BERKE & MOLNÁR
ÜGYVÉDI IRODA

Hírlevél
2018. március

Az Európai Unió új adatvédelmi rendeletének (GDPR) hatása a biztosítók és biztosításközvetítők adatkezelési tevékenységére

1. Az adatvédelmi rendelet hatálybalépése és alkalmazása

1.1 A szemünk előtt és mindannyiunk aktív részvételével az arany és az olaj után az adat vált a gazdaság legjelentősebb erőforrásává. A világ öt legértékesebb tőzsdén jegyzett vállalata adatokkal gazdálkodik. Nem mindegy tehát, hogy a vállalkozások ezt a kiemelt kinccsé vált erőforrást hol és milyen körülmények között tárolják, rendszerezik, továbbítják, használják fel pl. profilalkotásra és válnak meg tőlük, ha az adatkezelési cél megszűnt. Kiemelt jelentősége van ennek a biztosítási szektorban, ahol a kockázatok átvállalására specializálódott biztosítók adat- és információ éhsége történetileg is ismert és indokolt, és a biztosítási piacon is terjedőben lévő új technológiáknak köszönhetően ezek az adatok ma már sokszor automatikusan rögzítődnek és továbbítódnak a biztosítóknak, információt szolgáltatva ügyfeleik egészséges, vagy éppen egészségtelen életmódjáról, vezetési szokásairól stb.

1.2 Az Európai Bizottság, a Tanács és az Európai Parlament csaknem négy éves jogszabály előkészítési munkáját követően, **2016. május 4.** napján az Európai Unió Hivatalos Lapja L 119. számában (59. évfolyam), kihirdették az EU Általános Adatvédelmi Rendeletét, amelynek címe az Európai Parlament és a Tanács (EU) 2016. április 27-i 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről („**Rendelet**”). A Rendelet rövid neve angolul General Data Protection Regulation, rövidítve **GDPR**.

1.3 A Rendelet ugyan a kihirdetését követő huszadik napon hatályba lépett, azonban alkalmazni csak **2018. május 25.** napjától kötelező. Eddig kell a vállalkozásoknak, így pl. a személyes adatokat kezelő biztosítóknak és biztosításközvetítőknek is felkészülniük annak alkalmazására.

1.4 Az EU jog szupremáciájának (elsődlegességének) elve alapján az EU jog, így a Rendelet is megelőzi a tagállami jogot, így az azzal ellentétes tagállami szabályozás nem érvényesül.

1.5 A Rendelet ún. közvetlen hatállyal bír, azaz teljes egészében kötelező és közvetlenül alkalmazandó az Európai Gazdasági Térség valamennyi tagállamában, azaz annak tagállami jogba való külön átültetése szükségtelen, sőt tilos is, elkerülendő az EU szabályozás lerontásának lehetőségét.

1.6 A Rendelet maga sem zárja ki ugyanakkor azt, hogy a tagállamok pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be.

1.7 A Rendelet közvetlen hatályából, illetve a pontosító rendelkezésekre vonatkozó megengedő szabályaiból fakadóan a tagállamoknak, így Magyarországnak is feladata, hogy **2018. május 25.** napjáig olyan jogszabályi környezetet teremtsen, amelyben az adatvédelmi jogszabályok már csak olyan kérdéseket szabályoznak, amelyeket a Rendelet nem érint, illetve részletszabályokat tartalmaznak a Rendelet előírásaihoz képest.

2. Az adatvédelem szabályozása

2.1 A személyes adatok védelme Európában már a második világháborút követően szabályozásra került, egyfelől az elsődleges uniós jog forrását alkotó nemzetközi szerződések, másfelől a másodlagos uniós jog forrását alkotó jogszabályok által.

2.2 Az **Emberi Jogok Európai Egyezménye**[1] garantálja a magán- és családi élet, a lakás és a levelezés tiszteletben tartását, e jog gyakorlását törvény csak a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében korlátozhatja.[2]

2.3 Az **Európa Tanács 108. számú egyezménye**[3] az adatvédelem területén elfogadott első jogilag kötelező erejű nemzetközi okmány. Az egyezmény célja, hogy *„minden egyén számára […] biztosítva legyen, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák személyes adatainak gépi feldolgozása során”*.

