KÉSZÜLJÜNK AZ ÚJ EURÓPAI ADATVÉDELMI SZABÁLYOZÁSRA!

AZ ÁLTALÁNOS ADATVÉDELMI RENDELET[1] ÁTTEKINTÉSE ÉS ÉRTELMEZÉSE EGY BIZTOSÍTÓTÁRSASÁG SZEMÜVEGÉN KERESZTÜL

dr. Szatmári-Margitai Gergely (a cikk írása idején a Magyar Posta Biztosító Zrt. jogtanácsosa)

ÖSSZEFOGLALÓ

Az EU Általános Adatvédelmi Rendelete (GDPR) 2016. május 24-én lépett hatályba, és két év felkészülési időszakot követően 2018. május 25-től kell alkalmazniuk a piacoknak. A GDPR elsődleges célja a tagországok gyakorlatának további egységesítése, a személyes adatok védelmének erősítése, illetve a korábbi szabályok modernizálása a technológiai változások fényében.

Habár az új szabályozás célja elsődlegesen nem a biztosítási piac – amely már eddig sem szűkölködött szabályokban –, mégis szükségszerűen ettől a területtől is megköveteli az alkalmazkodást. Első megközelítésben a GDPR nem szolgál sok újdonsággal, mivel a magyar jogi környezet az Európai Unió rendeletének megjelenését megelőzően is a szigorúbb szabályozások közé tartozott. Ugyanakkor ha jobban megnézzük, azt látjuk, hogy a GDPR a nyilvánvaló jogi feladatokon túlmenően a szervezetek informatikai és compliance területétől is jelentős alkalmazkodást követel meg, illetve ezen területek szorosabb együttműködését várja el a jövőben. Jelen cikk ezeket a feladatokat tekinti át, illetve értelmezi egy hazai biztosító szemüvegén keresztül.

SUMMARY

EU General Data Protection Regulation /GDPR/

It came into force on 24 May 2016 and it must be applied by markets from 25 May 2018, after a 2-year long preparation period. The main goal of the GDPR is the further integration of member states, the strengthening of personal data protection and the modernization of former regulations in the light of technological development.

Although the main target of the new regulation is not the insurance market - which has already had lots of rules - but it requires conformity of this field too. At a first glance GDPR doesn't serve too many new issues as the Hungarian legal environment used to be among the stictest regulations before the appearance of the European Union Act.

However, if we examine things more thoroughly we can see that GDPR requires a great deal of conformity from the the fields of organizational informatics and compliance and expects a stronger cooperation of them in the future, apart from apparent legal tasks.

This article studies these tasks and analizes them through the glasses of a domestic insurance company.

BIZTOSÍTÁS ÉS KOCKÁZAT

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

JEL: G22, K20

DOI: 10.18530/BK.2017.4.52
http://dx.doi.org/1018530/BK.2017.4.52

I. Bevezető

A cikk feldolgozza az új adatvédelmi rendelet adta szabályozást, a vizsgálat kifejezetten a biztosítási szektort érintő kérdésekre koncentrál.

II. Rövid történeti áttekintés

A rendelet elemzését megelőzően szükséges az adatvédelmi szabályozás fejlődésének rövid áttekintése. Szőke Gergely László tanulmányából[2] megtudhatjuk, hogy az adatvédelmi jog szakirodalma Majtényi László és Jóri András munkái alapján – közel egyezően – három korszakot különböztet meg. Az első generációs szabályok a '70-es években fejlődtek ki, ekkor az állam és az akkori kor számítógépes nyilvántartási rendszerei alakították ki a védelmet. A '80-as és '90-es évek az automatizált rendszereken kívül a papíralapú nyilvántartásokban lévő adatok védelmét is a rendelkezések körébe vonták. A harmadik generációt az európai integráció és a szektoriális szabályok megjelenése határozza meg. A negyedik generációba – meghatározása Hegedű Bulcsúhoz köthető – az internet megjelenésével felmerülő adatvédelmi kérdések és a magánszférát erősítő technológiák miatti védelem sorolandó.

Mindezek után felmerülhet a kérdés, hogy ha már a negyedik generációban is megjelent az internet és a magánszféra adatainak védelme, akkor miért kell új szabályozás. Az európai jogalkotók a rendelet preambulumában leszögezik, hogy azért szükséges újragondolni a szabályokat, mert a gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását, a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok kezelőit. Míg az irányelv hatálybalépésének idején a személyi számítógép és ügyfél/szerver struktúra volt irányadó, jelenleg már az ún. „harmadik platform", a teljesen digitalizált környezet adott.

