Miskolci Egyetem
Állam- és Jogtudományi Kar
Közigazgatási Jogi Tanszék

SZAKDOLGOZAT

Az adatvédelem és az információszabadság határterületei a közfeladatot ellátó gazdasági társaságok működésében

---

– az adatvédelmi tisztviselő szerepe a közérdekű adatigénylések teljesítése és az adatvédelmi incidensek bejelentése során az uniós, valamint hazai adatvédelmi szabályozás nóvumainak tükrében.

Dr. Czékmann Zsolt
tanszékvezető
egyetemi docens

dr. Gräf Richárd
adatvédelmi szakjogász
szakirányú továbbképzési szak
Neptun-kód: VVRAS0

Miskolc, 2026.

University of Miskolc
Faculty of Law
Department of Administrative Law

THESIS

The Interface between Data Protection and Freedom of Information in the Operations of Business Associations Performing Public Duties

---

– the role of the Data Protection Officer in the fulfilment of requests for access to data of public interest and the notification of personal data breaches in light of recent developments in EU and Hungarian Data Protection Law.

Dr. Zsolt Czékmann
Head of Department
Associate Professor

dr. Richárd Gräf
Postgraduate Specialisation Programme
in Data Protection Law
Neptun code: VVRAS0

Miskolc, 2026

TARTALOMJEGYZÉK

Bevezetés **4**

I. Alapjogi és fogalmi keretek **6**

I.1. Az információs alapjogok és az alkotmányos mércék 6

I.2. Adatfajták, azonosíthatóság és a szabályok együttalkalmazása 8

II. A gazdasági társaság adatkezelői és adatszolgáltatói helyzete **11**

II.1. Közfeladat, társasági forma és a nyilvánosság kötelezettje 11

II.2. Adatkezelői szerepek és a társasági működés adatai 13

III. Az adatvédelmi tisztviselő jogállása és szervezeti szerepe **15**

III.1. Kijelölés, függetlenség és a feladatellátás feltételei 15

III.2. Tanácsadás, összeférhetetlenség és adatkezelői felelősség 17

IV. A közérdekű adatigénylések teljesítése **18**

IV.1. Az igény azonosítása és az eljárás keretei 18

IV.2. Nyilvános személyes adatok, közpénz és üzleti titok 20

IV.3. A korlátozás indokolása és a részleges teljesítés 21

IV.4. Tisztviselői közreműködés, dokumentálás és jogorvoslat 23

V. Adatvédelmi incidensek felismerése és bejelentése **25**

V.1. Az incidens felismerése, a tudomásszerzés és a határidő 25

V.2. Kockázatértékelés, bejelentés és érintetti tájékoztatás 27

V.3. Elhárítás, bizonyítékok és a tisztviselő közreműködése 29

VI. Joggyakorlat és a két eljárás találkozása **31**

VI.1. A jogesetek tanulságai és a társasági adatkiadás 31

VI.2. Hibás adatkiadás és az incidensiratok megismerése 33

VII. Hazai és uniós szabályozási nóvumok **37**

VII.1. Hazai változások: együttműködés és közzététel 37

VII.2. Uniós fejlemények és az alkalmazás időbeli határai 39

VII.3. Jogalkalmazási tapasztalatok és kiberbiztonsági kapcsolat 40

VIII. Szervezeti és jogalkalmazási javaslatok **42**

Összegzés **46**

Irodalomjegyzék **48**

Internetes források **49**

Jogszabályjegyzék **50**

Hazai jogszabályok 50

Uniós jogforrások 50

Hivatkozott bírósági döntések **51**

„Az a kijelentés, hogy nem érdekel a magántitokhoz való jog, mert nincs titkolnivalód, ugyanolyan, mintha azt mondanád, nem érdekel a szólásszabadság, mert nincs mondanivalód.”

- Edward Snowden

B E V E Z E T É S

Dolgozatom tárgyát az adatvédelem és az információszabadság azon határterületei képezik, amelyek a közfeladatot ellátó gazdasági társaságok mindennapi működésében, különösen a közérdekű adatigénylések teljesítése során merülnek fel. E szervezeti körben a közpénzek felhasználásának ellenőrizhetősége és a személyes adatok védelme gyakran ugyanazon dokumentumhoz kapcsolódik – egy támogatási szerződés vagy vezetői javadalmazási kimutatás nyilvános gazdálkodási adatot és jogszerűen elzárható személyes információt egyaránt tartalmazhat.[1] Székely Iván a két információs alapjog közös rendeltetését az információs hatalmi különbségek mérséklésében ragadja meg[2], míg De Negri Laura a köztulajdonú gazdálkodó szervezetek piaci működése és átláthatósága közötti összefüggéseket vizsgálja.[3] Véleményem szerint e megközelítések együttesen is indokolttá teszik, hogy a társasági adatkiadást ne pusztán az irat elnevezése, hanem annak tényleges adattartalma és rendeltetése alapján értékeljük.

A témaválasztást az is indokolja, hogy az adatigénylés teljesítése maga is adatkezelési műveletek sorozata, hiszen az igénylő adatainak felvételétől a dokumentum felkutatásán és a kiadható tartalom kiválasztásán át a másolat továbbításáig jogi és technikai döntések kapcsolódnak egymáshoz. Amennyiben e folyamatban jogosulatlan személyesadat-közlés történik, az eredeti információszabadsági ügy adatvédelmi incidensbe torkollhat, ezért a jogszerű kiadás és a jogellenes közlés elhatárolását már a teljesítés előkészítésekor el kell végezni.[4] Szádeczky Tamás és Szőke Gergely László az információbiztonságot a titokvédelmi és nyilvánossági szabályok érvényesítésével összefüggésben tárgyalják[5] – ez az alaptézis az itt vizsgált társasági működésben arra irányítja a figyelmet, hogy a helyes jogi minősítést a kiadott fájl tényleges tartalmának is követnie kell.

---

[1] Magyarország Alaptörvénye (2011. április 25.), VI. cikk (3) bekezdés, 39. cikk (2) bekezdés; az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), 3. § 5–6. pont.

[2] SZÉKELY I.: [Fórumhozzászólás az adatvédelem és az információszabadság viszonyáról]. In *Fundamentum* 2004/4. 47–48. o.

[3] DE NEGRI L.: A köztulajdonban álló gazdálkodó szervezetek adatainak közzététele Németországban és Magyarországon: hasonlóságok és különbségek. In *Pro Futuro* 2022/1. 84–86. o.

[4] 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR), 4. cikk 2. és 12. pont, 33–34. cikk; Infotv. 30. § (1) bekezdés.

[5] SZÁDECZKY T. – SZŐKE G. L.: A bizalmasság és a nyilvánosság aktuális kihívásai az információbiztonság tükrében. In *Pro Futuro* 2018/2. 24–26. o.

Dolgozatom elsődleges célja annak áttekintése, milyen feltételekkel köteles egy állami gazdasági társaság az adatok megismerhetővé tételére, valamint hogyan illeszkedik az adatvédelmi tisztviselő közreműködése az adatigénylési és incidenskezelési eljárásba. Szabó Endre Győző a tisztviselő intézményét az elszámoltathatóságot támogató belső ellenőrzéshez kapcsolja,[6] ami a társasági felelősségi viszonyok vizsgálatához is kiindulópontot ad. Ennek figyelembevételével különösen arra keresek választ, miként egyeztethető össze a nyilvános adatok kiadása a személyes adatok védelmével, hol húzódik a tisztviselő szakmai tanácsadása és az adatkezelő döntési felelőssége közötti határ, továbbá mikor válik a hibás teljesítés bejelentendő incidenssé. További feladatként tűztem ki az új hazai rendelkezések és az uniós szabályozási fejlemények elemzését abból a szempontból, hogy azok milyen tényleges szervezési feladatokat keletkeztetnek a közfeladatot ellátó gazdasági társaságok számára.

A vizsgálatot három munkahipotézis vezeti. Elsőként azt feltételezem, hogy a jogszerű teljesítés alapfeltétele az adatfajták elkülönítése és a korlátozási indokok tételes vizsgálata – második feltevésem szerint a tisztviselő szerepe akkor tölthető be hatékonyan, ha korai bevonása megfelelő információhoz jutással és a végrehajtástól elkülönülő ellenőrzési lehetőséggel társul. Harmadikként azt vizsgálom, hogy az adatigénylési és incidenskezelési eljárás összekapcsolása csökkentheti-e a hibás közlés szervezeti kockázatát. E feltevések értékelését jogi érveléssel és szemléltető esetekkel végzem el, mindazonáltal a kockázatcsökkenés mértékére vonatkozó empirikus eredményt a dolgozat nem állapít meg. Kutatásom során elsősorban dogmatikai és joggyakorlatot elemző módszert követek: a jogszabályi rendelkezéseket európai bírósági döntések, a hazai joggyakorlatot bemutató intézményi források, adatvédelmi iránymutatások és szakirodalmi álláspontok összevetésével vizsgálom. A fentiek *primer jogforrásaként* az Európai Unió általános adatvédelmi rendelete (a továbbiakban: GDPR), és *az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény* (a továbbiakban: Infotv.) szolgál, míg az európai adatvédelmi kézikönyv az elszámoltathatóságot a megfelelés bizonyíthatóságával kapcsolja össze[7].

[6] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről – A GDPR szabályainak elemzése. In *Infokommunikáció és Jog* 2018/1. (70.) 3–4. o.

[7] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *Handbook on European data protection law. 2018 edition.* Luxembourg: Publications Office of the European Union, 2018. 134–136. o.

I. ALAPJOGI ÉS FOGALMI KERETEK

I.1. Az információs alapjogok és az alkotmányos mércék

Az információs önrendelkezés az egyénre vonatkozó információk kezelését korlátozó és ellenőrizhetővé tevő jogi garanciák rendszere, míg az információszabadság a közügyekre vonatkozó adatok megismerését szolgálja. Székely Iván korábban említett megközelítése szerint a két jog közös rendeltetése az információs hatalmi különbségek mérséklése: mindkettő javítja az egyén helyzetét az információs erőfölényben lévő szereplővel szemben.[8]

Ebből következően a társaság adatvédelmi feladatát nem tartom indokoltnak a nyilvánosság visszaszorításával azonosítani, hiszen a két jogosultság eltérő tárgyán keresztül egyaránt az ellenőrizetlen információs hatalom korlátozását szolgálja. Az alapjogok összehangolásának módszeréhez Székely Iván, Somody Bernadette és Szabó Máté Dániel döntéstámogatási megközelítése ad további támpontot. A szerzők a biztonsági megfigyelés körében a jogalap, a ténybeli szükségesség és az arányosság egymásra épülő vizsgálatát javasolják,[9] amelyet az adatkiadás eltérő helyzetében annak figyelembevételével alkalmazok, hogy előbb a nyilvánossági jogcímet és a tényleges adattartalmat kell feltárni, és csak ezt követően vizsgálható a korlátozás.

Egy közpénzügyi adat megismerése és egy munkavállaló magánéletének feltárása között így az adat konkrét rendeltetése, valamint az arra vonatkozó jogszabályi előírás tesz különbséget. A vizsgálat során ezért különválasztom a ténykérdést és a jogi értékelést: ténykérdés, hogy egy szerződés tartalmaz-e magánelérhetőséget, jogkérdés viszont, hogy e részletet milyen rendelkezés teszi megismerhetővé. A társaság vagy az érintett közléssel kapcsolatos érdeke önmagában egyik kérdést sem dönti el, így a tisztviselő szakmai közreműködése az érvelés következetességét is szolgálja. A személyesadat-minősítést, a közlési jogcímet és a szükséges védelmi intézkedést ennek megfelelően egymással összefüggő, de külön megállapításként indokolt rögzíteni.

[8] SZÉKELY I.: [Fórumhozzászólás ...], *i. m.* 47–48. o.

[9] SZÉKELY I. – SOMODY B. – SZABÓ M. D.: Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása, II. rész: Jogi és döntéstámogatási megközelítések. In *Információs Társadalom* 2017/1. 17–20. o.

A társasági működésben a két alapjog viszonya konkrét adatok szintjén ítélhető meg. Egy vezető közfeladatával összefüggő javadalmazásának megismerése az elszámoltathatóságot szolgálhatja, míg egészségi állapota vagy magánelérhetősége rendszerint más adatvédelmi megítélés alá esik, vagyis ugyanazon személyre vonatkozó információk között is eltérő megismerhetőségi szabályok érvényesülnek.[10] A közérdekből nyilvános személyes adatok kettős jogi természetét Bendik Tamás és Péterfalvi Attila is hangsúlyozzák.[11] Véleményem szerint az összehangolás első lépése ezért az adat és a nyilvánosságot igazoló közfeladat közötti kapcsolat feltárása – az érintett személy egészének általános „nyilvánossá" vagy „titkossá" minősítése e különbségeket elfedné.

Az Alaptörvény VI. cikk (3) bekezdése együtt rögzíti a személyes adatok védelmét és a közérdekű adatok megismeréséhez, terjesztéséhez való jogot, a közpénzekkel gazdálkodó szervezetek átláthatóságát pedig a 39. cikk (2) bekezdése külön is megerősíti. Az alapjog-korlátozás szükségességét és arányosságát az I. cikk (3) bekezdése alapján kell értékelni. E rendelkezésekből az következik, hogy a társasági forma önmagában nem határozza meg a közpénzekre vonatkozó adatok megismerhetőségét, a törvényi adatnyilvánossági szabályokat alkotmányos rendeltetésükkel összhangban kell alkalmazni.[12] Az uniós jogban az Alapjogi Charta 7. és 8. cikke a magánélet és a személyes adatok védelmét, 11. cikke pedig a véleménynyilvánítás és tájékozódás szabadságát biztosítja. Az Európa Tanács rendszerében az Emberi Jogok Európai Egyezményének 8. és 10. cikke adja az összehangolás fontos mércéit.[13] Az európai adatvédelmi kézikönyv is elkülönítve mutatja be az egyezményi és az uniós jogi keretet,[14] ami az alkalmazás határainak tisztázásához szükséges. A Charta 42. cikke ugyanis az uniós intézmények, szervek és hivatalok dokumentumaihoz való hozzáférésre vonatkozik, ezért egy magyar gazdasági társasággal szemben nem szolgál közvetlen, általános adatigénylési jogalapként. A jogforrások eltérő hatályát tehát a konkrét ügyre történő alkalmazás előtt kell megállapítani.

[10] Infotv. 26. § (2) bekezdés; GDPR 9. cikk (1) bekezdés; a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény, 2. § (1)–(2) bekezdés.

[11] BENDIK T. – PÉTERFALVI A.: Janus nyomában – a közérdekből nyilvános személyes adatok jellemzői és kezelésük különös szabályai. In *Pro Publico Bono – Magyar Közigazgatás* 2025/2. 55–57. o.

[12] Alaptörvény I. cikk (3) bekezdés, VI. cikk (3) bekezdés, 39. cikk (2) bekezdés.

[13] Az Európai Unió Alapjogi Chartája, 7–8., 11., 42., 51. és 52. cikk; az emberi jogok és az alapvető szabadságok védelméről szóló egyezmény, 8. és 10. cikk (kihirdette az 1993. évi XXXI. törvény).

[14] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 23–24, 27–29. o.

A Magyar Helsinki Bizottság kontra Magyarország ügyben az Emberi Jogok Európai Bírósága a kért információ rendeltetését, közérdekű jellegét, az igénylő szerepét és az adat rendelkezésre állását értékelte az Egyezmény 10. cikkéből levezethető hozzáférés feltételeinek meghatározásakor.[15] Mindazonáltal e feltételekből nem következik, hogy az Infotv. alapján minden magyar adatigénylőtől újságírói vagy civil ellenőrző szerepet lehetne megkövetelni, hiszen a hazai törvény bárki számára biztosítja az igény benyújtásának lehetőségét. Az európai alapjogi mérce a nemzeti jogosultság értelmezését segíti, annak törvényi tartalmát azonban nem helyettesíti.

I.2. Adatfajták, azonosíthatóság és a szabályok együttalkalmazása

Az Infotv. a közérdekű adatot a közfeladatot ellátó szerv tevékenységéhez kapcsolódó, személyes adatnak nem minősülő információként határozza meg, míg közérdekből nyilvános az az adat, amelynek megismerhetőségét törvény közérdekből előírja. A személyes adat a GDPR szerint azonosított vagy azonosítható természetes személyre vonatkozó információ, ezért a közérdekből nyilvános személyes adat sajátos metszetet képez. Bendik és Péterfalvi tanulmánya szerint e kategória egyszerre tárgya az információszabadságnak és a személyesadat-védelemnek[16], a nyilvánosság ennélfogva nem szünteti meg az adat személyes jellegét, és nem teszi mellőzhetővé az adatkezelés további feltételeinek vizsgálatát. A gyakorlatban az azonosíthatóságot a dokumentum környezetével együtt kell vizsgálni, hiszen a név törlése kevés lehet, amennyiben a munkakör, a szerződés tárgya és az esemény időpontja együttesen egyetlen személyre utal. Az álnevesítés során az összerendelés további információval még lehetséges: a kiegészítő azonosító információt őrző adatkezelő számára az adat személyes marad, más címzettnél azonban az azonosíthatóság tényleges lehetőségeit külön kell vizsgálni. Az anonimizálás eredményét ugyanakkor az észszerűen igénybe vehető azonosítási lehetőségek alapján kell megítélni. E különbség az adatigénylési másolat készítésénél azért jelentős, mert a név elhagyása után fennmaradó közvetett azonosítók is ellenőrzést igényelnek.[17, 18]

---

[15] Emberi Jogok Európai Bírósága: Magyar Helsinki Bizottság kontra Magyarország [Nagykamara], 18030/11. sz. kérelem, 2016. november 8., 149–180. pont, különösen 157–170. pont; Infotv. 28. § (1) bekezdés.

[16] Infotv. 3. § 5–6. pont; GDPR 4. cikk 1. pont. Bendik – Péterfalvi: *i. m.* 55–57. o.

