PRO PUBLICO BONO – Magyar Közigazgatás, 2025/2., 75–95. • DOI: 10.32575/ppb.2025.2.4

Tóth András

AZ ADATMEGOSZTÁS EURÓPAI SZABÁLYOZÁSÁNAK ÁTTEKINTÉSE, KÜLÖNÖS TEKINTETTEL AZ ADATRENDELETRE

An Overview of European Data Sharing Regulation, with a Particular Focus on the Data Act

Tóth András habilitált egyetemi docens, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, toth.andras@kre.hu

Az Európai Unió adatmegosztási szabályozása jelentős fejlődésen ment keresztül az elmúlt években, reagálva a digitális gazdaság kihívásaira és lehetőségeire. A tanulmány átfogó áttekintést nyújt az adatmegosztás európai jogi keretrendszeréről, különös hangsúlyt fektetve a nemrég elfogadott Adatrendeletre (Data Act). A cikk részletesen bemutatja a kormányzat és üzleti szféra közötti (G2B), a vállalkozások közötti (B2B), valamint a vállalkozások és kormányzat közötti (B2G) adatmegosztás szabályozását. Az Adatrendelet főbb pontjainak elemzése során kitér az adathozzáférés különböző szintjeire, a tisztességtelen szerződési feltételek tilalmára, valamint a nem személyes adatok jogellenes nemzetközi hozzáférésének megakadályozására irányuló intézkedésekre. A tanulmány rávilágít az adatmegosztás kulcsfontosságú szerepére az európai adatgazdaság fejlesztésében és versenyképességének növelésében. Emellett kritikai elemzést nyújt az egyes szabályozások közötti különbségekről és összefüggésekről, kiemelve azok potenciális hatásait az innovációra és a piaci versenyre. A cikk végül reflektál az adatvédelem és az adatmegosztás közötti egyensúly megteremtésének kihívásaira, valamint az EU globális digitális pozíciójának erősítésére irányuló törekvésekre.

Kulcsszavak:
adatmegosztás, adatrendelet, adatvédelmi jog, digitális jog, EU-szabályozás

The data sharing regulation of the European Union has evolved significantly in recent years in response to the challenges and opportunities of the digital economy. The paper provides a comprehensive overview of the European legal framework for data sharing, with a particular focus on the recently adopted Data Act. The paper describes in detail the regulation of government-to-business (G2B), business-to-business (B2B) and business-to-government (B2G) data sharing. The main points of the Data Act are analysed, including the different levels of data access, the prohibition of unfair contract

terms and measures to prevent unlawful international access to non-personal data. The study highlights the key role of data sharing in developing the European data economy and increasing its competitiveness. It also provides a critical analysis of the differences and interdependencies between different regulations, highlighting their potential impact on innovation and market competition. Finally, the article reflects on the challenges of striking a balance between data protection and data sharing, and on efforts to strengthen the EU's global digital position.

Keywords:
data sharing, Data Act, data protection law, digital law, EU regulation

BEVEZETÉS

Az adatvezérelt gazdaság a digitális átalakulás motorja.[1] Az Európai Unió fókuszában az adatok kapcsán sokáig az adatvédelem állt. Az elmúlt években a hangsúly az adatgazdaság és az adatmegosztás megkönnyítésére helyeződött át. Már a GDPR-ban is cél volt az adatmegosztás és az interoperabilitás megkönnyítése, de az adathordozhatósági jog például továbbfinomításra szorult már a Digital Markets Act-ben (DMA) is. Az Európai Unió a 2020-as Adatstratégiában célul tűzte ki az adatok szabad áramlásának biztosítását. Jelen tanulmányban elsőként az adatmegosztás európai szabályozását tekintjük át, aztán pedig az adatgazdaság kiemelkedő európai szabályozását: az Adatrendeletet.

AZ ADATMEGOSZTÁS EURÓPAI SZABÁLYOZÁSÁNAK ÁTTEKINTÉSE

A személyes adatok gyűjtése a személyre szabott szolgáltatásnyújtás kulcsává vált. Az Európai Unió szerint a jövő adatainak nagy része ipari és szakmai alkalmazásokból, közérdekű szakterületekről vagy a dolgok internetével kapcsolatos alkalmazásokból fog származni, aminek érdekében egyensúlyt kell teremteni az adatok áramlása és széles körű felhasználása, illetve a magánéletre, a védelemre, a biztonságra és az etikai kérdésekre vonatkozó magas szintű normák megőrzése között.[2] Ehhez képest az ipari adatok 80%-a felhasználatlan marad.[3] Emiatt a Nyílt adat irányelv,[4] a DGA[5] és az Adatrendelet[6] biztosítják az adatok újrafelhasználását. Az Európai Bizottság szerint az adatcsere olyan makrogazdasági előnyökhöz vezethet, amelyek összege az európai GDP 1–2,5%-át teszik ki.[7]

1 Carugati 2023: 189.
2 Európai Bizottság 2020 (a továbbiakban: Európai Adatstratégia).
3 European Commission 2020b (a továbbiakban: Adatrendelet Hatáselemzés).
4 Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) (Nyílt adat irányelv).
5 Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) (Adatkormányzási rendelet).
6 Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) (Adatrendelet).
7 European Commission 2020b.

Az adatok úgynevezett nem versenyző javak, vagyis ugyanazt az adatot párhuzamosan többen is felhasználhatják, anélkül, hogy annak értéke csökkenne.[8] Mivel az adatok gazdasági értéke így megsokszorozható az adatok megosztásával, az adatmegosztás alapvető előfeltétele az adatok gazdasági és társadalmi értéke teljes körű kiaknázásának.[9] Jelenleg az adatkezelésnek jelentős hányada még központosított számítógépes rendszerek által történik, de ez 2025-re úgy változik, hogy ez a 80% már szétszórt dolgok közti kapcsolatból (IoT) áll össze, mint például repülők, szélfarmok vagy közúti, vasúti szállítási eszközök által továbbított adatok.[10] A Bizottság szerint az ilyen ipari, továbbá közszféra által előállított adatok meghatározóak lesznek a jövőben.

Fogalmi keretek

A DGA szerint az adatmegosztás: adatszolgáltatás egy adatfelhasználó számára önkéntes megállapodások vagy az uniós vagy nemzeti jog alapján, közvetlenül vagy közvetítőn keresztül, például – kedvezményes díjért vagy díjmentesen – nyílt felhasználási vagy kereskedelmi engedélyek alapján. Ez a meghatározás mind a személyes, mind a nem személyes adatokat lefedi azzal, hogy a személyes adatok megosztására a GDPR[11] vonatkozik, és be kell szerezni a jogosult hozzájárulását. Mivel az EU-jogban az adat kapcsán nincs kizárólagos jog (nem versenyző jószágként),[12] ezért nem átruházásról beszél a DGA, hanem továbbhasznosítási célú szolgáltatásról (hozzáférés, megosztás).[13] Az adatmegosztás lehet ingyenes (például közhivatalok esetében, ahol ez főszabály), de az ellenérték sem jelent feltétlenül pénzbeli ellenszolgáltatást, lehet kölcsönösen létrehozott adatpool. Az adatmegosztás lehet önkéntes, de alapulhat jogi előíráson is, mint például az Adatrendelet azon előírása, amely veszélyhelyzet esetére kötelező B2G adatmegosztást ír elő a pandémia tapasztalatai alapján.[14] Vannak szektorspecifikus kötelező adatmegosztási előírások is az EU-jogban.[15] Az adatmegosztás lehet magánszereplők közötti (B2B), közszféra és magánszféra közti (G2B), valamint magán- és közszféra közti (B2G).

Az adathordozás[16] bár felhasználói jog, egyfajta B2B adatmegosztásként is értelmezhető.[17] Ennél persze erősebb a kötelező adatmegosztás, amely már nem azon múlik, hogy a felhasználó

8 OECD 2015.

9 Von Ditfurth – Lienemann 2022: 272.

10 Európai Adatstratégia.

11 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (Általános Adatvédelmi Rendelet: GDPR).