Az adatok gyűjtése és cseréje, elemzése olyan mértéket öltött az internetnek a mindennapi életünkbe történő beépülésével – lásd okostelefon, okostévé, „dolgok internete" –, hogy annak csak szilárd, szigorú és következetes uniós adatvédelmi kerete biztosíthatja a szabályok betartásának kikényszeríthetőségét. Ezen fejlődést az irányelv már nem tudta követni, nem adta meg a szükséges védelmet, illetve a jogi forma – irányelv – eltérő nemzeti szabályozásoknak adott lehetőséget, amely szabályozások így tagállamonként

eltérő jogokat biztosítottak a természetes személyeknek, miközben a személyes adatok védelméhez való jog olyan alapvető jog, mely állampolgárságtól, lakóhelytől függetlenül megilleti az embert.

III. A GDPR részletes elemzése

Elmondható, hogy az irányelv a harmonizációt, a rendelet az egységes szabályozást szolgálja, mert nem igényel tagállami átültetést, ezáltal az eddigi széttagolt tagállami szabályozások helyett következetesebb és egységesebb jogszabályi környezetet eredményez. A szabályozási keret fejlődése, szigorítása egyértelműen az online felületeken – pl. vásárlás, szerződéskötés – történő adatforgalom védelmét kívánja szolgálni. A rendelet preambulumának (10) pontja kimondja, hogy a tagállamok számára mozgásteret biztosít a szabályok pontosításához, kifejezetten kiemeli a személyes adatok jogszerű kezelési feltételeinek meghatározását.

A rendelet az egységes szabályozást szolgálja, mert nem igényel tagállami átültetést.

A rendelet a fentieken túl egyértelművé teszi, hogy a személyes adatok védelmét nem kizárólag elméletben kívánja megvalósítani, hanem kötelezi a tagállamokat, hogy a már meglévő felügyeleti szerveknek a szabályok betartásának ellenőrzéséhez és biztosításához egyenértékű hatáskört biztosítson, mely a jogsértések esetére azonos szankció alkalmazását teszi lehetővé. A jogalkotó a szabályok betartásának védelme érdekében továbbment, és kimondta azt is, hogy a védelemnek technológiailag semlegesnek kell lennie, nem függhet a felhasznált technikai megoldásoktól, vagyis akár automatizált, akár manuális, a személyes adatok védelmére vonatkozó szabályoknak meg kell valósulniuk.

A preambulum a személyes adatok kezelését hozzájáruláson alapulónak akkor tekinti, ha egyértelmű megerősítő cselekedettel önkéntesen, konkrétan a tájékoztatást követően teszi meg a természetes személy. A hozzájárulás bármilyen formában (írásban – akár elektronikus úton – vagy szóban) megadható, azonban az adatkezelőnek képesnek kell lennie a hozzájárulás megtörténtének az igazolására. A szabályozás a hallgatást, az előre bejelölt négyzetet vagy a nem cselekvést a fentiek alapján nem tekinti hozzájáruláson alapulónak. A tájékoztatással szembeni követelmény az egyértelműség és a tömörség. Ezen követelmények olvasásakor felmerül a kérdés, hogy ezek miként valósulhatnak meg a teljes körű tájékoztatás követelményével egyetemben, mert az elképzelhetetlen, hogy minden részlet szerepeljen egy tájékoztatóban, ugyanakkor az rövid és tömör is legyen.
A rendelet 6. cikke az Info törvénnyel szemben megkülönbözteti a szerződésen és a hozzájáruláson alapuló adatkezelést.

A személyes adatok kezelése akkor is jogszerű, ha jogszabály által megállapított rendelkezésen alapszik, de ez nem szükségszerűen jelent valamely parlament által elfogadott jogszabályt.

A fent említett, a tájékoztatással szembeni világosság, tömörség és egyértelműség követelményének való megfelelést a jogalkotó a preambulum (60) pontjában nevesített, ún. az információkat szabványosított ikonokkal történő megjelenítés lehetőségének a választhatóságával kívánja segíteni. Ilyen megoldások nem ismeretlenek az európai szabályozásban, valószínűsíthetően nem lesz haszontalan a fogyasztó szempontjából nézve, de kétségeim vannak, hogy ezeket jobban meg fogják nézni, vagy jobban fogják tudni értelmezni, mint a szöveges felvilágosítást.

