési szervezet kialakításának számos működési és személyi feltétele van, de nem elhanyagolhatók a szemléletbeli változások sem. A belső ellenőrzési és a compliance kontrollfunkciók történeti fejlődésük alapján már szervezeti helyük, elfogadottságuk tekintetében is előrébb tartanak. Nagyobb hitelintézeteknél már jellemzően igazgatósági vagy legalább főosztályi szervezeti formában működnek. Az adatvédelmi felelős – aki gyakran más feladatot is ellát emellett – a „mesék legkisebb fiúja" a kontrollfunkciók körében.

Amennyiben a kockázatalapú ellenőrzésből indulunk ki, az ellenőrizendő terület nagysága, a lehetséges megfelelési kockázatok, a hatósági bírság mértéke, az egyéb következmények (adattörlés, kártérítés, jó hírnév sérelme stb.) alapján felvetődik a személyes adatvédelmi ellenőrzési funkció szerepének, szervezeti, működési feltételeinek újragondolása.

Az ellenőrizendő területet tekintve, szinte nincs a hitelintézetnek olyan folyamata, szervezeti egysége, amely ne kapcsolódna valamilyen módon a személyes adatkezeléshez. Az adatkezelési szituációknak is számos esete van, attól kezdve, hogy valaki belép egy bankfiókba, ahol kamerás képfelvételt rögzítenek róla, személyes adatokat tartalmazó nyomtatványokat tölt ki, szerződést köt, vagy akár elektronikus úton kezdődik meg termékek, szolgáltatások igénybevételével kapcsolatban a személyes adatainak a kezelése, direktmarketing-nyilatkozatokat tölt ki, személyes adatainak kezelése történik követeléskezeléssel összefüggésben, és tömegszerű adattovábbításra kerül sor rendszeres adatszolgáltatás keretében vagy éppen eseti megkeresések alapján a hatóságok részére, stb.

Vélelmezhetően a jövő egyik feladata többek között az adatvédelmi megfelelőségi kontroll módszereinek olyan elméleti kimunkálása lesz, amely más kontrollfunkciók esetében már nagyobb múltra tekint vissza. A jövő előbb-utóbb valószínűleg egy olyan hitelintézeti adatvédelmi kontrollszervezet lesz, amely a számos személyes adatkezeléssel járó folyamatban tudatos és széles körű, kockázatalapú ellenőrzéssel hatékonyan működik közre az adatvagyon jogszerű és biztonságos kezelésének elősegítésében, a megfelelési és működési kockázatok mérséklésében.

Mindez olyan adatvédelmi tisztviselőt – lényegében adatvédelmi ellenőrzési vezetőt – igényel majd, aki a személyes adatvédelemhez kapcsolódó jogi ismereteken túl képes a hitelintézet folyamatainak olyan áttekintésére, amelynek során tanácsadással is segíteni tudja a jogszerű adatkezelést és a személyes adatvédelemmel járó folyamatok átfogó ellenőrzési rendszerének kialakítását.

10. ÖSSZEGZÉS

A GDPR-nak a jövő év májusától történő alkalmazására való felkészülés eredményessége döntő hatással lesz a hitelintézetek jövőbeni működési kockázataira. Azt, hogy a hitelintézet adatvagyona kiemelt üzleti erőforrás, vélelmezhetően kevesen vitatnák. Az adatvagyonnal foglalkozó irodalomban ugyanakkor utalnak arra (és tapasztalataink is ezt támasztják alá), hogy az adatvagyonnak jellemzően még nincs olyan önálló gazdája a szervezeteknél, aki – valahol az „üzleti terület és az informatikai terület határán" elhelyezkedve – az adatvagyon minél hatékonyabb hasznosulását segítené elő.

Az adatvagyon komplex kezelésének kérdése ugyanakkor felveti az ezzel összefüggő operatív és ellenőrzési feladatkörök, kapcsolódásaik és szükséges elhatárolásuk szervezeti, személyi feltételeinek vizsgálatát, mivel csak több szakterület tevékenységének összehangolásával valósulhat meg az adatvagyon jogszerű, minél alacsonyabb megfelelési kockázattal történő és üzletileg is optimalizált kezelése.

HIVATKOZÁSOK

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

CMS (2016): Az EU új Adatvédelmi Rendelete és az Infotv. – a 25 legfontosabb különbség. 2016. november.

EC (2016): Article 29 Data Protection Working Party. Guidelines on Data Protection Officers ('DPOs'). Adopted on 13 December 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

Európai Parlament és a Tanács (2016): 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). http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32016R0679

Jóri András – Soós Andrea Klára (2016): *Adatvédelmi Jog – Magyar és európai szabályozás.* Budapest: HVG-ORAC Lap és Könyvkiadó Kft.

Kővári Attila (2015): Adatvagyon felelős. BI Projekt (2015. június 18.). http://wwww.biproject.hu/blog/Adatvagyon-felelos.htm.

Liber Ádám (2012): A jogos érdeken alapuló adatkezelésről. *Infokommunikáció és Jog*, 2(49), 79–88. o., https://infojog.hu/liber.adam-a jogos eredeken-alapuló adatkezelesrol-20122-49-79-8.

Liber Ádám (2011): Az Eu Bíróság ASNEF/FECEMD ítélete – döntés a jogos érdeken alapuló adatkezelésről. DataPrivacy.hu, 2011. 11.27., http://www.dataprivacy.hu/?p=864

MNB (2016): A Magyar Nemzeti Bank 5/2016. (VI.06.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról. https://www.mnb.hu/letoltes/5-2016-belso-vedelmi-vonalak-kialak-es-muk.pdf.

MNB (2017): A Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszer védelméről. https://www.mnb.hu/letoltes/7-2017-informatikai-rendsz-ved.pdf

Péterfalvi Attila [szerk.] (2012): *Adatvédelem és információszabadság a mindennapokban*. Budapest: HVG-ORAC Lap és Könyvkiadó Kft.

Szabó Endre Győző (2016): *Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I. Az adathordozhatóság és az adatvédelmi hatásvizsgálat.* Pázmány Law Working Papers 26, http://plwp.eu/evfolyamok/2016/182-2016-26.