DOI 10.26521/Profuturo/1/2019/3877

Váradi Szilvia*

A közszférára vonatkozó adatvédelmi szabályok a GDPR tükrében

adatvédelem – GDPR – személyes adatok – közszféra – közhatalmi szervek

Az Európai Unió 2016-ban ért végére nagyszabású és majd kilenc évet felölelő adatvédelmi reformjának. Ennek legfőbb eredménye az Általános Adatvédelmi Rendelet (*General Data Protection Regulation,* a továbbiakban: GDPR),[1] amely kétéves felkészülési időt követően, 2018. május 25-én lépett hatályba. Az elmúlt időszakban a GDPR-ral kapcsolatban megjelent szakirodalmi munkák közül kevés foglalkozik a rendelet speciálisan a közszférára vonatkozó szabályozásával és az e területre gyakorolt hatásaival.[2] E területen több mint egy évvel a hatálybalépést követően is tapasztalható bizonytalanság, ezért jelen tanulmány célja a GDPR közszférára vonatkozó releváns szabályainak azonosítása és elemzése.

Mivel az Európai Unió jogalkotásra jogosult intézményei a GDPR-t rendeleti formában alkották meg, az automatikusan az uniós tagállamok nemzeti jogának részévé vált, és nem igényelt további implementációt. A rendelet mint közvetlen hatállyal bíró jogforrás többnyire nem igényel és nem is tűr a tagállam részéről belső átültető jogszabályt, mivel az esetlegesen az egyes tagállamok által beépített módosítások révén a rendelet egységes érvényesülésének és alkalmazásának követelménye sérülne.[3] A GDPR ugyanakkor lehetővé teszi a tagállamok számára, hogy a rendelet bizonyos szabályainak alkalmazását pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be.[4] Amennyiben ilyen szabályozás megalkotása kötelező, annak elmulasztása uniós jogi kötelezettség megszegésének minősül.[5]

* Dr. Váradi Szilvia egyetemi adjunktus, Szegedi Tudományegyetem Állam- és Jogtudományi Kar Nemzetközi Jogi és Európa-jogi Tanszék, varadiszilvia@juris.u-szeged.hu.

1 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg). HL L 119, 2016. 05. 04., 1–88.

2 Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018.; Jóri András–Soós Andrea Klára: *A GDPR magyarázata*. HVG-ORAC, Budapest, 2018.

3 Chalmers, Damian–Davies, Gareth–Monti, Giorgio: *European Union Law. Cases and Materials*. Cambridge University Press, Cambridge, 2010, 99.

4 GDPR Preambulum (10).

5 128/78. sz., *Az Európai Közösségek Bizottsága kontra Nagy-Britannia és Észak-Írország Egyesült Királysága* ügyben 1979. február 7-én hozott ítélet (ECLI:EU:C:1979:32).

1. A közszféra: közhatalmi szervek vagy testületek

A közszférában működő szervezetek nagy számban gyűjtenek és tárolnak adatokat, amelyek közül igen sok szenzitív adatnak minősül. Ugyanakkor a GDPR megalkotásakor a Tanács eredeti javaslata szerint nem szabályozták volna uniós szinten a közszféra általi személyes adatok kezelését, mivel az elsődleges cél a digitális egységes piac megteremtését elősegítő, tehát a magánszektorra vonatkozó szabályozás egységesítése volt. A Tanács ezért nemzeti szintű szabályozást javasolt a közszektorra nézve.[6] Az uniós jogalkotási folyamat során végül a Tanács finomított ezen az álláspontón, amelynek eredményeként a GDPR hatálya – számos kivétel megfogalmazása mellett – kiterjed erre a területre is.[7]

A GDPR értelmében „adatkezelő" alatt közhatalmi szerv, ügynökség vagy bármely egyéb szerv is értendő, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; „adatfeldolgozó" pedig a természetes vagy jogi személy mellett közhatalmi szerv, ügynökség vagy bármely egyéb szerv is lehet, amennyiben az az adatkezelő nevében személyes adatokat kezel.[8] Ezeken túl azonban a GDPR nem tartalmaz egyértelmű definíciót a „közszféra" vagy a „közhatalmi szervek vagy testületek" fogalmára nézve. A korábbi uniós adatvédelmi szabályozás, a 95/46/EK irányelv (a továbbiakban: 1995-ös adatvédelmi irányelv)[9] alapján létrehozott Adatvédelmi Munkacsoport[10] szerint az ilyen jellegű fogalmakat a nemzeti jog alapján kell meghatározni. A közhatalmi szervek vagy testületek magukban foglalnak minden nemzeti, regionális vagy helyi szintű hatóságot, és az adott alkalmazandó nemzeti jog értelmében tipikusan egy sor más közjogi jellegű szervet is. A közhatalmi feladat nemcsak közhatalmi szervek vagy testületek útján látható el, de más természetes vagy jogi személy által is mind közjogi, mind magánjogi szabályok alapján, leginkább olyan területeken, mint közösségi közlekedési szolgáltatások, víz- vagy energiaszolgáltatás, közútkezelés stb.[11] Ez utóbbi esetek nagyban hasonlítanak ahhoz, mint amikor az adatalany személyes adatait közhatalmi szervek vagy testületek kezelik, mivel ezek jellemzően kötelező, jogszabály alapján végzett adatkezelések, így az adatalanyoknak nincs vagy csak igen kevés beleszólásuk van adataik kezelésébe.

