TANULMÁNYOK

Az Európai Unió általános adatvédelmi rendelete, a GDPR

1. rész: Alapfogalmak, alapelvek

TÓSZEGI Zsuzsanna

Jogod van mindenhez, jogod
Illyés Gyula[1]

Az informatikai infrastruktúra nagymértékben meghatározza az adatkezelők és adatfeldolgozók cselekvési szabadságát és lehetőségeit. Ez a felismerés egyáltalán nem új, mint ahogy az sem, hogy a technológia fejlődésével együtt kell járnia a privát szféra védelmének. A műszaki-technológiai – és azon belül kiemelten is az infokommunikációs – fejlődés jelentős társadalmi változásokat idéz elő, amelyekre a jogi szabályozásnak reagálnia kell. Az adatvédelemben és más jogterületeken egyre másra jelentek meg a technológiai megoldások, amelyek közvetlen szabályozó szerepet töltenek be. Az 1990-es évek derekán dolgozták ki a magánszférát erősítő technikai és szervezeti megoldásokat (Privacy Enhancing Technologies – PET), amelyek célja, hogy ne csak az adatokat, de az érintetteket is védjék és segítsék őket információs önrendelkezési joguk gyakorlásában.[2]
Kétrészes cikkünk első részében az EU általános adatvédelmi rendeletének legfontosabb szabályait ismertetjük, a Könyvtári Figyelő következő számában megjelenő második részben pedig a nyilvános könyvtári ellátás szempontjából legfontosabb kérdésekre térünk ki.

A magánélet védelmétől az információs önrendelkezési jogig – az adatvédelem kialakulása

A világ nagy jogrendszereiben elterjedt kifejezés az adatvédelem (*Datenschutz, data protection* stb.) – holott a fogalom meglehetősen pontatlan, hiszen nem az adat, hanem a személyes adatokkal bíró ember védelmét jelenti. A magyar jogi szakirodalomban az adatvédelemben részesülő személyre vonatkozóan az 'adatalany' kifejezés honosodott meg, az adatok védelmét jelentő tevékenységekre inkább az adatbiztonság kifejezést használják.
Majtényi László véleménye szerint nem kis nehézséget okoz azonban „a megis-

merő és a szorongatott személyiség", az individuum fogalmának tisztázása. A jog „a létezők világából a személyiségről tud" a legkevesebbet.[3] *Sólyom László* úgy véli, a 'személyiség' fogalma helyett inkább a személyiségi jogból mint jogi kategóriából érdemes kiindulni: a személyiségi jogok ugyanis „az ember jogállásának alapvető kifejezői közé tartoznak." Az emberről alkotott kép egy adott társadalommodell része, amely megszabja a személyiségi jogok viszonyát az alapvető jogintézményekhez, köztük például az alkotmányos szabadságjogokhoz vagy a tulajdonhoz.[4]

A modern jogrendszer fontos részét képező általános személyiségi jog és a nevesített személyiségi jogok jogintézményének polgári jogi, illetve büntetőjogi eredete a római jog világáig nyúlik vissza. Történetileg először a magánszféra védelme alakult ki – a fogalomkörbe a személyes adatok, az egyéni autonómia, a döntési szabadság, a testi önrendelkezés és a személyiségvédelem stb. aspektusai tartoznak. Alkotmányosan védett jogként a magánszféra védelmének megfogalmazását *Samuel Warren* és *Louis Brandeis* nevéhez kötik – ők a szerzői annak az 1890-ben publikált tudományos közleménynek, amely megalapozta a magánélethez való jog egyesült államokbeli pályafutását.[5]

A magánszféra védelmébe a következőket értik bele:

- a háborítatlan magán- és családi élet, a becsület és a jó hírnév, valamint a személyes identitás oltalmát;
- a fizikai és lelki integritás biztosítását;
- mentességet a magánélet tényeinek feltárásától és a megfigyeléstől;
- a levelezés és a szóbeli közlések védelmét.[6]

Az információs jogok kialakulása és fejlődése részben a jogi szabályozáshoz, részben a jogi normák társadalmi, kulturális beágyazottságához kötődik; e két aspektus szoros összefüggésben van egymással. Szabályai nélkül nem érthető meg az emberi társadalom működése – és egy adott történelmi korszak érvényes (jogi) normái sem értelmezhetők a társadalmi háttér nélkül.[7]

A XIX. század végén kialakult „magánszférához való jog" egy évszázad alatt általános szabadságjoggá vált, amely az állami hatalommal és a szervezeti túlerővel, illetve az új technológiából adódó veszélyekkel szemben védi az emberi méltóságot és függetlenséget. A személyes adatok védelméhez való jog a XX. század második felében kibővült az információkhoz való hozzájutás szabadságjogával. Sólyom László gyakran idézett megfogalmazásában: „Az információszabadság nem politikai jelszó, hanem szakkifejezés […] azoknak a jogintézményeknek az összefoglaló neve", amelyek a vélemény- és sajtószabadság, illetve a polgárok „informált részvételének" biztosítása érdekében nyilvánossá teszik az államapparátus információit.[8]

Az információszabadság és az adatvédelem a XX. század végén vált egységes rendszerré. Az információs önrendelkezési jog a sajtó- és véleményszabadságból származó információszabadsággal együtt a kommunikációs alapjogok közé tartozik. Magyarország hatályos Alaptörvénye kimondja: „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez."[9]

Az európai adatvédelem korszakai

Majtényi László a következő adatvédelem korszakokat különbözteti meg Európában: az első generációs szabályok az 1970-es években jelentek meg, amikor felismerték a számítógépes nyilvántartásokban rejlő, a polgárok magánszférájára leselkedő veszélyt. Az 1980-as, '90-es években megjelenő második generációs törvények már nem az adatrögzítés technikájára koncentráltak: az adatvédelem szempontjából egyformán ítélték meg az automatizált és a papíralapú nyilvántartásokat. A harmadik generációs jogalkotás az európai integráció sajátosságait tükrözi, miközben fölerősödtek a technológiai fejlődésből, különösen az internet terjedéséből eredő kihívások – mindez előre vetítette „az új médiumra szabott, a nemzeti keretek felett álló" szabályok létrehozását.[10]

Jóri András az európai adatvédelem történetét szintén három korszakra osztja: az első szakasz „az adatvédelmi szabályok megjelenésétől az információs önrendelkezési jog kifejtését adó 1983-as német alkotmánybírósági határozatig", a második pedig „az információs önrendelkezési jog doktrínájának megfogalmazásától" a harmadik etap elejéig tartott. Jóri a harmadik korszak kezdetét az „új adatvédelem" szabályainak megjelenéséhez köti: a korszakhatárt a távszolgáltatók személyesadat-kezelését korlátozó 1997-es német törvény, a *Teledienstedatenschutzgesetz* jelenti.[11]

Mindkét jogtudós külön fejezetet szentelt a német alkotmánybírák „népszámlálás-ítéletként" elhíresült döntésének, amely az egész világon az adatvédelmi jog fordulópontjává vált.

A *Német Szövetségi Alkotmánybíróság* 1983. decem-

ber 15-én kelt, a népszámlálási törvényről hozott határozatában kimondta: „Az alapjog biztosítja az egyénnek azt a jogát, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról." A német alkotmánybírák szerint ez a jog csakis „túlnyomó közérdekből, az arányosság követelményét szem előtt tartva korlátozható", de ekkor is biztosítani kell a személyiségi jogok védelmét. Jogi dokumentumban ekkor fogalmazták meg először az információs önrendelkezési jog mibenlétét.[12]

Az ügy előzménye az 1983-as népszámlálási törvény, amely a foglalkoztatási, munkahelyi, illetve az épület- és lakásstatisztikai adatokra is kiterjedt. A törvény alapján a felvett adatokat össze lehetett kapcsolni a lakcímnyilvántartással. A bíróság nemcsak az egyének önrendelkezési jogára, de a demokratikus társadalomra nézve is veszélyesnek ítélte, ha olyan helyzet alakulhatna ki, „amelyben a polgár nem tudhatja, hogy ki, mit, mikor és milyen alkalomból tud róla." A döntés leszögezi: a törvénynek azon szakaszai, amelyek lehetővé tették (volna) a felvett adatok statisztikai és igazgatási célú összekapcsolását, alkotmányellenesek.[13]

E perdöntő ítélet a német polgároknak köszönhető. A népszámlálási törvény ellen számos csoport polgári engedetlenségre, a népszámlálás bojkottálására szólított fel. Néhányan – szám szerint huszonhatan – nem elégedtek meg a bojkottal: ők az alkotmánybírósághoz fordultak. A testület megvizsgálta a beadványt és érdemi döntést hozott az ügyben.[14]

A német alkotmánybíróság az általános személyiségi jogból levezetve megfogalmazta az információs önrendelkezési jogot, vagyis az egyén „illetékességét arra, hogy alapvetően mikor és milyen mértékben fedi fel személyes életének tényállásait". Természetesen az információs önrendelkezési jog nem korlátlan, de a korlátozás csak „kényszerítő közérdekből" történhet, és a korlátozást úgy kell megfogalmazni, hogy a polgár képes legyen megérteni annak célját és feltételeit.[15]

A népszámlálás-ítélet hosszú időre meghatározta az adatvédelem alakulását – és nemcsak Németországban, de számos európai országban. Hazánkban az 1983-as döntés szellemében született meg „a magyar adatvédelmi jog ősforrása," a 15/1991. (IV. 13.) AB határozat, amely közvetett módon mindmáig érezteti hatását.[16]

Az információs jogok rövid történeti fejlődése Magyarországon

Az alábbiakban dióhéjban áttekintjük az információs jogok terén bekövetkezett magyarországi fejleményeket.

Az Alkotmánybíróság messze ható jelentőségű 15/1991. határozata nemcsak azt állapította meg, hogy „a korlátozás nélkül használható, általános és egységes személyazonosító jel (személyi szám) alkotmányellenes", hanem azt is, hogy „személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása alkotmányellenes".[17]

A határozat indoklásában olyan részletességgel fejtették ki a személyes adatok védelméhez való alkotmányos jog értelmezését, „hogy az megfelel egy alkotmányos adatvédelmi törvény vázlatának is." Az Alkotmánybíróság a személyes adatok védelméhez való jogot információs önrendelkezési jogként értelmezte, megfogalmazta a célhoz kötöttség elvét, az ebből adódó főszabályokat, továbbá meghatározta az adattovábbítás és a nyilvánosságra hozatal fő garanciáit.[18]

Az első meghatározó jelentőségű jogi aktus *a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény* (Avtv.) parlamenti elfogadása volt. A jogszabály létrehozta a hatósági jogkörrel felruházott *adatvédelmi ombudsman*i intézményt. Később, az Európai Unióhoz való csatlakozás során végzett jogharmonizáció következtében az adatvédelmi biztost bizonyos közigazgatási hatósági jogkörökkel is felruházták.

Az eleinte bevezetett fogalmak: a 'személyes adatok védelme' és a 'közérdekű adatok nyilvánossága' az idők során kibővültek: az 1990-es évek elejétől a 2010-es évtized elejéig terjedő időszakban az első kifejezést az 'információs önrendelkezési jog', a másodikat az 'információszabadság' váltotta föl – a két terület 'információs jogok' összefoglaló néven ment át a köztudatba.

2011 áprilisában – az akkor elfogadott Alaptörvény *Szabadság és felelősség* fejezet VI. cikk (3) bekezdése úgy rendelkezett, hogy a személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog érvényesülését egy e célra létrehozott, független hatóság fogja ellenőrizni. Az *Országgyűlés* még ugyanabban az évben elfogadta *az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt* (Infotv.). A törvényi előírások alapján megalapították a *Nemzeti Adatvé-*

*delmi és Információszabadság Hatóság*ot (NAIH), és egyúttal megszüntették az adatvédelmi biztos intézményét.[19]

Az Európai Unió adatvédelmi intézkedései

Az infokommunikációs eszközök robbanásszerű terjedése az EU döntéshozóit arra késztette, hogy szabályozási szinten foglalkozzanak az online térben zajló, az emberek mind nagyobb hányadát érintő folyamatokkal, és hathatósan lépjenek föl a természetes személyek adatai védelme érdekében. Az uniós adatvédelmi jog fejlődésének egyik jelentős mérföldköve, az 1995-ben kihirdetett ún. adatvédelmi irányelv[20] elsődleges célja még nem az alapjogok védelmének erősítése, hanem a belső piacok működését segítő intézkedések deklarálása volt, de hozzájárult az egyének magánszférájának magasabb védelmi szintjéhez.[21]

A Bizottság 2012 elején tette közzé az adatvédelmi rendeletjavaslatot, amelynek szövegét négyéves vita és egyeztetés után fogadták el *A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet* címen.[22]

A GDPR néven ismertté vált jogszabály (General Data Protection Regulation – az Európai Unió általános adatvédelmi rendelete) 2016. május 24-én lépett hatályba, rendelkezéseit 2018. május 25. napjától kell az Európai Unióban – egész pontosan az Európai Gazdasági Térség (EGT) országaiban[23] – kötelezően és közvetlenül alkalmazni.

