AZ ÁLTALÁNOS ADATVÉDELMI RENDELET BIZTOSÍTÓK ÁLTALI ALKALMAZÁSÁNAK EGYES KÉRDÉSEI

Dr. Zavodnyik József (ügyvéd, KLART Legal Ügyvédi Társulás)

ÖSSZEFOGLALÓ

A személyes adatok gyűjtésének és megosztásának mértéke jelentősen növekedett az elmúlt években. Ebben a helyzetben fontos, hogy a természetes személyek saját személyes adataik felett ellenőrzést gyakorolhassanak. Ezt szolgálja az általános adatvédelmi rendelet (GDPR), amely 2018. május 25-től számos adatvédelmi követelményt fogalmaz meg a szervezetekre és így a biztosítókra is. A GDPR új követelményeket határoz meg, így például egy új, az adathordozhatósághoz való jogot hoz létre, amely szorosan kapcsolódik a hozzáférési joghoz, azonban sokféleképpen különbözik ettől, és lehetővé teszi az érintettek számára, hogy az adatkezelő a rendelkezésükre bocsássa az általa kezelt személyes adatokat strukturált, általánosan használt és gépileg olvasható formátumban, és továbbítsa ezeket az adatokat egy másik adatkezelőnek. A GDPR szerint az is kötelező a biztosítók számára, hogy kijelöljék az adatvédelmi tisztviselőt. A GDPR értelmezését segítik az adatvédelmi munkacsoport (Working Party 29) iránymutatásai, amelyek a legjobb gyakorlatokra vonatkozó ajánlásokat is tartalmaznak az egyes tagállamokban rendelkezésre álló tapasztalatok alapján. A tanulmány az iránymutatásokra figyelemmel ismerteti a GDPR egyes rendelkezéseit.

SUMMARY

The extent of the collection and distribution of personal data has increased significantly over the last few years. It is very important in this particular situation that natural persons have a control over their own personal data. The General Data Protection Regulation (GDPR) serves this purpose, which from May 25, 2018, sets out a number of data protection requirements for organizations and thus for insurance companies. GDPR establishes new requirements, such as creating a new data portability right that is closely related to access law but differs from it in a number of ways and allows the affected subjects to have their personal data handled by the data controller at their disposal structured, commonly used and machine readable format, and forward these data to another data controller. According to GDPR, insurance companies are also obligated to designate the data protection officer. The interpretation of GDPR is facilitated by the guidelines of the Working Party 29 on the Protection of Individuals with regard to the Processing of Personal Data, which also contain recommendations on the best practices based on the experience available in each member states. The study presents certain provisions of GDPR, taking into account the guidelines.

Kulcsszavak: adatvédelem, biztosítás, GDPR
Key words: data protection, insurance, GDPR

JEL: G22, K20

DOI: 10.18530/BK.2018.2.14
http://dx.doi.org/1018530/BK.2018.2.14

1. Bevezető

A biztosítási tevékenység lényeges és szükségszerű eleme a biztosító által átvállalt kockázattal, illetőleg a kockázat átvállalása tárgyában létrejövő szerződés megkötésével és teljesítésével kapcsolatos adatok kezelése. Ezen adatok közül sok személyes adatnak minősül, amelynek biztosító általi kezelésére csak a jogszabályok szabta keretek között kerülhet sor.

A személyes adat egy azonosított vagy azonosítható természetes személyre (az érintettre) vonatkozó bármely információ. Az a természetes személy azonosítható, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.[1]

Mivel a biztosítók nagy mennyiségben kezelnek személyes adatokat (közöttük – elsősorban, de nem kizárólagosan az élet-, betegség és balesetbiztosításokkal, illetve felelősségbiztosításokkal összefüggésben – különleges személyes adatoknak minősülő egészségügyi adatokat is), érzékenyen érintik őket az adatkezelésre vonatkozó jogszabályi környezet változásai.

2018. május 25-től kell alkalmazni 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 szóló 2016/679/EU rendelet (általános adatvédelmi rendelet, a továbbiakban: Rendelet) előírásait. Míg az nem igazán vitatható, hogy a Rendeletet alkalmazniuk kell a biztosítóknak,[2] az alkalmazás miként je számos kérdést vet fel. Az adatvédelmi hatóságok által is helyesnek ítélt válaszok megtalálása pedig a korábbinál nagyobb jelentőséggel bír, hiszen a Rendelet megsértésének igen súlyos következményei lehetnek.

Az európai biztosítási, biztostásközvetítői szakmai szervezetek már jó ideje készülnek a Rendelet előírásainak alkalmazására,[3] érzékelve, hogy az új adatvédelmi szabályozás a vállalkozások oldalán megnöveli az adatvédelmi szabályozásból fakadó kockázatot és az e kockázat kezelése által igényelt terheket. A biztosítóknak, biztosításközvetítőknek át kell gondolniuk, milyen kihatással lesznek tevékenységükre az automatizált döntéshozatalra és profilalkotásra vonatkozó korlátozások, de akár az adattakarékosság elvének hangsúlyosabbá válása is, hiszen az elmúlt években az egyik leggyakoribb kifogás a hazai biztosítókkal szemben is a túlzott, indokolatlan adatgyűjtés volt.[4]

A Rendelethez történő igazodás olyan időszakban történik, amikor egyébként is növekszik a biztosítókat a fogyasztók irányában terhelő tájékoztatási kötelezettségek jelentette teher, amelynek kapcsán elegendő csak az Európai Parlamentnek és a Tanácsnak a lakossági befektetési csomagtermékekkel, illetve biztosítási alapú befektetési termékekkel kapcsolatos kiemelt információkat tartalmazó dokumentumokról szóló, 2018. január 1-jétől alkalmazandó 1286/2014/EU rendeletét megemlíteni, amely – ugyan még nem a Rendeletre, hanem az Európai Parlamentnek és a Tanácsnak a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelvére (a továbbiakban: 95/46/EK irányelv) utalva – hangsúlyozza, hogy a személyes adatok 1286/2014/EU rendelet alkalmazásában történő bármely feldolgozásának, így például a személyes adatok illetékes hatóságok közötti cseréjének vagy továbbításának összhangban kell lennie az adatvédelmi szabályozással.[5]

Nem feledhető ugyanakkor az sem, hogy az adatvédelmi szabályozásnak csak az egyik eleme a Rendelet, várható az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről szóló rendelet (elektronikus hírközlési adatvédelmi rendelet) elfogadása is.[6]

A válaszok, különösen a hosszabb távon is irányadónak tekinthető válaszok megfogalmazását megnehezíti, hogy a gyors technológiai fejlődés folyamatosan új adatkezelési összefüggéseket tár fel. Elég itt csak az egész biztosítási tevékenységre hatást gyakorló blockchain (blokklánc) technológiákra utalnunk, amelyek egyes adatvédelmi vetületeivel kapcsolatban 2017-ben a Nemzeti Adatvédelmi és Információszabadság Hatóság is szükségét érezte a megnyilatkozásnak.[7]

A hazai biztosítók Rendelethez történő alkalmazkodását nehezítheti továbbá, hogy késedelem mutatkozik az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) Rendelettel kapcsolatos módosításában.[8]

Az ágazati szabályozás, így például a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény (a továbbiakban: Bit.) is több, az adatkezelést érintő rendelkezést tartalmaz. Az ágazati szabályozásban fellelhető adatkezelési szabályok közül példaként említhetők a Bit.-nek a panaszkezeléssel kapcsolatos rendelkezései, amelyek értelmében telefonon történő panaszkezelés esetén a biztosító és az ügyfél közötti telefonos kommunikációt a biztosító hangfelvétellel rögzíti, és a hangfelvételt öt évig megőrzi.[9] Emellett külön is felhívjuk a figyelmet arra a rendelkezésre, amely szerint a biztosítási szerződési feltételeknek tartalmazniuk kell a személyes adatok kezelésére vonatkozó elvi és gyakorlati tudnivalókat, amennyiben a szerződő vagy a biztosított természetes személy, illetve – részben vagy egészben – természetes személyek csoportja.[10]

A Rendelet és az ágazati jogszabályok viszonyát illetően kiemelendő, hogy az adatkezelés általános szabályait a Rendelet tartalmazza, az ágazati szabályozással kapcsolatban pedig általános elvárás, hogy a bennük foglalt szabályok semmilyen módon se rontsák le az adatvédelem Rendeletben biztosított védelmi szintjét.[11]

Az elmúlt időszakban a szakmai felügyeleti hatóság, a Magyar Nemzeti Bank (a továbbiakban: MNB) is késznek mutatkozott adatkezeléssel kapcsolatos kérdésekben megnyilatkozni.[12]

A fentiekből megállapíthatóan a biztosítási piac szereplői nincsenek könnyű helyzetben az adatkezelési gyakorlatuknak a Rendelettel történő összhangba hozatala során, miközben az adatvédelmi előírások megsértése több vonatkozásában is hátrányos lehet az adatkezelők számára:

- jelentős mértékű bírság megfizetésére kötelezhetők: a Rendelet értelmében a kiszabható bírság mértéke elérheti a 20 millió eurót, illetve az előző üzleti évben elért forgalom 4 százalékát,[13]
- a Rendelet megsértése révén kárt szenvedett személy kártérítést követelhet,[14]
- az adatvédelmi rendelkezések megsértése mellett adott esetben a versenyjogi szabályok megsértésének a megállapítására is sor kerülhet, ennek minden következményével, amivel összefüggésben utalunk a német versenyhatóság által a Facebook ellen a gazdasági erőfölény tilalmának a felhasználók különböző forrásokból származó, különböző szolgáltatások (pl. WhatsApp, Instagram) igénybevétele által rendelkezésre álló adatainak összekapcsolásában, azon alapuló profilalkotásban megmutatkozó adatkezelési gyakorlat révén megvalósított feltételezett megsértése miatt indított eljárásra,[15]
- az adatvédelmi jogsértés mellett a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmának a megsértése is felmerülhet, például ha az érintett adatkezeléshez történő hozzájárulásának hátterében (az adatkezelés céljáról történő tájékoztatás valóságnak meg nem felelő volta stb.) megtévesztés vagy kényszer áll,[16] amely az MNB vagy a Gazdasági Versenyhivatal eljárását vonhatja maga után.

A GDPR lehetőséget jelent a biztosítók eddigi adatkezelési tevékenységének az áttekintésére és szükség esetén átalakítására.

