Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái; bűnügyi személyes adatok

Balogh Gyöngyi – Bíró János – Deák Ferenc – Kovács Melinda – Tömösi Ramóna

A hatályosított kiadvány
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„**A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése**” című projekt
keretében készült el és jelent meg.

Szerzők:
© Dr. Bíró János
© Dr. Deák Ferenc
© Dr. Kovács Melinda
© Dr. Tömösi Ramóna
© Dr. Sziklay Júlia

Hatályosítást végezte:
Dr. Tömösi Ramóna

Szakmai lektor:
Dr. Péterfalvi Attila

Olvasószerkesztő:
Császár-Biró Anna

A kézirat lezárásának dátuma:
2019. május 7.

Kiadja:
© NKE, 2019

Felelős kiadó:
Prof. Dr. Kis Norbert
Dékán

TARTALOM

1. A GDPR ÉS A HAZAI ADATVÉDELMI JOG TÁRGYI HATÁLYÁNAK ELHATÁROLÁSI KÉRDÉSEI

1.1. Történeti áttekintés

Magyarországon a demokratikus jogállam létrejötte óta az Alkotmányban, majd az Alaptörvényben nevesített alapvető jogok közé tartozik a személyes adatok védelme, amelyet az Alkotmánybíróság 15/1991. (IV. 13.) AB határozata információs önrendelkezési jogként határozott meg. Az adatvédelem alapvető szabályait először a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban Avtv.) tartalmazta. Az Alkotmánybíróság AB határozatai a továbbiakban is kulcsszerepet töltöttek be. Az Alkotmánybíróság az ítélkezési gyakorlatában következetesen figyelembe vette az adatvédelem korszerű európai és nemzetközi jogi eredményeit, így például az Emberi Jogok Európai Bírósága esetjogát, összekapcsolva ezáltal a magyar jogi szabályozást az európai jogfejlődés főáramával. Magyarország az európai csatlakozás kapcsán harmonizálta a magyar jogot a 95/46/EK európai parlamenti és tanácsi irányelv és más, adatvédelemmel összefüggő uniós aktusokban meghatározott követelményekkel.

Az Alkotmány helyébe lépő Alaptörvény számos, az Alkotmánybíróság által kimunkált alkotmányos követelményt az Alaptörvényben meghatározott tételes jog szintjére emelt. Ami a személyes adatok védelmét illeti, a korábbi Alkotmányban foglaltakkal azonosan szerepel az Alaptörvényben, tehát az alapvető jog már elért védelmi szintjének alapvető alkotmányos keretei továbbra is adottak. Az alapvető szabályokat 2012-től már nem az Avtv., hanem az annak helyébe lépő új adatvédelmi törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) tartalmazza, mellyel összhangban szektorális törvények (például a büntetőeljárási törvény, az egészségügyi adatkezelésről szóló törvény) rendelkeznek a különféle, kötelező adatkezelésekről.

(Az Infotv. a korábbi Avtv. szabályozási modelljét átvéve, a magyar információs alapjogi hagyományoknak megfelelően egy törvényben szabályozza a személyes adatok védelmét és a közérdekű adatok megismerésére vonatkozó alapvető szabályokat, azonban tárgyunk szempontjából csak az adatvédelem lényeges, ezért a továbbiakban az Infotv. információszabadságra vonatkozó szabályainak ismertetését mellőzzük.)

Összességében megállapítható, hogy a magyar adatvédelmi jog a rendszerváltástól a GDPR alkalmazhatóvá válásáig terjedő időszakban részben belső, részben nemzetközi és európai jogi impulzusok hatására a nemzeti jogrend keretei között változott, fejlődött. Ennek eredményeként a személyes adatok védelmének hazánkban biztosított szintje az Európai Unió tagállamai között az egyik legmagasabbnak tekinthető.

A jelenhez érkezve meghatározó jelentőségű a GDPR, mert ezáltal az adatvédelem általános jogi kereteinek szabályozása nagyrészt európai uniós szintre került át. Ugyanakkor nemzeti szinten továbbra is az Infotv. tartalmazza az adatvédelem alapvető szabályait a GDPR hatályán kívüli tárgykörökben.

A GDPR alkalmazandóvá válásával számos adatkezelésre vonatkozó szektorális jogszabály is

felülvizsgálandó. E folyamat a jelen jegyzet írásakor folyamatban van.

Az Infotv. 2018-as módosítása a GDPR-on kívül egy másik uniós jogi szabályozási aktus átültetése miatt is szükséges volt. Ez *„a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv”* (a továbbiakban bűnügyi adatvédelmi irányelv).

1.2. Az európai uniós és magyar szabályozás összefüggései

A szabályozás tagállami szintjének taglalását megelőzően a jobb áttekintés érdekében érdemes röviden felvázolni az adatvédelmi szabályozás egészét, így az Infotv. és a GDPR viszonyát, valamint a tágabb alkotmányos és jogrendszeri összefüggéseket.

1.2.1. A GDPR összefüggése a magyar jogrendszerrel

A személyes adatok védelméhez való jog az Alaptörvényben nevesített alapvető jog. Az Alaptörvény I. cikk (3) bekezdése szerint az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható. Az Infotv. az Alaptörvény I. cikk (3) bekezdésének megfelelően törvényi szinten határozza meg a személyes adatok védelméhez való jog alapvető szabályait, valamint a jogkorlátozás általános kereteit.

A GDPR európai parlamenti és tanácsi rendelet, amely általános hatályú, teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállam területén. A GDPR nem törvény, ezért nem felel meg az Alaptörvény I. cikk (3) bekezdése szerinti törvényi szabályozási követelménynek. A GDPR magyar jogrendszerhez kapcsolódása azonban nem az Alaptörvény I. cikk (3) bekezdésén alapul, hanem az Alaptörvény E) cikkén, amelynek (3) bekezdése szerint az Európai Unió joga megállapíthat általánosan kötelező magatartási szabályt. Ennek feltételeit ugyanezen cikk (2) bekezdése tartalmazza. Eszerint Magyarország az alapító szerződésekből fakadó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges mértékig az Alaptörvényből eredő egyes hatásköreit a többi tagállammal közösen, az Európai Unió intézményei útján gyakorolhatja. Az e bekezdés szerinti hatáskörgyakorlásnak összhangban kell állnia az Alaptörvényben foglalt alapvető jogokkal és szabadságokkal, továbbá nem korlátozhatja Magyarország területi egységére, népességére, államformájára és állami berendezkedésére vonatkozó elidegeníthetetlen rendelkezési jogát.

1.2.2. Az Alaptörvény és a GDPR

Az Alaptörvény E) cikk (3) bekezdése ugyanezen cikk (2) bekezdésre utalva tartalmi elvárásokat fogalmaz meg az Európai Unió joga által megállapított, Magyarországon kötelezően alkalmazandó magatartási szabályokat illetően. Témánk szempontjából ilyen különösen az Alaptörvényben foglalt alapvető jogokkal és szabadságokkal való összhang követelménye. Ez vonatkozik a GDPR-ra is,

amely az Európai Parlament és a Tanács közös jogalkotási aktusa. A Tanács és az Európai Parlament nincs alávetve a magyar Alaptörvénynek, ezért felmerülhet az a kérdés, hogy mi a garancia GDPR szabályozási tartalmának az Alaptörvénnyel való összhangjára.

A kérdés megválaszolásához érdemes felidézni, hogy a gyors infokommunikációs fejlődés, valamint az adatvédelmi jogi szabályozást szükségessé tevő más veszélyek és kihívások a globalizáció körülményei közepette világszerte jelentkeznek. Az egyes országok az internet és az információs társadalmak korában hasonló kihívásokkal szembesülnek, amelyekre a technikai fejlettségüknek, a rendelkezésre álló erőforrásainak, és nem utolsó sorban a társadalmi berendezkedésüknek megfelelően reagálnak. A fejlett demokratikus jogállamok értékrendje és eszközrendszere hasonló, ezért a globális jellegű kihívásokra – ide értve az adatvédelem terén jelentkezőket is – elsősorban az együttműködés előnyeinek kiaknázásával és hasonló jogi szabályozási eszközök létrehozásával reagáltak. Az adatvédelem nemzetköziesedése – valamint Európa demokratikus országaiban az europaizálódása – évtizedes múltra tekinthet vissza. Elég az Európa Tanács Adatvédelmi Egyezményére, vagy az Európai Alapjogi Chartára gondolni. Tehát egyáltalán nem új jelenség az, hogy a nemzeti jogrendszeri keretek között alapvető jognak minősülő adatvédelem szabályozási tartalmát mind nagyobb mértékben befolyásolták a nemzetközi és európai jogi hatások. Ezt alátámasztja az is, hogy már a GDPR alkalmazandóvá válása előtt is egy európai uniós szabályozási aktust, a 95/46/EK európai parlamenti és tanácsi irányelvet átültető szabályok képezték a magyar adatvédelmi törvény normaanyagának jelentős részét. Magyarország eddig is a fejlett demokratikus jogállamok közös értékrendjének megfelelően építette fel a jogrendjét, ezért képes volt arra, hogy megrázkódtatások nélkül integrálja a kívülről érkező szabályozási impulzusokat. Bízni lehet abban, hogy az sem fog alkotmányos konfliktust okozni, hogy a GDPR által az adatvédelem jogi szabályozásának tetemes része az európai uniós jog részévé vált. Annál is inkább, hiszen Magyarország részt vett az Európai Parlament és a Tanács munkájában a GDPR előkészítése során, ezért mód volt a magyar alkotmányos szempontok artikulálására.

A GDPR és a magyar alkotmányossági követelmények összeegyeztetése szempontjából az is lényeges, hogy bár a GDPR a tagállamok jogegységesítését célozza, ám számos kérdésben megengedi, sőt megkívánja azt, hogy a tagállamok pontosító vagy kiigazító szabályokat fogadjanak el. Ez lehetőséget ad a tagállamoknak arra, hogy a nemzeti jogfejlődésük és az alkotmányos berendezkedésük sajátosságaihoz igazítsák a GDPR alkalmazását.

1.2.3. A szabályozás szerkezete

1.2.3.1. A szabályozás európai uniós és tagállami összetevői

A GDPR tárgyi hatálya nem terjed ki valamennyi, személyes adatra vonatkozó adatkezelésre. A magyar joghatóság alá tartozó, ám a GDPR hatályán kívül eső adatkezeléseket illetően a magyar állam az Alaptörvény I. cikk (3) bekezdése alapján köteles a személyes adatok védelmének alapvető szabályait törvénybe foglalni. (Ugyanez következik az Európa Tanács 1998. évi VI. törvénnyel kihirdetett adatvédelmi egyezményéhez tett magyar nyilatkozatból is.) Az uniós jog előfoglalásának elvére tekintettel a GDPR alkalmazandó válását követően a magyar (tehát tagállami szintű) adatvédelmi jogi szabályozási hatáskör a GDPR-ral összefüggésben alapvetően a következőkre korlátozódik:

- a GDPR-t illetően csak azon pontosító és kiegészítő szabályokra, amelyek megalkotására a GDPR kifejezetten lehetőséget ad a tagállamok számára, és amelyek szükségesek a GDPR alkalmazásához, valamint
- a GDPR hatályán kívül eső, ám az Alaptörvényből levezethetően adatvédelmi jogi szabályozást igénylő tárgykörökre.

A 2018-ban a GDPR alkalmazandóvá válása kapcsán módosított Infotv. tárgyi hatálya eszerint lett meghatározva. (A GDPR és az Infotv. hatályának pontos elhatárolásáról később lesz szó.)

1.2.3.2. Vertikális tagolódás

A GDPR-hoz kapcsolódó végrehajtási aktusok megalkotására is az európai uniós szabályozási mechanizmus keretén belül fog sor kerülni.

A tagállami szabályozás jogkörben maradó tárgyköröket illetően változatlanok a szabályozás vertikális szerkezetét meghatározó alkotmányos követelmények: az Alaptörvény I. cikk (3) bekezdése törvényi jogforrási szintű szabályozást kíván meg. A 34/1994. (VI. 24.) AB határozatban foglaltak alapján az alapvető joggal távoli és közvetett kapcsolatban álló részletszabályokat alacsonyabb jogforrási szintű jogszabály is megállapíthatja, de ez jogszabálynak nem minősülő norma szintjére nem szubdelegálható.

1.2.4. Néhány gondolat az Infotv. és a GDPR értelmezése kapcsán

Az absztrakt szinten definiált jogi normák a jogalkalmazás során mindig jogértelmezésre szorulnak. A jogértelmezés módszerei a jogi tanulmányok részei és bő szakirodalommal rendelkeznek. Jelen pontban elég egy szűkebb tárgykörre felhívni a figyelmet, mégpedig arra, hogy mind a magyar jogrendnek, mind az Európai Unió jogrendjének megvannak a maguk sajátos jogértelmezési forrásai, vagyis azok a szabályok, tételek, elvek, amelyek figyelembe veendők egy-egy adatvédelmi tárgyú jogi norma értelmezésekor. Lényeges, hogy a magyar jog és az európai uniós értelmezési forrásai általában nem „csereszabatosak", ezért a jogalkalmazónak tudnia kell azt, hogy mikor melyikhez folyamodhat. Ezeket célszerű az alábbiak szerint csoportosítani:

1. A magyar jogrend „belső" jogértelmezési forrásai.
2. A magyar jogszabályok értelmezése az európai unió jogrendjével összefüggésben.
3. Az Európai Unió jogi normáinak értelmezése.

A téma bonyolultsága és terjedelme miatt csak vázlatosan, részlegesen és hangsúlyozottan praktikus szempontokat szem előtt tartva utalunk néhány, az adatvédelmi jogi normarendszer tagállami és európai uniós szintjével kapcsolatban figyelembe veendő jogértelmezési forrásra:

a) A magyar tagállami adatvédelmi jog értelmezése: az Alaptörvény 28. cikke szerint a bíróságok a jogalkalmazás során a jogszabályok szövegét elsősorban azok céljával és az Alaptörvénnyel összhangban értelmezik. Az Alaptörvény és a jogszabályok értelmezésekor azt kell feltételezni, hogy a józanésznek és a közjónak megfelelő, erkölcsös és gazdaságos célt szolgálnak. Az Alaptörvény ezt a bíróságoknak címezi, ám a gyakorlatban valamennyi jogalkalmazó szervre irányadóak, az Infotv.-vel összefüggésben is. Hasonlóképpen törvények is tartalmaznak a személyes adatok kezelésével és védelmével kapcsolatos, a magyar jog által szabályozott jogviszonyokra is vonatkoztatható értelmezési szabályt, például a Ptk., vagy a magánélet védelméről szóló törvény. Az értelmezést segítik a jogszabályokban rögzített értelmező rendelkezések és jogelvek is. Az Alkotmánybíróság adatvédelmi vonatkozású AB határozataiban lefektetett tételek, valamint az adatkezeléssel, adatvédelemmel kapcsolatos ügyekben hozott magyar bírósági határozatok is tartalmaznak a jogszabályok értelmezésekor figyelembe veendő iránymutatásokat.[1]
b) Szempontunkból elsősorban az uniós irányelvet átültető törvények értelmezése a lényeges, mert az Infotv. is ilyen természetű, hiszen az adatvédelmi normaanyagának nagy része a bűnügyi adatvédelmi irányelvet ülteti át.

[1] Az Alaptörvény VII. módosítása is tartalmaz a jogszabályok értelmezésével kapcsolatos előírásokat, azonban az ezek alkalmazásához szükséges törvénymódosítások tartalma még nem ismert.

Az Európai Bíróság az irányelveket átültető tagállami jogszabályok kapcsán dolgozta ki az úgynevezett értelmezési doktrinát, amely szerint a tagállamok bíróságai az uniós irányelvben rögzített eredmény eléréséhez az irányelvekkel összhangban, az irányelvek szövege és célja fényében kötelesek értelmezni a nemzeti jogot. Ez nemcsak a tagállamok bíróságaira, hanem a nemzeti jog értelmezésére és alkalmazására hatáskörrel rendelkező valamennyi tagállami hatóságra vonatkozik.

Ugyanakkor az irányelvet átültető jogszabályok – mint például az Infotv. – értelmezésekor az értelmezési doktrína mellett a magyar jogrendben érvényesülő, a fenti a) pontnál vázolt „belső" értelmezési források is figyelembe veendők, hiszen az irányelvet átültető jogszabályok is a magyar jogrendszer részei.

c) A GDPR értelmezése: a magyar jogszabályokkal kapcsolatban fentebb vázolt értelmezési előírások több okból sem vonatkoztathatók rá:
   - Formálisan azért nem, mert a GDPR kívül esik a magyar jogszabályok Alaptörvényben meghatározott rendszerén.[2]
   - Lényegében azért nem, mert a tagállamok nem jogosultak a rendeleti szintű európai uniós jogalkotási aktus értelmezésére, következésképp az értelmezés módját meghatározó jogszabályok és kötelező jellegű határozatok megalkotására sem.

A GDPR egységes értelmezését alapvetően az Európai Bíróság ítélkezési gyakorlata és az Európai Adatvédelmi Testület állásfoglalásai biztosítják, ugyanakkor érdemes szem előtt tartani, hogy a GDPR maga is tartalmaz értelmezésére vonatkozó előírásokat, lásd például a (150) vagy (153) preambulumbekezdéseket.[3]

Megemlítendő még az Emberi Jogok Európai Bíróságának (EJEB) esetjoga is, amely támpontul szolgálhat az alapvető jogokra vonatkozó európai uniós szintű jogforrások értelmezéséhez. Ez azért lehetséges, mert az Európai Unióról szóló szerződés 6. cikk (3) bekezdése szerint az alapvető jogok, ahogyan azokat az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (EJEE) biztosítja, továbbá ahogyan azok a tagállamok közös alkotmányos hagyományaiból következnek, az uniós jogrend részét képezik mint annak általános elvei, továbbá az Európai Unió Alapjogi Chartája 52. cikkének (3) bekezdése azt a kötelezettséget írja elő, hogy a Chartában foglalt, az EJEE által biztosított jogoknak megfelelő jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az EJEE-ben szerepelnek.

1.2.5. A szabályozás széttagoltságáról és egységéről

Az eddigi gondolatmenet a GDPR és a magyar adatvédelmi jog (elsősorban az Infotv.) különbözőségeit hangsúlyozta mind a jogrendszeri kapcsolódások, mind a szabályozás struktúrája, mind a jogértelmezés kapcsán. Ugyanakkor szem előtt tartandó, hogy az adatvédelmi szabályozás európai uniós és nemzeti normaanyaga együttesen tartalmazza a Magyarországon alkalmazandó jogot. Mind az érintett adatalanyok, mind az adatkezelők és adatfeldolgozók, mind a tagállami jogalkalmazó szervek számára lényeges, hogy a szabályozás konzisztens rendszert alkosson, amelyben világosan

[2] Az Alaptörvény T) cikke szerint „általánosan kötelező magatartási szabályt az Alaptörvény és az Alaptörvényben megjelölt, jogalkotó hatáskörrel rendelkező szerv által megalkotott, a hivatalos lapban kihirdetett jogszabály állapíthat meg. [...] (2) Jogszabály a törvény, a kormányrendelet, a miniszterelnöki rendelet, a miniszteri rendelet, a Magyar Nemzeti Bank elnökének rendelete, az önálló szabályozó szerv vezetőjének rendelete és az önkormányzati rendelet. Jogszabály továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendelete."

[3] Az uniós jogi szabályozási aktusok általában bőségesen tartalmaznak fogalommeghatározásokat, valamint olyan, bekezdésekre tagolt preambulumszöveget, amely megvilágítja a szabályok célját, illetve összefüggéseit, segítséget nyújtva a jogértelmezéshez.

elhatárolható legyen egymástól az európai uniós és a nemzeti jog szabályozási területe, illetve világosak legyenek azok az összefüggések, amelyek olyankor lényegesek, amikor adott esetben olyan adatkezelés jogszerűségét kell megítélni, amely a jogi szabályozás nemzeti és európai uniós szintjéhez is kapcsolódik valamilyen módon. Lássuk, milyen tényezők biztosítják a közös nevezőt a szabályozás e két, egymástól eltérő része között:

- Az adatvédelmi jog alapvető szerkezete és jogintézményei az elmúlt évtizedek során kialakultak és megszilárdultak, mind az elveket (például az adatkezelés célhoz kötöttsége), mind a jogviszonyok tartalmát és alanyait (érintett, adatkezelő stb.), mind a sajátos szakkifejezések (például hozzájárulás, adattörlés) jelentését illetően. Ezek általánosan elfogadottá váltak a demokratikus jogállamok nemzeti jogrendszereiben, a vonatkozó nemzetközi dokumentumokban és a szaktudományos közösség által. A GDPR és az Infotv. egyaránt ezekre a fogalmakra, elvekre és jogintézményekre alapoz. Tehát az adatvédelmi jog nemzeti és európai uniós szintje nagyjából ugyanazokból elemekből, „építőkockákból" lett konstruálva, ezért az egyes elemeik könnyen összehasonlíthatók egymással, sőt, gyakorta megfeleltethetőek is egymásnak.
- Történetileg úgy alakult, hogy 2012-ben az Európai Unió adatvédelmi reformja keretében párhuzamosan két, egymással összefüggő jogalkotási aktus előkészítése kezdődött meg, nevezetesen a GDPR-é és a bűnügyi adatvédelmi irányelvé. E kettősségnek nem az volt az oka, hogy az Európai Unió két alapvetően eltérő adatvédelmi rezsimet akart volna létrehozni, hanem pusztán az, hogy bár az adatvédelem egészét illetően az uniós szinten az egységesen magas védelmi szint biztosítása érdekében a jogegységesítés tűnt kívánatosnak, az előkészítő tárgyalások során az az álláspont győzedelmeskedett, hogy a (némileg leegyszerűsítve megfogalmazva) bűnüldözés olyan speciális, a nemzeti szuverenitáshoz közel álló tárgykör, amelyhez kapcsolódó adatkezelések esetében az adatok védelmét és az áramlását illetően nagyobb teret kell hagyni a tagállami jogalkotás számára. Ennek megfelelően e tárgykörben nem a jogegységesítés, hanem a jogharmonizáció kívánatos, következésképp nem uniós rendeleti úton, hanem irányelv által szabályozandó. (Emlékeztetőül: az irányelv az elérendő célokat illetően minden címzett tagállamra kötelező, azonban a forma és az eszközök megválasztását a nemzeti hatóságokra hagyja.) Ezek alapján érthető az, hogy a bűnügyi adatvédelmi irányelv felépítése és számos szabálya párhuzamos az alapul vett GDPR joganyagával, mind az elveket, mind a fogalmakat, mind a jogintézményeket illetően. Ez természetesen korántsem jelenti azt, hogy a két szabályozás teljesen azonos lenne, hiszen a bűnügyi adatvédelmi irányelv szabályozási tárgykörébe tartozó adatkezeléseknek számos olyan jellemzője van, amely eltér a GDPR által szabályozottaktól, ezért attól eltérő szabályozást igényel. (Ezeket később vesszük sorra.)
- A fentiek azért lényegesek, mert a bűnügyi adatvédelmi irányelvet harmonizáló magyar szabályok (részben) az Infotv.-be kerültek beépítésre. Ekkortól kezdve az Infotv. adatvédelmet érintő szabályozási tartalmának gerincét olyan szabályok alkotják, amelyek – mint az eddigiekből kiderült – a GDPR-el együtt készültek; céljaikban és a szabályozást illetően sok azonosság és párhuzamosság található.
- A GDPR meghatározott tárgykörökben lehetővé teszi a tagállamok számára a GDPR terminológiája szerint „pontosító" és „kiigazító" szabályok alkotását a GDPR alkalmazásával kapcsolatban. Ez technikailag elsősorban azzal valósul meg, hogy az Infotv. a törvény hatályának szabályozásakor felsorolja azokat a törvényhelyeket, amelyek nemcsak az Infotv. szabályozási tárgykörében alkalmazandók, hanem egyúttal a GDPR alkalmazásakor is, kiegészítő jelleggel.
- Azok a törvények is kapcsolatot teremtenek az adatvédelem európai uniós és nemzeti szintje között, amelyek a GDPR hatálya alá eső tárgykörben a GDPR által meghatározott keretek között szabályoznak egyes kötelező szektorális (például egészségügy, adóügyek stb.) adatkezeléseket. A GDPR alkalmazandóvá válásával az annak hatálya alá tartozó adatkezelési tárgykörökben az adatkezelés lehetséges jogalapjait a GDPR határozza meg, ám a kötelező adatkezelések, illetve

bizonyos az érintett hozzájárulása alapján végezhető adatkezelések esetében az érintettek és a kezelendő adatok körét, az adatkezelés időtartamát, valamint más lényeges sajátosságait továbbra is szektorális törvények tartalmazzák.

- Az Infotv. lényegében a GDPR szabályait rendeli alkalmazni bizonyos olyan adatkezelések esetében is, amelyekre nem terjed ki a GDPR hatálya. (Erről később még szó lesz.)
- Az uniós és a tagállami jog viszonyát általános érvénnyel rendező szabályok is segítik a jogalkalmazót az uniós és a nemzeti adatvédelmi jog komplexumában való eligazodásban.
  - Például az uniós jog elsőbbségére tekintettel esetleges kollízió esetén elsőbbséget élvez a GDPR alkalmazása a magyar jogszabályokkal szemben, beleértve az Infotv.-t és más törvényeket is.
  - Másik példa: az értelmezési doktrína alapján az Infotv. bűnügyi adatvédelmi irányelvet átültető szabályait annak szövegével és céljával összhangban kell értelmezni.
- Maguk az uniós szabályozási aktusok is tartalmaznak az uniós és a tagállami jog viszonyát rendező szabályokat. A bűnügyi adatvédelmi irányelv I. cikk (3) bekezdése szerint ez az irányelv nem akadályozza meg a tagállamokat abban, hogy az érintettek jogainak és szabadságainak védelme érdekében a személyes adatok illetékes hatóságok által végzett kezelésére az ezen irányelvben megállapítottnál magasabb védelmi szintet biztosító garanciákról rendelkezzenek. Ez tehát azt jelenti, hogy a bűnügyi adatvédelmi irányelv minimumharmonizációt tűz ki célul a hatálya alá tartozó tárgykörökben.

Összefoglalóan megállapítható, hogy a GDPR és az Infotv. a jellegbeli és jogforrási különbözőségek ellenére a szabályozási tartalmat tekintve a fogalomrendszer, az elvek és a jogintézmények tekintetében lényegében azonos koncepcionális alapokra épülő és részben párhuzamos szabályozást tartalmaz. A GDPR általános hatállyal tartalmazza a valamennyi tagállamban teljes egészében kötelezően és közvetlenül alkalmazandó szabályokat. A nemzeti szabályozás a GDPR által megengedett „pontosító" és „kiegészítő" szabályozáson kívül a személyes adatok kezelésének a GDPR hatályán kívül eső tárgykörökben történő kezelését szabályozza, mégpedig főként a GDPR mintájára megalkotott bűnügyi adatvédelmi irányelv joganyagát átültetve.

E hasonlóságok, párhuzamosságok és összefüggések lehetővé teszik azt, hogy a Magyarországon alkalmazandó adatvédelmi szabályozás jellegében nagyon eltérő két fele (az európai uniós és a nemzeti szabályozás) a gyakorlatban elhatárolható, összehasonlítható, szükség szerint egymásra tekintettel alkalmazható legyen.

A jogi szabályozás tárgyi és tartalmi párhuzamosságaira tekintettel, valamint figyelembe véve, hogy a szabályozás súlypontja immár a GDPR, a továbbiakban, e jegyzet következő fejezeteiben a nemzeti szabályozás ismertetésekor nem szükséges megismételni a GDPR megfelelő részének taglalásakor egyszer már leírtakat (fogalmak, elvek, jogintézmények stb.), hanem elégséges megmutatni azt, hogy melyek az adott fejezethez tartozó magyar jogforrási hivatkozások, továbbá rámutatni arra, hogy az adott tárgykörben melyek az eltérések a GDPR-hoz képest.

1.3. Az adatvédelmi szabályozás nemzeti szintje – Az Infotv. hatálya

Következő teendőnk az adatvédelmi szabályozás európai uniós és magyar szintje közötti határvonal feltérképezése, hiszen a magyar szabályozás tartalmának ismertetése előtt nem árt pontosítani, hogy annak hatálya kikre, mely szervekre, milyen adatkezelésekre és milyen területre terjed ki. Nagy totálban szemlélve a következőképp épül fel a szabályozás rendszere:

- Európai uniós szinten a GDPR tartalmazza a valamennyi tagállamban közvetlen hatályú és közvetlenül alkalmazandó szabályokat, továbbá a GDPR-t a hatálya alá tartozó adatkezelések tekintetében a GDPR-ben meghatározottaknak megfelelően magyar „kiigazító" és „pontosító"

szabályok egészítik ki.[4] E GDPR kiigazító és pontosító szabályokat részben az Infotv. tartalmazza, részben a GDPR hatálya alá tartozó szektorális adatkezelésekre vonatkozó magyar jogszabályok.
  - A magyar adatvédelmi szabályozás központjában az Infotv. van, amelynek hatálya a GDPR hatálya alá nem tartozó, de a magyar alkotmányos követelményekre, illetve európai uniós jogharmonizációs kötelezettségre tekintettel magyar adatvédelmi szabályozást igénylő adatkezelésekre terjed ki. A magyar adatvédelmi szabályozáshoz sorolhatók továbbá az Infotv. hatálya alá tartozó adatkezelésekre vonatkozó szektorális törvények és más jogszabályok is.

A felvázolt jogi szabályozási komplexumból a GDPR és az Infotv. hatályának elhatárolása a lényeges, mert az adatvédelmi szabályozás többi felvázolt elemei, például a szektorális törvények, a végrehajtási aktusok, valamint a pontosító és kiigazító szabályok ezek valamelyikéhez tartoznak.