A rendelet az átláthatóság követelményének szabályozásával – véleményem szerint – komoly technológiai kihívás elé állítja az adatkezelőket, mert megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás és kommunikáció könnyen hozzáférhető, közérthető, valamint világos és egyszerű nyelvezettel megfogalmazott legyen. Ez a követelmény az adatvédelem, a versenyjog és a fogyasztóvédelem metszésében „született" követelmény.[3]

A rendelet fenti pontja megköveteli a „mindenről" történő tájékoztatást, ami nem újdonság az adatvédelem területén, de ezen túlmenően az 58-as pont szükség esetén elvárja a vizuális megjelenítést is. A 63-as pont pedig már – bár feltételesen fogalmaz – azt a követelményt támasztja, hogy az adatkezelő távoli hozzáférést biztosítson egy biztonságos rendszerhez, melyben személyes adataihoz az érintett egyszerűen és észszerű időközönként hozzáférhessen, hogy az adatkezelés jogszerűségét megállapítsa és ellenőrizze. Ez az elszámoltathatóság követelményének az egyik eleme: a szabályozó a rendeletnek való megfelelés érdekében folyamatok kialakítását, valamint azok bemutatásának a képességét várja el az adatkezelőktől.

A gyakorlatban tapasztaltak alapján kétséges, hogy az ügyfelek az egyre hosszabb és bonyolultabb tájékoztatókat el fogják-e olvasni, és szánnak-e majd időt azok értelmezésére.

A szabályozás előírja az érintettek részére az adatokhoz történő díjmentes hozzáférés biztosítását, lehetőséget a helyesbítésre, esetlegesen a törlésre. A rendelet alapján az adatkezelőnek indokolatlan késedelem nélkül, de legkésőbb 30 napon belül indokolással ellátott választ kell küldeni.

Kétséges, hogy az ügyfelek az egyre hosszabb és bonyolultabb tájékoztatókat el fogják-e olvasni, és szánnak-e majd időt azok értelmezésére.

A jogalkotó elvárja az adatkezelőktől az automatizált módon működő adatkezelésnél, hogy az adatok géppel olvashatóak legyenek, és azokat interoperábilis formátumban az érintettek megkapják, de ez nem kötelezi arra az adatkezelőket, hogy egymással műszakilag kompatibilis rendszereket vezessenek be vagy tartsanak fenn.

Véleményem szerint a gyakorlatban – bár biztosító esetében egyelőre az online kötéseket kivéve nem fog számottevő szerepet játszani – a rendelet 20. cikkében szabályozott adathordozhatósághoz való jognak[4] lesz jelentősége, mert lehetővé teszi az érintettnek, hogy a rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható

formátumban megkapja, és azt másik adatkezelőnek átadja. Ez újabb feladatot generál az adatkezelőnek, amikor beérkezik a kérés az érintettől, aki valószínűsíthetően azonnal akarja adatainak kiadását vagy a megjelölt másik adatkezelőnek azok közvetlen továbbítását.
Amennyiben az adatok illetéktelenekhez kerülnek akár elektronikus, akár fizikai módon (adatvédelmi incidens[5]), az adatkezelőnek a tudomására jutástól a lehető leghamarabb, de legfeljebb 72 órán belül jelentést kell tennie a felügyeleti hatóságnál. A bejelentések miatt compliance és IT fejlesztés válhat szükségessé. Magas kockázatú incidens esetén az incidenssel érintetteket is tájékoztatni kell, ami komoly reputációs kockázatot és az adatkezelővel szembeni fogyasztói bizalom megrendülését jelentheti.

Incidens esetén a felügyeleti hatóságot és az érintettet kell tájékoztatni. A rendelet tervezete 24 órán belüli értesítést írt elő, azonban ez a viták során nem tűnt reálisnak. A rendelet 9. cikk (2) bek. a.) pontja kizárólag az egészségügyi adatok esetén írja elő a kifejezett hozzájárulást, a 6. cikk (1) bek. a.) pontjában nem szerepel a „kifejezett" fogalom, azonban valószínűsíthetően a gyakorlatban minden adatkezelés esetén írásbeli hozzájárulást fog kérni az adatkezelő, mert az „opt-out" hozzájárulás nem hozzájárulás. A személyes adatok kezelése kapcsán megjelölt új elv, az „adattakarékosság" még inkább szűkíti az adatkezelési jogalapot. A rendelet nem határoz meg konkrét adatmegőrzési határidőket, ezért ezekre továbbra is a tagállami jogszabályok vonatkoznak.