Mindazonáltal megjegyezzük, a Rendelet nemcsak valamiféle fenyegetést jelent a biztosítók számára, hanem egyrészt lehetőséget a biztosítók eddigi adatkezelési tevékenységének az áttekintésére és szükség esetén átalakítására, másrészt üzleti lehetőséget. Az adatkezelő vállalkozások által az adatkezelésre vonatkozó jogszabályi előírások megsértése jelentette kockázat megnövelheti a keresletet az ezen kockázatra kiterjedő, a bírság megfizetését átvállaló biztosítási fedezetek iránt. Az az aggály ugyanakkor még megválaszolandó, hogy nem ütköznek-e jóerkölcsbe az ilyen biztosítási szerződések.[17]

Az alábbiakban néhány olyan kérdésre hívjuk fel a figyelmet, amelyek a Rendelet biztosítók általi alkalmazásával kapcsolatban merülhetnek fel. Kizárólag a biztosítási jogviszonyokkal kapcsolatos, a szerződő feleket, biztosítottakat, kedvezményezetteket érintő adatkezelés egyes kérdéseire térünk ki, a teljesség igénye nélkül, mellőzve például a biztosító mint munkáltató általi adatkezelés problémáinak áttekintését, de a veszélyközösség védelme céljából történő adatátadás Bit.-ben lévő szabályainak vizsgálatát is, [18] illetve a Rendelet érintettek jogaival kapcsolatos szabályainak ismertetését. A Rendelet és az ágazati szabályozás előírásai mellett a 95/46/EK irányelv 29. cikke[19] alapján létrejött munkacsoport (a továbbiakban: 29-es munkacsoport) biztosítással kapcsolatos

megállapításaira és a releváns joggyakorlatra, különösen a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) megállapításaira támaszkodtunk.

2. Az adatkezelési tevékenység főszereplői

Az adatkezelési tevékenység két főszereplője

- az érintett, akinek a személyes adatai kezelésre kerülnek, és
- az adatkezelő, aki kezeli az érintett személyes adatait.

Egyes esetekben nem egyetlen, hanem több adatkezelő azonosítható, közös adatkezelést valósítva meg. Gyakori az is, hogy az adatkezelő adatfeldolgozó(ka)t vesz igénybe, amikor az adatkezelést az adatkezelő nevében az adatfeldolgozó végzi.

2.1. Az érintett

Az érintetti oldalon (azaz azon természetes személy oldalán, akire a biztosító által kezelt személyes adat vonatkozik, és aki ezen adat révén azonosított vagy azonosítható) problémákhoz vezethet a biztosítási jogviszony többszereplős volta. Az adatkezeléssel kapcsolatos kötelezettségek biztosító általi teljesítésekor így mindenképpen átgondolandó a szerződő féllel nem azonos biztosított és kedvezményezett személyes adatai kezelésének a jogalapja, a feléjük fennálló kötelezettségek és az őket megillető jogok köre.

A biztosítónak ennek megfelelően kellő körültekintéssel kell eljárnia például a kedvezményezett adatai kezelése jogalapjának a tisztázásakor. Egyes esetekben ehhez jogszabályi segítséget kapnak a biztosítók. A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: Pmt.) értelmében a szolgáltató az üzleti kapcsolat létesítése vagy az ügyleti megbízás végrehajtása előtt köteles lefolytatni az ügyfél személyazonosságának igazoló ellenőrzését.[20] Külön szabályok vonatkoznak ugyanakkor az életbiztosítási ágba tartozó biztosításokra: a biztosító ezen biztosítások esetén az üzleti kapcsolat létesítését megelőzően az ügyfél és a tényleges tulajdonos azonosításán és személyazonosságának igazoló ellenőrzésén túlmenően köteles a) a szerződés megkötésekor ismert kedvezményezett, illetve a biztosítási szerződés alapján a biztosító szolgáltatására jogosult nevét megállapítani, továbbá b) a szerződés megkötésekor nem ismert kedvezményezettre, illetve a biztosítási szerződés alapján a biztosító szolgáltatására jogosultra vonatkozó, a későbbi azonosításhoz szükséges valamennyi információt rögzíteni. Ha az életbiztosítási ágba tartozó biztosítás kedvezményezettje, illetve a biztosítási szerződés alapján a biztosító szolgáltatására jogosultak személye a szerződés megkötésekor nem ismert, a kedvezményezett, illetve a biztosítási szerződés alapján a biztosító szolgáltatására jogosult személyazonosságának igazoló ellenőrzését legkésőbb a kifizetéssel egyidejűleg vagy a szerződésből (kötvényből) eredő jogoknak a jogosult általi érvényesítéséig lefolytatja.[21] Megjegyzendő, hogy ha a szerződés megkötésénél nincs jelen a kedvezményezett, a személyes adatait nem tőle szerezték meg, akkor is teljesíteni kell részére az adatkezelési tájékoztatást, a rendelkezésére bocsátva a Rendeletben meghatározott információkat. A tájékoztatást főszabály szerint a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül kell teljesíteni.[22]

A biztosítási tevékenység kapcsán gyakorta kerül sor elhunyt személyek adatainak a kezelésére. A Rendeletet nem kell alkalmazni az elhunyt személyekkel kapcsolatos személyes adatokra, ezek kezelését a jogszabály tagállami hatáskörbe utalja.[23] A magyar szabályozás kimondja, hogy a Bit. alkalmazásában az elhunyt személyhez kapcsolódó adatok kezelésére a személyes adatok kezelésére vonatkozó jogszabályi rendelkezések az irányadók, és az elhunyt személlyel kapcsolatba hozható adatok tekintetében az érintett jogait az elhunyt örököse, illetve a biztosítási szerződésben nevesített jogosult is gyakorolhatja.[24]

2.2. Adatkezelő, adatfeldolgozó, közös adatkezelés

A biztosítási jogviszonnyal összefüggésben több vállalkozás, személy kerülhet kapcsolatba az érintett személyes adataival, így a biztosítón kívül például a biztosításközvetítő és a kárrendezésben közreműködő vállalkozás. Tisztázandó ezen személyek adatkezelési minősége, mindenekelőtt az, hogy adatkezelőnek (közös adatkezelőnek) vagy adatfeldolgozónak minősülnek-e. E minősítés következményeit minden vonatkozásban le kell vonni, mind a biztosító és más vállalkozás közötti szerződés tartalmát, mind az adatvédelmi tisztviselő kijelölésének a kötelezettségét illetően.[25]

Az adatkezelő az a vállalkozás, amely a személyes adatok kezelésének céljait és eszközeit meghatározza, az adatfeldolgozó pedig az a természetes vagy jogi személy, amely az adatkezelő nevében személyes adatokat kezel.[26] Az adatkezelői vagy adatfeldolgozói minőségének megítélése legfőképpen attól függ, hogy az adatkezelést érintő érdemi döntéseket melyik vállalkozás hozza meg. Az ugyanakkor nem szükségszerű, hogy az adatkezeléssel kapcsolatos valamennyi érdemi döntést egy vállalkozás, egy adatkezelő hozza meg, a Rendelet lehetővé teszi azt, hogy egy adatkezelésben több adatkezelő vegyen részt (közös adatkezelés). Ebben az esetben az adatkezelés céljait és eszközeit két (vagy több) adatkezelő közösen határozza meg.[27]

Ha a biztosító adatfeldolgozót vesz igénybe, akkor egyebek között szem előtt tartandó, hogy

- a biztosító mint adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, amelyek megfelelő garanciákat nyújtanak az adatkezelés Rendelet szerinti követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására,[28]
- a Rendelet meghatározza az adatfeldolgozói szerződés egyes tartalmi elemeit,[29] ugyanakkor
- az adatfeldolgozói szerződésre adott esetben az ágazati szabályozásnak a kiszervezési szerződésekre irányadó előírásait is megfelelően alkalmazni kell, különös tekintettel arra, hogy a Bit. előírja, ha a kiszervezett tevékenység keretében a biztosító ügyfeleinek személyes adatát továbbítja a kiszervezett tevékenységet végzőhöz, úgy a szerződésben rögzíteni kell az adatfeldolgozás rendjét és az adatvédelem szabályait,[30]

- az adatfeldolgozói szerződésben rögzíteni kell a biztosító mint adatkezelő egyértelmű utasításait az adatfeldolgozó adatkezelési tevékenységét illetően (a Rendelet értelmében az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi[31]), mivel ennek hiányában felmerülhet a közös adatkezelés megvalósulása, és ebben az esetben a másik vállalkozásnak is teljeskörűen eleget kell tennie az adatkezelőre irányadó szabályoknak.

3. Az adatkezelés jogszerűsége feltételeinek vizsgálata

Ahhoz, hogy a személyes adatok adatkezelése jogszerűnek minősüljön, minimálisan vizsgálandó

- a tervezett adatkezelés célja,
- az adatkezelés céljának megvalósításához szükséges adatok köre és az adatok adott adatkezelő általi kezelhetősége,
- az adatkezelés jogalapja,
- az adatkezelés elveinek érvényesülése,
- az adatkezelés időtartama.

3.1. Az adatkezelés célja

A Rendelet a személyes adatok kezelésére vonatozó elvek között rögzíti a célhoz kötöttség elvét, amelynek értelmében a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és az adatokat nem lehet ezekkel a célokkal össze nem egyeztethető módon kezelni.[32]

A személyes adatok kezelése céljának a Rendelet szerint konkrétnak, explicit módon megfogalmazottnak, jogszerűnek és már a személyes adatok gyűjtésének időpontjában meghatározottnak kell lennie.[33] Ennek megfelelően a meghatározott cél nélküli, előre nem meghatározott jövőbeni felhasználásra (készletre) való adatgyűjtés- és tárolás jogellenes,[34] de az is jogellenességet eredményez, ha az adatkezelési cél túlságosan tág módon kerül meghatározásra, azaz ha nincs összefüggésben az adatkezelés a megjelölt céllal. [35]

Amint arra a 29-es munkacsoport rámutat, a célhoz kötöttség elve annak a megértésére vonatkozik, hogy miért kerül sor bizonyos személyes adatok feldolgozására. Ez annyit jelent, hogy a lehető legkonkrétabban meg kell határozni azokat a célokat, amelyek érdekében a tervezett intézkedés a személyes adatok összegyűjtését és feldolgozását elrendelheti. Ezáltal a minimális adatgyűjtés elvének is jobban eleget lehet tenni. A minimális adatgyűjtés elve azt a célt szolgálja, hogy a kitűzött cél érdekében a lehető legkevesebb adat feldolgozására kerüljön sor. [36]

Csak olyan személyes adat kezelhető tehát, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.[37] Ha például a biztosítótársaság egészségügyi dokumentációt kíván megismerni, illetőleg különböző orvosi vagy kórházi igazolások csatolását írja elő ahhoz, hogy elbírálhassa kárigényüket, akkor ezekben az esetekben is a célhoz kötött adatkezelés elvéből kell kiindulni, és azt kell megvizsgálni, hogy a kezelendő adatkör a biztosítási szerződésből származó követelések megítélésével közvetlenül összefüggésbe hozható-e. Ehhez figyelembe kell venni a konkrét biztosítási szerződést, a biztosító által kialakított általános szerződési feltételeket, amelyek olykor speciális mentesüléseket vagy a biztosító által kizárt speciális kockázatokat is tartalmazhatnak, és ennek fényében dől el, hogy a biztosító adatigénye indokolt-e. Ha olyan egészségügyi adat került a biztosító birtokába, amely az igény elbírálásával közvetlenül nem függ össze, ahhoz nem elengedhetetlenül szükséges, a biztosító köteles azt törölni.[38]

A minimális adatgyűjtés elve azt a célt szolgálja, hogy a kitűzött cél érdekében a lehető legkevesebb adat feldolgozására kerüljön sor.