E fejezet a magyar adatvédelmi szabályozás hatályát tárgyalja, ezért a továbbiakban az Infotv. hatályát vizsgáljuk, mégpedig a szabályozásnak azt a részét, amely nem tartozik „pontosító" vagy „kiegészítő" szabályként a GDPR-hoz.[5]

A fennmaradó, az Infotv. hatálya alá tartozó tárgykörök az Infotv. 2. §-a szerint következők:

1. A személyes adatok bűnüldözési célból történő kezelése.
2. A személyes adatok honvédelmi és nemzetbiztonsági célból történő kezelése.
3. A személyes adatok nem automatizált kezelése.
4. A természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzett adatkezelése.
5. Az elhunyt személy adatainak kezelése.

A fenti felsorolás elemei az adatkezelés, vagyis az Infotv. 3. § 10. pontjában értelmezett gyűjtőfogalom egyes részhalmazait, kategóriáit jelölik.

A felsorolt adatkezelési kategóriákat illetően az Infotv. hatálya a személyes adatok Magyarországon végzett kezelésére terjed ki. Ugyanakkor a fenti 1. és 2. esetben az Infotv. a szektorális jogszabályokra (lásd például a nemzetbiztonságról szóló törvényt, a büntetőeljárásról szóló törvényt) utalva értelmezi az adott adatkezelési kategóriát, következésképp ezen adatkezelési kategóriák esetében

- a vonatkozó szektorális törvények mindenkori adatkezelési szabályozási tartalmát, valamint
- az esetleges speciális hatálymeghatározását is figyelembe kell venni abban a tekintetben, hogy az adott adatkezelési kategóriát illetően meddig terjed az Infotv. hatálya.

Az Infotv. – GDPR elhatárolás problematika azon adatkezelési kategóriák esetében merül fel, amelyek esetében az adatvédelmi szabályozásnak van, vagy (legalábbis lehetne) európai uniós jogi szabályozási szintje. A felsoroltak többsége ilyen, de a 2., vagyis a személyes adatok honvédelmi és nemzetbiztonsági célból történő kezelése kilóg a sorból, mert e tárgyköröket az uniós jog nem szabályozza. Ám e körben is felmerülnek hatályelhatárolási és kollíziós kérdések. (Például „A teljes

[4] Lásd például a GDPR 6. cikk (3) bekezdését, amely a 6. cikk (1) bekezdés c) és e) pontjában meghatározott adatkezelési jogalapokkal összefüggésben lehetővé teszi a tagállami jog számára a GDPR-ban meghatározott szabályok alkalmazását kiigazító rendelkezések megalkotását, „ideértve az adatkezelő általi adatkezelés jogszerűségére irányadó általános feltételeket, az adatkezelés tárgyát képező adatok típusát, az érintetteket, azokat a jogalanyokat, amelyekkel a személyes adatok közölhetők, illetve az ilyen adatközlés céljait, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát és az adatkezelési műveleteket, valamint egyéb adatkezelési eljárásokat, így a törvényes és tisztességes adatkezelés biztosításához szükséges intézkedéseket is, ideértve a IX. fejezetben meghatározott egyéb konkrét adatkezelési helyzetekre vonatkozóan. Az uniós vagy tagállami jognak közérdekű célt kell szolgálnia, és arányosnak kell lennie az elérni kívánt jogszerű céllal."

[5] A teljesség kedvéért megemlítendő, hogy az Infotv. olyan további intézményi és eljárásjogi kereteket biztosító szabályokat is tartalmaz, amelyek mind a GDPR-ral, mind az Infotv. hatálya alá tartozó adatkezelésekkel összefüggésben alkalmazandók, például a Hatóság eljárásai. E szabályokat itt és most, vagyis a GDPR és az Infotv. hatályának elhatárolásakor nem szükséges részletezni.

adatkezelés kategóriára kiterjed-e a magyar adatvédelmi szabályozás hatálya?" stb. Részletesen lásd később.)

Ezután az egyes adatkezelési kategóriákra áttérve megállapítható, hogy a fenti lista elemei heterogének abból a szempontból, hogy némelyeknél az adatkezelés célja (honvédelem, nemzetbiztonság), másiknál az adatkezelő kiléte, illetve az adatkezelés jellege (természetes személy otthoni tevékenysége keretében végzett), vagy az adatok jellege (elhunyt személyre vonatkozó) tűnik az adott kategóriát meghatározó ismérvnek. E sokféleség miatt valamennyi kategóriát külön-külön részletesen meg kell vizsgálnunk, választ keresve a következőkre:

A. Miért az Infotv. hatálya alá tartozik (és nem a GDPR alkalmazandó rá)?
B. Mi az adott adatkezelési kategória tartalma?
   A meghatározáshoz az adatkezelés következő jellemzői közül szükség szerint egyet vagy többet fogunk használni: érintettek köre, adatfajták, adatkezelők, adatkezelés célja.
C. Miképpen válaszolhatók meg a jogi határeseteknél felmerülő Infotv./GDPR hatályelhatárolási kérdések?
   Ez azért merül fel, mert az Infotv. és GDPR hatálya szerinti elhatárolás mesterséges, jogi elhatárolás. Egyáltalán nem biztos, hogy a személyes adat a kezelése folyamán mindvégig csak az egyik adatvédelmi rezsim (a GDPR vagy az Infotv.) hatálya alá fog tartozni. Számos olyan helyzet alakulhat ki, amikor jogértelmezést igényel, hogy az adott adat kezelése az adott pillanatban a GDPR-nak vagy az Infotv.-nek feleltethető-e meg. (Ilyen helyzeteket idézhetnek elő például a GDPR és az Infotv. hatálya közötti határt átlépő adattovábbítások, egyazon adatkezelő többféle tevékenysége, másodlagos adatkezelés cél létrejötte stb.)

Ezek után vizsgáljuk meg a fenti öt adatkezelés kategóriát a fenti A – C kérdések szempontjából!

1.3.1. A személyes adatok bűnüldözési célból történő kezelése

A. E kategória azért tartozik az Infotv. hatálya alá, mert – mint arról már szó volt – az uniós adatvédelmi reform során az a döntés született, hogy e tárgykört ne a GDPR szabályozza, hanem a bűnügyi adatvédelmi irányelv. Magyarország jogharmonizációs kötelezettségének tett eleget azzal, hogy a bűnügyi adatvédelmi irányelv szabályait átültette A törvényi szabályozás az Alaptörvény I. cikk (3) bekezdésében foglaltak miatt is szükséges.

Az adatkezelőre és az adatfeldolgozóra vonatkozó általános szabályokat az Infotv. 25/A. – 25/D. §-ai tartalmazzák. Az adatkezelőre, a közös adatkezelőre és az adatfeldolgozóra vonatkozó értelmező rendelkezések rendre az Infotv. 3. 9. 9a. és 18. pontjaiban találhatók. Az Infotv. hivatkozott szabályai hasonlóak a GDPR 24. cikk (Az adatkezelő feladatai), 25. cikk (Beépített és alapértelmezett adatvédelem), 26. cikk (Közös adatkezelők) és 28. cikk (Az adatfeldolgozó) joganyagához, ezért az azokról leírtak közül a közszférában működő adatkezelőkre és az adatfeldolgozókra vonatkozó megállapítások lényegében az Infotv.-vel kapcsolatban is irányadók.

Az Infotv. nem használja a beépített és alapértelmezett adatvédelem fogalmakat, de a bűnügyi adatvédelmi irányelv 20. cikkét átültető szabályok (lásd még a bűnügyi adatvédelmi irányelv (53) és (55) preambulumbekezdéseit is) az adatkezelő általános feladatai között tartalmazzák a beépített és alapértelmezett adatvédelem követelményeit.

A jogharmonizáció során a bűnügyi adatvédelmi irányelv törzsszövegének megfelelő szabályok kerültek beépítésre az Infotv.-be, azonban a bűnügyi adatvédelmi irányelv célját és összefüggéseit megvilágító preambulumszöveg átültetésére természetesen nem kerülhetett sor, ezért e tekintetben az Infotv. „szűkszavúbb". A bűnügyi adatvédelmi irányelv céljának és tartalmának megértéséhez, valamint az Infotv. és a GDPR hatályának pontos elhatárolásához nemcsak az Infotv. vonatkozó szabályainak figyelembe vétele szükséges, hanem a bűnügyi adatvédelmi irányelv megfelelő

preambulumbekezdéseié is. Ezek segítségül hívásának semmi akadálya, hiszen az európai uniós jog értelmezési doktrínája alapján az uniós jogot átültető Infotv.-t a bűnügyi irányelv céljára és tartalmára tekintettel kell értelmezni.

B/ Az Infotv. 3. § 10a. pontja értelmezi a bűnüldözési célú adatkezelést.

Az összetett értelmező rendelkezés felsorolja azon tevékenységi célokat, amely tevékenységekhez kapcsolódó adatkezelés az Infotv. értelmében bűnüldözési célú adatkezelés:

- a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzése vagy elhárítása,
- a bűnmegelőzés, a bűnfelderítés, a büntetőeljárás lefolytatása vagy ezen eljárásban való közreműködés,
- a szabálysértések megelőzése és felderítése, valamint a szabálysértési eljárás lefolytatása vagy ezen eljárásban való közreműködés,
- a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenység,
- az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelése.

Az Infotv. 3. 10a. pontja számos olyan tevékenységre is a bűnüldözés részeként utal, amelyet egyébként sem a magyar jogi szaknyelv, sem a közvélekedés nem nevez így. Ennek nem szükséges nagy jelentőséget tulajdonítani. A törvény jobb híján ezt a kifejezést használja a felsorolt tevékenységek összefoglaló megnevezésére, ugyanis a bűnüldözés fogalom értelmezésénél irányadó, a magyar jogba átültetendő uniós jog olyan bűncselekmény fogalmat használ, amely nem azonos a magyar bűncselekmény fogalom szaknyelvi jelentésével: a bűnügyi adatvédelmi irányelv (13) preambulumbekezdése a bűncselekmény fogalom Európai Unió Bírósága szerinti értelmezésére utal.[6] E „bűncselekmény" és „bűnüldözés" fogalmak tehát olyan jogi terminus technicusok, amely a magyar jogban az Infotv.-vel összefüggésben értelmezettek, és nem változtatják meg e fogalmak köznyelvi és jogi szaknyelvi jelentését.

Az Infotv. értelmező rendelkezése az alanyi (szervi) és a jelleg oldaláról is szabályozza a felsorolt tevékenységeket, mégpedig azáltal, hogy a bűnügyi célú adatkezelés csak olyan szerv vagy személy tevékenysége lehet, aki vagy amely felsorolt feladatok ellátása során a jogszabályban meghatározott feladat- és hatáskörében jár el. Ez az Infotv. 3. § 10a. pontjának szövegéből is kiolvasható, de bűnügyi adatvédelmi irányelv vonatkozó 3. cikk 7. pontjából, az „illetékes hatóság" fogalom meghatározásából talán még egyértelműbb.[7]

Az értelmező rendelkezés alanyi és tárgyi oldalának összekapcsolása kizárja a bűnügyi célú

[6] A bűncselekmény fogalom uniós szintű értelmezése az Emberi Jogok Európai Bíróságának (EJEB) esetjogából eredeztethető. Az EJEB az Engel és társai kontra Hollandia ügyben foglalkozott a bűncselekmény értelmezési kritériumaival. Az első Engel-kritérium a rendelkezés nemzeti jog szerinti büntetőjogi besorolását érinti. Az EJEB ezt mindazonáltal nem tekinti mérvadónak, hanem csupán a vizsgálat kiindulópontjának. A második Engel-kritérium az adott jogsértést szankcionáló szabályozás címzetti körére vonatkozik. Ha a szabályozás mindenkire vonatkozik, nem pedig – mint például a fegyelmi jog területén – egy bizonyos jogállással rendelkező csoportra, akkor ez a szankció büntetőjogi jellege mellett szól. A második kritérium emellett a büntetőjogi rendelkezésben előírt szankció célját veszi alapul. A büntetőjogi jelleg megállapítására nem kerül sor, ha a szankció csak a vagyoni kár megtérítését szolgálja. Ha azonban annak célja a megtorlás és a megelőzés, akkor büntetőjogi szankcióról van szó. Az EJEB ezenfelül újabb ítélkezési gyakorlatában azt is figyelembe veszi, hogy a jogsértés szankcionálása olyan jogi tárgyak védelmét szolgálja-e, amelyek védelmét rendszerint büntetőjogi rendelkezések útján biztosítják. E szempontokat összességében kell értékelni. A harmadik Engel-kritérium az előírt büntetés jellegét és súlyát érinti. Szabadságvesztés esetében általánosságban a szankció büntetőjogi jellege vélelmezendő, amely vélelem csak kivételesen dönthető meg. Főszabály szerint a meg nem fizetése esetén szabadságvesztésre átváltoztatható, vagy a bűnügyi nyilvántartásba történő felvétellel járó pénzbüntetés is a büntetőeljárás fennállása mellett szól.

[7] „Illetékes hatóság": a) olyan közhatalmi szerv, amely a bűncselekmények megelőzését, nyomozását, felderítését vagy üldözését, illetve büntetőjogi szankciók végrehajtását illetően eljárni jogosult beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését; vagy b) bármely egyéb, olyan szerv vagy más jogalany, amely a tagállami jog alapján közfeladatokat lát el és közhatalmi jogosítványokat gyakorol a bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása céljából, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.

adatkezelés köréből (tehát az Infotv. hatálya alól) az olyan tevékenységekhez kapcsolódó adatkezelést, amelyek valamiképp bűncselekmények megelőzésével, a közbiztonságot fenyegető veszélyek elhárításával stb. kapcsolatosak, de a közhatalmi szférán kívül és közhatalmi jogosítványok nélkül végzik azokat. Ennek értelmében nem bűnügyi adatkezelés, és nem tartozik az Infotv. hatálya alá például:

- a sportrendezvényre belépők személyazonosságának ellenőrzése a rendezvény szervezői által,
- a lakók által a társasházban felszerelt zárt láncú biztonsági kamerarendszer alkalmazása,
- a jegyellenőr, amikor feljegyzi a tömegközlekedési eszközön potyázó utas személyazonosító adatait, valamint a pályaudvarokon és a tömegközlekedési eszközökön a közlekedési vállalat által felszerelt kamerák,
- az autópálya üzemeltető által az autópályadíj megfizetésének ellenőrzése és forgalomszámlálás céljából felszerelt kamerák alkalmazása,
- a magánszemély vagy cég által megbízott személy- és vagyonőr, vagy magánnyomozó adatkezelő tevékenysége stb.

Az értelmező rendelkezés alanyi és tárgyi oldalának összekapcsolásából az is következik, hogy a „bűnügyi célú adatkezelés" minőség fennállásához nem elég általánosságban az, hogy a tevékenységet ellátó szerv vagy személy jogszabályban meghatározott feladat- és hatáskörébe tartozzon az értelmező rendelkezésben felsorolt tevékenységek (közül egy vagy több) végzése, hanem az is szükséges, hogy az adott, konkrét adatkezelő tevékenység ténylegesen is ebbe a körbe tartozzon. (Az Infotv. szerint: a keretei közé tartozzon és a céljából történjen.)

Példa: a rendőrség a bűnüldözési, a közrend- és közbiztonság fenntartásával kapcsolatos, valamint az államigazgatási feladatainak ellátásához egyaránt jogosult személyes adatok kezelésére, ám abból, hogy vannak bűnüldözési feladatai, nem következik, hogy az államigazgatási feladataihoz kapcsolódó adatkezelését is bűnüldözési adatkezelésnek kellene tekinteni.[8]

Az elemzett értelmező rendelkezés tárgyi oldalával, vagyis a bűnügyi tevékenységek felsorolásával kapcsolatban megállapítható, hogy az Infotv. 3. § 10a. pontjában említett tevékenységeket, valamint az azokkal kapcsolatos feladat- és hatásköröket és az adatkezelést törvények (a rendőrségről szóló törvény, a büntetőeljárásról szóló törvény stb.) és más jogszabályok szabályozzák.[9] Három olyan tárgykör van, amely mégis magyarázatot igényel:

(1) A felsorolás nagyrészt olyan fogalmakkal operál (mint például a bűnüldözés, a bűnfelderítés vagy a büntetőeljárás), amelyek jelentése mind a magyar jogban, mind a vonatkozó nemzetközi dokumentumokban ismert, meghatározott és általánosan elfogadott. Kivétel a szabálysértés, amely a magyar jogban ugyan ismert, meghatározott és elfogadott, ám olyan jogintézmény, amely nem minden európai ország jogrendszerében található meg. Az egyes államok történeti jogfejlődése adhat magyarázatot arra, hogy a magyaréhoz hasonlóan ismeri-e a „bűncselekmény vagy szabálysértés" felosztást, vagy más jogi szabályozási konstrukciót alkalmaz. A bűnügyi adatvédelmi irányelv nem is használja a szabálysértés fogalmat. Ennek ellenére az tette szükségessé a szabálysértéssel kapcsolatos tevékenységek beemelését a bűnügyi adatkezelésre vonatkozó értelmező rendelkezésbe, hogy a bűnügyi adatvédelmi irányelv átültetése során az az által alapul vett bűncselekmény-fogalom

[8] Vesd össze a bűnügyi adatvédelmi irányelv (12) preambulumbekezdésével: „A tagállamok megbízhatják az illetékes hatóságokat olyan egyéb feladatokkal is, amelyeknek ellátása nem feltétlenül a bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása – többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából történik, és ebben az esetben az említett egyéb célokból történő, egyébiránt az uniós jog hatálya alá tartozó személyesadat-kezelés az (EU) 2016/679 rendelet hatálya alá tartozik." Ugyanilyen értelmű a GDPR (19) preambulumbekezdése is.

[9] A bűnügyi adatvédelmi irányelv 20 preambulumbekezdése szerint ez az irányelv nem gátolja meg a tagállamokat abban, hogy a nemzeti büntetőeljárási szabályaikban pontosabban meghatározzák a bíróságok és egyéb igazságügyi hatóságok által végzett személyes adatok kezelésével kapcsolatos adatkezelési műveleteket és adatkezelési eljárásokat, különösen, ami a bírósági határozatokban és jegyzőkönyvekben szereplő személyes adatokat illeti.

az irányadó a magyar törvényalkotó számára is (lásd a 13. preambulumbekezdés kapcsán fentebb kifejtetteket).

(2) Az értelmező rendelkezésben szereplő közrend és közbiztonság fogalmak fontos szerepet kapnak a Rendőrség és más rendvédelmi szervek joggyakorlatában és mindennapos tevékenységében, ám sem az Infotv., sem más törvény nem ad olyan általános érvényű definíciót, amely eligazítana abban, hogy mit is jelentenek e kifejezések, ráadásul a szaktudományban is vitatott a meghatározásuk, valamint az egymással való összefüggésük kérdése.[10] A jelzett definíciós bizonytalanságok okán, általános érvényű „közrend" és „közbiztonság" fogalommeghatározások hiányában adatkezelésenként lehet megállapítani azt, hogy adott tevékenység az Infotv. szabályozási rendszerében közrendet vagy a közbiztonságot fenyegető veszélyek megelőzése vagy elhárítására irányulónak tekintendő-e, mert csak így dönthető el, hogy a személyes adatok ahhoz kapcsolódó kezelése az Infotv. 3. § 10a. pontja értelmében az Infotv. hatálya alá tartozó bűnügyi adatkezelés-e.

(3) Az Infotv. 3. § 10a. pontban felsorolt tevékenységek utolsó blokkja, vagyis az előzőleg felsorolt tevékenységekhez tartozó levéltári, tudományos, statisztikai vagy történelmi célú adatkezelés kilóg a felsorolásból, mert:

- amíg a korábban felsorolt tevékenységek besorolhatók voltak egy nagyon tágan értelmezett „bűnüldözés" fogalom jelentéstartományába, ez semmiképpen sem, továbbá
- a közhatalmi kényszer sem jellemző rá.

Az eddigi gondolatmenet alapján talán ellentmondásosnak tűnhet, hogy a tárgyalt utolsó blokk olyan tevékenységeket sorol be a bűnügyi adatkezelés körébe, amelyek bár valamilyen kapcsolatban vannak azzal, de mégiscsak más célra irányulnak. Ennek ellenére a bűnügyi adatvédelmi irányelv többszörösen implikálja azt, hogy a bűnügyi adatkezeléshez kapcsolódó statisztikai stb. adatkezelés is a tagállami jog által harmonizálandó tárgykör, vagyis nem tartozhat a GDPR hatálya alá (lásd a bűnügyi adatvédelmi irányelv (26) preambulumbekezdésének utolsó mondatát és a 4. cikk (3) bekezdését).

Példa: A Rendőrség bűnüldöző tevékenységéhez kapcsolódó, annak céljából és keretében végzett, személyes adatokra kiterjedő statisztikai adatgyűjtés a fentiek értelmében bűnügyi célú adatkezelés, amely az Infotv. hatálya alá tartozik. Ugyanakkor a Rendőrség államigazgatási feladataihoz tartozó, személyes adatot érintő statisztikai adatgyűjtés már a GDPR hatálya tartozik. (lásd a bűnügyi adatvédelmi irányelv 9. cikk (2) bekezdését.) Itt tehát azt láthattuk, hogy a jogi szabályozás hatályelhatárolása, vagyis egy elméleti kritériumrendszer mintegy „kettévágta" a gyakorlatban egységes statisztikai adatgyűjtést egy GDPR hatálya alá tartozó és egy Infotv. hatálya alá tartozó részre.[11]

---

[10] Az Alkotmánybíróság 13/2001. (V.14.) AB határozatának indoklása rámutatott arra, hogy „[...] a közbiztonság mibenléte, viszonya a közrendhez, a belső rendhez, illetve utóbbiak fogalmi meghatározása tudományos viták tárgya. [...] A jogrendszer e szempontból releváns elemeinek áttekintése is azt mutatja azonban, hogy a közbiztonság többértelmű kategória, a kifejezés mögött tartalmilag többféle érdek és érték, illetve több, alapvetően eltérő jellegű feladat húzódik. A jogrendszerben a közbiztonság hol a közrend egyik elemeként jelenik meg [...], hol a közrend képezi a közbiztonság egyik elemét [...], hol pedig egymás mellett egyenértékű kategóriaként szerepel [...] A közbiztonság kétségtelenül alkotmányos értéktartalommal bír. A fogalom, a jelenség és a cél struktúrája azonban olyan bonyolult és szerteágazó, hogy az értelmezésben nagyfokú bizonytalanságra, illetve önkényességre vezethet."

[11] Ez nem kuriózum; érdemes szem előtt tartani, hogy az állami szférában végzett adatkezeléseknél – és most nem csak a bűnügyi célból végzett adatkezelésről van szó - előadódhatnak olyan helyzetek, amikor egy igazgatási és informatikai rendszerszervezési szempontból egységes adatkezelési rendszer valamilyen furcsa kimérának látszik adatvédelmi jogi szempontból, mert egyes részeire a GDPR vonatkozik, mások az Infotv. hatálya alá esnek.

C. Kérdéses lehet a GDPR és az Infotv. hatályának elhatárolása a következő határeseteknél is:

- Bűnügyi adatkezelés lehet-e az olyan adatgyűjtés, amelyet egy bűnüldöző szerv konkrét bűncselekmény gyanúja nélkül végez? Mennyire közvetlen és intenzív kapcsolatban kell lennie az adatkezelésnek valamilyen bűncselekménnyel, hogy az bűnügyi adatkezelésnek minősüljön? A bűnügyi adatvédelmi irányelv (12) preambulumbekezdése a bűnügyi adatkezeléshez sorolja a bűnüldöző szervek olyan, bűnüldözés kapcsán végzett tevékenységeit is, amelyek esetében még nincs tisztázva az, hogy az adott eset bűncselekménynek minősül-e. Ha utóbb kiderül, hogy az eset nem volt bűncselekmény, az visszamenőleg már nem vonja kétségbe az addig jogszerűen végzett adatkezelés bűnügyi jellegét.
- Előfordul, hogy olyan adatkezelő gyűjt és tárol adatokat bűnüldözési célból, amelyik nem tartozik az Infotv. 3. § 10a. pontban felsorolt szervi, illetve alanyi körbe. Ennek egyik esete az elektronikus hírközlési szolgáltatók számára előírt adatmegőrzési kötelezettség. Az elektronikus hírközlési szolgáltatók nem tartoznak a közfeladatot ellátó szervek körébe és nem rendelkeznek közhatalmi jogosítványokkal. Az adatokat nem saját céljaik érdekében őrzik meg, hanem azért, mert a 2003. évi C. törvény a bűnüldöző és más állami szervek adatigényének kielégítése érdekében erre kötelezi őket. A bűnügyi adatkezelésre vonatkozó értelmező rendelkezés alanyi és tárgyi oldalának fentebb részletezett összefüggéséből az következik, hogy ez e szolgáltatók által végzett bűnüldözési célú adatmegőrzés nem felel meg a bűnüldözési adatkezelés definíciójának. Valóban, a bűnügyi adatvédelmi irányelv (11) preambulumbekezdése megerősíti, hogy a GDPR-t kell alkalmazni „[...] *azokban az esetekben, amikor valamely szerv vagy jogalany egyéb célból gyűjt és kezel tovább személyes adatokat annak érdekében, hogy egy rá vonatkozó jogi kötelezettséget teljesítsen*."
- Vajon az Infotv. vagy a GDPR hatálya alá tartozik-e az adatfeldolgozás olyankor, ha egy bűnüldözési feladatot ellátó szerv az e tevékenységéhez kapcsolódó adatok feldolgozásával közhatalmi szférán kívüli szervet vagy személyt bíz meg?

A bűnügyi adatvédelmi irányelv (11) preambulumbekezdése értelmében a bűnügyi adatkezelés adatfeldolgozója e tevékenységével összefüggésben a bűnügyi adatvédelmi irányelv szerinti adatfeldolgozónak minősül, függetlenül attól, hogy egyébként közfeladatot ellátó szervnek minősül-e, illetve rendelkezik-e közhatalmi jogosítványokkal, tehát a magyar jog szempontjából e tevékenység az Infotv. hatálya alá tartozik. Ám a fentiektől meg kell különböztetni a következő esetköröket:

- Ha az adatfeldolgozó tevékenysége a bűnügyi feladatot ellátó szerv által kezelt olyan adatok feldolgozására is kiterjed, amelyek a GDPR hatálya alá tartoznak (lásd például a Rendőrség államigazgatási feladataihoz kapcsolódó személyes adatok feldolgozását), úgy az adatfeldolgozó ezen tevékenységére is a GDPR alkalmazandó.
- Ha az adatfeldolgozó egyidejűleg másik, GDPR hatálya alá tartozó adatkezelő szerv számára is végez adatfeldolgozást úgy erre a GDPR szabályai alkalmazandók.
- Bonyolultabb a GDPR és az Infotv. hatályának elhatárolása olyankor, amikor „hatályátlépő" adattovábbításra kerül sor, mert ilyenkor egyszerre több szempontot kell figyelembe venni. A bűnügyi adatvédelmi irányelv (29) és (34) preambulumbekezdései a GDPR és a bűnügyi adatvédelmi irányelv hatályának elhatárolására vonatkoznak. Ezen útmutatatások szerint a következő esetkörökről lehet szó:

  A (29) preambulumbekezdés szerint, ha a személyes adatok kezelését azonos vagy más adatkezelő a bűnügyi adatvédelmi irányelv hatálya alá tartozó olyan célból végzi, amely eltér attól a céltól, amelyre az adatgyűjtés eredetileg irányult, az ilyen adatkezelést azzal a feltétellel lehetővé kell tenni, hogy az ilyen adatkezelésre a vonatkozó jogi rendelkezések megfelelő felhatalmazást adnak, továbbá az adatkezelés az említett eltérő cél szempontjából szükséges és arányos.

  A (34) preambulumbekezdés szerint a bűnügyi adatvédelmi irányelv szabályai alkalmazandók abban az esetben, ha a személyes adatokat az irányelv alkalmazása során olyan címzettnek továbbítják, aki vagy amely nem tartozik ennek a bűnügyi adatvédelmi irányelv hatálya alá. Ha

a személyes adatokat eredetileg bűnügyi célú adatkezelést végző szerv (azaz illetékes hatóság) gyűjtötte a bűnügyi adatvédelmi irányelvben meghatározott valamelyik cél érdekében, a GDPR-t kell alkalmazni az adatok bűnügyi adatvédelmi irányelvben meghatározottaktól eltérő célból történő kezelésére, feltéve, hogy az említett adatkezelésre uniós vagy tagállami jog felhatalmazást ad.
A GDPR alkalmazandó abban az esetben, ha a személyes adatokat az ezen irányelv hatálya alá nem tartozó célokból továbbítják. A GDPR alkalmazandó a személyes adatok olyan címzett által végzett kezelésére, aki vagy amely nem minősül illetékes hatóságnak, illetve nem a bűnügyi adatvédelmi irányelv értelmében vett ilyen hatóságként jár el, és akivel vagy amellyel egy illetékes hatóság jogszerűen személyes adatokat közöl.

- A bűnüldözési célú és a nemzetbiztonsági célú adatkezelések adatkezelési cél szerinti elhatárolásáról a nemzetbiztonsági célú adatkezelések tárgyalásánál lesz szó.

1.3.2. A személyes adatok honvédelmi és nemzetbiztonsági célból történő kezelése

A. E kategória azért tartozik az Infotv. hatálya alá, mert a GDPR nem vonatkozik a nemzetbiztonsági célból kezelt adatok védelmére, ugyanis e tárgykör kívül esik az uniós jog hatályán. Továbbá nem tartozik a GDPR hatálya alá a tagállamok által olyan tevékenységek keretében végzett személyes adatok kezelése sem, amelyeket a tagállamok az Unió közös kül- és biztonságpolitikájával összefüggésben végeznek. Ugyanakkor Magyarországon a GDPR hatálya alá nem tartozó személyes adatkezelések adatvédelmi szabályozása az Alaptörvény I. cikk (3) bekezdése értelmében alkotmányos követelmény.

