A „nagy mennyiségű személyes adat” értelmezése az EIR-ek biztonsági osztályba sorolásánál - Iránymutatás

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/1

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.12	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A jelenlegi jogszabályok nem adnak egzakt választ arra, mi minősül „nagy számban” történő személyes adatkezelésnek, az adatvédelmi hatóságok gyakorlata is csak orientáló jellegű, de az megállapítható, hogy egy települési vagy regionális szintű adatkezelés a kérdéses fogalom alá esik. Az ennél kisebb méretű adatkezelések esetén egyedi kockázatelemzés alapján, esetről esetre szükséges meghatározni az említett feltétel fennállását, figyelemmel arra is, hogy bekövetkezhet-e a 7/2024. (VI. 24.) MK rendeletben meghatározott „közepes” vagy a „nagy” káresemény.

A személyes adatok vagy a különleges adatok „nagy számban” történő sérülésének lehetőségét a GDPR 32. cikkében elvárt (egyébként magas szintű) intézkedések tükrében kell értékelni: személyes adatok vagy különleges adatok akkor sérülhetnek „nagy számban”, ha az elvárt adatbiztonsági intézkedések betartása mellett is bekövetkezhet a „közepes” vagy a „nagy” káresemény.

A 7/2024. (VI. 24.) MK rendeletben az egyes osztályba sorolásoknál meghatározott lehetséges következmények vagylagosak; az a körülmény, hogy a személyes vagy különleges adatok száma adott esetben nem minősül „nagy”-nak, nem zárja ki az adott osztályba sorolást, ha egyéb szempontok megvalósulnak.

2. A DOKUMENTUMBEN ELŐFORDULÓ RELEVÁNS FOGALMAK

A dokumentumban előforduló releváns fogalmak meghatározása a GDPR[1] alapján a következők:

a) „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

b) „különleges adat” vagy „személyes adat különleges kategóriája”: faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

c) „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan

[1] 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 szóló, 2016. április 27-i, (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet)

vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja. A Kiberbiztonsági törvény[2], illetve a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet hatálya alá tartozó szervezet adatkezelőnek minősül, amennyiben személyes adatot vagy különleges adatot kezel;

d) „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Az elektronikus információs rendszer definíciója a Kiberbiztonsági törvény szerint:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy

c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

3. PROBLÉMAFELVETÉS

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: Rendelet) 1. melléklete szerint

a) *„2.2.2. Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel: az elektronikus információs rendszerben ... legfeljebb kis mennyiségű személyes adat sérülhet”*

b) *„2.2.3. A „jelentős” biztonsági osztály esetében közepes káresemény következhet be, mivel: nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet”*

c) *„2.2.4. A „magas” biztonsági osztály esetében nagy káresemény következhet be, mivel ... különleges személyes adat nagy mennyiségben sérülhet”*

Látható tehát, hogy a biztonsági osztályba sorolás *egyik* kritériuma, hogy a személyes adatok nagy számban történő kezeléséről van-e szó. A Rendelet nem egyértelmű, de a szövegezésből az tűnik ki, hogy a „nagy mennyiségű” személyes adat – mint az osztályba sorolás egyik kritériuma – vagylagos kritérium. Amennyiben tehát pl. a jelentős biztonsági osztályba sorolásnál a „nagy mennyiségű” személyes adat kritériuma nem lenne megállapítható, de a *„jogszabállyal (orvosi,*

[2] A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény

ügyvédi, biztosítási, banktitok stb.) védett adat” kritériuma (lsd. 2.2.3.3. kritérium) igen, a „jelentős” biztonsági osztályba sorolás nem maradhat el. Hasonlóképpen, a „jelentős” biztonsági osztályba kell sorolni az elektronikus információs rendszert, ha abban különleges személyes adat kezelése történik.

A 2.2.3. és a 2.2.4. pont szerinti kritériumoknál figyelemmel kell lenni arra is, hogy a Rendelet különbséget tesz a „rendes” és a „különleges” személyes adatok között, sőt arra is, hogy a Rendelet csak „kis mennyiségű” és „nagy mennyiségű” személyes adat között tesz különbséget, nincs tehát „normál mennyiségű” személyes adat.