[6] Blume, Peter: The Public Sector and the Forthcoming EU Data Protection Regulation. *European Data Protection Law Review,* 2015/1, 32–38. (https://doi.org/10.21552/EDPL/2015/1/7).

[7] GDPR 2. cikk.

[8] GDPR 4. cikk (7) és (8).

[9] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. HL L 281, 1995. 11. 23., 31–50.

[10] Az ún. 29-es Munkacsoportot az 1995-ös adatvédelmi irányelv 29. és 30. cikkeinek megfelelően állították fel. Önálló uniós munkacsoport volt, amely a személyes adatok és a magánélet védelmével foglalkozott, 2018. május 25-én szűnt meg, mivel a GDPR létrehozta helyette az Európai Adatvédelmi Testületet, szintén független európai szervként. A Testület tagjai a nemzeti adatvédelmi hatóságok képviselői és az európai adatvédelmi biztos, székhelye Brüsszel. Hatáskörében eljárva általános iránymutatásokat és kötelező döntéseket is hozhat.

[11] Article 29 Data Protection Working Party: *Guidelines on Data Protection Officers ('DPOs').* 16/EN WP 243, 13 December 2016, 6. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (2019. 05. 15.).

A közhatalom gyakorlása közvetlenül jogszabályhoz kötött, jogszabály hozza létre a közhatalmi szervezetet, jogszabály ruházza fel cselekvési hatáskörrel, és jogszabály rögzíti az elérendő célokat is, amelyek érdekében az adott szerv a tevékenységét kifejti.[12] Ezt a jellemzőt a GDPR is megerősíti, amikor kimondja: a közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie.[13]

Magyarországon az általános forgalmi adóról szóló 2007. évi CXXVII. törvény értelmében közhatalom gyakorlására jogosult személy vagy szervezet az, akit vagy amelyet Magyarország Alaptörvénye, illetve a Magyarország Alaptörvényének felhatalmazása alapján megalkotott jogszabály hatalmaz fel a közhatalom gyakorlásának jogával. A törvény szerint közhatalmi tevékenység különösen *„a jogszabályalkotási, az igazságszolgáltatási, az ügyészi, a védelmi, a rendvédelmi, a külügyi és igazságügyi igazgatási, a közigazgatási jogalkalmazói, a hatósági ellenőrzési és pénzügyi ellenőrzési, a törvényességi felügyeleti és ellenőrzési, az államháztartási, európai uniós és egyéb nemzetközi támogatás elosztásáról való döntési tevékenység”*.[14] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) a közfeladatot ellátó szerv fogalmát használja, amely állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy lehet.[15]

A GDPR rendelkezései alapján azok a közhatalmi szervek, amelyek egy egyedi, konkrét közérdekű vizsgálat érdekében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek, ebben az esetben a GDPR nem alkalmazható.[16] Ilyen közhatalmi szervek lehetnek például az adó- és vámhatóságok, a pénzügyi nyomozóegységek, a független közigazgatási hatóságok, valamint az értékpapírpiacok szabályozásáért és felügyeletéért felelős pénzügyi hatóságok.[17]

A GDPR tartalmaz jogalapot *„a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak”* a kezelésére nézve, mivel megerősíti, hogy a büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet.[18] Az egyes hatáskörrel rendelkező, különösen rendőri és igazságügyi hatóságok általi személyes adatok kezelése azonban nem tartozik a GDPR tárgyi hatálya alá, ha az bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása

[12] Varga Zs. András: *Ombudsman, ügyész, magánjogi felelősség: Alternatív közigazgatási kontroll Magyarországon.* Pázmány Press, Budapest, 2012, 237.

[13] GDPR Preambulum (45).

[14] Áfatv. 7. § (1) és (2).

[15] Infotv. 26. § (1).

[16] GDPR Preambulum (31) és 4. cikk 9. pont.

[17] GDPR Preambulum (31).

[18] GDPR 10. cikk.

vagy büntetőjogi szankciók végrehajtása céljából valósul meg. Erre külön jogszabály alkalmazandó.[19]

A tagállamok azon közhatalmi tevékenysége is kivételt képez a GDPR hatálya alól, amelyet az uniós kül- és biztonságpolitika keretében fejtenek ki.[20] Ez a rendelkezés elsősorban a személyes adatoknak a tagállami külügyminisztériumok egységei és az azokhoz kapcsolódó külügyi szolgálatok általi kezelését veszi ki a tárgyi hatály alól, bár ebben az esetben a szerveknek a kivételhez igazolniuk kell, hogy a konkrét adatkezelés ténylegesen az uniós kül- és biztonságpolitikához kötődik.

Mindezek alapján a közszféra speciális tevékenységei során megvalósuló adatkezelésére, leginkább a felügyeleti, bűncselekmény felderítési és megelőzési jellegűekre a GDPR szabályai nem alkalmazhatók. Ezeket a helyzeteket célszerű a személyes adatok kezelésének megkezdése előtt tisztázni, elkülönítve azokat a közszféra egyéb gyakori adatkezelési tevékenységeitől, amelyekre viszont a GDPR szabályai teljes egészében vonatkoznak.