12 Amely esetében a használat nem csökkenti a jószág értékét.

13 Botta 2023: 11.

14 Adatrendelet 14–15. cikk.

15 Lásd az Európai Parlament és a Tanács 1907/2006/EK rendelete (2006. december 18.); Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) 36. cikk; Az Európai Parlament és a Tanács (EU) 2018/858 rendelete (2018. május 30.) 61. cikk; Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) 23. cikk; Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) 112. cikk; Az Európai Parlament és a Tanács 2008/6/EK irányelve (2008. február 20.) 11a. cikk.

16 Lásd GDPR 20. cikk.

17 Botta 2023: 11.

él-e a jogával. A GDPR 20. cikkében foglalt vonatkozó jog csak akkor alkalmazandó, ha a személyes adatok kezelése hozzájárulás vagy szerződés alapján történik, és azokat különböző adatkezelők között továbbítják. A GDPR szerinti adathordozhatósághoz való jog gyakorlása azonban csak szerződés teljesítése céljából vagy hozzájárulás alapján feldolgozott személyes adatokra korlátozódik. Ez kizárja a jogos érdekek alapján történő adatkezelést,[18] és nem vonatkozik a nem személyes adatokra. Gyakorlati korlát, hogy nem a digitális ökoszisztémákban való valós idejű adatfelhasználás lehetővé tételére, hanem gyakran a múltbeli adatok másolataira korlátozódik.[19]

A GDPR 20. cikkéhez hasonló felhasználói (ingyenes) adathordozási jogot tartalmaz a nem személyes adatok tekintetében az Adatrendelet.[20] Az Adatrendelet további korlátozásokat is tartalmaz:

- a címzett (a felhasználó kérelme nyomán adatokat fogadó harmadik fél) az adatokat tovább nem oszthatja meg harmadik féllel,[21] és nem használhatja fel a kapott adatokat olyan termékek fejlesztésére, amelyek versenyeznek az adatbirtokos termékeivel;[22]
- a DMA[23] hatálya alá tartozó kapuőr nem tekinthető jogosult adatátvevőnek;[24]
- a kis- és középvállalkozásnak (kkv-nak) minősülő birtokosok viszont nem kötelesek adatokat megosztani harmadik felekkel, de adatcímzettnek minősülhetnek.[25]

Különbség a GDPR és az Adatrendelet szerinti adathordozás között, hogy előbbi jogként természetesen ingyenes, kivéve, ha a GDPR 12. cikk (5) bekezdése alapján az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, mert ebben az esetben az adatkezelő észszerű összegű díjat számíthat fel. Az Adatrendelet alapján a felhasználó kérésére a harmadik féllel történő adatmegosztás már tisztességes, észszerű, diszkriminációmentes (FRAND) díjon történhet.[26] Az ellenszolgáltatás egyébként hozzájárulhat ahhoz, hogy az adatok megosztásra előkészítettsége magasabb minőségű legyen.[27] Ha azonban a megosztás kedvezményezettje kkv, az adatmegosztásért járó ellentételezés nem haladhatja meg az adatbirtokosnak a tranzakció lebonyolítása érdekében felmerülő közvetlen költségeit.[28]

A DMA szintén tartalmaz adathordozásra vonatkozó kötelezettséget. A DMA 6. cikk (9) bekezdése előírja, hogy a kapuőrnek a végfelhasználók és a végfelhasználók által felhatalmazott harmadik felek kérésére díjmentesen biztosítania kell számukra a végfelhasználók

[18] GDPR 6. cikk (1) bekezdés *f)* pont.
[19] Adatrendelet Hatáselemzés 16.
[20] Adatrendelet 5. cikk (1) bekezdés.
[21] Adatrendelet 6. cikk (2) bekezdés *c)* pont.
[22] Adatrendelet 6. cikk (2) bekezdés *e)* pont.
[23] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) (Digitális Piacokról Szóló Jogszabály: DMA).
[24] Adatrendelet 5. cikk (3) bekezdés.
[25] Adatrendelet 7. cikk.
[26] Adatrendelet 8. cikk (1) bekezdés.
[27] Monti–Tombal–Graef 2022.
[28] Adatrendelet 9. cikk.

által az érintett alapvető platformszolgáltatások használatával összefüggésben folytatott tevékenységük során keletkezett adatok tényleges hordozhatóságát, többek között díjmentes eszközöket biztosítva az ilyen adathordozhatóság tényleges gyakorlásához, valamint többek között az ilyen adatokhoz való folyamatos és valós idejű hozzáférés biztosításával. Ez a rendelkezés a GPDR-ral szemben mind a személyes, mind pedig a nem személyes adatokat lefedi, ráadásul folyamatos alapon, illetve az Adatrendelettel szemben előírja, hogy a kapuőrnek az ilyen adatmegosztást ingyenesen kell teljesítenie, miközben az Adatrendelet alatti adatmegosztásnak kapuőr nem lehet jogosultja.

A DCSD irányelv[29] 16. cikk (4) bekezdése alapján a szerződés megszüntetésekor a kereskedőnek tartózkodnia kell a fogyasztó által megadott vagy létrehozott bármely, a személyes adatoktól eltérő tartalom felhasználásától, és a fogyasztó kérésére számítástechnikai úton beolvasható adatformátumban ingyenesen rendelkezésre kell bocsátania az ilyen tartalmat a szerződés megszüntetését követően. A CRD irányelv[30] 5. cikk (1) bekezdés *g)* és *h)* pontja, valamint 6. cikk (1) bekezdés *r)* és *s)* pontja segíti a fogyasztókat abban, hogy előzetesen azonosítsák a függőségi helyzeteket azáltal, hogy előírják a kereskedő számára, hogy a szerződés megkötése előtt tájékoztassa a fogyasztót az áruk digitális elemekkel, digitális tartalommal és digitális szolgáltatásokkal való funkcionalitásáról, kompatibilitásáról és interoperabilitásáról. A szerződéskötés előtti tájékoztatásból fakadó ezen követelmények a szerződés szerves részét képezik a DCSD irányelv értelmében.[31] A hordozhatóságra vonatkozó GDPR 20. cikke szerinti követelmény megsértése így a digitális tartalom vagy a digitális szolgáltatás hibás teljesítését eredményezheti a DCSD irányelv rendelkezései értelmében, kivéve, ha a szerződés a nemzeti jogszabályok értelmében semmis vagy megtámadható.[32]

Mind az Adatrendelet, mind pedig a DMA folyamatos és valós idejű adatmegosztást ír elő. Az, hogy a GDPR-t ki kell egészíteni az adatáramlás előmozdítására, már a bizottsági szakértői anyagban is felmerült az adathordozhatósággal összefüggésben, hiszen az csak a múltbeli adatok hordozására kínál megoldást, de nem biztosítja a folyamatos adatmegosztást.[33]

Kötelező B2B adatmegosztások az EU-jogban

A DMA 6. cikk (8) bekezdése előírja a kapuőrnek, hogy a hirdetők és a hirdetés-közzétevők, valamint a hirdetők és a hirdetés-közzétevők által felhatalmazott harmadik felek kérésére díjmentes hozzáférést kell biztosítania számukra a teljesítménymérő eszközeihez, valamint a hirdetési portfólió független értékelésének a hirdetők és a hirdetés-közzétevők általi

[29] Az Európai Parlament és a Tanács (EU) 2019/770 irányelve (2019. május 20.).

[30] Az Európai Parlament és a Tanács 2011/83/EU irányelve (2011. október 25.) a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről (CRD: *Consumer Rights Directive*).

[31] DCSD irányelv (42) preambulumbekezdés.

[32] DCSD irányelv (48) preambulumbekezdés.

[33] Crémer – de Montjoye – Schweitzer 2019: 8.

elvégzéséhez szükséges adatokhoz, beleértve az összesített és a nem összesített adatokat is. Ennek az adatmegosztási kötelezettségnek a célja a piac átláthatóságának növelése;[34] a hirdető összehasonlíthatja a hirdetési költségeket a kapuőr által a különböző kiadóknak fizetett díjakkal.