Mint ismeretes, az Európai Unió jogrendjében a legfelsőbb szintű, kötelező jogalkotási aktus a rendelet, amely az EU egész területén teljes egészében alkalmazandó.[24]

Az adatvédelmi szabályozási folyamat a GDPR bevezetése óta is folytatódik: 2018. december 11-én lépett hatályba *A természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet* és az *1247/2002/EK határozat hatályon kívül helyezéséről szóló 2018. október 23-i 2018/1725/EU európai parlamenti és tanácsi rendelet*, az *'EUI-GDPR'*. Az összes uniós intézmény, szerv, hivatal és ügynökség személyesadat-kezelési tevékenységére vonatkozó jogszabály jelentős előrelépés az egységes európai adatvédelmi szabályozás terén, mivel az EU intézményeinek adatvédelmi tevékenységét hozza összhangba a GDPR szabályaival.[25]

Az EU általános adatvédelmi rendelete, a GDPR

A Rendelet legfőbb célja, hogy az Európai Unióban egységes jogalkalmazás alakuljon ki a természetes személyeket megillető alapvető jog, a személyes adataik védelme terén. A GDPR szabályai a természetes személyekre vonatkoznak – akkor is, ha az adatok kezelése nem az Unió területén zajlik, de az EU területén tartózkodó polgár személyes adataira vonatkozik.[26] Ki kell azonban emelni, hogy a személyes adatok védelme nem abszolút jog.

Olvassuk el figyelmesen a Rendelet (4) preambulumbekezdését!

GDPR Preambulum (4)

A személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal.

Ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen ami a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához és a tájékozódás szabadságához, a vállalkozás szabadságához, a hatékony jogorvoslathoz és a tisztességes eljáráshoz, és a kulturális, vallási és nyelvi sokféleséghez való jogot illeti.

A GDPR hatálya

Egy jogszabály hatályossága a jogi norma *alkalmazhatóságát,* illetve *alkalmazandóságát jelenti.* „A hatályos jogszabály alapján *adott időben*, *adott területen* és *adott személyekre nézve jogviszonyok keletkezhetnek*, *módosulhatnak* vagy *szűnhetnek meg*."[27] Emellett gyakran meghatározzák a jogszabályok tárgyi hatályát.

Akire a GDPR érvényes: a Rendelet személyi hatálya

A GDPR hatálya nemcsak az EU tagországok állampolgáraira, illetve az Unióban lakóhellyel rendelkező személyekre, hanem az EU területén tartózkodó valamennyi természetes személyre is kiterjed.

A GDPR személyi hatálya minden azonosított vagy azonosítható természetes személyre kiterjed, de a személyes adataik védelméhez fűződő jog csak az „élő természetes személyeket illeti meg. Ennek alapja, hogy az ember jogképessége a halállal megszűnik, mivel a személyiségi jogok alanya csak jogképes személy lehet. […] A személyhez fűződő jogok esetében jogutódlásra nincs lehetőség."[28]

A Rendelet preambulumának 27. bekezdése lehetővé teszi az EU tagállamok számára, hogy a saját jogi szabályozásuk keretei között rendelkezzenek az elhunyt személyek személyes adatainak kezeléséről. A magyar jogalkotó élt ezzel a lehetőséggel, és az Infotv. 25. §-ában szabályozta e kérdéseket. Röviden összefoglalva: az érintett még életében tehet a személyes adatainak a halálát követő sorsáról rendelkező jognyilatkozatot, amelyben átruházhatja a hozzáférésre, a helyesbítésre, a törlésre, a zárolásra és a tiltakozásra vonatkozó jogait.[29]

A korábbi adatvédelmi biztos, Jóri András és munkatársai *A GDPR magyarázata* c. könyvükben hoszszan ismertetik *az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvénynek* (Eüatv.), mint egy szektorális adatvédelmi törvénynek az elhunyt személyek adatkezelésére vonatkozó rendelkezéseit. Az Eüatv. 7. § (5) bekezdése szabályozza, hogy az érintett életében, illetve a halála után ki gyakorolhatja a törvényben meghatározott adatkörökben az érintett számára biztosított jogokat. Természetesen attól, hogy rájuk nézve a GDPR hatálya megszűnik, az elhunyt személyeket – a *Polgári Törvénykönyv*ben elismert módon – megilleti az ún. kegyeleti jog [Ptk. 2:50. §].[30]

A Rendelet személyi hatálya nem terjed ki a jogi személyekre, illetve a jogi személyként létrehozott vállalkozásokra, tehát a személyes adatok védelme nem vonatkozik a cégnév, a székhely stb. adatokra. A NAIH állásfoglalása szerint az egyéni vállalkozók is ebbe a körbe tartoznak: „Az egyéni vállalkozó esetében nem jön létre új, önálló jogalany, a »gazdálkodó szervezet« valójában maga az egyéni vállalkozóként működő természetes személy. […] El kell tehát különíteni a természetes személy személyes adatát az egyéni vállalkozó gazdasági tevékenységi köréhez kötődő adatától, ez utóbbit a GDPR nem részesíti védelemben."[31] Jóri András és szerzőtársai kifejtik, miért nem értenek egyet ezzel az állásponttal, és azt tanácsolják az adatkezelőknek, az egyéni vállalkozók személyes adatait tekintsék a GDPR hatálya alá tartozóknak.[32]

Amire a GDPR érvényes: a Rendelet tárgyi hatálya

A (26) preambulumbekezdés a következőképpen rendelkezik: „Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell."

GDPR 2. cikk
Tárgyi hatály

(1) E rendeletet kell alkalmazni 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 2. cikk (1) bekezdése alapján a Rendelet tárgyi hatálya nem vonatkozik a nem strukturált módon kezelt, nem gépesített, manuális módon kezelt adatállományok kezelése.

A tagállami nemzeti jogban azonban kiterjesztő értelmezésben is meg lehet határozni a tárgyi hatályt – a magyar jogalkotó élt ezzel a lehetőséggel. Az Infotv. 2. § (4) bekezdése alapján Magyarországon

az Infotv. hatálya alá tartozó, manuálisan kezelt, nem strukturált adatállományokra is vonatkoznak az adatvédelmi szabályok.[33]

A tárgyi hatály alól kivételt képeznek a magáncélú adatkezelések, amennyiben az adatkezelést „természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik". [GDPR 2. cikk (2) c) bekezdés] Nagyon fontos korlátozás azonban, hogy a kivétel nem vonatkozik azokra az esetekre, ha a magánszemély bármilyen módon nyilvánosságra hozza egy vagy több másik érintett személyes adatát/adatait – például, ha egy közösségi oldalon közzéteszi valakinek akár a képmását, akár a nevét vagy bármi más, az érintett azonosítására alkalmas személyes adatát.

A GDPR tárgyi hatálya nem vonatkozik sem az uniós jog hatályán kívül eső tevékenységekre, sem azokra, amelyeket a „ tagállamok az EUSZ V. címe 2. fejezetének hatálya alá tartozó tevékenységek[34] során végzik" és azokra sem, amelyeket „az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését." [GDPR 2. cikk (2) a), b), d) bekezdés]

Összefoglalva a kivételeket: a GDPR tárgyi hatálya nem terjed ki

- a kizárólag magáncélú, nyilvánosságra nem hozott,
- a nemzetbiztonsági és a közös kül- és biztonságpolitikával kapcsolatos,
- a bűnüldözési célú és
- az uniós jog hatályán kívüli

adatkezelésekre.

Ahol a GDPR érvényes: a Rendelet területi hatálya

GDPR 3. cikk
Területi hatály

(1) E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.

(2) E 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:
   a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
   b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó.

(3) E rendeletet kell alkalmazni a személyes adatoknak a nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.

Összefoglalva: a Rendelet területi hatálya kiterjed az Európai Unióban tevékenységi hellyel rendelkező („bejegyzett") adatkezelőkre és -feldolgozókra, akár az EU-ban, akár azon kívül történik az adatkezelés. „Irreleváns a kezelt személyes adatok érintettjeinek állampolgársága is: a Rendelet akár abban az esetben is alkalmazandó tehát, ha az Unióban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó az Unión kívül végzi harmadik országbeli állampolgárok adatainak kezelését vagy feldolgozását."[35]

A GDPR magyarázata c. kötet kitér a Rendelet egyik nagyjelentőségű vonatkozására, az extraterritoriális hatályára, amelynek értelmében a szabályok azokra az adatkezelőkre és adatfeldolgozókra is vonatkoznak, amelyek az Unióban nem rendelkeznek tevékenységi hellyel, de adatkezelésük az EU területén tartózkodó, és nem is feltétlenül uniós tagország állampolgárságával bíró érintettek személyes adataira vonatkozik.[36]

Hatósági felügyelet

A GDPR alkalmazásában a nemzeti adatvédelmi hatóságok játszanak elsődleges szerepet. Feladatuk a személyesadat-kezelés során a természetes személyek jogainak és szabadságainak védelme, melynek során szoros együttműködésben felügyelniük kell az Unión belüli szabad adatáramlást.

Az Európai Adatvédelmi Testület

A GDPR 68. cikke rendelkezik a jogi személyiséggel rendelkező uniós szerv, az *Európai Adatvédelmi Testület* létrehozásáról, melynek tagjai az európai adatvédelmi biztos és a tagállamok által kijelölt egy-egy felügyeleti hatóság vezetője. A Testület feladata a Rendelet egységes és helyes alkalmazásának biztosítása, ellenőrzése, iránymutatások, ajánlások kibocsátása, az adatvédelmi jogszabályokra és gyakorlatokra vonatkozó ismeretek és dokumentáció cseréje, nyilvánosan hozzáférhető elektronikus nyilvántartás vezetése az egységességi mechanizmus keretében kezelt ügyekkel kapcsolatban a felügyeleti hatóságok és a bíróságok által hozott határozatokról stb. A Testület feladatait a GDPR 70. cikke tartalmazza.

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

A NAIH jogállását az Infotv. 38. § határozza meg, mely szerint a hatóság autonóm államigazgatási szerv, feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése, továbbá a személyes adatok Európai Unión belüli szabad áramlásának elősegítése.
A GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében a NAIH gyakorolja.
A NAIH független, csak a törvénynek van alárendelve, feladatkörében nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el, számára feladatot csak törvény állapíthat meg.

A GDPR legfontosabb alapfogalmai

A továbbiak megértéséhez meg kell állnunk az alapfogalmaknál – itt azokat ismertetjük, amelyek nélkül nem lehet értelmezni a Rendelet által meghatározott szabályokat.

Az érintett

Érdekes módon a Rendelet fogalommeghatározásai között nincs külön definiálva, kit kell érintettnek tekinteni – ezt csak a személyes adat fogalmából lehet levezetni: az 'érintett' az azonosított vagy azonosítható természetes személy.
A GDPR személyi hatályáról szóló fejezetben már volt szó arról, hogy a Rendelet csak az élő természetes személyekre vonatkozik, az elhunyt személyekre nem, továbbá arról, hogy Magyarországon az Infotv. és az Eüatv. alapján miként lehet érvényesíteni az elhunyt személyek adataihoz kapcsolódó bizonyos adatvédelmi jogokat.
Fontos ismételten tudatosítani, csak a természetes személyek tartoznak a GDPR hatálya alá, a jogi személyek (vállalkozások, szervezetek stb.) nem.