B. A GDPR szabályozási tartalmával nagymértékben párhuzamos az új szabályok és jogintézmények a bűnügyi adatvédelmi irányelv átültetése révén váltak az Infotv. részévé. A törvénymódosításnak az volt a koncepciója, hogy továbbra is fenn kell tartani az adatvédelmi szabályozás horizontális egységét, vagyis a jövőben is egy törvény, az Infotv. tartalmazza az adatvédelem alapvető szabályait, továbbá a törvény normaanyagának tárgykörök szerinti diverzitása ne haladja meg a szükséges mértéket. Ezért úgy alakult, hogy a bűnügyi adatvédelmi irányelvet átültető szabályok formálták ki azt a belső szabályozási felépítést és tartalmat, amelyek az Infotv. hatálya alá tartozó más adatkezelésekre, elsősorban a honvédelmi és a nemzetbiztonsági célú adatkezelésre is vonatkozik. Az Infotv. olyannyira egyként kezeli e tárgyköröket, hogy valamennyit együtt, egy pontban sorolja fel a törvény hatályánál (lásd Infotv. 2. § (3) bekezdés). E szabályozási modell célszerűségét az adja, hogy az ebbe a körbe tartozó adatkezelési kategóriák sok tekintetben hasonlóak egymáshoz, például:

- az adatkezelés rendszerint törvényi kötelezettségen alapul,
- egyes, a GDPR szabályozási rendszerében általánosan érvényesülő érintetti jogok honvédelmi, bűnüldözési és nemzetbiztonsági célú adatkezelésekkel kapcsolatban nem értelmezhetők (lásd adathordozhatóság) vagy az adatkezelés céljának függvényében esetleg korlátozottan érvényesíthetők (lásd az érintett hozzáférési joga).

B/1. A személyes adatok nemzetbiztonsági célból történő kezelése

A fejlett demokratikus jogállamokban a személyes adatok védelmének szabályai a nemzetbiztonsági szolgálatokra is vonatkoznak. Magyarországon nemzetközi összehasonlításban is kiemelkedően erős az adatvédelem garanciarendszere a nemzetbiztonsági célú adatkezelések tekintetében.

Az Infotv. 3. § 10b. pontja a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelését, valamint a Terrorelhárítási Központ (TEK) jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelését sorolja nemzetbiztonsági célból végzett adatkezelés körébe.

A nemzetbiztonsági szolgálatok feladat- és hatáskörét, valamint az e szolgálatok által végzett adatkezelés szabályait a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény tartalmazza (Nbtv.).

A TEK a rendőrség szerve, azonban egyes tevékenységei, így például a terrorizmus megelőzése, felderítése, elhárítása, valamint a külföldön túszejtő akciókban bajba jutott állampolgárokkal kapcsolatos információgyűjtés, elemzés és értékelés esetében az Nbtv. szabályai alkalmazandók. E tevékenységek körét a Rendőrségről szóló 1994. évi XXXIV. törvény 7/E. § (6) bekezdése határozza meg. Az Infotv. szerint a TEK e tevékenységekkel kapcsolatos adatkezelése nemzetbiztonsági célú adatkezelés.[12]

A nemzetbiztonsági célból végzett adatkezelés értelmezésével kapcsolatban a következő Infotv. – GDPR hatályelhatárolási kérdések merülnek fel:

- Az Nbtv. külön szabályozza a nemzetbiztonsági szolgálatok adatkezelését (Nbtv. 38. § – 52/M. §) és titkos információgyűjtő tevékenységét[13] (Nbtv. 53.§ – 66. §). Adatvédelmi jogi szempontból a titkos információgyűjtés nem más, mint információk megszerzése, tárolása, feldolgozása, továbbítása és felhasználása, ezért ez is az Infotv. hatálya alá tartozó nemzetbiztonsági célú adatkezelés körébe tartozik.[14]
- A nemzetbiztonsági szolgálatok a klasszikus titkosszolgálati tevékenységeken kívül hatósági jellegű feladatokat is ellátnak, melyek során sor kerülhet személyes adatok kezelésére. Például a Nemzetbiztonsági Szakszolgálat ellátja a biztonsági okmányok védelmével összefüggő hatósági felügyeletet. E feladatok is a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörébe tartoznak, ezért az ezekkel kapcsolatos adatkezelés is az Infotv. hatálya alá tartozó nemzetbiztonsági adatkezelés.
- Az Infotv. hatálya a nemzetbiztonsági szolgálatok valamennyi jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelésére kiterjed. A nemzetbiztonsági szolgálatok által végzett nemzetbiztonsági célú adatkezelésre részben külföldön kerül sor (lásd például az Információs Hivatal hírszerző tevékenységét).
- A nemzetbiztonsági szolgálatok egyes feladatai bűnfelderítéssel kapcsolatosak. Például az Nbtv. 5. § h) pont ha) és hb) alpontja, valamint j) pont ja) és jb) alpontja az Alkotmányvédelmi Hivatal feladatkörébe utal bizonyos bűncselekményekkel kapcsolatos információszerzést és a nyomozás elrendelése előtti felderítést. A bűnfelderítéshez kapcsolódó adatkezelés az Infotv. 3. § 10a. pontjában meghatározott bűnüldözési célú adatkezelésnek is megfeleltethető, ám ebben az esetben nemzetbiztonsági célnak alárendelve. Azonban bármiként legyen is, ez nem változtat azon, hogy ez az adatkezelés (nemzetbiztonsági célú adatkezelésként és emellett esetleg bűnüldözési célú adatkezelésként is) az Infotv. (és nem a GDPR) hatálya alá tartozik.

B/2. A személyes adatok honvédelmi célból történő kezelése

Az Infotv. 3. § 10c. pontja a honvédségi adatkezelésről szóló törvény (lásd a 2013. évi XCVII. törvényt) és a Magyarország területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyarország területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról szóló törvény (lásd a 2011. évi XXXIV. törvényt) hatálya alá tartozó adatkezelést sorolja a honvédelmi célból végzett adatkezelés körébe.

Az említett törvények kellő pontossággal, az egyes nyilvántartások és adatkezelési tevékenységek szintjén meghatározzák a honvédelmi célú adatkezelés tartalmát. Tárgyunk szempontjából kiemelendők a következők:

[12] E fejezetben a további, a nemzetbiztonsági szolgálatokra vonatkozó megállapítások a TEK itt vázolt tevékenységeire is értendők.

[13] A titkos információgyűjtést gyűjtőfogalomként használjuk, amibe beleértendő a leplezett eszközök alkalmazása is.

[14] A titkos információgyűjtés egyes eszközeinek és módszereinek adatvédelmi jogi hatály szempontjából történő megítélése jelenleg részben még kidolgozatlan. Például kérdéses, hogy ha egy törvény alapján titkos információgyűjtésre jogosult szerv a bűnüldözési vagy nemzetbiztonsági feladatai ellátásának támogatása érdekében fedővállalkozást (például internetes szolgáltatót, kereskedelmi tanácsadó irodát stb.) hoz létre, a fedővállalkozás által végzett nyílt adatkezelés révén megvalósított titkos információgyűjtés a GDPR vagy az Infotv. hatálya alá tartozik-e.

- Az értelmező rendelkezés két törvényre utal. Kizárólag az ezek hatálya alá tartozó szabályok képezik a honvédelmi célú adatkezelés joganyagát. Tehát csak e két törvényben, valamint ezek végrehajtási rendeleteiben rögzített adatkezelési szabályok határoznak meg honvédelmi célú adatkezelést.
- Ha az említett két törvényben szabályozott adatkezelések adatkezelői egyéb, e törvények hatályán kívül eső adatkezelési tevékenységet is folytatnak, úgy e tevékenységek nem minősülnek honvédelmi célból végzett adatkezelésnek.
- A más jogszabályokban található, honvédelmi jellegű adatkezelési tárgyú szabályok, például bizonyos adatkezelésekből honvédelmi célból történő adatszolgáltatásokra, vagy a honvédelmi rendeltetésű létesítmények nyilvántartására stb. vonatkozó, másutt előforduló szabályok nem feleltethetők meg az Infotv. 3. § 10c. pontjában foglaltaknak, ezért nem vonatkoznak rájuk a honvédelmi célú adatkezelések szabályai.
- A nemzetbiztonsági célú adatkezeléstől eltérően a honvédelmi célú adatkezelés Infotv.-ben hivatkozott joganyaga a honvédelmi szervezetrendszer személyügyi és részben levéltári adatkezelését is szabályozza, ezért ezek is a honvédelmi célú adatkezelés részét képezik. Ez a Katonai Nemzetbiztonsági Szolgálat személyi állományának nyilvántartására is vonatkozik.

C. A határesetek problematikája – hatály kollíziós és elhatárolási kérdések a nemzetbiztonsági és a honvédelmi célú adatkezelésekkel kapcsolatban

A most tárgyalt két adatkezelési kategória esetében némileg másként merül fel e kérdéskör, mint a korábban tárgyalt bűnügyi célú adatkezelés esetében. Ennek az az egyik oka, hogy a honvédelem és a nemzetbiztonság – a bűnüldözéssel szemben – kívül esik az uniós jogi szabályozási aktusok tárgykörén. Ebből az következik, hogy:

- A honvédelmi és nemzetbiztonsági adatkezelésre és adatvédelemre vonatkozó jogszabályok kapcsán nem hívható segítségül az uniós értelmezési doktrína, hiszen nincs olyan uniós jogi szabályozási aktus, amellyel összefüggésben a magyar jogot (az Infotv. hatályát) értelmezni lehetne.

Van egy másik, a magyar jogi szabályozásból következő oka is annak, hogy a hatályelhatárolás kérdések másként merülnek fel a most tárgyalt két adatkezelési kategória esetében. Az Infotv. más jellegadó ismérvek mentén értelmezi a nemzetbiztonsági célú adatkezelést, mint a honvédelmi célú adatkezelést:[15]

- A nemzetbiztonsági célú adatkezelések esetében az értelmezés alapvetően alanyi (szervi) meghatározottságú („*nemzetbiztonsági szolgálatok [...] adatkezelése*”), pontosítva azzal, hogy „*jogszabályban meghatározott feladat- és hatáskörében [...]*”.
- A honvédelmi célú adatkezelés esetében az értelmező rendelkezés egyszerűen két törvény megjelölésén alapul.

A jogértelmezés és a jogi ismeretek elsajátítása szempontjából szerencsés, hogy a most tárgyalt két értelmező rendelkezés egyszerű, világos feltételekre épül, amelyek sokkal kevesebb értelmezési és hatályelhatárolási kérdést vetnek fel, mint a bűnügyi adatvédelmi irányelvből származó bonyolult „bűnügyi célú adatkezelés” definíció. Ennek ellenére a következő határesetek magyarázatot igényelnek:

- Ha a személyes adatok kezelésének célja megváltozik vagy kibővül és az új adatkezelési cél kívül esik az Infotv. hatályán, úgy arra a GDPR szabályai alkalmazandók. (Ennél a határesetnél elvileg nem zárható ki az adatkezelési cél olyan megváltozása, amely azt eredményezné, hogy az adatkezelés kikerül az Infotv. hatálya alól, ám a tágabb értelemben vett honvédelem vagy nemzetbiztonság tárgykörében maradna és ezért a GDPR hatálya sem terjedne ki rá, ám egyelőre nem sikerült olyan gyakorlati példát találni, amely ezt az esetet reprezentálná.)

[15] Ez nem kritikai észrevétel, pusztán a szabályozás különbözőségére mutatunk rá.

Példa: az érintettek hozzájárulása alapján a honvédelmi adatkezelésről szóló törvényben szabályozott személyzeti nyilvántartás adatait használják fel egy konferencia résztvevőinek szóló meghívók kiküldéséhez. Ez az adatkezelés a GDPR hatálya alá tartozik.

- Mi a helyzet az adatfeldolgozó megbízásával?

A honvédelmi célú adatkezelés esetében egyértelmű a válasz:

- A Honvédség törvényben szabályozott központi adatfeldolgozó szerve a törvényben meghatározott tevékenysége során ex lege a honvédelmi célú adatkezelés körébe tartozó adatfeldolgozó tevékenységet végez.
- Abban a hipotetikus esetben, ha a honvédségi adatkezelő szerv más szervet vagy személyt bízna meg a 3. § 10c. pontban leírtaknak megfelelő adatkezelésekkel kapcsolatos adatfeldolgozási műveletek elvégzésével, úgy az is az Infotv. 3. § 10c. pontban hivatkozott két törvény hatálya alá tartozna, következésképp az Infotv. honvédelmi célú adatkezelésekre megállapított szabályai vonatkoznának rá. E megállapítás azonban csak a honvédelmi célú adatkezelést végző adatkezelőtől származó adatfeldolgozási műveletekre vonatkozik, az adatfeldolgozó által esetleg egyidejűleg végzett, (például más adatkezelőtől származó) adatfeldolgozási megbízások ellátásának jogi megítélésére nem terjed ki.

Fogósabb kérdés az adatfeldolgozás jogi megítélése a nemzetbiztonsági célú adatkezelések esetében.

A hatály problematikáját egy spekulatív példán szemléltetjük, amelynek mindössze annyi a tényállása, hogy az egyik nemzetbiztonsági szolgálat egyik szerve egy nemzetbiztonsági szervezetrendszeren kívüli adatfeldolgozót, (a példa szerint egy fordítással és tolmácsolással foglalkozó vállalkozást) bíz meg az Nbtv. szerinti feladat- és hatáskörében eljárva gyűjtött információk feldolgozásával (idegen nyelvű hangfelvételek leiratának elkészítésével és magyar nyelvre fordításával). Vajon része-e a fordítóiroda tevékenysége az Infotv.-ben értelmezett „nemzetbiztonsági célú adatkezelés" fogalomnak?

Az Infotv. 3. § 10b. pontja kifejezetten a „*a nemzetbiztonsági szolgálatok [...] adatkezelése*"-ként értelmezi a nemzetbiztonsági célú adatkezelést. A példabeli esetben azonban:

- nem adatkezelésről, hanem adatfeldolgozásról, továbbá
- nem a nemzetbiztonsági szolgálatok tevékenységéről, hanem egy közszférán kívül működő vállalkozás által végzett adatfeldolgozási műveletekről van szó, ezért a megszorító értelmezés szerint nem tekinthető a nemzetbiztonsági célból végzett adatkezelés részének és nem tartozik az Infov. hatálya alá. Ám a megszorító értelmezés elfogadása messzire ható, és alkotmányossági szempontból negatív következményekkel járna. Ugyanis eszerint az értelmezés szerint a példabeli adatfeldolgozó szerv tevékenysége kikerülne az Infotv. hatálya alól, ám a GDPR-t sem lehetne rá alkalmazni, hiszen az adatfeldolgozás mégiscsak nemzetbiztonsági célt szolgál. Ez azt eredményezné, hogy az adatfeldolgozás jogi vákuumba kerülne, ahol nem érvényesek a személyes adatok védelmének szabályai. Ez a helyzet sértené az Alapörvény I. cikk (3) bekezdésében foglaltakat. Ezért az Alaptörvénnyel összhangban lévő jogértelmezés az, hogy a nemzetbiztonsági célú adatkezelésbe az adatok feldolgozása is beletartozik.

1.3.3. A személyes adatok nem automatizált kezelése

A. A GDPR 2. cikk (1) bekezdése szerint a rendeletet a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni. A GDPR hatálya alá tartozó adatkategóriák és automatizáltság mértékek egymásra vonatkoztatását az alábbi táblázat szemlélteti:

GDPR hatálya	**Adatkezelés**	**Tervezetten vagy ténylegesen nyilvántartás részévé tett adat**
Nem automatizált	-	-
Részben automatizált	X	-
Automatizált	X	X

Emlékeztetőül: a GDPR hatálya a bűnügyi, honvédelmi és nemzetbiztonsági célú adatkezelésekre, valamint a természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzett adatkezelésére sem terjed ki – ezeket másutt tárgyaljuk.

A GDPR (6) és (15) preambulumbekezdései azt a magyarázatot fűzik ehhez, hogy a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. A természetes személyek védelme a személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni. Olyan iratok, illetve iratok csoportjai, és azok borítóoldalai, amelyek nem rendszerezettek meghatározott szempontok szerint, nem tartoznak e rendelet hatálya alá.

Magyarországon a személyes adatok védelme alapvető jog és az Alaptörvény I. cikk (3) bekezdése alapján az államnak adatvédelmi jogi szabályozás hatálya alá kell helyeznie azokat az adatkezeléseket, amelyekre a fentiek értelmében a GDPR hatálya nem terjed ki.

B. Az Infotv. 2. § (4) bekezdése lényegében úgy rendelkezik, hogy erre az adatkezelés kategóriára
- a GDPR-t (pontosabban a GDPR azon fejezeteit, melyet az Infotv. 2. § (4) bekezdés a) pontja felsorol), valamint
- az Infotv. GDPR-t kiegészítő és pontosító szabályait (lásd az Infotv. 2. § (4) bekezdés b) pontját) kell alkalmazni.

Az Infotv. ezen a ponton figyelembe veszi azt, hogy ez az adatkezelési kategória lényegében azonos azzal az adatkezelés tárgykörrel, amelyre a GDPR-t kell alkalmazni, egy kivétellel: az adatkezelés nem automatizált. Ez az eltérés a magyar adatvédelmi jog szempontjából nem lényeges, ezért nem lenne ésszerű másként szabályozni a „manuális" adatkezeléseket, mint az automatizáltakat, amelyekre a GDPR alkalmazandó. A magyar törvényalkotónak nincs hatalma ahhoz, hogy visszahelyezze a nem automatizált adatkezeléseket a GDPR hatálya alá, de azt megteheti, hogy a GDPR szabályainak alkalmazását írja elő ezek esetében. Így is történt.

Ennél az adatkezelés kategóriánál is fogalmak és jelzők értelmezésén múlik, hogy adott adatkezelés az Infotv., vagy a GDPR hatálya alá tartozik-e.[16] Az értelmezésre váró kifejezések: „*adatkezelés*", „*nyilvántartási rendszer*", „*automatizált*", „*részben automatizált*" és „*nem automatizált*". Minthogy ennél az adatkezelés kategóriánál nem abból kell kiindulni, hogy hogyan

[16] Bár ennek nincs sok gyakorlati jelentősége, hiszen – mint láthattuk – végső soron így is, úgy is a GDPR szabályait kell alkalmazni.

határozza meg az Infotv. a saját hatályát, hanem abból, hogy a GDPR szerint mi nem tartozik a GDPR hatálya alá, ezért az értelmezést igénylő kifejezéseknél nem az Infotv. értelmező rendelkezési számítanak, hanem a GDPR fogalommeghatározásai. Az adatkezelés fogalommeghatározását a GDPR 4. cikk 2. pontja,[17] a nyilvántartási rendszerét a 4. cikk 6. pontja[18] tartalmazza. Az adatkezelés automatizálásának fokozataihoz nem járul GDPR fogalommeghatározás. Az automata, automatikus jelentése: önműködő, emberi beavatkozás nélkül működő. Az infokommunikáció gyors fejlődésének körülményei közepette nem lenne célszerű általános érvényű és technikai részletekbe bocsátkozó meghatározást adni az automatizáció mibenlétéről és fokozatairól. Adatvédelmi jogi szempontból mindenesetre megállapítható, hogy bizonyos adatkezelési tevékenységek, mint például az automatizált döntéshozatal, a profilalkotás, valamint a gyakorlatban elterjedt biometrikus technológiák alkalmazása automatizált adatkezelést valósít meg, és egyébként is, az automatizáció mind nagyobb teret nyer.

C. Határesetek, elhatárolási és kollíziós kérdések

- Ennél az adatkezelés kategóriánál egy olyan hatályelhatárolási kérdéssel találkozzunk, amellyel eddig még nem: a GDPR kivételek prioritási sorrendjének problematikájával.

Példa: a nem automatizált bűnügyi célú adatkezelés esete

- Erre az adatkezelésre biztosan nem alkalmazandó a GDPR, mégpedig rögtön két okból sem: mert nem automatizált és mert bűnügyi célú. Tehát az Infotv. hatálya alá fog tartozni. A gond csak ott van, hogy az Infotv. más szabályokat rendel alkalmazni a bűnügyi célú adatkezelések és a nem automatizált adatkezelések esetében. Ráadásul e két szabályrendszer nem alkalmazható egyszerre. (Emlékeztetőül:
  - Bűnügyi célú adatkezelés --> Infotv. 2. § (3) bekezdés: „e törvényt kell alkalmazni”.
  - Nem automatizált adatkezelés --> Infotv. 2. § (4) bekezdés: „a GDPR-t kell alkalmazni”.)
- A (látszólagos) ellentmondást az oldja fel, hogy az Infotv. meghatározza a kivételek sorrendjét. A 2. § (4) bekezdését kisegítő jelleggel kell alkalmaznia (2) és (3) bekezdéshez képest. Ennek megfelelően a példabeli adatkezelés esetében kizárólag az adatkezelés bűnügyi célja fogja eldönteni, hogy az Infotv. mely szabályai alkalmazandók rá; az adatkezelés nem automatizált jellegét pedig figyelmen kívül kell hagyni ebből a szempontból.

- Megemlítendő, hogy ha egy adatkezelés működése során annak automatizáltsági szintje megváltozik, illetve az adatokat nyilvántartásba rendezik (vagy az adatkezelés nyilvántartási rendszer jellegét megszüntetik), az esetleg azt eredményezheti, hogy az eredetileg a GDPR hatálya alá tartozó adatkezelés az Infotv. hatálya alá kerül és viszont.

[17] 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;

[18] Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

1.3.4. A természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzett adatkezelése

A. GDPR 2. cikk (2) bekezdés c) pontja szerint e rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik.

A GDPR hatálya alá nem tartozó személyes adatkezelés magyarországi adatvédelmi jogi szabályozása az Alaptörvény I. cikk (3) bekezdésére tekintettel alkotmányossági követelmény.

B. Az Infotv. 2. § (6) bekezdése szerint nem kell alkalmazni e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire. E szabályozás nem változott a GDPR alkalmazandóvá válásával kapcsolatban. A magyar törvényalkotó e szabályozással formálisan eleget tesz az Alaptörvény I. cikk (3) bekezdéséből eredeztethető szabályozási kötelezettségének, ám a korábbiakhoz hasonlóan továbbra sem tartja szükségesnek a természetes személy kizárólag saját személyes céljait szolgáló adatkezeléseinek érdemi adatvédelmi szabályozását. Ennek részben elvi, részben gyakorlatias oka van:

- Az elvi ok az, hogy a magánszemély magánszféráján belül maradó, kis volumenű, többnyire mások tudomására egyáltalán nem jutó adatkezelés általában nem alkalmas olyan jog- és érdeksérelem okozására, ami miatt adatvédelmi jogi szabályozás alá kellene vonni.
- A gyakorlatias ok az, hogy a természetes személy kizárólag saját célját szolgáló adatkezelésének körülményei (például a lakásban elhangzott szóbeli közlés, az az adatkezelő személy ingzsebén tárolt jegyzetfüzetben rögzített információk stb.) nem tennék lehetővé az adatkezelés jogszerűségének ellenőrzését. Vagy ha mégis, az az ellenőrzött személy magán- és családi élete, otthona, kapcsolattartása tiszteletben tartásához fűződő jogának aránytalan korlátozásával, vagyis sérelmével járna.

C. Elhatárolási kérdések

A GDPR (18) preambulumbekezdése ad értelmezési támpontokat a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelését illetően. Eszerint ez olyan tevékenység, amely semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek. Fontos kivétel, hogy a GDPR-t kell alkalmazni azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják.

1.3.5. Az elhunyt személy adatainak kezelése

A. A GDPR (27) preambulumbekezdése rögzíti, hogy a GDPR-t nem kell alkalmazni az elhunyt személyekkel kapcsolatos személyes adatokra, ám a tagállamok számára lehetővé kell tenni, hogy az elhunyt személyek személyes adatainak kezelését szabályozzák.

A halál bekövetkeztével a természetes személy megszűnik létezni, ezért ezt követően nem létezik az a jogalany, akit korábban a személyes adatok védelme megilletett, tehát a személyes adatok védelmének törvényi szabályozására irányuló alkotmányos kötelezettség az elhunyt személy adataira nem értelmezhető.

B. A magyar jogrendszerben eddig sem volt ismeretlen az, hogy az elhunyt adatainak kezeléséhez joghatások járulhatnak (lásd például a kegyeleti jogot), melynek alanyai tipikusan az elhunyt személy örökösei és hozzátartozói lehetnek. Az Infotv. 25. §-a ezen túlmenően lehetőséget biztosít az érintettet

őt életében megillető jogainak[19] „post mortem" érvényesítésére az érintett halálát követő öt éven belül az érintett által tett nyilatkozattal meghatalmazott személy, ennek hiányában (részleges jogkörrel) az érintett Polgári Törvénykönyv szerinti közeli hozzátartozója számára.

Az Infotv. fentebb vázolt szabályai meghatározzák az érintett halál után is gyakorolható érintetti jogait, valamint annak lehetséges jogosultjait. E szabályozás a jogviszony másik pólusán fenntartja az adatkezelő kötelezetti minőségét is. Ám ehhez egy olyan tartalmú jogviszonyt kapcsol az Infotv. 25. §-a, amely számos tekintetben eltér az érintettet még életében megillető információs önrendelkezési jogtól:

- tartalmát tekintve nem terjed ki az információs önrendelkezési jogból eredő valamennyi részjogosultságra, hanem kizárólag csak az Infotv. 25. §-ában meghatározottakra;
- járulékos jellegű, azaz az elhaltat az életében megillető jogokhoz kapcsolódik;
- időben korlátozott: a jogok érvényesítésére az érintett halálát követő öt éven belül van lehetőség;[20]
- jogosulti oldalon más a jogviszony alanya (az elhunyt érintett hiányában az általa korábban meghatalmazott személy vagy a közeli hozzátartozó).

Ezen sajátosságok miatt indokolt az elhunyt személy adatainak kezelését önálló kategóriaként besorolni az Infotv. hatályának vizsgálatakor.

Értelmezésünk szerint az Infotv. 25. § szabályai közül csak az érintett életében tett, az Infotv. 25. § (1) bekezdése szerinti nyilatkozat megtétele tartozik az információs önrendelkezési jog körébe.

C. Az elhunyt személy adatainak kezelésére vonatkozó szabályok attól függetlenül alkalmazandók, hogy az érintett adatainak kezelése még életében a GDPR vagy az Infotv. hatálya alá tartozott-e az adott adatkezelőnél. Hatályelhatárolási és kollíziós kérdések nem merülnek fel.

[19] Lásd hozzáféréshez való jog, helyesbítéshez való jog, az adatkezelés korlátozásához való jog, törléshez való jog.

[20] E jogviszony tartalmának részletei további elméleti kidolgozást igényelnek. Például jelenleg még nem egyértelmű, hogy fennáll-e az adatkezelő tájékoztatási kötelezettsége az érintett halála után történt adattovábbításokról, vagy az információs önrendelkezési jogból következő, a fentiek szerint a halál után egy ideig még „továbbélő" tájékoztatási jogosultság az érintett halála előtt történt adattovábbításokra korlátozódik.

2. ALAPELVEK, ALAPFOGALMAK

A személyes adatok védelméhez fűződő jog jogi szabályozásában nagy szerepük van az alapelveknek, az alapelvi szemléletmódnak. Az adatvédelem kialakulásának folyamata és a szabályozás egységesülése az alapelvek kialakulásával is járt. Már 1980-ban az OECD-irányelvek[21] tartalmaztak adatvédelmi alapelveket, ajánlásként a tagállamok számára, mégpedig az alábbiakat:

- korlátozott adatgyűjtés alapelve
- adatminőség alapelve
- cél meghatározásának alapelve
- felhasználás korlátozásának alapelve
- biztonság alapelve
- nyíltság alapelve
- személyes részvétel alapelve
- elszámoltathatóság alapelve

Ezen OECD-irányelvhez hasonló tartalommal került elfogadásra 1981-ben az Európa Tanács Adatvédelmi Egyezménye.[22] Tehát az adatkezelés elvei már korán megjelentek az adatvédelmi jogban. Az adatvédelmi irányelv is – irányelv minőségénél fogva is – tartalmazta az adatkezelési alapelveket.

Hazai vonatkozásban elmondható, hogy az adatvédelmi szabályok kialakulásában iránymutató volt a 15/1991. (IV. 13.) AB-határozat, mely meghatározta az információs önrendelkezési jog lényegét, és az adatkezelés főbb elveit is. Mind az Avtv., mind az Infotv. alapelvi rendelkezéseket is szabályozott, melyek tartalommal való megtöltése, értelmezése a jogalkalmazás feladata.

Az adatvédelmi reform során a korábbi alapelvek is felülvizsgálatra kerültek. Az uniós jogalkotó láthatóan azok többségének megtartása mellett döntött. Tehát elmondható, hogy az irányelv és az Infotv. szabályozásához képest a GDPR az alapelvek tekintetében nagy változást nem okozott. Az alapelvi rendelkezések egyes részletei, megfogalmazásuk változott, esetleg hangsúlyosabbá vált, de kifejezetten új alapelv nem jelent meg. Viszont látszódik a szabályozásból a jogalkotó azon szándéka, hogy az alapelveknek nagy hangsúlyt adjon, azok érvényesülését kikényszerítse: ezt egyrészt az elszámoltathatóság elve, másrészt a szankcionálás biztosítja. A rendelet központi jelentőségű rendelkezéseinek, így az adatkezelés alapelveinek megsértése esetére a súlyosabb, nagyobb összegű bírság (legfeljebb 20 millió euró) szabható ki.

A Rendelet a (26) preambulumbekezdésében rögzíti, hogy „Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.”, továbbá „Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni.” Vagyis a GDPR hatálya ennek megfelelően értelmezendő az alapelvek tekintetében is.

A GDPR a hatály tisztázása és a fogalommagyarázat után rögtön a II. fejezetben, az 5. cikkben sorolja fel az adatvédelmi jog azon főbb alapelveit, melyek mintegy megkerülhetetlen szempontrendszerként egyfajta keretet szabnak az adatok kezelésének, iránymutatásul szolgálnak egy-egy adatkezelés megítélésénél. Alapelvet, illetve alapelv jellegű rendelkezést a rendelet más

---

[21] Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) irányelvei a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról.