A DMA 6. cikk (10) bekezdése szerint a kapuőrnek az üzleti felhasználók és az üzleti felhasználók által felhatalmazott harmadik felek kérésére díjmentesen tényleges, kiváló minőségű, folyamatos és valós idejű hozzáférést kell biztosítania számukra azokhoz az összesített és nem összesített adatokhoz – beleértve a személyes adatokat is –, amelyeket az említett üzleti felhasználók és az ezen üzleti felhasználók által nyújtott termékekkel és szolgáltatásokkal kapcsolatba kerülő végfelhasználók az érintett alapvető platformszolgáltatások vagy az azokkal együtt vagy az azok támogatása céljából nyújtott szolgáltatások használatával összefüggésben adnak meg vagy generálnak, valamint lehetővé kell tennie ezen adatoknak az üzleti felhasználók és az üzleti felhasználók által felhatalmazott harmadik felek általi használatát. A személyes adatokat illetően a kapuőr csak abban az esetben biztosíthat hozzáférést az adatokhoz, és csak abban az esetben teheti lehetővé azok felhasználását, ha az adatok közvetlen összefüggésben vannak az érintett üzleti felhasználó által az érintett alapvető platformszolgáltatáson keresztül kínált termékek vagy szolgáltatások végfelhasználói általi használatával, és ha a végfelhasználók a hozzájárulásuk megadásával beleegyeznek az ilyen adatmegosztásba. A DMA 6. cikk (11) bekezdése szerint a kapuőrnek az online keresőprogramokat nyújtó, harmadik félnek minősülő vállalkozások kérésére tisztességes, észszerű és megkülönböztetéstől mentes módon hozzáférést kell biztosítania számukra a kapuőr online keresőprogramjával végzett díjmentes és fizetett keresések során a végfelhasználók által generált rangsorolási, keresési, kattintási és megtekintési adatokhoz. A személyes adatnak minősülő keresési, kattintási és megtekintési adatokat anonimizálni kell.[35] Vagyis a DMA előzőekben említett kötelező adatmegosztási előírásai közül ezek a *click&query* adatok az egyetlenek, amelyek esetében a kapuőr ellenszolgáltatást követelhet, a többit egyfajta jogként ingyenesen kell biztosítania. A kötelezettség hatóköre kiterjed egyrészt az ingyenes (organikus), másrészt a szponzorált (hirdetések) keresési eredményekre is.

A G2B adatmegosztás európai szabályozása

A G2B adatmegosztást a Nyílt adat irányelv és a DGA szabályozza az Európai Unióban. A Nyílt adat irányelv a közszektorbeli szervek és közvállalkozások által birtokolt dokumentumok megosztását írja elő. Az irányelv általános elve az, hogy az állami szerveknek lehetővé kell tenniük a közfeladataik ellátása során előállított dokumentumok magánfelek általi újrafelhasználását

[34] DMA (45) preambulumbekezdés.

[35] Az adatok akkor minősülnek anonimizáltaknak, ha a személyes adatokat visszavonhatatlanul megváltoztatják oly módon, hogy az információk ne vonatkozzanak azonosított vagy azonosítható természetes személyre, továbbá, ha a személyes adatokat oly módon teszik anonimmá, hogy az érintett nem, illetve már nem azonosítható. Lásd DMA (62) preambulumbekezdés.

egyéb kereskedelmi és nem kereskedelmi célokra.[36] Amennyiben lehetséges, az érintett ágazati szervek a dokumentumokat nyílt, géppel olvasható, hozzáférhető és újrafelhasználható formátumban teszik elérhetővé.[37] A közszféra szervei általában díjmentesen osztják meg a kért dokumentumokat, de a sokszorítás, anonimizálás során felmerülő költséget megtéríttethetik.[38] A költségtáblát előzetesen közzé kell tenni.[39] A megosztott dokumentumokra kizárólagos jog nem alapítható.[40] A közpénzből finanszírozott kutatási adatokhoz (például statisztikák, mérési eredmények) is hozzáférést kell biztosítani FAIR *(findability, accessibility, interoperability and reusability)* alapon. Ez a hozzáférés-biztosítási alap előírja a megtalálhatóságot (legyenek kereshetők a kutatási eredmények egy adatbázisban) és az interoperábilis felhasználhatóságot. A közszféra szerveinek ingyenes hozzáférést kell biztosítaniuk a nagy értékű adatkészletekhez[41] (például meteorológiai adatok),[42] néhány kivételtől eltekintve, például: amelyek állami vállalkozásokkal kapcsolatosak,[43] a könyvtárak és múzeumok birtokában lévő adatkészletek,[44] és olyan esetekben, amikor az adatok nyilvánosságra hozatala jelentős hatást gyakorolna a közszférabeli szerv költségvetésére.

A Nyílt adat irányelv nem terjed ki azokra a dokumentumokra, amelyeket harmadik felek szellemi tulajdonjogai védenek (például szerzői jog), valamint a személyes adatokat tartalmazó dokumentumokra.[45] Ezt az EU szabályozása a DGA-val pótolja ki.[46] Ebből következően a DGA szerinti adatmegosztási feltételek is hasonlók a Nyílt adat irányelvben szabályozottakhoz, így a címzett nem jogosult a megosztott adatokra vonatkozó kizárólagos jogra.[47] A személyes adatokat anonimizálni kell a megosztás előtt.[48] A kompenzációt illetően azonban a Nyílt adat irányelv és a DGA már eltér. A Nyílt adat irányelv szerint a közjogi szerveknek lehetővé kell tenniük a dokumentumok ingyenes újrafelhasználását,[49] és kivételesen biztosítják a megosztással kapcsolatos költségek felszámítását. Ezzel szemben a DGA megengedi, hogy díjakat számítsanak fel az adatok további felhasználásának engedélyezéséért. A kért díjat a DGA szerint előre meg kell határozni, arányosan és objektíven indokoltan, a különböző címzettek között megkülönböztetéstől mentesen. A DGA előírja, hogy a díjat az adatok sokszorosítása, valamint az anonimizálás és az érintett hozzájárulásának kérése során felmerülő költségek alapján kell kiszámítani. A DGA alapján a közszféra szervei kedvezményes díjért vagy ingyenesen hozzáférhetővé tehetik az adatokat nem kereskedelmi célból (például tudományos kutatás) vagy kkv-k számára.

36 Nyílt adat irányelv 3. cikk (1) bekezdés.
37 Nyílt adat irányelv 5. cikk (1) bekezdés.
38 Nyílt adat irányelv 6. cikk (1) bekezdés.
39 Nyílt adat irányelv 7. cikk (1) bekezdés.
40 Nyílt adat irányelv 12. cikk (1) bekezdés.
41 Nyílt adat irányelv 14. cikk (1) bekezdés.
42 Nyílt adat irányelv I. melléklet.
43 Nyílt adat irányelv 14. cikk (3) bekezdés.
44 Nyílt adat irányelv 14. cikk (1) bekezdés.
45 DGA (6) preambulumbekezdés.
46 DGA (10) preambulumbekezdés és 3. cikk (1) bekezdés.
47 DGA 4. cikk.
48 DGA 5. cikk (3) bekezdés *a)* pont.
49 Nyílt adat irányelv 6. cikk (1) bekezdés.

Kötelező B2G adatmegosztás

A kötelező B2G adatmegosztást az Adatrendelet írja elő vészhelyzet esetére. Az Adatrendelet szerint nem személyes adatokat kell megosztani,[50] ebből fakadóan az adatbirtokosnak a személyes adatokat anonimizálnia kell.[51] Abban az esetben azonban, ha a kért adatok továbbra is tartalmaznak személyes adatot, a hatóság a kapott adatokat a GDPR követelményeinek megfelelően dolgozza fel.[52] A kötelező adatmegosztást indokoló rendkívüli igény megszűnése után a hatóságnak minden esetben törölnie kell a kapott adatokat.[53] A megkereső hatóság megoszthatja a kapott adatokat más állami szervekkel, amelyek szintén részt vesznek a rendkívüli helyzetre való reagálásban.[54] Ezzel szemben a címzett hatóság magánszemélyeknek már nem adhatja tovább az adatokat.[55] Az adatbirtokos a kért adatokat – mikro- és kisvállalkozások kivételével – térítésmentesen biztosítja.[56] Mivel a rendkívüli helyzet ritka, így az adatbirtokos üzleti tevékenységét várhatóan nem érinti negatívan az adatmegosztási kötelezettség.[57] Amennyiben azonban nem rendkívüli helyzetben, hanem meghatározott közérdekű feladat teljesítése érdekében kérték az adatmegosztást, akkor az adatbirtokos jogosult lehet kompenzációra. Ez nem haladhatja meg az adatbirtokosnál az adatmegosztási kérelmek teljesítésével kapcsolatban felmerülő technikai és szervezési költségeket, ideértve a kért adatok anonimizálásával kapcsolatban az adatbirtokost terhelő költségeket, és magába foglalhat észszerű profitot.[58]

A FRAND feltételek jelentősége az Európai Unió szabályozásában

Az Adatrendelet 8. és 9. cikke alapján az adatbirtokos a felhasználó kérésére megkülönböztetéstől mentesen és észszerű áron hozzáférhetővé teszi a termékhasználat során keletkezett nem személyes adatokat harmadik fél számára (nem személyes adatok adathordozhatósága). Az Adatrendelet 10. cikke előírja, hogy minden EU-tagállam vitarendezési testületeket hozzon létre, amelyek felügyelik annak eldöntését, hogy a FRAND-ot helyesen határozták-e meg a nem személyes adatok adathordozhatóságával kapcsolatos vitákban.