Adatvédelmi szempontból aggályos, túlzott adatgyűjtésnek minősül, ha például útlemondási biztosítás kapcsán a biztosító részletekbe menően kívánja megismerni a biztosított egészségügyi dokumentációját a háziorvosi, kórházi igazolások csatolásán felül. Ezekben az esetekben is a célhoz kötött adatkezelés elve a jogszerűség megítélésének mércéje, vagyis a kezelendő adatkörnek a cél eléréséhez kell igazodnia. [39]

A biztosítási titoknak is minősülő személyes adatok biztosítók általi adatkezelése szempontjából megkerülhetetlen a jelenleg hatályos szabályozás: a Bit. értelmében a biztosító kezelheti a természetes személynek minősülő ügyfeleinek azon biztosítási titoknak minősülő adatait, így személyes adatait is, amelyek a biztosítási szerződéssel, annak létrejöttével, nyilvántartásával, a szolgáltatással összefüggnek. Az adatkezelés célja

- ebben a körben csak a biztosítási szerződés megkötéséhez, módosításához, állományban tartásához, a biztosítási szerződésből származó követelések megítéléséhez szükséges, vagy a Bit. által meghatározott egyéb cél lehet,
- ugyanakor az adatok más célból is kezelhetők, de csak az ügyfél előzetes hozzájárulásával (lásd az adatkezelés jogalapjának kérdését később). [40]

Marketing-adatbázis építése érdekében is kezelhetők tehát személyes adatok, ugyanakkor e körben is figyelembe veendők a célhoz kötöttség elvéből fakadó követelmények, amelyek értelmében például a „marketing” mint cél túl általános, nem elég pontos.[41]

Az adatkezelés céljának meghatározása az érintettet megillető tájékoztatási jog kapcsán is kiemelkedő jelentőséggel bír. A Rendelet vonatkozásában is irányadó a Kúriának még az Infotv. alkalmazásával tett megállapítása, amely szerint az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell adatai kezelésének céljáról, jogalapjáról, az arra jogosult személyéről, az adatkezelés időtartamáról. Ha tehát az adatgyűjtésre értékesítési célból is sor került, akkor az érintett tájékoztatásának erre is ki kellett volna terjednie, ami nem teljesül azzal, ha az adatkezelő az adatkezelés céljaként a reklám- és marketinganyagok küldését jelölte meg. Ezzel a pontos és tényszerű információ egyértelműen hiányzik, amely a kellő tájékoztatáshoz elengedhetetlen. A nem kellő tájékoztatás a hozzájárulás hiányához vezet. Az adatkezelés célja tehát nem elhanyagolható információ.[42]

3.2. Kezelhető és nem kezelhető személyes adatok, a kezelhető személyes adatok különleges kategóriája

Az adatkezelés elveinek megfelelő adatkezelési tevékenységet folytató, kizárólag az adatkezelés céljai szempontjából megfelelő és releváns személyes adatokat kezelő biztosító számára is megvizsgálandó, hogy vannak-e korlátai a cél eléréséhez egyébként szükséges adat kezelésének. Tisztázandó például, hogy az érintett személy nemi hovatartozására vonatkozó, illetve azzal összefüggő adat milyen célból kezelhető a biztosító által.

Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény megfogalmazza a nemi hovatartozáson alapuló egyenlő bánásmód követelményét, kimondva, hogy a biztosítási szolgáltatások és a biztosítási elven alapuló szolgáltatások esetében – ide nem értve a csoportos élet-, baleset- és betegségbiztosításokat – a nemi hovatartozáson alapuló megkülönböztetés az e szolgáltatásokat szabályozó törvény eltérő rendelkezése hiányában sérti az egyenlő bánásmód követelményét, ha a szolgáltatást nyújtó eljárása az egyének által egyedileg fizetendő díj nagyságában vagy az őket megillető szolgáltatásban a nemi hovatartozáson alapuló közvetlen vagy közvetett különbségtételt eredményez.[43] A Bit. értelmében ugyanakkor a biztosító magatartása nem sérti a nemi hovatartozáson alapuló egyenlő bánásmód követelményét, ha a biztosító kizárólag a) a tartalékképzés, b) a biztosító pénzügyi eszközei összetételének összesített árképzési szempontú nyomon követésével összefüggő belső árazás, c) a viszontbiztosítási szerződések árazása, d) a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló törvényben meghatározott gazdasági reklám, továbbá hirdetési tevékenység, e) az élet-, baleset- és betegségbiztosítási szerződésekkel összefüggésben kockázatelbírálási tevékenység végzése céljából a nemi hovatartozásra vonatkozó, illetve azzal összefüggő adatot, információt kezel, tárol és felhasznál.[44] Nem esik a Bit. által érintett körbe, ha a biztosító a Bit. által meghatározottaktól eltérő célból kezeli a nemi hovatartozásra vonatkozó adatokat.

Míg tehát a nemi hovatartozásra vonatkozó adatokat egyes esetekben kezelheti a biztosító, vannak olyan személyes adatok, amelyek biztosító általi kezelésére nem kerülhet sor (vagy csak igen szűk, különleges körben). Főszabály szerint ilyen adatoknak minősülnek a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok. Ezeket a biztosító csak akkor kezelheti (azzal, hogy a büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet), ha azt az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi. A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet.[45]

Léteznek továbbá olyan, a biztosítók által gyakorta kezelt személyes adatok, amelyek kezelésére különleges szabályok vonatkoznak. A személyes adatok különleges kategóriájába sorolandó – hasonlóan a korábbi szabályozáshoz[46] – egyebek között az egészségügyi adat (egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, idetértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról[47]), amelynek kezelése főszabály szerint ugyancsak tilos, ugyanakkor a Rendelet több kivételt enged e tilalom alól, így ha az érintett kifejezetten hozzájárul ezen adat egy vagy több konkrét célból történő kezeléséhez. Mindazonáltal a tagállam előírhatja, hogy a tilalom nem oldható fel az érintett hozzájárulásával, illetve további feltételeket – köztük korlátozásokat – írhat elő az egészségügyi adatok kezelésére vonatkozóan,[48] ezért mindenképpen figyelemmel kell kísérni a magyar jogi szabályozás változásait.

Az egészségügyi adat kezelése főszabály szerint ugyancsak tilos, ugyanakkor a Rendelet több kivételt enged e tilalom alól.

A Bit. jelenleg azt írja elő, hogy az ügyfél egészségi állapotával összefüggő egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvényben (a továbbiakban: Eüak.) meghatározott egészségügyi adatokat a biztosító a Bit.-ben meghatározott célokból, az Eüak. rendelkezései szerint, kizárólag az érintett írásbeli hozzájárulásával kezelheti.[49]

Az egészségügyi adatok kezelésére akkor is lehetőség van, ha az a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra és különösen a szakmai titoktartásra vonatkozóan.[50] Ez a kivétel ugyanakkor nem adhat szabad kezet a biztosítási szektor számára, hiszen az egészségügyi adatok ilyen közérdekű kezelése nem eredményezheti a személyes adatok más célokból harmadik személyek, így biztosítók általi kezelését.[51] Figyelemmel a Bit.-ben foglaltakra az is leszögezhető, hogy minden olyan esetben, amikor az adatkérés nem korlátozódik a biztosítási szerződésből származó követelések megítélésével közvetlenül összefüggő adatkörre, akkor túl széles körű az adatkezelés. Esetenként vizsgálandó, hogy az igényelt egészségügyi adatokra a törvényi mentesülések, valamint a biztosítási szerződésben meghatározott kizárások megítéléséhez esetleg szükség lehet egészségügyi adatok megadására.[52]

Felhívjuk továbbá a figyelmet arra, hogy

- a különleges adatokat (azaz például egészségügyi adatokat) kezelő adatkezelő sosem hivatkozhat kizárólag valamelyik, a Rendelet 6. cikke szerinti jogalapra az adatkezelési tevékenység jogszerűvé tétele érdekében. A Rendelet 6. cikke ebben az esetben nem az uralkodó rendelkezés, hanem azt mindig együttesen kell alkalmazni a 9. cikkel annak biztosítása érdekében, hogy a Rendelet minden vonatkozó előírása, intézkedése teljesüljön,[53]
- az Európa Tanács Miniszteri Bizottsága 2016-ban külön ajánlást adott ki az egészségügyi adatok biztosítási célból történő kezeléséről (beleértve a genetikai vizsgálatokat is).[54]

3.3. Az adatkezelés jogalapja

A Rendelet értelmében a személyes adatok kezelésének jogalapja a következő lehet:

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 vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek 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.

Az alábbiakban a biztosító általi adatkezelés szempontjából elsősorban releváns négy jogalap egyes kérdéseire térünk ki.