[22] Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során.

részeiben is találhatunk – például privacy by design (25. cikk), adattovábbításra vonatkozó általános elv (44. cikk). Ezen elvek az adott témakörnél tárgyalandóak.

A GDPR az alábbi főbb alapelveket nevesíti az 5. cikkében:
- jogszerűség, tisztességes eljárás, átláthatóság,
- célhoz kötöttség,
- adattakarékosság,
- pontosság,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg,
- elszámoltathatóság.

2.1. Jogszerűség, tisztességes eljárás, átláthatóság elve

Az alapelvek között az első helyen fogalmazódik meg a GDPR-ban ez a jogelv, mely három, különállóan is értelmezhető elvet foglal magában, és mindegyik eleme olyan alapvető követelményt jelent, mely áthatja az adatvédelmi szabályozást: személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.[23]

A jogszerűség értelme a fogalomból eredően nyilvánvaló: jogellenes célból, jogellenes módon személyes adatok nem gyűjthetőek, azokkal semmiféle művelet nem végezhető. Ez a követelmény lényegében azt jelenti, hogy a kötelezően alkalmazandó jogi szabályozás minden előírása teljesítendő az adatkezelő által, mert enélkül az adatkezelés nem tekinthető jogszerűnek. A korábbi hazai szabályozás a törvényességet jelölte meg mint alapvető kritériumot – e vonatkozásban a jogszerűségnek még kiterjesztőbb értelmezése van, nem csak törvényi szintű, hanem mindenfajta jogi előírás betartását és betartatását feltételezi.

Megjegyzendő, hogy a hazai eljárásjogi szabályozásban, az Ákr-ben is megjelenik alapelvi szinten a jogszerűség elve,[24] de itt ez eljárási, és nem anyagi jogi alapelvként értelmezendő.

A tisztességesség elve részben párhuzamba vonható a polgári jognak a rendeltetésszerű joggyakorlásra, jóhiszeműségre és tisztességre vonatkozó elvével.

Sok esetben az adatkezelés látszólag jogszerű, van célja és jogalapja is, az adatkezelő formálisan betartja az adatkezelésre vonatkozó szabályokat, az adatok felvétele, kezelése mégis kifogásolható. A jogalkotó a tisztességes adatkezelés elvével egyfajta morális, erkölcsi színezetet ad a látszólag csak technikai jellegű adatkezelési folyamatoknak. Az adatkezelés egészének tisztességessége is az adatkezelés jogszerűségének feltételei közé sorolódott, és ez az emberi méltóság védelmével hozható összefüggésbe. A tisztességesség elvének értelmezéséhez álljon itt két konkrét eset:

Példa: A tisztességtelen adatkezelés körébe sorolandóak a rejtett kamerás megfigyelések.

Példa: A követeléskezeléssel foglalkozó cégek adatkezelésével kapcsolatban a NAIH több alkalommal megállapította annak tisztességtelenségét, ha a követeléskezelő a követelésben nem érintett, az adós környezetében élő más személyektől gyűjt személyes adatokat az adósáról, mert a saját adatairól mindenki csak maga rendelkezhet. Az ilyen adatgyűjtés különösen sérti a személyiségi jogot, mert kiszolgáltatottá teszi az adatalanyokat, egyenlőtlen helyzetet eredményez, amelyben az adatalany nem tudja, hogy az adatkezelő mit tud róla. Az így gyűjtött adatok minősége, valóságtartalma is megkérdőjelezhető az adatforrásnak az adatalanyhoz fűződő viszonyától függően. Az adatgyűjtés az adatalany személyének megítélését a mikrokörnyezetében, az érintett által ápolt vagy nem ápolt

[23] GDPR 5. cikk (1) bekezdés a/ pont.
[24] Ákr. 2. §.

ismeretségi, illetve rokoni körében hátrányosan befolyásolhatja.

Az átláthatóság vagy transzparencia elve még nagyobb hangsúlyt kapott a GDPR-ban a korábbi szabályozáshoz képest. Az átláthatóság az érintett szempontjából vizsgálandó: azt a követelményt testesíti meg, hogy az adatalany követni tudja az adatai sorsát, hogy információja legyen az adatkezelés folyamatáról. Az átlátható adatkezelés biztosítása érdekében a GDPR szabályozza, hogy az adatkezelőknek proaktív módon megfelelő tájékoztatást kell adniuk az érintettek számára még az adatkezelés megkezdése előtt, az adatalanyok pedig a tájékoztatáshoz és a hozzáféréshez való joguk által érvényesíttethetik ezt az elvet. (Ezen témák részletes kifejtése másik fejezetben található.)

Ezen alapelv értelmezéséhez a (39) preambulumbekezdés nyújt segítséget. Ebben a jogalkotó kiemeli, hogy az átláthatóság tekintetében a tájékoztatásnak világosnak, egyszerű nyelvezetűnek, közérthetőnek kell lennie, és könnyen hozzáférhető kell legyen. Kiemeli az adatkezelő személyéről és az adatkezelés céljáról való tájékoztatás fontosságát.

A GDPR (60) preambuluma alapján a tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól.

2.2. Célhoz kötöttség elve

Az adatvédelmi szabályozás kiemelt elveként tekinthetünk a célhoz kötöttség elvére. Az említett OECD Irányelvek közül két irányelv deklarálta ezt az alapelvet (az adatgyűjtés célját az adatgyűjtés időpontjáig meg kell határozni, továbbá az adatok felhasználása e tekintetben korlátozott, nem lehet felhasználni eltérő célból). Az adatvédelmi irányelv is megfelelően tartalmazta a célhoz kötöttség előírását.

A magyar jogban az Avtv. és az Infotv. is lényegében azonos tartalommal deklarálta ezt az elvet. A 15/1991. (IV. 13.) AB-határozat az információs önrendelkezési jog legfontosabb feltételeként és garanciájaként nevezte meg a célhoz kötöttség követelményét. A határozat szerint személyes adatot kezelni/feldolgozni csak pontosan meghatározott és jogszerű célra lehet, és minden szakaszban meg kell felelni ennek a célnak. Az adatkezelés/adatfeldolgozás célját – és annak megváltozását is – közölni kell az érintettel, hogy megalapozottan dönthessen az adatok kiadásáról, megítélhesse az adatkezelés/feldolgozás hatását a jogaira. A célhoz kötött adatkezelés elvéből az következik, hogy a meghatározott cél nélküli, előre nem meghatározott jövőbeni felhasználásra, vagyis készletre való adatgyűjtés és -tárolás alkotmányellenes.

A 29-es adatvédelmi munkacsoport a 3/2013. számú véleményében részletesen elemezte ezt az elvet. Kiemelte, hogy az adatkezelés céljának meghatározása az adatvédelem szabályozásának középpontjában áll. Az adatkezelési cél meghatározása szükséges feltétele az adatkezelés jogszerűségének, továbbá a célmeghatározás szükséges az alkalmazandó adatvédelmi garanciák megállapításához is.

A GDPR szabályozása is egyik fő vezérelvének tekinti a célhoz kötöttséget, melynek lényegi tartalma változatlan a korábbi szabályozáshoz képest: ezen elvből következően minden adatkezelésnek jogszerű célja kell legyen, a célt előre meg kell határozni. A GDPR 5. cikk (1) bekezdésének b) pontja tartalmazza a célhoz kötöttség követelményét. Eszerint személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és az adatok csak e célokkal összeegyeztethető módon legyenek kezelve.

A célhoz kötöttség elvének lényegi tartalma és részletei az alábbiakban fogalmazható meg:

Alapvető az adatkezelési cél azonosítása, meghatározása. A cél meghatározása nélkül a személyes adatokon végzett műveletek cél nélküliek lesznek, és készletre történő adatkezelés történik, amely jogellenes. A jogszerű adatkezelési célt még az adatkezelés megkezdése előtt – de legkésőbb az adatkezelés megkezdésekor – kell megjelölni. Ha egy adatgyűjtésnek nincs célja, vagy nincs konkrétan meghatározott célja, vagy jövőbeni, illetve bizonytalan célra irányul, akkor készletező adatgyűjtésről beszélünk.

Az adatkezelési cél meghatározása az adatkezelő feladata illetve az adatkezelő felelősségi körébe esik. Az adatkezelői szerep megállapításánál kiemelt szerepe van a cél meghatározásának, illetve a cél meghatározása vonatkozásában a mérlegelési jogkörnek és döntéshozatalnak. Az adatkezelés célját mindenképpen az adatkezelő határozza meg, és fordítva, a célmeghatározás mindig adatkezelői minőséget eredményez.

Az adatkezelés célját világosan, egyértelműen meg kell határozni úgy, hogy az érintettek azt értelmezni tudják. Vagyis a célnak kifejezettnek kell lennie, és arról érthetően kell tájékoztatni az érintetteket. Továbbá részletezni is kell annak megállapításához, milyen adatkezelési műveletek kapcsolhatóak az adott célhoz. A célmeghatározás részletessége alapvetően az adatkezelés körülményeitől és az adatok fajtáitól függ. A túl tág, általános megfogalmazású cél nem felel meg a célhoz kötöttség követelményének.

A Rendelet (39) preambulumbekezdése azt hangsúlyozza, hogy az adatkezelés céljáról megfelelő tájékoztatást kell adni, és az adatkezelés konkrét céljainak explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már az adatgyűjtés időpontjában meghatározottaknak kell lenniük.

Az adatkezelési célról adott tájékoztatás formája, módja nincs a jogszabályok által meghatározva, azonban célszerű az írásbeli tájékoztatás, az átláthatóság, az elszámoltathatóság miatt. A megfelelő célmeghatározás és az arról adott megfelelő tájékoztatás által válik lehetővé az adatalanyok számára az információs önrendelkezési joguk gyakorlása.

Fontos, hogy a cél jogszerű legyen, jog gyakorlását vagy kötelezettség teljesítését szolgálja. Vagyis az adatkezelés kizárólag jogszerű célra irányulhat.

Nem elegendő az, ha egy adatkezelésnek megfelelő jogalapja van, ezzel együtt a célhoz kötöttségnek is érvényesülnie kell. Tehát megfelelő jogalap megléte esetén is vizsgálandó az adatkezelési cél. Például önmagában az érintett hozzájárulása esetén még nem jogszerű az adatkezelés, mert elfogadható adatkezelési célnak is fenn kell állnia a célhoz szükséges adatok kezelése vonatkozásában. Adatkezelési cél megjelölése nélküli érintetti hozzájárulás az adatvédelmi jogi szabályozás szempontjából nem lehetséges.

Az adatkezelésnek a folyamat minden szakaszában, illetve minden adatkezelési műveletet tekintve meg kell felelnie az adatkezelési célnak, például az adat felvételekor, nyilvántartásakor, felhasználásakor, továbbításakor is.

A célhoz kötöttség követelménye szoros összefüggésben van az adatminimalizálás elvével, ugyanis csak az adatkezelési cél megvalósulásához szükséges, e cél elérésére alkalmas személyes adatok kezelhetőek. Vagyis mindig az adott célhoz kell viszonyítani az adott adatot, és eldönteni, ténylegesen szükséges-e a cél eléréséhez, és valóban alkalmas-e erre.

A célhoz kötöttség elvének nem felel meg, ha az adatkezelés céljának megjelölése túl általános, semmitmondó, és ezáltal nem alkalmas arra, hogy az adatalany meg tudja ítélni az adatai felhasználását. Ez átvezet az adatkezelő kötelezettségeinek témájához és az előzetes tájékoztatás követelményéhez amiatt, hogy az adatkezelési célról is megfelelő tájékoztatást kell adni.

A már nyilvánosságra hozott személyes adatok további közzététele, felhasználása esetén sem hagyható figyelmen kívül a célhoz kötöttség követelménye – az ilyen továbbfelhasználás akkor jogszerű, ha az eredeti céllal összhangban van. Megemlítendő, hogy ezzel ellentétben az információszabadság jogának érvényesülése érdekében kifejezetten jogellenes a közérdekű adatigénylések során célmegjelölést kérni és az adatigénylés célját vizsgálni.

A célhoz kötöttség követelménye adatvédelmi alapelv, de elmondható, hogy az információszabadság vonatkozásában is van jelentősége. A célmeghatározás, a célhoz kötöttség követelménye nem alkalmazandó a közérdekű adatok vonatkozásában, viszont a közérdekből nyilvános adatok tekintetében igen. Az Infotv. a közérdekből nyilvános adatok terjesztése tekintetében a célhoz kötöttségnek való megfelelőséget írja elő. Ez a nyilvános személyes adatok esetében azt jelenti, hogy ezen adatokat csak a közfeladat ellátása átláthatóvá tételével kapcsolatban vagy a véleménynyilvánítás szabadsága keretei között szabad felhasználni.

Ha az adatkezelés célja megváltozik, akkor ezen célnak megfelelően kell megítélni a jogalap kérdését, a szükségesség elvét és az egyéb garanciák érvényesülését. Ha az adatkezelési cél megszűnik, akkor törlési kötelezettség áll fenn.

A rendelet kifejezetten nevesít olyan adatkezelési célokat, melyeket összeegyeztethetőnek tekint az eredeti adatkezelési céllal, ezek: közérdekű archiválás, tudományos és történelmi kutatás, statisztikai cél. Ez esetben is csak megfelelő garanciák mellett végezhető az adatkezelés, továbbá az uniós vagy tagállami jog eltéréseket állapíthat meg e tekintetben.[25]

Példa: Egy weboldalhoz kapcsolódó adatkezelés vizsgálata során a NAIH megállapította, hogy az adatkezelő célja nem a honlapon megjelölt játékszolgáltatás nyújtása, hanem a valós cél személyes adatok gyűjtése adatbázis építése és értékesítése érdekében, és ezért a cég valótlan adatkezelési célt jelölt meg és elhallgatta a tényleges célt. Az adatkezelő bírósághoz fordult, kifogásolva, hogy az üzleti érdekével ellentétes az, hogy fel kell tárnia az értékesítési tevékenységét e vonatkozásban. A bíróság az adatvédelmi hatóság jogértelmezését erősítette meg ítéletében.

2.3. Adattakarékosság elve

A GDPR az 5. cikk (1) bekezdés c) pontjában adattakarékosság elveként nevesíti azt az alapelvet, mely szerint a személyes adatok megfelelőek és relevánsak kell legyenek az adatkezelés céljához képest, továbbá a szükségesre kell korlátozódniuk.[26]

Az adattakarékosság elve másképpen fogalmazva az adatminimalizálás elve vagy szükségesség elve, tehát ezek a meghatározások lényegében azonos tartalmat takarnak.

Ez az alapelv is szerepelt a korábban hatályos jogi szabályozásban, tehát az adatvédelmi irányelvben illetve az Avtv-ben és az Infotv-ben. Ennek lényege szerint csak olyan személyes adat kezelhető, mely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Az adatkezelőnek még az adatkezelés tényleges megkezdése előtt vizsgálnia kell, hogy szükségesek-e, illetve mely adatok szükségesek az adott célhoz, és egyáltalán szükség van-e személyes adatok kezelésére az adott tevékenység végzéséhez.

A szükségesség elvére számos jogszabály utal, és sok szektorális, ágazati szabályozás meghatározza a kezelendő adatok körét.

Az adattakarékosság elve szorosan összefügg a célhoz kötöttség elvével, mivel a szükséges adatkör meghatározása során mindig az adatkezelés céljához kell viszonyítani. De meg is különböztetendő e két elv: a célhoz kötöttség az adatkezelési cél konkrét meghatározásának igényét jelenti, az adattakarékosság elve pedig az adott cél eléréséhez ténylegesen szükséges adatok kezelését engedi.

A szükségesség elvének korábbi szabályozása kismértékben változott amiatt, hogy a GDPR szerint az adatkezelési célhoz képest megfelelő és releváns adatok kezelése tekinthető jogszerűnek. A szükséges, megfelelő, releváns adatok körének meghatározása sok esetben nem is olyan egyszerű kérdés, és esetről esetre mérlegelendő. Ennek eldöntéséhez az adatkezelési cél pontos, konkrét megnevezése nélkülözhetetlen, mert ehhez viszonyítottan vonható meg az adatkezelés által érintett adatok határa.

Az uniós jogalkotó a *privacy by design* és a *privacy by default* elvének meghatározásakor további szempontokat adott a szükségesség elvének érvényesüléséhez.[27] A beépített adatvédelem elve szerint az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania

[25] GDPR 89. cikk.
[26] GDPR 5. cikk (1) c/ pont.
[27] GDPR cikk.

az adatvédelmi elvek és követelmények érvényesülése érdekében, például az adattakarékosság hatékony megvalósítása érdekében. Az alapértelmezett adatvédelem elve pedig azt mondja, hogy az adatkezelőnek az intézkedéseivel biztosítania kell, hogy kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. A szükségesség ezen szempontja kell érvényesüljön az adatok mennyisége, kezelésük mértéke, tárolási időtartama és hozzáférhetősége tekintetében is.

A GDPR (39) preambulumbekezdése előírja, hogy az adatok körét a célhoz szükséges minimumra szükséges korlátozni, és ezért a tárolásuk a lehető legrövidebb ideig történjen. Ennek érdekében az adatkezelőnek törlési vagy rendszeres felülvizsgálati határidőket kell megállapítania.

2.4. A pontosság elve

A GDPR által meghatározott alapelvek közül a következő a pontosság elve, melyet a GDPR 5. cikk (1) bekezdés d pontja tartalmaz, és amely meghatározás hétköznapi értelme is meglehetősen jó eligazítást nyújt az elv tartalmának megítéléséhez.

A pontosság elve szerint[28] a személyes adatoknak pontosnak és szükség esetén naprakésznek is kell lenniük. A pontatlan személyes adatokat – haladéktalanul – törölni vagy helyesbíteni kell, de legalábbis ésszerű intézkedéseket kell tenni ennek érdekében. Ha az érintett személy bejelenti az adatai – például a neve vagy e-mail-címe – megváltozását, akkor az adatkezelő köteles az adatot a nyilvántartásaiban, az adatbázisában módosítani és a régi adatot törölni.

A pontos adatrögzítésre kiemelten figyelni kell, és ez különösen az adatfelvételre, az adatok rögzítésére vonatkoztatandó, mert az elírás, a hibás adatok további problémákat okozhatnak az adatkezelési folyamat során. A személyek azonosítása és azonosíthatósága is csak pontos adatok rendelkezésre állása esetén lehetséges. Egyes adatelírási, egyéb adminisztratív problémák adatvédelmi incidens bekövetkezéséhez is vezethetnek.

A naprakészség követelménye az adatok frissességére, karbantartására, az adatmódosulások átvezetésére utal. Ez nem abszolút követelmény, hanem szükség szerint kell gondoskodni erről, és esetről esetre mérlegelendő. Az adatok naprakészsége azért lehet fontos elv bizonyos esetekben, hogy elavult adatokon ne alapuljon döntés, már nem aktuális adatok ne legyenek felhasználva. Emellett nyilván üzleti érdek is lehet az adatbázis aktualizálása, frissítése.

A pontosság elvéből következik a helyesbítéshez való jog, vagyis az érintett jogosult arra, hogy kérése esetén az adatkezelő – indokolatlan késedelem nélkül – helyesbítse a megjelölt pontatlan személyes adatokat, tehát az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

A pontatlanság az adatkezelés korlátozását is eredményezheti: az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az érintett vitatja a személyes adatok pontosságát. Ez a korlátozás arra az időtartamra vonatkozik, amely alatt az adatkezelőnek lehetősége van a személyes adatok pontosságának ellenőrzésére.

A teljesség követelménye – az Infotv-nyel ellentétben – a GDPR-ban már nem szerepel.

Példa: Egyes cégek esetében gyakran tapasztalható, hogy adatbázisaikban a magánszemélyek korábbi, már megváltozott telefonszámait, lakcímeit is továbbra is nyilvántartják annak ellenére, hogy azokon az érintett már nem érhető el, és annak ellenére, hogy új, aktuális elérhetőségi adatokkal is rendelkeznek. A lakcímadat kezelésének célja általában az adott személlyel való kapcsolattartás. A kapcsolattartási cél eléréséhez elegendő az érintett aktuális lakcímadatának kezelése. Az elavult, nem naprakész lakcím- és levelezésicím-adatok nem alkalmasak ezen cél elérésére.

[28] GDPR 5 cikk (1) bekezdés d/ pont.

2.5. A korlátozott tárolhatóság alapelve

A GDPR (39)-es preambulum bekezdése határozza meg a korlátozott tárolhatóság elvének irányvonalait. A hazai adatvédelmi jogban ez az elv a célhoz kötött adatkezelés elvével mutat rokon vonásokat.

Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg. Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról.

A személyes adatkezelés konkrét céljainak mindenekelőtt explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már a személyes adatok gyűjtésének időpontjában meghatározottaknak kell lenniük. A személyes adatoknak a kezelésük céljára alkalmasaknak és relevánsaknak kell lenniük, az adatok körét pedig a célhoz szükséges minimumra kell korlátozni. Ehhez pedig biztosítani kell különösen azt, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon.

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg.

A személyes adatok kezelésére vonatkozó elvek között külön kiemelésre került a GDPR 5. cikk e) pontjában a korlátozott tárolhatóság elve. A tárolásnak olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor. Ebben az esetben ugyanakkor az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására fokozott figyelemmel kell lenni.

A korlátozott tárolási időtartamoknak nagy jelentősége van az úgynevezett kötelező erejű vállalati szabályok alapján történő adattovábbítások során is.

2.6. Az integritás és bizalmasság elve

A GDPR 5. cikk *f)* pontja szerint a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (integritás és bizalmas jelleg).

A GDPR (49)-es preambulum bekezdése szerint az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység (CERT), hálózatbiztonsági incidenskezelő egységek (CSIRT), elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos.

A biztonságtechnológiai szolgáltatók által folytatott adatkezelés adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képességét hivatott biztosítani. Az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben nyújt védelmet az adatkezelőknek és közvetetten az érintetteknek.

Az érintett adatkezelők jogos érdekéhez kapcsolódó biztonságtechnikai szolgáltatások magukban foglalhatják például az elektronikus kommunikációs hálózatokhoz való engedély nélküli hozzáférés és a rosszindulatú programterjesztés megakadályozását, továbbá a szolgáltatás megtagadásával járó támadások, valamint a számítógépes és elektronikus kommunikációs rendszerekben való károkozás megállítását.

A bizalmas jellegű adatkezelés sérülése a szakmai titoktartási kötelezettség által védett személyes adatok körében különösen hangsúlyosan jelenik meg. E körben kell tehát értékelni a különböző titoktartásra köteles szakmák képviselőinek adatkezelését, így az adatkezelés vizsgálható az egészségügyi adatok körében az orvosi titoktartással együtt, az ügyvédi hivatás körében, a bank-, biztosítás-, értékpapír-, pénztártitok körében is.

Az egyes szakmákhoz kötődő, titoktartással övezett adatkezelések szabályait a tagállami jogalkotók részletesen szabályozzák. E szabályozási környezetben nagy hangsúlyt kap annak megítélése, hogy ki által és milyen feltételekkel ismerhető meg valamely bizalmas adat, másként fogalmazva védett adat.

Az egyes hatóságok, így például a tagállami adatvédelmi hatóságok, a pénzpiacok felügyeletét ellátó hatóságok, adóhatóságok az adott eljárásukhoz szükséges mértékben az adat bizalmas jellegétől függetlenül megismerhetik ezeket a személyes adatokat.

A bizalmas jelleg sérülésének az alábbi eseményeket tekinthetjük:

- az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány;
- ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett;
- ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak,
- ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak;
- ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából;
- ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

A bizalmas jellegű adatkezelés fenntartása az adatkezelők és az adatfeldolgozók részéről tevőleges magatartást kíván meg. A biztonság fenntartása és a GDPR rendelkezéseit sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz.

Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés – mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

Az adatvédelmi incidensek megelőzése, bekövetkezésük esetén azok feltárása és elhárítása közvetlen összefüggésben áll az adatkezelés bizalmasságának elvével.

A GDPR (85) preambulum bekezdése szerint az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek.

Többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt okozhat az adatkezelő.

Ezek elkerülését, illetve mérséklését szolgálja az az adatkezelői kötelezettség, amely szerint az adatvédelmi incidenst indokolatlan késedelem nélkül, a tudomására jutástól számított 72 órán belül be kell jelenteni a felügyeleti hatóságnál.

Az adatkezelés bizalmi jellegének megőrzésénél nemcsak strukturális és intézményi kötelezettségeket állapít meg a GDPR, hanem a bizalmi jellegű adatkezelésnek meghatározza a személyi követelményét is a tisztviselőkkel összefüggésben; akár az adatkezelő oldalán működnek adatvédelmi tisztviselőkként, akár a felügyeleti hatóságok alkalmazásában álló tisztviselőkről van szó.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

A fentiek értelmében tehát az adatok bizalmas kezelése kiterjed az uniós vagy tagállami jognak megfelelően mindegyik felügyeleti hatóság tagjára vagy tagjaira és személyzetére is a feladataik ellátása és hatáskörük gyakorlása során a tudomásukra jutott bármely bizalmas információ tekintetében hivatali idejük alatt és annak lejártát követően is, amelynek következtében szakmai titoktartási kötelezettség terheli őket. Hivatali idejük alatt ez a szakmai titoktartási kötelezettség különösen vonatkozik a természetes személyek által e rendelet megsértését illetően tett bejelentésekre.

Minden tagállami tisztviselő ennek az elvnek a figyelembevételével köteles eljárni a mindennapi munkája során érvényre juttatva az objektív, pártatlan és független ügyintézés elveit, annak érdekében, hogy az érintettek bizalma töretlen maradjon az adott felügyeleti hatóság irányába.

2.7. Alapfogalmak a GDPR 4. cikkének részletes bemutatásán keresztül

A GDPR 4. cikke tartalmazza a rendelet által visszatérő jelleggel alkalmazott fogalmak jelentős részének meghatározását. A GDPR, vagy a GDPR által hivatkozott más uniós jogi norma által kifejezetten nem definiált fogalmak jelentéstartalmát ugyanakkor az egyes tagállamok belső normái alapján kell meghatározni (például „*közhatalmi szerv*”),[29] illetve segíthetik az értelmezést az Európai Adatvédelmi Testület által jóváhagyott vagy kibocsátott vélemények, iránymutatások is.[30]

A GDPR 4. cikkében meghatározott fogalmak közül is ki kell emelni a *személyes adat*, az érintett, az *adatkezelő*/*adatkezelés*, *adatfeldolgozó* meghatározását, mivel ezek a hivatkozott cikkben definiált további fogalmak megértéséhez is szükségesek.

A *személyes adat*, valamint az érintett fogalmát a GDPR 4. cikk 1. pontja definiálja, mely szerint „*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*

[29] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv 29. cikke szerint létrehozott adatvédelmi munkacsoport (a továbbiakban: Adatvédelmi Munkacsoport) által kibocsátott „Guidelines on Data Protection Officers (’DPOs’)” 2.1.1. pont, 6. o. (az angol nyelvű változatban).

[30] Az Adatvédelmi Munkacsoport által kibocsátott, és az Európai Adatvédelmi Testület által annak 2018. május 25. napján tartott első plenáris ülésén jóváhagyott, tehát 2018. május 25. napjától is hivatkozható dokumentumainak a jelen szakanyag előkészítéséig jóváhagyott listája a következő címről érhető el: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható." A személyes adat fogalmával szorosan összefügg a genetikai adat GDPR 4. cikk 13. pontjában, a biometrikus adat GDPR 4. cikk 14. pontjában, valamint az egészségügyi adat GDPR 4. cikk 15. pontjában meghatározott fogalma, melyeket a tantárgyi tematika 2. és 3. pontja ismerteti részletesen, ezért jelen fejezet nem tárgyalja.

A GDPR 4. cikk 2. pontja határozza meg az adatkezelés fogalmát, mely szerint „*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.*" A definíció tehát nem taxatív, azonban önmagában az a tény, hogy valamely tevékenység személyes adatok kezelésnek minősül, még nem egyenértékű a GDPR szabályainak alkalmazásával: arra csak abban az esetben kerülhet sor, ha a személyes adatok kezelése a GDPR 2. cikk (1) bekezdésében meghatározott tárgyi hatály alá tartozik, és nem tarozik a GDPR hatály alól kivett, a rendelet 2. cikk (2) bekezdésében meghatározott körbe.

A GDPR 4. cikk 7. pontja szerint „*adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan 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.*" Az adatkezelő fő fogalmi ismérvei tehát az adatkezelés céljának és eszközeinek meghatározása. A GDPR 4. cikk 8. pontja szerint „*adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel",* az adatfeldolgozó tehát maga is adatkezelési tevékenységet végez, vonatkozásában azonban nem valósul meg az adatkezelői minőséget eredményező kritériumok egyike sem. Mivel az adatkezelés fogalmának ismertetésére, az adatkezelő és az adatfeldolgozó elhatárolására, valamint az adatvédelmi jog egyéb szereplőinek bemutatására a tantárgyi tematika 4. pontjában kerül sor, jelen fejezet nem tárgyalja részletesebben.

A GDPR 4. cikk 3. pontja szerint „*az adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából*", e fogalomnak alapvetően a GDPR 18. cikke szerinti érintetti jog gyakorlása szempontjából van jelentősége.

A GDPR 4. cikk 4. pontja szerint „*profilalkotás: a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják*"; a profilalkotással kapcsolatos szabályozást a tantárgyi tematika 5. pontja ismerteti részletesen.

A GDPR 4. cikk 5. pontja szerint „álnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni." Az álnevesítés következtében tehát az adat nem veszíti el személyes adat jellegét, arra továbbra is a személyes adatok védelmére vonatkozó szabályokat kell alkalmazni, az álnevesítés révén azonban biztosítható az adat védelmének magasabb szintje. Az álnevesítéssel kapcsolatban a GDPR (28) preambulumbekezdése rögzíti, hogy „*A személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint segíthet az adatkezelőknek és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek. Az „álnevesítés" e rendeletbe történő kifejezett bevezetése nem irányul más adatvédelmi intézkedés kizárására*".