2.4 Az **Európa Tanács ajánlások** formájában ad iránymutatást a személyes adatok védelme területén, ezek közül kiemelt jelentősége van a biztosítási célból gyűjtött és feldolgozott személyes adatok védelméről szóló 2002(9) számú, 2002. szeptember 18. napján elfogadott ajánlásnak.

2.5 Az **Európai Unió Alapjogi Chartájának**[4] 7. és 8. cikkében a magánélet tiszteletben tartása és a személyes adatok védelme egymással szorosan összefüggő, de különálló alapvető jogként nyer elismerést. A chartát beillesztették a Lisszaboni Szerződésbe[5], ezért jogilag kötelező erejű az Európai Unió intézményeire és testületeire és az – uniós jog végrehajtásakor – az uniós tagállamokra nézve.

2.5 Az **Adatvédelmi Irányelv**[6] jelenleg az adatvédelem legjelentősebb jogforrása az Európai Unióban. Az Adatvédelmi Irányelv az elérendő célokat illetően kötelező a tagállamokra, azonban annak átültetése – sok esetben jelentősen - eltérő tagállami szabályozásokhoz vezetett.

2.6 Magyarországon jelenleg az **Infotv.**[7] rendelkezik a személyes adatok védelméről, emellett a **Bit.**[8] rendelkezései tartalmaznak speciális szabályokat a biztosítási titoknak minősülő (személyes) adatok kezelésére vonatkozóan.

3. A Rendelet célja

3.1 A Rendelet preambulumának (9) bekezdése alapján az Adatvédelmi Irányelv célkitűzései és elvei továbbra is érvényesek, azonban az Adatvédelmi Irányelv sem akadályozta meg azt, hogy az adatvédelem végrehajtása a tagállamokban széttagolt módon valósuljon meg, továbbá nem akadályozta meg a jogbizonytalanságot és azt sem, hogy széles körben az a benyomás alakuljon ki, hogy a természetes személyek védelme jelentős kockázatoknak van kitéve. Az a tény pedig, hogy a személyes adatok védelme eltérő védelmet élvezett az egyes tagállamokban, útjában áll a személyes adatok Európai Unióban történő szabad áramlásának.

3.2 A Rendelet egyértelmű célja az egységes szabályozás megteremtése, ezáltal a jogbizonytalanság megszüntetése.

4. A Rendelet tárgyi hatálya

4.1 A Rendelet hatálya:

a) a személyes adatok részben vagy egészben automatizált kezelésére, valamint

b) a személyes adatok nem automatizált, azonban nyilvántartási célú adatkezelésére

terjed ki.

[1] Az emberi jogok és alapvető szabadságok védelméről szóló, Rómában 1950. november 4-én kelt egyezmény

[2] Emberi Jogok Európai Egyezménye, 8. cikk

[3] Az Európa Tanács 1981. január 28-i 108. számú egyezménye a személyes adatok gépi felhasználása során az egyének védelméről

[4] Az Európai Unió Alapjogi Chartáját 2000-ben, Nizzában hirdette ki a Parlament, a Tanács és a Bizottság

[5] Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról, amelyet Lisszabonban, 2007. december 13-án írtak alá

[6] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

[7] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

[8] A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény

5. A Rendelet területi hatálya

5.1 A Rendelet alkalmazandó:

a) minden az EU területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó tevékenységével összefüggésben végzett adatkezelésre akkor is, ha az adatkezelés az EU területén kívül történik,

b) minden, az EU területén tartózkodó érintett személyes adatainak kezelésére akkor is, ha az adatkezelő vagy az adatfeldolgozó az EU területén nem rendelkezik tevékenységi hellyel, ha az adatkezelési tevékenység:

ba) áruknak vagy szolgáltatásoknak az EU területén tartózkodó érintettek számára történő nyújtásához kapcsolódik, vagy

bb) az érintettek EU területén tanúsított viselkedésének megfigyeléséhez kapcsolódik,

c) minden az EU területén kívül végzett adatkezelésre, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.

6. A személyes adat fogalma

6.1 A személyes adat meghatározása lényeges újdonságot nem mutat a jelenlegi szabályozáshoz képest. A Rendelet **4. cikk 1. pontja** alapján személyes adat az: *„azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, 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."*

6.2 A Rendelet **preambulumának (26) bekezdése** alapján: *„Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést -, amelyről ésszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető ésszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni (...)"*

7. A különleges adat fogalma

7.1 A különleges adat meghatározása sem mutat újdonságot a jelenlegi szabályozáshoz képest, azzal a kivétellel, hogy annak köre kibővült. A Rendelet **9. cikk (1) bekezdése** alapján a személyes adatok különleges kategóriái: *„A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok (...)"*.