2. A személyes adat

A továbbiakban a személyes adat fogalmát célszerű áttekintenünk ahhoz, hogy láthatóvá váljék, mely adatok kezelése minősül védelem alatt állónak. Személyes adat alatt értünk bármely információt, amely egy természetes személyre, az ún. adatalanyra vonatkozik, aki ez alapján azonosíthatóvá válik. Ez az információ 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”* lehet.[21]

Míg az 1995-ös adatvédelmi irányelv azok részletezése nélkül az érintettre vonatkozó bármely információt személyes adatnak minősített,[22] a GDPR egyik fontos újítása, hogy kifejezetten személyes adatként nevesíti azokat is, amelyek a modern technológiák útján keletkeznek. A másik fontos megállapítás, hogy kizárólag a természetes személyekhez köthető személyes adatokat minősíti védendőnek, a jogi személyekre vonatkozókat nem, ez utóbbiakat a GDPR kifejezetten kizárja hatálya alól.[23] A jogi személyek személyes adatainak védelme nemzetközi szinten is megosztó kérdés. Míg az Európai Unió kifejezetten nem szabályozza, az Európa Tanács

[19] Az adatvédelmi reform másik eredménye, amely kifejezetten a rendőri és igazságügyi együttműködés keretében végzett adatkezelésre vonatkozó adatvédelmi szabályokat rögzíti, az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről. HL L 119, 2016. 05. 04., 89–131.

[20] GDPR 2. cikk (2) bekezdés *b)* pont.

[21] GDPR 4. cikk (1).

[22] 1995-ös adatvédelmi irányelv 2. cikk *a)* pont.

[23] GDPR Preambulum (14).

ugyanolyan szintű védelmet javasol,[24] mint a természetes személyek esetében.[25] A magyar Alkotmánybíróság gyakorlata azt mutatja, hogy a jogi személy adatvédelme az adatvédelmi törvény rendelkezéseivel összhangban nem biztosított, habár az alapjogok alkotmányos védelmét általában a jogi személyek is érvényesíthetik.[26]

A személyes adatok közül a GDPR értelmében tilos a különleges adatok kezelése, amelyek *„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".*[27] Ezek a szenzitív adatok, amelyek védelméhez fokozott egyéni és társadalmi érdekek kapcsolódnak. A rendelet csak néhány kivételt enged a tilalom alól – megfelelő garanciák betartásával. Ezek egyike, amikor az érintett az adatkezeléshez kifejezett hozzájárulását adja, ennek hiányában pedig akkor engedhető meg, amikor az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, az adatkezelés jelentős közérdek miatt szükséges, illetve amikor az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem.[28] Azok a közhatalmi tevékenységek, amelyek során szenzitív személyes adatokat kezelnek, a fenti esetekben megengedettek.

3. Az adatkezelés alapelvei

A GDPR egyik uralkodó, az adatkezelésre vonatkozó alapelve az ún. *célhoz kötöttség elve,* amely szerint a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, így azok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon.[29] Ez az elv az adatvédelem hagyományos elvének tekinthető, Magyarországon például az Alkotmánybíróság 15/1991. (IV. 13.) határozatával került be a jogrendszerbe.[30] A másik elv, amelyet a GDPR helyezett előtérbe, az *adattakarékosság elve,* miszerint a személyes adatoknak az adatkezelés célja szempontjából megfelelőnek és relevánsnak kell lenniük, és az ahhoz szükséges körre kell korlátozódniuk.[31] A közhatalmi szervek vagy testületek esetében a közérdek kivételt biztosíthat az utóbbi alól, még olyan esetekben is, amikor az adatalany kérte az adat törlését. A célhoz kötöttség elvének természetesen ebben az esetben

[24] *Bernh Larsen Holding AS és mások kontra Norvégia ügy,* 2013. március 14-i ítélet (ügyszám: 24117/08) 104. pont.

[25] Szoboszlai Judit: A jogi személyek adatvédelmével kapcsolatban felmerülő kérdések. *Collega,* 2002/3, 3.

[26] 34/1994. (VI. 24.) AB határozat, ABH 1994, 177, III. 2. pont.

[27] GDPR 9. cikk (1).

[28] GDPR 9. cikk (2).

[29] GDPR 5. cikk (1) bekezdés *b)* pont.

[30] 15/1991. (IV. 13.) AB határozat, ABH 1991, 40.

[31] GDPR 5. cikk (1) bekezdés *c)* pont.

is érvényesülnie kell – az adatkezelés minden szakaszában. Ily módon a cél nélküli, irreleváns adatok készletezése ezen elv alapján a közhatalmi szerveknél is kizárt. Mindezeket kiegészíti a *pontosság elve,* mivel a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük, ezért minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.[32] Gyakori probléma a tárolt személyes adatok helytállósága és minősége, amely a magánszektort sem kerüli el. Az adatbázisok és nyilvántartó rendszerek gyakran hatalmas mennyiségű elavult és szükségtelen adatot tartalmaznak. Ezért a GDPR alapján nemcsak kötelezettsége az adatkezelőknek, de a célszerűség is azt diktálja, hogy frissítsék és aktualizálják ezeket. Érdemes megjegyezni ezen a ponton, hogy a magyar adatvédelmi szabályozás európai szinten is igen magas színvonalúnak tekinthető, és a GDPR-ban foglalt szabályok nagy részét már korábban magában foglalta,[33] így például a fenti elveket már a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) is tartalmazta.

Rendkívül fontos, és szintén áthatja az új adatvédelmi rendelet egész szellemét, hogy a személyes adatok kezelése jogszerűen és tisztességesen, valamint az érintett számára átlátható módon történjen. Ahhoz, hogy ezt a célt meg lehessen valósítani, a GDPR 6. cikke szigorúan meghatározza az adatkezelés jogszerűségének feltételeit, vagyis az adatkezelés lehetséges jogalapjait. Ezek közül kizárólag a témánk szempontjából releváns jogalapokat elemezzük.