A GDPR 4. cikk 6. pontja szerint „*nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.*" A definíció elsősorban a GDPR tárgyi hatályára vonatkozó, 2. cikk (1) bekezdése szerinti rendelkezések értelmezéséhez szükséges.

A GDPR 4. cikk 9. pontja szerint „*címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.*" A definíció jelentősége a személyes adat harmadik személy számára történő közlése kapcsán jelentős, melyre a GDPR számos ponton utal (például az érintett tájékoztatása kapcsán a GDPR 13. cikk (1) bekezdés e) pontja és 14. cikk (1) bekezdés e) pontja; az érintett hozzáférési joga kapcsán a GDPR 15. cikk (1) bekezdés c) pontja).

A GDPR 4. cikk 10. pontja szerinti „*harmadik fél*" fogalmának elsősorban a GDPR 6. cikk (1) bekezdés f) pontja szerinti jogalap alkalmazása körében van jelentősége. E fogalom szerint „*harmadik fél": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.*"

Ugyancsak az adatkezelés jogalapjára vonatkozó rendelkezések, pontosabban a GDPR 6. cikk (1) bekezdés a) pontjának, valamint a GDPR 9. cikk (1) bekezdés a) pontjának értelmezése szempontjából jelentős az érintett hozzájárulása mint jogalap fogalmi elemeinek ismerete. A GDPR 4. cikk 11. pontja szerint „*az érintett hozzájárulása" az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.*"

Az információs társadalommal összefüggő szolgáltatások fogalmának ismerete a gyermekkorú – a GDPR 8. cikke alapján a 16. életévüket, eltérő tagállami rendelkezés esetén is legfeljebb a 13. életévüket – betöltött gyermekkorú személyek adatkezeléshez történő hozzájárulásának érvényessége kapcsán releváns. A GDPR 4. cikk 25. pontja szerint „*az információs társadalommal összefüggő szolgáltatás: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás."*[31]

Az úgynevezett adatvédelmi incidensekre vonatkozó szabályok ismerete az adatbiztonságra vonatkozó követelmények teljesülésének vizsgálata, így különösen a GDPR 33-34. cikkének alkalmazása során lényeges. A GDPR 4. cikk 12. pontja szerint „*adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.*"

---

[31] Az Európai Parlament és a Tanács 2015/1535 irányelve „1. cikk (1) […] b) „szolgáltatás": az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.

E fogalommeghatározás alkalmazásában:

i. „távolról" azt jelenti, hogy a szolgáltatást a felek egyidejű jelenléte nélkül nyújtják;

ii. „elektronikus úton" azt jelenti, hogy a szolgáltatás kezdőpontjától való elküldése és célállomásán való fogadása adatok feldolgozására (beleértve a digitális tömörítést is) és tárolására szolgáló elektronikus berendezés útján történik, valamint annak elküldése, továbbítása és vétele teljes egészében vezetéken, rádión, optikai vagy egyéb elektromágneses eszköz útján történik;

iii. „a szolgáltatást igénybe vevő egyéni kérelmére" azt jelenti, hogy az adatok továbbításával nyújtott szolgáltatás egyéni kérelemre történik."

Az adatkezelő tevékenységi központja, a személyes adatok határon átnyúló kezelése, a felügyeleti hatóság,[32] valamint az érintett felügyeleti hatóság fogalmainak ismerete különösen a GDPR VI-VII. fejezetei, illetve az egyes tagállami felügyeleti hatóságok illetékességének, a GDPR alkalmazása körében történő együttműködésük rendje szempontjából releváns, melyeket szoros összefüggésük okán együttesen indokolt ismertetni. Ezen fogalmak értelmezésével kapcsolatban lényeges információkat tartalmaz még az Adatvédelmi Munkacsoport WP 244 rev.01 számú iránymutatása.[33]

A GDPR 4. cikk 23. pontja szerint „*személyes adatok határokon átnyúló adatkezelése":*

a) *személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy*

b) *személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket.*"

A GDPR 4. cikk 16. pontja szerint „*tevékenységi központ:*

a) *az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;*

b) *az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak.*"

Az adatkezelő/adatfeldolgozó tevékenységi központjának fenti meghatározása alapján lehetséges az úgynevezett fő felügyeleti hatóság (tehát – főszabály szerint – a GDPR 60. cikke szerinti eljárásban a döntés meghozatalára jogosult hatóság) meghatározása személyes adatok határon átnyúló kezelésével járó ügyekben. A GDPR 4. cikk 22. pontja szerint ugyanakkor „*érintett felügyeleti hatóság: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint*:

a) *az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;*

b) *az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy*

c) *panaszt nyújtottak be az említett felügyeleti hatósághoz.*"

Személyes adatok határon átnyúló kezelése esetén tehát minden esetben azonosítható egy fő felügyeleti hatóság az adatkezelő tevékenységi központja/egyetlen tevékenységi helye alapján a GDPR 56. cikk (1) bekezdése szerint, míg a GDPR 4. cikk 22. pontjában felsorolt egy vagy több feltétel teljesülése esetén más hatóság(ok) érintett hatóságként határozható(k) meg. A GDPR 56. cikk (2) bekezdésében írt esetet kivéve az előbbiekben említett hatóságok jogosultak eljárni fő- és érintett hatóságként

[32] A GDPR 4. cikk 21. pontja szerint „felügyeleti hatóság: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv.

[33] Az Adatvédelmi Munkacsoport által kibocsátott „Lead supervisory authority Guidelines for identifying a controller or processor's lead supervisory authority" 1.1-2.2. pont, 3-8. o. (az angol nyelvű változatban).

személyes adatok határon átnyúló kezelése esetén a 60. cikkben foglaltak szerint.

A GDPR VII. fejezete szerinti együttműködési és egységességi eljárásokhoz való szoros kapcsolódása miatt itt indokolt ismertetni az úgynevezett releváns és megalapozott kifogás fogalmát, melynek a fő felügyeleti hatóság és a többi érintett hatóság közötti együttműködés (GDPR 60. cikk (4)-(6) bekezdései) és ezzel összefüggésben az Európai Adatvédelmi Testület vitarendezési eljárása (GDPR 65-66. cikk) kapcsán van jelentősége. A GDPR 4. cikk 24. pontja szerint tehát „*releváns és megalapozott kifogás: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét.*”

A képviselő GDPR 4. cikk 17. pontja szerinti fogalmának alapvetően abban az esetben van relevanciája, ha az adatkezelés a GDPR 3. cikk (2) bekezdésében meghatározott okok miatt tartozik a GDPR hatálya alá, ezért az adatkezelő vagy adatfeldolgozó a GDPR 23. cikkei alapján írásban köteles képviselőt kinevezni. A „*képviselő: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában*.”

A „*vállalkozás*” (GDPR 4. cikk 18. pont), valamint a *vállalkozáscsoport* (GDPR 4. cikk 19. pont)[34] fogalmának uniós szinten történő megfogalmazása alapvetően a felügyeleti hatóságok által a GDPR 83. cikke alapján kiszabható bírság alkalmazása miatt indokolt. A GDPR 4. cikk 18. pontja szerint „*vállalkozás: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.*”, a GDPR 4. cikk 19. pontja szerint pedig „*vállalkozáscsoport: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások.*” A „*kötelező erejű vállalati szabályok*” (GDPR 4. cikk 20. pont), valamint a *nemzetközi szervezet* (GDPR 4. cikk 26. pont) meghatározása a személyes adatok harmadik országba, vagy nemzetközi szervezetek részére történő továbbítására vonatkozó szabályai (GDPR V. fejezet), valamint az adattovábbításra tekintettel meghatározott további rendelkezései (például érintetti jogok, jogalapok stb.) miatt lényeges.

A GDPR 4. cikk 20. pontja szerint „*kötelező erejű vállalati szabályok: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részére történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ.*” A GDPR 4. cikk 26. pontja szerint „*nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.*”

[34] Ld. még a GDPR (37) preambulumbekezdését.

2.8. A személyes adatok kezelésének alapelvei a bűnügyi irányelvvel összefüggésben

Az Infotv. 4. § (1) – (4) bekezdései tartalmazzák a személyes adatok kezelésének elveit[35]. Az alapelvek katalógusa túlnyomó részben nem a bűnügyi adatvédelmi irányelv harmonizálásának eredménye, hanem hanem jóval korábban, a magyar alkotmányos jogfejlődés során vált törvényben rögzített jogi normává.[36]

A hatályos Infotv. és a GDPR adatkezelés alapelveit a következő táblázat hasonlítja össze:

Infotv. 4. § – A személyes adatok kezelésének alapelvei	**GDPR 5. cikk – A személyes adatok kezelésére vonatkozó elvek [A személyes adatok:]**
(1) Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, [...]	b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; [a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés] („célhoz kötöttség”);
(1) [...] az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.	a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);
(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.	c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”)
(3) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.	
(4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.	d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”); e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; [a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel] („korlátozott tárolhatóság”);

[35] A 4. § (5) bekezdése egy olyan korábbi hozzátoldás, amely egy sajátos adatkezelési szituációra vonatkozó, kazuisztikus szabályozást tartalmaz, ezért alapelvnek aligha tekinthető: „A személyes adatok kezelését tisztességesnek és törvényesnek kell tekinteni, ha az érintett véleménynyilvánítási szabadságának biztosítása érdekében az érintett véleményét megismerni kívánó személy az érintett lakóhelyén vagy tartózkodási helyén felkeresi, feltéve, hogy az érintett személyes adatait e törvény rendelkezéseinek megfelelően kezelik és a személyes megkeresés nem üzleti célra irányul. A személyes megkeresésre a munka törvénykönyve szerinti munkaszüneti napon nem kerülhet sor.”

[36] Lásd. például 15/1991. (IV. 13.) AB határozat, 29/1994. (V. 20.) AB határozat.

(4a) Az adatkezelés során arra alkalmas műszaki vagy szervezési – így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító – intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.	f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).
	(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”)

A táblázatban [szögletes zárójelek között, dőlt betűvel] jelöltük azokat a részleteket, amelyek az alapelvek lényegi összehasonlítása során figyelmen kívül hagyhatók és aláhúzással azokat a részeket, amelyek esetében (legalábbis látszólag) nincs megfeleltethető alapelvi szabály a másik jogi normában. A kapcsolódó megjegyzések:

1. A GDPR 5. cikk (1) bekezdés a) pontjától eltérően az Inftv. nem fogalmazza meg külön alapelvként azt, hogy az adatkezelést az érintett számára átlátható módon kell végezni, ám a magyar szabályozás az Alkotmánybíróság iránymutatásának[37] megfelelve messzemenően megfelel ennek az elvnek, hiszen főszabályként tájékozódási és hozzáférési jogot biztosít az érintett számára, amely csak olyan mértékben és módon korlátozható, amely szükséges és arányos intézkedésnek minősül egy demokratikus társadalomban.
2. Az Infotv. 4. § (1) bekezdésében említett tisztességes eljárás kapcsán a bűnügyi adatvédelmi irányelv (26) preambulumbekezdése megjegyzi, hogy „a személyes adatok kezelésének minden esetben jogszerűnek, tisztességesnek és átláthatónak kell lennie az említett természetes személyek vonatkozásában, és arra csak jogszabályban meghatározott konkrét célokból kerülhet sor. Ez önmagában nem akadályozza meg a bűnüldöző szerveket az olyan tevékenységek végzésében, mint például a fedett nyomozás vagy a videokamerás megfigyelés. Ilyen tevékenységek a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása, többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése céljából végezhetők, ha jogszabályon alapulnak és – kellő tekintettel az említett természetes személyek jogos érdekeire – egy demokratikus társadalomban szükséges és arányos intézkedésnek minősülnek. A tisztességes adatkezelés elve – mint adatvédelmi elv – a tisztességes eljáráshoz való jognak a Charta 47. cikkében és az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (EJEE) 6. cikkében meghatározott fogalmától elkülönülő fogalom.”
3. Az Infotv. 4. § (3) bekezdése az alapelvek között helyez el egy olyan szabályt, amely tulajdonképpen a személyes adat definíciójának is a részét képezhetné. Az ehhez kapcsolódó adatvédelmi követelmény az Infotv. 4. § (4) bekezdésében található, amelynek a GDPR 5. cikk (1) bekezdés e) pontjában foglaltak feleltethetők meg.
4. Az Infotv. 4. § (4a) bekezdésében szabályozott integritási és bizalmassági elv az egyetlen olyan alapelv, amely a bűnügyi adatvédelmi irányelv átültetésekor került bele az Infotv. joganyagába.
5. Az Infotv. nem emeli ki külön alapelvként az adatkezelő elszámoltathatóságát, ám az Infotv. is tartalmazza azokat a szabályokat és jogintézményeket, amelyek a GDPR szabályozási rendszerében az elszámoltathatóságot szolgálják. Ezek különösen a következők:

[37] Bármilyen jogszabály, amely – az alkalmazott eljárásra tekintet nélkül – személyes adat felvételéről, gyűjtéséről, tárolásáról, rendezéséről, továbbadásáról, nyilvánosságra hozásáról, megváltoztatásáról, a további felhasználás megakadályozásáról, az adatból új információ előállításáról, vagy akármilyen más módon történő felhasználásáról (a továbbiakban: a személyes adat feldolgozásáról) rendelkezik, csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adat útját a feldolgozás során követni, és jogait érvényesíteni tudja. Az erre szolgáló jogintézményeknek tehát biztosítaniuk kell az érintett beleegyezését a feldolgozásba, illetve pontos garanciákat kell tartalmazniuk azokra a kivételes esetekre nézve, amikor az adatfeldolgozás az érintett beleegyezése (esetleg tudta) nélkül történhet. (15/1991. (IV. 13.) AB határozat).

a) A beépített adatvédelem és alapértelmezett adatvédelem szabályainak megfeleltethető, az adatkezelőt terhelő kötelezettségek, l. Infotv. 25/A. §
b) Az adatkezelői és az adatfeldolgozói nyilvántartás és az elektronikus napló, l. Infotv. 25/E. § és 25/F. §.
c) Az adatvédelmi hatásvizsgálat és az előzetes konzultáció, l. Infotv. 25/G. §
d) Adatbiztonsági intézkedések, l. Infotv. 25/I. §
e) Az adatvédelmi incidensek kezelése, l. Infotv. 25/J §, 25/K. §
f) Az adatvédelmi tisztviselő, l. Infotv. 25/L. §

Az elszámoltathatóság GDPR-ban rendelkezésre álló eszközei közül a magatartási kódexek (l, GDPR 40-41. cikk) és a kötelező erejű vállalati szabályok (lásd GDPR 47. cikk) az Infotv. hatálya alá tartozó bűnüldözési, honvédelmi és nemzetbiztonsági célú adatkezelések adatkezelői esetében azok közhatalmi jellegére tekintettel nem vehetők számításba.

Mindezek alapján az állapítható meg, hogy az Infotv. és a GDPR az adatkezelés alapelveinek tartalmát, lényeges részét tekintve nagyjából megfeleltethető, legalábbis annyira, hogy a GDPR adatkezelés elveiről írtak – a fenti megjegyzéseket is figyelembe véve – alapul vehetők az Infotv. adatkezelés alapelveinek tanulmányozásakor.

3. AZ INFOTV. ÉS A GDPR SZAKKIFEJEZÉSEINEK ÖSSZEHASONLÍTÁSA

Mind az Infotv., mind a GDPR tartalmaz olyan jogi szakkifejezéseket, amelyek egységes értelmezését maga az adott norma (a jogalkotó) határozza meg. Ezeket az Infotv. értelmező rendelkezéseknek, a GDPR fogalommeghatározásoknak nevezi, de a lényegük ugyanaz: a jogalkalmazóknak (valamint a gyakorlatban az érintetteknek, az adatkezelőknek, az adatfeldolgozóknak stb.) szóló, a szakkifejezés értelmezésére vonatkozó, kötelező erejű meghatározások. Ezek értelmezési tartománya rendszerint az adott jogszabály alkalmazására terjed ki, amit a jogi normában a felvezető szövegrész („*E törvény alkalmazásában [...]*”, „*E rendelet alkalmazásában* [...]”) tesz egyértelművé. A jogszabályban meghatározott értelmezések a jogalkotótól erednek, ezért autentikus értelmezésnek szokás nevezni azokat.

Az Infotv. és GDPR egyazon jogterületre, a személyes adatok védelmére vonatkozik és a hatályuk ugyan egyértelműen elhatárolható, ám a jogalkalmazás során gyakran adódik olyan helyzet, amikor a két jogi normát egységes rendszerben, egymásra tekintettel kell értelmezni és alkalmazni. Ennek az egyik alapvető feltétele, hogy a fogalmi rendszerük megfeleltethető legyen, vagyis azoknál a szabályozási részterületeknél, amelyek esetében a jogi szabályozás párhuzamos, illetve a másikra tekintettel alkalmazandó, ott a két jogi norma lehetőleg páronként azonos jelentésű fogalmak minél egységesebb készletéből építse fel a szabályozás rendszerét. Ha ez az elvárás nem teljesül, vagyis az együttesen, illetve egymásra tekintettel alkalmazandó jogi normák másként építenék fel a fogalmi rendszereiket, illetve ugyanaz a szakkifejezés mást jelentene az egyik jogi normában, mint a másikban, az a jogalkalmazók legrosszabb rémálma lenne. Vizsgáljuk meg, hogy mennyire feleltethető meg a szabályozás fogalmi rendszere az Infotv. és a GDPR esetében! A két jogi norma szakkifejezéseinek összehasonlító referenciatáblázatát a 12.2-es számú melléklet tartalmazza.[38]

Az Infotv. mintegy 13 olyan értelmező rendelkezést tartalmaz, amelynek fogalommeghatározás-megfelelője hiányzik GDPR-ból, viszont a GDPR 7 fogalommeghatározását az Infotv. nem tartalmazza. Továbbá az elnevezés szerint megfeleltethető szakkifejezések némelyikéhez más szövegű értelmezés járul az Infotv.-ben és a GDPR-ban.

Közelebbről vizsgálva az alábbiak szerint tipizálhatók az eltérések okai:

- A két jogi norma részben más jellegű adatkezelésekre vonatkozik. A GDPR szabályozásának fókuszában az érintett hozzájárulása alapján, a piaci szférában, nemritkán transznacionális nagyvállalatok által végzett adatkezelés van. Ezzel szemben az Infotv. a gyakorlatban főként a bűnüldözési, honvédelmi és nemzetbiztonsági célból, állami szervek által, kötelező jelleggel végzett adatkezelésekre alkalmazandó. Ennek megfelelően a GDPR alkalmazása során lényeges a például kötelező erejű vállalati szabályok vagy a vállalkozáscsoport fogalom meghatározása, az Infotv. alkalmazása során azonban nem. Ugyanez a helyzet a másik oldalról például a bűnüldözési célú adatkezelés vagy a nemzetbiztonsági célú adatkezelés esetében, amelyeket az Infotv. értelmez, a GDPR nem. Tehát a joganyag azon részeinél, ahol a két jogi norma más tárgyköröket

[38] A táblázatban csak a személyes adatok védelmével kapcsolatos fogalmakat tüntettük fel, vagyis kihagytuk az Infotv. információszabadsággal kapcsolatos értelmező rendelkezéseit, valamint a GDPR tagállami hatóságok eljárásaival kapcsolatos fogalommeghatározásait.

szabályoz, és ezért nem merül fel tárgyi és eljárási jogi összefüggések a jogi normák között, ott nem fontos a szakkifejezések megfeleltethetősége.

- Az Infotv. értelmező rendelkezést ad a *különleges adatra*. A GDPR-ban ugyanerre vonatkozó fogalommeghatározás nem szerepel, ám a 9. cikk (1) bekezdésében azonos értelemben használja a *személyes adatok különleges kategóriái* kifejezést és állapít meg adatkezeléssel kapcsolatos szabályt e kategória vonatkozásában. Ez azt jelzi, hogy a fogalmi megfeleltetés nem csak két értelmező rendelkezés (fogalommeghatározás) között lehetséges. (Ugyanez állapítható meg a *közös adatkezelőről* is. L. az Infotv. 3. § 9a. pontját és a GDPR 26. cikkét.)
- Némelyik értelmező rendelkezésnél találhatók kisebb szövegeltérések, amelyek általában lényegtelenek, a jogalkalmazást nem befolyásolják. Az Infotv. értelmező rendelkezései esetenként részletezőbbek a GDPR fogalommeghatározásainál. Például az Infotv. 3. § 1. pontja az érintettre vonatkozó értelmező rendelkezésben kiemeli, hogy bármely információ alapján azonosított vagy azonosítható személyről van szó. A GDPR megelégszik annyival, hogy a személyes adatra vonatkozó fogalommeghatározásban az azonosított vagy azonosítható személyre utal. Ez nem eredményez tartalmi eltérést. Továbbá az Infotv. tartalmaz olyan értelmező rendelkezést is, amelynek bevezetésére célszerűségi, kodifikációs okból került sor (például harmadik ország).
  A fentebb vázolt eltérések nem vonják kétségbe hogy az Infotv. és a GDPR fogalmi rendszere közös alapokon nyugszik. Az eltérések olyan különbségekben nyilvánulnak meg, amelyek a gyakorlatban nem nehezítik a két jogi norma terminológiai megfeleltetését. Ugyanakkor vannak további, magyarázatot igénylő eltérések is.
- A GDPR nem tartalmazza az adatkezeléssel kapcsolatos alapvető fogalmak egy részének (adatfeldolgozás, adattovábbítás, adattörlés, nyilvánosságra hozatal, adatmegsemmisítés) meghatározását, noha e fogalmakat a GDPR is használja. Ez azért nem jelent problémát a jogalkalmazás során, mert ezek esetében olyan alapvető fogalmakról van szó, amelyek az adatvédelmi jog születésével egyidősek, az azóta eltelt idő alatt letisztázódott és megszilárdult a jelentésük, ezért ezen fogalmak azonosan értelmezendők az Infotv. és a GDPR alkalmazása során.
- Az Infotv. 5. § (7) bekezdése akként egészíti ki a különleges adat Infotv. 3. § 3. pontjában meghatározott értelmezési tartományát, hogy a bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni. (A GDPR nem tartalmaz hasonló kiegészítést a „személyes adatok különleges kategóriái” esetében.)

4. A SZEMÉLYES ADAT FOGALMÁNAK RÉSZLETES BEMUTATÁSA

4.1. Bevezetés

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) [a továbbiakban: GDPR; Rendelet] középpontjában a személyes adatok és azok védelme áll, ezért fontos tisztában lenni azzal, hogy pontosan mit is értünk személyes adatok alatt. A Rendelet célja a megfelelő jogszabályi keretek között ezek szabad áramlásának elősegítése, úgy, hogy közben a lehető legteljesebb szinten biztosítva legyen védelmük.

Věra Jourová, a jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős biztos 2018. május 24-én közölt nyilatkozatában az alábbiakat mondta:

„*A 21. században a személyes adatok igazi értéket jelentenek, mi pedig tulajdonképpen minden egyes lépésünkkel adatokat hagyunk hátra, különösen a digitális világban. A személyes adatokat illetően az emberek helyzete jelenleg olyan, mintha pőrén állnának egy kirakatban.*

Az adatvédelem alapvető jog az EU-ban. Az új szabályok jóvoltából az európaiak visszaszerzik az ellenőrzést adataik felett. A döntés arról, hogy mi történjen és ki, milyen jellegű adatokkal rendelkezzen, immár a mi kezünkben van.”[39]

Miért is ennyire fontos a személyes adatok védelme? Mit is értünk pontosan e fogalom alatt? Létezett-e egyáltalán 2018. május 25. előtt is ez a kategória, vagy a Rendelet honosított meg egy új jogintézményt, amely védelmet biztosít a magyar állampolgárok számára is?

4.2. Történelmi előzmények

A nemzetközi szabályozás keretein belül az első adatvédelmi törvények az 1970-es években jelentek meg, azonban ekkor még jellemző volt az egységes szabályozás hiánya. Az 1980-as évektől már nemzetközi dokumentumok elfogadására is sor került. Az Európai Unióban egészen a közelmúltig az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (a továbbiakban: Irányelv) tartalmazta a legfontosabb szabályokat, melyeket Magyarország is átemelt és törvényben hirdetett ki. Ezt követte a Rendelet, amely már közvetlenül alkalmazandó és teljes közvetlen hatállyal bír.

---

[39] Lásd: http://europa.eu/rapid/press-release_STATEMENT-18-3889_hu.htm

Hazánkban az 1980-as évek vége, 1990-es évek eleje indította el a változást, az Alkotmány rendszerváltást követő módosításával jelent meg a személyes adatok védelmére vonatkozó első rendelkezés.[40] Ezt követően az Alkotmánybíróság a személyes adatok védelme tekintetében nagy jelentőségű, 15/1991. (IV.13.) AB határozatában[41] megállapította, hogy „személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes", valamint kimondta, hogy „a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám) alkotmányellenes".

A személyes adat fogalmát az első adatvédelmi törvény, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) határozta meg. A jogszabályt Magyarország Európai Unióhoz történő csatlakozását követően jelentősen módosították, átültetve az Irányelv rendelkezéseit a magyar jogba. A következő jelentős módosítást a 2012. január 1-jétől hatályos, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) jelentette, azonban a személyes adat fogalmában ez nem eredményezett jelentős változást. Az Alkotmány helyébe lépő Alaptörvény VI. cikkének (3) bekezdése a korábbiakhoz hasonlóan deklarálja a személyes adatok védelméhez való jogot, illetve a (4) bekezdés e védelem érvényesülésének ellenőrzését „sarkalatos törvénnyel létrehozott, független hatóság" feladatává teszi. Az Infotv. középpontjában elsősorban a magánszféra és az egyén védelme áll, melyet a személyes adatok védelmére vonatkozó szabályok biztosítanak.

Az Irányelv helyett alkalmazandó új jogi norma, a GDPR 2016-tól hatályos, azonban egy felkészülési időszakot követően alkalmazni csak 2018. május 25-től kötelező. A Rendelet a személyes adat fogalmában az Irányelvhez képest kismértékű változást hozott, amely az Infotv-ben is megjelenik.

4.3. A személyes adat fogalma

A GDPR 4. cikkének 1. pontja határozza meg a személyes adat fogalmát a következőképpen:

„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."

A fogalmat az Infotv. GDPR-ral összefüggésben elfogadott és 2018. július 26-tól hatályos módosítása is tartalmazza, azonban azt a megoldást választva, hogy a GDPR definícióját három részre bontva három különböző fogalom jelenik meg az értelmező rendelkezések között: a személyes adat,[42] az érintett[43] és az azonosítható természetes személy.[44]

A GDPR-ban meghatározott fogalomból tulajdonképpen csak az első mondatrész – „azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ" – az, amely a szó szoros értelmében véve a személyes adat definíciójának tekinthető.

Fentiek értelmében a fogalom megértéséhez a következő elemek vizsgálata szükséges:

- adat,
- azonosított vagy azonosítható,

[40] 1949. évi XX. törvény 59.§ „A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog."

[41] Lásd: http://public.mkab.hu/dev/dontesek.nsf/0/1CE263A376458F27C1258382003C412C?OpenDocument

[42] Infotv. 3.§ 2. pont.

[43] Infotv. 3.§ 1. pont.

[44] Infotv. 3.§ 1a. pont.

- természetes személy,
- vonatkozó,
- bármely információ.

A fogalom értelmezéséhez a fenti elemeket logikai sorrendben tárgyaljuk.

4.3.1. Adat

Noha az adat a központi elemét képezi a személyes adatok fogalmának, elkülönülten nem definiálta a jogalkotó, hasonlóan az Avtv-hez, ahol erre szintén nem került sor. A GDPR és az Infotv. fogalommeghatározásait alapul véve azonban kikövetkeztethető ennek a tartalma is. „Egyaránt adatnak minősül valamely ismeret és az ezen ismeret alapján bárki számára levonható következtetés is", azaz nem csak az „objektív körülmények, a tények és információk tekinthetők adatnak, hanem adatnak minősül a szubjektum szintjén megjelenő vélemény, elképzelés, következtetés is". Ennek értelmében nemcsak az „érintettre ténylegesen vonatkozó, valós információk adatok, hanem úgyszintén adatnak tekinthetők az esetleges nem aktuális, valótlan vagy téves ismeretek is."[45] Lényegében minden adatnak minősül – függetlenül attól, hogy például papír alapon létezik, vagy elektronikusan, azonosítónak tekinthető, vagy egy jellemzőnek –, ami egy adott természetes személyre vonatkozik, és amely alapján az közvetlenül vagy közvetve beazonosítható.

4.3.2. Természetes személy

A természetes személy fogalmát az Emberi Jogok Európai Nyilatkozatának 6. cikkében találhatjuk, mely szerint „mindenkinek joga van ahhoz, hogy jogalanyiságát bárhol elismerjék."[46] Valamennyi emberi lény jogosult személyes adatainak védelmére, illetve az azok feletti rendelkezésre. A természetes személyeket e jog megilleti függetlenül nemzetiségüktől, tartózkodási helyüktől, állampolgárságuktól.[47]

Személyes adatok védelméről élő természetes személyek esetében beszélhetünk. A polgári jog szabályai alapján az egyén születésétől – meghatározott, kivételes esetben fogantatásától – haláláig lehet jogviszonyok alanya. Az elhunytak adatai vonatkozásában a kegyeleti jogok játszhatnak szerepet, illetve egyes esetekben egy elhunyt bizonyos – korábban személyes adatnak minősülő – adatai más, még élő személyek vonatkozásában jelenthetnek személyes adatot (például örökösök). Ez akkor jelenthetne problémát, ha erre vonatkozóan nem léteznének speciális szabályok, amelyek kezelésüket meghatározzák. Egy örökölhető betegségben elhunyt esetében ugyanis az adat hozzátartozói számára személyes adatnak minősülhet, amely az ő szempontjukból speciális védelmet kell, hogy kapjon. Ezért ezekre az adatokra külön szabályok vonatkoznak, melyek kötik a halál bekövetkezését követően is az egészségügyi tevékenységet végzőket, illetve iránymutatást adnak számukra az adatok kezelését illetően.