7.2 A hazai biztosítási piacon is elterjedt formája az elektronikus (tehát papírmentes) szerződéskötésnek, amikor az ügyfelek egy tablet képernyőfelületén az aláíráshoz egy biometrikus azonosítókat is rögzítő tollat használnak. A biometrikus aláírás során ilyen esetben keletkező és rögzített azonosítók (sebesség, gyorsulás, nyomáserősség) a Rendelet fent hivatkozott rendelkezésének alkalmazásában biometrikus azonosítónak minősülnek és különleges adatként vehetők fel, tárolhatók, kezelhetők, rendelhetők hozzá konkrét természetes személyhez stb.

8. Az adatkezelés jogalapja

8.1 Az adatkezelőkről és az adatfeldolgozókról a 15. pontban adunk tájékoztatást, azonban a továbbiak értelmezése céljából érdemes előre megjegyezni, hogy a biztosítók és biztosításközvetítők adatkezelési tevékenységük jellege alapján *adatkezelők* és *adatfeldolgozók* egyaránt lehetnek.

8.2 Az adatkezelés jogalapját illetően lényeges eltérés a jelenlegi szabályozáshoz képest a biztosítók és biztosításközvetítők számára is az, hogy a Rendelet alapján nem a hozzájárulás az egyetlen lehetséges jogalapja a személyes adatok kezelésének.

8.3 A Rendelet **6. cikk (1) bekezdése** alapján – biztosítók és biztosításközvetítők számára is - az alábbiak jelenthetnek jogalapot az adatkezeléshez:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez (**hozzájáruláson alapuló adatkezelés**),

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az adatkezelés már a szerződés megkötését megelőzően is szükséges, az érintett kérésére történő egyes lépések megtételéhez (**szerződésen alapuló adatkezelés**),

c) az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez** szükséges,

d) 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 a személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek (**jogos érdeken alapuló adatkezelés**).

9. Adatkezelés az érintett hozzájárulásával

9.1 A hozzájárulás csak bizonyos esetekben kötelező, ilyen esetek lehetnek pl. a különleges adatok kezelése, adatok továbbítása harmadik országba, stb.

9.2 Amennyiben az adatkezelés hozzájáruláson alapul, a hozzájárulásnak **(i)** önkéntesnek, **(ii)** konkrétnak, **(iii)** megfelelő tájékoztatáson alapulónak és **(iv)** egyértelműnek kell lennie. Az érintettnek a hozzájárulást nyilatkozattal vagy a megerősítést félreérthetetlenül kifejező cselekedettel kell megadnia.

9.3 A fentiek szerinti hozzájárulás lehet írásbeli, de hozzájárulásnak minősül az elektronikus úton tett hozzájárulás is, lényeges az, hogy a hozzájárulásnak tevőlegesnek kell lennie, így egy online felületen előre bejelölt check-box vagy a nem cselekvés nem minősül hozzájárulásnak.

9.4 A személyes adatok kezeléséhez való hozzájárulásnak *egyértelműnek*, míg a különleges adatokhoz való hozzájárulásnak *kifejezettnek* kell lennie.

9.5 Fontos szabály, hogy az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett hozzájárult személyes adatainak kezeléséhez.

9.6 A hozzájárulás írásban vagy a nélkül bármikor visszavonható. A visszavonás természetesen nem érinti a visszavonás előtti adatkezelés jogszerűségét. Az érintettet – egyebek mellett – a visszavonás jogáról is tájékoztatni kell.

9.7 A Rendelet a gyermekek hozzájárulását csak az információs társadalommal összefüggő (online) szolgáltatások esetén szabályozza. Online szolgáltatások esetén a gyermek hozzájárulása akkor jogszerű, ha a gyermek a 16. életévét betöltötte, egyebekben pedig akkor, ha az adatkezeléshez való hozzájárulást a szülői felügyeletet gyakorló szülő adta meg.

10. Adatkezelés hozzájárulás nélkül

10.1 Amennyiben a hozzájárulás beszerzése nem kötelező, biztosítók és biztosításközvetítők esetében a személyes adatok kezelésének jogalapja szerződésen, jogi kötelezettség teljesítésén vagy jogos érdeken alapuló adatkezelés lehet.