3.3.1. Hozzájárulás

Az érintett hozzájárulása az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.[55]

A hozzájárulás érintett általi megadásához a biztosítónak mint adatkezelőnek olyan előre megfogalmazott hozzájárulási nyilatkozatról kell gondoskodnia, amelynek az érintett számára érthető nyelvezete világos és egyszerű, továbbá nem tartalmaz tisztességtelen feltételeket. Ahhoz, hogy a hozzájárulás tájékoztatáson alapulónak minősüljön, az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával. A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.[56] Nem mellőzhető az sem, hogy a hozzájárulást adatkezelési célonként szükséges megadni, egy hozzájárulás nem vonatkozhat több adatkezelési célra. Az ezzel ellentétes megoldás jogellenes adatkezelést eredményez.[57]

Általános éllel tehát azt lehet mondani, hogy az adatkezelési célonként megadott hozzájárulás is csak akkor lehet megfelelő jogszerű alap, ha az érintettnek megfelelő tájékoztatás után lehetővé tették a választást, valódi választási lehetőséget biztosítva a hozzájárulás megadása vagy visszautasítása tekintetében, bárminemű hátrány nélkül.[58]

Bizonytalan jogi helyzethez vezethet, ha a biztosító csak akkor köti meg a biztosítást, ha az érintett hozzájárul például az egészségügyi adatainak a kezeléséhez, és elzárkózik a szerződéskötés elől a hozzájárulás hiányában, mivel a joggyakorlat szerint, ha az adatkezeléshez történő hozzájárulás megtagadása miatt az érintettel a szerződéskötést megtagadják, a hozzájárulás önkéntességének az elve is sérülhet.[59] Ebben a megközelítésben az érintett adatkezeléshez adott hozzájárulása tehát nem szükségszerűen minősül a jogszabályi követelményeknek eleget tevő hozzájárulásnak, a hozzájárulás hiányában azonban nem kerülhet sor az egészségügyi adatok kezelésére, mely adatok ismeretének hiányában pedig a biztosító nem végezheti el a kockázatfelmérést, nem tudja megkötni a biztosítási szerződést. A kérdés Rendelet alapján történő megválaszolása során figyelemmel kell majd lenni a következőkre is: a Rendelet szerint annak megállapításakor, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni egyebek mellett azt a tényt, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételeül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez,[60] nem mellőzve ugyanakkor azt sem, hogy a Rendelet értelmében a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.[61] Mindehhez a Bit. még hozzáteszi, hogy hozzájárulás megtagadása miatt az ügyfelet nem érheti hátrány, és annak megadása esetén részére nem nyújtható előny.[62] A szabályozási összhang hiánya által felvetett kérdések megválaszolása a joggyakorlatra vár, addig a biztosítóknak mérlegelniük kell, hogy jogértelmezésük milyen kockázattal jár az esetleges adatvédelmi felügyeleti eljárásokra tekintettel.

A hozzájárulás mint jogalap a biztosítás esetén kiemelt jelentőséggel bír a Bit. révén, hiszen a Bit. értelmében ha az adatkezelés nem szükséges a biztosítási szerződés megkötéséhez, módosításához, állományban tartásához vagy a biztosítási szerződésből származó követelések megítéléséhez (vagy a Bit.-ben meghatározott más cél eléréséhez), akkor a biztosító csak az ügyfél előzetes hozzájárulásával végezhet adatkezelést[63] – azaz a Bit. szerint nem lehet az adatkezelés jogalapja az érdekmérlegelés, míg a Rendelet erre lehetőséget ad. Ez is azt támasztja alá, hogy mindenképpen indokolt lenne annak alaposabb vizsgálata, milyen jogszabály-módosítások szükségesek az ágazati szabályozás és a Rendelet közötti teljes összhang megteremtéséhez.

Az elmúlt időszak hazai joggyakorlatából a hozzájárulás körében azon esetre utalunk, amikor az adatvédelmi biztoshoz forduló érintett azt kifogásolta, hogy a számlavezető bankja felhatalmazást kért arra, hogy banktitoknak minősülő adatokat továbbítson egy biztosító részére. A bank által kidolgozott „Biztosítotti nyilatkozat”-ot a bankkártyához kapcsolódó utas- és balesetbiztosítási szolgáltatás esetében alkalmazták. A nyilatkozat szövege szerint az ügyfél hozzájárult ahhoz, hogy a bank a biztosító részére átadja a biztosítási szerződés hatályának személyére történő kiterjesztése, illetve a biztosítási szolgáltatás igénybevétele céljából a nyilatkozatban megadott banktitoknak és személyes

adatnak minősülő adatokat. A nyilatkozat alapján a pénzintézet a bankkártya birtokosának nevét, anyja nevét, születési idejét, lakcímét, személyazonosító igazolványa számát, bankkártyája számát és típusát továbbíthatta. A biztos úgy foglalt állást, hogy a fenti adatkör biztosító általi kezelése valóban szükséges és elengedhetetlen a bankkártyához kapcsolódóan igénybe vehető kiegészítő biztosítási szolgáltatás teljesítéséhez.[64]

3.3.2. Szerződés teljesítése

A személyes adatok kezelésére akkor is sor kerülhet, ha az olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

Közvetlen és objektív kapcsolatnak kell lennie az adatkezelés és a szerződés teljesítése között.

E rendelkezést szigorúan kell értelmezni, így a rendelkezés nem vonatkozik olyan helyzetekre, ahol az adatkezelés valójában nem szerződés teljesítéséhez szükséges, hanem azt az adatkezelő az érintettre erőlteti.[66] Emellett közvetlen és objektív kapcsolatnak kell lennie az adatkezelés és a szerződés teljesítése között, amely kapcsolat nem áll fenn, ha például a biztosító a személyes adatokat marketingcélokra kívánja felhasználni, hiszen ez az adatkezelés az ügyféllel kötött biztosítási szerződés teljesítéséhez nem szükséges.[67]

Ez a jogalap egyrészről csak azon adatkezelésre vonatkozik, amely a szerződés teljesítéséhez szükséges, és nem vonatkozik például a nemteljesítés miatti intézkedésekre, illetve a szerződés végrehajtásakor felmerülő egyéb eseményekre,[68] másrészt a szerződés megkötése előtt elvégzett adatkezelésre, a szerződéskötés előtti kapcsolatokra is kiterjed, feltéve, hogy arra nem az adatkezelő vagy egy harmadik személy, hanem az érintett kezdeményezésére kerül sor. Így például, ha valaki casco gépjármű-biztosítási árajánlatot kér a gépjárművére egy biztosítótól, a biztosító feldolgozhatja az ehhez szükséges adatokat (pl. a gépjármű típusát, korát és más, releváns adatot). Ezzel szemben nem tekinthető az érintett kérésére végzett szükséges intézkedésnek a részletes kockázatfelmérés, például az érintett orvosi vizsgálatairól szóló adatok kezelése azt megelőzően, hogy a biztosító egészség- vagy életbiztosítási szerződést kötne, így ebben az esetben más jogalapja lehet az adatkezelésnek.[69]

A közvetlen üzletszerzéshez szükséges adatkezelés sem történhet ezen a jogalapon. Egyes esetekben az adatkezelésre érdekmérlegelés alapján, más esetekben (pl. a kiterjedt profilalkotás, adatmegosztás, online közvetlen üzletszerzés vagy viselkedésalapú hirdetés esetén) az érintett hozzájárulásával kerülhet sor.[70]

3.3.3. Jogi kötelezettség teljesítése

Jogszerű az adatkezelés abban az esetben is, ha az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. [71]

E jogalap akkor alkalmazható, ha a jogi kötelezettséget jogszabály írja elő és nem például szerződés.[72] Mindazonáltal az ilyen jogalapnak vagy jogalkotási intézkedésnek világosnak és pontosnak, alkalmazásának pedig előreláthatónak kell lennie a hatálya alá tartozó személyek számára.[73]

Jogi kötelezettség akkor áll fenn, ha az adatkezelő nem döntheti el, teljesíti-e a kötelezettséget vagy sem. A jogi kötelezettségnek kellően egyértelműnek kell lennie az általa igényelt személyes adatok feldolgozását illetően, így ez a jogalap csak olyan jogi kötelezettségek esetén alkalmazható, amelyek kifejezetten az adatfeldolgozás jellegére és tárgyára vonatkoznak. Az adatkezelő nem rendelkezhet indokolatlan mértékű mérlegelési jogkörrel a jogi kötelezettségnek való megfelelés módját illetően. A 29-es munkacsoport felhívja a figyelmet arra, hogy a jogalkotás egyes esetekben csak általános célkitűzést állapít meg, a specifikusabb kötelezettségeket pedig más szinteken határozzák meg, például másodlagos jogalkotás során vagy egy hatóság által konkrét esetekben hozott, jogilag kötelező érvényű határozat útján. Ebben az esetben is beszélhetünk jogi kötelezettségről, feltéve, hogy az adatfeldolgozás jellege és tárgya jól meg van határozva, és a megfelelő jogalap vonatkozik rá. Más a helyzet azonban, ha a szabályozó hatóság csak általános szakpolitikai iránymutatást és feltételeket biztosít, amelyek alapján úgy dönthet, hogy használja végrehajtási hatáskörét (pl. szabályozó iránymutatás a pénzügyi intézmények részére az átvilágítási szabványokra vonatkozóan). Az adatkezelés ilyen esetben más jogalapon, érdekmérlegelésen alapulhat.[74]

Nem tekinthető tehát jogi kötelezettség előírásának a Bit. azon rendelkezése, amely szerint a biztosító jogosult kezelni ügyfeleinek azon biztosítási titoknak minősülő adatait, amelyek a biztosítási szerződéssel, annak létrejöttével, nyilvántartásával, a szolgáltatással összefüggnek, itt más jogalapot kell keresni.[75] Ezzel szemben jogi kötelezettséget ír elő például a Pmt. az ügyfelek azonosítása kapcsán, meghatározva, hogy az ügyfél azonosítása során milyen adatokat kell rögzíteni.[76] A Pmt. arra is kötelezi a biztosítót, hogy a személyazonosság igazoló ellenőrzése érdekében a Pmt.-ben meghatározott okiratok bemutatását követelje meg, és a személyazonosság igazoló ellenőrzése érdekében a bemutatott okiratról – a pénzmosás és a terrorizmus finanszírozásának megelőzése és megakadályozása, a Pmt.-ben meghatározott kötelezettségek megfelelő teljesítése, az ügyfél-átvilágítási kötelezettség teljes körű végrehajtása, valamint a felügyeleti tevékenység hatékony ellátása céljából – másolatot készítsen.[77] A Pmt. ez utóbbi rendelkezése révén e körben megoldást nyert a korábban az adatvédelmi biztos, illetve hatóság által többször kifogásolt probléma, a biztosítók személyazonosító okmányok másolására vonatkozó gyakorlata azzal, hogy a NAIH kifogásolta a Pmt. ezen rendelkezését, javasolva a szabályozás módosítását.[78] Számos korábbi adatvédelmi biztosi, majd hatósági állásfoglalás leszögezte, hogy a fényképes igazolvány személyazonosítás céljából való bemutatása nem sérti a jogszabályi rendelkezéseket, a másolatok kezelése azonban nem felel meg a célhoz kötöttség követelményének, és a személyazonosító és egyéb okmányok másolására irányuló biztosítói gyakorlat törvényes jogalap és cél hiányában, az okmányvédelmi szempontokat is figyelembe véve nem elfogadható.[79] A Pmt. rendezi ezt a kérdést,

de hangsúlyozzuk, hogy kizárólag csak az általa meghatározott körben: az okirat lemásolását csak a személyazonosság igazoló ellenőrzése érdekében, a pénzmosás és a terrorizmus finanszírozásának megelőzése és megakadályozása, a Pmt.-ben meghatározott kötelezettségek megfelelő teljesítése, az ügyfél-átvilágítási kötelezettség teljes körű végrehajtása, valamint a felügyeleti tevékenység hatékony ellátása céljából teszi lehetővé.