Ugyanígy speciális esetet jelent az, ha az adatkezelő nincs tisztában azzal a ténnyel, hogy az érintett időközben elhunyt és továbbra is személyes adatként kezeli az információkat.

Noha a GDPR az elhunytak személyes adataira nem alkalmazandó, a (27)-es preambulumbekezdés lehetőséget biztosít a tagállamok számára az elhunyt személyek hozzátartozói és örökösei vonatkozásában a személyes adatokra vonatkozó jogosultságok érvényesítését biztosító jogszabályi rendelkezések meghozatalára. E rendelkezések az Infotv. 25. §-ban 2018. VII. 26-tól találhatóak meg.

---

45 Adatvédelem és információszabadság a mindennapokban (Szerkesztette: Péterfalvi Attila) HVG-ORAC 2012., p. 59.

46 Lásd: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=hng

47 GDPR (2) preambulumbekezdés.

Néhány példa személyes adatokra:
- TAJ szám,
- adószám,
- fizikai jellemzők (magasság, szemszín, testsúly…),
- online azonosítók,
- GPS adatok.

Ugyanakkor nem terjed ki a GDPR hatálya:
- az elhunyt személy nevére,
- a személynevet tartalmazó jogi személy elnevezésére (például Kovács Bt.).

4.3.3. Bármely információ

Bármilyen személyre vonatkozó állítás lehet, amely azonosított, vagy azonosítható élő, természetes személlyel kapcsolatos. Az információk lehetnek objektívek, vagy szubjektívek és nem szükséges az sem, hogy valósak legyenek. Azaz személyes adatnak minősülhet akár valótlan, vagy nem igazolt információ is, ha az előbbi feltételek teljesülnek.

Az információ tartalma szempontjából a személyes adat fogalma valamennyi, információt tartalmazó adatra kiterjed, a forma, azaz a megjelenés módja tekintetében bármilyen alakban előforduló ismeretről szó lehet. A személyes adatok védelmének szükségességére az egyre inkább elterjedő, automatizált adatfeldolgozásra képes eszközök hívták fel a figyelmet, de e vonatkozásban nem csak az informatikai rendszerekben tárolt adatokra kell gondolnunk, hanem a papír alapú, a hang- és videófelvételekre is.

4.3.4. Vonatkozó

Az információ akkor személyes adat, ha egy adott (az adott) egyénről szól. Ez nem minden esetben könnyen eldönthető, például egy gépjármű rendszáma lehet személyes adat, ha egyértelműen a tulajdonoshoz tudom kötni és nem az, ha beazonosítási lehetőség nélkül egy parkolóházban található több tucat jármű mellett elhaladva nem tudjuk beazonosítani a tulajdonos személyét.

Az adott egyénre vonatkozó információ tartalom, cél vagy eredmény elem lehet.[48]

Tartalom elem, ha egy adott személyről szól az információ, cél elem, ha az adatot abból a célból használják fel, hogy az egyénnel kapcsolatban tegyenek lépéseket (például teljesítményértékelés elvégzése). Eredmény elem, ha nem feltétlenül van meg a tartalom vagy a cél elem, de az információ felhasználása valószínűleg hatással van egy adott személy jogaira és érdekeire, figyelembe véve az adott esetet övező valamennyi körülményt.

[48] WP 29 4/2007. vélemény – https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

4.3.5. Azonosított vagy azonosítható

Azonosítottnak tekinthető egy természetes személy, ha a rendelkezésre álló információk – személyes adatok – alapján elkülönül egy adott csoport minden más tagjától, még akkor is, ha erre az azonosításra bármilyen oknál fogva nem kerül sor. (Azonosító lehet például valamilyen fizikai jellemző, munkahelyi beosztás stb.)

A közvetlen vagy közvetett módon történő azonosítás elhatárolása is esetenként elérő lehet. Egy elterjedt családi és keresztnév például lehetetlenné teheti a közvetlen azonosítást, míg egy egyedi esetében akár több tízezres populáció vonatkozásában megvalósulhat ez. Ettől függetlenül egy elterjedt név esetében is személyes adatról kell beszélnünk, ha az azonosítás, azonosíthatóság feltétele fennáll. Ha azonban semmilyen formában nem kapcsolható össze az érintett és az adat, akkor nem beszélhetünk személyes adatról, így ez az információ nem tartozik a személyes adatok védelmére vonatkozó rendelkezések hatálya alá.

A közvetett módon történő azonosításhoz adnak támpontot a Rendelet fogalommeghatározásában felsoroltak, azaz a név, szám, helymeghatározó adat, online azonosító, természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező.

Azok az adatok esetében, melyeket olyan formában tettek megismerhetetlenné, amely visszafordíthatatlan, anonimizálásról beszélhetünk. Ez esetben az érintett többé nem azonosítható, ezért már nem beszélhetünk személyes adatról, így a Rendelet (és az Infotv.) szabályai sem vonatkoznak rájuk. Az anonim adatok esetében különösen fontos, hogy sem az adatkezelő, sem egyéb személy ne tudja többé azonosítani az adott személyt. Ugyanakkor azt is figyelembe kell venni, hogy egyes, korábban anonimizált adatok a technikai fejlődés során esetlegesen azonosíthatóvá válnak (például nagyméretű adatbázisok összevetése által, amelyeket manuálisan nem, de informatikai eszközökkel már meg lehet oldani). Erre is utal a preambulumbekezdés, amikor kijelenti, hogy az adatkezeléskor rendelkezésre álló technológiákat és a technológia fejlődését is számításba kell venni. A Rendelet (26)-os preambulumbekezdése szerint azokat az álnevesített adatokat, melyeket valamely további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni

Szükséges megemlíteni a pszeudonimizálás fogalmát is, melynek segítségével ugyanazon személyre vonatkozó további adatokat lehet gyűjteni anélkül, hogy az illető személyét megismernék. Ezek elengedhetetlenek bizonyos kutatások (orvostudományi, gyógyszerészeti stb.) lefolytatásához, vagy statisztikák elkészítéséhez. A pszeudonimizált adatok tulajdonképpen közvetett azonosítást lehetővé tevő adatok, megfelelő technikai intézkedéseket kell tenni, hogy az újbóli azonosítás ne legyen lehetséges. A (26)-os preambulumbekezdés ugyanakkor kimondja, hogy a Rendelet nem vonatkozik az anonim információk kezelésére, ideértve a statisztikai vagy kutatási célú adatkezelést is.

5. AZ ADATKEZELÉS FOGALMÁNAK ISMERTETÉSE

Az adatvédelem középpontjában maga az érintett áll, aki bármely információ alapján azonosított, vagy azonosításra kerülhet.

Az GDPR egyik kulcsfogalma az adatkezelés, melynek részletes leírását a fogalommeghatározások között találjuk. Az adatkezelés fogalma elválaszthatatlan annak tárgyától, a személyes adat fogalmától, amelyet a GDPR rendkívül körültekintően úgy határoz meg, hogy 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.

Az egységesült európai adatvédelmi szabályozásban fellelhető adatkezelésre adott fogalommeghatározás a GDPR 4. cikk 2. pontjában az alábbiak szerint fogalmaz:

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.

A GDPR (4) preambulum bekezdése szerint a személyes adatok kezelését az emberiség szolgálatába kell állítani. A GDPR a magyar alapjogi megközelítés keretein túllépve, azaz az állami beavatkozás és objektív intézményvédelmi garanciák kiépítésének kötelezettségén túlmenően új célokat jelöl meg preambulum bekezdéseiben, amelyek az adatkezelés fogalmának értelmezési tartományát az előttünk álló hatósági eljárásokban új dimenziókba fogják helyezni.

Ahogyan arra a GDPR (5) preambulum bekezdése is utal, a belső piac működéséből eredő gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását. Megnövekedett az állami és a magánszereplők, köztük a természetes személyek, egyesületek és a vállalkozások között Unió-szerte zajló személyes adatok cseréje. Az uniós jog együttműködésre és személyes adatok cseréjére kötelezi tagállamok nemzeti hatóságait annak érdekében, hogy képesek legyenek feladataikat ellátni, illetve hogy más tagállam hatóságai nevében eljárjanak.

Az adatkezelés fogalmának ilyen tág meghatározása mögött a GDPR (6) preambulum bekezdése szerint az a felismerés húzódik, hogy a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi.

Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét.

Eszerint az adatvédelem és azon belül az adatkezelés fogalom meghatározásának horizontja kiszélesedett az egységes európai szabályozás elfogadásával és kilépve a hagyományos alapjogi, az adott tagállam és az érintett viszonyaként értelmezett keretekből egy tágabb viszonyrendszer között

nyer elhelyezést, ahol adatkezelőkként már nem csak állami, közhatalmi szervek jelenhetnek meg az adott jogviszonyban, hanem az adatkezelők személyi körének – ahogy az a következő pontokban részletesebben is kifejtésre kerül majd – széles spektrumát ismerhetjük meg.

Másfelől az adatkezelés fogalmának tág meghatározása nemcsak a széles adatkezelői személyi körből fakad, hanem a technológiai fejlődés által lehetővé tett nagyszámú, adattárolásra alkalmas számítógépes rendszerek, okos eszközök elterjedésével is magyarázható.

Az adatkezelés lehet automatizált módon végzett, vagy nem automatizált módon végrehajtott adatkezelés. Az adatoknak a nem automatizált kezelésére akkor kell alkalmazni a GDPR rendelkezéseit, ha azok valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartás részévé kívánnak tenni. A GDPR tárgyi hatálya és így az adatkezelés fogalmi köre a nyilvántartási céltól függetlenül kiterjed valamennyi automatizált adatkezelésre. Az automatizált adatkezelés fogalmába az automatizált eszköz útján történő adatkezelések tartoznak, amelyek – a manuális (azaz kézi) adatkezeléssel szemben – jellemzően az adatokon elektronikus eszközzel, számítógéppel végzett adatkezelési műveleteket jelentik.

A GDPR a manuálisan végzett adatkezelések vonatkozásában tartalmaz megszorító rendelkezéseket. A kézi, azaz a nem automatizált (más kifejezéssel: papír alapú) adatkezelések esetében a rendelet hatálya csak azokra az adatokra terjed ki, amelyek valamely nyilvántartási rendszer részei, vagy amelyek kezelése nyilvántartási céllal történik.

Azt, hogy mi minősül nyilvántartási rendszernek, a GDPR 4. cikk 6. pontja határozza meg. E szerint nyilvántartási rendszer a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető. A nyilvántartás fogalma tehát tágan értelmezendő, annak minősülhet bármilyen jegyzék, lista, gyűjtemény, amelyben az adatok bármilyen, az érintettel összefüggésbe hozható szempont szerint csoportosításra került.

A GDPR által adott adatkezelés-fogalomban meghatározott tevőleges magatartások közül a rendelet csupán egyet nevesít. Az adatkezelés korlátozása a GDPR 4. cikk 3. pontja szerint a tárolt személyes adatok megjelölését jelenti valamely jövőbeli cél érdekében.

A fogalommeghatározás egyéb elemei a konkrét esetekben nyernek majd részletesebb kibontást. Különös figyelmet kell majd fordítaniuk a tagállami hatóságoknak az Európai Adatvédelmi Testület által elfogadott véleményekben megfogalmazódott, az új szabályozásban megjelenő fogalmak pontos és egységes tartalmú alkalmazását elősegítő iránymutatásokra.

6. AZ ADATKEZELŐ ÉS AZ ADATFELDOLGOZÓ ELHATÁROLÁSA

A GDPR 4. cikk 7. pontja tartalmazza az adatkezelő fogalmának meghatározását, mely szerint adatkezelőnek minősül az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan 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 GDPR (22) preambulum bekezdése szerint az adatkezelő vagy adatfeldolgozó a tevékenységi helyén folytatott működése során, az Unió területén végzett bármely személyesadat-kezelést e rendelettel összhangban kell végezni, tekintet nélkül arra, hogy maga az adatkezelés az Unió területén történik-e. A tevékenységi hely valamely tevékenység tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlását feltételezi. E keretek jogi formája – legyen szó akár fióktelepről vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező.

A lehetséges adatkezelők és adatfeldolgozók körét szélesíti ki a GDPR (24) preambulum bekezdése, amely szerint az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó általi kezelése abban az esetben is e rendelet hatálya alá tartozik, amennyiben az érintettek Unión belüli magatartásának a megfigyeléséhez kapcsolódnak. Annak meghatározása, hogy az adatkezelés az érintettek magatartásának megfigyelésének minősül-e, meg kell megvizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezt követően a természetes személy profiljának megalkotását is magában foglaló adatkezelési technikákat alkalmaznak-e, annak érdekében, hogy elsősorban a természetes személyre vonatkozó döntéseket hozzanak, valamint, hogy elemezzék vagy előre jelezzék a természetes személy személyes preferenciáit, magatartását vagy beállítottságát.

Az adatkezelő pontos beazonosításához tehát ezen értelmezési keretek között kell meghatározni azt, hogy az érintettre vonatkozó, személyes adatait érintő döntés ki által és hol született meg.

A GDPR 36. preambulum bekezdése különös jelentőséget tulajdonít a tevékenységi központ meghatározásának, mely mozzanatnak döntő jelentősége van az adatkezelők meghatározásánál.

Meg kell említeni azt is, hogy a GDPR alkalmazási időszakát megelőző hazai szabályozásban is meghatározó jelentőségű előkérdésként jelentkezett a Hatóság vizsgálati és hatósági eljárásaiban annak körültekintő megállapítása, hogy az adatkezelésre vonatkozó döntések hol születtek meg.

Az adatkezelő Unión belüli tevékenységi központja az Unión belüli központi ügyvitelének helye, kivéve, ha a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy másik Unión belüli tevékenységi helyén hozzák, amely esetben ez utóbbi másik tevékenységi központot kell a tevékenységi központnak tekinteni.

Az adatkezelő Unión belüli tevékenységi központját objektív szempontok alapján kell meghatározni, és e fogalom magában foglalja az adatkezelés céljára és eszközeire vonatkozó fő döntéseket meghatározó ügyvezetési tevékenység tényleges és valós, tartós jelleget biztosító körülmények közötti gyakorlását. E szempont nem függhet attól, hogy a személyes adatok kezelése a szóban forgó helyszínen zajlik-e. A személyes adatok kezelésére szolgáló műszaki eszközök jelenléte és használata, illetve az adatkezelési tevékenység önmagában nem jár tevékenységi központként való minősítéssel, és ezért nem meghatározó szempontja a tevékenységi központnak.

Az adatfeldolgozó tevékenységi központja az Unión belüli központi ügyvitelének helye kell, hogy legyen, vagy ha az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az a hely, ahol az Unióban a fő adatkezelési tevékenységek zajlanak. Az 29. Cikk szerinti Adatvédelmi Munkacsoport által kiadott, az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásához adott, WP 244 rev. 01 számú iránymutatása elemzi az adatkezelő tevékenységi központjának meghatározását.

Az Iránymutatás szemléletes példákon keresztül mutatja be az adatkezelés központi helyének meghatározását, melynek az adatkezelő személyének meghatározásán túl döntő szerepe van a fő felügyeleti hatóság megállapításánál is, valamint a tagállami felügyeleti hatóságok együttműködésének is alapvető kérdése.

A tevékenységi központ megállapításához előbb meg kell határozni az adatkezelő Unión belüli központi ügyvitelének helyét, ha van ilyen. Az általános adatvédelmi rendeletből következő megközelítés szerint az Unión belüli központi ügyvitel helyén születnek a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntések, és az ilyen döntések végrehajtatására is ez a hely rendelkezik hatáskörrel.

Amennyiben egy multinacionális vállalat az adatkezelési tevékenységeinek céljaival és eszközeivel kapcsolatos döntéseket az Unión belüli egyik tevékenységi helyén összpontosítja (és ez a tevékenységi hely rendelkezik hatáskörrel ilyen döntések végrehajtására), akkor csak egy fő felügyeleti hatóságot kell meghatározni az adott multinacionális vállalat esetében.

Ilyen helyzetekben elengedhetetlen, hogy a vállalkozások pontosan megjelöljék, hol születnek az adatkezelés céljaival és eszközeivel kapcsolatos döntések. A tevékenységi központ helyes megjelölése az adatkezelők és adatfeldolgozók érdeke, hiszen egyértelművé teszi, mely felügyeleti hatósággal kell kapcsolatban lenniük az általános adatvédelmi rendeletben foglalt kötelezettségeik teljesítésével összefüggő különféle feladataikat illetően.

Ezek közé tartozik adott esetben az adatvédelmi tisztviselő kijelölése, vagy a hatósággal való egyeztetés olyan adatkezelési tevékenység esetén, amelynek kockázatát az adatkezelő észszerű módon nem tudja mérsékelni. Az általános adatvédelmi rendelet vonatkozó rendelkezései ezeket a kötelezettségek teljesítésével összefüggő feladatokat hivatottak megkönnyíteni.

Az alábbiakban néhány példa ennek szemléltetésére:

1. példa: Egy élelmiszer-kiskereskedő székhelye (azaz központi ügyvitelének helye) a hollandiai Rotterdamban található. Emellett több más uniós tagállamban is rendelkezik tevékenységi helyekkel, amelyek egyénekkel állnak kapcsolatban. Mindegyik tevékenységi helyen ugyanazokkal a szoftverekkel kezelik a fogyasztók személyes adatait üzletszerzés céljából. A fogyasztói személyes adatok üzletszerzési célú kezelésének céljaival és eszközeivel kapcsolatos összes döntést a rotterdami székhelyen hozzák. Következésképpen a vállalat fő felügyeleti hatósága ennek a határokon átnyúló adatkezelési tevékenységnek a tekintetében a holland felügyeleti hatóság.

2. példa: Egy bank székhelye Frankfurtban található, az összes banki adatkezelési tevékenységét onnan szervezik, biztosítási üzletága viszont Bécsben működik. Ha az összes biztosítási célú adatkezelési tevékenységre vonatkozó döntések meghozatala és e döntések végrehajtása az Európai Unió egész területét tekintve a bécsi tevékenységi hely hatáskörébe tartozik, akkor az általános adatvédelmi rendelet 4. cikkének 16. pontjában foglaltak szerint a tevékenységi központot a személyes adatok kezelésének céljára és eszközeire tekintettel kell meghatározni, azaz a biztosítási célú adatkezelések központja ebben az esetben Bécs.

Könnyen belátható, hogy a személyes adatok banki célú kezelése számos különféle adatkezelési tevékenységet foglal magában. Az egyszerűség kedvéért azonban az összeset egyetlen célként kezeljük. Ugyanez vonatkozik a biztosítási célú adatkezelésre. A főhatóság a személyes adatok határokon átnyúló, biztosítási célú kezelését illetően az osztrák felügyeleti hatóság, a személyes adatok banki célú kezelését illetően pedig a német hatóság (a hesseni tartományi felügyeleti hatóság) lesz, függetlenül attól, hol találhatóak az ügyfelek.

Az adatfeldolgozó fogalmát a GDPR 4. cikk 8. pontja határozza meg. Eszerint adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozó a tevékenységét tehát kizárólag az adatkezelő nevében végezheti. Ennek alapja az adatkezelővel kötött szerződés vagy más jogi dokumentum, amelyben pontosan meghatározásra kerülnek az adatfeldolgozó kötelezettségei.

Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Az adatfeldolgozóval kötött szerződésnek vagy más jogi aktusnak az alábbiakat kell tartalmaznia:

- az adatkezelés tárgyát,
- időtartamát,
- jellegét és célját,
- a személyes adatok típusát,
- az érintettek kategóriáit, valamint
- az adatkezelő kötelezettségeit és jogait.

A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli.

E tevékenységbe bele tartozik a személyes adatoknak harmadik ország vagy nemzetközi szervezet számára való továbbítását is.

Az adatfeldolgozónak kötelessége biztosítani azt az adatkezelés teljes időtartama alatt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállaljanak.

Az adatfeldolgozónak további kötelezettsége, hogy garantálja az adatkezelés biztonságát.

Az érintett jogainak gyakorlása biztosítása körében kiemelkedő feladata az adatfeldolgozóknak is, hogy az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segítsék az adatkezelőket abban, hogy teljesíteni tudják kötelezettségüket az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolásában.

Az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha jogszabály a személyes adatok tárolását írja elő.

Az adatfeldolgozó köteles az adatkezelővel folyamatos kapcsolatot tartani annak érdekében, hogy rendelkezésére bocsásson minden olyan információt, amely az adatkezelő kötelezettségeinek teljesítéséhez szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a GDPR rendelkezéseit vagy a tagállami vagy uniós egyéb adatvédelmi rendelkezéseket. Az adatfeldolgozót terhelő felelősség körében van jelentősége ennek a rendelkezésnek. Az adatfeldolgozói minőség általános szerződési feltételeken is alapulhat.

Ha egy adatfeldolgozó e rendeletet sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni.

7. AZ ADATVÉDELMI JOG EGYÉB SZEREPLŐINEK ISMERTETÉSE

7.1. Az érintett

Az adatvédelemi jog egyéb szereplőinek első helyén az érintett áll. A GDPR 4. cikk 1. pontja szerint érintett az azonosított vagy azonosítható természetes személy. 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.

Az érintetti jogok biztosítása teszi lehetővé a magánszféra védelmét. A GDPR 15. cikke rögzíti az érintett hozzáférési jogát, melynek keretében az azonosítás, vagy annak lehetősége esetére az érintettet az alábbi jogok illetik meg.

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- az adatkezelés céljai;
- az érintett személyes adatok kategóriái;
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

A GDPR (71) preambulum bekezdése meghatározó jelentőségű az érintetti jogok értelmezési tartalmának szempontjából. E szerint az érintett jogosult arra, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen alapuló – akár intézkedést is magában foglaló – döntés hatálya, amely a rá vonatkozó egyes személyes jellemzők kiértékelésén alapul, és amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti, mint például egy online hitelkérelem automatikus elutasítása vagy emberi beavatkozás nélkül folytatott online munkaerő-toborzás.

Ilyen adatkezelésnek minősül a „profilalkotás" is, vagyis a természetes személyekre vonatkozó személyes jellemzők bármilyen automatizált személyes adatok kezelése keretében történő kiértékelése, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők elemzésére és előrejelzésére, ha az az érintettre nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti.

Megengedhető azonban az efféle adatkezelésen – ideértve profilalkotást is – alapuló döntéshozatal, ha azt az olyan uniós vagy tagállami jog kifejezetten engedélyezi, amelynek hatálya alá az adatkezelő tartozik, például a csalások és az adócsalás nyomon követése és megelőzése céljából, feltéve hogy erre az uniós intézmények vagy a tagállami felügyeleti hatóságok szabályaival, előírásaival és ajánlásaival összhangban kerül sor, vagy az adatkezelő által nyújtott szolgáltatás biztonságának és megbízhatóságának a biztosítása érdekében, vagy ha arra valamely, az érintett és egy adatkezelő közötti szerződés megkötése vagy teljesítése érdekében van szükség, vagy ha az érintett ahhoz kifejezett hozzájárulását adta.

Az ilyen adatkezelés mindazonáltal csakis megfelelő garanciák mellett végezhető, amelybe beletartozik az érintett külön tájékoztatása és az ahhoz való joga, hogy emberi beavatkozást kérjen és kapjon, különösen hogy kifejtse álláspontját, hogy magyarázatot kapjon az ilyen értékelés alapján hozott döntésről és, hogy megtámadja a döntést. Az ilyen intézkedés gyermekre nem vonatkozhat.

Az érintett szempontjából tekintve tisztességes és átlátható adatkezelés biztosítása érdekében az adatkezelő a profilalkotáshoz megfelelő matematikai és statisztikai eljárásokat alkalmaz, olyan technikai és szervezési intézkedéseket vezet be, amelyek biztosítják különösen az adatok pontatlanságát előidéző tényezők korrekcióját és a hibalehetőségek minimálisra csökkentését.

A személyes adatok biztonságáról oly módon kell gondoskodni, amely alapján az érintett érdekeit és jogait potenciálisan veszélyeztető tényezőket figyelembe veszik, és megakadályozzák többek között az olyan hatások érvényesülését, amelyek a természetes személyek közötti hátrányos megkülönböztetést eredményeznek faji vagy etnikai származás, politikai vélemény, vallási vagy világnézeti meggyőződés, szakszervezeti tagság, genetikai vagy egészségi állapot, szexuális irányultság vagy nemi identitás alapján.

Azokat az adatkezeléseket, amelyek a homogén csoportba tartozó érintettek között önkényes megkülönböztetésre adnának alapot, más szóhasználattal élve diszkriminatív hatásúnak tekinthetünk, illetve ilyen hatást kiváltó intézkedéseket eredményeznek, az adatkezelők kötelesek elkerülni. A személyes adatok különleges kategóriáin alapuló automatizált döntéshozatal és profilalkotás csak bizonyos meghatározott feltételek mellett engedélyezhető.

Az érintettekre negatív hatású adatkezelés elkerülését biztosító új szabályozás a beépített és alapértelmezett adatvédelem, melynek keretében már az adatkezelési műveletek megtervezésekor olyan megfelelő szintű technikai és szervezési intézkedéseket hajt végre az adatkezelő, amely biztosítja az érintettek számára a szükséges garanciák beépülését az adatkezelés teljes folyamatába.

Az érintettet érintő adatkezelés alapfeltételeit a GDPR 5. cikke tartalmazza; annak tisztességesnek és átláthatónak kell lennie. Gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem kezelhetik ezekkel a célokkal össze nem egyeztethető módon (célhoz kötöttség).

Az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és az adatkezelésnek, tulajdonképpen a magánszféra azonosítás következtében történő feltárásának a szükségesre kell korlátozódnia (adattakarékosság).

A kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék (pontosság).

A tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül

majd sor (korlátozott tárolhatóság).

Az érintettre vonatkozó személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (integritás és bizalmas jelleg).

Az adatkezelő felelős a fenti elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására is az érintettek irányába. (elszámoltathatóság).

Ha az érintett gyermek, a GDPR 8. cikk (1) bekezdése szerint az információs társadalommal összefüggő szolgáltatások vonatkozásában a gyermek személyes adatainak kezelése akkor jogszerű, ha betöltötte a 16. életévét. Ezen életkor alatt a gyermekek személyes adatainak a kezelése csak akkor jogszerű, ha a hozzájárulást a gyermek felett szülői felügyeleti jogot gyakorló szülő adta meg. A gyermekeket, mint érintetteket megillető jogokat helyettük és nevükben a szülők gyakorolják.

7.2. A címzettek

A GDPR 4. cikk 9. pontja szerint *címzett* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

A GDPR (31) preambulumbekezdés szerint az alábbi, hivatalos feladataikkal kapcsolatos jogi kötelezettségeik keretében eljáró közhatalmi szervek nem tekinthetőek címzettnek:

- az adó- és vámhatóságok,
- a pénzügyi nyomozóegységek,
- a független közigazgatási hatóságok, valamint
- az értékpapírpiacok szabályozásáért és felügyeletéért felelős pénzügyi hatóságok.

E közhatalmi szerveknek a címzetti minőség alóli kivételét az indokolja, hogy, amikor személyes adatokat kapnak, az adattovábbítás az uniós vagy a tagállami jog alapján egy konkrét közérdekű vizsgálat lefolytatásához szükségesek.

A közhatalmi szervek nyilvánosságra hozatal iránti kérelmeit eseti alapon, írásban, indokolással ellátva kell benyújtani, és azok nem vonatkozhatnak teljes nyilvántartási rendszerekre, illetve nem eredményezhetik nyilvántartási rendszerek összekapcsolását. Az említett személyes adatok e közhatalmi szervek általi kezelése során – az adatkezelés céljának megfelelően – a vonatkozó adatvédelmi szabályokat be kell tartani.

A hazai eljárásjogok a közhatalmi szervek adatigényét azzal a kodifikációs technikával biztosítja, hogy pontosan meghatározza azokat az állami szerveket, amelyek jogosultak a személyes adatoknak valamely, az adott eljáráshoz kapcsolódó megismeréséhez.

A címzettekhez történő adattovábbítás alapvető feltétele, hogy nem sérülhet a természetes személyeknek a GDPR által biztosított védelmi szintje.

Az adatkezelő tájékoztatási kötelezettségébe tartozik, hogy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor e körülményről tájékoztassa az érintetteket.

A személyes adatok helyesbítése, korlátozása, törlése körében az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel,

illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

Az adatkezelő által vezetett nyilvántartás tartalmazza az olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket.

A felügyeleti hatóságok az adattovábbítások megfelelő garanciájaként értékelhetik a személyes adatok továbbítására a címzettekkel kötött szerződést.

A felügyeleti hatóságok korrekciós hatáskörükben eljárva jogosultak elrendelni a címzettek értesítését is a személyes adatok helyesbítéséről, törléséről, az adatkezelés korlátozásáról, valamint elrendelhetik a címzett, vagy nemzetközi szervezet felé irányuló adatáramlás felfüggesztését is.

7.3. Harmadik fél

Harmadik fél az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

A harmadik fél pozíciójának meghatározásánál tehát azokat a szervezeti felépítéseket és szerződéses kapcsolatokat kell elsősorban vizsgálni, amely alapján a harmadik fél különállósága, önállósága megállapíthatóvá válik. Az adatkezelőktől, adatfeldolgozóktól való elkülönülés vizsgálata különösen akkor lehet fontos, ha az adatvédelemmel kapcsolatos kötelezettségek teljesülésnek vizsgálatára kerülhet sor.

Kiemelendő a fogalommeghatározásból az is, hogy az érintettől is önálló a harmadik fél, azaz az adatkezelés által nem beazonosított, vagy beazonosítható; másként fogalmazva az adatkezelés nem őrá irányul.

Az adatkezelés megfelelő jogalappal végzett műveletei között találjuk a GDPR 6. cikk *f*) pontjában a harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelést. A harmadik fél jogos érdekének elismerése, mint megfelelő jogalap csak akkor lehetséges, ha az érintett személyes adatainak a védelmét garantálják; különös figyelemmel kell lenni ebben a körben arra a körülményre, ha az érintett még gyermek.