[17] GDPR 4. cikk 1. és 5. pont, (26) preambulumbekezdés; Európai Unió Bírósága: C-413/23 P. sz. Európai Adatvédelmi Biztos kontra Egységes Szanálási Testület ügy, 2025. szeptember 4., ECLI:EU:C:2025:645, 52. és 75–85. pont.

[18] GULYÁS G. Gy.: Gépi tanulási módszerek alkalmazása deanonimizálásra. In *Információs Társadalom* 2017/1. 72–74, 78. o.

Gulyás Gábor György a deanonimizálás kutatási eredményeit bemutatva arra mutat rá, hogy a közvetlen azonosítók eltávolítása mellett megmaradó jellemzők más adathalmazzal összekapcsolva újraazonosítást tehetnek lehetővé.[19] E kettős nézőpontot pontosítja a C-413/23 P. számú, EDPS kontra SRB ügyben hozott ítélet. Bár az ügy az uniós intézmények adatkezelésére irányadó (EU) 2018/1725 rendeletet érintette, a Bíróság az 52. pontban a személyes adat fogalmának a GDPR-ral egységes értelmezését írta elő. Az azonosító információt megőrző adatkezelőnél az adat személyes marad – más címzettnél viszont a kiegészítő információhoz való hozzáférést, a védelem tényleges megkerülhetőségét és az egyéb adatokkal való összekapcsolást is értékelni kell. A kulcs átadásának elmaradása tehát önmagában nem bizonyítja az azonosíthatatlanságot. Az idő-, költség- és technológiai feltételek együttes vizsgálata alapján ugyanakkor előfordulhat, hogy a címzett számára az érintett nem azonosítható. Véleményem szerint az ítélet jelentősége éppen abban áll, hogy a minősítést a konkrét adatkezelés körülményeihez, nem pedig az „álnevesített” megjelöléshez kapcsolja.[20]

A társasági iratokra alkalmazva e megállapítást, a nyilvános másolat ellenőrzésekor a megmaradó adattartalmat és a hozzáférhető külső információt együttesen tartom szükségesnek értékelni. Egyetlen telephely egyetlen munkakörének és egy pontos időpontnak a megjelölése például a név kitakarása után is azonosíthatóvá teheti az érintettet, így az ellenőrzés tárgya a közlés tényleges eredménye, amelyet az eltávolított mezők száma önmagában nem ír le. Az ítéletből az álnevesített fájl korlátlan nyilvánosságra hozhatósága sem következik: újabb továbbításnál az új címzettek azonosítási lehetőségeit ismét értékelni kell. Egy meghatározott címzettnek történő átadás és az internetes közzététel ezért eltérő vizsgálatot kíván. A társaság saját adatkezelésének jogalapját és az Infotv. szerinti megismerhetőséget mindkét esetben külön igazolni szükséges.[21] A GDPR 86. cikke lehetővé teszi, hogy a hivatalos dokumentumokban szereplő személyes adatokat az uniós vagy tagállami jog szerint közöljék, a nyilvános hozzáférés és a személyes adatok védelmének összeegyeztetése érdekében.

[19] GULYÁS: *i. m.* 72–74, 78. o.

[20] Európai Unió Bírósága: C-413/23 P. sz. Európai Adatvédelmi Biztos kontra Egységes Szanálási Testület ügy, 2025. szeptember 4., ECLI:EU:C:2025:645, 52. és 75–85. pont; GDPR 4. cikk 1. és 5. pont, (26) preambulumbekezdés.

[21] Európai Unió Bírósága: C-413/23 P. sz. ügy, 84–85. pont; GDPR 5–6. és 86. cikk; Infotv. 26. § (1)–(2) bekezdés.

A közlés jogszerűségének vizsgálatában a megfelelő törvényi nyilvánossági rendelkezést és a GDPR szerinti adatkezelési jogalapot egyaránt azonosítani kell: a 6. cikk (1) bekezdés c) vagy e) pontja alkalmazható lehet, azonban a választást a konkrét kötelezettséghez és adatkezelési célhoz kell igazítani. A hozzájárulás beszerzése nem helyettesíti a törvényi adatkiadási kötelezettséget.[22] Váradi Szilvia közszférára vonatkozó elemzése a jogszabályhoz kötött feladatellátást és az érintett korlátozott választási lehetőségét emeli ki. A közszolgáltatást magánjogi szervezet is elláthatja, ami az adatkezelés garanciális vizsgálatát e szervezeti körben is indokolja.[23] Ebből a társasági adatkiadásra nézve azt a következtetést vonom le, hogy a jogalapot a konkrét művelethez kell rendelni. A közszolgáltatás teljesítéséhez felvett ügyféladat és az ugyanazon iratból készített közérdekű másolat eltérő célt szolgál, ezért a közfeladat puszta megnevezése nem igazolja, hogy a teljes ügyfélirat korlátozás nélkül megismerhető legyen. Az együttalkalmazás az alapelvek érvényesítését is megköveteli.

Az adattakarékosság annak vizsgálatát jelenti, hogy mely személyes adatok szükségesek a jogszerű közléshez – nem jogosít fel a törvény alapján megismerhető információ önkényes visszatartására. A pontosság a kiadott változat helyességét, az integritás és bizalmas jelleg pedig a továbbítás megfelelő biztonságát érinti. Az európai adatvédelmi kézikönyv az elszámoltathatóságot a megfelelést bizonyíthatóvá tevő intézkedésekkel kapcsolja össze, mely számomra rávilágít arra, hogy a társaság csak akkor tudja igazolni a helyes mérlegelést, ha a közlés indoka és technikai végrehajtása is visszakövethető.[24] Az információbiztonság szerepét Szádeczky Tamás és Szőke Gergely László a titokvédelmi és nyilvánossági szabályok érvényesítésével összefüggésben vizsgálják, megközelítésükben a technikai védelem a jogszerű hozzáférést is támogatja.[25] Az állami gazdasági társaságok számára ez véleményem szerint kettős tervezési feladatot jelent atekintetben, hogy a belső példányhoz csak az arra jogosultak férjenek hozzá, a nyilvános másolat ugyanakkor valóban olvasható és használható legyen. A minden adatot hozzáférhetetlenné tevő biztonsági megoldás az információszabadságot, a teljes belső példány kiadása pedig a személyesadat-védelmet sértheti. A jogszerű hozzáférést ezért az adott dokumentumváltozathoz és az azt megismerő személy jogosultságához szükséges igazítani.

[22] GDPR 6. cikk (1) bekezdés c) és e) pont, (3) bekezdés, 86. cikk.
[23] VÁRADI Sz.: A közszférára vonatkozó adatvédelmi szabályok a GDPR tükrében. In *Pro Futuro* 2019/1. 40–41. o.
[24] GDPR 5. és 24. cikk. European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 134–136. o.
[25] SZÁDECZKY – SZŐKE: *i. m.* 24–26. o.

II. A GAZDASÁGI TÁRSASÁG ADATKEZELŐI ÉS ADATSZOLGÁLTATÓI HELYZETE

II.1. Közfeladat, társasági forma és a nyilvánosság kötelezettje

A közfeladatot ellátó gazdasági társaság, a köztulajdonban álló társaság és a nonprofit társaság fogalma eltérő szempontokat fejez ki. A közfeladat az ellátott tevékenység jogi rendeltetésére, a köztulajdon a tulajdonosi befolyásra, a nonprofit jelleg pedig a társasági működés sajátosságára utal. A *2009. évi CXXII. törvény* a köztulajdonban álló társaságokra külön átláthatósági előírásokat tartalmaz. Az alkalmazandó szabályok meghatározásához ezért a létesítő okirat mellett a társaság közfeladatát és az adott adat nyilvánosságát meghatározó jogszabályokat is fel kell tárni.[26] De Negri Laura összehasonlító elemzése a piaci működés és a közvagyonnal való gazdálkodás átláthatóságának együttes követelményeire irányítja a figyelmet, hiszen a társaság szerződéses partnerekkel versenyző piaci szereplő lehet, ugyanakkor közpénzek felhasználásáról is köteles számot adni. E kettősségből általános titkosság nem vezethető le, így a vizsgálat során követett megközelítésem szerint minden adatkörnél külön kell tisztázni a közfeladati vagy közvagyoni kapcsolatot és az esetleges törvényi korlátozást. Az üzleti működés sajátosságai a megismerés határainak vizsgálatához, nem a teljes szervezet kivonásához szolgáltatnak érveket.[27]

Kormány Béla a magyar és a lengyel vagyongazdálkodási modell összehasonlításában a magyar rendszer közfeladatot előtérbe helyező rendeltetését és a nyilvános elszámoltathatóság jelentőségét hangsúlyozza. A közszolgáltatási és piaci tevékenység együttes jelenléte szerinte a teljesítmény értelmezését is befolyásolja.[28] E megállapítást az információszabadság felől értékelve abból indulok ki, hogy a közfeladat indokolja az ellenőrizhetőséget, miközben a társaság piaci működése az egyes korlátozási okok tartalmi vizsgálatában kaphat szerepet. A nyilvános adatoknak ezért azt is meg kell mutatniuk, milyen feladat ellátására és milyen feltételekkel használták fel a közvagyont.

[26] 2009. évi CXXII. törvény, 1. § a)–b) pont, 2. §.
[27] DE NEGRI: *i. m.* 84–86. o.
[28] KORMÁNY B.: A nemzeti vagyongazdálkodás intézményi modelljei – magyar–lengyel összehasonlító elemzés. In *Jegyző és Közigazgatás* 2026/1. 31. o. A tanulmány nyilvánosan hozzáférhető részlete, III.1. pont. https://szakcikkadatbazis.hu/doc/6523176 (2026. 10. 05.)

De Negri és Kormány megközelítése eltérő kérdésből indul ki, amennyiben az előbbi az adatközzététel jogi kereteit, az utóbbi pedig a tulajdonosi működés intézményi rendjét vizsgálja – a két nézőpontot az ellenőrizhetőség kapcsolja össze. Ha a társaság feladata és a közpénzfelhasználás rendeltetése nem ismerhető meg, a szerződéses adatok puszta felsorolása sem ad teljes képet a működésről. Ezzel együtt az átláthatósági igény nem keletkeztet korlátlan személyesadat-közlési jogosultságot: a feladat eredményessége a nyilvános gazdálkodási adatok, valamint a szükséges és megfelelően elkülönített személyes adatok alapján értékelendő.

Az Infotv. 26. § (1) bekezdése a közfeladatot ellátó szerv kezelésében lévő közérdekű és közérdekből nyilvános adatok megismerhetőségét írja elő: a közfeladatot ellátó szervre irányadó szabályok és az egyes adatfajták meghatározása alapján kell vizsgálni, hogy a társaságra milyen kötelezettség hárul. Az adat eredetének megjelölése nem feltétlenül dönti el ezt a kérdést, hiszen egy minisztériumtól kapott dokumentum másolata a társaságnál is rendelkezésre állhat – ettől elkülönül az, hogy milyen tartalommal és milyen korlátok között ismerhető meg.[29, 30] A rendelkezésre állás ellenőrzése tényleges iratfeltárást igényel, amelynek során meg kell vizsgálni, megtalálható-e a dokumentum a társaság irattárában, elektronikus rendszerében vagy az ügyintézőknél, és a kért adatkör ebből kinyerhető-e. A társaság nem köteles nem létező elemzést vagy új szakmai állásfoglalást létrehozni pusztán az igény miatt. Az adat hiánya azonban nem azonos azzal, hogy az adat nincs a kérelmező által megnevezett táblázatba rendezve. Az egyszerű másolatkészítést és elkülönítést az új tartalom előállításától indokolt különválasztani, és a ténylegesen elvégzett keresést rögzíteni.[31] Az adatkeresés és az új tartalom létrehozása közötti határt a 13/2019. (IV. 8.) AB határozat is elemzi. A döntés megkülönbözteti a már rögzített adatok kikeresését és rendszerezését a minőségileg új információ előállításától.[32]

Társasági környezetben ezért az a kérdés, hogy a kért eredmény meglévő adatok közlésével előáll-e, vagy új szakmai ítéletet kíván - a szerződésekben szereplő összegek kigyűjtése és a szerződések gazdasági célszerűségének utólagos értékelése ugyanis eltérő művelet, ezért az utóbbi elmaradása nem igazolja az előbbi megtagadását.

[29] Infotv. 3. § 5–6. pont, 26. § (1) bekezdés.
[30] DE NEGRI: *i. m.* 84–86. o.
[31] Kúria: A „közérdekű adatok kiadásával kapcsolatos perek" bírósági gyakorlata tárgykörére felállított joggyakorlat-elemző csoport összefoglaló véleménye. 2017.EI.II.J.GY.P.3. sz., lezárva 2018. december 3. [67]–[73] bekezdés, 17. o.
[32] 13/2019. (IV. 8.) AB határozat, Indokolás [51]–[60], különösen [55] és [59]–[60].

Külön jogértelmezési kérdés merül fel, amennyiben a társaság egy másik szerv döntésének előkészítésében vesz részt, mert ilyenkor a döntési hatáskör, az irat keletkeztetése, az adatkezelői szerep és a megismerés biztosításának kötelezettsége eltérő szervezetekhez kapcsolódhat. A *lex specialis* elve alkalmazásához előbb azonosítani kell az állítólagos normakonfliktust, vagyis, hogy ugyanarra a jogviszonyra és ugyanarra a kérdésre ad-e eltérő választ a különös szabály, ugyanis a feladatmegosztást rögzítő rendelkezés és az adatok nyilvánosságát szabályozó norma eltérő tárgyát nem célszerű pusztán elnevezés alapján összemosni.[33] A korlátozás önálló vizsgálatához Székely, Somody és Szabó egymásra épülő döntéstámogatási módszere is értelmezési támpontot ad.[34] A különös rendelkezés és az Infotv. viszonyára a 4/2021. (I. 22.) AB határozat ad konkrét példát. A paksi beruházás nyilvánossági szabályának értelmezésekor a testület nem fogadta el az Infotv. egészének félretételét, az alvállalkozók esetében pedig a közfeladatot ellátó jellegre alkotmányos követelményt állapított meg.[35] Az esetből a társaságok számára az a módszertani tanulság vonható le, hogy a korlátozó szabály tárgyi és személyi hatályát egyaránt igazolni kell, a különleges beruházásra hivatkozás ugyanis nem helyettesíti annak bemutatását, hogy éppen a megkeresett társaság és a kért adatkör miért tartozik a rendelkezés alá.

Véleményem szerint a különös szabály elsődlegessége csak a rendelkezés tényleges tartalmának vizsgálatával állapítható meg. Amennyiben az ágazati törvény meghatározott adatfajta megismerését korlátozza, annak hatályát és alkotmányos indokát kell értékelni – ha azonban csupán a döntés-előkészítés vagy a tulajdonosi joggyakorlás felelősét jelöli ki, külön érvelést igényel, hogy ebből miért következne más szerv adatkiadási kötelezettségének kizárása. Az Infotv. alapján rendelkezésre álló adat megismeréséről és a szakpolitikai döntés meghozataláról szóló hatáskörök így egymás mellett is értelmezhetők. De Negri átláthatósági elemzése e vizsgálathoz a társasági működés és a nyilvánossági kötelezettség elkülönítésének szempontját adja.[36]

[33] Alaptörvény I. cikk (3) bekezdés; Infotv. 26. § (1) bekezdés, 27. § (2), (5)–(6) bekezdés, 30. § (5) bekezdés. A lex specialis alkalmazásának itt bemutatott elhatárolása a dolgozat saját jogértelmezési következtetése.
[34] SZÉKELY I. – SOMODY B. – SZABÓ M. D.: *i. m.* 17–20. o.
[35] 4/2021. (I. 22.) AB határozat, rendelkező rész 1. pont; Indokolás [62]–[68], [73]–[74], [99].
[36] DE NEGRI: *i. m.* 84–86. o.

II.2. Adatkezelői szerepek és a társasági működés adatai

A GDPR adatkezelő-fogalma az adatkezelés céljainak és eszközeinek meghatározásához kapcsolódik, míg a közös adatkezeléshez közös meghatározás, az adatfeldolgozói szerephez pedig más adatkezelő nevében végzett kezelés szükséges (önmagában a tulajdonosi kapcsolat vagy az iratok átadása nem teszi a szereplőket közös adatkezelővé). Az Infotv. információszabadsági kötelezettjének azonosításakor pedig a hazai törvény szerinti adatfajtát és kötelezettséget kell vizsgálni. A két rendszer terminológiáját nem lehet úgy felcserélni, hogy egy GDPR szerinti szerepmegjelölés önmagában eldöntse az adatigénylés sorsát.[37, 38] A különböző adatkezelési célok feltárásában Váradi elemzésének célhoz kötöttségi és adattakarékossági megközelítése is irányadó.[39] E szempontokra tekintettel egy szerződés életútját célszerű végig követni a keletkezéstől a megőrzésen át a kiadásig.

Az eredeti ügyleti példány, a tulajdonosnak megküldött beszámoló és a nyilvános másolat között lehetnek tartalmi eltérések, ezért az adatkiadás előkészítőjének a megfelelő példányt kell azonosítania, és a védett tartalmat azon a változaton kell ellenőriznie, amely ténylegesen az igénylőhöz kerül. A gyakorlati adatáramlás feltérképezése egyúttal az incidenskezelés előfeltétele, mert a társaságnak tudnia kell, mely szervezeti egység őrzi a szerződést, ki készít róla nyilvános másolatot, milyen szolgáltató üzemelteti a levelezést, és hol találhatók a továbbítás naplói.