3.3.4. Érdekmérlegelés

A Rendelet szerint jogszerű az adatkezelés akkor is, ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek 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.[80]

A 29. cikk szerinti munkacsoport ugyan még a 95/46/EK irányelv kapcsán, de már kifejtette álláspontját az adatkezelő jogszerű érdekeinek fogalmáról, az ezen jogalappal összefüggő egyes kérdésekről, egyebek között az alábbiakra mutatva rá:

- a mérlegelési teszt (azaz az adatkezelő jogszerű érdekeinek összevetése az érintett érdekeivel vagy alapvető jogaival és szabadságaival) eredménye határozza meg, hogy ez a rendelkezés alkalmazható-e az adatkezelés jogalapjaként,
- a jogszabálynak megfelelő értékelés nem egyszerű mérlegelési teszt, amely során kizárólag két egyszerűen számszerűsíthető és összehasonlítható „fontosságot" kell egymással összehasonlítani. A teszt során számos tényezővel kell teljeskörűen számolni annak érdekében, hogy biztosítsák az érintettek érdekeinek vagy alapvető jogainak megfelelő figyelembevételét,
- ez a jogalap egyrészt nem tekinthető az olyan ritka vagy váratlan helyzetekben kínálkozó utolsó lehetőségnek, amikor a jogszerű adatfeldolgozás egyéb jogalapjai már nem alkalmazhatók, másrészt azonban automatikusan sem lehet választani, és használatát nem lehet indokolatlanul kiterjeszteni arra a vélelemre alapozva, hogy a többi jogalaphoz képest kevésbé szigorú,
- ahhoz, hogy a „jogszerű érdek" alkalmazható legyen, törvényesnek kell lennie (vagyis meg kell felelnie a vonatkozó uniós és nemzeti jognak), kellően egyértelműnek (kellően pontosnak) kell lennie annak érdekében, hogy a mérlegelési tesztet el lehessen végezni az érintettek érdekeire és alapvető jogaira vonatkozóan, továbbá valós és fennálló érdeknek kell lennie (azaz nem lehet elméleti érdek).[81]

Ez a jogalap alkalmazható lehet például a hagyományos közvetlen üzletszerzés esetén, azzal, hogy ez nem jelenti azt, hogy az adatkezelők erre a jogalapra hivatkozva aránytalan mértékben ellenőrizhetik az ügyfeleik online és offline tevékenységeit, különböző forrásokból nagy mennyiségű, eredetileg más kontextusban és más célra gyűjtött adatokat gyűjthetnek róluk, illetve az ügyfelek személyiségére és igényeire vonatkozó összetett profilokat hozhatnak létre – és kereskedhetnek azokkal például adatbrókerek közvetítésével – az ügyfelek tudta, a tiltakozást lehetővé tévő működőképes mechanizmus vagy akár előzetes tájékoztatáson alapuló hozzájárulásuk nélkül. A 29-es munkacsoport szerint az ilyen profilalkotási tevékenység erősen beleavatkozhat az érintett magánéletébe, és ebben az esetben az érintett érdekei és jogai magasabb rendűnek bizonyulnak az adatkezelő érdekénél.[82]

A szolgáltatónak lehet jogszerű üzleti érdeke annak biztosítása, hogy az ügyfelei ne éljenek vissza a szolgáltatással.

A 29-es munkacsoport véleménye több példát is ismertet az érdekmérlegelésen alapuló adatkezeléssel összefüggésben, amelyek közül kettőre hívjuk fel a figyelmet:

- a pizzérialánc eladja Claudia pizzafogyasztási szokásainak, ideértve az ételrendelések időpontjának és jellegének adatait, egy biztosítónak, amely az egészségbiztosítási díjai átszámításához felhasználja az adatokat. Az egészségbiztosítónak lehet jogszerű érdeke (a vonatkozó szabályozások által megengedett mértékig) az ügyfelei egészségi kockázatainak felmérése, és a biztosító az eltérő kockázatokra eltérő díjat állapíthat meg. Az adatgyűjtés ilyen módja azonban, illetve már önmagában az adatgyűjtés mértéke is eltúlzott. A Claudia helyzetében lévő értelmes személy valószínűleg nem számít rá, hogy a pizzafogyasztási szokásairól szóló információkat fel fogják használni az egészségbiztosítási díjának kiszámításához. A profilalkotás túlzott jellegén és a valószínűsíthetően pontatlan következtetéseken (a pizzát másnak is rendelhették) túlmenően az érzékeny adatok kinyerése (egészségi adatok) a látszólag ártalmatlan adatokból (ételrendelés) hozzájárul ahhoz, hogy a mérleg az érintett érdekei és jogai felé billen el. Végül az adatfeldolgozás jelentős pénzügyi hatást gyakorol az érintettre. Mindent összevetve ebben az esetben az érintett érdekei és jogai elsőbbséget élveznek az egészségbiztosító jogszerű érdekeinél, így ez a jogalap nem alkalmazható, [83]
- lehetséges, hogy egy vállalat privát üzleti érdeke bizonyos fokig egybeesik a közérdekkel, ami történhet például a pénzügyi csalások vagy a szolgáltatások tisztességtelen igénybevétele elleni küzdelem esetében. A szolgáltatónak lehet jogszerű üzleti érdeke annak biztosítása, hogy az ügyfelei ne éljenek vissza a szolgáltatással (illetve fizetés nélkül ne kapjanak szolgáltatást), ezzel egy időben a vállalat ügyfeleinek, az adófizetőknek és a széles közösségnek szintén az a jogszerű érdeke, hogy a tisztességtelen tevékenységeket visszafogják, illetve – amennyiben megtörténtek – felfedjék. Általánosságban az, hogy az adatkezelő nemcsak a saját jogszerű (pl. üzleti) érdekében cselekszik, hanem a szélesebb közösség érdekében is, jobban az említett érdek felé billenti a mérleget. Minél lényegesebb a közérdek vagy a szélesebb közösség érdeke, és minél egyértelműbben elfogadott és elvárt a közösségben és az adatkezelők körében az, hogy az adatkezelő cselekedhet és adatokat dolgozhat fel ezeknek az érdekeknek az érvényesítése során, annál nagyobb súlyt képvisel ez a jogszerű érdek a mérlegelésben.[84]

3.4. Az adatkezelés elveinek érvényesülése

A személyes adatok kezelésének eleget kell tenniük a Rendelet által rögzített elveknek: a jogszerűség, tisztességes eljárás és átláthatóság elvének, a célhoz kötöttség elvének, az adattakarékosság elvének, a pontosság elvének, a korlátozott tárolhatóság elvének, illetőleg az integritás és bizalmas jelleg elvének.[85]

Ezeknek az elveknek minden esetben érvényesülniük kell, függetlenül az adatkezelés jogalapjától. Még ha az adatkezelésben érintett hozzá is járult a személyes adatainak kezeléséhez, az nem jogosítja fel az adatkezelőt arra, hogy a Rendelet szerinti kötelezettségeinek mértéke csökkenjen, vagy arra, hogy olyan adatkezelést végezzen, amely nem szükséges a meghatározott adatkezelési cél eléréséhez.[86] Erre azért is érdemes kiemelt figyelmet fordítani, mert az elmúlt években éppen az volt az egyik visszatérő kifogás a biztosítók adatkezelési gyakorlatával összefüggésben, hogy túlzott adatigénylésekkel lépnek fel, például olyan adatra tartanak igényt, amellyel kapcsolatban teljesen egyértelmű, hogy az nem befolyásolhatja a kár megtérítésére irányuló kérelem elbírálását.[87]

Az igényelt adatok körének meghatározása során tehát tiszteletben kell tartani az adattakarékosság elvét, amely megköveteli, hogy a kezelt adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak legyenek, és a szükségesre korlátozódjanak.[88] Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.[89]

3.5. Az adatkezelés időtartama

A jogszerű adatkezelés fontos eleme a kezelt személyes adatok tárolási időtartamának, a személyes adatok törlési határidejének a meghatározása. Ennek révén lehet eleget tenni a „korlátozott tárolhatóság" elvének, amelynek értelmében a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor).[90] Így tud eleget tenni az adatkezelő az érintett felé fennálló tájékoztatási kötelezettségének is, amely magában foglalja a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól való tájékoztatást is,[91] továbbá csak így készíthető el az adatkezelési tevékenységek nyilvántartása, amelynek lehetőség szerint tartalmaznia kell a különböző adatkategóriák törlésére előirányzott határidőkre vonatkozó információkat is.[92]

Egyes esetekben a biztosítók helyzetét megkönnyíti, hogy jogszabály határozza meg az adatkezelés időtartamát, így például a Pmt., amelynek alapján a biztosító az ügyfél-azonosítási kötelezettség teljesítése során birtokába jutott személyes adatokat az üzleti kapcsolat megszűnésétől, illetve az ügyleti megbízás teljesítésétől számított nyolc évig jogosult kezelni.[93]

A Bit. is tartalmaz az adatkezelés időtartamára vonatkozó előírásokat, egyebek között kimondva, hogy a biztosító a személyes adatokat a biztosítási jogviszony fennállásának idején, valamint azon időtartam alatt kezelheti, ameddig a biztosítási jogviszonnyal kapcsolatban igény érvényesíthető, illetőleg a létre nem jött biztosítási szerződéssel kapcsolatos személyes adatokat addig kezelheti, ameddig a szerződés létrejöttének meghiúsulásával kapcsolatban igény érvényesíthető.[94] Mindemellett a Bit. azt is előírja, hogy a biztosító köteles törölni minden olyan, ügyfeleivel, volt ügyfeleivel vagy létre nem jött szerződéssel kapcsolatos személyes adatot, amelynek kezelése esetében az adatkezelési cél megszűnt, vagy amelynek kezeléséhez az érintett hozzájárulása nem áll rendelkezésre, illetve amelynek kezeléséhez nincs törvényi jogalap.[95]

4. Profilalkotás, automatizált döntés, adatvédelmi hatásvizsgálat

A profilalkotást és az automatizált döntéshozatalt egyre több ágazatban használják, a biztosítási szektorban is egyre elterjedtebb.