Az érintett adatalany *hozzájárulása*[34] a személyes adatok kezelésének legalapvetőbb jogalapja, azonban a közszféra szempontjából megkötésekkel alkalmazható. Az 1995-ös adatvédelmi irányelv szerint az érintett hozzájárulása önkéntes, egyértelmű és kifejezett kellett hogy legyen. A GDPR értelmében a hozzájárulásnak továbbra is kifejezettnek kell lennie,[35] amelynek konkrét és megfelelő, világosan és közérthetően megfogalmazott tájékoztatáson kell alapulnia.[36] Ugyanakkor a GDPR egyértelmű hozzájárulás alatt azt érti, amikor az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy a beleegyezését adja az adatkezeléshez.[37] Így az új szabályozás szigorúbb mivolta abban érhető tetten, hogy az adatalany tevőlegesen kell, hogy beleegyezését adja személyes adatainak kezeléséhez, passzív magatartással, nemtevéssel immáron nem tekinthető megadottnak a beleegyezés. A rendelet aktív magatartást vár el az adatalanyoktól, egyben felruházza őket azon jogosítványokkal, amelyek a személyes adataik feletti nagyobb kontrollt biztosítják számukra. Ezzel párhuzamosan elszámoltathatóvá teszi az adatkezelőket az adatkezelési folyamataik biztonságának garantálása tekintetében.

A közhatalmi szervek közhatalmi jogosítványaik gyakorlása során mindezektől eltekinthetnek a személyes adatok harmadik ország vagy nemzetközi szervezet ré-

[32] GDPR 5. cikk (1) bekezdés *d)* pont.
[33] Lásd az Infotv. korábbi módosításait.
[34] GDPR 6. cikk (1) bekezdés *a)* pont.
[35] GDPR 4. cikk 11. pont.
[36] GDPR 12. cikk (1).
[37] GDPR 4. cikk 11. pont.

szére történő továbbítása esetén, és nemcsak fontos közérdekre hivatkozással.[38] Ebben a rendelkezésben tetten érhető a vertikális viszony a tagállam és annak állampolgárai között a közhatalom gyakorlása során, amely a hozzájárulás önkéntességét is megkérdőjelezi. A magánszektor esetében a hozzájárulásnak alapvető jelentősége van az adatkezelés jogszerűsége szempontjából, a közhatalmi szervekre azonban ez a jogalap nem alkalmazandó, ameddig valóban a közhatalmi jellegű közérdekű adatkezelés keretei között végzik tevékenységüket. Továbbá az adatalany és az adatkezelő közötti szerződés teljesítésének jogalapja sem alkalmazandó a közhatalmi feladatot ellátó szervek esetében.[39]

A közszféra adatkezelésének jogszerűségéhez a következő jogalapok legalább egyikének alkalmazása elengedhetetlen: 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.[40]

A GDPR a *kötelező adatkezelés* eseteit is szabályozza. Ez akkor áll fenn, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges; vagy ha közérdekű, vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.[41] E jogalapokat az uniós jognak vagy azon tagállami jognak kell megállapítania, amelynek hatálya alá az adatkezelő tartozik. Ekkor az adatkezelés célját e jogszabályra hivatkozással kell meghatározni, és az adatkezelésnek egyben szükségesnek is kell lennie a közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához. Az uniós vagy tagállami jognak közérdekű célt kell szolgálnia, és arányosnak kell lennie az elérni kívánt jogszerű céllal.[42] A magyar Infotv. szerint kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.[43] Ez egyben azt is jelenti, hogy közérdekű adatkezeléskor nem követelmény az adatalany hozzájárulása, mivel az adatkezelés jogalapja a jogszabály által adott.

Kiemelendő, hogy a *jogos érdek* jogalapként nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.[44] Amennyiben csak ez a jogalap áll meg, a személyes adat nem kezelhető. Ezért az adatkezelés megkezdése előtt célszerű értékelni, mely jogalap lesz alkalmazható az adott esetre, sőt éppen a jogalkotó által a jogalap meghatározása során. Fontos megemlíteni például, hogy a helyi jogalkotó, így az önkormányzatok szűk mozgástérrel rendelkeznek a rendeletalkotásban és így a mérlegelésben: csak világos törvényi felhatalmazás

[38] GDPR 49. cikk (3), amely külön kivételi lehetőség a GDPR 49. cikk (1) bekezdés *d)* pontja alapján.
[39] GDPR 49. cikk (3).
[40] GDPR 6. cikk (1) bekezdés *c), d), e)* pontok.
[41] GDPR 6. cikk (1) bekezdés *c)* és *e)* pontok.
[42] GDPR 6. cikk (3).
[43] Infotv. 5. § (3).
[44] GDPR 6. cikk (1) bekezdés *f)* pont.

birtokában rendelhetik el a személyes adatok kezelését, ugyanis kötelező adatkezelés esetén a fentiekben leírtak alapján már törvényi szinten rendelkezni kell az adatkezelés legfontosabb körülményeiről.[45]

A fentieken túl közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból is folytatható adatkezelés megfelelő garanciák mellett és olyan technikai megoldásokkal, mint például az álnevesítés.[46]