Az adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait.

Az ilyen jogos érdekről lehet szó olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll.

A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor.

Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

Mivel a tagállami jogalkotó feladata, hogy jogszabályban határozza meg, hogy a közhatalmi szervek milyen jogalapon kezelhetnek személyes adatokat, az adatkezelő jogszerű érdekét alátámasztó jogalapot nem lehet alkalmazni a közhatalmi szervek által feladataik ellátása során végzett adatkezelésekre.

Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése, valamint a személyes adatok közvetlen üzletszerzési célú kezelése szintén az érintett adatkezelő jogos érdekének minősül.

7.4. Képviselő, uniós képviselő

A képviselő fogalmát a GDPR 4. cikk 17. pontja határozza meg, mely szerint „képviselő": az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában.

A képviselő az adatkezelő vagy az adatfeldolgozó nevében jár el, és e minőségében bármelyik felügyeleti hatóság megkeresheti. Az adatkezelő vagy az adatfeldolgozó írásbeli megbízás útján kifejezetten kijelöli a képviselőt arra, hogy nevében az e rendelet értelmében fennálló kötelezettségei tekintetében eljárjon. A képviselő kijelölése nem érinti az adatkezelőre, illetve adatfeldolgozóra e rendelet értelmében háruló hatásköröket és felelősséget. A képviselő feladatait az adatkezelőtől vagy az adatfeldolgozótól kapott – és ideértve az illetékes felügyeleti hatóságokkal az e rendeletnek való megfelelés biztosítása érdekében tett bármely lépés tekintetében való együttműködést is előíró – megbízással összhangban látja el. Meg nem felelés esetén, a kijelölt képviselővel szemben az adatkezelő vagy az adatfeldolgozó kikényszerítési eljárásokat indíthat.

Az adatkezelők, illetve adatfeldolgozók képviselői egyesületi formában is működhetnek, ahol az egyesület célja az e rendelet hatékony alkalmazásának az elősegítése érdekében magatartási kódexek kidolgozása és létrehozása. E magatartási kódexek keretében meg lehet határozni az adatkezelők és az adatfeldolgozók kötelezettségeit, figyelembe véve azt a kockázatot, amellyel az adatkezelés a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően jár.

A GDPR 27. cikke szerint az Unióban tevékenységi hellyel nem rendelkező adatkezelő, vagy adatfeldolgozó akkor köteles kijelölni, ha az adatkezelési tevékenységek: áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.

Az uniós képviselő kijelölésének kötelezettsége nem terheli az adatkezelőket és adatfeldolgozókat azokban az esetekben, ha az adatkezelés alkalmi jellegű és nem terjed ki sem a személyes adatoknak a különleges kategóriáira, sem a büntetőjogi felelősség megállapításához kapcsolódó személyes adatok nagy számban történő kezelésére. Az uniós képviselő kijelölésének mellőzésénél arra is figyelmemmel kell lenni, hogy – figyelembe véve az adatkezelés jellegét, körülményeit, hatókörét és céljait – valószínűsíthetően nem jelent kockázatot a természetes személyek jogaira és szabadságaira nézve.

Közhatalmi vagy egyéb, közfeladatot ellátó szervekre nem vonatkozik az uniós képviselő kijelölésének kötelezettsége, hiszen ezen szervek jogszabályból fakadó hatáskörüknél fogva látják el feladataikat, illetve a következő alpontban tárgyalt adatvédelmi tisztviselő segíti a munkájukat.

Az adatkezelő vagy az adatfeldolgozó által a képviselő számára adott megbízásnak a GDPR 27. cikk (4) bekezdése szerint ki kell terjednie arra, hogy az adatkezeléssel összefüggő minden ügyben, az e rendeletnek való megfelelés biztosítása érdekében – különösen a felügyeleti hatóságok és az érintettek megkeresésére – az adatkezelő vagy az adatfeldolgozó helyett vagy mellett a képviselő járjon el.

A képviselő kiemelt feladata az adatkezelési nyilvántartások vezetése, amelyet a felügyeleti hatóságok megkeresése esetén a hatóság rendelkezésére kell bocsátani; ezen túlmenően pedig együttműködési kötelezettség terheli a felügyeleti hatósággal.

7.5. Adatvédelmi tisztviselő

A GDPR 37. cikk (1) bekezdése szerint az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik. Ez a kijelölési kötelezettség nem vonatkozik az igazságszolgáltatási feladatkörükben eljáró bíróságokra.

Szintén kötelező adatvédelmi tisztviselő kijelölése, ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél, céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé.

Adatvédelmi tisztviselő kijelölése szükséges akkor is, ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáira vonatkoznak, illetve a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni.

Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon. Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztviselőt a 39. cikkben említett feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel. Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti. Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség. Az Adatvédelmi Munkacsoport a WP 243 rev.01 számú iránymutatásában részletes szempontrendszert dolgozott ki az adatvédelmi tisztviselők kijelölésével kapcsolatban.[49]

[49] Lásd: https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf

8. A SZEMÉLYES ADAT KÜLÖNLEGES KATEGÓRIÁINAK RÉSZLETES BEMUTATÁSA

8.1. A különleges adat fogalma és kezelésükre vonatkozó főbb szabályok

A GDPR a különleges adatok fogalmát nem az értelmező rendelkezésekben tünteti fel, hanem külön cikkben utal rá, hogy mely személyes adatokat kell különleges védelemben részesíteni. A 9. cikk (1) bekezdésében kerül megállapításra, hogy különleges adat a személyes adatok különleges kategóriáiba tartozó minden adat, azaz:

- a faji, vagy etnikai származásra,
- politikai véleményre,
- vallási vagy világnézeti meggyőződésre vagy
- szakszervezeti tagságra utaló személyes adatok, valamint
- a genetikai adatok,
- a természetes személyek egyedi azonosítását célzó biometrikus adatok,
- az egészségügyi adatok és
- a természetes személyek szexuális életére vagy szexuális irányultságára vonakozó személyes adatok.

Ezen adatokat a jogalkotó azért részesíti a személyes adatok „általános” kategóriához képest erősebb védelemben, mert az alapvető jogokra és szabadságokra nézve kezelésük körülményei jelentős kockázattal járnak.[50] Főszabály szerint ezek kezelése tilos, azonban a Rendelet is állapít meg kivételeket és a tagállamok számára is megengedett külön rendelkezések meghozatala megfelelő garanciák mellett.

A Rendelet szerinti kivételek a következők:[51]

- Az érintett kifejezett hozzájárulását adta a személyes adatok egy vagy több konkrét célból történő kezeléséhez,
  - kivéve, ha az uniós vagy nemzeti jog úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával;
- Az adatkezelés az adatkezelőnek vagy az érintettnek:
  - foglalkoztatás,
  - szociális biztonság,
  - szociális védelmi jogszabályok területét érintő kötelezettségei teljesítése és konkrét joggyakorlása érdekében szükséges;
- Létfontosságú érdekek védelme cselekvőképtelenség esetén;

---

[50] GDPR (51) preambulumbekezdés.

[51] GDPR 9. cikk (2) bekezdés. A felsorolás nem szó szerinti idézet, a pontos listát lásd a Rendeletben. A különleges adatok kezelésére vonatkozó kivételeket az Infotv. 5.§ (2)-(8) bekezdése tartalmazza.

- Az adatkezelés valamely politikai, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik azzal rendszeres kapcsolatban állnak a szervezet céljaihoz és az adatok nem adhatók ki az érintettek hozzájárulása nélkül;
- Az adatkezelés olyan személyes adatokra vonatkozik, amelyet az érintett egyértelműen nyilvánosságra hozott;
- Az adatkezelés jogi igények:
  - előterjesztéséhez,
  - érvényesítéséhez, illetve
  - védelméhez szükséges, vagy
  - amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el.
- Jelentős közérdek;
- Az adatkezelés:
  - megelőző egészségügyi, vagy
  - munkahelyi egészségvédelmi célokból,
  - a munkavállaló munkavégzési képességének felmérésére,
  - orvosi diagnózis felállítása,
  - egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve
  - egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges,
  - uniós vagy nemzeti jogszabály alapján vagy egészségügyi szakemberrel kötött szerződés értelmében a (3) bekezdésben[52] említett feltételekre és biztosítékokra figyelemmel;
- A népegészségügy területét érintő közérdek;
- Az adatkezelés:
  - közérdekű archiválási célból,
  - tudományos kutatás,
  - történelmi kutatási, vagy
  - statisztikai célokból szükséges olyan uniós jogszabály vagy
  - nemzeti jogszabály alapján, amely
  - arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényegét, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

A tagállamok további feltételeket – például korlátozásokat – tarthatnak érvényben, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.[53]

Az Infotv. a GDPR-t megelőzően a különleges adat fogalmának meghatározásakor különleges adatként feltüntette a „bűnügyi személyes adat" kategóriát is. Az európai adatvédelmi reform következtében azonban e területet a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó 2016/680/EU irányelv[54] szabályozza. A Rendelet 10. cikke értelmében a tagállami jogalkotóknak a bűnügyi személyes adatok kezelésével összefüggésben „az érintett jogai és szabadságai tekintetében megfelelő garanciákat" kell biztosítania. A bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak a Rendelet 6. cikk (1) bekezdése alapján történő

[52] A különleges adatokat abban az esetben lehet ezekből a célokból kezelni, ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy nemzeti jogszabályban, illetve illetékes tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási (például gyógyszerészi titok, orvosi titok) kötelezettség hatálya alá tartozik, illetve olyan más személy által, aki szintén uniós vagy nemzeti jogszabályban, illetve illetékes tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alá esik.

[53] GDPR (53) preambulumbekezdés.

[54] Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L0680&from=HU

kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést uniós vagy tagállami jog lehetővé teszi.

Ezen kívül figyelembe kell venni az Infotv. 5. § (7) bekezdését, mely szerint bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.

8.1.1. A genetikai adatok és kezelésükre vonatkozó főbb szabályok

A GDPR 4. cikkének 13. pontja szerint genetikai adat „egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered". A (34) preambulumbekezdés további pontosítást tartalmaz, mely szerint a „genetikai adatot olyan, a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő személyes adatként kell meghatározni, és amely az érintett személytől vett biológiai minta elemzésének – különösen kromoszómaelemzésnek, illetve a dezoxiribonukleinsav (DNS) vagy a ribonukleinsav (RNS) vizsgálatának, vagy az ezekből nyerhető információkkal megegyező információk kinyerését lehetővé tevő bármilyen más elem vizsgálatának – az eredménye."

A GDPR egyik újdonsága, hogy a genetikai (és a biometrikus) adatok fogalmát külön határozta meg. A genetikai adatok különleges védelemben való részesítését az elmúlt évtizedek egyre gyorsabb tudományos fejlődése tette szükségessé. A genetikai kutatások újabb és újabb kérdéseket vetnek fel az adatok védelme területén is, maga a genetikai adat pedig a felhasználásban rejlő veszélyek miatt kell, hogy különleges védelemben részesüljön.[55]

Magyarországon az Eütv. már 1997-es hatályba lépésekor részletesen meghatározta az új eljárások, kutatási módszerek főbb szabályait. Ezt követően – az érintett terület fontosságára és a visszaélésekkel okozható károk miatt – megjelent a büntetőjogi védelem is. A jelenleg hatályban lévő Büntető törvénykönyv (2012. évi C. törvény) XVI. fejezete több keretdiszpozíciót tartalmaz az érintett területre vonatkozóan, többek között a következőket: „beavatkozás az emberi génállományba", „genetikailag megegyező emberi egyedek létrehozása".

Az orvosi genetika tudományának kialakulásával – amely „a genom veleszületett és szerzett rendellenességével foglalkozó orvosi tudomány"[56] – igény támadt nemzetközi szinten az emberi méltóság védelmének megerősítésére. Ennek kapcsán szükséges megemlíteni az 1997-ben Oviedoban elfogadott páneurópai Bioetikai Konvenciót (Egyezményt), valamint 1998-as első Kiegészítő Jegyzőkönyvét, amely megtiltja az emberi lények klónozását és, amelyet Magyarország a 2002. évi VI. törvénnyel ratifikált. Ehhez a témakörhöz tartozik még az Európai Unió Alapjogi Chartája,[57] amely tiltja a genetikai diszkriminációt.

A GDPR alkalmazását megelőzően hazánkban már egy 2008-as törvény meghatározta a genetikai adat fogalmát, a humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény (a továbbiakban: Hgtv.).

A genetikai mintákat és az ehhez kapcsolódó genetikai és személyazonosító adatokat az

---

55 Lásd: a NAIH közleménye a DNS-elemző szolgáltatások igénybevételének veszélyeiről http://naih.hu/files/2019-03-23-genetikai-adatok.pdf

56 Dr. Kosztolányi György: A genomika kölcsönhatásai a medicinával és az egyetemes tudománnyal (Magyar Tudomány 2002/5; 567.o.)

57 Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:12012P/TXT

úgynevezett biobankokban[58] lehet gyűjteni, tárolni.[59] A jogszabály által szabályozott eljárások[60] mindegyike során olyan adatok, információk birtokába jutnak az abban résztvevők, melyek védelme kiemelten fontos.

A Hgtv. 23.§-a alapján a genetikai minta, illetve adat tárolása során biztosítani kell a genetikai minta, illetve adat védelmét megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel, továbbá illetéktelen személy hozzáférésével szemben. A genetikai adatot kódolt formában lehet csak tárolni és a kódkulcshoz a 25.§-ban meghatározott „felelős személy" férhet hozzá. A felelős személynek orvostudományi vagy biológiatudományi, egyetemi szintű (vagy azzal egyenértékű) végzettséggel kell rendelkeznie és ezen a területen legalább két éves szakmai gyakorlata kell legyen.

A Hgtv. ugyanakkor más szempontból közelíti meg a genetikai adatok kezelését, mint a Rendelet. A Rendelet megközelítése szerint fokozottan védendő személyes adatról van szó és e védelem biztosítása céljából állapít meg rendelkezéseket, addig a Hgtv. középpontjában a humángenetikai kutatások „tárgyát" képező humángenetikai adatok védelme áll.

Jelenleg Magyarországon több biobank is működik, ahol genetikai mintákat (adatokat) tárolnak. Létezik olyan biobank, ahol önkéntes alapon kódolt, vagy anonim módon lehetséges mintát elhelyezni, melyeket beleegyezés alapján genetikai kutatásokra is fel lehet használni, és amelyek akár hazai, akár külföldi kutatók számára is továbbíthatóak. A genetikai adatok harmadik országba történő továbbításának szabályait a Hgtv. 28.§-a tartalmazza.

8.1.2. A biometrikus adat és kezelésükre vonatkozó főbb szabályok

A GDPR 4. cikkének 14. pontja szerint biometrikus adat „egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat".

Biometrikus adat lehet bármilyen biológiai jellegzetesség, pszichológiai sajátosság, életvitel vagy olyan ismétlődő tevékenység, amely során e jellegzetességek és/vagy tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek. Ilyen például az ujjlenyomat, íriszkép, hang, vagy akár az aláírás is. Biometrikus adat egyik jellegzetessége, hogy ezek egyaránt tekinthetők az adott egyénre vonatkozó információ tartalmának, valamint olyan elemnek, amely kapcsolatot teremt az adott információ és az egyén között, azaz azonosítóként működhetnek.[61]

A biometrikus adatok a GDPR-on kívül több más hazai jogszabályban is megjelennek. Ezek közül megemlítendő a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény (a továbbiakban: Bnytv.) és a sportról szóló 2004. évi I. törvény (a továbbiakban: Sporttv.).

A Bnytv. a bűnügyi személyes adatokat tartalmazó nyilvántartások rendszerének felépítését is

---

58 Biobank: genetikai mintát és az ehhez kapcsolódó genetikai és személyazonosító adatokat az e törvény szerinti humángenetikai vizsgálat, illetve humángenetikai kutatás céljából tartalmazó – jogszabályban meghatározott működési, illetve kutatási engedéllyel rendelkező – mintagyűjtemény, ide nem értve az egészségügyi ellátás vagy orvostudományi kutatás céljából levett, vagy valamilyen egészségügyi ellátás, beavatkozás során másodlagosan keletkezett biológiai sejt- és szövetmintákat, valamint e mintákhoz kapcsolódó személyazonosító és egyéb egészségügyi adatokat tartalmazó mintagyűjteményt

59 Hgtv. 3.§ 7. pont.

60 Humángenetikai vizsgálat, humángenetikai kutatás, klinikai genetikai vizsgálat, genetikai szűrővizsgálat, kutatási célú genetikai vizsgálat, genetikai tanácsadás.

61 WP 29 – 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről.

tartalmazza, amelyet ezen adatok különleges védelmére figyelemmel alakítottak ki.[62] A Bnytv. 35.§-a szerint a bűnügyi és rendészeti biometrikus adatok nyilvántartása két részből – a daktiloszkópiai nyilvántartásból és DNS-profil nyilvántartásból – áll. A nyilvántartásban szereplő adatok kezelésének, felhasználásának, tárolásának módjai, az adatok más országokba történő továbbításának lehetőségére vonatkozó szabályok a törvényből megismerhetőek.

A Sporttv. biometrikus adatként a képmást, az ujjnyomatot, az íriszképet vagy vénalenyomatot[63] nevesíti. Ezeket a biometrikus adatokat vissza nem fejthető alfanumerikus kódként – biometrikus sablonként – kezelhetik meghatározott esetekben a sportesemények szervezői.

A GDPR 9. cikke tartalmazza a biometrikus adatok kezelésére vonatkozó tilalmakat, melyek korábban a különleges adatokkal kapcsolatos részben kifejtésre kerültek.

8.2. Az egészségügyi adat fogalma és kezelésükre vonatkozó főbb szabályok

A GDPR 4. cikkének 15. pontja szerint egészségügyi adat „egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról".

Magyarországon az egészségügyi adatok kezelésére ágazati jogszabályok is tartalmaznak előírásokat, így az egészségügyről szóló 1997. évi CLIV. törvény (a továbbiakban: Eütv.), az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.) és az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről szóló 62/1997. (XII.21.) NM rendelet.

Az Eütv. és az Eüak. vonatkozásában is a GDPR fogalmi rendszerét kell alkalmazni. Az Eüak. 2019. április 26-i módosításával került ki az egészségügyi adat fogalma a törvényből, azonban ezzel összefüggésben felmerült az elhunyt személyek adatainak kezelésével kapcsolatos probléma.

Az egészségügyi adatokkal ugyanis szoros összefüggésben áll az egészségügyi dokumentáció fogalma, amelyet mind az Eütv,[64] mind az Eüak.[65] meghatároz. Ezért volt fontos, hogy a GDPR által bevezetett személyes adat fogalmán túl az egészségügyi jogviszonyokban az elhunyt személyek egészségügyi adatairól, azok sorsáról is rendelkezzenek, különös tekintettel az alábbiakban tárgyalt egészségügyi dokumentáció megismeréséhez való jogra.

Az egészségügyi dokumentáció egészségügyi és személyazonosító adatokat tartalmaz. E tekintetben személyazonosító adatnak minősül a beteg családi és utóneve, leánykori neve, születési helye TAJ száma stb. Az Eütv. részletesen tartalmazza a betegek, valamint az egészségügyi ellátó személyzet jogait és kötelezettségeit, melyek közül több az egészségügyi adatok megismerésére is tartalmaz szabályokat. Ezek közé tartozik például a kapcsolattartás joga (Eütv. 11.§), melynek keretein belül a beteg megtilthatja, hogy gyógykezelésének tényét vagy a gyógykezelésével kapcsolatos egyéb információt más előtt feltárják. Az egészségügyi dokumentáció megismerésének joga (Eütv. 24.§), valamint az orvosi titoktartáshoz való jog (Eütv. 26.§) biztosítja azt, hogy a beteg megismerhesse a rá vonatkozó egészségügyi dokumentáció tartalmát, másolatot kaphasson arról, illetve ezt az általa felhatalmazott személyek is megtehessék. E jog keretein belül van lehetőség arra – ami eltérés a

[62] A szabályozás átalakítását az Alkotmánybíróság 144/2008. (XI.26.) AB határozata tette szükségessé, amely megállapította, hogy a Bnyt. rendelkezései nem biztosították maradéktalanul a személyes adatok kezelése során a célhoz kötöttség elvének érvényesülését, a szükségesnél hosszabb ideig tárolták ezen adatokat, nem volt nyomon követhető, hogy ki, mikor és miért fért hozzájuk.

[63] Sporttv. 72/A.§.

[64] Eütv. 3.§ p).

[65] Eüak. 3.§ e).

GDPR személyes adatok kezelésére vonatkozó rendelkezéseihez képest –, hogy elhunyt személy esetén házastárs, egyeneságbeli rokon, testvér, élettárs, vagy törvényes képviselő is megismerhessen bizonyos adatokat. Ugyanakkor az orvosi titoktartáshoz való jog érvényesülése biztosítja, hogy a beteg dönthessen arról kinek adható róla információ és kinek nem, kivéve a jogszabályban meghatározott eseteket, amelyek ezeket a tilalmakat felülírhatják. Hozzájárulás hiányában is közölhető egészségügyi adat, ha ezt törvény elrendeli, ha mások életén, testi épségének és egészségének védelme szükségessé teszi, vagy amikor a beteg ápolását, gondozását végző személlyel szükséges közölni olyan információkat, amelyek ahhoz szükségesek, hogy a beteg egészségi állapota ne károsodjon.

Az egészségügyi dokumentációba többek között beletartoznak a beteg személyazonosító adatai, a kórelőzménye, kórtörténete, diagnózisok, vizsgálati eredmények, elvégzett beavatkozások, azok eredményei, a beteg testéből kivett szövetminták, a gyógyszer-túlérzékenységre vonatkozó adatok, és a bejegyzést tevő egészségügyi dolgozók nevei és a bejegyzések időpontja is.[66]

Az egészségügyi és személyazonosító adatok kezelésének célját az Eüak. 4.§-ból ismerhetjük meg. Ezek között megtalálható az egészség megőrzésének, javításának, fenntartásának előmozdítása mellett a népegészségügyi, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele is.

Az egészségügyi adatok hazai kezelésével kapcsolatban szükséges megemlíteni az Elektronikus Egészségügyi Szolgáltatási Térre (EESZT) vonatkozó szabályokat. A bevezetés előkészületei 2012-ben kezdődtek meg. A rendszer célja, hogy az egészségügyi adatok elektronikusan hozzáférhetőek legyenek mind a betegek, mind az egészségügyi ellátásban résztvevők (orvosok, gyógyszerészek) részére. A létrehozást európai uniós támogatás tette lehetővé,[67] a rendszer üzemeltetéséért az Állami Egészségügyi és Ellátó Központ felel.

A hozzáférők száma relatíve széles körűnek tekinthető, azonban az egyes szereplők csak korlátozott mértékben férhetnek hozzá és csak az őket érintő adatokhoz. A rendszer lényege tulajdonképpen az, hogy egy személy valamennyi, egészségügyi ellátásra vonatkozó adata egy adatbázisban megjelenjen és ehhez az ellátás típusától függően az egészségügyi dolgozók hozzáférhessenek.

A szabályokat az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016. (XII.21.) EMMI rendelet (EESZT rendelet) tartalmazza, amely az Eüak. rendelkezéseire épül. A rendelethez több megjelölt államigazgatási szerv köteles csatlakozni, amelyeknek biztosítania kell az adatok védelmét is.[68] A csatlakozás – és hozzáférés – lehetőségét az Eüak. alapján állapítják meg. A rendszer használatát a közfinanszírozott járó- és fekvőbeteg-ellátó intézmények, háziorvosok, gyógyszerészek kezdték meg, ma már lehetőség van segítségével eRecept kiváltására személyazonosság igazolásával és TAJ-kártya felmutatásával, vagy tárolóelemmel rendelkező e-személyi igazolvánnyal bizonyos helyeken. A rendszer továbbfejlesztése zajlik, ma már az Országos Mentőszolgálat és a magánegészségügyi szolgáltatók egy része is csatlakozott, de tervben van a korábban keletkezett betegadatok és dokumentumok feltöltése, illetve telemedicina szolgáltatások támogatása is.

66 A betegdokumentáció teljes tartalmát ld. Eütv. 136.§.

67 Lásd: https://e-egeszsegugy.gov.hu/eeszt

68 Például: EESZT rendelet 3.§ (2) bekezdés e), g) pont.

9. A PROFILALKOTÁS ÉS A GDPR

9.1. A profilalkotás fogalma és jelentősége

9.1.1. A profilalkotás fogalma

Az úgynevezett profilalkotás fogalmát a GDPR 4. cikk 4. pontja határozza meg, eszerint profilalkotásnak minősül a „*személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.*”

A profilalkotásnak tehát alapvetően három, konjunktív fogalmi eleme van:[69]

- a GDPR 4. cikk 1. pontja szerint személyes adatnak minősülő adatokon végzik (kizárólag érintettnek minősülő, tehát élő természetes személyes adatait felhasználva, hiszen az elhunyt személyekre vonatkozó adatok nem minősülnek személyes adatnak);
- a személyes adatok kezelésére automatizált formában kerül sor (ez azt jelenti, hogy az adatkezelésre elektronikus formában, tehát nem papír alapon kerül sor, az adatkezelésnek azonban nem kell teljes egészében emberi beavatkozástól függetlennek – automatizáltnak – lennie);
- a profilalkotási tevékenység célja valamely természetes személy személyes jellemzőinek értékelése (önmagában az érintettek valamely szempont szerint osztályozása, csoportosítása tehát nem profilalkotási tevékenység).

A fentieket összegezve, a profilalkotás információk gyűjtését jelenti egy adott érintettről (vagy érintettek egy csoportjáról), továbbá magában foglalja személyes jellemzőinek vagy viselkedésmintájának értékelést annak érdekében, hogy az értékelés eredményeképpen csoportba, illetőleg kategóriába sorolható legyen.

9.1.2. A profilalkotás jelentősége

A profilalkotás jelentősége első megközelítésben abban áll, hogy a valamely érintettre vonatkozó, akár önmagukban kevéssé releváns, pontosabban az érintett magánszféráját látszólag csekély mértékben érintő információk egymásra tekintettel történő értelmezésével olyan további információk nyerhetők,

---

[69] A 95/46 EK irányelv 29 cikke szerint létrehozott munkacsoport (a továbbiakban: Adatvédelmi Munkacsoport) által kibocsátott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, II.C pont, 8. o. (az angol nyelvű változatban).

melyek az érintett magánszférája, lehetőségei, személyes életútja jelentős mértékű befolyásolására, meghatározására alkalmasak. A GDPR (30) preambulumbekezdése szerint ugyanis a „*természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel. Ezáltal olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyes profiljának létrehozására és az adott személy azonosítására.*"

A profilalkotás jelentőségével kapcsolatban érdemes továbbá felhívni az figyelmet Európai Adatvédelmi Biztos (European Data Protection Supervisor) 3/2018. számú véleményére a profilalkotás jelentőségével kapcsolatban,[70] mely szerint a profilalkotás nem csupán az érintettek fogyasztási szokásai kapcsán releváns, hiszen a felhasználói profilok felhasználhatóak annak értékelésére, hogy az adott egyén valószínűsíthetően mely hírek iránt érdeklődik, milyen világnézetet képvisel stb., ezáltal befolyásolás lehetősége miatt fokozottan kiszolgáltatottá válik.[71]

A profilalkotás jelentősége a GDPR területi hatályára vonatkozó rendelkezései körében is megmutatkozik, a GDPR 3. cikk (2) bekezdés b) pontja szerint ugyanis a rendeletet „*kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek […] az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.*" A GDPR hivatkozott rendelkezéseit a gyakorlat nyelvére fordítva, akár egy, az Európai Unióban tevékenységi hellyel nem rendelkező adatkezelő, vagy adatfeldolgozó tevékenysége is a GDPR hatálya alá esik, abban a részben, amennyiben annak célja az érintettek EU-belül tanúsított viselkedésének megfigyelése, például a profilalkotási tevékenység érdekben.[72]

9.2. A profilalkotásra vonatkozó, a GDPR 5. cikke szerinti elvek[73]

A profilalkotási tevékenység és a GDPR 5. cikkében található elvek viszonyával kapcsolatban a GDPR (72) preambulumbekezdése kimondja, hogy a profilalkotást is a GDPR-nak a személyes adatok kezelésére vonatkozó rendelkezései szabályozzák, például az adatkezelés jogalapja (GDPR 6. cikk) és az adatkezelési elvek (GDPR 5. cikk) tekintetében.

A fentiek alapján tehát elmondható, hogy az adatkezelés valamennyi, a GDPR 5. cikkében meghatározott elve változatlan tartalommal vonatkozik a profilalkotással összefüggésben végzett adatkezelésekre is. A célhoz kötöttség elvével kapcsolatban azonban külön is megjegyzendő, hogy a profilalkotási tevékenység különösen magában hordozza annak veszélyét, hogy a személyes adatokat az eredeti céltól eltérő célra használják fel. Annak megítélése során, hogy az új adatkezelési tevékenység célját tekintve összeegyeztethető-e azzal a céllal, melyből az adatok gyűjtésére eredetileg sor került, a GDPR 6. (4) bekezdésében – valamint a GDPR (50) preambulumbekezdésében – meghatározott szempontokat kell figyelembe venni, az általános szabályok szerint. Különös figyelmet kell tovább fordítni a gyermekek mint adatalanyok tekintetében végzett profilalkotási tevékenységgel kapcsolatos adatkezelésekre.[74]

---

70 EDPS Opinion on online manipulation and personal data, 8-9. o.

71 Összegzően ld.: EDPS Opinion on online manipulation and personal data, 22. o.

72 Magyarázatképpen ld. még a GDPR (24) preambulumbekezdését.

73 A profilalkotással összefüggő adatkezelés és az adatkezelés általános elvei viszonyáról részletesen lásd az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, III.A. pontját, 9-12. o. (az angol nyelvű változatban).