Profilalkotásnak minősül a Rendelet szerint a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.[96] A profilalkotás esetén egy szervezet kifejezetten szeretné elemezni vagy megjósolni az egyes ügyfelek személyes preferenciáit, viselkedését és attitűdjeit, amelyek később az említett ügyfelek tekintetében hozott intézkedések vagy döntések meghozatalában segítenek.[97]

A profilalkotás vonatkozásában is érvényesülnie kell a jogszerűség, tisztességes eljárás és átláthatóság elvének.

A profilalkotás vonatkozásában is érvényesülniük kell a személyes adatok kezelésének Rendeletben rögzített elveinek, így a jogszerűség, tisztességes eljárás és átláthatóság elvének is.[98] Ezt szolgálandó az érintettet tájékoztatni kell a profilalkotás tényéről és annak következményeiről.[99]

Az automatizált döntéshozatal esetében az adatkezelő az érintettre, annak jogi helyzetére hatást gyakorló döntését technikai eszközökkel automatizált döntéshozatal által hozza meg. Az ehhez szükséges adatok rendelkezésre állhatnak magának az érintettnek az adatközlése által, de az érintettről más módon rendelkezésre álló adatok is felhasználásra kerülhetnek. A Rendelet alapján minden érintett számára biztosítani kell a jogot arra, hogy megismerje azt, hogy a személyes adatok automatizált kezelése milyen logika alapján történt, valamint azt, hogy az adatkezelés – legalább abban az esetben, amikor az profilalkotásra épül – milyen következményekkel járhat, továbbá hogy minderről tájékoztatást kapjon.[100]

Ennek a tájékoztatásnak kellő részlezetettségűnek kell lennie, ezért az adatkezelők nem tesznek eleget a Rendeletben előírt kötelezettségüknek egy semmitmondó, formális tájékoztatással. Ha például egy hitelintézet automatikus döntéshozatalt alkalmaz a hitelkérelmek elbírálására, akkor érthetően meg kell magyaráznia az alkalmazott logikát (így a döntés meghozatalakor figyelembevételre kerülő főbb jellemzőket, az adatok forrását és relevanciáját), annak jelentőségét (pl. azt, hogy az automatikus döntéshozatal miként járul hozzá igazságos és felelős hitelezési döntések meghozatalához), az érintettre nézve milyen várható következményeket (e körben lehetőség szerint az érintett számára érthető, kézzelfogható példákkal), az automatizált döntéshozatali eljárás megfelelő voltának folyamatos tesztelésére, ellenőrzésére vonatkozó információkat.[101]

Ha például a biztosító az ügyfelek vezetési viselkedésének figyelemmel kísérésén alapuló automatizált döntéshozatali eljárást alkalmaz a gépjármű-biztosítási díjak megállapítására, akkor ismertetheti, hogy a veszélyes vezetés nagyobb kárkifizetésekhez vezet, ezt alátámasztandó például egy applikáció révén bemutatva a sebesség és a féktávolság közötti összefüggést, grafikonokkal alátámasztott javaslatot is megfogalmazva arról, hogy miként lehet kedvezően változtatni a vezetési szokásokon, csökkentve ezzel a biztosítási díjak mértékét is.[102]

Felhívjuk a figyelmet, hogy profilalkotás és automatizált döntéshozatal alkalmazása esetén a biztosítónak adatvédelmi hatásvizsgálatot kell végeznie. Ilyen hatásvizsgálat lefolytatására akkor kell sort keríteni, ha az adatkezelés valamely (különösen új technológiákat alkalmazó) típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Ekkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. A Rendelet értelmében e körbe tartozik a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen (ideértve a profilalkotást is) alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek.[103]

Az adatvédelmi hatásvizsgálat lefolytatásának kötelezettsége nemcsak a 2018. május 25. után megkezdett adatkezelési tevékenységeket érinti, hanem a már folyamatban lévő adatkezelési műveleteket is. Ez utóbbi körben adatvédelmi hatásvizsgálatot kell lefolytatni, ha az adatkezelés végrehajtásának körülményei (hatókör, cél, a gyűjtött személyes adatok köre, az adatkezelők vagy címzettek kiléte, az adatmegőrzési időszak, a technikai és szervezési intézkedések stb.) megváltoznak, és amelyek esetében valószínűsíthető, hogy magas kockázattal járnak. Ezenfelül akkor is szükség lehet adatvédelmi hatásvizsgálatra, ha az adatkezelési műveletekből eredő kockázatok módosulnak, például azért, mert új technológiákat kezdenek el használni, vagy a személyes adatokat eltérő célra használják fel.[104]

Megjegyezzük, a Rendelet kapcsán aggályként fogalmazódott meg egyes szakmai szervezetek részéről, hogy miközben a profilalkotásnak nemcsak negatív hozadékai lehetnek az ügyfelek számára, a Rendelet jelentősen korlátozhatja a pénzügyi intézményeknek azon lehetőségeit, hogy az adatok elemzésével jobban meg tudják ismerni ügyfeleiket, személyre szabottabb szolgáltatásokat alakítsanak ki, és megelőzzék a csalásokat.[105]

5. Adathordozhatóság

A biztosítók számára valószínűsíthetően jelentős kihívást jelent majd az érintettek adathordozhatósághoz való jogának érvényre juttatása.

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha az adatkezelés hozzájáruláson vagy szerződésen alapul, és az adatkezelés automatizált módon történik. Ha ez technikailag megvalósítható, az érintett kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is.[106] Az adathordozhatóság révén tehát az érintettek által rendelkezésre bocsátott adatok továbbításra kerülnek egy másik szolgáltatóhoz (akár ugyanabban az üzleti ágazatban, akár egy másikban). [107]

Az adathordozhatósághoz való jog nem korlátlan.

Az adathordozhatósághoz való jog (amelyről az adatkezelőnek tájékoztatnia kell az érintettet [108]) nem korlátlan. Az érintett csak akkor élhet e joggal, ha

- az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, illetve ha az adatkezelés szerződés teljesítéséhez szükséges, így e jog nem gyakorolható akkor, ha az adatkezelés jogalapja a hozzájárulástól vagy szerződéstől eltérő egyéb jogalap, azaz például ha a személyes adatok kezelésére valamely, az adatkezelőre alkalmazandó jogi kötelezettség teljesítéséhez van szükség. Az adathordozhatósághoz való jog az érintett által tudatosan és aktívan továbbított adatokra, továbbá az érintett tevékenysége révén generált személyes adatokra terjed ki,[109] nem terjed ki ugyanakkor például a Pmt. szerinti azonosítás céljából kezelt személyes adatokra,[110]
- a személyes adatok kezelése automatizált módon történik,
- nem érinti hátrányosan mások jogait és szabadságait, így különösen nem sérti más érintettek Rendelet szerinti jogait abban az esetben, amikor az adott személyes adatállomány egynél több érintettre vonatkozik,
- nem sérti a törléshez való jogra vonatkozó rendelkezéseket, mivel a hozzáféréshez való jog ugyan nem érinti az érintett jogát arra, hogy a személyes adatainak törlését elérje, azonban nem járhat az érintettre vonatkozó olyan személyes adatok törlésével, amelyeket az érintett valamely szerződés teljesítése céljából bocsátott rendelkezésre, ha és ameddig a szóban forgó személyes adatokra szükség van az adott szerződés teljesítéséhez,[111]

- a Rendelet szerinti jogait, nem pedig kizárólag valamely ágazati jogszabály szerinti jogait kívánja gyakorolni.[112]

A 29-es munkacsoport szerint az adatkezelőknek bevált gyakorlatként olyan eszközöket (pl. letöltő eszközöket és felhasználói program interfészeket) kell kifejleszteniük, amelyek hozzájárulnak az adathordozhatósági kérelmek megválaszolásához. Az adatokat tagolt, széles körben használt, géppel olvasható formátumban kell továbbítaniuk, és törekedniük kell az adathordozhatósággal kapcsolatos kérelem érvényesítése során használt adatformátum interoperabilitásának biztosítására.[113]

6. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő (korábban: belső adatvédelmi felelős) intézménye nem új, azonban míg a 95/46/EK irányelv nem írta elő az adatkezelők és az adatfeldolgozók számára adatvédelmi tisztviselő kijelölését, addig a Rendelet alapján egyes adatkezelők és adatfeldolgozók már kötelesek erre. Az adatvédelmi tisztviselő számos adatkezelő számára a Rendelet által teremtett új jogi keret középpontjában áll majd, ellátva a Rendeletben előírt feladatait (a Rendeletnek való megfelelés ellenőrzése, adatvédelmi hatásvizsgálat kapcsán szakmai tanács nyújtása, együttműködés az adatvédelmi felügyeleti hatósággal, nyilvántartás vezetése stb.).[114]

A biztosítók szokásos üzletmenetük keretében történő, személyes adatokat érintő adatkezelése egyike a 29-es munkacsoport által a nagymértékű vagy nagy számban történő adatkezelésre felhozott példáknak.[115] De az érintettek rendszeres és szisztematikus megfigyelésére is sor kerülhet a biztosító által például adatvezérelt marketingtevékenység, profilalkotás vagy éppen a biztosítási díjak mértékének megállapítása során kockázatértékelési célból alkalmazott pontozás (scoring) esetén.[116] Figyelemmel erre az állapítható meg, hogy főszabály szerint a biztosítók kötelesek adatvédelmi tisztviselő kijelölésére.