A Rendelet nem határozza meg a „nagy mennyiségű” személyes adat fogalmát, ilyen definíció a Kiberbiztonsági törvényben sem szerepel.

A *„személyes adatok nagy számban történő kezelése”* kifejezés szerepel ugyanakkor a GDPR-ban, egzakt meghatározás nélkül. A kérdéses kifejezés értelmezését a WP29 (A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport – az Európai Adatvédelmi Testület elődje) végezte el a vonatkozó iránymutatásaiban. Azonban a WP29 is elismerte,[3] hogy *„[v]alójában nem lehet pontosan megadni sem a kezelt adatok mennyiségét, sem az érintett személyek számát, amely minden helyzetben alkalmazandó lenne. Ez azonban nem zárja ki annak lehetőségét, hogy idővel kialakul egy általános gyakorlat annak pontosabb és/vagy számszerűsített meghatározására, hogy mit jelent a ’nagy mértékű / nagy számban történő’ kifejezés bizonyos típusú adatkezelési tevékenységek tekintetében.”*

4. A „SZEMÉLYES ADATOK NAGY SZÁMBAN TÖRTÉNŐ KEZELÉSE” ÉRTELMEZÉSE

A GDPR több helyen is említi ezt a kifejezést, mindig személyes adatok különleges kategóriáinak és a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok (bűnügyi adatok) nagy számban történő kezelésével összefüggésben.[4] A GDPR még két esetben említi „nagy mennyiségű” személyes adat/információ kezelését[5] (függetlenül az adat fajtájától).

Az a tény, hogy a GDPR a különleges adatok és a bűnügyi adatok kapcsán említi a „nagy számban” történő adatkezelést, nem jelenti azt, hogy a Rendelet alkalmazásában (különösen az 1. melléklet 2.2.3. pontja alkalmazásában) is csak a különleges adatok és a bűnügyi adatok kezelésével összefüggésben lehet használni ezt a kifejezést: ahogy fentebb utaltunk rá, a 2.2.3. és a 2.2.4. pont szerinti kritériumoknál figyelemmel kell lenni arra is, hogy a Rendelet különbséget tesz a „rendes” és a „különleges” személyes adatok között.

[3] Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban – **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf**, 9. oldal

[4] lsd. GDPR 27. cikk (2) bek. a) pont, 35. cikk (3) bek. b) pont, 37. cikk (1) bek. c) pont.

[5] Lsd. GDPR (63) és (75) preambulumbekezdését

A WP29 két iránymutatásában[6] is (lényegileg azonos tartalommal) értelmezte a „nagy mennyiségben / nagy számban” kifejezést. Fontos azonban megemlíteni, hogy – ahogy arra a WP29 is rámutat – a „nagy mennyiségben” / „nagy számban” kifejezéseket mindig abban az összefüggésben kell értelmezni, amilyen összefüggésben a GDPR említi[7] (a GDPR a hatásvizsgálattal és az adatvédelmi tisztviselő kijelölésével, továbbá az érintett hozzáférési jogának gyakorlásával, illetve a GDPR 24. cikke szerinti adatkezelői kötelezettségekkel összefüggésben említi a „nagy számban”, illetve „nagy mennyiségben” kifejezéseket). Erre figyelemmel a következőkben írtak pusztán orientáló jellegűek.

A GDPR (91) preambulumbekezdése is nyújt némi támpontot, amikor *„jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelésé”*-ről, illetve *„az érintettek jelentős számára hatással”* levő adatkezelést vonja a „nagy számban” kifejezés alá. A WP29 szerint *„különösen az alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e:*

a. az érintettek száma konkrét számadatként vagy a lakosság arányában;

b. a kezelt adatok mennyisége vagy adatfajták köre;

c. az adatkezelési tevékenység időtartama vagy állandó jellege;

d. az adatkezelési tevékenység földrajzi kiterjedése.”