A személyes adat

GDPR 4. cikk

Fogalommeghatározások

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.

A GDPR alkalmazása során az adatkezelés jogszerűségének megállapítása szempontjából a legelső és legfontosabb a személyes adatok körének pontos behatárolása, amely alapvető fontosságú egyrészt a vonatkozó adatvédelmi követelmények meghatározása, másrészt a személyes adatok kezelése kapcsán fennálló adatkezelői, illetve adatfeldolgozói felelősség megállapítása szempontjából.[37] A személyes adat fogalmának egyértelmű meghatározása alapján lehet elbírálni, egy adott adatkezelési cselekményre érvényesek-e az adatvédelmi jogok, illetve vonatkozik-e rá a Rendelet hatálya.[38]
A jogi szakirodalom hosszan időz a Rendeletnek a 'személyes adat' definíciója élén álló 'azonosított vagy azonosítható' fordulat értelmezésével – a részletektől eltekintve, a pontos megértés kedvéért egy

idézetet citálunk: „Javasoljuk azt a meghatározást, amely szerint valaki azonosítható, ha elég információ áll rendelkezésre, hogy elkülönült létezésének, egyénként való létének tényét tükrözze, és akkor válik azonosítottá, ha elég információ áll rendelkezésre a vele történő kapcsolatfelvételhez vagy a másoktól való, valamilyen módon történő megkülönböztetéséhez, felismeréséhez."[39]

Itt nincs hely és lehetőség még csak példálózva sem felsorolni a személyes adatok összességét az ún. természetes személyazonosító adatoktól kezdve a családi állapotra, a vagyoni helyzetre vonatkozó adatokon át a képmásig és a hangfelvételig – a GDPR kommentárokban ezek megtalálhatók. A későbbi témánk szempontjából fontos két megállapításra hívjuk fel a figyelmet: a személyes adatok közé sorolandók „a természetes személy által olvasott művek, a természetes személy olvasási szokásai" – amint azt az adatvédelmi biztos 1998. évi beszámolójában megállapította.[40]

A második szempont, amely alapvető változás a korábbi évek, évtizedek váltakozó megítélése után: a GDPR egyértelműen érvel amellett, hogy az online azonosítók is a személyes adatok körébe tartoznak.

GDPR Preambulum (30)

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 személyek profiljának létrehozására és az adott személy azonosítására.

Külön kell szólni a GDPR által az ún. különleges kategóriába tartozó – régebben 'érzékeny' vagy 'szenzitív' jelzővel illetett, az Infotv. által 'különleges adat'-nak nevezett – személyes adatok speciális köréről, amelyek kezeléséről a 9. cikk szól.

GDPR 9. cikk

A személyes adatok különleges kategóriáinak kezelése

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.

Természetesen időről időre szükség van, illetve lehet a különleges kategóriájú adatok kezelésére – az adatkezelést lehetővé és/vagy szükségessé tevő eseteket a 9. cikk (2) bekezdés a) – j) pontjai tartalmazzák. Néhány jellemző példa arra, mikor van lehetőség, illetőleg szükség különleges adatok kezelésére:

- ha ahhoz az érintett kifejezett hozzájárulását adta;
- az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében elengedhetetlen;
- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez kell;
- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik;
- az adatkezelésre jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez van szükség;
- az adatkezelést jelentős közérdek érvényesítése indokolja;

és végül a j) pont teljes terjedelmében idézve:

GDPR 9. cikk
A személyes adatok különleges kategóriáinak kezelése

(2) Az (1) bekezdés nem alkalmazandó abban az esetben, ha:
j) az adatkezelés a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

A közgyűjteményi terület számára rendkívül fontos szabályra cikkünk második részében visszatérünk.
A GDPR nem nevesíti, de a vonatkozó magyar jogszabály, az Infotv. fontos rendelkezéseket tartalmaz a közérdekből nyilvános személyes adatok vonatkozásában. „A közérdekből nyilvános személyes adatok a magánszféra és a közszféra érzékeny határvonalán sorakoznak fel, megismerhetőségük biztosításakor ügyelni kell arra, hogy egyrészről a közszféra átláthatóságának az adatvédelem ne képezze indokolatlanul a gátját, másrészről viszont az egyén magánszférájában ne váljon kiszolgáltatottá."[41]
Lezárva ezt a fejezetet, röviden megemlítjük, hogy a büntetőjogi felelősség megállapításával, illetve a bűncselekményekkel összefüggő személyes adatok kezelése „csak közhatalmi szerv által végzett adatkezelés keretében történhet." [GDPR 10. cikk]

Az adatkezelés

GDPR 4. cikk
Fogalommeghatározások

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.

Az adatkezelés fogalmának lényege a meghatározás első része: minden olyan művelet adatkezelésnek minősül, amely személyes adattal, vagyis – visszautalva az előző meghatározáshoz –, amely azonosított vagy azonosítható természetes személyre vonatkozó adattal történik, a „bármely művelet vagy műveletek összessége" szövegrész pedig azt a jogalkotói szándékot tükrözi, hogy a Rendelet a személyes adatokkal végzett összes műveletet a hatálya alá vonja.
A definícióhoz tartozó felsorolás példálózó jellegű, csak a leggyakoribb eseteket tartalmazza. A meghatározásból egyenesen következik, hogy a GDPR nem vonatkozik az anonim adatok kezelésére –, amint azt a 26. preambulumbekezdés megfogalmazza.
Más szabály érvényes az utólag álnevesített adatra, amelyről a 28. és 29. preambulumbekezdés rendelkezik: az álnevesítés csökkentheti az érintettek számára a kockázatokat, és egyúttal segítheti az adatkezelőket és adatfeldolgozókat az adatvédelmi kötelezettségeknek való megfelelésben.

A napi gyakorlat szempontjából kiemelkedő jelentőségű a 32. preambulumbekezdés, amely külön magyarázatra sem szorul:

GDPR Preambulum (32)
az adatkezelési hozzájárulásról

Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.

Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. Ha az érintett hozzájárulását elektronikus felkérést követően adja meg, a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik.

Az adatkezelő

GDPR 4. cikk
Fogalommeghatározások
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.

A definíció legfontosabb eleme, hogy az adatkezelő önállóan határozza meg az adatkezelés célját és eszközeit, vagyis az adatkezelő az adatkezelést irányító, azért felelős jogalany, amely felelősségre vonható az e tevékenysége körében okozott esetleges kárért.
Az esetek többségében azt, hogy egy szervezet vagy egy természetes személy adatkezelő-e, a tevékenységi kör határozza meg – az adatkezelői minőséghez nem szükséges, hogy az adatkezelés folyamatában ténylegesen részt vegyen, döntéseket hozzon, vagy tevőlegesen kezelje a személyes adatokat: a definíció csak annyit mond, hogy az adatkezelés célját és eszközeit kell önállóan meghatároznia.
Előfordul, hogy egy szervezet – például egy könyvtár vagy egy felsőoktatási intézmény – számára jogi norma írja elő az adatkezelést; ez esetben a jogszabály értelmezéséből derül ki, hogy mely szervezet minősül adatkezelőnek.
Fontos leszögezni: az adatkezelő szervezet munkavállalói nem adatkezelők – a GDPR szerint ők a „személyes adatok kezelésére feljogosított személyek”, akik végrehajtják az adatkezelési tevékenységet; az adatkezelés jogszerűségéért a szervezet felelős.[42]
Tekintsük át, melyek az adatkezelésre vonatkozó érdemi döntések:

– az adatkezelési cél meghatározása (miért van szükség adatkezelésre?);
– a kezelt személyes adatok körének kijelölése (milyen adatokra terjed ki az adatkezelés?);
– az adatkezelés jogalapja (az adott adatkezelés(ek)re a GDPR melyik jogalapja vonatkozik?);
– az adatkezelés időtartama (az adatkezelő mennyi ideig őrzi a személyes adatokat?);
– a személyesadat-kezelés módja (az adatkezelő milyen módon, milyen eszközzel gyűjti az adatokat? papíron vagy elektronikusan? űrlapon vagy checkbox bejelölésével? beléptetőkapuval vagy kamerával? stb., stb.);
– hozzáférés a személyes adatokhoz (kik, milyen jogosultsággal férhetnek hozzá az adatok kategóriájához, illetve az egyes személyes adatokhoz?);
– döntés az adattovábbításról (közlik-e az adatokat hatósággal, egyéb szervvel vagy például továbbítják-e harmadik harmadik országba vagy nemzetközi szervezet részére az adatokat?);
– az érintettek jogainak biztosítása (hogyan gondoskodik erről az adatkezelő?);
– adatfeldolgozó igénybevétele (az adatkezelő megbízásából kezeli az adatokat más személy vagy szervezet – például honlapszolgáltató, informatikai rendszer üzemeltető?);

– adatbiztonsági intézkedések (az adatkezelő hogyan teremti meg a személyes adatok biztonságának feltételeit?).[43]

A GDPR fogalommeghatározásában szerepel arra vonatkozó utalás, hogy az adatkezelő „másokkal együtt" is meghatározhatja az adatkezelés céljait és eszközeit: ez esetben közös adatkezelőkről beszélünk. Az ő számukra a Rendelet kötelezően előírja a megállapodást a GDPR-ban meghatározott kötelezettségek teljesítésének módjáról. [GDPR 26. cikk]

Az adatfeldolgozó

GDPR 4. cikk
Fogalommeghatározások
8. „adatfeldolgozó"

az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

A Rendelet definíciójából következik, hogy az adatfeldolgozó nem azonos az adatkezelővel – ez utóbbi határozza meg az adatkezelés célját és eszközeit, az adatfeldolgozó pedig az adatkezelő felelősségi körébe tartozó személyes adatokkal adatkezelési műveleteket hajt végre.

A GDPR 28. cikke foglalkozik részletesen az adatfeldolgozókra vonatkozó szabályokkal, melyek közül a legfontosabbak: [44]

– Kizárólag a Rendelet követelményeinek megfelelő, az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására képes adatfeldolgozókat lehet igénybe venni.
– Az adatfeldolgozó által végzett adatkezelést szerződésnek vagy más jogi aktusnak kell szabályoznia.
– Az adatfeldolgozó az adatkezelő előzetes felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

A nyilvántartási rendszer

A Rendelet megfogalmazásában a nyilvántartási rendszer a „személyes adatok bármely módon – centralizált, decentralizált, vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető". [GDPR 4. cikk 6. pont]

A nyilvántartási rendszer fogalmának két kulcseleme a tagolt (strukturált) adatkezelési mód, illetve a kereshetőség, amelynek főként a GDPR tárgyi hatályánál van szerepe – ugyanis a Rendelet nem terjed ki azokra a nem automatizált módon történő adatkezelésekre, amelyek nem képezik nyilvántartási rendszer részét. (Mielőtt azonban a papíralapú nyilvántartások „gazdái" örömüket fejeznék ki afölött, hogy az így tárolt személyes adatokra nem vonatkozik a GDPR, hadd hívjuk föl a figyelmet, hogy ez esetben fölmerül az a kérdés, milyen jogcímen tárolja az adatkezelő a szóban forgó adatokat. Ha az adatkezelő nem tudja igazolni az adatkezelés célját és jogalapját, az adatkezelés jogellenesnek minősül.)[45]

A GDPR tárgyi hatályánál felhívtuk a figyelmet az Infotv. 2. § (4) bekezdésére, melynek alapján a törvény hatálya a papíralapú nyilvántartásokra is vonatkozik.

Álnevesítés

A személyazonosság elrejtésére szolgáló, hatékony módszer az álnevesítés (pszeudonimizálás), melynek során a természetes személy és a róla kezelt adatok csak egy külön kezelt adatállomány segítségével feleltethetők meg egymásnak. A tényleges adatkezelés az álnevesített adatokkal zajlik.

Az álnevesítést gyakran alkalmazzák például a statisztikai felmérésekben. Az eljárás lényege, hogy a természetes személy és a róla gyűjtött adatok egy külön tárolt azonosító segítségével kapcsolhatók össze, az adatkezelésbe csak a kódokkal jelölt adatokat vonják be. A névtelenített adatok kezelésére vonatkozóan az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell hoznia: például meg kell jelölnie azokat a feljogosított személyeket, akik az érintettek és a róluk gyűjtött adatok közötti kapcsolatot megteremtő azonosítókhoz (kódokhoz) hozzáférhetnek. [GDPR (29) preambulumbekezdés]

Profilalkotás

Az automatizált adatkezeléshez – és az arra alapozott egyedi döntéshozatali eljáráshoz – hasonlóan kell az ún. profilalkotás során az érintettek magánszféráját védő garanciákat és mechanizmusokat biztosítani.