A Rendelet értelmében a vállalkozáscsoport közös adatvédelmi tisztviselőt is kijelölhet, ha az adatvédelmi tisztviselő valamennyi tevékenységi helyről könnyen elérhető.[117]

Az adatvédelmi tisztviselő más tagállamban székhellyel rendelkező biztosító magyarországi fióktelepe általi kijelölésének kérdésével külön állásfoglalásban foglalkozott a NAIH, egyebek között kifejtve, hogy ha az Európai Unió más tagállamában – vagy adott esetben harmadik államban – székhellyel rendelkező, Magyarországon csupán fióktelepet fenntartó biztosító a Rendelet alapján adatvédelmi tisztviselő kijelölésére köteles, ezen kötelezettségének a vállalkozáscsoport akár egyetlen közös adatvédelmi tisztviselő kijelölésével is eleget tehet. Ebből következően a biztosító magyarországi fióktelepe a Rendelet alkalmazásának kezdetét követően nem köteles önálló, csak az adott fióktelep vonatkozásában illetékes adatvédelmi tisztviselő kijelölésére, feltéve, hogy a vállalkozáscsoporti szinten kijelölt adatvédelmi tisztviselő ilyen körülmények között is könnyen elérhető az érintettek, valamint az adatvédelmi felügyeleti hatóság számára. A magyarországi fióktelep vonatkozásában elvárásként jelenik meg, hogy a fióktelep személyzetének rendelkeznie kell a vállalkozáscsoport adatvédelmi tisztviselőjével történő kommunikációhoz szükséges, az adatvédelmi tisztviselő munkájának érdemi támogatására alkalmas nyelvi képességekkel.[118]

7. Összegzés

A Rendelet alkalmazásával kapcsolatban számos olyan kérdés fogalmazható meg, amelyek megválaszolásában az Európai Adatvédelmi Testületnek és a tagállami adatvédelmi felügyeleti hatóságoknak (esetünkben elsősorban a NAIH-nak) kiemelkedő szerepe lesz. A Rendelet és a jogyakorlat helyes értelmezése különösen fontos a jelentős mennyiségű személyes adatot kezelő biztosítók számára, amit ugyanakkor nehezítenek az ágazati szabályozás adatkezelést érintő előírásai. E feszültség feloldása érdekében mindenképpen támogatandó az ágazati szabályozás módosítása, a Rendelettel való maradéktalan összhangba hozatala.

HIVATKOZÁSOK

[1]Vö. Rendelet 4. cikk 1. pont.

[2]Amint azt a NAIH a NAIH/2018/766/2/V. számú állásfoglalásában kiemeli, a GDPR hatálya a nyilvántartási céltól függetlenül kiterjed valamennyi automatizált adatkezelésre. Az automatizált adatkezelés fogalmába az automatizált eszköz útján történő adatkezelések tartoznak, amelyek – a manuális (azaz kézi) adatkezeléssel szemben – jellemzően az adatokon elektronikus eszközzel, számítógéppel végzett adatkezelési műveleteket jelentik. A biztosítók esetében az automatizált adatkezelés általánosnak tekinthető.

[3]Lásd pl. az Insurance Europe által a Rendelettel kapcsolatban készített anyagokat (https://www.insuranceeurope.eu/search?search_api_views_fulltext=GDPR), illetőleg a Steptoe & Johnson LLP által a BIPAR részére készített anyagot: Commentary on the General Data Protection Regulation (http://www.bipar.eu/fr/page/commentaire-sur-le-gdpr).

[4]Lásd pl. Az adatvédelmi biztos beszámolója 2006. p. 101., Az adatvédelmi biztos beszámolója 2010. p. 145.

[5]Lásd az Európai Parlament és a Tanács lakossági befektetési csomagtermékekkel, illetve biztosítási alapú befektetési termékekkel kapcsolatos kiemelt információkat tartalmazó dokumentumokról szóló 1286/2014/EU rendelete 21. cikkének (1) bekezdését és (34) preambulumbekezdését. Lásd még az Európai Bizottságnak a lakossági befektetési csomagtermékekkel, illetve biztosítási alapú befektetési termékekkel kapcsolatos kiemelt információkat tartalmazó dokumentumokról szóló 1286/2014/EU európai parlamenti és tanácsi rendeletnek a kiemelt információkat tartalmazó dokumentumok megjelenítése, tartalma, felülvizsgálata és módosítása, valamint az ilyen dokumentumok rendelkezésre bocsátására vonatkozó kötelezettség teljesítése tekintetében meghatározott szabályozástechnikai standardok megállapítása révén történő kiegészítéséről szóló 2017. március 8-i 2017/653/EU felhatalmazáson alapuló rendeletét. Lásd továbbá a MABISZ Kiemelt Információkat tartalmazó Dokumentummal (KID) kapcsolatos útmutatóját (http://mabisz.hu/hu/kid.html), illetve Haraszti Zsófia – Mátyás Miklós Dániel – Turi Petra: PRIIPS rendelet: a jogszabálycsomag kialakításához vezető út és a végleges szabályok értékelése, Biztosítás és Kockázat 2017/4.

[6]Lásd az Európai Parlament és a Tanács 2017. január 10-i javaslatát, COM(2017) 10 final 2017/0003 (COD).

[7]A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, 2017. július 18. https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf A biztosítási tevékenység több elemét érintő blockchain és a GDPR közötti feszültségre hívja fel a figyelmet pl. Egri Szilvia: Elhasalhat a blockchain a GDPR oltárán, https://fintechzone.hu/elhasalhat-a-blockchain-a-gdpr-oltaran/.

[8]A jelenleg hatályos Infotv. és az Infotv. módosításáról szóló, 2017 augusztusában benyújtott (majd visszavont) tervezet összehasonlítását lásd https://twobirdsideas.hu/2017/09/04/az-infotv-modositasa-osszehasonlitottuk-az-im-tervezet-a-hatalyos-torvenyszoveggel/.

[9]Bit. 159. § (2) bekezdés. A biztosítók panaszkezelésének szabályozásáról lásd a Bit. 159. §-át és a biztosítók, a többes ügynökök és az alkuszok panaszkezelésének eljárásával, valamint panaszkezelési szabályzatával kapcsolatos részletes szabályokról szóló 437/2016. (XII. 16.) Korm. rendeletet.

[10]Bit. 121. § (1) bekezdés k) pont.

[11]A tagállami szabályozás keretei között ezt a megközelítést lásd pl. 3356/2017. (XII. 22.) AB határozat 35. pont.

[12]Lásd pl. az MNB átfogó vizsgálatot lezáró H-JÉ-II-B-1/2018. számú határozatát, amelynek rendelkező része szerint az MNB az ügyfelek adatainak kezelésével összefüggésben figyelmezteti a biztosítót, hogy a megszűnt biztosítási szerződések kapcsán személyes adatot a jövőben csak addig kezeljen, amíg a biztosítási jogviszonnyal kapcsolatban igény érvényesíthető, illetve amelynek kezeléséhez van törvényi jogalapja, előírva, hogy a Biztosító a figyelmeztetéssel kapcsolatban megtett intézkedésekről – dokumentumokkal alátámasztottan – 2018. április 30. napjáig írásban tájékoztassa

az MNB-t. http://alk.mnb.hu/data/cms2456906/keksz_15531941.pdf

[13]Rendelet 83. cikk (3) bekezdés.

[14]Rendelet 82. cikk.

[15]http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html

[16]Vö. Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679 p. 8.

[17]2011-ben a biztosításfelügyeleti hatóság (akkor a Pénzügyi Felügyeletek Állami Felügyelete) jóerkölcsbe ütközőnek minősítette az egyik biztosítónak azt a biztosítási termékét, amely szerint a biztosító szolgáltatása mérsékelte volna a gépjármű üzembentartójával szemben közúti sebességtúllépés miatt kiszabott közigazgatási bírságot, és felfüggesztette a termék terjesztését. Lásd PSZÁF: a jóerkölcsbe ütközik a gyorshajtási bírság elleni biztosítás, https://www.portfolio.hu/finanszirozas/bankok/pszaf-a-joerkolcsbe-utkozik-a-gyorshajtasi-birsag-elleni-biztositas.159386.html

[18]Bit. 149–151. §

[19]A 95/46/EK irányelv 29. cikkének (1) bekezdése kimondta, hogy létrejön a személyesadat-feldolgozás vonatkozásában az egyének védelmével foglalkozó munkacsoport: A munkacsoport az egyes tagállamok által kijelölt felügyelő hatóság vagy hatóságok képviselőjéből, a közösségi intézmények és szervek nevében létrehozott hatóság vagy hatóságok képviselőjéből, továbbá az Európai Bizottság egy képviselőjéből áll [29. cikk (2) bekezdés]. A Rendelet alapján a 29-es munkacsoport helyébe lép mint független, jogi személyiséggel rendelkező uniós szerv az Európai Adatvédelmi Testület, amelynek feladata, hogy elősegítse a Rendelet egységes alkalmazását. Lásd elsősorban a Rendelet (139), (140) és (143) preambulumbekezdését, illetve 68–76. cikkét.

[20]Pmt. 13. § (1) bekezdés. Lásd még a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól szóló 19/2017. (VII. 19.) MNB rendeletet, amelynek értelmében például a biztosító a Pmt.-ben meghatározottakon kívül egyszerűsített ügyfél-átvilágítást alkalmazhat az életbiztosítási ágba tartozó biztosítás esetén, amennyiben ügyfele olyan biztosítást köt, amelynek az éves biztosítási díja nem haladja meg a kettőszázhatvanezer forintot, vagy amennyiben az egyszeri biztosítási díj nem haladja meg a hatszázötvenezer forintot [11. § 7. pont].

[21]Pmt. 13. § (3) és (4) bekezdés.

[22]Lásd a Rendelet 14. cikkét.

[23]Rendelet (27) preambulumbekezdés.

[24]Bit. 143. § (3) és (4) bekezdés.

[25]A Rendelet 37. cikke az adatvédelmi tisztviselő kijelölése tekintetében mind az adatkezelőkre, mind az adatfeldolgozókra vonatkozik, Attól függően, hogy ki felel meg a kötelező kijelölés kritériumainak, egyes esetekben csak az adatkezelő vagy csak az adatfeldolgozó, míg más esetekben az adatkezelő és az adatfeldolgozó is köteles adatvédelmi tisztviselőt kijelölni (e tisztviselőknek ezt követően együtt kell működniük). A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban (az elfogadás időpontja: 2016. december 13., legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.) p. 11. Az adatvédelmi tisztviselő személyével kapcsolatos követelményekről lásd még pl. a NAIH NAIH/2018/929/2/K. számú állásfoglalását.

[26]Vö. Rendelet 4. cikk 7. és 8. pont.

[27]Vö. Rendelet 26. cikk (1) bekezdés.