10.2 Az adatkezelés jogalapja, azaz jogszerűsége tekintetében a Rendelet úgy rendelkezik, hogy a tagállamok fenntarthatnak vagy bevezethetnek konkrétabb rendelkezéseket, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, így meghatározhatják az érintetteket, az adatok típusát, azokat a jogalanyokat, akikkel az adatok közölhetők, stb.

11. Az adatgyűjtés céljától eltérő célból végzett adatkezelés

11.1 Ha az adatkezelés céljától eltérő célból történő adatkezelés nem az érintett hozzájárulásán alapul, úgy az eltérő célú adatkezelés akkor jogszerű, ha az összeegyeztethető azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték. Ennek megállapításához az adatkezelő figyelembe veszi:

a) az eredeti cél és a további adatkezelés célja közötti kapcsolatot,

b) az adatkezelő és az érintett közötti kapcsolat esetén az érintett esetleges elvárását a további adatkezeléssel kapcsolatban,

c) a további adatkezelés hatását az érintettekre,

d) a megfelelő garanciák meglétét.

11.2 Amennyiben az eltérő célú adatkezelés nem összeegyeztethető ez eredeti céllal, úgy az adatkezelő köteles biztosítani, hogy az adatkezelés jogalapja a továbbiakban is megalapozott legyen, és az érintettet a további adatkezelés jogalapjáról és céljáról tájékoztatni köteles.

12. Az érintettek megerősített jogai

12.1 Az előzetes tájékoztatás

12.1.1 Az adatkezelés megkezdése előtti tájékoztatási kötelezettség köre kibővült. Az adatkezelőnek részletes információkat kell nyújtania az érintettek számára a következőkről:

a) az adatkezelő, és ha van ilyen, képviselőjének kiléte és elérhetőségei,

b) az adatvédelmi tisztviselő elérhetőségei,

c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja,

d) jogos érdeken alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekei,

e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,

f) adott esetben annak ténye, hogy az adatkezelő harmadik országba kívánja továbbítani a személyes adatokat (ez esetben a Bizottság megfelelőségi határozatának létéről vagy annak hiányáról, illetve a megfelelő garanciákról is tájékoztatást kell adni),

g) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai; ilyen időtartam lehet pl. a biztosítási szerződés tartama, stb.,

h) az érintett egyes jogainak érvényesítése, ideértve a hozzájárulás visszavonásának jogát is,

i) a felügyeleti hatósághoz címzett panasz benyújtásának joga,

j) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,

k) az automatizált döntéshozatalról, ideértve a profilalkotást is, illetve az alkalmazott logikáról és arról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír,

l) ha a személyes adatokat nem az érintettől gyűjtik, az adat forrásáról.

12.1.2 Az adatkezelőknek mindenképpen szükséges áttekinteniük, hogy jelenleg megadják-e az érintetteknek mindezen információkat, ha nem, tájékoztatási kötelezettségüket meg kell feleltetni a fenti rendelkezéseknek.

12.1.3 A tájékoztatást az adatkezelés megkezdésekor kell megadni, amennyiben az adatokat nem az érintettektől gyűjtik, a tájékoztatás megadása a Rendeletben szabályozott későbbi időpontban történik.

12.1.4 Amennyiben az adatokat nem az érintettől gyűjtik, és az információk rendelkezésre bocsátása lehetetlen, vagy aránytalanul nagy erőfeszítést igényel, úgy az adatkezelő az információkat nyilvánosan elérhető formában is rendelkezésre bocsáthatja.

12.2 Az érintett hozzáférési joga

12.2.1 Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arról, hogy adatainak kezelése folyamatban van-e, és ha igen, a személyes adatokhoz és a Rendeletben meghatározott információkhoz hozzáférést kapjon.

12.2.2 A tájékoztatás akár papír alapon, akár elektronikus úton is megtehető.

12.3 Az érintett helyesbítéshez, törléshez („elfeledtetéshez”) és korlátozáshoz való joga

12.3.1 Az érintett jogosult arra, hogy kérje adatainak helyesbítését, amennyiben azok pontatlanok, illetve kiegészítését, amennyiben azok

hiányosak, a Rendeletben meghatározott okokból való törlését vagy korlátozását.

12.3.2 Az érintett jogosult arra, hogy kérésére az adatkezelő törölje a rá vonatkozó személyes adatot, amennyiben a Rendeletben meghatározott indokok valamelyike fennáll.