A rendelet 9. cikk (1) bek. az egészségügyi adatok kezelését tiltja, ez alól kivétel, ha az érintett kifejezetten hozzájárulását adja, vagyis a biztosítók számára az eddigi gyakorlatban változás nem lesz.

A rendelet előírja az érintett részére történő tömör, átlátható, érthető és könnyen hozzáférhető, világos, közérthető tájékoztatást, melynek a kérelem beérkezésétől számított legkésőbb 30 napon belül kell díjmentesen eleget tenni. A tájékoztatás kérése arra is vonatkozhat az érintettől, hogy személyes adatainak kezelése folyamatban van-e.
Az ún. „felejtéshez való jog" biztosító esetében nem számottevő intézmény, mert az kifejezetten a Google ellen hozott ítélet kapcsán került a rendeletbe, ezáltal kíván a Google keresőmotorjaira, illetve a tartalomszolgáltatók tevékenységére reflektálni.

Szabó Endre Győző, a NAIH elnökhelyettese korábban idézett vizsgálatában az adathordozhatóság kapcsán hangsúlyozza, hogy a „rá vonatkozó" kitétel és az „általa rendelkezésre bocsátott" fordulat szűkebb és tágabb értelmezésnek is teret ad. Nem maradhat azonban kétségünk afelől, hogy a hatóság a lehető legszélesebb értelmezést szeretné érvényesíteni. A NAIH elnökhelyettesének írásából kiderül az is, hogy egyeztetés alatt van, miként gyakorolható az internetes ügyintézés során megadott információk (például egy biztosítási kötvényhez szükséges adatok, ahol az egyes szereplők – szerződő, biztosított, kedvezményezett – eltérnek) esetében az adathordozhatóság.

A rendelet kapcsán mindenhol az olvasható, hogy a nyilvántartások vezetése és a dokumentáltság válik hangsúlyossá. Ezen követelmény megjelenik a belső adatvédelmi szabályok kialakításában (24. cikk), a magatartási kódexek (40. cikk) és a 30. cikkben nevesített nyilvántartások vezetésében. Ez az ún. „elszámoltathatóság" túldokumentáltsághoz vezethet, ami esetlegesen az adatkezelő és adatfeldolgozó párhuzamos dokumentációja alapján további – akár szükségtelennek is nevezhető – költségeket eredményez. Mindezek alapján megállapítható, hogy a korábbinál szélesebb körű és nem mindig észszerű dokumentálási kötelezettség és adminisztrációs teher került kialakításra az adatkezelők számára.
A beépített és alapértelmezett adatvédelem elve alapján az adatkezelőnek két kötelezettsége jelenik meg, az egyik a megfelelő technikai és szervezési intézkedések, a másik, hogy az adott konkrét adatkezelési cél szempontjából szükségesek legyenek, vagyis ez az előírás is azt a célt szolgálja, hogy az adatkezelő ne rendelkezzen több adattal, mint amennyi feltétlenül szükséges a cél eléréséhez. Természetesen az ilyen jellegű „szűkítések", pontosítások megoldása, kivitelezése költséges fejlesztéseket eredményez. Itt szükséges megjegyezni, hogy jó lenne, ha a szemlélet akként változna, hogy egy vállalat életében bármilyen üzleti vagy IT fejlesztési projekt van, annak része kell, hogy legyen már az indításakor az adatvédelmi szempontoknak való megfelelés előzetes értékelése, amennyiben a projekt „végterméke" természetes személyek személyes adatait érinti.

A rendelet kapcsán a nyilvántartások vezetése és a dokumentáltság válik hangsúlyossá.

Az adatbiztonság fogalma a rendeletben sem változik, általános keretet biztosít, nem határozza meg az adatbiztonsági intézkedések végrehajtásának módját, az alkalmazandó eljárásokat, technológiákat.