[28]Rendelet 28. cikk (1) bekezdés.

[29]Lásd a Rendelet 28. cikkének (3) bekezdését.

[30]Lásd a Bit. 91. §-ának (2) bekezdését.

[31]Rendelet 29. cikk.

[32]Rendelet 5. cikk (1) bekezdés b) pont.

[33]Rendelet (39) preambulumbekezdés.

[34]Vö. 3356/2017. (XII. 22.) AB határozat 32. pont.

[35]Vö. 3062/2017. (III. 31.) AB határozat 28. pont.

[36]A 29. cikk szerinti munkacsoport 01/2014. számú véleménye a szükségesség és arányosság fogalmának alkalmazásáról és az adatvédelemről a bűnüldözési ágazatban p. 20.

[37]Lásd pl. NAIH-3090-8/2013/V.

[38]Az adatvédelmi biztos beszámolója 2009. pp. 100–101.

[39]Az adatvédelmi biztos beszámolója 2010. pp. 144–145.

[40]Bit. 135. § (1) és (2) bekezdés.

[41]Vö. Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről pp. 76–77. Az adott esetben a marketing-adatbázis forrása a cégek által működtetett honlapon történő regisztráció. Az adatbázis-marketing során az egyik cég közvetíti mások ajánlatát, ennek során SMS-t vagy e-mailt küld a regisztráltaknak. A telemarketing során a szerződéses partnerük által működtetett call center különböző bankok, biztosítók termékét, biztosítását reklámozza. A cég nevében telefonáló szerződéses partnerük közvetíti a saját vagy mások ajánlatát az adatbázisaiból kapott listán szereplő ügyfeleknek. A telemarketing kampányok során nem a hirdető, hanem egy külön call center kapja meg az adatokat, és végzi a telefonhívásokat.

[42]BH2016. 290. (Kúria Kfv.II.37.886/2015.) 20. pont.

[43]Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény 30/A. § (1) bekezdés.

[44]Bit. 134. § (1) bekezdés.

[45]Rendelet 10. cikk.

[46]Például a Nemzeti Adatvédelmi és Információszabadság Hatóság a 2012. évi tevékenységéről szóló beszámolójában (pp. 41–42.) az érintett egészségi állapotáról szóló dokumentáció különleges adatnak minősül, így szigorúbb szabályozás alá tartozik.

[47]Rendelet 4. cikk 15. pont.

[48]Rendelet 9. cikk (1) bekezdés, (2) bekezdés a) pont, (4) bekezdés.

[49]Bit. 136. §.

[50]Rendelet 9. cikk (2) bekezdés i) pont.

[51]Rendelet (54) preambulumbekezdés.

[52]Vö. A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről p. 68.

[53]Vö. a 29. cikk szerinti munkacsoport 06/2014. számú véleménye p. 17.

[54]Lásd az Európa Tanács Miniszteri Bizottságának CM/Rec (2016)8 ajánlását.

[55]Rendelet 4. cikk 1. pont.

[56]Rendelet (42) preambulumbekezdés.

[57]Vö. Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679 p. 11.

[58]Vö. idem. p. 4. A hozzájáruláshoz szükséges előzetes tájékoztatásról lásd pp. 14–15.

[59]NAIH/2015/328/20/H.

[60]Rendelet 7. cikk (4) bekezdés.

[61]Rendelet (42) preambulumbekezdés.

[62]Bit. 135. § (2) bekezdés.

[63]Bit. 135. § (1) és (2) bekezdés.

[64]Az adatvédelmi biztos beszámolója 2009 p. 102.

[65]Rendelet 6. cikk (1) bekezdés b) pont.

[66]A 29. cikk szerinti munkacsoport 06/2014. számú véleménye p. 18.

[67]Vö. Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679 pp. 9–10.

[68]A 29. cikk szerinti munkacsoport 06/2014. számú véleménye p. 19.

[69]Vö. idem. p. 19.

[70]Idem. p. 20.

[71]Rendelet 6. cikk (1) bekezdés c) pont.

[72]A 29. cikk szerinti munkacsoport 06/2014. számú véleménye p. 20.

[73]Rendelet (41) preambulumbekezdés.

[74]Lásd a 29. cikk szerinti munkacsoport 06/2014. számú véleményét p. 21.

[75]Bit. 135. § (1) bekezdés.

[76]Lásd a Pmt. 7. §-a (2) bekezdésének a) pontját.

[77]Pmt. 7. § (3) és (8) bekezdés.

[78]Lásd a NAIH elnökének levelét a nemzetgazdasági miniszterhez, https://naih.hu/files/NAIH-3383-2-2017-J-170629.pdf .

[79]Lásd Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről pp. 100–101.

[80]Rendelet 6. cikk (1) bekezdés f) pont.

[81]A 29. cikk szerinti munkacsoport 06/2014. számú véleménye pp. 3., 9. és 27.

[82]Idem. pp. 26–28.

[83]Idem. p. 36.

[84]Idem. p. 38.

[85]Rendelet 5. cikk (1) bekezdés.

[86]Vö. Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679 pp. 4–5.

[87]Lásd pl. az adatvédelmi biztos beszámolója 2010 pp. 145–146.

[88]Rendelet 5. cikk (1) bekezdés c) pont.

[89]Rendelet (39) preambulumbekezdés.

[90]Rendelet 5. cikk (1) bekezdés e) pont.

[91]Rendelet 13. cikk (2) bekezdés a) pont, 14. cikk (2) bekezdés a) pont.

[92]Rendelet 30. cikk (1) bekezdés f) pont.

[93]Pmt. 56. § (2) bekezdés.

[94]Bit. 142. § (3) bekezdés és 143. § (1) bekezdés.

[95]Bit. 143. § (2) bekezdés.

[96]Rendelet 4. cikk 4. pont.
[97]A 29. cikk szerinti munkacsoport 06/2014. számú véleménye p. 51.
[98]Rendelet 5. cikk (1) bekezdés a) pont.
[99]Rendelet (60) preambulumbekezdés, 13. cikk (2) bekezdés f) pont, 14. cikk (2) bekezdés g) pont.
[100]Rendelet (63) preambulumbekezdés, 13. cikk (2) bekezdés f) pont, 14. cikk (2) bekezdés g) pont. Az automatizált döntéshozatal kapcsán lásd különösen a Rendelet 22. cikkét és (71) preambulumbekezdését.
[101]Vö. Rendelet 13. cikk (2) bekezdés f) pont, 14. cikk (2) bekezdés g) pont, illetve Article 29 Data Protection Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 pp. 14–15.
[102]Vö. Article 29 Data Protection Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 p. 15.
[103]Rendelet 35. cikk (3) bekezdés a) pont.
[104]A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e" p. 16.
[105]Vö. pl. European Banking Federation's response to the European Commission Green paper on retail financial Services (18 March 2016), http://www.ebf-fbe.eu/wp-content/uploads/2016/03/EBF_020359-EBF-Response_-Green-Paper-RFS_-18-03-2016.pdf p. 35.
[106]Rendelet 20. cikk (1) és (2) bekezdés.
[107]A 29. cikk szerinti munkacsoport iránymutatása az adatok hordozhatóságáról p. 5.
[108]Rendelet 13. cikk (2) bekezdés b) pont, 14. cikk (2) bekezdés c) pont.
[109]A 29. cikk szerinti munkacsoport iránymutatása az adatok hordozhatóságáról p. 3.
[110]Lásd idem. pp. 9–10.
[111]Rendelet 20. cikk és (68) preambulumbekezdés.
[112]A 29. cikk szerinti munkacsoport iránymutatása az adatok hordozhatóságáról p. 9.
[113]Vö. idem. p. 3.
[114]A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban pp. 19–22.
[115]Idem. p. 10.
[116]Lásd idem. p. 11.
[117]Rendelet 37. cikk (2) bekezdés.
[118]NAIH/2017/6175/V. A vállalkozáscsoport közös adatvédelmi tisztviselőjével összefüggésben lásd még a 29. cikk szerinti munkacsoport iránymutatását az adatvédelmi tisztviselőkkel kapcsolatban pp. 12–13.

IRODALOMJEGYZÉK

A 29. cikk szerinti munkacsoport 01/2014. számú véleménye a szükségesség és arányosság fogalmának alkalmazásáról és az adatvédelemről a bűnüldözési ágazatban

A 29. cikk szerinti munkacsoport 06/2014. számú véleménye az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról

A 29. cikk szerinti munkacsoport iránymutatása az adatok hordozhatóságáról (elfogadás időpontja: 2016. december 13., a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.)

A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e" (az elfogadás időpontja: 2017. április 4., a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4.)

A 29. cikk szerinti munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban (az elfogadás időpontja: 2016. december 13., legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.)

Article 29 Data Protection Working Party: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (adopted on 3 October 2017)

Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679 (adopted on 28 November 2017)

Az adatvédelmi biztos beszámolója 2009

Az adatvédelmi biztos beszámolója 2010

Egri Szilvia: Elhasalhat a blockchain a GDPR oltárán, 2018. március 6., https://fintechzone.hu/elhasalhat-a-blockchain-a-gdpr-oltaran/, letöltés időpontja: 2018. április 5.

European Banking Federation's response to the European Commission Green paper on retail financial Services (18 March 2016), http://www.ebf-fbe.eu/wp-content/uploads/2016/03/EBF_020359-EBF-Response_-Green-Paper-RFS_-18-03-2016.pdf, letöltés időpontja: 2018. április 5.

Haraszti Zsófia – Mátyás Miklós Dániel – Turi Petra: PRIIPS rendelet: a jogszabálycsomag kialakításához vezető út és a végleges szabályok értékelése, Biztosítás és Kockázat 2017/4.
https://doi.org/10.18530/bk.2017.4.14

Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, 2017. július 18. https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf, letöltés időpontja: 2018. április 5.

Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2012. évi tevékenységéről

Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2013. évi tevékenységéről

Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2016. évi tevékenységéről

Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive, 2017. december 19., http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html, letöltés időpontja: 2018. április 5.

PSZÁF: a jóerkölcsbe ütközik a gyorshajtási bírság elleni biztosítás, 2011. december 2., ttps://www.portfolio.hu/users/elofizetes_info.php?t=cikk&i=159386, letöltés időpontja: 2018. április 5.

Steptoe & Johnson LLP: Commentary on the General Data Protection Regulation http://www.bipar.eu/fr/page/commentaire-sur-le-gdpr, letöltés időpontja: 2018. április 5.