A DMA 6. cikk (11) bekezdése értelmében a kapuőr státusszal rendelkező keresőmotorok a versenytárs keresőmotorok számára FRAND alapon rangsorolási, lekérdezési, kattintási és megtekintési adatokat biztosítanak, amelyeket a végfelhasználók generálnak.

---

50 Adatrendelet 17. cikk (2) bekezdés *e)* pont.
51 Adatrendelet 18. cikk (4) bekezdés.
52 Adatrendelet 19. cikk (1) bekezdés *b)* pont.
53 Adatrendelet 19. cikk (1) bekezdés *c)* pont.
54 Adatrendelet 17. cikk (4) bekezdés.
55 Adatrendelet 17. cikk (3) bekezdés.
56 Adatrendelet 20. cikk (1) bekezdés.
57 Adatrendelet (75) preambulumbekezdés.
58 Adatrendelet 20. cikk (2) bekezdés.

AZ EURÓPAI UNIÓ ADATRENDELETE

Az Adatrendelet végleges szövegét 2023. november 27-én fogadták el.[59] Az Adatrendelet az adatok szűk körére, az internetre kapcsolt eszközök (IoT) által generált adatokra és az azokhoz való hozzáférésre vonatkozik. Az Adatrendelet a kapcsolt (online) termékek és kapcsolódó szolgáltatások körében szabályoz.

A nem személyes adatok szabad áramlásáról szóló rendelet[60] biztosítja, hogy a nem személyes adatokat az EU-n belül bárhol lehet tárolni, feldolgozni és továbbítani. Az Adatrendelet lényegében megkönnyíti a vállalkozások és a polgárok számára e jog tényleges gyakorlását.[61] Az adatokból kikövetkeztetett vagy származtatott információkat úgy kell tekinteni, mint amelyek nem tartoznak a rendelet hatálya alá, és amelyek következésképpen nem tartoznak az adatbirtokos azon kötelezettségének hatálya alá, hogy azokat a felhasználó vagy az adatátvevő számára hozzáférhetővé tegye, kivéve, ha a felhasználó és az adatbirtokos másként állapodik meg.[62]

A rendelet hatálya alá tartoznak azok az összekapcsolt termékek, amelyek alkotóelemeik révén adatokat szereznek meg, generálnak vagy gyűjtenek a teljesítményükre, használatukra vagy környezetükre vonatkozóan, és amelyek képesek ezeket az adatokat nyilvánosan elérhető elektronikus hírközlési szolgáltatáson, fizikai kapcsolat útján vagy eszközön való hozzáférésen (IoT) keresztül továbbítani.[63] Ilyen termékek lehetnek például járművek, háztartási berendezések és fogyasztási cikkek, orvostechnikai és egészségügyi eszközök, illetve mezőgazdasági és ipari gépek.[64] Az Adatrendelet a virtuális asszisztensekre is kiterjed, amennyiben azok interakciót folytatnak egy összekapcsolt termékkel vagy kapcsolódó szolgáltatással.[65] Az Adatrendelet feltöri az ügyfeleket utópiaci szolgáltatásokba záró ökoszisztémákat: például egy internetre kötött liftet a gyártótól független szerviz nem tudja megjavítani, ha nem kap valós idejű hozzáférést a lift műszaki állapotához.

Az Adatrendelet azon a felismerésen nyugszik, hogy egyes termékek és kapcsolódó szolgáltatások használata közben minimum két szereplőnek köszönhető a termék használatával generált adatok létrejötte: egyrészt a termék gyártójának (tervezőjének), másrészt az azt használó személynek (felhasználónak).[66] A felhasználók nélkül tehát az adatok létre sem jönnének, miközben bizonytalan az IoT-eszközök által generált adatok sorsának jogi helyzete, beleértve a felhasználók és az általuk megbízott harmadik felek[67] hozzáférését. Az Adatrendelet szabályozási koncepciója nem foglal állást az adatbirtokosok jogalapját illetően, és nem hoz létre új hozzáférési jogosultságokat.[68] A rendelet abból a helyzetből indul ki, amit az adattulajdonos

[59] Council of the European Union 2023.
[60] Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.).
[61] Adatrendelet Hatáselemzés 4.
[62] Adatrendelet (15) preambulumbekezdés.
[63] Adatrendelet (14) preambulumbekezdés.
[64] Adatrendelet (14) preambulumbekezdés.
[65] Adatrendelet 1. cikk (4) bekezdés.
[66] Adatrendelet (6) preambulumbekezdés.
[67] Például akkor, amikor a termékhez kapcsolódóan szükséges igénybe venniük egy utópiaci szolgáltatást (jellemzően javítást vagy karbantartást).
[68] Adatrendelet (7) preambulumbekezdés.

de facto vagy *de iure* ténylegesen élvez a termékek vagy a kapcsolódó szolgáltatások révén generált adatok felett. Ez a helyzet most legtöbb esetben kizárólagosságot eredményez az adatok terén, ami miatt mind az azt generáló felhasználók, mind pedig harmadik felek kiszorultak azok hasznosításából.[69] A Bizottság szerint az IoT-eszközök által generált adatok 80%-a így például teljesen felhasználatlan marad. Ezzel együtt biztosítani kell, hogy a hozzáférés biztosítása ne érintse hátrányosan az adatokat rendelkezésre bocsátó vállalkozások beruházási motivációit. Ennélfogva elkerülendő, hogy az adatokat olyan összekapcsolt termék kifejlesztéséhez használják fel, amelyet a felhasználók felcserélhetőnek vagy helyettesíthetőnek tekintenek, különösen az összekapcsolt termék jellemzői, ára és rendeltetése alapján.[70] Ez ugyanis nem innováció, hanem másolás. (Egyébként ez a megközelítés a versenyjogi gyakorlatban is, lásd Magill-ügy.)[71] Nincs akadálya viszont annak, hogy a felhasználó az Adatrendelet értelmében biztosított jogának gyakorlása során kapott adatokat egy olyan harmadik félnek adja át vagy adatja át az adatbirtokossal, amely az adatbirtokos által nyújtott valamely szolgáltatással esetlegesen versenyben álló utópiaci szolgáltatást kínál.[72] Biztosítani kell viszont az üzleti titok védelmét, ami így nem szolgálhat alapul a hozzáférési igény elutasításához, kivéve, ha nagy valószínűséggel súlyos gazdasági kárt eredményezne. Az adatbirtokos szintén nem köteles arra, hogy az adatok tisztítása és átalakítása terén jelentős beruházásokat eszközöljön. Az adatbirtokos kizárólagos alapon sem bocsáthat adatokat az adatátvevő rendelkezésére, kivéve, ha azt a felhasználó kéri.[73]

Az Adatrendelet hat témakörben tartalmaz szabályozást:[74]

- termékadatoknak és kapcsolódószolgáltatás-adatoknak a felhasználó számára történő rendelkezésre bocsátása;
- adatoknak az adatbirtokosok által a felhasználótól független adatátvevők számára történő rendelkezésre bocsátása;
- adatoknak az adatbirtokosok által közszférabeli szervezetek, a Bizottság, az Európai Központi Bank és uniós szervek számára történő rendelkezésre bocsátása, amennyiben rendkívüli igény van az említett adatokra egy közérdekből végzett konkrét feladat teljesítéséhez;
- az adatkezelési szolgáltatások (felhő) közötti váltás megkönnyítése;
- harmadik felek nem személyes adatokhoz való jogellenes hozzáférése elleni biztosítékok bevezetése;
- az adatokhoz való hozzáférésre, azok továbbítására és felhasználására vonatkozó interoperabilitási szabványok kidolgozása.