A rendelet lényeges és új jogintézménye az adatvédelmi hatásvizsgálat (35. cikk), amelynek elvégzése abban az esetben szükséges, ha a – különösen új technológiákat alkalmazó – adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira nézve. A rendelet egyfelől példákkal tartalmazza azokat az esetköröket, amikor a hatásvizsgálatot el kell végezni, másfelől a további esetköröket a rendelet felügyeleti hatóságok hatáskörébe utalja. Az előzetes konzultációt talán a hatásvizsgálat speciális esetének is lehetne nevezni, amikor a felügyeleti hatósággal egyeztet az adatkezelő. Fontos megjegyezni, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság által összeállítandó jegyzék még nem ismert. Nehezíti a helyzetet, hogy a hatásvizsgálat elvégzésének gyakorlati szempontjai nem egyértelműek.

A rendeletben a jelenlegi belső adatvédelmi felelős jogintézményét felváltja az adatvédelmi tisztviselő szabályozása. Tekintettel arra, hogy a biztosítóknál eddig is volt ilyen pozíció, ez nem teszi kérdésessé az új tisztség alkalmazását, de a szabályozásban megjelenő nagyfokú függetlenség hangsúlyozása említésre érdemessé teszi ennek az „intézménynek" a rövid ismertetését. Ennek alapján megfelelő tapasztalattal rendelkező saját alkalmazott (más feladatot is elláthat, ha az nem összeférhetetlen az adatvédelmi tisztséggel), de szerződéssel külsős adatvédelmi szakértő is betöltheti a pozíciót.

Az adatvédelmi tisztviselő függetlenségét biztosítani kell oly módon, hogy utasításokat senkitől nem fogadhat el, feladata kapcsán el nem bocsátható, szankcióval nem sújtható,

közvetlenül a legfelsőbb vezetőnek tartozzon felelősséggel, az érintett által közvetlenül felkereshető legyen, és elegendő forrással (pénz, infrastruktúra, képzés és idő) rendelkezzen. Véleményem szerint a rendelet magatartási kódexre vonatkozó rendelkezései a MABISZ-ra és tagjaira rónak feladatokat abban az esetben, ha a magyar biztosítási szektor részéről a szektorra vonatkozó közös magatartási kódex elkészítése iránti közös igény merülne fel. Kiemelendők a tanúsítások (42. cikk), melyek igazolják, hogy az adatkezelő által végrehajtott műveletek megfelelnek a rendelet előírásainak, ezek megléte esetén is vizsgálódhat a hatóság. Reálisan nem várható, hogy a közeljövőben sor kerül a tanúsítási mechanizmusok kialakítására és a tanúsító szervezetek kijelölésére, azonban a későbbiekben a megfelelés igazolásának jó eszközei lehetnek.

A rendeletből, tanulmányokból és előadásokból az a megállapítás is levonható, hogy az adatvédelem szabályainak be nem tartása vagy a hanyag adatkezelés komoly bírságokat fog eredményezni, és kétségünk sem lehet afelől, hogy ennek érvényt is fognak szerezni az adatvédelmi hatóságok.

Az adatvédelem szabályainak be nem tartása vagy a hanyag adatkezelés komoly bírságokat fog eredményezni.

IV. Összegzés

A szabályozás alapján véleményem szerint az látszik, hogy a korábbi „irány” változatlanul megmarad, de egységesebb, szigorúbb és részletesebb előírások várhatók a nemzeti hatóságtól, mely a megfelelő állomány elérése után alapos vizsgálatokat fog lefolytatni, és valószínűsíthetően nem fog visszarettenni a magasabb összegű bírságolástól sem.

A rövid áttekintés során remélem sikerült felkeltenem a kollégák „érdeklődését” a rendelet részletes átolvasásához.

HIVATKOZÁSOK

[1] 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 - 2016/679 (továbbiakban: „GDPR” – General Data Protection Regulation rövidítése). A GDPR-t2016. május 4-én hirdették ki, és május 24-én hatályba lépett, alkalmazni 2018. május 25. napjától kell.

[2] Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Információ és jog, 2013/3. pp. 107–112.

[3] Szabó Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről. Az adathordozhatóság és az adatvédelmi hatásvizsgálat, Pázmány Law Working Papers 2016/26.

[4] A személyes adatok feletti rendelkezést tovább erősíti.

[5] Az irányelvben még nem jelent meg, de a magyar szabályozás számára nem ismeretlen.

IRODALOMJEGYZÉK

Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Információ és jog, 2013/3. pp. 107–112.

Szabó Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről. Az adathordozhatóság és az adatvédelmi hatásvizsgálat, Pázmány Law Working Papers 2016/26.

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