A WP29 példákat is ad *„a nagymértékű vagy nagy számban történő adatkezelésre:*

- *a betegek adatainak kezelése a kórház szokásos működése keretében*
- *városi tömegközlekedést használó személyek utazási adatainak kezelése (például menetjegyek nyomon követése)*
- *egy nemzetközi gyorsétteremlánc ügyfeleire vonatkozó valós idejű helymeghatározási adatok statisztikai célú kezelése egy ilyen tevékenység végzésére specializálódott adatkezelő útján*
- *ügyféladatok kezelése egy biztosító társaság vagy egy bank szokásos üzletmenete keretében*
- *személyes adatok keresőmotor általi kezelése viselkedésalapú reklám céljából*
- *adatok (tartalom, forgalom, hely) kezelése telefon- vagy internetszolgáltatók által”*[8]

[6] Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e – **https://www.naih.hu/files/WP248_rev01_hu.pdf**, illetve Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban – **https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf**

[7] Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban – 9. oldal, 14. lábjegyzet.

[8] Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban – 10. oldal

A hatásvizsgálatokkal összefüggésben a WP29 szerint „nagy számban” történő adatkezelések a következők:[9]

- *„A betegek genetikai és egészségügyi adatait kezelő kórház (kórházi információs rendszer).”*
- *„A közösségi médiából származó nyilvános adatok gyűjtése profilalkotás céljából.”*
- *„A feliratkozóknak általános napi sajtószemle küldéséhez levelezőlistát használó internetes magazin.”*

A NAIH gyakorlatában a hatásvizsgálati „fekete” listában[10] fordul elő a „nagy számban” kifejezés, továbbá egyes határozatokban a bírságkiszabás szempontjából releváns (súlyosító) körülmény, ha a jogsértéssel érintett személyek száma magas.[11]

Ami az egyes pontok lehetséges magyarázatát illeti, a következőkre érdemes felhívni a figyelmet.

ad a) Egy országos adatbázis (pláne az állami alapadatbázisok) vitán felül állóan „nagy számban” kezelnek személyes adatot. Tekintve azonban, hogy az „adatkezelés” nem csak az adatok tárolását, hanem az azokhoz való hozzáférést is jelenti (GDPR 4. cikk 2 pont), a „nagy számban” történő adatkezelés kategóriájába kell sorolni mindazon EIR-ek által történő adatkezelést is, amelynek révén az említett országos adatbázishoz hozzá lehet férni. Más szavakkal: egy országos adatkezelési rendszer regionális és helyi szintű komponenseit is „nagy számban” történő adatkezelés körébe lehet vonni, különösen, ha a helyi rendszereken keresztül az országos rendszer más komponensei is elérhetők.

Figyelemmel a WP29 által adott példákra, egy szervezeten belül az érintettek *egészét* érintő adatkezelés „nagy számban” / „nagy mennyiségben” történő adatkezelésnek minősülhet, különösen, ha maga a szervezet is nagyobb, tagolt struktúrájú (pl. kórház, bank, biztosító társaság, internetszolgáltató a fenti példálózó listában) vagy tevékenysége legalább egy település egészét lefedi.

ad b) A *„kezelt adatok mennyisége vagy adatfajták köre”* szempontjából nézve a kérdést, minél több adatmezőt tartalmaz egy rekord, annál nagyobb számban történő adatkezelésről beszélhetünk. Nem esik ebbe körbe pl. egy hírlevélre feliratkozáskor kezelt néhány személyes adat, de mindenképpen nagy mennyiségű személyes adatkezelésnek minősül pl. a profilozáshoz használt adatok kezelése, vagy olyan adatkezelés, amely több forrásból megszerzett adatok összevetésén alapuló elemzést végez. Mivel ez az eset különálló esetként szerepel a WP29

[9] Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e – 13-14. oldal

[10] pl. hitelképesség értékelése, fizetőképesség értékelése, profilozás, munkavállaló munkájának megfigyelése, illetve a kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése

[11] Lásd pl. NAIH/2019/55 (kb. 800.000 érintett), NAIH/2019/2668 (több mint 6.000 érintett), NAIH/2019/3107/7, NAIH/2020/54/4 („tízezres nagyságrend”), NAIH/2020/308, NAIH/2020/952 (kb. 15.000 db személyes adat), NAIH/2020/974/4 (kb. 680.000 fő), NAIH/2020/1137 (kb. 100 érintett), NAIH/2020/1160/10, NAIH/2020/1866/5 (kb. 300 fő), NAIH/2020/2546/15, NAIH/2020/2758/4 („milliós nagyságrend”) határozatok.