A minisztérium, a társaság és az informatikai szolgáltató közötti feladatmegosztás csak e konkrét műveletek alapján értékelhető. Álláspontom szerint az adatigénylési szabályzatnak ezért az iratok felkutatásáért, jogi minősítéséért és technikai kiadásáért felelős szereplőket is meg kell neveznie, a tisztviselő bevonási pontjaival együtt. A társaság működésében a személyzeti, szerződéses és gazdálkodási adatok külön vizsgálati csoportot alkotnak: a köztulajdonú társaságokra vonatkozó törvény meghatározott vezetői és javadalmazási adatokat közzétenni rendel, míg a közpénzekből finanszírozott szerződések nyilvánosságát az Infotv. szabályai is érintik. E rendelkezésekből azonban nem következik, hogy valamennyi munkavállalói irat vagy teljes szerződéses melléklet korlátozás nélkül hozzáférhető.

[37] GDPR 4. cikk 7–8. pont, 26. és 28. cikk; Infotv. 3. § 9. pont, 26. § (1) bekezdés.
[38] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 101–102. o.
[39] VÁRADI: *i. m.* 43–44. o.

A közzétételre előírt adatkört és az egyedi igény alapján megismerhető adatokat egyaránt a rájuk irányadó normákból kell levezetni.[40, 41] Célszerű előzetesen azonosítani a rendszeresen felmerülő nyilvános adatokat, és elkülöníteni azokat a magánelérhetőségektől vagy technológiai részletektől, ami a későbbi egyedi vizsgálatot is segítheti, mivel az adatvédelmi tisztviselő feladata elsősorban a személyes adatok kezeléséhez kapcsolódik, a közpénzügyi és társasági jogi kérdésekben más szakmai területekkel működik együtt.

III. AZ ADATVÉDELMI TISZTVISELŐ JOGÁLLÁSA ÉS SZERVEZETI SZEREPE

III.1. Kijelölés, függetlenség és a feladatellátás feltételei

A GDPR 37. cikke meghatározza az adatvédelmi tisztviselő kötelező kijelölésének eseteit. Ezek közé tartozik a közhatalmi vagy egyéb közfeladatot ellátó szervek adatkezelése, továbbá meghatározott, nagy mértékű rendszeres és szisztematikus megfigyelést, illetve különleges vagy büntetőjogi személyes adatok nagy mértékű kezelését magában foglaló főtevékenység. A társaság esetében az adott tevékenység és jogállás vizsgálata szükséges, a köztulajdon megállapítása ugyanis önmagában nem helyettesíti a 37. cikk szerinti minősítést. A tisztviselő szakmai alkalmasságát a jog és a gyakorlat ismerete, valamint feladatainak ellátására való képessége alapján kell értékelni.[42]

Szabó Endre Győző a tisztviselői intézmény elemzésében a jogszabályi szerep és a szervezeti elvárások közötti eltérés veszélyére hívja fel a figyelmet, és a tisztviselőt az elszámoltathatóságot támogató belső ellenőrzéshez kapcsolja.[43] Török Tamás Sándor ugyancsak a kockázatok és a megfelelés igazolhatósága felől értelmezi a tisztviselő helyét[44], e két megközelítés közös eleme a tényleges működés ellenőrizhetősége. Ebből fakadóan a közfeladatot ellátó társaságnál a kijelölő okirat mellett azt is vizsgálni kell, hogy a tisztviselő hogyan jut az ügyek adataihoz, miként közli véleményét, és ki hajtja végre a szükséges intézkedést.

[40] 2009. évi CXXII. törvény, 2. § (1)–(3) bekezdés; Infotv. 26. § (2) bekezdés, 27. § (3) bekezdés.
[41] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.
[42] GDPR 37. cikk (1)–(6) bekezdés.
[43] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 3–4. o.
[44] TÖRÖK T. S.: Az adatvédelmi tisztviselő pozíciója és szerepe a mesterséges intelligenciáról szóló rendelet kockázati rendszerében. In *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok* 2024/III. 18–20. o.

E feltételek teljesülését a névleges kijelölés önmagában nem biztosítja. A közös vagy külső tisztviselő alkalmazása szervezési lehetőség, amelynek értékét az elérhetőség és a tényleges kapacitás adja. Véleményem szerint a szerződés megkötésekor az adatvédelmi tanácsadás általános megnevezése mellett az ügyek továbbítását, a sürgős incidensjelzés módját és a helyettesítés feltételeit is rögzíteni kell, különös tekintettel az adatigénylési határidőkre és az incidensvizsgálat gyorsaságára. Aggályosnak tartom az olyan konstrukciót, amelyben a tisztviselő a társaság irataihoz csak a vezetői döntés után jut hozzá, mert a szakmai hozzáférés késedelme éppen a megelőző tanácsadás lehetőségét szűkíti le.

A GDPR 38. cikke szerint a tisztviselőt megfelelően és időben be kell vonni a személyes adatok védelmét érintő ügyekbe. Biztosítani kell feladatainak ellátásához az erőforrásokat, az adatokhoz és műveletekhez való hozzáférést, valamint szakértelmének fenntartását. Feladatainak ellátásával kapcsolatban nem utasítható: e feladatok ellátása miatt nem bocsátható el és nem sújtható szankcióval, továbbá közvetlenül a legfelső vezetésnek tartozik felelősséggel. A függetlenség így a szakmai vélemény kialakításának és közlésének intézményi feltétele, miközben a tisztviselő a szervezeten belül működik.[45] A vezető és a tisztviselő közötti szakmai eltérést célszerű dokumentálni, ami új jóváhagyási jogot nem hoz létre, azonban ellenőrizhetővé teszi a döntés indokait. Az európai adatvédelmi kézikönyv is az önálló ellenőrzési és tanácsadói funkcióval kapcsolja össze a tisztviselő helyzetét.[46]

Szabó a feladatellátás anyagi és személyi feltételeit, valamint a műveletekhez való hozzáférést a tisztviselő működésének fontos biztosítékaként tárgyalja.[47] Az adatigénylés teljesítésére nézve ebből azt a következtetést vonom le, hogy a tisztviselőnek a bizonytalan esethez szükséges példányt és a tervezett közlés körülményeit időben meg kell kapnia, jóllehet nem indokolt minden irat előzetes személyes ellenőrzését általános követelménnyé tenni. Ha az ügyintéző csak az elküldés után továbbítja a fájlt, az utólagos vélemény feltárhatja a már bekövetkezett hibát, az adott közlés megelőzésében azonban értelemszerűen nem tölthet be szerepet. A belső és a külső ellenőrzés függetlenségét ugyanakkor külön kell kezelni.

[45] GDPR 38. cikk (1)–(3) bekezdés.
[46] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 175–178. o.
[47] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 7. o.

Jóri András a korábbi adatvédelmi biztosi intézmény elemzésében a felügyelő szerv függetlenségének garanciális jelentőségét vizsgálta.[48] E történeti intézményi megközelítés nem ruház hatósági jogkört a társaság tisztviselőjére. A tisztviselő a szervezeten belül tanácsol és ellenőriz, míg a felügyeleti hatóság külső jogérvényesítési feladatot lát el – a szakmai autonómia mindkettő működésében jelentős, azonban eltérő hatáskörrel és eltérő jogkövetkezményekkel érvényesül.

III.2. Tanácsadás, összeférhetetlenség és adatkezelői felelősség

A tisztviselő feladatai közé tartozik a tájékoztatás és tanácsadás, a megfelelés ellenőrzése, az adatvédelmi hatásvizsgálattal kapcsolatos tanácsadás és ellenőrzés, továbbá a felügyeleti hatósággal való együttműködés és kapcsolattartás. A GDPR 39. cikke a kockázatokra figyelemmel végzett feladatellátást ír elő, amely alapján az adatigénylési ügyben elsősorban a személyes adatok minősítéséhez, a közlés jogalapjához, az adatbiztonsághoz és a folyamat megfelelőségéhez kapcsolódó közreműködés vezethető le. A teljes információszabadsági ügyintézés automatikus átruházását a rendelet nem írja elő.[49] Az adatigénylési folyamatban a tisztviselő kockázathoz igazított közreműködését Török elszámoltathatósági értelmezése is segíti.[50] Ennek alkalmazását három ponton látom indokoltnak: a személyes adatok jogi minősítésében, a kész kiadási változat ellenőrzési módszerének kialakításában, és a visszatérő hibák értékelésében.

E pontok összefüggnek, azonban eltérő munkát kívánnak, így a tisztviselő például javasolhatja a magánelérhetőségek eltávolítását és a technikai ellenőrzést, miközben az iratgazda készíti el a másolatot, a társaság döntésre jogosult vezetője pedig a teljesítésről határoz. A társaság működésében ezért célszerű elkülöníteni az ügyintéző, a jogi szakértő, az iratgazda és a tisztviselő szerepét. Az iratgazda feltárja a tényleges adattartalmat, a jogi terület vizsgálja a nyilvánossági és korlátozási szabályokat, a tisztviselő ellenőrzi a személyes adatok kezelésének feltételeit, az adatkiadásról pedig a társaság erre jogosult szereplője dönt. A munkamegosztás azonban nem jelent egymástól elszigetelt véleményezést – a technikai kitakarás például csak akkor lesz helyes, ha a jogi minősítésből egyértelműen kiderül, milyen adatokat kell eltávolítani.

[48] JÓRI A.: Az adatvédelemért és az információszabadságért felelős biztos intézményéről. In *Fundamentum* 2010/2. 25–26. o.
[49] GDPR 39. cikk (1)–(2) bekezdés.
[50] TÖRÖK: *i. m.* 18–20. o.

A tisztviselő más feladatot is elláthat, de az adatkezelőnek biztosítania kell az összeférhetetlenség hiányát. Az Európai Unió Bírósága az *X-FAB Dresden-ügyben* hangsúlyozta, hogy ilyen konfliktust okozhat az adatkezelés céljainak és eszközeinek meghatározásával járó más feladat. A megítélés az adott szervezet tevékenységétől, felépítésétől és belső szabályaitól függ, és nem oldható meg minden esetben egy munkaköri cím alapján – a tényleges döntési jogosultság és az ellenőrzési feladat kapcsolatát ezért az adott szervezet működésére tekintettel szükséges megítélni.[51] Szabó tanulmánya az egyéb feladatok mellett ellátott tisztviselői munkánál ugyancsak az összeférhetetlenség elkerülését hangsúlyozza.[52]

Mindezek alapján az adatigénylések körében az ügyintézésben való részvételt és a döntési hatáskör összpontosítását eltérő súlyú kérdésnek tartom. Amennyiben a tisztviselő javaslatot tesz a védendő személyes adatokra, az a tanácsadói szerepébe illeszkedik, ha viszont egyedül ő határozza meg a teljes adatkezelési folyamatot, ő hagyja jóvá a közlést, majd saját döntése megfelelését is ő ellenőrzi, az összeférhetetlenség kockázata lényegesen nagyobb. A GDPR 24. cikke az adatkezelő feladatává teszi a megfelelő intézkedések végrehajtását és a megfelelés igazolását (az incidens hatósági bejelentésének kötelezettje ugyancsak az adatkezelő), ezért a tisztviselő saját munkavégzésének megítélése külön jogi kérdése, amelyet nem lehet azonosítani a társaság GDPR szerinti megfelelési kötelezettségével.[53]

IV. A KÖZÉRDEKŰ ADATIGÉNYLÉSEK TELJESÍTÉSE

IV.1. Az igény azonosítása és az eljárás keretei

Az Infotv. 28. §-a szerint az igény szóban, írásban vagy elektronikus úton nyújtható be. A törvényes ügyintézés kezdőpontja a kérés tartalmának és beérkezésének rögzítése. Az igénylőtől nem követelhető meg, hogy a társaság belső irattári rendjét vagy a kért adatok pontos jogi minősítését ismerje – amennyiben a kérés nem egyértelmű, a törvény szerinti pontosításra kell felhívni.[54]

[51] Európai Unió Bírósága: C-453/21. sz. X-FAB Dresden ügy, 2023. február 9., ECLI:EU:C:2023:79, 38–46. pont, különösen 44. és 46. pont; GDPR 38. cikk (6) bekezdés.
[52] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 7–8. o.
[53] GDPR 24. cikk (1) bekezdés, 33. cikk (1) és (3) bekezdés, 38–39. cikk. SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 3–4, 8. o.
[54] Infotv. 28. § (1) és (3) bekezdés.

A társaság feladata ekkor a bizonytalanság megjelölése és a tisztázható adatkör körülírása, melynek körében az igény teljesítése nem tehető indokolatlanul bonyolult belső terminológia használatától függővé. Az eljárás célját az információs erőfölény csökkentése határozza meg, amint arra Székely korábban ismertetett megközelítése is utal. Ebből azt a következtetést vonom le, hogy az adatkérés pontosításának a megismerhetőség elősegítését kell szolgálnia. Az adatigényléssel érintett adatkörök tekintetében a társaság megjelölheti a kezelhető időszakot vagy az azonosítható szerződéscsoportot, és jelezheti, milyen rögzített adatokkal rendelkezik, ami csökkentheti a félreértést anélkül, hogy az igénylőre hárítaná a belső nyilvántartási rendszer ismeretét (a társaság számára eképpen a lehető legkorábban láthatóvá válik, mely szervezeti egységek bevonása szükséges).

Az igény pontosítása az ügy szempontjából szükséges kérdésekre szorítandó, az egyértelmű kérés pedig pusztán terjedelme miatt nem tekinthető értelmezhetetlennek – jóllehet az Infotv ebben az esetben lehetővé teszi az adatigénylésre nyitva álló határidő egy alkalommal, 15 nappal történő meghosszabbítását.[55] Fontos továbbá, hogy a kész irat, a létező adat és az új szakmai értékelés elkülönítése szükséges – utóbbi eltérő megítélése a már rögzített adatok kiadását nem zárja ki. Az igénylő személyes adatainak kezelése az igény teljesítéséhez szükséges körre korlátozódik, az Infotv. alapján a név és a kapcsolattartást lehetővé tevő elérhetőség hiánya a teljesítési kötelezettséget érinti, ebből azonban nem következik általános okmányellenőrzési jog. A törvény meghatározott időn belüli ismételt, változatlan adatokra irányuló igényekre külön szabályt tartalmaz, de ez sem teszi megengedetté a korlátlan személyes profil létrehozását.[56]

A teljesítés főszabály szerint az igény beérkezésétől számított legfeljebb tizenöt napon belül esedékes. Nagy terjedelmű vagy nagyszámú adatot érintő igény, illetve a közfeladat ellátásához szükséges munkaerőforrás aránytalan igénybevétele esetén a határidő egyszer, tizenöt nappal meghosszabbítható, az igénylő határidőben történő értesítésével (lásd az előző bekezdésben). A pontosítás és egyes törvényben meghatározott megkeresések saját határidő-számítási szabályait külön kell alkalmazni.

[55]Infotv. 29. § (2) bekezdés.
[56]Infotv. 28. § (2) bekezdés, 29. § (1a)–(1b) bekezdés; GDPR 5. cikk (1) bekezdés b)–c) és e) pont.

A költségtérítés jelenlegi rendszere az adathordozó és a kézbesítés jogszabály szerint figyelembe vehető költségeire épül, az ügyintéző munkaideje pedig nem számolható el a korábbi szabályozásból átvett általános díjtételként.[57] A nyilvántartás személyesadat-tartalmát illetően Váradi a szükségtelen adatok felhalmozásának elkerülését és a célhoz kötöttséget emeli ki.[58] Az adatigénylő adatainak kezelésénél ebből következik az ügyadat és a személyes kapcsolattartási adat megkülönböztetése, hiszen a teljesített adatkör, a válasz dátuma és a kitakarás indoka később személyazonosítás nélkül is értékelhető lehet. Az igénylő elérhetőségének megőrzési szükségletét ezzel szemben az adott eljárás, az esetleges jogorvoslat és a törvényi törlési kötelezettség alapján kell megítélni. A statisztikai elemzéshez nem indokolt változatlanul megtartani minden ügy teljes levelezését.

IV.2. Nyilvános személyes adatok, közpénz és üzleti titok

Az Infotv. 26. § (2) bekezdése a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy meghatározott adatait közérdekből nyilvánossá teszi. A társasági vezetők és más, törvényben meghatározott személyek javadalmazási adataira a köztulajdonú társaságokra vonatkozó szabályok is irányadók. A nyilvánosság vizsgálatának alapja ezért a személy feladata, a kért adat típusa és az adott törvényi rendelkezés. Egy munkavállalói adat attól még nem válik kiadhatóvá, hogy az érintett munkabérét közvetetten közpénzből finanszírozzák, így a releváns nyilvánossági előírást az adott adat tekintetében kell megtalálni.[59] A közérdekből nyilvános személyes adatok terjesztésére is irányadó a célhoz kötöttség – a törvény az adatok honlapon történő közzétételére külön előírásokat követel meg, ezért az egyedi adatigénylés teljesítését és az internetes közzétételt nem célszerű azonos műveletként kezelni. Egy jogosultnak küldött válasz kötelezettségét nem lehet pusztán egy tervezett későbbi honlapfrissítéssel kiváltani. Fordítva pedig az egyedi kiadásra alkalmas irat nem feltétlenül tehető ugyanabban a formában, korlátlan időtartamra és valamennyi járulékos személyes adattal együtt a társaság honlapjára.[60]

[57] Infotv. 28. § (3) bekezdés, 29. § (1)–(2b), (3) és (5) bekezdés. A költségtérítésnél a hatályos törvényben meghatározott költségelemekből kell kiindulni.
[58] VÁRADI: *i. m.* 43–44. o.
[59] Infotv. 26. § (2) bekezdés; 2009. évi CXXII. törvény, 2. § (1)–(2) bekezdés. BENDIK – PÉTERFALVI: *i. m.* 55–57. o.
[60] Infotv. 26. § (2) bekezdés, 30. § (2) bekezdés; GDPR 5. cikk (1) bekezdés b) pont. BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

Az *Endemol Shine Finland-ügy* ezen, és további tanulsága, hogy a közlés formája nem mentesít az adatvédelmi vizsgálat alól, a Bíróság ugyanis az érintett büntetőjogi adatok szóbeli közlését is adatkezelésként értékelte a rendelet hatályába tartozó nyilvántartási környezetben. Az ügyben vizsgált korlátlan hozzáférés nem jelenthető ki általánosan megengedettnek a nyilvántartás nyilvánosságára hivatkozva. E döntés saját tárgyából nem következik viszont, hogy magyar közérdekű adatigényléshez minden esetben személyes érdekeltséget kellene igazolni. A döntés jelentőségét a közlés adatkezelési természetében és az adatfajta szerinti értékelésben látom.[61]

Az üzleti titok védelmének törvényi feltétele a gazdasági tevékenységhez kapcsolódó információ titkossága, vagyoni értéke és a titokban tartás érdekében tanúsított elvárható magatartás. Az Infotv. 27. § (3) bekezdése ugyanakkor a közpénzek felhasználásával és a közvagyonnal összefüggő meghatározott adatok tekintetében kizárja az üzleti titokra hivatkozó általános elzárást. A védett ismeretek aránytalan sérelmére vonatkozó szabály és a nyilvános közpénzügyi adatok kiadásának kötelezettsége együtt vizsgálandó, a szerződéses titoktartási kikötés pedig önmagában nem írhatja felül a törvényből következő nyilvánosságot.[62] A kiadás előkészítésekor ezért adatonként kell értékelni a szerződés tartalmát, tekintettel arra, hogy az ellenérték, a teljesítés tárgya és a szerződő fél kiléte más funkciót tölt be, mint egy részletes gyártási eljárás vagy nem nyilvános algoritmusleírás. Az üzleti partner álláspontja segítheti a tényleges titokvédelmi körülmények feltárását, de a döntési felelősség nem helyezhető át hozzá – indokolt megkérdezni, mely részek titkosak, hogyan őrzik titkosságukat, és milyen konkrét, aránytalan (!) érdeksérelmet okozna a megismerés. Az egész szerződésre alkalmazott, tartalom nélküli üzleti titokként történő megjelölést elégtelen indokolásnak tartom mindamellett, hogy – gyakorlati tapasztalataim alapján – erre az adatkezeléssel érintett fél számtalan esetben előszeretettel hivatkozik.