GDPR 4. cikk
Fogalommeghatározások
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.

A címzett és a harmadik fél

A GDPR fogalommeghatározásai között szerepel a ’címzett’ és a ’harmadik fél’ – mindkettő lehet természetes személy vagy szervezet, de különbséget kell tenni közöttük. A címzett az, „akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.” Nem minősülnek azonban címzettnek azok a közhatalmi szervek, amelyekhez jogszabályban meghatározott tevékenységük körében továbbítanak személyes adatokat (ilyen például az adóhatóság). [GDPR 4. cikk 9. pont]
A harmadik fél fogalma: „ 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”. [GDPR 4. cikk 10. pont]
A címzett és a harmadik fél meghatározása azért különös jelentőségű, mert az adatkezelési tájékoztatóban az adatkezelő köteles az érintetteket informálni

– egyrészt arról, továbbítja-e a személyes adataikat, és ha igen, mely címzetteknek, illetve harmadik félnek,
– másrészt arról, ha történik adattovábbítás, a címzett milyen műveleteket végez(het) a megnevezett adatokkal, vagy az adatok körével.

Az érintett hozzájárulása

GDPR 4. cikk
Fogalommeghatározások
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.

Az érintett hozzájárulása az adatkezelés jogszerű voltának egyik fontos és gyakori pillére. A négy feltétel: az önkéntesség mellett a konkrét és megfelelő tájékoztatásra alapozott, egyértelmű akaratnyilvánítás csak együttesen értelmezhető. Kiemelt jelentősége miatt az érintett hozzájárulásával kapcsolatos kérdéseket *A GDPR jogalapjai* c. fejezetben bővebben kifejtjük.
A Rendelet 4. cikk 13–15. pontja a személyes adatok ún. különleges kategóriába tartozó genetikai, biometrikus és egészségügyi adatok fogalmát határozza meg. Általánosságban megfogalmazva különleges adatoknak a természetes személy testi, fiziológiai, genetikai, viselkedési jellemzőire, egészségi állapotára stb. vonatkozó adatok minősülnek.
A GDPR fogalommagyarázatai közül cikkünk potenciális olvasóinak érdeklődésére tekintettel már csak egyet, a 21. pontban említett felügyeleti hatóságot emeljük ki: Magyarországon ez a független közhatalmi szerv a *Nemzeti Adatvédelmi és Információszabadság Hatóság* (NAIH), melynek feladat- és hatáskörét a hatóságról szóló alfejezetben ismertettük.

Mikor jogszerű az adatkezelés?

A GDPR két oldalról is megfogalmazza az adatkezelés jogszerűsége iránti követelményeket: egyrészt a Rendelet alapelveinek maradéktalan betartásával, másrészt a megfelelő jogalap kiválasztásával – azonban a jogszerű adatkezelés ennél is többet jelent.
„Az adatkezelés jogszerűsége nem szűkíthető le pusztán arra, hogy az adatkezelő betartja-e az adatkezelésre vonatkozó törvényi szabályokat, illetve rendelkezik-e formális jogalappal a személyes adatok keze-

lésére: a jogalkotó ezen túl az adatkezelés egészének tisztességességét is beemeli a jogszerűség feltételei közé. Az adatkezelés tisztességes volta az emberi méltóság védelmével áll szoros kapcsolatban."[46]

A Rendelet adatkezelési alapelvei

A GDPR 5. cikke rögzíti a személyes adatok kezelésére vonatkozó alapelveket, amelyek egyúttal a személyesadat-kezelés gyakorlati követelményeit is meghatározzák:

- jogszerűség,
- tisztességes eljárás,
- átláthatóság,
- célhoz kötöttség,
- adattakarékosság,
- pontosság, naprakészség,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg,
- elszámoltathatóság.

A *Magyarázat a GDPR-ról* c. könyv szerkesztőjét, *Péterfalvi Attilá*t és munkatársait idézzük – az ő véleményük szerint az adatkezelés három fő pillére: „a releváns jogalap kiválasztása és az adatbiztonság teljesülése mellett a célhoz kötöttség elvének való megfelelés" meghatározó a GDPR szabályozásában. A célhoz kötöttség a többi alapelv érvényesülésének, ezáltal az adatkezelés megkezdésének is előfeltétele, amelynek a teljesülése minden fázisban „vizsgálható és vizsgálandó".[47]

A célhoz kötöttség elvéről a Rendelet 5. cikk (1) bekezdésének b) pontja a következőket mondja ki: a személyes adatok „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".

Az 5. cikk (1) bekezdés a) pontja kiegészítő magyarázatok nélkül leszögezi, hogy a „személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni". A jogszerűség vonatkozásában meg kell felelni a Rendelet és a vonatkozó tagállami jogszabályok előírásainak. A tisztességes adatkezelés túlmutat a törvényességen: az érintett magánszférájának és információs önrendelkezési jogának tiszteletben tartását jelenti.[48]

A GDPR 39., 58. és 60. preambulumbekezdése részletesen ismerteti az átláthatóság alapelvét biztosító gyakorlati követelményeket.

A természetes személyek számára átláthatóvá kell tenni, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, miként használják fel, azokba hogyan tekintenek bele. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen – ennek keretében az érintetteket tájékoztatni kell az adatkezelő kilétéről és az adatkezelés céljáról, továbbá arról, hogy jogukban áll tájékoztatást kapni a róluk kezelt adatokról, a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról, valamint arról, mi módon gyakorolhatják az adatkezelés kapcsán őket megillető jogokat. Ha a személyes adatokat az érintettől gyűjtik, az érintettet tájékoztatni kell arról is, köteles-e a kért személyes adatokat közölni, továbbá arról, milyen következményekkel jár az adatszolgáltatás elmaradása.

Az adatkezelésről szóló tájékoztatás nyújtható elektronikus formátumban is, így például a nyilvánosságnak szánt tájékoztatás közölhető honlapon keresztül. Az érintetteket a profilalkotás tényéről és annak következményeiről is tájékoztatni kell.

A GDPR alapelveiről szóló 5. cikk (1) bekezdésének c) pontja szerint a személyes adatok „az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk (»adattakarékosság«)". Az itt megfogalmazott alapelvek kifejtését a 39. preambulumbekezdés tartalmazza: „Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni." A személyes adatoknak alkalmasaknak és relevánsaknak kell lenniük a kezelésük céljára, a kezelt adatok körét a cél eléréséhez szükséges minimumra kell korlátozni. Biztosítani kell, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon: e cél elérése érdekében „az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg."

Az adattakarékosság hatékony megvalósítása érdekében hozott intézkedések közé tartozhat például az álnevesítés és a titkosítás [GDPR 25. cikk (1) bekezdés, 32. cikk (1) bekezdés a) pont, 89. cikk (1) bekezdés stb.].

A pontosság követelményét az 5. cikk (1) bekezdés d) pontja mondja ki. A 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". A 39. preambulumbekezdés

további támpontot szolgáltat: a személyes adatokat oly módon kell kezelni, amely biztosítja az adatok megfelelő szintű biztonságát és bizalmas kezelését, továbbá megakadályozza a személyes adatokhoz, illetve azok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést és az adatok jogosulatlan felhasználását.

A következő alapelv a „korlátozott tárolhatóság". E követelménynek az a tárolási mód tesz eleget, amely az érintettek azonosítását csak a személyesadat-kezelés céljainak eléréséhez szükséges ideig teszi lehetővé. Ennél hosszabb ideig történő adattárolás csak a 89. cikk (1) bekezdésében meghatározott „közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból" lehet jogszerű, de ez esetben is végre kell hajtani az érintettek jogainak és szabadságainak védelme érdekében előírt, a célnak megfelelő technikai és szervezési intézkedéseket. [GDPR 5. cikk (1) bekezdés e) pont]

Az „integritás és bizalmas jelleg" az adatbiztonság technológiájával kapcsolatos kötelező elvárásokat fogalmazza meg. Az 5. cikk (1) bekezdés f) pont előírásai 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". A XXI. században hajlamosak lennénk ezt a követelményt az informatikai biztonság kérdéskörére szűkíteni, de tévedés ne essék: a papíralapú nyilvántartásokra ugyanúgy vonatkoznak a felsorolt kritériumok.

A fent ismertetett, az 5. cikk (1) bekezdésében leírt alapelveket mondhatni, megkoronázza a (2) bekezdésben megfogalmazott „elszámoltathatóság" elve, amely az adatkezelőt teszi felelőssé az alapelveknek való megfelelésért, és azt is előírja, hogy „képesnek kell lennie e megfelelés igazolására". A gyakorlatban ez azt jelenti, hogy ez irányú tevékenységét valamennyi adatkezelőnek átláthatóan, a szabályok maximális betartásával kell végeznie. A rendelet számos kötelező jellegű intézkedést ír elő az adatkezelők számára:

- Meg kell határozniuk az adatkezelés módját, és megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. [GDPR 25. cikk]
- Nyilván kell tartaniuk az általuk végzett összes adatkezelési tevékenységet. [GDPR 30. cikk]
- Meghatározott esetekben – például közfeladatot ellátó szervek esetén – adatvédelmi tisztviselőt kell alkalmazniuk. [GDPR 37. cikk]
- Amennyiben adatfeldolgozót (pl. informatikai-rendszer- vagy honlap-üzemeltetőt) vesznek igénybe, adatfeldolgozói szerződést kell kötniük. [GDPR 28. cikk]
- Egy esetleges adatvédelmi incidens kapcsán is keletkeznek kötelezettségeik. [GDPR 32., 33., 34. cikk]

A GDPR jogalapjai

Az adatkezelők számára a legfontosabb kérdés a személyesadat-kezelés jogszerűsége. A személyes adatok védelmével korábban foglalkozók számára feltűnő, hogy a GDPR-ban meghatározott jogalapok köre sokkal szélesebb, mint a magyar jogrendszerben előzőleg ismerteké, mely utóbbi csak a hozzájáruláson alapuló, illetve a törvényi, rendeleti úton kötelező erejű adatkezelést ismerte.

A Rendelet 6. cikke rögzíti azokat az eseteket, amelyek teljesülése esetén megvan a kellő „jogalap" – ha úgy tetszik, felhatalmazás – a személyes adat kezelésére.

GDPR 6. cikk
Az adatkezelés jogszerűsége

(1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:
- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

– az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
– az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
– az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az első albekezdés f) pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

Az adatkezelés során perdöntő a megfelelő jogalap alkalmazása. Azon túl, hogy a releváns jogalap kiválasztása lényegében meghatározza az adatkezelő számára követendő eljárást, ez biztosítja a személyesadat-kezelés elvi alapjait: az átláthatóságot és az elszámoltathatóságot. Legalább ennyire fontos, hogy a jogalap teremti meg az érintettnek az adott eljárás során gyakorolható jogait (pl. a tájékoztatáshoz, tiltakozáshoz, törléshez, adathordozhatósághoz stb. fűződő jogokat).

Kérdés: a Rendelet 6. cikkének bevezető gondolata azt jelenti, hogy ugyanazon adatkezelési eljárás során egyidejűleg két vagy több jogalap is alkalmazható? A cikk írásakor rendelkezésre álló két kommentár-kötetben egymásnak ellentmondó vélemények kaptak helyet – és ez nem könnyíti meg a jogszerű eljárást követni akaró adatkezelők dolgát.