4. Az adatalany jogai

A GDPR megalkotásának legfőbb célja egy erősebb és koherensebb adatvédelmi rendszer létrehozása volt az Európai Unióban, az adatkezelők felelősségére és a szabályozás hatékony kikényszeríthetőségére építve. Fontos emlékeztetni, hogy az adatvédelem első generációs szabályai az 1970-es években jelentek meg,[47] és elsősorban a számítógépes (és legalább részben automatizált) nyilvántartásokkal szemben igyekeztek védelmet biztosítani. Így az adatvédelmi jog kialakulása alapvetően az 1970-es évekre kibontakozó technológiai forradalomra adott válaszlépésként értékelhető.[48] Ez a jelenség napjainkban még inkább jellemző, a rendkívül gyors technológiai fejlődés következtében az adatalanyok (felhasználók) általában nem értik a technológiai eszközök és alkalmazások működését, és az ezen eszközökön folytatott adattovábbítás során nem látják át személyes adataik pontos útvonalát, azt, hogy adataikkal mi is történik. Ezért a GDPR megalkotásának további célja volt, hogy a természetes személyek maguk rendelkezhessenek személyes adataikkal, amely kapcsán viszont kiemelkedő jelentőséggel bír az infokommunikációs eszközökbe vetett bizalom megteremtése és megerősítése. A bizalom kérdése egyrészt az adatalany tevékenysége érdekében fontos, másrészt a digitális egységes piac fejlődése érdekében is alapvető. Ezen célok elérése érdekében a GDPR nagy hangsúlyt helyez a jogbiztonság és a gyakorlat biztonságának erősítésére az egyének, gazdasági szereplők és közhatalmi szervek tekintetében is.[49]

Az adatkezelőnek a személyes adatok kezelésének megkezdése előtt, az adatgyűjtés időpontjában minden releváns információt meg kell adnia az adatalanynak, tömör, átlátható, érthető és könnyen hozzáférhető tájékoztatás formájában, világosan és közérthetően megfogalmazva.[50] A rendelkezésre bocsátandó információk, így a *tájékoztatás* tekintetében a közhatalmi szervek a magánszférához képest nagyobb szabadsággal rendelkeznek az adatkezelést lehetővé tevő jogszabályi jogalapnak köszönhetően: az adatalannyal az adatkezelés jogalapját, illetve az adatke-

[45] Péterfalvi Attila (szerk.): *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC, Budapest, 2012, 95.

[46] GDPR 89. cikk (1).

[47] Magyarországon a Polgári Törvénykönyv 1977-es módosításában például a következő szerepelt: *„A számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat."* Lásd ehhez Péterfalvi: i. m., 50.

[48] Szőke Gergely László: *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*. HVG-ORAC, Budapest, 2015, 22–25.

[49] GDPR Preambulum (7).

[50] GDPR 12. cikk (1).

zelő (és – ha van ilyen – az adatkezelő képviselőjének) kilétét, elérhetőségeit, valamint az adatvédelmi tisztviselő elérhetőségeit kell közölni. Az adatvédelmi tisztviselő elérhetőségeit a felügyeleti hatóságnak is továbbítani kell.[51]

Az adatalany rá vonatkozóan gyűjtött személyes adataihoz való *hozzáférésének joga* az 1995-ös adatvédelmi irányelvben is szerepelt, ezzel növelve a személyes adatok feletti rendelkezés lehetőségét és az átláthatóságot. A GDPR értelmében az adatalany ennek keretében megismerheti különösen az adatkezelés céljait, ha lehetséges, az adatkezelés időtartamát, a személyes adatok címzettjeit, és újdonságként – legalább akkor, amikor az profilalkotásra épül – az adatkezelés következményeit.[52] Szintén újdonság, hogy minden adatalanynak joga van ún. érintetti hozzáférési kérést előterjeszteni az adott adatkezelőhöz (amely közhatalmi szerv is lehet), amely alapján az adatkezelőnek egy hónapon belül[53] kell a kért tájékoztatást megadnia.[54] A közhatalmi szervek számára is plusz adminisztratív terhet jelenthet mindez, egyrészt azért, mert hatalmas mennyiségű személyes adatot kezelnek, másrészt azért, mert ezt a hozzáférést az adatalany részére *„egyszerűen és észszerű időközönként”* kell biztosítani.[55] Ezen rendelkezés alapján kívánatos lenne a közszféra számára is, hogy áttekintse az adatkezelési folyamatait, a tárolt adatokat, valamint megfelelően felkészült és megfelelő ismerettel rendelkező munkatársakat jelöljön ki ezen hozzáférési kérések kezelésére.

A GDPR-ban rögzített, a pontatlan személyes adat indokolatlan késedelem nélküli helyesbítéséhez való jog[56] nem új joga az adatalanynak, mint ahogyan a törléshez való jog[57] sem, hiszen ezeket már az 1995-ös adatvédelmi irányelv és az 1992-es magyar Avtv. is tartalmazta. A törléshez való jog a „felejtés joga” vagy az „elfeledtetéshez való jogként” került a köztudatba az Európai Bíróság esetjogának[58] is köszönhetően. Az *elfeledtetéshez való jog* a közszféra adatkezelési tevékenysége során szintén kisebb szerepet játszik a magánszférához képest, mivel az adatalany nem kérheti személyes adatainak törlését az adatkezelés céljának meghiúsulása vagy a hozzájárulásának visszavonása esetén még akkor sem, ha az adatkezelésnek nincs más jogalapja. Ez a kivétel kifejezetten azokra az esetekre vonatkozik, amikor a személyes adatok kezelésére kötelező adatkezelés keretében kerül sor, vagyis az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése miatt, vagy közérdekből (ideértve a népegészségügy területét érintő közérdeket is), vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából[59] – az ilyen típusú adatkezelések pedig