A különös társasági szabályok vizsgálatára konkrét példa a 2009. évi CXXII. törvény 3/A. §-a. A rendelkezés bizonyos külföldi beruházási, külügyi és nemzetközi szerződéses adatok megismerésénél külön feltételeket, miniszteri véleményezést és határidő-számítást állapít meg. Ebből nem vezethető le valamennyi társasági szerződés általános titkossága, így az alkalmazás előtt a tárgyi hatályt, a megjelölt közérdek veszélyeztetését, a megtagadás fennálló indokát és időbeli korlátját kell azonosítani.

[61] Európai Unió Bírósága: C-740/22. sz. Endemol Shine Finland ügy, 2024. március 7., ECLI:EU:C:2024:216, 26–39. és 56–61. pont.

[62] Az üzleti titok védelméről szóló 2018. évi LIV. törvény, 1. § (1)–(2) bekezdés; Infotv. 27. § (3) bekezdés. DE NEGRI: *i. m.* 84–86. o.

A *lex specialis* elv itt konkrét törvényi előíráshoz, nem a társaság általános működési sajátosságához kapcsolódik.[63] A társasági forma és a nyilvánossági kötelezettség összefüggését De Negri elemzése is a közvagyoni működésre tekintettel tárgyalja,[64] ami a különös szabály határainak megállapításához általános értelmezési támpontot ad.

IV.3. A korlátozás indokolása és a részleges teljesítés

Az Infotv. 27. § (5)–(6) bekezdése alapján a döntés megalapozását szolgáló adatok megismerhetőségére sajátos időbeli és tartalmi szabályok vonatkoznak. A tízéves időtartam ismerete önmagában nem elegendő, mert azonosítani kell a ténylegesen előkészített döntést és az adat ennek megalapozásában betöltött szerepét. A döntés után a törvényben meghatározott további feltételek alapján vizsgálandó a korlátozás fenntartása. A Kúria összefoglaló véleménye is a tartalmi megítélés, a konkrét döntés és a védett működési érdek vizsgálatának jelentőségét emeli ki.[65] A 4/2021. (I. 22.) AB határozat a nyilvánosságkorlátozó ágazati szabály mellett is megköveteli az adatokhoz kapcsolódó érdekek vizsgálatát és az elutasítás tartalmi indokolását. A döntés megalapozását szolgáló adatoknál a konkrét döntési kapcsolat és az érdemi bírói kontroll jelentőségét hangsúlyozza.[66] A társaság gyakorlatában ezért a döntési eljárás folyamatban létére történő hivatkozás önmagában kevés, a kiadni kért részlet szerepét ugyanis szintén be kell mutatni. Egy műszaki alternatíva előzetes értékelése és a már kifizetett összeg például ugyanabban a feljegyzésben szerepelhet, mégsem feltétlenül ugyanaz az elzárási indok vonatkozik rájuk.

Egy minisztériumnak megküldött társasági feljegyzésnél például tisztázni kell, mely döntés előkészítéséhez kapcsolódott, megtörtént-e már a döntés, és a dokumentum mely része tartalmaz tényleges előkészítő megfontolást. A tényadat, a szerződés összege és a belső alternatívák értékelése ugyanabban az iratban is eltérően ítélhető meg, ezért a „belső használatra” felirat vagy az irat továbbításának címzettje nem pótolja ezt az elemzést. Véleményem szerint az elutasítás indokolásának legalább a döntési folyamatot és az adott tartalommal összefüggő védett érdeket azonosíthatóvá kell tennie, mindazonáltal e követelmény nem járhat a jogszerűen védett részletek felfedésével.

[63] 2009. évi CXXII. törvény, 3/A. § (1)–(4) bekezdés.
[64] DE NEGRI: *i. m.* 84–86. o.
[65] Infotv. 27. § (5)–(6) bekezdés; Kúria: *i. m.* [65] bekezdés, 16. o.
[66] 4/2021. (I. 22.) AB határozat, Indokolás [83]–[90], [96]–[97].

Az Infotv. 30. § (1) bekezdése szerint a meg nem ismerhető adatot a másolaton felismerhetetlenné kell tenni, ami a vegyes iratoknál a részleges teljesítés törvényi alapját adja. Az értékelés során különíthető el a közérdekű adat, a közérdekből nyilvános személyes adat, a más jogcímen védett személyes adat és az egyéb korlátozott információ. A társaság nem köteles a védett adatot azért felfedni, mert az ugyanabban a dokumentumban szerepel, de a védett adat jelenléte nem igazolja automatikusan a teljes irat visszatartását sem. A közlés formájánál az igénylő kívánságát is a törvény keretei között figyelembe kell venni.[67, 68] Szádeczky és Szőke a biztonsági követelmények és a nyilvánosság viszonyában is a jogilag meghatározott hozzáférésből indulnak ki.[69] Ezt a részleges teljesítésre alkalmazva a jogi és a technikai ellenőrzés két külön kérdésre válaszol – a jogi minősítés megmondja, mely adatot kell eltávolítani, a technikai ellenőrzés azt igazolja, hogy az eltávolítás a kiadott példányban valóban megtörtént. Ha a két ellenőrzés csak ugyanazon munkatárs emlékezetére épül, a hiba felismerésének esélye csökkenhet. Indokolt ezért az eltávolítandó adatkör rövid írásbeli rögzítése és a kész példány második ellenőrzése. A jogi minősítés és a technikai eltávolítás eredményének egyezését külön ellenőrizni szükséges (*szakavatott kollégák esetében is előfordul, hogy a kitakarás eszközéül használt fekete téglalap az elektronikus dokumentumban törölhető marad, így a tartalom kereséssel sajnos elérhető marad...*).

A kiadás biztonsága érdekében ezért javasolt, hogy a kiadásra szánt másolatot egy másik munkatárs nyissa meg, ellenőrizze (’próbálja ki’) a kitakarás(ok)kal érintett mellékleteket és a dokumentumtulajdonságokat. Az ellenőrzés terjedelmét az alkalmazott fájlformátumhoz és az adatok érzékenységéhez kell igazítani, és a vizsgálatnak a végleges, ténylegesen elküldött változatra kell kiterjednie.

IV.4. Tisztviselői közreműködés, dokumentálás és jogorvoslat

A tisztviselő bevonásának legfontosabb pontja a bizonytalan személyesadat-minősítés, a különleges adatok megjelenése és a szokatlan közlési kockázat. Egy már közzétett szerződés pontos hivatkozással történő megküldéséhez rendszerint kisebb szakmai vizsgálat szükséges, mint egy munkavállalókkal kapcsolatos belső jelentés kiadásához.

[67] Infotv. 30. § (1)–(2) bekezdés.
[68] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.
[69] SZÁDECZKY – SZŐKE: *i. m.* 24–26, 35–36. o.

A kockázathoz igazított bevonásnak ugyanakkor nem lehet az a következménye, hogy a tisztviselő a problémás ügyekről sem szerez időben tudomást (a GDPR szerinti korai bevonás és az Infotv. szerinti belső ügyintézési szabályzat követelménye e ponton egyébként egymást erősíti).[70] A tisztviselő tanácsadó és ellenőrző szerepének korábban bemutatott szakirodalmi értelmezése az ügykezelésben azt kívánja meg, hogy a szakmai vélemény tárgya azonosítható legyen.[71] Tekintettel arra, hogy a ”GDPR szempontból rendben” megállapítás önmagában nem mutatja meg, mely fájlt és mely adatokat vizsgálták, a véleménynek a döntéshez szükséges részletességgel kell megjelölnie az értékelt személyes adatot, a közlési jogcímet és a javasolt védelmet. A társaság vezetője így a vélemény ismeretében dönthet, az ügyirat pedig később megmutatja, hogy a végrehajtás követte-e a szakmai javaslatot.

A teljesítés nyilvántartásában a kért adatkör, a határidő, az iratgazda, a kiadási döntés indoka, az alkalmazott kitakarás és a továbbítás ténye rögzítése indokolt tekintettel arra, hogy a visszakereshetőség a későbbi jogorvoslatot és az esetleges incidens kivizsgálását is segíti (nem mellesleg az éves NAIH-adatszolgáltatás követelménye). Ez álláspontom szerint nem teszi azonban szükségessé a korlátlan személyesadat-megőrzést – az igénylő elérhetőségének kezelési idejét a törvényi és eljárási szükséglethez kell kötni. A nyilvános válasz és az indokolást tartalmazó belső ügyirat elkülönítése útján a társaság a bizonyítás szempontjait a kiadott másolat tartalmától függetlenül is kezelheti. Az elutasításról az igénylőt a törvényi határidőn belül, indokolással és a jogorvoslati lehetőségekről szóló tájékoztatással kell értesíteni, mérlegelést engedő rendelkezés alkalmazásakor a megtagadási ok szűk értelmezése és a nyilvánossághoz fűződő közérdek súlya is vizsgálandó. A továbbiakban az Infotv. 31. §-a szerint az elutasítás jogszerűségét és indokait az adatkezelő bizonyítja, a költségtérítés megalapozottságára ugyancsak őt terheli bizonyítás.

A hatósági vizsgálat és a bírósági út lehetőségeit, valamint azok határidőit pontosan kell közölni, mert a késedelmes vagy hiányos válasz a megismerési jog gyakorlását közvetlenül nehezíti.[72] A külső jogvédelem jelentőségét Jóri intézményi elemzése történeti összefüggésben is megvilágítja – a független felügyelet az információs jogok gyakorlati érvényesülésének fontos garanciája.[73]

[70] GDPR 38. cikk (1) bekezdés, 39. cikk (2) bekezdés; Infotv. 30. § (6) bekezdés.
[71] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 3–4, 7–8. o.
[72] Infotv. 30. § (3) és (5) bekezdés, 31. § (1)–(5) bekezdés, 31/A–31/C. §, 52. § (1) bekezdés.
[73] JÓRI: *i. m.* 25–26. o.

A tisztviselő belső kontrollja ezért a jogorvoslati lehetőséghez kapcsolódó előkészítést támogathatja, de nem váltja ki a hatóság vagy a bíróság vizsgálatát. A válasz jogorvoslati tájékoztatását annak alapján kell megszerkeszteni, milyen döntés született és milyen eljárás kezdeményezhető, a tisztviselő elérhetőségének feltüntetése ugyanis önmagában nem pótolja e tájékoztatást. A társaság álláspontjának védhetőségét véleményem szerint az ügyre szabott indokolás adja, amely a hivatkozott normaszöveg mellett a kért adat és a korlátozás kapcsolatát, valamint a részleges teljesítés vizsgálatát is bemutatja. A tisztviselő szakmai véleménye értékes része lehet a belső iratanyagnak, de a társaság saját döntését nem helyettesíti. A jogorvoslati szakasz számára a feltárt tények, a minősítési indokok és a kiadott vagy visszatartott adatkör így együttesen válnak rekonstruálhatóvá, ami az elutasítás jogszerűségének érdemi ellenőrzését is elősegíti.

V. ADATVÉDELMI INCIDENSEK FELISMERÉSE ÉS BEJELENTÉSE

V.1. Az incidens felismerése, a tudomásszerzés és a határidő

A GDPR 4. cikk 12. pontja szerint az adatvédelmi incidens *a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.* A fogalom tehát nem korlátozódik adatlopásra, hiszen egy téves címzés a bizalmasságot, az iratban szereplő adatok jogosulatlan módosítása az integritást, az adatok elvesztése pedig a rendelkezésre állást érintheti. A személyes adatok érintettségét minden eseménynél külön meg kell állapítani: tisztán üzleti, személyhez nem kapcsolódó információ sérülése önmagában nem GDPR szerinti incidens.[74] Szádeczky és Szőke az információbiztonság fogalmában a bizalmasság, sértetlenség és rendelkezésre állás hármas követelményét különítik el.[75]

Ennek alapján a társaság vizsgálata nem szűkíthető a ”kikerült-e adat” kérdésére. Ha az egyetlen példányban őrzött személyes adat elveszik, a hozzáférhetőség sérülése jogosulatlan címzett nélkül is bekövetkezhet, ha viszont egy nyilvános gazdálkodási táblázat átmenetileg nem érhető el, először tisztázni kell, érint-e az esemény személyes adatot.

[74] GDPR 4. cikk 12. pont, 32. cikk (1) bekezdés b)–c) pont.
[75] SZÁDECZKY – SZŐKE: *i. m.* 25–26. o.

A technikai esemény és a GDPR szerinti incidens közötti különbség az adatok és a bekövetkezett következmény együttes vizsgálatával állapítható meg. Az adatigénylés teljesítésekor a jogszerűen kiadható adat közlése nem válik incidenssé pusztán azért, mert az érintett a nyilvánosságot sérelmesnek tartja – a kiadási döntést és a biztonság sérülését ezért külön kell értékelni. Ha a társaság a törvény alapján nyilvános vezetői javadalmazást adja ki a megfelelő formában, az adatkezelés jogszerű lehet, amennyiben azonban ugyanazzal a fájllal egy nem nyilvános egészségügyi melléklet is eljut az igénylőhöz, a védett rész jogosulatlan közlése incidensvizsgálatot kíván. Egy ügyben szabályos teljesítés és hibás járulékos adatközlés egyszerre is történhet, mely reláció kapcsán, az adat személyes jellegének és nyilvánosságának külön értékeléséhez a Bendik–Péterfalvi-tanulmány fogalmi megközelítése is valamelyest támpontot nyújt.[76]

A GDPR 33. cikk (1) bekezdése szerint az adatkezelő az incidenst indokolatlan késedelem nélkül, és ha lehetséges, a tudomásszerzéstől számított hetvenkét órán belül jelenti be, kivéve, ha az valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira. A hetvenkét órán túli bejelentéshez a késedelem indokait is mellékelni kell, a határidő ugyanis órákban meghatározott követelmény – a hétvége vagy a munkatárs szabadsága nem hoz létre általános szünetelési időt (*megjegyzés: a NAIH gyakorlatában a Pp. szerinti határidőszámítás elfogadására volt már példa*). A bejelentési kötelezettség az adatkezelőt terheli, nem csak az ügyet később megismerő tisztviselőt.[77] Szabó Endre Győző és Révész Balázs az incidensjelzés intézményét a következmények enyhítését szolgáló védelmi mechanizmusként értelmezik.[78] E felfogás gyakorlati értékét a társasági adatkiadásnál abban látom, hogy az első jelzésnek már cselekvést kell kiváltania. A fájl nyilvános elérhetőségének korlátozása, a téves címzett megkeresése és a kiadott mellékletek azonosítása sok esetben a teljes jogi értékelés befejezése előtt megkezdhető, így a gyors intézkedés és az ellenőrzött bejelentés egymást kiegészítő feladat, a tényfeltárás közben is folytatható a kár enyhítése.

Az Európai Adatvédelmi Testület 9/2022. számú iránymutatása a tudomásszerzést azzal kapcsolja össze, hogy az adatkezelő észszerű bizonyossággal megállapíthatja a személyes adatok sérülését okozó biztonsági esemény bekövetkezését. A kezdeti gyanú tisztázása rövid vizsgálatot indokolhat, mindazonáltal nem adhat alapot a határidő mesterséges késleltetésére.

---

[76] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.
[77] GDPR 33. cikk (1) bekezdés.
[78] SZABÓ E. Gy. – RÉVÉSZ B.: Adataink biztonságban – adatainkban a biztonság? In *Információs Társadalom* 2017/1. 52–53. o.

Ha a társaság már ismeri a tévesen elküldött mellékletet és annak védett személyes adattartalmát, a vezetői ülés vagy a tisztviselő későbbi írásbeli állásfoglalása nem teremti meg újra a tudomásszerzés időpontját.[79] E körben javasolt az első jelzés, a tények ellenőrzése és a döntés időpontjának rögzítése (a következő példán keresztül szemléltetve): hétfő reggel kilenc órakor megállapított incidensnél a hetvenkét órás időpont csütörtök reggel kilenc óra. A bejelentést ugyanakkor indokolatlan késedelem nélkül kell megtenni, a számítás pedig nem indokolja az utolsó óráig történő várakozást (*re vera autem...*).