A *Magyarázat a GDPR-ról* c. kötetben ez olvasható: „A jogalapokkal kapcsolatban szükséges arra is rámutatni, hogy egy adatkezelésnek csak egy jogalapja lehet." A szerzők véleménye szerint „több jogalap egyidejű alkalmazása sérti az átláthatóság és a tisztesség elvét".[49]

A GDPR magyarázata c. kötet szerzői azt írják: a 6. cikk (1) bekezdésben olvasható „legalább az alábbiak egyike teljesül" szövegből az következik, hogy „több jogalap is fennállhat egyszerre." Jóri András és szerzőtársai idézik a 29. cikk szerinti adatvédelmi munkacsoport állásfoglalását, amely egyértelműen leszögezi, hogy egyes ügyleteknél egyidejűleg számos jogalap alkalmazható.[50]

Amikor a jogalap az érintett hozzájárulása

Az érintett (jogalany) hozzájárulása a korábbi magyar szabályozásból ismert jogalap, amelyhez a Rendelet négy, egyidejűleg meglévő kritériumot határoz meg, megszabva a hozzájárulás feltételeit, amelyeket a GDPR fogalommeghatározásai között már idéztünk.

A hozzájárulás önkéntes volta azért fontos, hogy az érintett biztosan ne valamilyen negatív következmény elkerülése érdekében, vagy megfélemlítés, kényszerítés stb. hatása alatt egyezzen bele az adatai kezelésébe. A GDPR preambulumában külön kitérnek arra, hogy az önkéntes hozzájárulás olyan esetekben „nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez, amelyekben az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn". A munkáltató mint adatkezelő és a munkavállaló mint érintett között tipikusan függő helyzet áll fenn, és amennyiben egy adott adatkezelés során a munkavállaló nem tudja szabad akaratát gyakorolni, a hozzájárulás – mint az adatkezelés jogalapja – nem érvényesíthető.

A *'konkrét'* feltétel akkor valósul meg, ha az adatkezelő pontosan körülírja, meghatározza, milyen személyesadat-kezelésre kéri az érintett hozzájárulását. A *'megfelelő tájékoztatáson alapuló'* hozzájáruláshoz az adatkezelőnek az adatkezelés megkezdése előtt kell az érintettet informálnia a következőkről:

– az adatkezelő adatai,
– az adatkezelés célja,
– a kezelt személyes adatok köre,
– a hozzájárulás visszavonhatósága és a jogorvoslati lehetőségek,
– az adattovábbítás ténye és címzettje,
– történik-e automatizált döntéshozatal, illetve profilalkotás.

Hogy miként zajlik a hozzájáruláshoz az 'egyértelmű kinyilvánítás', azt a Rendelet fent idézett szövege lényegében megmagyarázza: az érintett vagy nyilatkozattal, vagy ún. ráutaló magatartással járul hozzá személyes adatai kezeléséhez. A nyilatkozat nemcsak papíron, aláírással érvényes, de digitális közegben is, ha a hozzájárulást kérő aktív pont, jelölőnégyzet (checkbox) bejelölésével is történhet. A cselekvéssel, ráutaló magatartással történő hozzájárulás számos formája ismert: ide tartozik egy olyan rendezvényen

való részvétel, ahol előzetesen tájékoztatták a résztvevőket a kép- és hangfelvételek készítéséről, vagy ha valaki egy névjegykártyát dob be egy e célra kihelyezett gyűjtőbe és így tovább.

GDPR 7. cikk
A hozzájárulás feltételei

(1) Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.
(2) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti e rendeletet, kötelező erővel nem bír.
(3) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Mivel a 7. cikk (1) szakasza alapján az adatkezelőnek igazolnia kell az érintett hozzájárulását, a papíralapú nyilvántartásokat és az informatikai eszközökkel megadott hozzájárulási nyilatkozatokat egyaránt őriznie, tárolnia kell – csakúgy, mint a hozzájárulás esetleges visszavonásáról szóló kérelmeket.
Amennyiben az érintett hozzájárulása teremti meg a jogszerű adatkezelés kereteit, sokkal részletesebb tájékoztatást kell nyújtani a természetes személy számára: tájékoztatni kell az adattörlés lehetőségéről, az adatkezelés visszavonhatóságáról, az adathordozhatóságról stb. A jogos érdek mint jogalap esetén is él az érintett tiltakozáshoz való joga, és emellett ez a jogalap előzetes érdekmérlegelési teszt készítésére kötelezi az adatkezelőt.

A gyermekek által adott hozzájárulás sajátos követelményei

A jogi kommentárok nélkül nem könnyű megérteni a Rendeletben a gyermekek személyes adatainak kezelésére vonatkozó előírásokat. A 38. preambulumbekezdés első mondata általánosságban, nem kötelező erővel fogalmazza meg, hogy: „A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal.” Következik egy szűkítő értelmezés, amely bizonyos esetekben kötelező előírást tartalmaz: „Ezt a különös védelmet főként a gyermekek személyes adatainak olyan felhasználására kell alkalmazni, amely marketingcélokat, illetve személyi vagy felhasználói profilok létrehozásának célját szolgálja, továbbá a gyermekek személyes adatainak a közvetlenül a részükre nyújtott szolgáltatások igénybevétele során történő gyűjtésére.” A harmadik mondat nem az előző kettő gondolatmenetét folytatja, csak „megágyaz” a normaszövegben később, a 8. cikkben leírt kitételnek: „A közvetlenül a gyermek részére nyújtott megelőzési és tanácsadási szolgáltatások esetében nincs szükség a szülői felügyelet gyakorlójának hozzájárulására.”
Az (58) preambulumbekezdéssel könnyű azonosulni: „Mivel a gyermekek különös védelmet igényelnek, a kifejezetten gyermekekre vonatkozó adatkezelés vonatkozásában minden információt és kommunikációt olyan világos és közérthető nyelven kell megfogalmazni, amelyet a gyermek könnyen megért.”
És akkor nézzük a Rendelet egyik sarokkövének tartott, a gyermekek különös védelmére vonatkozó szabályt:

GDPR 8. cikk
A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában

(1) Ha a 6. cikk (1) bekezdésének a) pontja alkalmazandó, a közvetlenül gyermekeknek kínált, informá-

ciós társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

Az első feladat „az információs társadalommal összefüggő szolgáltatások" kitétel értelmezése – ehhez Jóri Andrást és munkatársait hívjuk segítségül: a fogalom magyarázatát a 2015/1535/EU számú, *A műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról* szóló irányelv tartalmazza. Az Irányelv 1. cikk (1) bekezdésének b) pontja szerint a 'szolgáltatás' „az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás".[51]

A fentiekből az következik, hogy a Rendelet 8. cikkében leírt korlátozó szabályt – ti. hogy a 16 év alatti gyermekek önállóan nem járulhatnak hozzá személyes adataik kezeléséhez, és az adatkezelésre az engedélyt kizárólag a szülői felügyeletet gyakorló adhatja meg – csak „az információs társadalommal összefüggő szolgáltatások" körében kell betartani. Joggal merül föl a kérdés: a nem internetes, és nem „közvetlenül gyermekeknek kínált" szolgáltatások körében hogyan kell jogszerűen kezelni a gyermekek személyes adatait?

A GDPR magyarázata kommentárkötet szerzői erről így vélekednek: „a 8. cikk alapján tett hozzájárulás érvényességének megítélése elválik a tagállami kötelmi jog alapján a jognyilatkozatok érvényességére, hatályára vonatkozó rendelkezések szerinti megítéléstől. Lehetséges, hogy a Rendelet szerint a hozzájárulás érvényes, ám a tagállami jog szerint érvénytelen jognyilatkozat, és fordított eset is elképzelhető."[52]

A *Magyarázat a GDPR-ról* c. könyv 14. fejezete tárgyalja a gyermekek védelmének kérdéskörét; a szerzők is felhívják a figyelmet arra, hogy a GDPR csak egy részét fedi le a gyermekek személyesadat-kezelésének. „A többi esetben a Ptk. IV. címében – *A kiskorúság miatti korlátozott cselekvőképesség és cselekvőképtelenség* – foglaltak irányadóak. […] A Ptk. értelmében főszabályként a 14 év alattiak jognyilatkozata – a kifejezetten csekély jelentőségű ügyleteket leszámítva – semmis, nevükben a törvényes képviselő (szülő, illetve gyám) jár el."[53]

Amikor a jogalap a szerződés

A szerződéses jogalap a GDPR egyik újdonsága, amely tulajdonképpen megkönnyíti az adatkezelő helyzetét: alkalmazása sokkal egyértelműbb, mint az érintett hozzájárulásán alapuló adatkezelés. Amennyiben ez a jogalap érvényes, az érintett nem vonhatja vissza a hozzájárulását, nem tiltakozhat az adatainak a kezelése ellen stb. Két esetben alkalmazható ez a jogalap: ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy ha a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges az adatkezelés. [GDPR 6. cikk b) pont)

A Rendelet nem írja elő, milyen személyes adatokat kell a szerződéses jogalap körébe tartozó megállapodások körében kezelni – erre a tagállami jog az irányadó.

Amikor a jogi kötelezettség teljesítése a jogalap

A GDPR 6. cikk. 1. bekezdés c) pontja szerint az adatkezelés abban az esetben is jogszerű, ha a személyesadat-kezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.

Bár a Rendelet szerint a jogi kötelezettség jogalapját elegendő jogszabályi szinten meghatározni, a tagállami jogalkotás lehetőségével élve a magyar jogalkotó törvényi előíráshoz köti a személyes adatok kezelését. [Infotv. 5. §]

Amikor a jogalap a létfontosságú érdekek védelme

Személyes adat akkor is kezelhető, amikor az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek – életének, testi épségének – védelme miatt szükséges [GDPR 6. cikk d) pont). Ebbe az esetkörbe főleg a balesetek, természeti csapások elszenvedői, a váratlan rosszullétbe, humanitárius és más olyan veszélyhelyzetbe kerülők személyesadat-kezelése tartozik, amikor az érintettnek nem áll módjában az adatkezeléshez a hozzájárulását megadni.

Amikor a közérdekű feladatellátás vagy a közhatalom-gyakorlás a jogalap

A GDPR 6. cikk e) pontja értelmében a személyesadat-kezelés akkor is jogszerű, ha „az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges".
Hogy egy feladat közérdekűnek minősül-e, azt uniós vagy tagállami jogszabály határozza meg (a magyar jogszabályokban a '*közfeladat'* kifejezés szerepel). Magyarországon a közérdekű feladatot ellátó szervekről az államháztartásról szóló 2011. évi CXCV. törvény 3/A. § (1) bekezdése így szól: „Közfeladat a jogszabályban meghatározott állami vagy önkormányzati feladat."[54] 2019. január 1-jén lépett hatályba a *45/2018. (III. 19.) Korm. rendelet az állami és önkormányzati közfeladat-kataszterről,* amelynek 1.§ 4. pontja így szól: *„közfeladat-kataszter: a hatékony állami feladatellátás biztosítása, továbbá a kormányzati döntéshozatal támogatása céljából az egyes közfeladatokat a teljesség igényével – a közfeladat ellátásáért felelős, valamint a közfeladatot megállapító jogszabály meghatározásával – leíró, deklaratív hatályú, internetes felületen elérhető és nyilvános digitális adatbázis."*[55] A készülő új közfeladat-kataszter segít abban a kérdésben eligazodni, mi számít Magyarországon közérdekű feladatnak.
A közhatalmi jogosítvány gyakorlása egybe is eshet a közfeladattal, de annál szűkebb körre vonatkozik. Ebbe a tevékenységi körbe tartozik a közigazgatás, a rendvédelem, az igazságszolgáltatás stb. – konkrétabban például az adó- és vámhatóság, a szakmai kamara, az önkormányzat.