[69] Holm-Hadulla – Meiborg 2023.
[70] Adatrendelet (32) preambulumbekezdés.
[71] Adatrendelet (35) preambulumbekezdés.
[72] Adatrendelet (30) preambulumbekezdés.
[73] Adatrendelet 8. cikk (4) bekezdés.
[74] Adatrendelet 1. cikk (1) bekezdés.

Az Adatrendelet viszonya más EU-s szabályozásokhoz

A versenyjog csak az erőfölénnyel rendelkező, a DMA pedig csak a kapuőrnek kijelölt adattulajdonosok esetében alkalmazandó. Az adatokhoz való hozzáférés versenyjogi kikényszerítése nagyon körülményes,[75] ráadásul a szerződő felek közötti egyensúlyhiány nem a piaci struktúrából, hanem sokszor az erőfölény szintjét el nem érő egyensúlyhiányból fakad: az adatot igénylő fél, akinek szüksége van az adatokra az innovatív digitális üzleti modellek fejlesztéséhez, csak az adatbirtokostól kaphatja meg az adatokat.[76] A DMA egyébként is a kapuőrnél keletkező adatokhoz való hozzáférést nem átfogó jelleggel, hanem a versenyélénkítés szempontjából meghatározott viszonyrendszerben biztosítja. Így a DMA 6. cikk (9) bekezdés előírja a valós idejű adathordozást a kapuőrtől a végfelhasználó által választott másik szolgáltatóhoz mind a személyes, mind pedig a nem személyes adatok tekintetében, a 6. cikk (10) bekezdés biztosítja, hogy az üzleti felhasználók hozzáférjenek a saját vagy felhasználóik által a kapuőr platformján generált adatokhoz, a 6. cikk (11) bekezdése pedig a versenytárs online keresési szolgáltatóknak biztosítja a kapuőr *click&query* adataihoz való hozzáférést, hogy saját keresési szolgáltatásuk optimalizálását elvégezhessék.[77]

Amennyiben a felhasználók érintettnek minősülnek, akkor az Adatrendelet termékadatoknak és kapcsolódószolgáltatás-adatoknak a felhasználó számára történő rendelkezésre bocsátására vonatkozó szabályai kiegészítik az érintett GDPR szerinti hozzáférési jogait, illetve az adathordozhatósághoz való jogokat.[78]

A végberendezésen tárolt és onnan elért adatokhoz való hozzáférés az Európai Parlament és a Tanács 2002/58/EK irányelve hatálya alá tartozik, amelynek értelmében e hozzáférés az előfizető vagy felhasználó hozzájárulásához kötött, kivéve, ha az feltétlenül szükséges a felhasználó vagy az előfizető által kifejezetten kért, információs társadalommal összefüggő szolgáltatás nyújtásához, vagy ha annak kizárólagos célja egy közlés továbbítása.[79] A dolgok internetéhez kapcsolódó berendezés akkor minősül végberendezésnek, ha közvetlenül vagy közvetve egy nyilvános kommunikációs hálózathoz kapcsolódik.

Adatmegosztás

Az Adatrendelet az adatmegosztás három szintjét különbözteti meg, ebből kettő a felhasználóra, egy pedig az általa felkért harmadik személyre vonatkozik. A kkv-k mentesülnek az adatmegosztási kötelezettség betartásának szabályozási terhe alól.[80] Szintén a kkv-kat védi, hogy az adatbirtokosok által megkövetelt ellentételezés nem tartalmazhat árrést, ha az adatok címzettje kkv.

[75] Tóth 2021.
[76] Adatrendelet Hatáselemzés 6.
[77] Lásd DMA (61) preambulumbekezdés.
[78] Adatrendelet 1. cikk (5) bekezdés.
[79] Adatrendelet (36) preambulumbekezdés.
[80] Adatrendelet 7. cikk (1) bekezdés.

Az adatbirtokos kizárólag a felhasználóval kötött szerződés alapján használhat fel nem személyes adatnak minősülő adatokat (és bocsáthat harmadik felek rendelkezésére nem személyes termékadatokat),[81] és azokat nem használhatja fel arra, hogy olyan betekintést nyerjen a felhasználó gazdasági helyzetét, eszközeit és termelési módszereit illetően, amely alááshatja az említett felhasználó üzleti pozícióját azon piacokon, amelyeken a felhasználó aktív.[82] Van olyan vélemény, amely szerint amiatt, hogy az adatbirtokos csak a felhasználóval kötött szerződés alapján használhatja fel a nem személyes adatokat, abból az következik, hogy azok erősebb védelem alatt állnak, mint a személyes adatok.[83]

Az első felhasználói hozzáférési szint az úgynevezett *access by design* alapú hozzáférés. Ez azt jelenti, hogy az összekapcsolt termékeket úgy kell megtervezni és gyártani, a kapcsolódó szolgáltatásokat pedig úgy kell megtervezni és nyújtani, hogy a termékadatok és a kapcsolódószolgáltatás-adatok alapértelmezés szerint könnyen, biztonságosan, díjmentesen, egy átfogó, strukturált, széles körben használt és géppel olvasható formátumban, és amennyiben releváns, valamint technikailag kivitelezhető, közvetlenül legyenek hozzáférhetők a felhasználó számára.[84] Ez az *access by design* ugyanannak a szabályozási koncepciónak a megjelenése, amelyet már a GDPR 25. cikkében is láthattunk *(privacy by design)*.[85] A hozzáférést a felhasználó számára egyszerű, automatikus végrehajtást lehetővé tevő kérési mechanizmus révén kell biztosítani, anélkül, hogy a gyártónak vagy az adatbirtokosnak vizsgálnia kellene vagy jóvá kellene hagynia a kérelmet. Ez azt jelenti, hogy az adatokat csak akkor kell rendelkezésre bocsátani, ha a felhasználó ténylegesen hozzáférést akar kapni.[86] Amennyiben nem a felhasználó az érintett, hanem egy vállalkozás, akkor az ilyen felhasználó adatkezelőnek minősül, akinek adatkezelőként valamely összekapcsolt termék vagy kapcsolódó szolgáltatás felhasználása révén generált személyes adatok tekintetében a GDPR 6. cikk (1) bekezdésében előírt olyan jogalappal kell rendelkeznie, mint például az érintett hozzájárulása, vagy egy olyan szerződés teljesítése, amelyben az érintett félként vesz részt.

A felhasználóknak a termék megvásárlása során (lízinget és bérlést is ideértve) egyértelmű tájékoztatást kell nyújtani azon termékadatokra vonatkozóan, amelyeket az összekapcsolt termék generálni képes, ideértve az ilyen adatok típusát, formátumát és becsült mennyiségét. A kapcsolódó szolgáltatás nyújtására vonatkozó szerződés megkötése előtti tájékoztatási kötelezettségnek a leendő adatbirtokost kell terhelnie, függetlenül attól, hogy az adatbirtokos köt-e szerződést.[87]

Előfordul bizonyos termékek esetén, hogy azt többen is használhatják annak jellegéből adódóan. Az Adatrendelet szerint ebből kifolyólag a termékeket úgy szükséges megtervezni, hogy

[81] Adatrendelet 4. cikk (14) bekezdés.
[82] Adatrendelet 4. cikk (13) bekezdés.
[83] Szilágyi 2024.
[84] Adatrendelet 3. cikk (1) bekezdés.
[85] Holm-Hadulla – Meiborg 2023: 189.
[86] Adatrendelet (21) preambulumbekezdés.
[87] Adatrendelet (24) preambulumbekezdés.

minden azt használó személy hozzáférhessen külön-külön a saját maga által generált adatokhoz, például felhasználói fiókok létrehozásával.[88]