V.2. Kockázatértékelés, bejelentés és érintetti tájékoztatás

A hatósági bejelentés alóli kivétel a GDPR 33. cikk (1) bekezdése szerint akkor áll fenn, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az érintetti tájékoztatás főszabályát ezzel szemben a 34. cikk (1) bekezdése szerinti valószínűsíthető magas kockázat alapozza meg. Bekövetkezett kár bizonyítása egyik kötelezettségnek sem feltétele – a döntést az előrelátható következmények alapján, a rendelkezésre álló információk figyelembevételével kell meghozni. Az adatkezelő üzleti hírnevének vagy esetleges bírságának veszélye ettől eltérő kérdés, így a vizsgálatban az adatok jellege, az azonosíthatóság, az érintettek száma és helyzete, a hozzáférő személy, valamint a lehetséges következmények kapnak szerepet. A GDPR preambuluma például hátrányos megkülönböztetést, személyazonossággal való visszaélést, pénzügyi veszteséget és jóhírnév-sérelmet is említ. A következmény súlyát és bekövetkezésének valószínűségét együtt szükséges vizsgálni.[80]

Török a kockázathoz igazított megfelelést előzetes, ellenőrizhető intézkedések rendszerével kapcsolja össze.[81] E megközelítést az incidens utáni értékelésre alkalmazva a társaság számára nem indokolt minden eseményt azonos súlyúnak minősítő sablon – olyan szempontrendszer szükséges, amely rögzíti az adat jellegét, a jogosulatlan hozzáférést, valamint az érintetteket fenyegető lehetséges hátrányok súlyát és bekövetkezésük valószínűségét. Az értékelésben a biztosan ismert tényt és a még vizsgált körülményt el kell választani.

---

[79] Európai Adatvédelmi Testület: Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.0, elfogadva 2023. március 28. 31–36. pont, 11–12. o. https://dataprotection.gov.sk/files/metod-edpb/edpb_guidelines_202209_personal_data_breach_notification_v2-0_en.pdf (2026. 10. 04.)

[80] GDPR 33. cikk (1) bekezdés, 34. cikk (1) bekezdés, (75), (76), (85) és (86) preambulumbekezdés.

[81] TÖRÖK: *i. m.* 17–19. o.

Ha nem állapítható meg, hány címzett nyitotta meg az iratot, ezt bizonytalanságként kell feltüntetni, és a további feltárást ehhez igazítani. Egy tévesen továbbított, névvel összekapcsolt egészségügyi irat más következménnyel járhat, mint egy már jogszerűen közzétett vezetői tisztség megismétlése, ugyanakkor kevés érintett esetén is jelentős lehet a kockázat, amennyiben az adat különösen érzékeny vagy az érintett kiszolgáltatott. A visszahívás sikerére vonatkozó technikai üzenet, a címzett törlési nyilatkozata és az adatok tényleges visszaállíthatatlansága eltérő bizonyító értékű körülmény. A megbízható címzett közreműködése csökkentheti ugyan a továbbterjedés kockázatát, a már bekövetkezett jogosulatlan közlést azonban nem szünteti meg visszamenőleg. A GDPR 33. cikk (5) bekezdése éppen ezért valamennyi adatvédelmi incidens dokumentálását előírja, a tények, hatások és orvosló intézkedések rögzítésével – a nyilvántartási kötelezettség a be nem jelentett eseményekre is kiterjed, ugyanakkor a 33. cikk szerinti hatósági bejelentés küszöbe és a 34. cikk szerinti érintetti tájékoztatás magas kockázathoz kötött követelménye különbözik. A társaságnak mindhárom kérdésben külön következtetést kell kialakítania: történt-e incidens, fennáll-e hatósági bejelentési kötelezettség, és szükséges-e az érintettek közvetlen tájékoztatása.[82]

A három szint elkülönítésének szakirodalmi előzménye Szabó és Révész fokozatos incidenskezelési megközelítése.[83] A hatályos GDPR követelményeit ettől függetlenül is pontosan kell alkalmazni, hiszen a dokumentálás körét nem lehet pusztán a nagyobb eseményekre korlátozni. A belső feljegyzésnek egy kisebb, be nem jelentett incidensnél is meg kell mutatnia, mi történt, miért nem állt fenn bejelentési kötelezettség, és milyen intézkedés követte az eseményt, így a bejelentés elmaradása ellenőrizhető szakmai döntésként jelenik meg (magas kockázat esetén az érintettet indokolatlan késedelem nélkül, világos és közérthető módon kell tájékoztatni). A GDPR 34. cikk (3) bekezdése meghatározott kivételeket tartalmaz, így az érintett adatokhoz hozzáférést ténylegesen megakadályozó védelem vagy a magas kockázat fennmaradását kizáró későbbi intézkedés esetét. Aránytalan erőfeszítésnél nyilvános közlemény vagy hasonlóan hatékony intézkedés válhat szükségessé. E kivételek alkalmazása konkrét feltételek igazolását igényli, így a puszta állítás, hogy „az adatokat biztonságosan kezeltük”, nem helyettesíti annak bemutatását, mi védte az érintett tartalmat.[84, 85]

[82] GDPR 33. cikk (1) és (5) bekezdés, 34. cikk (1) bekezdés.
[83] SZABÓ – RÉVÉSZ: *i. m.* 52–53. o.
[84] GDPR 34. cikk (1)–(4) bekezdés.
[85] SZABÓ E. Gy. – RÉVÉSZ: *i. m.* 52–53. o.

A bejelentésben ismertetni kell továbbá az incidens jellegét, lehetőség szerint az érintettek és az adatnyilvántartások kategóriáit, hozzávetőleges számát, továbbá a kapcsolattartó elérhetőségét, a valószínű következményeket és az orvosló intézkedéseket. A GDPR 33. cikk (4) bekezdése megengedi az információk részletekben történő közlését, ha azok nem adhatók meg egyszerre, a bejelentés ezért nem halasztható pusztán a ”forenzikus” vizsgálat lezárásáig. Az adatfeldolgozó az adatkezelőnek indokolatlan késedelem nélkül jelzi az incidenst, és a szerződéses értesítési rendnek ezt a kötelezettséget működőképessé kell tennie.[86] A részletekben történő közlés lehetőségét az elszámoltathatóság szakirodalmi megközelítésével együtt értékelve a bejelentés és a belső vizsgálat között folyamatos kapcsolat szükséges.[87] A társaság korai bejelentése tartalmazhat előzetes érintetti becslést, amelyet az iratfeltárás után pontosítani kell, a kiegészítésnek pedig világossá kell tennie, mely korábbi információ változott és miért. Az eljárás szervezési feltételeként egyetlen, hozzáférésében korlátozott eseménydokumentáció vezetését tartom indokoltnak, hogy a jogi terület és az informatikai szakértő ugyanazon tényállapotot használja, a tisztviselő pedig követni tudja a változást – a párhuzamos, egymástól eltérő belső feljegyzések szükségtelen bizonytalanságot teremthetnek, amikor az észleléstől a bejelentésig tartó folyamatban a történeti tényállás az incidens origója, és az egyenlet *neuralgikus pontja*.

Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH), incidensbejelentő felületet biztosít. Az európai adatvédelmi kézikönyv a bejelentés érdemi tartalmát a hatóság intézkedési lehetőségével kapcsolja össze.[88] A benyújtás visszaigazolását és a kiegészítések tartalmát célszerű az ügyirathoz kapcsolni, a bejelentés pontosságát nem növeli a feltételezések bizonyított tényként való előadása. Az ismeretlen érintetti számot, a még vizsgált hozzáférést és a tervezett intézkedést ennek megfelelően szükséges megjelölni. A hatósági közlésnek az esemény érdemi megértését kell szolgálnia, ezért az irreleváns személyes adatok vagy a teljes eredeti irat szükségtelen továbbítása kerülendő.[89]

[86] GDPR 33. cikk (2)–(4) bekezdés.
[87] TÖRÖK: *i. m.* 18–19. o.
[88] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 173. o.
[89] Nemzeti Adatvédelmi és Információszabadság Hatóság: Adatvédelmi incidensbejelentő rendszer. https://www.naih.hu/adatvedelmi-incidensbejelento-rendszer (2026. 10. 04.)

V.3. Elhárítás, bizonyítékok és a tisztviselő közreműködése

Az adatkezelő a GDPR 32. cikke alapján a kockázatokhoz igazodó technikai és szervezési intézkedéseket köteles alkalmazni. Incidensnél e keretben a további jogosulatlan hozzáférés megakadályozása, a rendelkezésre állás helyreállítása és az intézkedések eredményének ellenőrzése egyaránt szerepet kap. A társaság számára ez jelentheti hibás hozzáférés megszüntetését, a téves címzett megkeresését, a fájl lecserélését vagy a mentésből történő helyreállítást, az alkalmazott intézkedésnek azonban az adott esemény okához kell kapcsolódnia – a formális szabályzatmódosítás nem pótolja a tényleges technikai hibajavítást.[90] Kiss Attila és Krasznay Csaba a biztonsági célú felhasználói viselkedéselemzésnél is rámutatnak a személyes adatok kezelésének korlátaira.[91] E megállapítást az incidensvizsgálat szűkebb helyzetére alkalmazva abból indulok ki, hogy a naplóadatok feltárása önálló adatkezelési művelet, amelynek célját, terjedelmét és hozzáférési rendjét rendezni kell. Egy hibás szerződésküldés vizsgálata nem igazolja valamennyi munkavállaló teljes levelezésének határozatlan idejű átvizsgálását. A vizsgálatot az érintett időszakra, fájlra és továbbítási műveletre célszerű korlátozni, majd új bizonyíték alapján lehet indokoltan bővíteni, hogy a kárelhárítás az érintetti jogok tiszteletben tartásával történjen.

A bizonyítékok megőrzése és a kárenyhítés közötti viszonyt előzetesen célszerű rendezni – egy hibás fájl nyilvános elérhetőségének gyors megszüntetése fontos, miközben az ügy kivizsgálásához az eredeti állapot és a hozzáférési naplók védett megőrzése is szükséges lehet. Az eljárásban minden lényeges intézkedésnél rögzíteni kell a végrehajtót, az időpontot és az ellenőrzött eredményt, hogy a műszaki helyreállítás és a jogi értékelés ugyanarra a rekonstruálható eseménysorra épülhessen. Az Európai Adatvédelmi Testület incidensiránymutatása a tisztviselő feladatát a tanácsadásban, az ellenőrzésben és a hatósági együttműködésben látja, az adatkezelő felelősségének fenntartásával. A társaság szervezetében a tisztviselő a személyesadat-érintettség megítélését, a kockázati értékelés következetességét és a bejelentés tartalmát segítheti. Az informatikai szakértő a rendszer működéséről ad ellenőrizhető tényeket, a vezetés pedig biztosítja az intézkedések végrehajtását és meghozza a szükséges döntéseket (a szerepek kapcsolódása különösen fontos a rövid határidő miatt).[92]

---

[90] GDPR 32. cikk (1)–(2) bekezdés, 33. cikk (3) bekezdés d) pont.

[91] KISS A. – KRASZNAY Cs.: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. In *Információs Társadalom* 2017/1. 65–66. o.

[92] Európai Adatvédelmi Testület: Guidelines 9/2022, *i. m.* 130–133. pont, 27. o.; GDPR 38–39. cikk.

Szabó a tisztviselő belső elérhetőségét és a munkatársak kapcsolatfelvételét is a szerep gyakorlati feltételeként tárgyalja.[93] Ez alapján az incidensjelzés útját olyan egyszerűen kell kialakítani, hogy a hibát észlelő munkatárs az eseményt jogi minősítés nélkül is továbbíthassa. A jelzéshez elég lehet az érintett fájl, a továbbítás időpontja és a feltételezett címzett megadása. A tisztviselő és az informatikai szakértő feladata az értékelés támogatása – a jelző munkatárstól nem várható el, hogy előzetesen maga döntse el a hatósági bejelentés szükségességét. A belső eljárás így a jogi minősítést a szakmai értékeléshez rendeli, és a vizsgálathoz rendelkezésre álló idő is megőrizhető. Az esemény lezárását követően a tisztviselő ellenőrizheti a javító intézkedés eredményét, a vezetés számára pedig (*megjegyzés: jobb esetben*) rövid értékelés készülhet az okról és az ismétlődés megelőzéséről. A feltárt hibás sablon vagy jogosultsági beállítás kijavítása konkrét megelőző intézkedést jelent.

VI. JOGGYAKORLAT ÉS A KÉT ELJÁRÁS TALÁLKOZÁSA

VI.1. A jogesetek tanulságai és a társasági adatkiadás

A jogi minősítés és a működési feltételek kapcsolatát a NAIH-5513-6/2024. számú jelentés szemlélteti. A KEHI ügyében a Hatóság a meglévő vizsgálati adatok kigyűjtését elvárta akkor is, amikor a központi iratkezelési rendszerből nem voltak közvetlenül lekérdezhetők.[94] A jelentés a Kúria Pfv.IV.20.275/2024/4. számú ítéletét is ismerteti, amely 8400 ügy iratainak áttekintése kapcsán különböztette meg az adatkeresést az új, minőségileg más adat előállításától.[95] A KEHI nem gazdasági társaság, így az ügy tényállása nem vihető át változatlanul a vizsgált szervezeti körre, a meglévő adatok felkutatásának módszertani követelménye azonban a társasági iratkezelésben is értelmezhető. A tények feltárását és a jogi értékelést külön kezelő döntéstámogatási módszert e körben is irányadónak tartom.[96]

[93] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–7. o.

[94] Nemzeti Adatvédelmi és Információszabadság Hatóság: A Nemzeti Adatvédelmi és Információszabadság Hatóság jelentése a Kormányzati Ellenőrzési Hivatal információszabadsággal kapcsolatos jogsértése tárgyában. NAIH-5513-6/2024. 9–10. o. https://www.naih.hu/files/infoszab_jelentes_naih-5513-6-2024.pdf (2026. 10. 05.)

[95] Kúria: Pfv.IV.20.275/2024/4. számú ítélet. A döntést a NAIH-5513-6/2024. számú jelentés 10. oldalán közölt ismertetés alapján hivatkozom.

[96] SZÉKELY I. – SOMODY B. – SZABÓ M. D.: *i. m.* 17–20. o.

Véleményem szerint egy adatigénylés vizsgálata legalább két, egymáshoz kapcsolódó feltárást kíván: meg kell állapítani, mely iratokban szerepelhet a kért adat, valamint azt is, hogy az adatok összegyűjtéséhez milyen művelet szükséges. A szerződések között szétszórtan megtalálható összegek kigyűjtése más feladat, mint azokból a társaság gazdasági eredményességére új szakmai értékelést készíteni. A válaszban ezért a keresés tényleges eredményét kell közölni, hiszen az, hogy a belső program nem ad kész kimutatást, önmagában nem mutatja meg, létezik-e a megismerni kívánt adat. A paksi beruházásról szóló 4/2021. (I. 22.) AB határozat másik problémát szemléltet: a különleges adatkorlátozás együttalkalmazását az általános nyilvánossági garanciákkal. Az indokolás az elutasítás tartalmi vizsgálatát és az érdekek egyedi mérlegelésének szükségességét hangsúlyozza.[97] E döntés alapján azt a következtetést vonom le, hogy a döntés indokának a kért adathoz és a védett érdekhez kell kapcsolódnia – ebből kiindulva, az ágazati szabályok megléte mellett fel kell tárni a részleges teljesítés lehetőségét (jóllehet az ítélet tanulsága nem jelenti a beruházás saját szabályainak valamennyi társaságra történő kiterjesztését). A döntésekből levont következtetések alkalmazását a következő hipotetikus tényállásokon keresztül mutatom be, amelyek a minősítés egyes lépéseit és a szervezeti szerepeket szemléltetik:

Az *első esetben* egy közfeladatot ellátó társaság támogatási programhoz készít feljegyzést, amelyet a döntésre jogosult minisztériumnak továbbít, majd egy igénylő a feljegyzésben szereplő költségadatokat és a döntés szakmai indokait kéri a társaságtól. A dokumentum a társaság irattárában is megtalálható. A társaság kezdeti álláspontja szerint kizárólag a minisztériumhoz lehet fordulni, mert a végső döntés ott született – ez az érvelés az irat eredetét, a döntési hatáskört és az adatkiadás kötelezettségét egyetlen kérdésként kezeli. A megoldás kiindulópontja ebben az esetben az Infotv. szerinti kötelezetti helyzet és a ténylegesen kezelt adatok vizsgálata: a minisztériumi hatáskör nem teszi önmagában nem létezővé a társaságnál őrzött információt.[98] Mivel a döntés-előkészítő tartalom viszont az Infotv. 27. §-a szerinti külön értékelést igényelhet, a társaságnak fel kell tárnia, mely döntéshez kapcsolódott a feljegyzés, és el kell különítenie a költségadatokat az esetleg továbbra is jogszerűen védett megfontolásoktól. A minisztériummal való egyeztetés a tények feltárását segítheti, de nem szolgálhat önálló, törvényben nem szereplő határidő-halasztásként.

[97] 4/2021. (I. 22.) AB határozat, Indokolás [86], [96]–[97].
[98] SZÁDECZKY – SZŐKE: *i. m.* 35–36. o.