Amikor az adatkezelő vagy harmadik fél jogos érdeke a jogalap

Talán megengedhető egy szubjektív megjegyzés: a legnehezebben értelmezhető és a legnagyobb kockázattal járó jogalap a Rendelet 6. cikkében meghatározott ún. jogos érdek. A GDPR jogszerűnek tekinti azt a személyesadat-kezelést is, amikor „az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek." [GDPR 6. cikk f) pont]
A definíció első részéből következik, hogy az adatkezelő megítélésén múlik, saját jogos érdekét fontosabbnak ítéli-e az érintettek jogainál. A GDPR előírja, hogy az érdekek ütköztetését az adatkezelő írásban – ún. érdekmérlegelési tesztben – dokumentálja, amelyben meg kell határoznia, az adatkezelés során milyen céllal, mennyi ideig, mely személyes adatokat kezel, és azt is bizonyítania kell, hogy az adatkezeléssel csakis a szükséges mértékben, arányosan korlátozza az érintett jogait és szabadságait.
Az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése során is alkalmazni kell a célhoz kötöttséget, az elszámoltathatóságot – és magától értetődően tisztességesen, átláthatóan, vagyis a GDPR alapelveit érvényesítve kell az érintettek személyes adatait kezelni.
A jogalapok ismertetését lezárva, Jóri András segítségével bemutatjuk az egyes jogalapok alkalmazásának előnyeit és hátrányait az adatkezelő szempontjából.
Az érintett hozzájárulásakor az adatkezelőre háruló tájékoztatási kötelezettség bővebb, az érintett visszavonhatja a hozzájárulását, és ez bizonytalanságot okoz, továbbá él az adathordozhatósághoz való jog.
A szerződés előnye, hogy sem a hozzájáruláson, sem az érdekmérlegeléssel járó jogos érdeken alapuló bizonytalanság nem áll fenn, hátránya az adathordozhatósághoz való jog.
A jogi kötelezettségen alapuló adatkezelés előnye, hogy sem a hozzájáruláson, sem az érdekmérlegeléssel járó jogos érdeken alapuló bizonytalanság nem áll fenn.
A létfontosságú érdek a legegyértelműbb jogalap: nincs sem előnye, sem hátránya.
A közérdekű vagy közhatalmi jogosítványon alapuló adatkezelés előnye szintén az, hogy sem a hozzájáruláson, sem az érdekmérlegeléssel járó jogos érdeken alapuló bizonytalanság nem áll fenn. Hátránya, hogy az érintett élhet a tiltakozáshoz való jogával, és őt erről előzetesen tájékoztatni kell.
Az adatkezelő jogos érdekére való hivatkozásnak számos hátránya van: bizonytalan a megítélése, az adatkezelőnek előre el kell készítenie az érdekmérlegelésre vonatkozó dokumentációt, előzetesen tájékoztatnia kell az érintettet az őt megillető jogokról, és az érintett tiltakozhat a személyes adatainak kezelése ellen. A jogos érdekre való hivatkozást a közhatalmi szervek nem alkalmazhatják.[56]

Az érintett jogai és az e jogokat biztosító intézkedések

A Rendelet III. fejezete kimondottan az érintett jogairól szól: az 1. szakasz az átláthatóságot és a vele kap-

csolatos intézkedéseket nevesíti, a 2. szakasz tárgya a tájékoztatás és a személyes adatokhoz való hozzáférés, a következő rész a helyesbítés és törlés kérdéseit taglalja, a 4. szakasz témaköre a tiltakozáshoz való jog és automatizált döntéshozatal egyedi ügyekben, az ötödik pedig a korlátozásokat közli.
A GDPR egyrészt megőrizte az adatvédelmi irányelvben megfogalmazott érintetti jogokat, másrészt két újdonságot is bevezetett: a törléshez (más szóval az elfeledtetéshez), illetve az adathordozhatósághoz való jogot; ez utóbbi kettő kifejezetten az infokommunikációs technológiai fejlődésre reflektál.

Az átláthatóság joga

Az átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések címet viselő 12. cikk szerint: az adatkezelő megteszi a szükséges intézkedéseket annak érdekében, hogy az érintett részére a személyesadat-kezelésre vonatkozó, a 13–22., illetve a 34. cikkekben említett valamennyi információt és tájékoztatást tömör, átlátható, érthető, könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek szóló információk esetében. Az információkat szóban, írásban vagy elektronikus úton kell megadni. (A hivatkozott cikkeket az alábbiakban ismertetjük.)

Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik

A GDPR 13. cikke értelmében: ha az érintettől gyűjtik a rá vonatkozó személyes adatokat, az adatkezelőnek az alább felsorolt információk mindegyikét az érintett rendelkezésére kell bocsátania, mégpedig a személyes adatok megszerzésének időpontjában:

a) az adatkezelőnek és képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő (vagy megbízott) elérhetőségei;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) amennyiben a jogalap az adatkezelő vagy harmadik fél jogos érdeke, ennek megnevezése;
e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái;
f) az adatkezelő harmadik országba vagy nemzetközi szervezet részére továbbítja-e a személyes adatokat.

A felsoroltak mellett – ugyancsak a személyes adatok megszerzésének időpontjában – a tisztességes és átlátható adatkezelés biztosítása érdekében az adatkezelőnek a következő kiegészítő információkról kell tájékoztatnia az érintettet:

a) a személyes adatok tárolásának időtartamáról;
b) azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
c) az adathordozhatósághoz való, illetve a hozzájárulás bármely időpontban történő visszavonásához való jogáról,
d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul, és az érintett köteles-e a személyes adatokat megadni;
f) történik-e automatizált döntéshozatal, illetve profilalkotás.

Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg

A 14. cikkben felsorolt előírások lényegében megegyeznek a GDPR 13. cikkben meghatározottakkal – kiegészítve két további feltétellel:

– az adatkezelőnek közölnie kell az érintettel a kezelt személyes adatok kategóriáit, illetve
– meg kell adnia a személyes adatok forrását – adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e.

Tájékoztatás az adatvédelmi incidensről

Miután a tájékoztatási kötelezettségekhez tartozik, a vonatkozó előírást itt idézzük: egy esetleges adatvédelmi incidens bekövetkezése esetén – amennyiben az valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve – az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintetteket a történtekről. [GDPR 34. cikk (1) bekezdés]

Az érintett hozzáférési joga

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arról, folyamatban van-e személyes adatainak kezelése, és ha igen, arra is jogosult, hogy hozzáférést kapjon a rá vonatkozó személyes adatokhoz, illetve az alább felsorolt információkhoz:

– a kezelt személyes adatok kategóriái, az adatkezelés célja(i), az adattárolás tervezett időtartama;

– azon címzettek vagy azon címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
– az érintettet tájékoztatni kell az őt megillető jogokról (helyesbítés, törlés, korlátozás, tiltakozás; panasz benyújtás, továbbá, ha az adatokat nem az érintettől gyűjtötték, azok forrása.

Amennyiben az érintett kéri, a rá vonatkozó személyes adatok másolatát az adatkezelő köteles az érintett rendelkezésére bocsátani. [GDPR 15. cikk]

A helyesbítéshez és a törléshez („az elfeledtetéshez") való jog

A Rendelet 16. cikke alapján az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat, illetve, hogy kérje a hiányos személyes adatok kiegészítését.

A Rendelet fogadtatása körüli sajtóvisszhang egyik leghangsúlyosabb eleme volt a törléshez való jog deklarálása, amely főként azért keltett nagy feltűnést, mert a GDPR bevezetésekor már széles körben tudatosodott, hogy „az internet nem felejt". A jogalkotó éppen ennek, az internethasználók számára kedvezőtlen helyzetnek a megváltoztatása érdekében írja elő a törlési kötelezettséget az adatkezelők számára. Az elfeledtetéshez való jog bevezetése a Rendelet egyik olyan újdonsága, amely kimondottan a technológiai fejlődésre reflektál.

A GDPR 17. cikkben foglalt szabályok szerint az érintett jogosult arra, hogy kérésére az adatkezelő törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles az érintett által kért adatokat indokolatlan késedelem nélkül törölni – feltéve, hogy:

– a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
– az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
– az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
– a személyes adatokat jogellenesen kezelték;
– a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
– a személyes adatok gyűjtése a 8. cikk (1) bekezdése szerint – vagyis 16 év alatti gyermekek részére kínált elektronikus szolgáltatások keretében – zajlott (lásd a GDPR 8. cikk című keretes szöveget].

Nagyon fontos kötelezettségeket, illetve kivételeket tartalmaz a 17. cikk (2) és (3) bekezdése, amelyek azonban még inkább fokozzák az elfedtetéshez való jog deklarálása és gyakorlati érvényessége közötti ellentmondásosságot:

– a nyilvánosságra hozott személyes adatot – a fent felsorolt esetekben – az adatkezelő köteles törölni, és meg kell tennie az észszerűen elvárható lépéseket annak érdekében, hogy az érintett által törölni kért adatot, illetve az arra mutató linkeket más adatkezelők is töröljék;
– a törlési kötelezettség alól kivételt képez, ha az adatkezelés az alábbi tevékenységek ellátása érdekében történt:
  • a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából, az adatkezelőre háruló jogi kötelezettség teljesítése érdekében,
  • közérdek,
  • közérdekű archiválás, tudományos és történelmi kutatás, statisztika,
  • jogi igények előterjesztése, érvényesítése, védelme.

Az adatkezelés korlátozásához való jog

Az érintett arra is jogosult, hogy kérésére az adatkezelő korlátozza személyes adatainak kezelését. [GDPR 18. cikk] A korlátozáshoz való jog gyakorlása meglehetősen bonyolult, ugyanis ez esetben több feltétel együttállását kell vizsgálni az alábbiak szerint:

– ha az érintett vitatja az adatok pontosságát, a korlátozás csak addig érvényes, amíg az adatkezelő ellenőrzi a vitatott adatok helyességét;
– ha az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett azok felhasználásának korlátozását kéri;
– az adatkezelőnek már nincs szüksége a szóban forgó személyes adatokra, de jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez az érintett igényli azokat;
– amennyiben az érintett tiltakozik az adatkezelés ellen, az idő alatt, amíg megállapítják, az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben, korlátozni kell az adatkezelést (lásd 21. cikk (1) bekezdés).

Az adathordozhatósághoz való jog

Amennyiben az érintett a fentiekben már említett hozzájáruláson, illetve szerződésen alapuló adatkezelési célra közölte személyes adatait, illetve, ha az adatkezelés automatizált módon történik, az érintett jogosult arra, hogy a rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa. Az adathordozhatósághoz való jog nem érintheti hátrányosan mások jogait és szabadságait. [GDPR 20. cikk]

A tiltakozáshoz való jog

A GDPR biztosítja az érintett jogát arra, hogy bármikor tiltakozzon személyes adatainak közérdekű feladatra vagy az adatkezelő jogos érdekére való hivatkozással történő kezelése ellen (vö. GDPR 6. cikk (1) bekezdés e) vagy f) pont), ideértve az említett rendelkezéseken alapuló profilalkotást is. Ez esetben az adatkezelő nem kezelheti tovább a személyes adatokat, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, illetve amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. [GDPR 21. cikk]

Az érintett jogainak korlátozása

Az adatkezelőkre vagy adatfeldolgozókra nézve lehetnek, illetve vannak olyan uniós vagy tagállami jogi kötelezettségek és intézkedések, amelyek korlátozhatják a 12–23. és a 34. cikkben foglalt jogokkal és kötelezettségekkel összhangban lévő rendelkezések hatályát. Ezen korlátozások tiszteletben tartják az alapvető jogok és szabadságok lényeges tartalmát, és a meghozott intézkedések egy demokratikus társadalomban az alábbiak védelméhez szükségesek és arányosak [GDPR 23. cikk (1) bekezdés]:

a) nemzetbiztonság;
b) honvédelem;
c) közbiztonság;
d) bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;
e) az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot;
f) a bírói függetlenség és a bírósági eljárások védelme;
g) a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;
h) az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység;
i) az érintett védelme vagy mások jogainak és szabadságainak védelme;
j) polgári jogi követelések érvényesítése.

Az (1) bekezdésben említett jogalkotási intézkedések részletes rendelkezéseket tartalmaznak a következőkre nézve: az adatkezelés céljaira vagy az adatkezelés és a személyes adatok kategóriáira, a bevezetett korlátozások hatályára, a visszaélést, illetve a jogosulatlan hozzáférést vagy továbbítást megakadályozó garanciákra, az adatkezelő meghatározására, az adattárolás időtartamára, az érintettek jogait és szabadságait érintő kockázatokra, illetve az érintetteknek a korlátozásról szóló tájékoztatására – kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját. [GDPR 23. cikk (2) bekezdés]

Adatkezelő és adatfeldolgozó

A korábbi szabályozásokban az adatkezelést végzők között nem tettek különbséget: a korábbi magyar adatvédelmi jog nem ismerte az adatfeldolgozás – és ezzel párhuzamosan – az adatfeldolgozó fogalmát. A GDPR-ban a két alany elhatárolásánál az adatkezelési cél és mód játszik szerepet.[57]

Az adatkezelőre vonatkozó előírások

Az adatkezelő definíciójában nem történt jelentős változás, az adatkezelés jogszerűségéért korábban is, jelenleg is az adatkezelő a felelős. A Rendelet az *elszámoltathatóság* alapelvének bevezetésével ír elő eddig nem ismert kötelezettséget az adatkezelők számára.[58]

Az adatkezelő feladatai, kötelezettségei

A Rendelet – többek között – az adatkezelőket kötelezi olyan technikai és szervezési intézkedések végrehajtására, amelyek biztosítják, hogy a személyes adatok kezelése a Rendelettel összhangban történik, és amelyek bizonyítják a GDPR-előírásoknak való megfelelést.