A második szint akkor alkalmazandó, ha a felhasználó nem tud az összekapcsolt termékből vagy a kapcsolódó szolgáltatásból közvetlenül hozzáférni az adatokhoz, ilyenkor az adatbirtokosoknak indokolatlan késedelem nélkül – az adatbirtokos rendelkezésére állóval megegyező minőségben – könnyen elérhető adatokat kell hozzáférhetővé tenniük a felhasználó számára biztonságosan, díjmentesen, egy átfogó, strukturált, széles körben használt és géppel olvasható formátumban, és – amennyiben releváns és technikailag kivitelezhető – folyamatosan és valós időben.[89] Ezt egyszerű kérelem alapján, elektronikus úton kell megtenni, amennyiben technikailag kivitelezhető. A felhasználó az ilyen kérelem alapján szerzett adatokat nem használhatja fel olyan összekapcsolt termék kifejlesztésére, amely verseng azon összekapcsolt termékkel, amelyből az adatok származnak, nem oszthatja meg az adatokat az említett szándékkal harmadik féllel, és nem használhat fel ilyen adatokat arra, hogy betekintést nyerjen a gyártó vagy – adott esetben – az adatbirtokos gazdasági helyzetébe, eszközeibe és termelési módszereibe.[90]

A felhasználók és az adatbirtokosok szerződésben korlátozhatják vagy megtilthatják az adatokhoz való hozzáférést, azok felhasználását vagy további megosztását, ha az ilyen adatkezelés alááshatná az összekapcsolt termékre vonatkozó, az uniós vagy nemzeti jogban megállapított biztonsági követelményeket, ami súlyosan hátrányos hatással járhat a természetes személyek egészségére, biztonságára vagy védelmére nézve.[91]

Üzleti titkok csak akkor őrizhetők meg és fedhetők fel, amennyiben az adatbirtokos és a felhasználó a felfedést megelőzően minden szükséges intézkedést megtett az üzleti titkok bizalmas jellegének megőrzése érdekében, különösen harmadik felek vonatkozásában.[92] Amennyiben az üzleti titok jogosultjának minősülő adatbirtokos bizonyítani tudja, hogy a felhasználó által a technikai és szervezési intézkedések ellenére nagy valószínűséggel súlyos gazdasági kárt szenved az üzleti titkok felfedése miatt, az adatbirtokos eseti alapon elutasíthatja a szóban forgó konkrét adatokhoz való hozzáférés iránti kérelmet.[93] Ilyenkor értesíteni kell az illetékes hatóságot.

A harmadik szintet az adatbirtokos arra vonatkozó kötelezettsége jelenti, hogy a felhasználó kérelmére az adatbirtokos rendelkezésére állóval megegyező minőségben és adott esetben folyamatosan és valós időben harmadik fél rendelkezésére bocsássa a termék vagy a kapcsolódó szolgáltatás használata révén generált adatokat.[94] Ez az előírás hasonlatos a GDPR 20. cikkében foglalt adathordozáshoz, de azt számos ponton kiegészíti. Egyrészt a GDPR szerinti adathordozás a hozzájárulás vagy szerződéses jogalap szerint kezelt személyes adatokra vonatkozik, ezzel szemben az Adatrendelet ilyen jogalapi megszorítást nem tartalmaz, továbbá a nem személyes adatokra is kiterjed. Másrészt, a GDPR 20. cikkétől eltérően az Adatrendelet előírja és biztosítja a harmadik felek hozzáférésének technikai megvalósíthatóságát a hatálya alá tartozó

88 Adatrendelet (21) preambulumbekezdés.
89 Adatrendelet 4. cikk (1) bekezdés.
90 Adatrendelet 4. cikk (10) bekezdés.
91 Adatrendelet 4. cikk (2) bekezdés.
92 Adatrendelet 4. cikk (6) bekezdés.
93 Adatrendelet 4. cikk (8) bekezdés.
94 Adatrendelet 5. cikk (1) bekezdés.

valamennyi adattípus esetében. Harmadrészt, az Adatrendelet lehetővé teszi továbbá az adatbirtokosok számára, hogy harmadik felek – de nem a felhasználó – által fizetendő, észszerű kompenzációt állapítsanak meg a felhasználó összekapcsolt terméke által generált adatokhoz való közvetlen hozzáférés biztosításával kapcsolatban felmerülő költségek tekintetében.[95]

Harmadik felek csak a felhasználóval megállapodott célokra kezelhetik az adatokat, és csak a felhasználónak az ilyen adatmegosztásra vonatkozó beleegyezésével oszthatják meg azokat egy másik harmadik féllel.[96] A felhasználó számára ugyanolyan könnyűnek kell lennie annak, hogy a harmadik fél adatokhoz való hozzáférését megtagadja vagy megszüntesse, mint amilyen a hozzáférés engedélyezése. A harmadik fél semmilyen módon nem kényszerítheti, vezetheti félre vagy manipulálhatja a felhasználót a hozzáférés megszerzése érdekében.[97] Harmadik fél ezenkívül:

- nem használhatja fel a kapott adatokat profilalkotásra, kivéve, ha ez a felhasználó által kért szolgáltatás nyújtásához szükséges;[98]
- a kapott adatokat nem használhatja fel olyan termék kifejlesztése céljából, amely verseng azon összekapcsolt termékkel, amelyből az elért adatok származnak;
- nem használhatja fel a rendelkezésre bocsátott, nem személyes termékadatokat vagy kapcsolódószolgáltatás-adatokat arra, hogy betekintést nyerjen az adatbirtokos gazdasági helyzetébe, eszközeibe és termelési módszereibe, vagy az adatbirtokos általi felhasználásukra vonatkozóan;[99]
- a kapott adatokat nem használhatja fel oly módon, amely hátrányosan hat az összekapcsolt termék vagy a kapcsolódó szolgáltatás biztonságára;[100]
- nem áshatja alá az üzleti titkok bizalmi jellegét;[101]
- nem akadályozhatja meg, hogy a felhasználó, aki fogyasztó is egyben, az általa kapott adatokat más felek rendelkezésére bocsássa.[102]

A DMA többek között előírja az adatok hozzájárulás nélküli kombinálásának tilalmát, amiből világos, hogy a DMA a hatálya alá tartozó kapuőrök esetében korlátozza az adatokhoz való hozzáférést. Ebből következően az Adatrendelet céljának eléréséhez nem szükséges – és ezért aránytalan is volna az ilyen kötelezettségek hatálya alá tartozó adatbirtokosokkal szemben –, hogy kapuőr is az adathozzáférési jog kedvezményezettjei közé tartozzon.[103] A DMA alapján kapuőr vállalkozások tehát nem minősülnek a rendelet szempontjából jogosult harmadik félnek, vagyis a felhasználókat nem hívhatják fel arra, hogy adatokat bocsássanak a rendelkezésükre; továbbá nem hívhatják fel a felhasználót arra, hogy az adatbirtokoshoz kérelmet intézzen, hogy ez utóbbi alapján adatokat bocsásson valamely szolgáltatásuk

95 Adatrendelet (35) preambulumbekezdés.
96 Adatrendelet (37) preambulumbekezdés.
97 Adatrendelet (38) preambulumbekezdés.
98 Adatrendelet 6. cikk (2) bekezdés *b)* pont.
99 Adatrendelet 6. cikk (2) bekezdés *e)* pont.
100 Adatrendelet 6. cikk (2) bekezdés *f)* pont.
101 Adatrendelet 6. cikk (2) bekezdés *g)* pont.
102 Adatrendelet 6. cikk (2) bekezdés *h)* pont.
103 Adatrendelet (40) preambulumbekezdés.

rendelkezésére; illetve nem kaphatnak olyan adatokat a felhasználótól, amelyekre a felhasználó kérelem alapján tett szert.[104] Ezen túl a harmadik fél a rendelkezésére bocsátott adatokat nem adhatja át a DMA szerinti kapuőrnek.[105] Amennyiben azonban a kapuőr az Adatrendelet alapján adatbirtokosnak minősül, akkor köteles az Adatrendelet megosztásra vonatkozó előírásait teljesíteni.