12.3.4 A törlésre irányuló kérelem esetén az adatkezelő az érintett törlési kérelme ellenére is kezelheti a személyes adatokat, amennyiben erre más érvényes jogalappal bír. Az ügyfelek törlési kérelme gyakran kollízióba kerül a **Bit. 142. § (3)** bekezdésének azon rendelkezésével, mely alapján a biztosító a személyes adatokat a biztosítási jogviszony fennállásának idején, valamint azon időtartam alatt kezelheti, ameddig a biztosítási jogviszonnyal kapcsolatban (vele szemben vagy általa) igény érvényesíthető. Miután a személyes adat törlése alatt az adat oly módon történő felismerhetetlenné tételét kell érteni, hogy az adat helyreállítása többé ne legyen lehetséges, és ennek során a számítógépes adathordozón levő adatokat helyreállíthatatlanul le kell törölni, a papír alapú, személyes adatokat tartalmazó listákat pedig ellenőrzötten meg kell semmisíteni, ezért az ügyfelek által kért törlés helyett sokszor csak zárolják az adatokat, arra való hivatkozással, hogy azok nem törölhetők mindaddig, amíg az elévülési időn belül pl. egy felmondott biztosítási szerződés alapján igény érvényesíthető.

12.3.5 Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, amennyiben a Rendeletben meghatározott indokok valamelyike fennáll.

12.4 Az érintett adathordozhatósághoz való joga

12.4.1 A hozzájáruláson alapuló adatkezelés esetén az érintett jogosult arra, hogy a rá vonatkozó személyes adatokat az adatkezelőtől megkapja, illetve ezeket az adatokat egy másik adatkezelőnek továbbítsa, vagy kérje a személyes adatok adatkezelők közötti továbbítását.

12.5 Az érintett tiltakozáshoz való joga

12.5.1 A jogos érdeken alapuló adatkezelés esetén az érintett jogosult arra, hogy tiltakozzon személyes adatainak kezelése ellen, ideértve a profilalkotást is. Ilyen esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja az érintett érdekeit meghaladó kényszerítő erejű jogos érdekét vagy azt, hogy jogos érdeke jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

12.5.2 A tiltakozási jog az üzletszerzési célú adatkezelés esetén is megilleti az érintettet, ideértve a profilalkotást is. Tiltakozás esetén a személyes adatok a továbbiakban nem kezelhetők.

12.6 Automatizált döntéshozatal - Profilalkotás

12.6.1 A Rendelet bevezeti a profilalkotás fogalmát, amely a személyes adatok automatizált kezelésének olyan formája, amelynek során a személyes adatokat a személyhez fűződő személyes jellemzők értékelésére, így pl. munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, tranzakciós szokásokhoz, érdeklődési körhöz stb. kapcsolódó jellemzők elemzésére használják.

12.6.2 Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan automatizált adatkezelésen, ideértve a profilalkotást is, alapuló döntés hatálya, amely rá nézve joghatással járna.

12.6.3 Az érintett az automatizált adatkezelésen alapuló döntés hatálya alóli mentesülésre nem jogosult, ha a döntés:

a) közte és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges,

b) a döntés meghozatalát tagállami vagy uniós jog teszi lehetővé, vagy

c) az érintett kifejezett hozzájárulásán alapul.

12.7 Az adatkezelő kötelezettsége az érintett jogainak gyakorlása esetén

12.7.1 Az adatkezelő indokolatlan késedelem nélkül, de mindenképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a 12.2-12.6 pontban meghatározott kérelmek nyomán hozott intézkedésekről.

12.7.2 Szükség esetén a határidő további két hónappal meghosszabbítható, ez esetben az adatkezelő a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

12.7.3 Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme alapján, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy

hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

13. Korlátozások

13.1 A tagállami vagy uniós jog a 12. pontban meghatározott jogokat és kötelezettségeket meghatározott érdekek figyelembevételével korlátozhatja. Ilyen érdekek lehetnek pl. nemzetbiztonsággal, honvédelemmel, közbiztonsággal, bűncselekmények megelőzésével, stb. összefüggő érdekek.