Az adatvédelmi tisztviselő a közreműködők személyes adatainak minősítését segíti, a támogatási program nyilvánosságáról azonban nem ő dönt, mert az eset tanulsága szerint a szervezetek közötti adatáramlás és a döntési hatáskör eltérő vizsgálatot kíván. Ezek összevetése mutatja meg a társaságnál értékelendő adatkört. A *második tényállásban* az igénylő egy közpénzből finanszírozott fejlesztési szerződést és mellékleteit kéri, a szerződés pedig tartalmazza a kedvezményezett nevét, a támogatás összegét és tárgyát, de egy mellékletben magánszemély bankszámlaadata, magántelefonszáma és részletes technológiai leírás is szerepel. A partner teljes titoktartást kér, így a társaság előtt két hibás rövidítés lehetősége áll – a teljes dokumentum kiadása a közpénzügyi kapcsolat miatt, vagy a teljes igény elutasítása a partner kérésére. A jogi megoldás az adatfajták elkülönítése. A közpénzfelhasználás törvény alapján nyilvános elemei kiadhatók, míg a járulékos személyes adatokhoz külön nyilvánossági jogcímet kell keresni. A technológiai részleteknél az üzleti titok feltételeit és az Infotv. kivételét kell mérlegelni. Amennyiben utóbbi releváns, részleges teljesítés érdekében a védett tartalmat a másolaton felismerhetetlenné kell tenni, a korlátozás okát pedig a válaszban meg kell jelölni (a partner titoktartási kikötése a törvényi vizsgálatot nem váltja ki).[99, 100]

A közérdekből nyilvános személyes adat kettős jogi helyzetéről szóló Bendik–Péterfalvi-elemzés is fogalmi támpontot ad arra, hogy a közzéteendő név és a személy magánadata ne kapjon azonos megítélést.[101] A szerződés közpénzügyi kapcsolatának feltárása után ugyanis minden személyes adat szerepét külön vizsgálni kell, hiszen a támogatási összeg és a jogszabály alapján megismerhető kedvezményezetti adat közléséhez fűződő érdekből nem következik a magántelefon vagy a bankszámlaadat szükséges volta. Az indokolásnak e különbséget kell követnie, a kitakarásnak pedig a megfelelő mellékletre is ki kell terjednie. A tisztviselő a személyes adatok, az iratgazda és a jogi terület a műszaki titok értékeléséhez járul hozzá, ugyanakkor a végleges fájlcsomag együttes ellenőrzése szükséges, mert egy változatlan melléklet a helyesen kitakart főszerződés mellett is adatvédelmi hibát okozhat.

[99] Infotv. 26. § (2) bekezdés, 27. § (3) bekezdés, 30. § (1) bekezdés; 2018. évi LIV. törvény, 1. § (1) bekezdés. A tényállás saját szerkesztésű, szemléltető eset.
[100] DE NEGRI: *i. m.* 84–86. o.
[101] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

VI.2. Hibás adatkiadás és az incidensiratok megismerése

A *harmadik esetben* a társaság egy szerződés PDF-változatában fekete alakzattal takarja el a magánelérhetőségeket, a szövegréteg azonban megmarad, ezért a kiadott fájlból az adatok kimásolhatók. A hibát az igénylő jelzi, és közli, hogy a dokumentumot munkatársának is továbbította. A társaságnak ekkor először meg kell őriznie a vizsgálathoz szükséges példányt, fel kell tárnia az érintett adatkört és a továbbítás körülményeit, valamint el kell készítenie a helyesen kitakart változatot.

A javított adatkiadás és az incidens kivizsgálása párhuzamos feladat. A védett személyes adatok hozzáférhetővé válása a biztonság sérülését jelenti, ezért a bejelentés kérdését a kockázatértékelés dönti el. Ugyanez a vizsgálat szükséges lenne téves e-mail-címre továbbított személyes adatnál is (a címzett törlési ígérete fontos körülmény, de a hozzáférés és a további továbbítás feltárását nem teszi feleslegessé). Amennyiben – *ab ovo* – megtörtént a továbbküldés, azt már tényleges eseményként kell figyelembe venni. A hatósági bejelentés és a magas kockázat esetén szükséges érintetti tájékoztatás feltételeit külön kell értékelni.[102] Az újraazonosítás kutatási eredményeinek az esetre vonatkozó további tanulsága, hogy a helyesen végrehajtott névkitakarás sem teszi automatikusan anonimmá a fájlt.[103] A társaság a javított változatnál ezért az esemény részleteiből és a megmaradó munkaköri adatokból történő azonosítást is kell ellenőrizze tekintettel arra, hogy a javítás célja az eredeti igény jogszerű teljesítése, vagyis, hogy a nyilvános tartalom legyen hozzáférhető, a védett személyes adat pedig a teljes, ténylegesen továbbított csomagban maradjon felismerhetetlen. Megelőzéshez tehát a hibás kitakarási módszert és az ellenőrzési pontot kell módosítani, az esemény feltárt okához igazodva.

A *negyedik tényállásban* egy újságíró az előző esemény bejelentését, az incidensnyilvántartás kapcsolódó bejegyzését és a társaság javító intézkedéseit kéri. Az iratok az érintettek neve mellett belső jogosultságokat, technikai hibahelyeket és hatósági kapcsolattartási adatokat tartalmaznak. Az „incidensirat” megnevezés önmagában sem teljes nyilvánosságot, sem általános titkosságot nem jelent. A társaság közfeladatával kapcsolatos működési adatok megismerhetőségét és az egyes személyes vagy más jogcímen védett részleteket külön kell értékelni. [104]

---

[102] GDPR 4. cikk 12. pont, 33–34. cikk. A tényállás saját szerkesztésű; nem hatósági határozat ismertetése.

[103] GULYÁS: *i. m.* 72–74, 78. o.

[104] Infotv. 3. § 5–6. pont, 26. § (1) bekezdés, 30. § (1) bekezdés; GDPR 33. cikk (3) és (5) bekezdés. A negyedik tényállás is saját szerkesztésű, szemléltető eset.

A három kért irat közül a NAIH-nak tett GDPR-incidensbejelentés és a belső nyilvántartási bejegyzés a társaság saját adatkezelési működését dokumentálja. Az esemény időpontja, általános jellege, az érintett adatkategóriák és a már rögzített összesített érintetti szám főszabály szerint kiadható működési adat. A bejelentés megtörténte és időpontja ugyancsak ellenőrizhetővé teszi a társaság eljárását. Az érintettek neve, magánelérhetősége, esetleges egészségügyi vagy egyéb személyes adata viszont nem válik közérdekből nyilvánossá attól, hogy az incidensiratban szerepel – e részleteket az Infotv. 30. § (1) bekezdése alapján a másolaton felismerhetetlenné kell tenni. Amennyiben a kis létszámú érintetti kör és a körülmények együtt azonosítást tesznek lehetővé, a megmaradó közvetett azonosítókat is vizsgálni szükséges. Új statisztika készítésének kötelezettségét e következtetés nem teremti meg: a már kezelt adatok részleges kiadásáról van szó.[105]

A kapcsolattartási adatok között különbséget kell tenni a közfeladat ellátásához kapcsolódó és a magánjellegű elérhetőségek között. A feladatkörében eljáró személy neve, beosztása és a közfeladattal összefüggő, törvény szerint nyilvános adata az Infotv. 26. § (2) bekezdése alapján megismerhető, míg az adatvédelmi tisztviselő szakmai elérhetőségének közzétételét a GDPR 37. cikk (7) bekezdése kifejezetten előírja. A bejelentésben feltüntetett kapcsolattartó neve és elérhetősége azonban a hatósági adattartalom előírása alapján még nem válik automatikusan teljes egészében nyilvánossá. Magántelefonszámot, személyes e-mail-címet vagy a feladatkör bemutatásához nem szükséges egyéni jogosultságot ezért nem indokolt kiadni. A tisztviselő e minősítést véleményezi, de saját adatai ügyében sem veszi át a társaság adatkiadási döntését.[106]

A javító intézkedésekből megismerhető a hibás PDF-kitakarás kijavításának ténye és időpontja, az alkalmazott ellenőrzés általános módja, a munkafolyamat módosítása és a már dokumentált eredmény. A közpénzügyi gazdálkodáshoz kapcsolódó, kezelt költségadatot sem teszi titkossá az intézkedés informatikai tárgya. De Negri átláthatósági megközelítését erre az esetre alkalmazva az intézkedés eredménye és finanszírozása a társaság ellenőrizhetőségéhez tartozik.

---

[105] Infotv. 26. § (1)–(2) bekezdés, 30. § (1) bekezdés; GDPR 5. cikk (1) bekezdés c) pont, 6. és 9. cikk. BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

[106] Infotv. 26. § (2) bekezdés; GDPR 33. cikk (3) bekezdés b) pont, 37. cikk (7) bekezdés. A hatósági bejelentés tartalmi előírása és a közérdekből nyilvános személyes adat terjesztésének jogcíme külön vizsgálandó.

Ha valamely részlet ténylegesen egy még meghozandó döntést készít elő, az Infotv. 27. § (5)–(6) bekezdésének feltételeit kell adatonként igazolni, az „intézkedési terv” felirat önmagában nem elegendő. Egy lezárt javítás dokumentált ténye nem tartható vissza pusztán arra hivatkozva, hogy a társaság a jövőben további fejlesztést tervez. A már végrehajtott és a még előkészítés alatt álló elemeket ezért ugyanazon iratban is külön értékelem.[107]

A technikai hibahelyeknél az Infotv. 27. § (2) bekezdés i) pontjára történő hivatkozás mellé konkrét korlátozó törvényi rendelkezés is szükséges. Ilyen különös norma a Kiberbiztonsági tv. 78. § (2) bekezdése: a kiberbiztonsági hatóság, a sérülékenységvizsgálatra jogosult szerv vagy gazdálkodó szervezet, valamint a kiberbiztonsági incidenskezelő központ eljárásában keletkezett adatokra vonatkozik, a 79. § kivételeivel. A személyi hatályhoz tehát az eljáró szereplőt, a tárgyi hatályhoz pedig az adat keletkezésének eljárási összefüggését kell azonosítani. A társaság saját GDPR-bejelentése, belső nyilvántartása és javítási feljegyzése önmagában nem felel meg e feltételeknek – a NAIH adatvédelmi eljárása sem azonos a törvény szerinti kiberbiztonsági eljárással. Ha azonban az irat a felsorolt szereplők eljárásában létrejött vizsgálati eredményt is tartalmaz, az érintett adatrészre a korlátozást külön alkalmazni kell. A 79. § szerinti közzétételi jogosultság nem teszi általánosan igényelhetővé az egyedi vizsgálat összes alapadatát.[108]

Az ettől eltérő, közvetlenül a közfeladatot ellátó szervezet döntésére irányadó szabályt a Kiberbiztonsági tv. 79/A. §-a tartalmazza. Személyi hatálya a törvény 1. és 2. §-ában meghatározott, egyben közfeladatot ellátó szervezetekhez kötött, tárgya pedig az általuk használt vagy szolgáltatott elektronikus információs rendszerrel vagy központi szolgáltatással kapcsolatos adat. Nem elegendő tehát a társaság közfeladatára hivatkozni: a törvény hatálya alá tartozást, az adat rendszerkapcsolatát és a megismerésből eredő kiberbiztonsági veszélyeztetést is igazolni kell. Az 1. § (1) bekezdés b) pontjánál például a többségi állami befolyás mellett a törvényi méretfeltétel is vizsgálandó. A húszéves felső időhatár nem jelenti minden rendszeradat húszéves titkosságát, az elutasítás feltétele a veszélyeztetés fennállása, és a teljesíthetőségről a szerv vezetője dönt.

[107] Infotv. 26. § (1) bekezdés, 27. § (3), (5)–(6) bekezdés. DE NEGRI: *i. m.* 84–86. o.

[108] Infotv. 27. § (2) bekezdés i) pont; Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.), 1. §, 78. § (2) bekezdés, 79. § (1)–(2) bekezdés. A 78. § (2) bekezdésének alkalmazásához az adat eljárási eredetét is igazolni kell.

E rendelkezés alapján egy még kihasználható sérülékenység konkrét műszaki részlete visszatartható lehet, a javítás általános ténye és időpontja azonban csak azonos feltételek igazolásával korlátozható.[109] A bemutatott tényállás alapján a PDF-ben megmaradt szövegréteg és a hibás kitakarás általános leírása nem tekinthető automatikusan védett kiberbiztonsági adatnak. A névhez rendelt belső jogosultságokat személyesadat-tartalmuk szerint kell minősíteni[110] – további technikai részlet kizárásához pedig a különös korlátozás, a döntés-előkészítő jelleg vagy az üzleti titok valamennyi alkalmazandó feltételét igazolni szükséges. Üzleti titokra csak a titkosság, a vagyoni érték és a megfelelő titokvédelmi intézkedések fennállásakor lehet hivatkozni, figyelembe véve a közpénzügyi adatok nyilvánosságát is. Szádeczky és Szőke történeti elemzésének elhatárolási szempontja itt is hasznos, a mai korlátozás jogalapját azonban a hatályos törvényből kell levezetni. A biztonsági aggály tehát részletes jogi vizsgálatot indokol, általános megtagadási okot önmagában nem hoz létre.[111]

A negyedik eset megoldását mindezek alapján részleges teljesítésben látom: a három kért iratból ki kell adni a megismerhető működési és intézkedési adatokat, a védett személyes adatokat és az igazoltan korlátozott adatrészeket pedig el kell különíteni. A válaszban minden visszatartott adatkörhöz hozzá kell rendelni a jogalapot és az ügyre szabott indokot, mérlegelést engedő szabálynál a nyilvánossághoz fűződő közérdek értékelése is szükséges. Az iratgazda feltárja a három iratot, a jogi terület elvégzi a normák hatályának vizsgálatát, a tisztviselő véleményezi a személyesadat-minősítést és a kitakarás ellenőrzését, az informatika pedig a ténylegesen továbbítandó fájlt vizsgálja. A döntés a társaság vezetői felelőssége marad, a 79/A. § szerinti ügyben kifejezetten a szerv vezetője dönt. Az adatigénylési határidőt a folyamatban lévő incidensvizsgálat önmagában nem függeszti fel, ezért a két eljárást párhuzamosan kell dokumentálni. E feladatmegosztást a VIII. fejezet mátrixában a negyedik eset adatkörére bontva is végigvezetem.[112]

---

[109] Kiberbiztonsági tv. 1–2. §, 79/A. § (1)–(2) bekezdés; Infotv. 27. § (2) bekezdés i) pont, 30. § (3) és (5) bekezdés, 31. § (2) bekezdés. A húszéves felső időhatár és a veszélyeztetés fennállása külön feltétel.

[110] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

[111] Infotv. 27. § (3), (5)–(6) bekezdés, 30. § (1) és (5) bekezdés; az üzleti titok védelméről szóló 2018. évi LIV. törvény, 1. § (1)–(2) bekezdés. SZÁDECZKY – SZŐKE: *i. m.* 35–36. o. A tanulmány történeti szabályozási környezetét a hatályos normáktól külön kezelem.

[112] Infotv. 29. § (1)–(2) bekezdés, 30. § (1), (3) és (5) bekezdés, 31. § (2) bekezdés; GDPR 38. cikk (1) bekezdés, 39. cikk (1) bekezdés a)–b) pont. SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–8. o.

VII. HAZAI ÉS UNIÓS SZABÁLYOZÁSI NÓVUMOK

VII.1. Hazai változások: együttműködés és közzététel

A *2026. évi XVIII. törvény* új rendelkezése szerint az adatok megismerhetővé tétele során a közfeladatot ellátó szerv és az igénylő jóhiszeműen, kölcsönösen együttműködve jár el – az Infotv. 26. § (1a) bekezdése ezt a nyilvánosság biztosítása érdekében követeli meg.[113] E cél összhangban áll Székely információs erőfölényre vonatkozó megközelítésével is.[114] A módosítás az Infotv. 30. § (2a) bekezdését is hatályon kívül helyezte, ezért a társaságnak a válasz sablonokban és belső útmutatókban is át kell vezetnie az alkalmazandó szabályokat, a korábbi rendelkezéshez kapcsolódó érvelés pedig nem vehető át változatlanul az új ügyekbe[115] – a korábbi joggyakorlat felhasználásánál a fentieken túl pedig az állítás időbeli érvényességét is vizsgálni kell. A 13/2019. AB határozat és a 2024-es KEHI-jelentés a tárolt adatok kikereséséhez továbbra is módszertani támpontot nyújt, de a bennük idézett költség- és eljárási szabályok egy része időközben megváltozott[116].

Kiemelendő szempont, hogy a társasági szabályzat aktualizálása az elszámoltathatóságot támogató tisztviselői ellenőrzéshez is szorosan kapcsolódik.[117] Ennek során a hatályos rendelkezést és az értelmezést segítő korábbi döntési érveket külön szükséges rögzíteni (ezzel ugyanis elkerülhető, hogy egy helyes joggyakorlati hivatkozás mellé már nem alkalmazandó díjtétel vagy megtagadási ok kerüljön). A Központi Információs Közadat-nyilvántartás kötelezetti körének bővülése 2026. augusztus 26-tól a köztulajdonban álló társaságokat is érinti – az Infotv. 37/C. §-a a meghatározott, ötmillió forintot meghaladó támogatások, szerződések és kifizetések adatait rendeli a felületre, a törvényi kivételekkel. A szabály kéthavi közzétételt és legalább tízéves hozzáférhetőséget ír elő, a NAIH közleménye pedig az új kötelezettek első közzétételi határidejét 2026. október 28-ban jelöli meg, az ott meghatározott kezdeti időszakra.

---

[113] Az európai uniós forrásokhoz való hozzáférés érdekében szükséges egyes törvények módosításáról szóló 2026. évi XVIII. törvény, 26. §; Infotv. 26. § (1a) bekezdés. Az elutasítási jogcímre vonatkozó megállapítás a dolgozat saját értelmezése.

[114] SZÉKELY I.: [Fórumhozzászólás], *i. m.* 47–48. o.

[115] 2026. évi XVIII. törvény, 30. §; az Infotv. 30. § (2a) bekezdésének hatályon kívül helyezése.

[116] 13/2019. (IV. 8.) AB határozat, Indokolás [55]–[60]; NAIH-5513-6/2024. számú jelentés, *i. m.* 9–10. o. Az új ügyekben az Infotv. hatályos szövege alkalmazandó; a korábbi döntésekben idézett, azóta módosult rendelkezések nem vehetők át változatlanul.