74 GDPR (38) preambulumbekezdés.

9.3. A profilalkotás és jogalapok

9.3.1. A jogalapok „általános" esetei[75]

Profilalkotással járó adatkezelési tevékenységre azon személyes adatok tekintetében, amelyek nem tartoznak a személyes adatok GDPR 9. cikk (1) bekezdésében meghatározott különleges kategóriáiba, elvileg bármely, a GDPR 6. cikkében meghatározott jogalapra hivatkozással sor kerülhet. A GDPR 6. cikk (1) bekezdésében meghatározott jogalapok közül az érintett hozzájárulását, a szerződés teljesítését, valamint az adatkezelő vagy harmadik fél jogos érdekét mint jogalapot emeljük ki.

a) Hozzájárulás

A fentiek értelmében nincs akadálya annak, hogy a profilalkotáshoz kapcsolódó adatkezelési tevékenységre az érintett hozzájárulására mint jogalapra hivatkozással kerüljön sor; az érvényes hozzájárulás feltételeit a GDPR alkalmazása körében a 95/46 EK irányelv 29. cikke szerint létrehozott munkacsoport (a továbbiakban: Adatvédelmi Munkacsoport) által kidolgozott, és a Testület által annak első plenáris ülésén jóváhagyott – tehát a GDPR alkalmazása körében is hivatkozható – WP 259 rev.01 számú, Guidelines on Consent under Regulation 2016/679 című dokumentuma[76] határozza meg.

Lényeges azonban már itt felhívni a figyelmet arra, hogy csak az érintett kifejezett hozzájárulása fogadható el adatkezelési jogalapként abban az esetben, ha az érintettre nézve joghatással járó döntés, vagy őt hasonlóképpen jelentős mértékben érintő döntés kizárólag automatizált adatkezelésen alapul (részletesen lásd az 1.3.2. pontot), vagy ha az ilyen döntés a személyes adatok különleges kategóriáiba tartozó adatokra vonatkozik (lásd az 1.3.3. pontot).

b) Az adatkezelés szerződés teljesítéséhez (megkötéséhez) szükséges

A jelen alpontban hivatkozott jogalapra történő hivatkozás csak és kizárólag abban az esetben fogadató el érvényesnek, amennyiben magának a szerződésnek a teljesítéséhez szükséges a profilalkotási tevékenység, illetőleg az azzal járó adatkezelés, annak hiányában tehát a szerződés teljesítése nem lehetséges, vagy amennyiben az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. A szükségesség kritériumát azonban szűken kell értelmezni, mint azt már az Adatvédelmi Munkacsoport WP 217-es számú, a jogos érdekről szóló véleményében is kifejtette.[77]

c) A profilalkotás az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges

Önmagában az adatkezelő/harmadik fél profilalkotáshoz fűződő érdeke természetesen nem teszi az ilyen adatkezelést jogszerűvé, ehhez az is szükséges, hogy az adatkezelésre megfelelő érdekmérlegelési teszt elvégzését követően kerüljön sor, és az érdekmérlegelési teszt eredményével az adatkezelés indokolható. Akkor jogszerű tehát a jogos érdekre alapított profilalkotási tevékenységgel együtt járó adatkezelés, amennyiben az érdekmérlegelési teszt alapján az adatkezelő/harmadik fél érdekei megelőzik az érintett érdekeit vagy alapvető szabadságait.[78]

---

75 Részletesen ld. az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, III.A. pontját, 12-15. o. (az angol nyelvű változatban).

76 Adatvédelmi Munkacsoport: Guidelines on Consent under Regulation 2016/679 című iránymutatása.

77 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directice 95/46 EC European Commission.

78 Részletesebben ld. az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, III.B.6 pontját, 14. o. (az angol nyelvű változatban).

9.3.2. Jogalapok, amennyiben a profilalkotásra kizárólag automatizált adatkezeléssel került sor, és a döntés az érintettre joghatással jár, vagy őt egyébként jelentős mértékben érinti

A GDPR 22. cikk (1) bekezdése szerint „*[A]z érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené”*. Lényeges, hogy ez a tilalom nem csak akkor kötelezi tartózkodásra az adatkezelőt (adatfeldolgozót), ha arra az érintett kifejezetten hivatkozik, hanem attól függetlenül is kötelező erővel érvényesülő szabály.[79]

A fenti tilalom azonban csak akkor érvényesül, ha az adatkezelésre teljes mértékben automatizált, egyedi döntéshozatallal kapcsolatban kerül sor (ideértve a profilalkotás, de akár más, automatizált döntéssel járó adatkezelést), egyáltalán nincs tehát érdemi, az eredményt érdemben befolyásoló emberi közreműködés a folyamatban, erre utal a „kizárólag” kifejezés a GDPR 22. cikk (1) bekezdésében. Mindebből az is következik, hogy nem vonja ki a tilalom hatálya alól az adatkezelési tevékenységet az, ha az emberi beavatkozás/közreműködés jellegénél fogva olyan, hogy a döntés tartalmára nem lehet döntő behatással, tehát ha nincs lehetőség a döntés emberi megfontoláson alapuló érdemi megváltoztatására.[80]

A GDPR 22. cikk (1) bekezdésében foglalt tilalom érvényesülésével kapcsolatos másik fontos előfeltétel, hogy a kizárólag automatizált döntésnek az érintettre joghatással kell bírnia, vagy az érintettet egyébként jelentés mértékben kell érintenie.[81]

A GDPR 22. cikk (1) bekezdésében megfogalmazott általános tilalom alóli kivételeket a GDPR 22. cikk (2) bekezdése határozza meg, mely alapján az (1) bekezdésben foglalt tilalom sem alkalmazandó abban az esetben, ha a döntés:

a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges; vagy
b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
c) az érintett kifejezett hozzájárulásán alapul.

Az a) és c) pont alatt hivatkozott kivételszabályokkal kapcsolatban fontos hangsúlyozni, hogy az érintett jogait ekkor is megfelelő garanciákkal kell biztosítani az adatkezelőnek, a GDPR 22. cikk (3) bekezdése szerint ugyanis a GDPR 22. cikk (2) bekezdés a) és c) pontjában említett esetekben az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

---

79 Az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, IV. rész,19. o. (az angol nyelvű változatban). A 22. cikk szerinti adatkezelés szabályairól részletesen ld. ugyanezen iránymutatás IV. részét.

80 Az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, IV.A. pont,21. o. (az angol nyelvű változatban).

81 Ezen feltételek elemzésével kapcsolatban részletesen ld. Az Adatvédelmi Munkacsoport már hivatkozott Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, IV.B. pont,21-22. o. (az angol nyelvű változatban).

9.3.3. Jogalapok a személyes adatok különleges kategóriáinak esetében

A személyes adatok GDPR 9. cikk (1) bekezdése szerinti, különleges kategóriáiba tartozó kezeléséről általánosságban elmondható, hogy arra jogszerűen csak akkor kerülhet sor, ha teljesül legalább egy, a GDPR 6. cikke szerinti, a jogszerűséget megalapozó feltétel, továbbá teljesül legalább egy, a GDPR 9. cikk (2) bekezdésében meghatározott feltétel. Ez a főszabály általánosságban elmondható a személyes adatok GDPR 9. cikk (1) bekezdése szerinti, különleges kategóriákba tartozó adatoknak profilalkotás céljából történő kezelésével kapcsolatban is.[82]

Abban az esetben azonban, ha a profilalkotási célú adatkezelést további, a GDPR 22. cikk (1) pontjában meghatározott speciális ismérvek jellemzik (kizárólag automatizált döntéshozatal, joghatás kiváltása az érintettre/az érintettet joghatás kiváltásához hasonlóan jelentős mértékben érintő döntés), már a GDPR 22. cikk (4) bekezdése szerinti korlátozásokat is figyelembe kell venni. Ez utóbbi bekezdés szerint a GDPR 22. cikk (2) bekezdésben említett döntések [kivételek a GDPR 22. cikk (1) bekezdésében foglalt tilalom alól] nem alapulhatnak a személyes adatoknak a GDPR 9. cikk (1) bekezdésében említett különleges kategóriáin, kivéve, ha a 9. cikk (2) bekezdésének a) pontja [az érintett kifejezett hozzájárulását adta] vagy g) pontja [az adatkezelés jelentős közérdek miatt szükséges uniós vagy tagállami jog alapján] alkalmazandó, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

9.4. Az érintettek jogai a profilalkotással kapcsolatban

A személyes adatok profilalkotással összefüggő kezelése vonatkozásában az érintetteket megilleti valamennyi, a GDPR III. fejezetében meghatározott általános érintetti jogosultság, azzal, hogy a tájékoztatáshoz, valamint a hozzáféréshez való jog kapcsán bizonyos többletjogosultságok is az adatalanyok rendelkezésére állnak.

A tájékoztatáshoz való jog[83] vonatkozásában mind a GDPR 13. (2) bekezdés f) pontja, mind a 14. cikk (2) bekezdés g) pontja előírja ugyanis, hogy az adatkezelőnek tájékoztatást kell adnia az érintett számára a GDPR 22. cikke (1) és (4) bekezdésében említett automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Indokolt kifejezetten felhívni a figyelmet arra is, hogy a GDPR 15. cikk (1) bekezdés h) pontja szerint[84] az érintett hozzáférési joga keretében jogosult hozzáférést is kapni a GDPR 13. (2) bekezdés f) pontja, mind a 14. cikk (2) bekezdés g) pontja szerinti információkhoz.

Megemlítendő még, hogy a tiltakozáshoz fűződő, GDPR 21. cikke szerinti joghoz a GDPR (70) preambulumbekezdés külön értelmező rendelkezéseket fűz.

---

82 Guidelines on individual decision-making and Profiling for the purposes of Regulation 2016/679, III.C. pont, 15. o. (az angol nyelvű változatban).

83 Lásd még (60) preambulumbekezdés: „[…] Az érintettet továbbá a profilalkotás tényéről és annak következményeiről tájékoztatni kell. […]".

84 Ld. még GDPR (63) preambulumbekezdés.

9.5. A profilalkotással kapcsolatos további lényeges rendelkezések

9.5.1. Adatvédelmi tisztviselő kinevezése

A GDPR adatvédelmi tisztviselőre vonatkozó rendelkezései alapján adatvédelmi tisztviselő kinevezése profilalkotási célú adatkezelési tevékenységek esetén indokolt, a GDPR 37. cikk (1) bekezdés b) alapján ugyanis az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé.[85]

A GDPR sem a fogalommeghatározások körében nem határozza meg, pontosan hogyan kell értelmezni az adatalanyok rendszeres és szisztematikus megfigyelése kifejezést, a (24) preambulumbekezdés[86] azonban említi az érintettek magatartásának megfigyelését. Ez utóbbi fogalom a preambulumbekezdés szövege alapján magánban foglalja az interneten történő nyomon követést, valamint a profilalkotási tevékenységet, továbbá – az Adatvédelmi Munkacsoport WP 243 rev.01 számú, az adatvédelmi tisztviselőről szóló iránymutatása alapján – az érintett (megfigyelt) magatartására alapított hirdetési tevékenységet is.[87]

Az Adatvédelmi Munkacsoport adatvédelmi tisztviselőkről szóló iránymutatása a „*rendszeres és szisztematikus megfigyelés*" fogalmán túl segítséget nyújt a „*fő tevékenység*", valamint a „*nagymértékű*" kifejezések értelezéséhez is.[88]

9.5.2. Adatvédelmi hatásvizsgálat

A GDPR 35. cikk (3) bekezdés a) pontja alapján a GDPR 35. cikk (1) bekezdésében említett adatvédelmi hatásvizsgálatot különösen abban az esetben kell elvégezni, ha az adatkezelés az adatkezelési tevékenység természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelésével jár, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek.[89]

Az Adatvédelmi Munkacsoport iránymutatást bocsátott ki az előzetes hatásvizsgálat elvégzésével kapcsolatban, mely iránymutatás egy kilenc elemű – nem taxatív – listán határozza meg azon szempontokat, melyeket indokolt figyelembe venni annak eldöntése során, hogy szükséges-e az

---

85 Az Adatvédelmi Munkacsoport Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01) című iránymutatása, 2.1.4. pont.

86 „GDPR (24) [ ] Annak meghatározása, hogy az adatkezelés az érintettek magatartásának megfigyelésének minősül-e, meg kell megvizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezt követően a természetes személy profiljának megalkotását is magában foglaló adatkezelési technikákat alkalmaznak-e, annak érdekében, hogy elsősorban a természetes személyre vonatkozó döntéseket hozzanak, valamint, hogy elemezzék vagy előre jelezzék a természetes személy személyes preferenciáit, magatartását vagy beállítottságát."

87 WP 243 rev.01, 8. o. (az angol nyelvű változatban).

88 WP 243 rev.01 2.1.2-2.1.3. pontjai.

89 A GDPR 35. cikk (3) bekezdés a) pontjának értelmezéséhez segítséget nyújt még a (91) preambulumbekezdés, mely szerint „*Adatvédelmi hatásvizsgálatot kell végezni továbbá, amikor az a személyes adatkezelés célja, hogy konkrét természetes személyekkel kapcsolatban döntést lehessen hozni azt követően, hogy elvégzik a természetes személyek személyes jellemzőinek szisztematikus és kiterjedt értékelését az említett adatokon alapuló profilalkotás alapján, illetve a személyes adatok különleges kategóriáira, a biometrikus adatokra vagy a büntetőjogi felelősség megállapítására és a bűncselekményekre vagy a kapcsolódó biztonsági intézkedésekre vonatkozó adatok kezelését követően.*"

adott adatkezelési tevékenységgel kapcsolatban adatvédelmi hatásvizsgálatot végezni, avagy sem.[90] E kilenc elemű lista első pontjában szerepel az adatalany munkahelyi tevékenységére, egészségügyi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságára vagy magatartására vonatkozó szempontok értékelése, ideértve a profilalkotást is.

A fenti hivatkozott iránymutatás hangsúlyozza ugyanakkor, hogy minden adatkezelést egyedileg kell értékelni, mivel a legtöbb esetben legalább kettő, az adatvédelmi hatásvizsgálat indokoltsága mellett szóló kritérium teljesülése teremti meg a hatásvizsgálat elvégzésének szükségességét, előfordulhat azonban, hogy már egyetlen elem teljesülése esetén is el kell végezni a vizsgálatot.[91]

1. példa – a profilalkotás fogalma

Profilalkotásnak minősül, ha valamely webáruház a regisztrált felhasználók korábbi megrendelései, és a róluk rendelkezésre álló egyéb adatok (például nem; életkor; lakóhely: város, vidék; vásárlások összege) alapján felhasználói profilt készít, és annak egyéb alapján állítja össze az adott, felhasználóként regisztrált személynek küldendő, marketing célú hírlevél tartalmát.

2. példa – a hozzájárulásban kifejezettől eltérő célú adatkezelés profilalkotás céljából

Egy online könyvkereskedés felületén regisztrált felhasználói hozzájárulásukat adhatják ahhoz, hogy számukra a webáruház hírlevelet küldjön, abból a célból, hogy ezáltal értesülhessenek a webáruház legújabb, kedvezményes termékeiről. Ha azonban a webáruház üzemeltetője a felhasználók adatait arra a célra is fel akarja használni, hogy a felhasználók regisztráció, illetve s későbbi rendelések során leadott személyes adatait felhasználva, egyéni profilt készítve a jövőben személyre szabott ajánlatokkal kereshesse meg őket, az újabb adatkezelés esetében az érintett hozzájárulása csak akkor hívható fel jogalapként, ha teljesülnek a GDPR 6. cikk (4) bekezdése szerinti kritériumok.

3. példa – a GDPR 6. cikk (1) bekezdés b) pontja szerinti jogalap (az adatkezelés szerződés megkötéséhez, vagy szerződés teljesítéséhez szükséges) és profilalkotás

A GDPR 6. cikk (1) bekezdés b) pontja nem hivatkozható érvényes adatkezelési jogalapként, ha a profilalkotásra arra hivatkozással kerül sor, hogy az:

- a szerződés megkötésére vonatkozó szolgáltatói döntéshozatal folyamatának felgyorsítását segíti elő; vagy
- kiszűri a szolgáltató szerződéskötésre vonatkozó döntéshozatalban részt vevő munkatársainak esetleges részrehajlását; vagy
- a segít kiszűrni a szolgáltatóval szerződő természetes személyek közül azokat, akiknek a fizetőképessége anyagi helyzetük miatt nagyobb kockázatot hordoz.

[90] Az Adatvédelmi Munkacsoport Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) című iránymutatása, III.B. a) pont.

[91] Az Adatvédelmi Munkacsoport Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) című iránymutatása, 9. o. (az angol nyelvű változatban.)

10. JOGSZABÁLYTÁR

1. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) [a továbbiakban: GDPR; Rendelet]
2. Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
3. Az Emberi Jogok Egyetemes Nyilatkozata Elérhetőség: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=hng (2018 november 23.)
4. Magyarország Alaptörvénye (2011. április 25.)
5. 2013. évi V. törvény a Polgári Törvénykönyvről
6. 2012. évi C. törvény a Büntető Törvénykönyvről
7. 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.)
8. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
9. 1997. évi CLIV. törvény az egészségügyről (Eütv.)
10. 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről (Eüak.)
11. 2008. évi XXI. törvény a humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól (Hgtv.)
12. 2002. évi VI. törvény az Európa Tanácsnak az emberi lény emberi jogainak és méltóságának a biológia és az orvostudomány alkalmazására tekintettel történő védelméről szóló, Oviedóban, 1997. április 4-én kelt Egyezménye: Az emberi jogokról és a biomedicináról szóló Egyezmény, valamint az Egyezménynek az emberi lény klónozásának tilalmáról szóló, Párizsban, 1998. január 12-én kelt Kiegészítő Jegyzőkönyve kihirdetéséről
13. 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról (Bnytv.)
14. 2004. évi I. törvény a sportról (Sporttv.)
15. Az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016. (XII.21.) EMMI rendelet
16. 34/1999. (IX.24.) BM-EüM-IM együttes rendelet az egészségügyről szóló 1997. évi CLIV. törvénynek a halottakkal kapcsolatos rendelkezései végrehajtásáról, valamint a rendkívüli halál esetén követendő eljárásról
17. 76/2004. (VIII.19.) ESzCsM rendelet az egyes személyazonosításra alkalmatlan ágazati (egész-

ségügyi, szakmai) adatok körének meghatározására, gyűjtésére, feldolgozására vonatkozó részletes szabályokról

18. 11/1987. EüM rendelet az orvosbiológiai kutatásokról
19. 18/1998. (XII. 27.) EüM rendelet az egészségügyről szóló 1997. évi CLIV. törvénynek a szerv- és szövetátültetésre, valamint –tárolásra és egyes kórszövettani vizsgálatokra vonatkozó rendelkezései végrehajtásáról
20. 4/2000. (II.25.) EüM rendelet a háziorvosi, házi gyermekorvosi és fogorvosi tevékenységről
21. 23/2002. (V.9.) EüM rendelet az emberen végzett orvostudományi kutatásokról
22. 24/2002. (V.9) EüM rendelet az emberi felhasználásra kerülő vizsgálati készítmények klinikai vizsgálatáról és a helyes klinikai gyakorlat alkalmazásáról
23. 62/1997. (XII.21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
24. 30/1998. (VI.24.) NM rendelet az emberi reprodukcióra irányuló különleges eljárások végzésére vonatkozó, valamint az ivarsejtekkel és embriókkal való rendelkezésre és azok fagyasztva tárolására vonatkozó részletes szabályokról
25. 62/1997. (XII.21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
26. 33/1998. (VI.24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről
27. 5/1998. (V.31.) SZEM rendelet a szerzett immunhiányos tünetcsoport terjedésének meggátlása érdekében szükséges intézkedésekről és a szűrővizsgálat elrendeléséről

11. FOGALOMTÁR

Biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

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.

Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.[92]

[92] GDPR 4. cikk 4. pont.

12. MELLÉKLETEK

12.1. Eltérő fogalomhasználat katalógusa

Az Infotv. 3. §-a az Infotv. 2. § (2) bekezdése alapján[93] eltérő, kiegészítő rendelkezéseket határoz meg a következő fogalmakkal kapcsolatban:

- a különleges adat (Infotv. 3. § 3. pont);
- bűnügyi személyes adat (Infotv. 3. § 4. pont);
- közérdekből nyilvános adat (Infotv. 3. § 6. pont);
- adattovábbítás (Infotv. 3. § 11. pont);
- nyilvánosságra hozatal (Infotv. 3. § 12. pont);
- adattörlés; (Infotv. 3. § 13. pont)
- adatmegsemmisítés (Infotv. 3. § 16. pont);
- adatfeldolgozás (Infotv. 3. § 17. pont);
- adatállomány (Infotv. 3. § 21. pont);
- EGT-állam (Infotv. 3. § 23. pont);
- harmadik ország (Infotv. 3. § 24. pont).

---

[93] Infotv. 2. § (2) Személyes adatoknak az (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) hatálya alá tartozó kezelésére az általános adatvédelmi rendeletet a III-V. és a VI/A. Fejezetben, valamint a 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23-24. pontjában, a 4. § (5) bekezdésében, az 5. § (3)-(5), (7) és (8) bekezdésében, a 13. § (2) bekezdésében, a 23. §-ban, a 25. §-ban, a 25/G. § (3), (4) és (6) bekezdésében, a 25/H. § (2) bekezdésében, a 25/M. § (2) bekezdésében, a 25/N. §-ban, az 51/A. § (1) bekezdésében, az 52-54. §-ban, az 55. § (1) és (2) bekezdésében, az 56-60. §-ban, a 60/A. § (1)-(3) és (6) bekezdésében, a 61. § (1) bekezdés a) és c) pontjában, a 61. § (2) és (3) bekezdésében, (4) bekezdés b) pontjában és (6)-(10) bekezdésében, a 62-71. §-ban, a 72. §-ban, a 75. § (1)-(5) bekezdésében és az 1. mellékletben meghatározott kiegészítésekkel kell alkalmazni.

12.2. Az Infotv. és a GDPR jogalkotó által értelmezett szakkifejezéseinek összehasonlító táblázata

Infotv. 3. §		GDPR 4. cikk	
1. érintett	Bármely információ alapján azonosított vagy azonosítható természetes személy	**1. érintett**	Azonosított vagy azonosítható természetes személy (A személyes adat fogalommeghatározása tartalmazza)
2. személyes adat	Az érintettre vonatkozó bármely információ	**1. 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
3. különleges adat	A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint 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 (Az 5. § (7) bekezdése szerint bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni)	**a személyes adatok különleges kategóriái**	A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos. [GDPR 9. cikk (1) bekezdés]
3a. genetikai adat	Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered	**13. genetikai adat**	Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered
3b. biometrikus adat	Egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat	**14. biometrikus adat**	Egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat

3c. egészségügyi adat	Egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról	**15. egészségügyi adat**	Egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról
4. bűnügyi személyes adat	A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat		
6. közérdekből nyilvános adat	A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli		
7. hozzájárulás	Az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez	**11. az érintett hozzájárulása**	Az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez
9. adatkezelő	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja	**7. adatkezelő**	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan 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
9a. közös adatkezelő	Az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval	**közös adatkezelők**	Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. (GDPR 26. cikk)
10. adatkezelés	Az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése	**2. 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

10a. bűnüldözési célú adatkezelés	A jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése		
10b. nemzetbiztonsági célú adatkezelés	A nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése		
10c. honvédelmi célú adatkezelés	A honvédségi adatkezelésről szóló törvény és a Magyarország területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyarország területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról szóló törvény hatálya alá tartozó adatkezelés		
11. adattovábbítás	Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele		
11a. közvetett adattovábbítás	Személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása		
11b. nemzetközi szervezet	A nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre	**26. nemzetközi szervezet**	A nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre
12. nyilvánosságra hozatal	Az adat bárki számára történő hozzáférhetővé tétele		
13. adattörlés	Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges		
15. adatkezelés korlátozása	A tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján	**3. az adatkezelés korlátozása**	A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából

16. adatmegsemmisítés	Az adatot tartalmazó adathordozó teljes fizikai megsemmisítése		
17. adatfeldolgozás	Az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége		
18. adatfeldolgozó	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel	**8. adatfeldolgozó**	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel
21. adatállomány	Az egy nyilvántartásban kezelt adatok összessége		
22. harmadik személy	Olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek	**10. harmadik fél**	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak
23. EGT-állam	Az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez		
24. harmadik ország	Minden olyan állam, amely nem EGT-állam		
26. adatvédelmi incidens	Az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi	**12. adatvédelmi incidens**	A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi
27. profilalkotás	Személyes adat bármely olyan – automatizált módon történő – kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul	**4. profilalkotás**	Személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják

28. címzett	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz	**9. címzett**	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak
29. álnevesítés	Személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni	**5. álnevesítés**	A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni
		6. nyilvántartási rendszer	A személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető
		16. tevékenységi központ	a) Az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni; b) Az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;
		17. képviselő	Az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában

		18. vállalkozás	Gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is
		19. vállalkozáscsoport	Az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások
		20. kötelező erejű vállalati szabályok	A személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ
		23. személyes adatok határokon átnyúló adatkezelése”	a) Személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy b) Személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

13. IRODALOMJEGYZÉK

15/1991. (IV.13.) AB határozat. Elérhetőség: http://public.mkab.hu/dev/dontesek.nsf/0/1CE263A376458F27C1258382003C412C?OpenDocument (utolsó letöltés: 2018. augusztus 15.)

35/2002. (VII. 19.) AB határozat. Elérhetőség: http://epa.oszk.hu/02300/02334/00011/pdf/EPA02334_Fundamentum_2002_03-04_147-149.pdf (utolsó letöltés: 2018. augusztus 15.)

Adatvédelem és információszabadság a mindennapokban; szerkesztő: Péterfalvi Attila (2012) HVG-ORAC Lap- és Könyvkiadó Kft.

Article 29 Data Protection Working Party (2017): Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01. Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (utolsó letöltés: 2018. szeptember 10.)

Article 29 Data Protection Working Party (2017): Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01. Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (utolsó letöltés: 2018. augusztus 15.)

Article 29 Data Protection Working Party (2017): Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01). Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (utolsó letöltés: 2018. augusztus 15.)

Article 29 Data Protection Working Party (2017): Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (utolsó letöltés: 2018. augusztus 15.)

Article 29 Data Protection Working Party (2017): Lead supervisory authority Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01. Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235 (utolsó letöltés: 2018. augusztus 15.)

Article 29 Data Protection Working Party (2018): Guidelines individual decision-making and Profiling for the purposes of Regulation 679/2016 (WP251rev.01). Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (utolsó letöltés: 2018. augusztus 15.)

Awareness of, and preparation for, General Data Protection Regulation (GDPR) in SMEs – Amárach Research URL: http://gdprandyou.ie/wp-content/uploads/2017/05/GDPR-in-SMEs_Final.pdf (utolsó letöltés: 2018. augusztus 15.)

BBC – Human embryos edited to stop disease – BBC. Elérhetőség: http://www.bbc.com/news/health-40802147 (utolsó letöltés: 2018. augusztus 15.)

BBC – Iceland's DNA: The world's most precious genes? – BBC, Emma Jane Kirby, 2014. június 19. Elérhetőség: http://www.bbc.com/news/magazine-27903831 (utolsó letöltés: 2018. augusztus 15.)

Beck'scher Online Kommentar Datenschutzrecht, 18th edn. C.H. Beck, Munich. Elérhetőség: https://beck-online.beck.de/?vpath=bibdata\komm\BeckOKDatenS_16\cont\BECKOKDATENS.INHALTSVERZEICHNIS.htm (utolsó letöltés: 2018. augusztus 15.)

Biobanks in the United States: How to identify an undefined and rapidly evolving population – US National Library of Medicine National Institutes of Health (2012. december 10.). Elérhetőség: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4076972 (utolsó letöltés: 2018. augusztus 15.)

Ábrahám Dominika, Dr. –Ujfaludi Zoltán, Dr. – Kiss Attila, Dr. (2015): Belső adatvédelem. Elérhetőség: https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/belso-adatvedelem-tananyag.original.pdf (utolsó letöltés: 2018. augusztus 15.)

Dósa Ágnes, Dr. – Hanti Péter, Dr. – Kovácsy Zsombor, Dr. (2016): Kommentár az egészségügyi törvényhez – Wolters Kluwer Kft., Budapest.

Tömösi Éva Ramóna, Dr. (2017): Egészségügyi adatok védelme, különös tekintettel a genetikai adatokra – ELTE ÁJTK JOTOKI Szakdolgozat.

Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) – EESZT Információs portál. Elérhetőség: https://e-egeszsegugy.gov.hu/eeszt (utolsó letöltés: 2018. augusztus 15.)

Európai Bizottság – Mit nevezünk személyes adatnak? Elérhetőség: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hu (utolsó letöltés: 2018. augusztus 15.)

Hanti Péter (2013): Kommentár az egészségügyi adatvédelmi törvényhez – Wolters Kluwer Kft., Budapest.

Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation – Brussels, 24 May 2018. Elérhetőség: http://europa.eu/rapid/press-release_STATEMENT-18-3889_hu.htm (utolsó letöltés: 2018. július 28.)

A 29. cikk alapján létrehozott adatvédelmi munkacsoport 4/2007 vélemény a személyes adat fogalmáról. Elérhetőség: https://docplayer.hu/203328-A-29-cikk-alapjan-letrehozott-adatvedelmi-munkacsoport-4-2007-velemeny-a-szemelyes-adat-fogalmarol.html (utolsó letöltés: 2018. augusztus 15.)

A 29. cikk alapján létrehozott adatvédelmi munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről. Elérhetőség: http://docplayer.hu/12558130-3-2012-sz-velemeny-a-biometrikus-technologiak-teren-tortent-fejlemenyekrol.html (utolsó letöltés: 2018. augusztus 15.)

3/2018 EDPS Opinion on online manilpulation and personal data. Elérhetőség: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf (utolsó letöltés: 2018. augusztus 15.)

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-085-8

A hatályosított kiadvány
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„**A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése**” című projekt
keretében készült el és jelent meg.