14. Az adatkezelési tevékenységek nyilvántartása

14.1 A jelenlegi rendszer, mely szerint az adatkezelést nyilvántartásba kell vetetni az adatvédelmi hatóságnál, *megszűnik*, azonban mind az adatkezelők, mind az adatfeldolgozók továbbra is kötelesek a Rendelet szerinti tartalommal belső nyilvántartás létrehozására; kivételt képeznek ez alól a 250 főnél kevesebb személyt foglalkoztató vállalkozások, kivéve, ha kockázatos adatfeldolgozást végeznek, vagy különleges adatot kezelnek. A nyilvántartást megkeresés esetén a felügyeleti hatóság rendelkezésére kell bocsátani.

15. Adatkezelők és adatfeldolgozók

15.1 A Rendelet, az Adatvédelmi Irányelvhez hasonló szabályozással, megtartja az adatkezelő és az adatfeldolgozó közötti megkülönböztetést.

15.2 Az *adatkezelő* az a természetes vagy jogi személy, aki vagy amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza, míg az *adatfeldolgozó* az a természetes vagy jogi személy, aki vagy amely az adatkezelő nevében személyes adatokat kezel.

15.3 Közös adatkezelőknek minősülnek az adatkezelők akkor, ha az adatkezelés céljait és eszközeit közösen határozzák meg. A közös adatkezelők a közöttük létrejött megállapodásban határozzák meg az érintettekkel szembeni felelősségük megoszlását, az érintettekkel szembeni szerepüket és a velük való kapcsolatukat. A megállapodás lényegét az érintettek rendelkezésére kell bocsátani.

15.4 A Rendelet meghatározza az adatkezelők és az adatfeldolgozók közötti szerződések kötelező tartalmi elemeit.

15.5 Kiemelendő továbbá, hogy a Rendelet bevezeti az adatkezelők és az adatfeldolgozók egyetemleges felelősségét; ami azt jelenti, hogy az érintettek a Rendelet rendelkezéseinek megsértése miatt kártérítést követelhetnek bármelyikükkel szemben.

15.6 Az adatkezelők és az adatfeldolgozók közötti szerződés szigorúbb tartalmi követelményei, valamint egyetemleges felelősségük miatt szükséges lesz **(i)** a közöttük létrejött és 2018. után is hatályos szerződések felülvizsgálata és a Rendeletnek való megfeleltetése; továbbá szükséges lesz **(ii)** a felelősség viselésének, megosztásának és a panaszok kezelésének szerződésben való szabályozása is.

16. Az adatkezelés biztonsága, az adatvédelmi incidens bejelentése

16.1 Az adatkezelők és az adatfeldolgozók kötelesek megfelelő technikai és szervezési intézkedések megtételére annak érdekében, hogy megfelelő adatbiztonságot garantáljanak és elkerüljék az *adatvédelmi incidens* bekövetkezését.

16.2 A Rendelet **4. cikk 12. pontja** alapján az adatvédelmi incidens: *„(...) a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”*.

16.3 Az adatkezelők az adatvédelmi incidensről belső nyilvántartást vezetnek, továbbá azt a tudomásszerzéstől számított 72 órán belül kötelesek bejelenteni a felügyeleti hatóságnak, az adatfeldolgozók pedig indokolatlan késedelem nélkül kötelesek bejelenteni az adatkezelőnek.

16.4 Az adatkezelő az érintetteket is köteles tájékoztatni az incidensről, amennyiben az valószínűsíthetően magas kockázattal jár rájuk nézve. Nem kell az érintetteket tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi

intézkedéseket hajtott végre, vagy ha az incidenst követően olyan intézkedéseket tett, amelyek alapján az érintettekre kockázatot nem jelent, vagy a tájékoztatás aránytalan erőfeszítéssel járna.

17. Adatvédelmi hatásvizsgálat

17.1 Új kötelezettség a Rendelet alapján az adatvédelmi hatásvizsgálat. Ezt abban az esetben kell előzetesen lefolytatni, ha az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

17.2 Adatvédelmi hatásvizsgálatot kell végezni különösen az alábbi esetekben:

a) a természetes személyekre vonatkozó egyes jellemzők automatizált adatkezelésen alapuló értékelése (pl. profilalkotás),

b) különleges adatok, vagy bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése, stb.

17.3 Az adatvédelmi hatóság összeállítja és nyilvánosságra hozza az olyan adatkezelési műveletek jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni, és összeállíthatja és nyilvánosságra hozhatja az olyan adatkezelési műveletek típusainak a jegyzékét is, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

17.4 Ha a hatásvizsgálat eredményeként az adatkezelési művelet olyan magas kockázattal jár, amelyet az adatkezelő nem képes mérsékelni, az adatkezelést megelőzően konzultálni kell az adatvédelmi hatósággal.