[117] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 3–4, 6–8. o.

A dolgozat lezárásakor ez még jövőbeli teljesítési határidő, már fennálló szervezési feladatokkal.[118] A közzététel gyakorlati teljesítéséhez a pénzügyi és szerződéses nyilvántartások összehangolását is szükségesnek tartom. Czékmann Zsolt az elektronikus demokrácia vizsgálatában az információhoz jutást az állam és az egyén kapcsolatának átalakulásához köti, melyből azon következtetést lehet levonni, hogy a nyilvánosság akkor segíti az ellenőrzést, ha az adat kereshető, időszerű és értelmezhető. A puszta feltöltés önmagában ennek érvényesüléséhez azonban sokszor kevés.[119]

Kormány Béla a tulajdonosi működés értékelésében a közérthető, összehasonlítható információ és a nyilvános elszámoltathatóság kapcsolatát is felveti.[120] E szempontot a hazai közzétételi paradigmaváltást alkalmazva a társaság számára az adatok minősége is feladattá válik: fontos, hogy a szerződéses nyilvántartásban a tárgy és az érték legyen következetesen rögzítve, a közzétett adat kapcsolódjon az érintett időszakhoz, és a javítás visszakereshetően történjen. A központi felületen megjelenő adatoknak így van értelmezhető kapcsolatuk a társaság saját dokumentumaival és az egyedi adatigénylésekre adott válaszokkal.

VII.2. Uniós fejlemények és az alkalmazás időbeli határai

Az (EU) 2025/2518 rendelet a GDPR végrehajtására vonatkozó további eljárási szabályokat állapít meg a határokon átnyúló adatkezelést érintő ügyekben – a már elfogadott jogszabályt 2027. április 2-től kell alkalmazni, az átmeneti rendelkezések figyelembevételével. Ezért a dolgozat lezárásakor felkészülést indokol, de nem írja át az aktuális adatigénylési és incidensbejelentési határidőket. Egy kizárólag belföldi társasági ügyre a határon átnyúló eljárási keret nem alkalmazható automatikusan, mert előbb a GDPR szerinti hatályt és az adott eljárás jellegét kell tisztázni.[121] A rendelet 24–25. cikke a közigazgatási ügyiratba való betekintést és a bizalmas információk kezelését is szabályozza.

---

[118] Infotv. 37/C. § (1)–(4) bekezdés; 2026. évi XVIII. törvény, 27. §. NAIH: Közlemény a Központi Információs Közadat-nyilvántartás felületén közzétételre kötelezett szervek és a közzéteendő adatok körének kiterjesztéséről. 2026. augusztus 14. https://naih.hu/hirek/849-koezlemeny-a-koezponti-informacios-koezadat-nyilvantartas-felueleten-koezzetetelre-koetelezett-szervek-es-a-koezzeteendo-adatok-koerenek-kiterjeszteserol (2026. 10. 04.)

[119] CZÉKMANN Zs.: Az egyén és az állam kapcsolatának megváltozása az IKT hatására – az e-demokrácia fogalmi alapjai. In *Miskolci Jogi Szemle* 2020/1. különszám. 31–32. o.

[120] KORMÁNY: *i. m.* 31. o.

[121] Az Európai Parlament és a Tanács (EU) 2025/2518 rendelete (2025. november 26.) az (EU) 2016/679 rendelet végrehajtására vonatkozó további eljárási szabályok megállapításáról, 1., 36. és 37. cikk.

A bizalmas kezelést kérő félnek egyértelmű megjelölést és indokolást kell adnia, a teljes változat mellett pedig lehetőség szerint nem bizalmas változat is szükséges. E szerkesztési elv a társaság számára gyakorlati tanulságot hordozhat. A tisztviselő a személyes adatok kezelésének feltételeit felkészülése során is tanácsadóként vizsgálja,[122] az iratok védett és megismerhető részeinek előzetes elkülönítése pedig a hatósági együttműködést segíti (miközben azért rögzítendő, hogy a rendeleti ügyirat-hozzáférésből nem vezethető le a társaság valamennyi dokumentumára kiterjedő új, Infotv. szerinti titokvédelmi jogcím).[123] Az Európai Bizottság COM(2025) 837 final számú Digital Omnibus javaslata több digitális jogszabály módosítását kezdeményezi, melynek keretében a GDPR incidensbejelentésénél magas kockázathoz kötött küszöböt, kilencvenhat órás időtartamot és egységes belépési pontot javasol. E változásokat jogalkotási javaslatként figyelembe véve, a hatályos belső szabályzatban továbbra is a GDPR 33. cikkének hetvenkét órás követelménye és jelenlegi kockázati kivétele alkalmazandó (*megjegyzés: a cikk számozása kissé megtévesztő, mert a kapcsolódó, mesterséges intelligenciáról szóló külön csomag eltérő tárgyú*).[124]

Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 2/2026. számú közös véleménye az egyszerűsítés mellett a hatékony védelem követelményeit is vizsgálja. Ezt értékelve úgy vélem, hogy nem csupán az óraszám változása jelentős: az új kockázati küszöb belső döntési útmutatót is kívánhat, miközben a tényfeltárás és dokumentálás szükséglete fennmaradhat.[125] E felkészülés a Szabó által bemutatott tanácsadói és megfelelés-ellenőrzési feladat gyakorlati alkalmazásához kapcsolódik.[126] A társaság felmérheti a javaslatból következő változtatásokat, a tervezett enyhítés azonban nem indokolja a jelenlegi bejelentés elmulasztását. A tisztviselőnek a jogforrás állapotát ellenőriznie kell, és a hatályos útmutatót a felkészülési anyagtól célszerű elkülöníteni – ez a Szabó által tárgyalt szerepek érvényesítéséhez is kapcsolódik.[127]

---

[122] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–8. o.

[123] (EU) 2025/2518 rendelet, 24–25. cikk, különösen 25. cikk (3) bekezdés.

[124] Európai Bizottság: Digital Omnibus, COM(2025) 837 final, 2025. november 19. Rendeletjavaslat, 3. cikk 8. pont, a GDPR 33. cikkének tervezett módosítása; 6. cikk, az egységes bejelentési belépési pont tervezete. https://data.consilium.europa.eu/doc/document/ST-15698-2025-INIT/en/pdf (2026. 10. 04.)

[125] Európai Adatvédelmi Testület – Európai Adatvédelmi Biztos: EDPB–EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus). Elfogadva 2026. február 10. 8.1. szakasz, 73–77. pont, 23–24. o. https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf (2026. 10. 04.)

[126] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–8. o.

[127] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–8. o.

VII.3. Jogalkalmazási tapasztalatok és kiberbiztonsági kapcsolat

Az Európai Adatvédelmi Testület 2024-ben közzétett tájékoztatása a tisztviselők kijelölését és jogállását érintő összehangolt vizsgálat tapasztalatait ismerteti. Az erőforrások, szakértelem, függetlenség és vezetői beszámolás hiányosságait is azonosítja, kedvező eredmények mellett – e tapasztalat irányt mutat a szervezési javaslatokhoz, de nem bizonyít azonos hiányosságot egy konkrét magyar társaságnál.[128] Az informatikai eseményeknél külön vizsgálandó a kiberbiztonsági szabályozás, hiszen a NIS2 irányelv és *a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény* hatálya alá tartozó társaságoknál további kockázatkezelési és incidensjelzési kötelezettség merülhet fel (a hatályt tevékenység, méret és a jogszabály szerinti besorolás alapján kell megállapítani).

A kiberbiztonsági és az adatvédelmi incidens eltérő fogalma miatt az egyik eljárás teljesítése nem helyettesíti automatikusan a másikat. Az Infotv. kiberbiztonsági érdekre vonatkozó korlátozási rendelkezése is konkrét törvényi alap és adatkör vizsgálatát kívánja. [129] A kiberbiztonsági és az adatvédelmi megfelelés közötti kapcsolatot Kiss és Krasznay a biztonsági célú adatkezelés feltételei felől is vizsgálják.[130] Az új szabályok követése ezért a társaságnál nem pusztán új bejelentési cím felvételét kívánja: az eseményről az informatikai és az adatvédelmi felelős ugyanazon tényeket kapja meg, miközben a rájuk vonatkozó jogi küszöböt külön értékeli. Az egyik rendszer számára szükséges technikai adatot a másik eljárásban csak akkor indokolt továbbítani, ha annak ott is van relevanciája és megfelelő jogalapja. A közös tényfeltárás és az elkülönített jogi döntés együtt biztosíthatja az eljárás áttekinthetőségét, a két megfelelési terület összekapcsolódása pedig a belső szabályzatok és felelősségi körök egyértelmű meghatározását is indokolttá teheti.

---

[128] Európai Adatvédelmi Testület: EDPB identifies areas of improvement to promote the role and recognition of DPOs. 2024. január 17. A Coordinated Enforcement Action, Designation and Position of Data Protection Officers oldalán közölt intézményi tájékoztatás. https://www.edpb.europa.eu/documents/coordinated-enforcement-framework/coordinated-enforcement-action-designation-and-position_fr (2026. 10. 04.)

[129] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2), 2–3., 21. és 23. cikk; Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, 1. és 66. §; Infotv. 27. § (2) bekezdés i) pont.

[130] KISS – KRASZNAY: *i. m.* 65–66. o.

Különösen fontos lehet annak előzetes rögzítése, hogy egy informatikai esemény észlelésekor mely szervezeti szereplőket, milyen adattartalommal és milyen sorrendben szükséges bevonni – az összehangolt működés álláspontom szerint ugyanis jelentős mértékben csökkentheti annak kockázatát, hogy ugyanazon eseményt eltérő szervezeti egységek egymástól függetlenül, hiányos információk alapján értékeljék. Az eljárások megfelelő dokumentálása egyúttal lehetővé teszi a megtett intézkedések és a jogi értékelés utólagos nyomon követését is. A gyakorlatban ezért az adatvédelmi és kiberbiztonsági feladatok kapcsolódási pontjainak előzetes azonosítása a hatékony incidenskezelés egyik (lényegében örökérvényű) szervezeti feltétele lehet.

VIII. SZERVEZETI ÉS JOGALKALMAZÁSI JAVASLATOK

A negyedik eset tanulságait egy alkalmazható döntési és felelősségi mátrixban foglalom össze. Jogi alapját az Infotv. belső szabályzatra vonatkozó előírása és a GDPR szervezési, elszámoltathatósági követelményei adják.[131] Kormány Béla intézményi megközelítése az elszámoltathatóság és a feladatok szervezése közötti kapcsolatot emeli ki: a társasági adatkiadásban ennek akkor van gyakorlati jelentősége, ha minden minősítési és végrehajtási lépéshez azonosítható felelős tartozik.[132] A mátrix jogi részét az 1., végrehajtási részét a 2. táblázat tartalmazza, ugyanazon A–E adatkörrel. Az adatkiadásról főszabály szerint a belső szabályzatban kijelölt vezető dönt, az iratgazda és a jogi terület előkészítése alapján (a tisztviselő tanácsadó és ellenőrző szerepet tölt be). A 79/A. § (2) bekezdése szerinti ügyben azonban a törvény által megjelölt szervvezető döntési jogosultságát külön követni kell. Az E sor szerinti hatályvizsgálatot minden más, rendszerhez kapcsolódó adatkörnél is el kell végezni. E rendben a felelősség és a szakmai közreműködés nem mosódik össze. A megfelelés bizonyíthatóságához a kiadott példány és a minősítés indokainak együttes megőrzése szükséges, amint azt az európai adatvédelmi kézikönyv elszámoltathatósági megközelítése is alátámasztja.[133]

[131] Infotv. 30. § (6) bekezdés; GDPR 5. cikk (2) bekezdés, 24. és 38–39. cikk. A bemutatott feladatmegosztás saját szervezési javaslat.
[132] KORMÁNY: *i. m.* 30–31. o.
[133] European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 134–136. o.

Az adatigénylés határideje a beérkezéstől számított legrövidebb idő – legfeljebb tizenöt nap – az Infotv. 29. § (2) bekezdésének feltételei mellett egyszer további tizenöt nappal hosszabbítható meg, az igénylő határidőn belüli értesítésével. A GDPR-incidens értékelése ettől külön folyamat: a bejelentés indokolatlan késedelem nélkül, ha lehetséges a tudomásszerzéstől számított hetvenkét órán belül esedékes, az érintetti tájékoztatás főszabálya pedig a valószínűsíthető magas kockázat.[134] Székely, Somody és Szabó döntéstámogatási módszerét követve előbb az adat és a jogcím, majd a korlátozás, végül a tényleges kiadási változat biztonsága vizsgálandó.[135]

1. táblázat A döntési mátrix jogi oldala[136]

Adatkör	Nyilvánossági jogcím	Korlátozás és indok	Döntéshozó
A Esemény	Infotv. 26. § (1): időpont, jelleg, rögzített összesített adatok és a bejelentés ténye kiadható.	Közvetett azonosítás: Infotv. 30. § (1). A Kiberbiztonsági tv. 78. § (2), illetve 79/A. § feltételei külön igazolandók.	Kijelölt vezető; iratgazda és jogi terület előkészítése.
B Érintettek	A működési adatok kiadása az Infotv. 26. § (1) alapján; az érintett magánadatára ez nem ad jogcímet.	Név, magánelérhetőség, egészségügyi adat és azonosító kitakarása: Infotv. 30. § (1); GDPR 5–6. és 9. cikk.	Kijelölt vezető, tisztviselői véleménnyel.
C Kapcsolat	Infotv. 26. § (2): feladatköri adatok; GDPR 37. cikk (7): közzétett tisztviselői elérhetőség.	Magánadat és szükségtelen egyéni jogosultság: Infotv. 30. § (1). A GDPR-bejelentés tartalmi előírása önmagában nem nyilvánossági jogcím.	Kijelölt vezető; a tisztviselő saját adatai ügyében is csak véleményez.
D Intézkedés	Infotv. 26. § (1), 27. § (3): javítás, dokumentált eredmény, közpénzügyi költségadat.	Infotv. 27. § (5)–(6) csak tényleges döntés-előkészítésnél. Üzleti titoknál a 2018. évi LIV. törvény 1. § feltételei szükségesek.	Kijelölt vezető; jogi, pénzügyi és informatikai előkészítés.
E Technikai részletek	A hibás kitakarás általános leírása főszabály szerint az Infotv. 26. § (1) alá tartozik.	Kiberbiztonsági tv. 78. § (2): eljárási eredet; 79/A. §: az 1–2. § szerinti közfeladatot ellátó szervezet rendszeradata és igazolt veszélyeztetés. Mindkettő adatonként vizsgálandó.	79/A. § alkalmazásakor a szerv vezetője; jogi és informatikai előkészítéssel.

[134] GDPR 32. cikk (1)–(2) bekezdés, 33. cikk (1) bekezdés; Infotv. 30. § (1) bekezdés. A konkrét ellenőrzési lépések saját szervezési javaslatok.

[135] SZÉKELY – SOMODY – SZABÓ: *i. m.* 17–20. o.

[136] Saját szerkesztés a VI.2. alfejezet negyedik esete alapján. Jogforrások: Infotv. 26. §, 27. § (2) bekezdés i) pont, (3), (5)–(6) bekezdés, 30. § (1) bekezdés; Kiberbiztonsági tv. 78. § (2) bekezdés, 79. és 79/A. §. Fogalmi támpont: BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

2. táblázat A döntési mátrix végrehajtási és felelősségi oldala[137]

Adatkör	Tisztviselői bevonás	Határidő	Technikai ellenőrzés	Dokumentálás
A Esemény	Újraazonosítás és a megmaradó személyesadat-tartalom vizsgálata.	Legfeljebb 15 nap; 30 nap csak törvényi hosszabbítás esetén.	Azonosítható személy nélkül olvasható eseményleírás; mellékletek ellenőrzése.	Iratjegyzék, kezelt összesített adatok, kiadási döntés és megküldött példány.
B Érintettek	A védendő adat és a kitakarás eredményének véleményezése.	Az adatigénylés határidején belül; a GDPR-határidők külön számítandók.	Szövegréteg, másolás, keresés, metaadatok és rejtett adatok ellenőrzése.	Eltávolított adatkör, jogalap, vizsgáló személy és ellenőrzött fájlverzió.
C Kapcsolat	A feladatköri és magánadatok elkülönítésének véleményezése.	Az adatigénylés határidején belül.	Közzétett szakmai csatorna egyeztetése; magánadat és egyéni azonosító eltávolítása.	Nyilvánossági jogcím, tisztviselői álláspont, végső vezetői döntés.
D Intézkedés	Az intézkedés adatvédelmi céljának és a szükséges személyes adatoknak a vizsgálata.	Az adatigénylés határidején belül; a javításról már kezelt adatokból.	Tény és terv elválasztása; dátum, eredmény és költség egyeztetése.	Intézkedési irat, végrehajtási igazolás; részleges elutasítás konkrét indoka.
E Technikai részletek	Adatvédelmi kockázat és a kiadási változat véleményezése; technikai szakértővel.	Az adatigénylés határidején belül; a feltárás nem jelent automatikus halasztást.	Védett és kiadható rész elválasztása; melléklet és végleges fájl ismételt ellenőrzése.	Adat eredete, eljáró szereplő, alkalmazott norma, pontos hatály és kiadási példány.

A negyedik esetben a mátrix A sora alapján a bejelentés és a nyilvántartás megismerhető tényadatait kiadnám, a B sorban az érintettek azonosítóit eltávolítanám, a C sorban pedig a törvény szerint nyilvános feladatköri adatokat megtartanám. A D sorban a végrehajtott javítást és a kezelt közpénzügyi költségadatokat hozzáférhetővé tenném, az E sorban kizárólag igazolt jogalappal zárnék ki adatrészt.

[137] Saját szerkesztés. A felelősségi és ellenőrzési rendhez: GDPR 5. cikk (2) bekezdés, 24., 32. és 38–39. cikk; Infotv. 29. § (1)–(2) bekezdés, 30. § (6) bekezdés. European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *i. m.* 134–136. o.; SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 6–8. o.