listájában, kevés érintettet érintő, de az egy-egy érintettről nagy számú adat kezelése megalapozza e kritériumnak az alkalmazását.

ad c) Hasonlóan az előző pontban írtakhoz, az „*adatkezelési tevékenység időtartama vagy állandó jellege”* kritérium esetén az állandó jelleggel (határozatlan időtartamra) létrehozott adatbázisokban történő adatkezelés „nagy számban” történő adatkezelésnek minősül, míg egyéb esetben az adatkezelés tervezett időtartama befolyásolja a kritérium megvalósulását. Egy adott eseményre korlátozódó adatkezelés nem fog – pusztán emiatt – „nagy számban” történő adatkezelésnek minősülni (de az eseményen részt vevők száma indokolhatja a „nagy számban” történő adatkezelés megállapítását).

ad d) Az „*adatkezelési tevékenység földrajzi kiterjedése”* szempontjából – figyelemmel a WP29 által felhozott példákat is – egy település egészét érintő adatkezelés már kielégíti a „nagy számban” történő adatkezelés kritériumát.

A WP29 iránymutatásából kiviláglik, hogy az általuk megadott kritériumok szintén vagylagosak, azaz bármelyikük bekövetkezése esetén megállapítható a „nagy számban” történő adatkezelés. Ha több kritérium is teljesül, a „nagy számban” történő adatkezelés megállapítása nagy bizonyossággal nem maradhat el.

5. EGYÉB SZEMPONTOK

A Rendelettel összefüggésben nem hagyhatók figyelmen kívül a Rendelet 1. melléklet 2.1. pontjában írt „Általános irányelvek” sem. Ezek szerint *„az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal”* kell érvényesíteni, továbbá *„az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg.”*

Az osztályba sorolás alapvetően a kár nagysága szerint történik („csekély”, „közepes”, illetve „nagy” káresemény).

A fentiek a GDPR logikájában „kockázatalapú” megközelítésnek nevezett hozzáállással mutatnak rokonságot. A GDPR alapvetően azt várja el az adatkezelőktől, hogy *„a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket”* hozzanak és hajtsanak végre *„annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot”* garantáljanak (32. cikk). [Ez a megközelítés jobban kidomborodik a Rendelet 1. melléklet 2.2.2., 2.2.3. és 2.2.4. pontjainak fentebb nem hivatkozott egyéb alpontjaiban (amelyek pl. a reputációs kárral vagy anyagi kárral vagy egyéb, társadalmi szempontból fontos következményekkel foglalkoznak).]

A személyes adatok vagy a különleges adatok „nagy számban” történő sérülésének lehetőségét tehát a GDPR 32. cikkében elvárt (egyébként magas szintű) intézkedések tükrében kell értékelni: személyes adatok vagy különleges adatok akkor sérülhetnek „nagy számban”, ha az elvárt

adatbiztonsági intézkedések betartása mellett is bekövetkezhet a „közepes” vagy a „nagy” káresemény. Az elvárt adatbiztonsági intézkedések tehát „mérséklő hatásúak” az osztályba sorolás szempontjából.

6. KÖVETKEZTETÉSEK

Nincs egzakt meghatározás a személyes vagy különleges adatok „nagy számára”, azt esetről esetre kell meghatározni, figyelemmel arra is, hogy bekövetkezhet-e a Rendeletben meghatározott „közepes” vagy a „nagy” káresemény. A személyes adatok vagy a különleges adatok „nagy számban” történő sérülésének lehetőségét a GDPR 32. cikkében elvárt (egyébként magas szintű) intézkedések tükrében kell értékelni: személyes adatok vagy különleges adatok akkor sérülhetnek „nagy számban”, ha az elvárt adatbiztonsági intézkedések betartása mellett is bekövetkezhet a „közepes” vagy a „nagy” káresemény.

A Rendeletben az egyes osztályba sorolásoknál meghatározott lehetséges következmények vagylagosak; az a körülmény, hogy a személyes vagy különleges adatok száma adott esetben nem minősül „nagy”-nak, nem zárja ki az adott osztályba sorolást, ha egyéb szempontok megvalósulnak.