Tisztességtelen feltételek

Valamely vállalkozás által egy másik vállalkozásra nézve egyoldalúan megállapított, adathozzáférésre és -felhasználásra, valamint az adatokkal kapcsolatos kötelezettségek megsértése vagy felmondása esetén fennálló felelősségre és jogorvoslatokra vonatkozó szerződési feltétel nem kötelező erejű az utóbbi vállalkozásra nézve, ha a feltétel tisztességtelen.[106] Másként: az Adatrendelet 13. cikke csak akkor alkalmazható, ha a szerződéses feltételt egyik vállalkozás a másikra egyoldalúan állapítja meg.[107] Ebből két következtetés adódik: az Adatrendelet a vállalkozások közötti adatmegosztási szerződésekben foglalt tisztességtelen feltételek körét arra az esetre rendezi, amikor az egyik fél egyoldalúan kényszerít ki valamely feltételt, illetve a tisztességtelen szerződési feltételekre vonatkozó szabályok csak a szerződés azon elemeire alkalmazandók, amelyek az adatok rendelkezésre bocsátásával kapcsolatosak, azaz az adathozzáférésre és -felhasználásra vonatkozó szerződési feltételekre, valamint az adatokkal kapcsolatos kötelezettségek megsértése és megszüntetése esetén fennálló felelősségre vagy jogorvoslatokra.[108]

A 13. cikk áll egy generálklauzulából, egy fekete és egy szürke listából.[109] Az Adatrendelet tehát megkülönbözteti a *per se* és a vélelmezhetően tisztességtelen szerződési feltételeket, amely utóbbi esetben a szerződési feltételt megállapító vállalkozás számára lehetővé kell tenni, hogy megcáfolhassa a tisztességtelenségre vonatkozó vélelmet. A generálklauzulát az adathozzáférés és -felhasználás terén az alkalmazott helyes üzleti gyakorlattól való jelentős eltérés és – konjunktív feltételként – a jóhiszeműség és tisztesség elvének a sértése alapozza meg.[110] *Per se* tisztességtelen az a szerződési feltétel, amelyik:[111]

- kizárja a feltételt egyoldalúan megállapító fél felelősségét a szerződéses kötelezettségek nemteljesítése esetén;
- kizárja az azon fél rendelkezésére álló jogorvoslati lehetőségeket, amellyel szemben a szerződési feltételt egyoldalúan kényszerítették ki;

104 Adatrendelet 5. cikk (3) bekezdés.
105 Adatrendelet 6. cikk (2) bekezdés *d)* pont.
106 Adatrendelet 13. cikk (1) bekezdés.
107 Szilágyi 2024: 585.
108 Adatrendelet (60) preambulumbekezdés.
109 Szilágyi 2024: 585.
110 Adatrendelet 13. cikk (3) bekezdés.
111 Adatrendelet 13. cikk (4) bekezdés.

– kizárólagos jogot biztosít a feltételt egyoldalúan kikényszerítő fél számára annak megállapítására, hogy a szolgáltatott adatok megfelelnek-e a szerződésnek.

Szürke listás kikötés például szolgáltatásváltás esetén aránytalanul hosszú felmondási idő [13. cikk (5) bekezdés *d)* pont], indokolatlanul rövid felmondási idő a feltétel alkalmazójának felmondása esetén [13. cikk (5) bekezdés *f)* pont].

Nem személyes adatok tekintetében jogellenes nemzetközi kormányzati hozzáférés

Harmadik országok elfogadhatnak olyan törvényeket, rendeleteket és egyéb jogi aktusokat, amelyek célja a határaikon kívül – többek között az Unióban – található nem személyes adatok közvetlen továbbítása vagy az azokhoz való kormányzati hozzáférés biztosítása. A harmadik országok bíróságai és igazságszolgáltatási fórumai által hozott olyan ítéleteket, valamint egyéb igazságügyi vagy közigazgatási – köztük bűnüldöző – hatóságai által hozott olyan határozatokat, amelyek a nem személyes adatok tekintetében ilyen továbbítást vagy hozzáférést írnak elő, akkor lehet végrehajtani, ha azok az adatokat igénylő harmadik ország és az Unió vagy valamely tagállama között létrejött hatályos nemzetközi megállapodáson, például kölcsönös jogsegélyről szóló megállapodáson alapulnak.[112] Az ilyen ügyeket szabályozó nemzetközi megállapodások hiányában a nem személyes adatok továbbítása vagy az azokhoz való hozzáférés csak akkor megengedett (hiszen az felvetheti például a biztonsághoz és a hatékony jogorvoslathoz való jognak vagy valamely tagállam nemzetbiztonsággal vagy védelemmel kapcsolatos alapvető érdekeinek sérelmét), ha bizonyítást nyer, hogy a harmadik ország jogrendszere megköveteli a határozat indokainak és arányosságának meghatározását, a bírósági végzés vagy a határozat konkrét jellegét, és azt, hogy a címzett indokolt kifogását olyan illetékes harmadik országbeli bíróság vagy igazságszolgáltatási fórum vizsgálja felül, amely hatáskörrel rendelkezik arra, hogy kellően figyelembe vegye az ilyen adatok szolgáltatójának releváns jogi érdekeit. [113]

Az adatkezelési szolgáltatónak a kérelem teljesítése előtt tájékoztatnia kell az ügyfelet arról, hogy egy harmadik ország hatósága az adataihoz való hozzáférés iránti kérelmet nyújtott be, kivéve, ha a kérelem bűnüldözési célokat szolgál, és mindaddig, amíg ez a bűnüldözési tevékenység eredményességének megőrzéséhez szükséges.[114]

Annak érdekében, hogy megelőzzék a harmadik országbeli hatóságok általi jogellenes kormányzati hozzáférést nem személyes adatokhoz, az Adatrendelet hatálya alá tartozó adatkezelési szolgáltatásokat – mint például a felhő – nyújtó szolgáltatóknak minden észszerű intézkedést meg kell tenniük annak érdekében, hogy megakadályozzák a nem személyes adatokat tároló rendszerekhez való hozzáférést, többek között – adott esetben – az adatok titkosítása, gyakori

[112] Adatrendelet 32. cikk (2) bekezdés.
[113] Adatrendelet 32. cikk (3) bekezdés.
[114] Adatrendelet 32. cikk (5) bekezdés.

ellenőrzések, a biztonságot szavatoló releváns tanúsítási rendszerek ellenőrzött betartása és a vállalati politikák módosítása révén.[115]

Az adatkezelési szolgáltatók a honlapjaikon elérhetővé teszik, hogy az adatkezelésének céljára telepített IKT-infrastruktúra mely joghatóság alá tartozik, és hogy az adatkezelési szolgáltató milyen technikai, szervezési és szerződéses intézkedéseket tett annak érdekében, hogy megakadályozza az Unióban tárolt nem személyes adatokhoz való nemzetközi kormányzati hozzáférést és azok továbbítását, amennyiben az ilyen adattovábbítás vagy hozzáférés az uniós joggal vagy a releváns tagállam nemzeti jogával való ütközéshez vezetne.[116]

ÖSSZEGZÉS

Az EU adatmegosztás-szabályozása önmagában demonstrálja a digitális átállás európai szabályozásának kihívásait. Az adatmegosztásra ugyanis a versenyjoggal együtt hét különféle szabályozás vonatkozik, amely összesen négyféle adatmegosztási irányt (B2B, B2C, B2G, G2B) ismer. Csak az adathordozás esetében el kell tudni igazodni a GDPR, a DMA, az Adatrendelet, a DCSD, a CRD szabályozásai között. Nem véletlen, hogy a Draghi-jelentés szerint is az uniós vállalatok több mint 60%-a a szabályozást tekinti a beruházások akadályának.[117] Az EU adatgazdasági szabályozása továbbá arra is példa, hogy az EU-ban a digitális gazdaság mennyire jogi lehetőségek (jelen esetben az utópiacok típusú) – és nem a piac kreativitása – által motivált.

Az EU Adatrendelete több szempontból is az ellentmondások jogszabálya lehet. Egyrészről a BusinessEurope és a Mechanical Engineering Industry Association a szerződéses szabadság és az önkéntes adatmegosztás megőrzése mellett érvel, hangsúlyozva a versenyképesség fenntartásának és az alapvető üzleti *know-how* védelmének fontosságát.[118] Ez a megközelítés visszhangozza a Draghi-jelentés versenyképesség növelése érdekében kevesebb európai szabályozás mellett érvelő megközelítését.[119] Másfelől azonban az adatok értékének kiaknázása döntő fontosságú lesz Európa versenyképessége szempontjából az elkövetkező évtizedekben.[120] Az EU által 2020-ban végzett felmérésből kiderült, hogy az európai vállalkozások 40%-a jelentősen alacsonyabb digitális intenzitást mutat, mint az Egyesült Államokban működő társaik.[121] Az Adatrendelet miatt az EU piacán potenciálisan új platformok jelenhetnek meg, amelyek viszont természetüknél fogva szabályozott jogosultságtól fognak függeni.[122] Ennek következtében a létrejövő üzleti modellek inkább a szabályozási megfelelésen, mint a kreativitáson alapulnak, a digitális szolgáltatások kevésbé dinamikus környezetének kialakulását eredményezve.