A NAIH-nak megküldött saját bejelentést és a belső nyilvántartást ezért nem utasítanám el egészében a Kiberbiztonsági tv. 78. § (2) bekezdésére hivatkozva. Ha a 79/A. § személyi és tárgyi feltételei, valamint a konkrét veszélyeztetés igazolhatók, az érintett rendszeradat kiadását a szervvezető megtagadja, a többi megismerhető rész kiadása mellett. A vezető ellenőrizhető döntéséhez az iratgazda elkészíti az adatkörönkénti minősítési lapot, a tisztviselő rögzíti szakmai álláspontját, az informatika pedig a továbbítandó fájl ellenőrzésének eredményét. Ezzel párhuzamosan külön incidenslapon marad nyomon követhető a kockázatértékelés, a bejelentési döntés és az érintetti tájékoztatás indoka.[138] A mátrixot egy, a hibás PDF-hez hasonló belső gyakorlattal is érdemes kipróbálni. Szabó és Révész adatbiztonsági megközelítését e körben a végrehajtási hibák felismerésére alkalmazom: a gyakorlat akkor eredményes, ha az ügyintéző megjelöli a védendő adatot, az ellenőrző munkatárs pedig a ténylegesen visszafejthető tartalmat megtalálja.[139] Kisebb szervezetben több előkészítő feladat kerülhet ugyanahhoz a személyhez, azonban a tisztviselő függetlenségét és a végső döntési felelősséget ilyenkor is meg kell őrizni. A modell tényleges kockázatcsökkentő hatásának méréséhez további gyakorlati vizsgálat szükséges.

De lege ferenda javaslatomat az Infotv. 30. § (6) bekezdésének kiegészítésére fogalmazom meg. A hatályos rendelkezés előírja a teljesítés rendjét rögzítő szabályzat elkészítését, annak garanciális minimumát azonban nem határozza meg kifejezetten. A negyedik eset elemzése megmutatja, hogy a jogi minősítés, a döntés és a technikai ellenőrzés felelőseinek elkülönítése, valamint a tisztviselő korai bevonásának rendezése a részleges teljesítés gyakorlati feltétele. A módosítás célja e követelmények egyértelmű rögzítése lenne. A hatályos jog alatt ezek belső szabályzatban már megvalósíthatók, kötelező törvényi minimumként azonban külön szövegezést kívánnak.[140] Az Infotv. 30. § (6) bekezdésének jelenlegi mondata után a következő két mondat beillesztését javaslom: „A szabályzat meghatározza az iratfeltárás, az adatok jogi minősítése, a teljesítésről és a korlátozásról való döntés, a kiadási példány technikai ellenőrzése és a teljesítés dokumentálása felelőseit.

[138] Infotv. 30. § (1) és (3) bekezdés, 31. § (2) bekezdés; GDPR 33. cikk (1) és (5) bekezdés, 34. cikk (1) bekezdés. Az adatkiadási döntés és az incidensértékelés egymástól elkülönülő döntési lapja saját szervezési javaslat.

[139] SZABÓ – RÉVÉSZ: *i. m.* 45, 52–53. o.

[140] Infotv. 30. § (6) bekezdés; GDPR 24. cikk (1) bekezdés, 38. cikk (1) bekezdés, 39. cikk (1) bekezdés a)–b) pont. A javasolt kiegészítés saját *de lege ferenda* álláspont, nem a hatályos normaszöveg.

Ha a szervnél adatvédelmi tisztviselő működik, a szabályzat rögzíti a személyes adatok megismerhetőségével kapcsolatos bizonytalanság vagy az adatkiadásból eredő adatvédelmi incidens gyanúja esetén történő bevonásának rendjét azzal, hogy közreműködése nem ruházza át rá a döntési felelősséget és nem módosítja a törvényi határidőket." A javaslat alapjogi hatását a személyes adatok védelmének és az információszabadságnak az együttes érvényesítésében látom: a dokumentált, adatra szabott döntés a kiadás igazolhatóságát, a technikai ellenőrzés pedig a jogellenes személyesadat-közlés megelőzését szolgálja. A módosítás új megtagadási okot és tisztviselői jóváhagyási jogot nem teremtene, a döntési és előkészítő feladatok kisebb szervezetben történő összevonását pedig nem tiltaná meg. A tisztviselő függetlensége és összeférhetetlenségének vizsgálata továbbra is a GDPR alapján érvényesülne. E megoldást arányosabbnak tartom az általános incidensirat-titkosságnál, mert a két alapjog védelméhez szükséges eljárási garanciát erősíti, miközben megőrzi a nyilvánosság törvényi kereteit.[141]

ÖSSZEGZÉS

Eme történeti áttekintés és distinkcióképzés, a hatályos EU-s és hazai jogszabályi rendelkezések együttvizsgálata, az alkalmazhatósági kérdések gyakorlati példákon keresztül történő bemutatása mind egy irányba terelik a dolgozat végkövetkeztetését – a közlés jogszerűségének a *sine qua non*ja, hogy azt elsősorban az egyes adatok minősítése határozza meg (amint arra a Bendik–Péterfalvi-tanulmány is rámutat). [142] A társasági forma, az irat elnevezése vagy a dokumentum eredete önmagában nem válaszol a megismerhetőségre – a közfeladati és közpénzügyi kapcsolatot, a személyes jelleg fennállását, a nyilvánossági rendelkezést és a lehetséges korlátozást egymásra épülő vizsgálatban kell azonosítani az Infotv. adatnyilvánossági rendelkezései és a GDPR együttalkalmazása alapján.[143] Ez Székely, Somody és Szabó döntéstámogatási megközelítésének az itt vizsgált tárgyra történő alkalmazását is jelenti.[144]

[141] Alaptörvény I. cikk (3) bekezdés, VI. cikk (3) bekezdés; GDPR 38. cikk (3) és (6) bekezdés, 39. cikk (1)–(2) bekezdés; Infotv. 29. § (1)–(2) bekezdés. Az alapjogi és szervezeti hatások értékelése a dolgozat saját következtetése.

[142] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.

[143] Infotv. 3. § 5–6. pont, 26. § (1)–(2) bekezdés, 30. § (1) bekezdés; GDPR 5–6. és 86. cikk.

[144] SZÉKELY I. – SOMODY B. – SZABÓ M. D.: *i. m.* 17–20. o.

A nyilvánosság és az adatvédelem összeegyeztetésére vonatkozó első kutatási kérdésre a részleges teljesítés adja a legfontosabb választ: amennyiben a vegyes irat kiadható tartalmát el kell különíteni a meg nem ismerhető adatoktól, a korlátozást az adott tartalommal összefüggésben szükséges indokolni. Amint a Bendik–Péterfalvi-tanulmány alapján is láthattuk, a közérdekből nyilvános személyes adat nem veszíti el személyes jellegét, így kezelésének célja és a közlés jogalapja továbbra is jelentős.[145] Az első munkahipotézis – miszerint az adatfajták elkülönítése és a tételes korlátozási vizsgálat a szabályos teljesítés alapfeltétele – megalapozott, és a leírtak alapján alátámasztható. A bejelentési rendszerek uniós egyszerűsítése esetén az elfogadott változást a magyar tájékoztatókban és belső eljárásokban is követni kellene. Saját javaslatom az Infotv. 30. § (6) bekezdését a felelősségi és ellenőrzési rend minimumával egészítené ki, de a gyakorlati hatás megítéléséhez empirikus kutatás is szükség lenne.

A tisztviselő szerepére vonatkozó kérdésben a korai, megfelelő információkra épülő tanácsadás és az önálló ellenőrzés bizonyult meghatározónak, összhangban Szabó tisztviselői intézményre vonatkozó elemzésével.[146] A más feladatokból származó összeférhetetlenséget a tényleges döntési hatáskör alapján szükséges megítélni – a második munkahipotézist a GDPR garanciái és az X-FAB ügy funkcionális megközelítése együttesen erősítik. A hibás adatkiadásnál az incidens megállapítását és a bejelentési kockázat értékelését külön kell elvégezni. A dokumentálás, a hatósági bejelentés és az érintetti tájékoztatás eltérő feltételeihez Szabó és Révész elemzése is támpontot nyújt.[147] A tudomásszerzés és a hetvenkét órás határidő rögzítése alapvető, a javított adatigénylési teljesítés és az incidenskezelés pedig párhuzamosan lehet szükséges, egymástól eltérő döntési indokokkal.

A harmadik munkahipotézist a bemutatott jogi és szervezési összefüggések alapján tartom indokolhatónak, mert az összekapcsolt, visszakereshető eljárás lehetővé teszi, hogy a társaság az adatkiadás során feltárt hibából az incidenskezelésben is tanuljon. A kockázatcsökkentés mértékét a választott módszer azonban nem mérte, így a negyedik eseten végigvezetett döntési és felelősségi mátrix, a végleges fájl ellenőrzése és a működő jelzési út a normákból levezetett működési modellnek tekinthető, amelynek tényleges eredményessége további gyakorlati vizsgálat tárgya lehet.

[145] BENDIK – PÉTERFALVI: *i. m.* 55–57. o.
[146] SZABÓ E. Gy.: Az adatvédelmi tisztviselőről, *i. m.* 3–4, 6–8. o.
[147] SZABÓ E. Gy. – RÉVÉSZ: *i. m.* 52–53. o.

IRODALOMJEGYZÉK

BENDIK T. – PÉTERFALVI A.: Janus nyomában – a közérdekből nyilvános személyes adatok jellemzői és kezelésük különös szabályai. In *Pro Publico Bono – Magyar Közigazgatás* 2025/2. 49–73. o.

CZÉKMANN Zs.: Az egyén és az állam kapcsolatának megváltozása az IKT hatására – az e-demokrácia fogalmi alapjai. In *Miskolci Jogi Szemle* 2020/1. különszám. 31–37. o.

DE NEGRI L.: A köztulajdonban álló gazdálkodó szervezetek adatainak közzététele Németországban és Magyarországon: hasonlóságok és különbségek. In *Pro Futuro* 2022/1. 83–101. o.

European Union Agency for Fundamental Rights – Council of Europe – European Data Protection Supervisor: *Handbook on European data protection law. 2018 edition.* Luxembourg: Publications Office of the European Union, 2018.

GULYÁS G. Gy.: Gépi tanulási módszerek alkalmazása deanonimizálásra. In *Információs Társadalom* 2017/1. 72–86. o.

JÓRI A.: Az adatvédelemért és az információszabadságért felelős biztos intézményéről. In *Fundamentum* 2010/2. 20–29. o.

KISS A. – KRASZNAY Cs.: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. In *Információs Társadalom* 2017/1. 55–71. o.

KORMÁNY B.: A nemzeti vagyongazdálkodás intézményi modelljei – magyar–lengyel összehasonlító elemzés. In *Jegyző és Közigazgatás* 2026/1. 30–32. o.

SZABÓ E. Gy. – Révész B.: Adataink biztonságban – adatainkban a biztonság? In *Információs Társadalom* 2017/1. 45–54. o.

SZABÓ E. Gy.: Az adatvédelmi tisztviselőről – A GDPR szabályainak elemzése. In *Infokommunikáció és Jog* 2018/1. (70.) 3–10. o.

SZÁDECZKY T. – SZŐKE G. L.: A bizalmasság és a nyilvánosság aktuális kihívásai az információbiztonság tükrében. In *Pro Futuro* 2018/2. 24–41. o.

SZÉKELY I. – SOMODY B. – SZABÓ M. D.: Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása, II. rész: Jogi és döntéstámogatási megközelítések. In *Információs Társadalom* 2017/1. 7–23. o.

SZÉKELY I.: [Fórumhozzászólás az adatvédelem és az információszabadság viszonyáról]. In *Fundamentum* 2004/4. 47–54. o.

TÖRÖK T. S.: Az adatvédelmi tisztviselő pozíciója és szerepe a mesterséges intelligenciáról szóló rendelet kockázati rendszerében. In *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok* 2024/III. 15–32. o.

VÁRADI Sz.: A közszférára vonatkozó adatvédelmi szabályok a GDPR tükrében. In *Pro Futuro* 2019/1. 39–54. o.

INTERNETES FORRÁSOK

Európai Adatvédelmi Testület: Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.0. Elfogadva 2023. március 28. https://dataprotection.gov.sk/files/metod-edpb/edpb_guidelines_202209_personal_data_breach_notification_v2-0_en.pdf (2026. 10. 04.)

Európai Adatvédelmi Testület: EDPB identifies areas of improvement to promote the role and recognition of DPOs. 2024. január 17. A Designation and Position of Data Protection Officers oldalán közölt tájékoztatás. https://www.edpb.europa.eu/documents/coordinated-enforcement-framework/coordinated-enforcement-action-designation-and-position_fr (2026. 10. 04.)

Európai Adatvédelmi Testület – Európai Adatvédelmi Biztos: EDPB–EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus). Elfogadva 2026. február 10. https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf (2026. 10. 04.)

Európai Bizottság: Digital Omnibus. COM(2025) 837 final, 2025. november 19., 2025/0360 (COD). Rendeletjavaslat a digitális jogszabályi keret egyszerűsítéséről. A Tanács ST 15698/25 jelzetű dokumentuma. https://data.consilium.europa.eu/doc/document/ST-15698-2025-INIT/en/pdf (2026. 10. 04.)

Európai Unió Bírósága: C-413/23 P. sz. Európai Adatvédelmi Biztos kontra Egységes Szanálási Testület ügy, 2025. szeptember 4., ECLI:EU:C:2025:645. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:62023CJ0413 (2026. 10. 13.)

Kúria: A „közérdekű adatok kiadásával kapcsolatos perek” bírósági gyakorlata tárgykörére felállított joggyakorlat-elemző csoport összefoglaló véleménye. 2017.EI.II.J.GY.P.3. sz. Lezárva 2018. december 3. https://kuria-birosag.hu/sites/default/files/joggyak/osszefoglalo_velemeny_adatvedelem.pdf (2026. 10. 04.)

Nemzeti Adatvédelmi és Információszabadság Hatóság: Adatvédelmi incidensbejelentő rendszer. https://www.naih.hu/adatvedelmi-incidensbejelento-rendszer (2026. 10. 04.)

Nemzeti Adatvédelmi és Információszabadság Hatóság: Közlemény a Központi Információs Közadat-nyilvántartás felületén közzétételre kötelezett szervek és a közzéteendő adatok körének kiterjesztéséről. 2026. augusztus 14. https://naih.hu/hirek/849-koezlemeny-a-koezponti-informacios-koezadat-nyilvantartas-felueleten-koezzetetelre-koetelezett-szervek-es-a-koezzeteendo-adatok-koerenek-kiterjeszteserol (2026. 10. 04.)

KORMÁNY B.: A nemzeti vagyongazdálkodás intézményi modelljei – magyar–lengyel összehasonlító elemzés. Jegyző és Közigazgatás, 2026/1. 30–32. o. A kiadó adatbázisában nyilvánosan hozzáférhető részlet. https://szakcikkadatbazis.hu/doc/6523176 (2026. 10. 05.)

Nemzeti Adatvédelmi és Információszabadság Hatóság: A Nemzeti Adatvédelmi és Információszabadság Hatóság jelentése a Kormányzati Ellenőrzési Hivatal információszabadsággal kapcsolatos jogsértése tárgyában. NAIH-5513-6/2024. https://www.naih.hu/files/infoszab_jelentes_naih-5513-6-2024.pdf (2026. 10. 05.)

JOGSZABÁLYJEGYZÉK

Hazai jogszabályok

Magyarország Alaptörvénye (2011. április 25.).

1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről.

2009. évi CXXII. törvény a köztulajdonban álló gazdasági társaságok takarékosabb működéséről.

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

2015. évi VII. törvény a Paksi Atomerőmű kapacitásának fenntartásával kapcsolatos beruházásról, valamint az ezzel kapcsolatos egyes törvények módosításáról. Az elemzés a 4/2021. (I. 22.) AB határozatban vizsgált 5. §-ra vonatkozik.

2018. évi LIV. törvény az üzleti titok védelméről.

2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

2026. évi XVIII. törvény az európai uniós forrásokhoz való hozzáférés érdekében szükséges egyes törvények módosításáról.

Uniós jogforrások

Az Európai Unió Alapjogi Chartája. HL C 326., 2012. október 26., 391–407. o.

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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR). HL L 119., 2016. május 4., 1–88. o.

Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről. HL L 295., 2018. november 21., 39. o.

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv). HL L 333., 2022. december 27., 80–152. o.

Az Európai Parlament és a Tanács (EU) 2025/2518 rendelete (2025. november 26.) az (EU) 2016/679 rendelet végrehajtására vonatkozó további eljárási szabályok megállapításáról. HL L, 2025/2518, 2025. december 12. Alkalmazás: 2027. április 2-től, az átmeneti szabályok szerint.

HIVATKOZOTT BÍRÓSÁGI DÖNTÉSEK

Emberi Jogok Európai Bírósága: Magyar Helsinki Bizottság kontra Magyarország [Nagykamara], 18030/11. sz. kérelem, 2016. november 8.

Európai Unió Bírósága: C-453/21. sz. X-FAB Dresden ügy, 2023. február 9., ECLI:EU:C:2023:79.

Európai Unió Bírósága: C-740/22. sz. Endemol Shine Finland ügy, 2024. március 7., ECLI:EU:C:2024:216.

Európai Unió Bírósága: C-413/23 P. sz. Európai Adatvédelmi Biztos kontra Egységes Szanálási Testület ügy, 2025. szeptember 4., ECLI:EU:C:2025:645.

Alkotmánybíróság: 13/2019. (IV. 8.) AB határozat, 4/2021. (I. 22.) AB határozat.

Kúria: Pfv.IV.20.275/2024/4. számú ítélet *(a NAIH-5513-6/2024. számú jelentés 10. oldalán közölt ismertetés alapján).*