Beépített és alapértelmezett adatvédelem

Az adatkezelők számára a Rendelet (78) preambulumbekezdése és 25. cikke írja elő a beépített és az alapértelmezett adatvédelem elveinek kötelező érvényesítését. A 'beépített adatvédelem' (privacy by design) és az 'alapértelmezett adatvédelem' (privacy by default) elvei az adatkezelő számára kötelezettségként fogalmazódnak meg, amelynek értelmében az adatkezelőnek olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyekkel eleget tud tenni a GDPR előírásainak.

Az intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelési folyamatot, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

A jogalkotó ezen a ponton nemcsak a GDPR hatálya alá tartozó adatkezelők számára írja elő a beépített és az alapértelmezett adatvédelem elveinek alkalmazását: a személyes adatok kezelésével járó szolgáltatások és termékek tervezőit, fejlesztőit és felhasználóit is arra kívánják ösztönözni, hogy már a kezdetektől, a tervezés, majd a fejlesztés során tartsák szem előtt a személyes adatok védelméhez való jogot, illetve a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy a kifejlesztett termékek, szolgáltatások alkalmasak legyenek arra, hogy az adatkezelők és az adatfeldolgozók képesek legyenek adatvédelmi kötelezettségeiknek eleget tenni.[59]

Az adatfeldolgozóra vonatkozó szabályok

A Rendelet alapfogalmai között szerepelnek az adatfeldolgozóra vonatkozó legfontosabb előírások – az alábbiakban néhány további rendelkezésre hívjuk fel a figyelmet.

A GDPR definíciójából következik, hogy az adatfeldolgozó önmagában nem értelmezhető: csak egy adatkezelő tevékenységéhez kapcsolódva lehet adatfeldolgozói tevékenységet – lényegében szolgáltatást – végezni. Az adatkezeléssel kapcsolatos felelősséget az adatkezelő viseli – beleértve azt, hogy az adatkezelő csak a Rendelet előírásainak megfelelő garanciákkal bíró, a szigorú követelményeknek eleget tévő adatfeldolgozót vehet igénybe. Az adatfeldolgozókra is vonatkozó fő szabályokat a GDPR 32-36. cikke tartalmazza.

Az alapkövetelmények között már hivatkoztunk a Rendelet szövegére, amely kiköti, hogy az adatfeldolgozó kizárólag az adatkezelő írásbeli utasításai alapján kezelheti a személyes adatokat – tehát ismét nyomatékosítani kell az adatkezelő felelősségét: neki kell megfelelő módon részletezett és dokumentált utasításokban szabályoznia az adatfeldolgozó által végzett adatkezelést.

Arról is az adatkezelőnek kell döntenie, a szolgáltatás befejezését követően mit kell tennie az adatfeldolgozónak a személyes adatokkal: köteles törölni, vagy visszajuttatni azokat az adatkezelőnek. [GDPR 28. cikk (3) bekezdés g) pont]

Adatfeldolgozói szerződés

Rendkívül gyakori megoldás, hogy egy adatkezelő adatfeldolgozót vesz igénybe a főtevékenységét segítő speciális szolgáltatások, mint például az informatikai rendszer üzemeltetése, a honlapszolgáltatás, a könyvelés, bérszámfejtés stb. terén. A GDPR a 28. cikk (3) bekezdésében részletesen meghatározza az adatkezelő és az adatfeldolgozó között kötelezően megkötendő adatfeldolgozói szerződés tartalmi követelményeit.

– Az adatfeldolgozó által végzett adatkezelést olyan szerződésnek vagy más jogi aktusnak kell szabályoznia, amely az adatfeldolgozót köti az adatkezelővel szemben, és pontosan meghatározza az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait.

A 'más jogi aktus' Jóri értelmezése szerint „lehet bármely (uniós vagy tagállami) jogszabály, normatív vagy egyedi hatósági aktus, vagy – ha ebből a vonatkozó polgári jogi szabályok szerint kötelem keletkezhet – egyoldalú jognyilatkozat."[60]

Az írásbeli megállapodásban elő kell írni, hogy az adatfeldolgozó

– a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli;
– biztosítja, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak, vagy jogszabályon alapuló titoktartási kötelezettség alatt állnak;
– meghozza a 32. cikkben előírt, az adatkezelés biztonságát szolgáló intézkedéseket és eleget tesz a 28. cikk 3. bekezdés d) – h) pontjaiban meghatározott előírásoknak.

Az adatkezelési tevékenységek nyilvántartása

A Rendelet 30. cikke részletes rendelkezéseket tartalmaz arról, hogy milyen nyilvántartást kell vezetnie írásban (ideértve az elektronikus formátumot is) valamennyi adatkezelőnek, illetve adatfeldolgozónak. Az azonosító adatokon túl a legfontosabb elemek az adatkezelés céljai, az érintettek, a személyes adatok, továbbá a címzettek kategóriái, adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, valamint az adatbiztonságot szolgáló technikai és szervezési intézkedések általános leírása.

Az adatkezelési nyilvántartások vezetéséhez jó segítséget nyújt a https://gdpr.hvgorac.hu/ oldalon közölt mintatáblázat, amelynek alapján az adatkezelők és adatfeldolgozók el tudják készíteni a saját nyilvántartásukat.[61]

Fontosnak tartjuk megemlíteni, hogy számos félreértésre ad okot a 30. cikk (5) bekezdésben említett kivétel, mely szerint az adatkezelési tevékenységek nyilvántartásával kapcsolatos „kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre". Ez a kritérium csak a kivételekkel együtt érvényes, amelyek közül a legfontosabb: „ha az adatkezelés nem alkalmi jellegű". Akár egyetlen személyt is foglalkoztat egy vállalkozás vagy szervezet, az ő adatainak a kezelése már nem lehet alkalmi jellegű – tehát a 30. cikkben előírt kötelezettség rá is vonatkozik.

Az adatkezelés biztonsága

Az adatkezelő és az adatfeldolgozó a tudomány és a technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázatok mértékének megfelelő szintű adatbiztonságot garantálja.

A Rendelet 32. cikke előírja

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állását kellő időben visszaállítás képességének biztosítását;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére, értékelésére szolgáló eljárást.
- A biztonság megfelelő szintjének meghatározásakor az adatkezelésből eredő, a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből eredő kockázatokra kell tekintettel lenni.
- Az adatkezelőnek és az adatfeldolgozónak intézkedéseket kell hoznia annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék a fent említett adatokat.

Összegezve a GDPR által előírt adatbiztonsági szabályokat: a megfelelő szintű védelmet a tudomány és technika mindenkori állásának, az adatkezelés jellemzőinek, illetve az érintettre vonatkozó kockázatainak, továbbá a megvalósítás költségeinek figyelembevételével kell kialakítani. Mindezeken túl a szabályozás általános, „példálózó szinten emel ki adatbiztonsági jó gyakorlatokat; ilyen például az információbiztonság »szentháromsága« (bizalmasság, sértetlenség, rendelkezésre állás), az alapvető biztonsági megfontolások (álnevesítés, titkosítás, biztonsági betörési teszt, incidenskezelés), vagy az elszámoltathatóság elvét, vagy a beépített és alapértelmezett adatvédelem koncepcióját."[62]

Az adatbiztonsági szabályoknak való megfelelés szempontjainak kidolgozásában jó segítséget nyújt *az állami és önkormányzati szervek információbiztonságáról szóló 2013. évi L. törvény*, illetve a kifejezetten az informatikai biztonságra kidolgozott *ISO 27001 szabvány* követelményrendszere.

Teendők adatvédelmi incidens esetén

A Rendelet 4. cikk 12. pontja írja le az 'adatvédelmi incidens' fogalmát:

GDPR 4. cikk

Fogalommeghatározások

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.

Az adatvédelmi incidens véletlenül, de abban az esetben is bekövetkezhet, ha az adatkezelő és/vagy az adatfeldolgozó elmulasztotta a Rendelet 5. cikk (1) bekezdés f) pontjában meghatározott ’megfelelő technikai és szervezési intézkedéseket’ megtenni. 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 33. cikkének tárgya az adatvédelmi incidens bejelentése a felügyeleti hatóságnak – miszerint az adatkezelő késedelem nélkül, 72 órával a tudomására jutás után bejelenti az adatvédelmi incidenst a felügyeleti hatóságnak (a NAIH-nak), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az adatfeldolgozó az adatvédelmi incidenst indokolatlan késedelem nélkül bejelenti az adatkezelőnek.
A bejelentésben ismertetni kell az adatvédelmi incidens jellegét, az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges mennyiségét, ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.
Az adatkezelőnek nyilván kell tartania az adatvédelmi incidenseket, feltüntetve a tényeket, az okozott hatásokat és a problémák elhárítására tett intézkedéseket. E nyilvántartás alapján a felügyeleti hatóságnak módjában áll a GDPR követelményeinek való megfelelés ellenőrzése.
A 34. cikk írja elő az adatkezelő kötelezettségét az érintett tájékoztatására vonatkozóan. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az eseményről.
Az érintett részére adott tájékoztatásban világosan és közérthetően kell ismertetni az adatvédelmi incidens jellegét, az abból eredő következményeket, illetve az orvoslására vonatkozó intézkedéseket. Titkosított adatok esetén nem kell tájékoztatni az érintettet; nagyszámú érintett esetén pedig elegendő nyilvánosan közzétett információk útján tájékoztatni az adatvédelmi incidensről.

Az adatvédelmi tisztviselő

Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik (kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat), ha az adatkezelési műveletek az érintettek rendszeres, szisztematikus, nagymértékű megfigyelését teszik szükségessé, illetve, ha nagy számban kezelnek a személyes adatok különleges kategóriáiba tartozó, vagy büntetőjoggal, bűncselekményekkel kapcsolatos adatokat. [GDPR 37. cikk (1) bekezdés]
A rendelet 38. cikke rendelkezik az adatvédelmi tisztviselő jogállásáról, amely a maga nemében különleges: függetlenített poszt, a szervezet vezetőjének van közvetlenül alárendelve, lehet belső munkatárs vagy külső megbízott. Az adatvédelmi tisztviselő szakmai tevékenységében nem utasítható, e feladatkörével kapcsolatban nem vonható felelősségre. Az adatvédelmi tisztviselő jogi, informatikai és a szervezetet illető belső kérdésekben szakértői szinten tájékozott szakember.
Az adatvédelmi tisztviselő feladatai a GDPR 39. cikke alapján: tájékoztat és szakmai tanácsokat ad az adatkezelő és/vagy az adatfeldolgozó adatkezelést végző alkalmazottai számára az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban; ellenőrzi a GDPR és más rendeletek előírásainak való megfelelést, továbbá együttműködik a felügyeleti hatósággal. A személyesadat-kezeléssel kapcsolatos kérdéseivel az érintett az adatkezelő adatvédelmi tisztviselőjéhez fordulhat.

***

A Rendelet számos cikkét kihagytuk az ismertetésből – részben terjedelmi okokból, részben a potenciális célközönség érdeklődési köre okán. Nem foglalkozunk az adattovábbítás részleteivel, a hatósági tevékenységgel, a bűnügyi irányelvből adódó feladatokkal és sok más, fontos kérdéssel – mint például a jogorvoslati és panasztételi lehetőségekkel. Az érdeklődők mindezeket megtalálják egyrészt a Rendelet szövegében, másrészt a sokszor hivatkozott kommentár-kötetekben. Cikkünk zárásaként a könyvtári szolgáltatások szempontjából két kiemelkedően fontos esetkörre térünk ki.