115 Adatrendelet 32. cikk (1) bekezdés.
116 Adatrendelet 28. cikk.
117 European Commission 2024: 18.
118 BusinessEurope 2022.
119 European Commission 2024.
120 DIGITALEUROPE 2023.
121 Eurostat 2021.
122 Broadbent 2023.

Kifejezett aránytévesztésnek tűnik, hogy a Data Act vagy a DGA[123] a nem személyes adatok tekintetében szigorúbb követelményeket támaszt az EU-n kívüli kormányzati hozzáférések terén, mint a GDPR. Az aránytévesztés annak fényében értendő, hogy a személyes adatok nyilván stratégiaibb értéket képviselnek, mint a nem személyes adatok. A Draghi-jelentés szerint az „adatok értékvesztése" (azaz az EU-ból harmadik országokba továbbított adatok mennyisége) ma 90%-ra becsülhető.[124]

Pozitívuma az Adatrendeletnek, hogy szigorú biztosítékokat vezet be a tisztességtelen B2B adatmegosztási szerződések ellen – megkönnyítve ezzel a kkv-k számára az adatokhoz való hozzáférést –, és kötelezi a Bizottságot, hogy kidolgozza és ajánlja az adatokhoz való hozzáférésre és felhasználásra vonatkozó kiegyensúlyozott, nem kötelező érvényű mintaszabályokat.[125] Szintén pozitívuma az erős befektetésvédelem, hiszen az Adatrendelet megtiltja az adatok felhasználását versenyző termékek fejlesztésére vagy abból a célból, hogy azáltal betekintést nyerjenek az adatbirtokos gazdasági helyzetére, eszközeire és termelési módszereire, vagy az adatbirtokos általi felhasználásukra vonatkozóan. Ezen túl a kapott adatok nem használhatók fel oly módon, amely hátrányos hatással van az összekapcsolt termék vagy a kapcsolódó szolgáltatás biztonságára, illetve nem áshatja alá az üzleti titkok bizalmi jellegét.

FELHASZNÁLT IRODALOM

Botta, Marco (2023): *Shall We Share? The Principle of FRAND in B2B Data Sharing.* RSC Working Paper 2023/30. Online: https://doi.org/10.2139/ssrn.4422925

Broadbent, Meredith (2023): *The EU Data Act: The Long Arm of European Tech Regulation Continues.* Center for Strategic and International Studies, 2023. június 29. Online: https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues

BusinessEurope (2022): *The Proposal for a Data Act: A BusinessEurope Position Paper. BusinessEurope,* 2022. január 31. Online: https://www.businesseurope.eu/publications/the-proposal-for-a-data-act-a-businesseurope-position-paper/

Carugati, Christophe (2023): The Antitrust Privacy Dilemma. *European Competition Journal,* 19(2), 167–190. Online: https://doi.org/10.1080/17441056.2023.2169310

Casolari, Federico – Buttaboni, Carlotta – Floridi, Luciano (2023): *The EU Data Act in Context: A Legal Assessment.* SSRN eLibrary. Online: https://ssrn.com/abstract=4584781

Council of the European Union (2023): *Data Act: Council Adopts New Law on Fair Access to and Use of Data.* Press release, 2023. november 27. Online: https://www.consilium.

[123] Nem személyes adatok harmadik országba való továbbítása esetén megfelelő biztosítékokat kell alkalmazni annak érdekében, hogy az adatok az európai uniós joggal egyenértékű védelmet élvezzenek, különös tekintettel az üzleti titkokra és a szellemi tulajdonhoz fűződő jogokra. Az Európai Bizottság végrehajtási aktusokat hozhat, amelyekben megállapítja, hogy egy harmadik ország lényegében egyenértékű védelmet biztosít, különösen, ha az EU-n belül sok kérelem érkezik az adott országban történő adat-újrafelhasználásra. DGA (21) preambulum-bekezdés.

[124] European Commission 2024: 67.

[125] Casolari–Buttaboni–Floridi 2023: 17.

europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/

Crémer, Jacques – de Montjoye, Yves-Alexandre – Schweitzer, Heike (2019): *Competition Policy for the Digital Era*. Final Report. Luxembourg: Publications Office of the European Union. Online: https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en

DIGITALEUROPE – European Round Table for Industry (2023): Joint Statement on the Data Act. *DIGITALEUROPE,* 2023. június 19. Online: https://www.digitaleurope.org/news/joint-statement-on-the-data-act-by-digitaleurope-and-the-european-round-table-for-industry/

Európai Bizottság (2020): *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai adatstratégia*. COM(2020) 66 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020DC0066

European Commission (2020a): Commission Staff Working Document – Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), SWD(2020) 295 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:0295:FIN

European Commission (2020b): *State of the Union Address by President von der Leyen at the European Parliament Plenary.* 2020. szeptember 16. Online: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

European Commission (2024): *The Future of European Competitiveness: A Competitiveness Strategy for Europe*. 2024. szeptember 9. Online: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

Eurostat (2021): How Digitalised Are EU's Enterprises? *Products Eurostat News,* 2021. október 29. Online: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211029-1

Holm-Hadulla, Moritz – Meiborg, Nora Johanna (2023): Data Access under the Data Act – New Momentum for the IoT Market (and Beyond)? *European Competition Law Review,* 44, 187–193.

Monti, Giorgio – Tombal, Thomas – Graef, Inge (2022): *Study for Developing Criteria for Assessing "Reasonable Compensation" in the Case of Statutory Data Access Right*. Brussels: Publications Office of the European Union. Online: https://doi.org/10.2838/19186

OECD (2015): *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing. https://doi.org/10.1787/9789264229358-en

Szilágyi Ferenc (2024): Az adathozzáférést és az adatfelhasználást szabályozó szerződések és a szerződési jogi szabályok az EU Adatrendelet (Data Act) keretrendszerében – I. rész. *Magyar Jog,* 71(10), 580–588.

Tóth András (2021): A mesterséges intelligencia versenyjogi vonatkozásai. In Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai: Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest: Ludovika, 465–489.

Von Ditfurth, Lukas – Lienemann, Gregor (2022): The Data Governance Act: Promoting or Restricting Data Intermediaries? *Journal of Competition and Regulation in Network Industries,* 23(4), 270–295. Online: https://doi.org/10.1177/17835917221141324

Jogi források

Az Európai Parlament és a Tanács 1907/2006/EK rendelete (2006. december 18.) a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az Európai Parlament és a Tanács (EU) 2018/858 rendelete (2018. május 30.) a gépjárművek és pótkocsijaik, valamint az ilyen járművek rendszereinek, alkotóelemeinek és önálló műszaki egységeinek jóváhagyásáról és piacfelügyeletéről, a 715/2007/EK és az 595/2009/EK rendelet módosításáról, valamint a 2007/46/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről

Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról

Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról

Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és – felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról

Az Európai Parlament és a Tanács 2008/6/EK irányelve (2008. február 20.) a 97/67/EK irányelvnek a közösségi postai szolgáltatások belső piacának teljes megvalósítása tekintetében történő módosításáról

Az Európai Parlament és a Tanács 2011/83/EU irányelve (2011. október 25.) a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről
Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról
Az Európai Parlament és a Tanács (EU) 2019/770 irányelve (2019. május 20.) a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól
Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról
Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról

Tóth András egyetemi docens, a Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Digitális és Technológia Jogi Tanszékének vezetője. 2010 óta a Gazdasági Versenyhivatal elnökhelyettese, a Versenytanács elnöke. A *European Competition and Regulatory Law Review* szerkesztőbizottsági tagja. A *Central European Lawyers Initiative* és a Jáki Szaniszló Társaság elnöke.