18. Adatvédelmi tisztviselő

18.1 A Rendelet az adatkezelő és az adatfeldolgozó számára adatvédelmi tisztviselő kijelölését teszi kötelezővé az alábbi esetekben:

a) az adatkezelést közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv végzi,

b) az adatkezelő vagy az adatfeldolgozó fő tevékenysége olyan adatkezelési műveleteket foglal magába, amely az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé,

c) az adatkezelő vagy az adatfeldolgozó fő tevékenysége a személyes adatok különleges kategóriáinak nagy számban történő kezelését foglalja magában.

18.2 Biztosításközvetítők esetében a fenti b)-c) pontok alapján adott esetben kötelező lehet az adatvédelmi tisztviselő kijelölése.

18.3 Egy vállalkozáscsoport *közös adatvédelmi tisztviselőt* is kijelölhet. Az adatvédelmi tisztviselő akár munkaviszonyban, akár megbízási jogviszonyban foglalkoztatható. A Rendelet részletesen meghatározza az adatvédelmi tisztviselő jogállását és feladatait.

19. Magatartási kódexek, tanúsítás

19.1 Újdonság, hogy az adatkezelőket vagy adatfeldolgozókat képviselő egyesületek vagy egyéb szervezetek magatartási kódexeket dolgozhatnak ki, amelyeket jóváhagyás céljából benyújtanak a felügyeleti hatóságnak.

19.2 Ha a magatartási kódex tervezete több tagállamot érintő adatkezelési tevékenységre vonatkozik, azt az Európai Adatvédelmi Testület véleményezi, és hagyja jóvá.

19.3 A kódex rendelkezéseinek betartását az illetékes felügyeleti hatóság által akkreditált szervezet ellenőrzi.

19.4 Az adatvédelmi rendelkezések megtartását adatvédelmi tanúsítással vagy un. adatvédelmi bélyegzővel is igazolni lehet. A tanúsítványt a Rendeletben meghatározott tanúsító szervezetek vagy az illetékes felügyeleti hatóságok állítják ki.

20. Személyes adatok továbbítása harmadik országba

20.1 A Rendelet fenntartja a harmadik országba való adattovábbítás általános tilalmát.

20.2 A tilalom nem áll fenn abban az esetben, ha a Bizottság megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít.

20.3 A Bizottság által az Adatvédelmi Irányelv alapján megállapított megfelelő védelmi szintet biztosító országokba az adattovábbítás a továbbiakban is jogszerű.

20.4 A Bizottság ezen országok listáját az Európai Unió Hivatalos Lapjában és annak honlapján közzéteszi.

20.5 Megfelelőségi határozat hiányában az adatkezelő, vagy az adatfeldolgozó egyéb más garanciák esetén továbbíthat adatot harmadik országba. Az adatvédelmi hatóság külön engedélye nélkül az alábbi garanciák megfelelők:

a) kötelező erejű vállalati szabályok (binding corporate rules – BCR),

b) a Bizottság által elfogadott általános adatvédelmi kikötések (standard data protection clauses),

c) egy adatvédelmi hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések (standard data protection clauses),

d) jóváhagyott magatartási kódex (approved code of conduct), vagy

e) jóváhagyott tanúsítási mechanizmus (approved certification mechanism).

20.6 Az adatvédelmi hatóság külön engedélyével megfelelő garancia lehet az adatkezelő vagy az adatfeldolgozó és a harmadik országbeli adatfeldolgozó között létrejött szerződéses rendelkezések (contractual clauses).

20.7 A Rendelet részletesen szabályozza a kötelező erejű vállalati szabályok tartalmát és jóváhagyásának rendjét.

20.8 Bizonyos esetekben megfelelőségi határozat vagy megfelelő garanciák hiányában is továbbítható az adat harmadik országba, ilyen esetek pl. az érintett kifejezett hozzájárulása, ha az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez szükséges, stb.

21. One-stop-shop mechanizmus

21.1 A Rendelet forradalmasítani kívánja az adatvédelmi jogszabályok érvényesítését, amennyiben úgy rendelkezik, hogy az adatkezelő vagy az adatfeldolgozó vállalkozások fő felügyeleti hatósága a vállalkozás tevékenységének központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság. A fő felügyeleti hatóság jogosult eljárni az adatkezelő vagy adatfeldolgozó által végzett *határokon átnyúló adatkezelés* tekintetében.