[51] GDPR 13. cikk.
[52] GDPR Preambulum (63).
[53] GDPR Preambulum (59).
[54] IT Governance Privacy Team: *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Publishing, Ely, 2017, 222.
[55] GDPR Preambulum (63).
[56] GDPR 16. cikk.
[57] GDPR 17. cikk.
[58] C-131/12. sz., *Google Spain SL and Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* ügyben 2014. május 13-án hozott ítélet (ECLI:EU:C:2014:317).
[59] GDPR 17. cikk (3) bekezdés *b)* és *c)* pontok.

rendkívül gyakoriak a közszférában. A személyes adat törlése akkor sem kérhető, amennyiben az adatkezelés közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges.[60] Mindezek alapján azt mondhatjuk, hogy az adatkezelés megfelelő jogalapjának megválasztása kiemelkedően fontos, mivel a GDPR több kivételt és így nagyobb mozgásteret enged a közhatalmi szervek számára.

A fentiek alapján megállapítható, hogy az elszámoltathatóság és így a felelősség megállapításának alappilléreit jelentő, a magánszféra esetében hangsúlyos eszközök, azaz az érintetti hozzájárulás és az elfeledtetéshez való jog a közszféra tekintetében csekély jelentőséggel bírnak. Ezen alapvető eszközök kapcsán a magánszférára nézve a GDPR-nak nagyobb ösztönző hatása van az adatkezelési folyamatok áttekintésére és újragondolására, adott esetben újraszervezésére.

Az adatalany *adathordozhatósághoz való joga* a közszférára szintén nem alkalmazandó a közérdekű vagy az adatkezelő közhatalmi jogosítványai gyakorlásának keretében végzett adatkezeléskor, ekkor az adatkezelő nem köteles a hordozhatóságot biztosítani.[61] Az adathordozhatóság a magánszektorban is leginkább a szolgáltatóváltás kapcsán bír jelentőséggel, főleg a szerződéses kapcsolatokban, így ösztönzi a digitális egységes belső piac fejlődését is – de nem korlátozódik kizárólag erre az esetre.[62]

Az adatkezeléssel szembeni *tiltakozás jogát* azonban a GDPR kifejezetten a közérdekű vagy az adatkezelő közhatalmi jogosítványai gyakorlásának keretében végzett adatkezelés esetén teszi lehetővé, amely alól csak akkor mentesülhet az adatkezelő, ha bizonyítja, hogy az adatkezelést *„kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak”*.[63] A fentiekben láthattuk, hogy az érintetti hozzájárulás és a törléshez való jog a közhatalmi szervek esetében csekély jelentőségű, ennek ellensúlyaként azonban az adatkezeléssel szembeni tiltakozás joga éppen a közhatalmi tevékenységek esetén biztosított. Ezt a jogot ugyanakkor gyengíti, hogy a GDPR a tagállamok számára például ezen jog kapcsán pontosítások és eltérések elfogadását engedi, vagyis tagállami jogi eszközökkel a tiltakozás joga korlátozható a szükségesség és arányosság elveivel összhangban.[64]

5. Az adatkezelő felelőssége

Figyelemmel arra, hogy a GDPR az adatkezelők és adatfeldolgozók *elszámoltathatóságára* és felelősségére épül, és azt rendkívül részletesen tartalmazza, jelen tanulmány a közhatalmi szervek szempontjából releváns rendelkezésekre koncentrál.

[60] GDPR 17. cikk (3) bekezdés *d)* pont.

[61] GDPR 20. cikk.

[62] Article 29 Data Protection Working Party: *Guidelines on the right to data portability.* 16/EN WP 242, 13 December 2016, 3. https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf (2019. 05. 15.).

[63] GDPR 21. cikk (1).

[64] GDPR Preambulum (156) k.

A közhatalmi szervek és testületek mint adatkezelők számára is kötelező feladat a megfelelő technikai és szervezési intézkedések végrehajtása, azok felülvizsgálata és naprakésszé tétele annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik.[65] E körben a közszférára is teljes mértékben vonatkozik a két alapvető, az adatvédelem megfelelő szintjét garantálni hivatott technikai megoldás: a beépített[66] és az alapértelmezett adatvédelem.[67] Ezek megfelelő alkalmazásával elérhető, hogy a jog beépüljön a technológiába.

A *beépített adatvédelem* a személyes adatok legmagasabb szintű védelmét hivatott elérni az adatkezelési folyamatok megtervezése során, már a kezdettől fogva szavatolva a magánélet védelmét és az adatvédelmi alapelvek érvényesülését. Ez olyan intézkedésekkel, módszerekkel, illetve technikai megoldásokkal valósítható meg, amelyek az adott infokommunikációs rendszeren belül automatikusan a legmagasabb szintű védelmet garantálják, mint például a titkosítás, az álnevesítés vagy a hozzáférési jogosultság beállítása.[68] Az *alapértelmezett adatvédelem* esetén olyan adatkezelési folyamatot, technológiát, szolgáltatást alkalmaznak, amely eleve biztosítja az adatvédelmi megfelelőséget. Ezek használatával az adatvédelmi incidensek is elkerülhetővé válnak.[69]