Az adatkezelés különös eseteire vonatkozó rendelkezések

A személyes adatok védelméhez fűződő jogok korlátozottan érvényesek és gyakorolhatók. Az érintetteknek tudomásul kell venniük, hogy egyéni érdekeikkel szemben a többség érdekei időnként elsőbbséget élveznek. A GDPR az általánosságban érvényes szabályoktól több eltérést is meghatároz, amelyek közül az alábbi kettőre hívjuk föl a figyelmet.

A személyes adatok kezelése és a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog

A 85. cikk szerint a tagállamoknak jogszabályban kell összeegyeztetniük a személyes adatok védelmét szolgáló, a GDPR által meghatározott jogot a véleménynyilvánítás szabadságához, illetve a tájékozódáshoz való joggal. E körbe beleértendő a személyes adatok újságírási célból, illetve tudományos, művészi vagy irodalmi kifejezés céljából végzett kezelése is.
A jelen cikkben gyakran idézett könyvükben Péterfalvi Attila és szerzőtársai kifejtik, hogy „a véleménynyilvánítás szabadsága magában foglalja a tájékozódás, vagyis az információk és eszmék megismerésének és közlésének szabadságát is [Charta 11. cikk (1) bekezdés].” Megfelelő információk nélkül nem lehetséges a vélemények és gondolatok kifejezése. A jogalkotóknak törekedniük kell arra, „hogy megfelelő és igazságos egyensúly álljon fenn a felmerülő érdekek […] valamint az egyén – személyes adatok védelméhez és az információk fogadásához és közléséhez fűződő – alapvető jogai között. Ugyanis bármely olyan beavatkozás, amely a jogszerű tartalmú adatátvitel blokkolását eredményezné, a tájékozódás szabadsága sérelmének veszélyével járna.”[63]

A közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott adatkezelésre vonatkozó garanciák és eltérések

A Rendelet számos helyén találkozunk a személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelésével, amely eseteket a GDPR – bizonyos feltételek teljesülése esetén – az eredeti adatkezelési céllal összeegyeztethető további adatkezelésnek minősít.
A 89. cikk (1.) bekezdése előírja, hogy a fent megjelölt célokból történő adatkezelést a Rendelettel összhangban „az érintett jogait és szabadságát védő megfelelő garanciák mellett kell végezni”, és amelynek érvényesítése érdekében olyan technikai és szervezési intézkedéseket kell tenni, amelyek „biztosítják különösen az adattakarékosság elvének betartását” – adott esetben az álnevesítést.
Cikkünk következő részében visszatérünk a közérdekű archiválás céljából, tudományos és történelmi kutatási vagy statisztikai célból folytatott adatkezelés értelmezésére, a Rendelet előírásainak gyakorlati alkalmazására.

Zárszó helyett

„Előbb tudjuk a világot, semmint ismernénk. Amikor a civilizáció új eszközei mind arra szolgálnak, hogy áttetszővé alázzanak minden embert, lehet, hogy semmi nem lehet fontosabb, mint az, hogy megőrizzük valahogy az arcunkat, a személyességet, a személyiséget a jövőnek.”[64]
Magyarország első adatvédelmi biztosának, Majtényi Lászlónak gondolatait idézve a szerző arra kéri a Tisztelt Olvasót: öntudatos polgárként ne hagyja, hogy a civilizációs eszközök használata miatt akár a saját, akár mások magánszférája sérüljön. Segítsük egymást abban, hogy megvédhessük magánéletünket, megőrizhessük személyes integritásunkat – találkozzunk bár érintettként vagy munkavállalóként a személyesadat-kezeléssel.

Irodalom és jegyzetek

1. ILLYÉS Gyula: Jog. In: Illyés Gyula összegyűjtött versei. https://reader.dia.hu/document/Illyes_Gyula-Illyes_Gyula_osszegyujtott_versei-906 [2019. február 8.]
2. POLYÁK Gábor – SZŐKE Gergely László: Technológiai determinizmus és jogi szabályozás, különös tekintettel az

adatvédelmi jog fejlődésére. In: Pro Publico Bono, 2015. 1. sz. 31–17. p.

3. MAJTÉNYI László: Az információs szabadságok : adatvédelem és a közérdekű adatok nyilvánossága. Budapest : Complex, 2006. 13. p.
4. SÓLYOM László: A személyiségi jogok elmélete. Budapest : Közgazdasági és Jogi Könyvkiadó, 1983. 9–10. p.
5. MAJTÉNYI László: A személyes adatok védelméhez való jog. In: Emberi jogok. Szerk. Halmai Gábor és Tóth Gábor Attila. Budapest : Osiris, 2003. 579. p.
6. MAJTÉNYI (2003), i. m. 580. p.
7. MAJTÉNYI (2006), i. m. 13. p.
8. SÓLYOM László: Egy új szabadságjog: az információszabadság. = Valóság, 1988. 9. sz. 14–34. p.
9. Magyarország Alaptörvénye. VI. cikk (3) bekezdés. https://net.jogtar.hu/jogszabaly?docid=A1100425.ATV
10. MAJTÉNYI (2006), i. m. 94. p.
11. JÓRI András [et. al.]: A GDPR magyarázata. Budapest : HVG ORAC, 2018. 29–30. p.
12. MAJTÉNYI (2006), i. m. 80. p.
13. JÓRI, i. m. 31–32. p.
14. NEMÉNYI László: Körkörös adatvédelem : A személyi adatokkal való önrendelkezés polgárjoga. = Beszélő, 3. évf., 49. sz. http://beszelo.c3.hu/cikkek/korkoros-adatvedelem [2019. február 8.]
15. JÓRI, i. m. 32–33. p.
16. JÓRI, i. m. 33. p.
17. 15/1991. (IV. 13.) AB határozat. Közzétéve: Magyar Közlöny, 1991. 39. sz. 805–814. p.
18. SÓLYOM László: Az emberi jogok az Alkotmánybíróság újabb gyakorlatában. = Világosság, 34. évf., 1993. 1. sz. 16–33. p.
19. JÓRI, i. m. 364–365. p.
20. Az Európai Parlament és Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
21. Magyarázat a GDPR-ról. (Szerk.) Péterfalvi Attila [et al.]. Budapest : Wolters Kluwer, 2018. 25. p.
22. A továbbiakban vagy „Rendelet', vagy az angol megnevezés akronímájával: ‚GDPR' néven hivatkozunk a jogszabályra. Dolgozatunk „keretes" szövegei a Rendelet hivatalos magyar fordításából származó idézetek. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN
23. EGT országok: az EU tagállamai, továbbá Izland, Liechtenstein és Norvégia
24. Európai Unió. Rendeletek, irányelvek és más jogi aktusok. https://europa.eu/european-union/eu-law/legal-acts_hu
25. Az EUI-GDPR hivatalos magyar nyelvű szövege megtalálható: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1725&from=EN
26. Magyarázat a GDPR-ról, i. m. 24. p.
27. Bevezetés az alkotmányjogba : az Alaptörvény és Magyarország alkotmányos intézményei. (szerk.) Schanda Balázs, Trócsányi László. Bp. : HVG-ORAC, 2014. https://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_548_Alkotmanyjog/ch04s09.html [2019. február 8.]
28. Magyarázat a GDPR-ról, i.m. 51. p.
29. Magyarázat a GDPR-ról, i. m. 52. p.
30. JÓRI, i. m. 54–56. p.
31. NAIH/2018/5233. sz. állásfoglalása – Péterfalvi Attila elnök levele, 2018. november 23.
32. JÓRI, i. m. 60–61. p.
33. Magyarázat a GDPR-ról, i. m. 54. p.
34. Az Európai Unióról szóló szerződés (egységes szerkezetbe foglalt változat) V. cím 2. fejezet A közös kül-és biztonságpolitikára vonatkozó különös rendelkezések. https://europa.eu/european-union/sites/europaeu/files/eu_citizenship/consolidated-treaties_hu.pdf [2019. február 7.]
35. JÓRI, i. m. 110. p.
36. JÓRI, i. m. 114. p.
37. Magyarázat a GDPR-ról, i. m. 63. p.
38. JÓRI, i. m. 53. p.
39. JAY, Rosemary – HAMILTON, Angus: Data protection in law and practice. London : Sweet amd Maxwell, 1999. 29. p. – idézi JÓRI, i. m. 61. p.
40. ABI 1998, 277. p. – idézi JÓRI, i. m. 77. p.
41. PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter: A nemzeti vagyon felhasználásával kapcsolatos adatok nyilvánossága a gyakorlatban. [tanulmány]. Budapest, 2017. – Idézi: Magyarázat a GDPR-ról, i. m. 75. p.
42. Magyarázat a GDPR-ról, i. m. 81. p.

43. Magyarázat a GDPR-ról, i. m. 81. p.

44. További részletek „Az adatfeldolgozóra vonatkozó szabályok" és az „Adatfeldolgozói szerződés című" alfejezetekben.

45. Magyarázat a GDPR-ról, i. m. 80. p.

46. RÉVÉSZ Balázs – SOMOGYVÁRI Katalin: Az információszabadság jelentése, tartalma. In: Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban. Budapest : HVG-Orac, 2012. 180–182. p. – Idézi: Magyarázat a GDPR-ról. i. m. 95-96. p.

47. Magyarázat a GDPR-ról, i. m. 96. p.

48. JÓRI, i. m. 193. p.

49. Magyarázat a GDPR-ról, i. m. 111. p.

50. JÓRI, i. m. 14. p.

51. JÓRI, i. m. 143. p.

52. JÓRI, i. m. 145. p.

53. Magyarázat a GDPR-ról, i. m. 379. p.

54. 2011. évi CXCV. törvény az államháztartásról. https://net.jogtar.hu/jogszabaly?docid=A1100195.TV

55. Megjelent: Magyar Közlöny, 2018. 38. sz. 1773–1775. p.

56. JÓRI, i. m. 123. p.

57. JÓRI, i. m. 86. p.

58. Magyarázat a GDPR-ról, i. m. 2017. p.

59. A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2016. évi tevékenységéről. B/13846. Budapest : NAIH, 2017. 29. p.

60. JÓRI, i. m. 231. p.

61. 30. cikk szerinti nyilvántartás mintája 1. és 2. https://gdpr.hvgorac.hu/segedanyagok/ [2019. február 8.]

62. Magyarázat a GDPR-ról, i. m. 211. p.

63. Magyarázat a GDPR-ról. i. m. 367–368. p.

64. MAJTÉNYI (2006), i. m. 41. p.

Beérkezett: 2019. február 8.

Új magyar könyvtári szabvány

A Magyar Szabványügyi Testület az OSZK megbízásából és közreműködésével, az Országos Könyvtári Szabványosítási Bizottság munkaterve alapján új magyar nyelvű szabványt adott ki: „MSZ ISO 2789:2019 Információs és dokumentáció. Nemzetközi könyvtári statisztika"
Az Országos Széchényi Könyvtár és a Könyvtári Intézet közreműködésével jelenleg is zajlik több jelentős, a könyvtárügyet érintő nemzetközi szabvány teljes körű honosítása és közzétételük előkészítése. A honosításokra az OSZK OKR Projektjének keretében kerül sor.
A statisztikai szabvány magyar nyelvű kiadása elérhető a Könyvtári Intézet Könyvtártudományi Szakkönyvtárából:
https://ki.oszk.hu/hir/konyvtartudomanyi-szakkonyvtar/az-msz-iso-2789 2019-kszk-ban-hozzaferheto

Valóságos könyvtár – könyvtári valóság. Könyvtár- és információtudományi tanulmányok 2018

Az ELTE BTK Könyvtár- és Információtudományi Intézet Kiszl Péter és Csík Tibor szerkesztésében megjelentette az Intézet népszerű rendezvénysorozatának 2017. novemberi konferenciáján elhangzott előadások szövegét Valóságos könyvtár – könyvtári valóság. Könyvtár- és információtudományi tanulmányok 2018 címmel. A kötet elektronikus változata szabadon letölthető az ELTE Digitális Intézményi Tudástárból (EDIT):
https://edit.elte.hu/xmlui/handle/10831/40281

(Katalist, 2019. február 23. ELTE BTK LIS tájékoztatása alapján)
(És elérhető a Könyvtári Intézet Könyvtártudományi Szakkönyvtárából is.)