21.2 Az egyes tagállamok felügyeleti hatóságai a hozzájuk benyújtott panaszokról tájékoztatják a fő felügyeleti hatóságot, amely ezt követően dönt arról, hogy eljár-e az ügyben. Ha a fő felügyeleti hatóság eljár az ügyben, úgy köteles együttműködni a többi érintett felügyeleti hatósággal.

21.3 A Rendelet meghatározza a fő felügyeleti hatóság és a többi felügyeleti hatóság közötti együttműködés szabályait is, továbbá arról is rendelkezik, hogy mi a megfelelő eljárás a hatóságok közötti egyet nem értés esetén. Erre és egyéb feladatokra is tekintettel létrejön az Európai Adatvédelmi Testület ("European Data Protection Board", röviden: "EDPB") melynek véleménye kötelező erővel bír majd.

21.4 Az EDPB a tagállami hatóságok egy-egy képviselőjéből áll fel és szavazati jog nélkül részt vesz majd benne az Európai Bizottság képviselője.

22. Fokozott kikényszeríthetőség, kártérítés és bírság

22.1 A Rendelet rendelkezéseinek megsértésével az adatkezelő vagy az adatfeldolgozó által okozott vagyoni és nem vagyoni károkért az érintettek kártérítésre lesznek jogosultak.

22.2 Az adatfeldolgozók csak azokért a károkért és sérelemért felelnek, amelyek a Rendelet rájuk vonatkozó rendelkezéseinek megsértéséből adódtak, vagy amennyiben az adatkezelők jogszerű utasításaitól eltérő magatartást tanúsítanak.

22.3 A bizonyítási teher az adatkezelőkön és adatfeldolgozókon lesz, így nekik kell majd bizonyítaniuk, hogy nem felelősek azért az eseményért, amely a kárhoz vagy a sérelemhez vezetett.

22.4 Abban az esetben, ha több adatkezelő vagy több adatfeldolgozó, vagy mind az adatkezelő, mind az adatfeldolgozó érintett az adatkezelésben, és bármelyikük felelős a károkozásért, úgy minden adatkezelő vagy adatfeldolgozó a kár egész összegével felel az érintett felé azzal, hogy a többi adatkezelővel, illetve adatfeldolgozóval szemben megtérítési igénnyel léphet fel.

22.5 A Rendelet rendelkezéseinek betartásáért a tagállamok felügyeleti hatóságai felelnek, akik e célból együttműködnek egymással és a Bizottsággal.

22.6 A felügyeleti hatóságok vizsgálati és korrekciós hatásköre rendkívül széles, súlyos esetben átmenetileg vagy akár végleg is *korlátozhatják* az adatkezelést, sőt elrendelhetik annak *megtiltását* is.

22.7 A felügyeleti hatóságok egyéb intézkedések mellett vagy azok helyett *bírság* kiszabására is jogosultak, amelynek mértéke alapvetően attól függ, hogy a Rendelet mely rendelkezését sértették meg. A mérlegelés során a súlyosító és enyhítő körülményeket is figyelembe veszik majd. A maximálisan kiszabható bírság összege **20 Mio EUR**, illetve a vállalkozás előző évi globális árbevételének a **4%**-a, amennyiben az magasabb összeg.

22.8 A Rendelet több, de nem alapvető fontosságú rendelkezésének megsértése esetén a bírság maximálisan kiszabható összege **10 Mio EUR**, illetve a vállalkozás előző évi globális árbevételének a **2%**-a, amennyiben az magasabb összeg.

Amennyiben a hírlevelekben bemutatott témák bármelyikéről további információkat szeretne kapni, szíveskedjen a megadott elérhetőségek valamelyikén közvetlenül kapcsolatba lépni kollégánkkal.

Dr. Molnár István
Partner, ügyvéd
T: +36 1 288 0839
F: +36 1 270 3379
E: istvan.molnar@berkemolnarlawfirm.hu
W: www.InsuranceBlog.hu

1024 Budapest
Ady Endre utca 19.
T: +36 1 288 0839
F: +36 1 270 3379
E: office@berkemolnarlawfirm.hu
W: www.InsuranceBlog.hu