A közhatalmi szervek számára is kötelezettség az adatkezeléshez olyan rendszerek és technológiák alkalmazása, amelyeket a beépített és az alapértelmezett adatvédelem elveinek megfelelően fejlesztettek és frissítettek. Ezért az alkalmazott intézkedéseknek és módszereknek is igazodniuk kell a végzett adatkezeléshez és a kezelt személyes adatok jellegéhez, a lehetséges adatkezelési kockázatokhoz. Az ilyen technológiák, szolgáltatások igénybevétele kapcsán a tanúsítási mechanizmusok, tanúsítványok, adatvédelmi címkék és jelzők segítségével az érintettek fel tudják mérni a biztosított adatvédelem szintjét.[70] Az adatvédelmi audit a magyar jogban nem újdonság, az Infotv. 2012 óta tartalmazza, és a magyar szakirodalom is régóta foglalkozik e témával.[71]

A GDPR új szabálya az is, hogy a magánszférához hasonlóan a közhatalmi szerveknek is írásbeli *nyilvántartást* kell vezetniük minden, a hatáskörükbe tartozó adatkezelési tevékenységről.[72] Ez a nyilvántartás nem nyilvános, az adatkezelő ezzel a GDPR-nak való megfelelést igazolja, így a hatáskörrel rendelkező felügyeleti hatóság számára kell kérésre rendelkezésre bocsátani.[73] Amit mindenképpen tartalmaznia kell a nyilvántartásnak, azok a következők: az adatkezelő neve és elérhetősége; az adatkezelés céljai; az érintettek kategóriáinak és a személyes adatok kategóriái-

[65] GDPR 24. cikk (1).

[66] GDPR 25. cikk (1).

[67] GDPR 25. cikk (2).

[68] Cavoukian, Ann: *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices,* 2–3. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (2019. 06. 25.).

[69] Lambert, Paul: *Understanding the New European Data Protection Rules*. CRC Press, Boca Raton, 2017, 339. (https://doi.org/10.1201/9781138069848).

[70] GDPR 42., 43. cikkek.

[71] Polyák Gábor–Szőke Gergely László: Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései. In: Drinóczi Tímea (szerk.): *Magyarország új alkotmányossága*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2011, 173–176.

[72] GDPR 30. cikk.

[73] GDPR 30. cikk (4).

nak ismertetése; a címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket; adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását.[74]

Az adatfeldolgozók esetében a nyilvántartásban az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái mellett az adatkezelés biztonsága érdekében alkalmazott technikai és szervezési intézkedések általános leírását is rögzíteni kell.[75] Ezeknek az információknak egyrészt az adatvédelmi kockázat felmérésében van kiemelkedő szerepe,[76] másrészt mindezen információk birtokában képes a hatáskörrel rendelkező felügyeleti hatóság megítélni a személyes adatok kezelésének jogszerűségét, és egy esetleges incidens esetén róla dönteni. Magyarországon ez a hatáskörrel rendelkező felügyeleti hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH).

A GDPR kifejezetten előírja az adatkezelők és adatfeldolgozók számára a felügyeleti hatósággal való *együttműködési kötelezettséget* annak megkeresése alapján.[77] Ez az együttműködés magában foglalja az adatkezelő *bejelentési kötelezettségét* adatvédelmi jogsértés, ún. adatvédelmi incidens esetén, indokolatlan késedelem nélkül, de legkésőbb az incidensről való tudomásszerzéstől számított 72 órán belül. A bejelentés alól kivételt képez az az eset, amikor az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.[78] Kiemelendő, hogy az adatkezelő által vezetett nyilvántartásban az adatvédelmi incidenseket is rögzíteni kell, feltüntetve az azokhoz kapcsolódó tényeket, azok hatásait és az orvoslásukra tett intézkedéseket, szintén a felügyeleti hatóság ellenőrzése esetére.[79]

Az új szabályozás adatbiztonságra vonatkozó további alapvető technikai eszköze, amelyről az adatkezelőnek kell gondoskodnia, az *adatvédelmi hatásvizsgálat*. Ez egy olyan analízist jelent, amelynek célja még az adatkezelés megkezdése előtt feltárni az adatvédelmi hiányosságokat, azt, ha az adatkezelés nincs összhangban a GDPR előírásaival, és ha az adatkezelés *„valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve",* leginkább valamely új technológia alkalmazása során.[80] Hatásvizsgálatot különösen akkor kell végezni, ha természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése történik, amely automatizált adatkezelésen (ideértve a profilalkotást is) alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek; ha különleges (szenzitív) adatok[81] vagy a büntetőjogi felelősség meg-

[74] GDPR 30. cikk (1).
[75] GDPR 30. cikk (2) bekezdés *b)* és *d)* pontok.
[76] Kazemi, Robert: *General Data Protection Regulation (GDPR)*. Tredition, Hamburg, 2018, 78.
[77] GDPR 31. cikk.
[78] GDPR 33. cikk.
[79] GDPR 33. cikk (5).
[80] GDPR 35. cikk (1).
[81] GDPR 9. cikk (1).

állapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok[82] nagy számban történő kezelése valósul meg; vagy nyilvános helyek nagymértékű, módszeres megfigyelése esetén.[83]

A felügyeleti hatóság (Magyarországon tehát a NAIH) összeállítja azon adatkezelési műveletek típusainak listáját, amelyek esetén mindig kell hatásvizsgálatot végezni, és azok listáját is, ahol nem kell.[84] Ugyanakkor még a fenti esetekben sem kell hatásvizsgálatot készíteni, amennyiben az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítése,[85] vagy közérdekű, vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtása érdekében szükséges,[86] és ezen jogalapokat uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, amely a konkrét adatkezelési műveletet is szabályozza, és e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot. Látható, hogy ezen kivétel is a közszférának kedvez: az ilyen jellegű adatkezelés esetén csak akkor kell hatásvizsgálatot készíteni, ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják.[87]

Mindazonáltal a magas szintű adatbiztonság megvalósítása érdekében a közhatalmi szervek számára is javasolt megtervezni és áttekinteni az adatkezelési folyamataikat, leginkább akkor, amikor az adatkezeléshez új technológiát vesznek igénybe. Ekkor azok a személyek is azonosíthatóvá válnak, akik az adatkezelést ténylegesen végzik, tehát hozzáférésük van a személyes adatokhoz. Az ő esetükben célszerű a megfelelő szakmai felkészítés arról, hogyan tudják az adatok védelmét biztosítani a jogosulatlan hozzáféréssel szemben.[88]

Amennyiben felmerülne, hogy az adatkezelés magas kockázatokkal jár, az adatkezelő konzultáció formájában a felügyeleti hatóság (NAIH) segítségét kérheti, amely a megkereséstől számított 8 héten belül írásban tanácsot ad, hogyan kezelje az adatkezelő a szituációt és milyen intézkedéseket tegyen.[89]

A fenti kivételekkel és a magánszektorra vonatkozó szabályokkal ellentétben éppen a közhatalmi szervekkel vagy – a bíróságok kivételével – egyéb, közfeladatot ellátó szervekkel szemben megfogalmazott kötelezettség az *adatvédelmi tisztviselő* (*data protection officer,* a továbbiakban: DPO) kijelölése. Több ilyen szerv számára közös adatvédelmi tisztviselő is kijelölhető, az adott szervek szervezeti felépítésének és méretének figyelembevételével. Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait, akit szakmai rátermettség és különösen az adatvédelmi jog

[82] GDPR 10. cikk.

[83] GDPR 35. cikk (3).

[84] GDPR 33. cikk (4) és (5). A NAIH által közzétett hatásvizsgálati lista: https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (2019. 07. 01.).

[85] GDPR 6. cikk (1) bekezdés *c)* pont.

[86] GDPR 6. cikk (1) bekezdés *e)* pont.

[87] GDPR 35. cikk (10).

[88] Az alapvető elektronikus adatbiztonsági kritériumokhoz lásd a 2013. évi L. törvényt az állami és önkormányzati szervek elektronikus információbiztonságáról.

[89] GDPR 36. cikk (1) és (2).

és gyakorlat szakértői szintű ismerete és a feladatra való alkalmasság alapján kell kijelölni.[90] A NAIH több állásfoglalása érinti az adatvédelmi tisztviselők kijelölésének egyes kérdéseit, így tisztázzák az adatkezelői szerepet a helyi önkormányzat és a polgármesteri hivatal viszonylatában, az adatvédelmi tisztviselő kijelölésére vonatkozó kötelezettség címzettjét,[91] illetve foglalkoznak az adatvédelmi tisztviselő képzettségével, végzettségével is.[92] A NAIH megerősítette, hogy közfeladatot nemcsak közhatalmi szerv láthat el, hanem a közjog vagy magánjog hatálya alá tartozó egyéb természetes és jogi személyek is, ahol a magánjogi szervezetek esetében – noha a GDPR alapján nem kötelező – jó gyakorlat lehet adatvédelmi tisztviselő kijelölése.[93]

A DPO feladatai közé tartozik az adatkezelővel, adatfeldolgozóval való együttműködés, illetve mind a szervezet, mind annak munkavállalói kérésére a tanácsadás a GDPR-nak való megfelelésről. A személyes adatok megőrzéséhez, tárolásához, dokumentálásához változtatásokat javasolhat, kitérve az infokommunikációs technológiák különböző formáinak (pl. hardver, szoftver, felhő számítási rendszerek stb.) alkalmazására.[94] Az adatvédelmi tisztviselő felel az adott szerv és a felügyeleti hatóság közötti kommunikációért is. Feladatai teljesítésével kapcsolatban titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség terheli.[95] A tagállamok további szabályokat határozhatnak meg nemzeti szabályozásukban, például az adatvédelmi tisztviselő regisztrálását. Ez Magyarországon az Adatvédelmi Tisztviselő Bejelentő Rendszer, amely a NAIH honlapjáról elérhető.[96]

A fenti szabályokon túlmenően a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása során is tapasztalhatunk eltéréseket. Az ilyen adattovábbításhoz nem szükséges külön engedély, ha az Európai Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő szintű védelmet biztosít. Ezek listáját a Bizottság az Európai Unió Hivatalos Lapjában és annak honlapján teszi közzé.[97] A Bizottság határozata hiányában csak megfelelő garanciák mellett történhet az adattovábbítás, mint például a közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz megléte.[98] Mindezek hiányában pedig akkor továbbítható az adat, ha az adattovábbítás fontos közérdekből szükséges; vagy az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges; az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges; vagy a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájé-

[90] GDPR 37. cikk.
[91] NAIH/2017/5364/2/V. számú állásfoglalás.
[92] NAIH/2017/5890/2/V. és NAIH/2018/204/2/V. számú állásfoglalások.
[93] NAIH/2018/0731/2/V. számú állásfoglalás.
[94] Lambert, Paul: *The Data Protection Officer: Profession, Rules, and Role*. CRC Press, Boca Raton, 2017, 46. (https://doi.org/10.1201/9781315396743).
[95] GDPR 38. cikk (5).
[96] https://dpo-online.naih.hu/ (2019. 08. 19.).
[97] GDPR 45. cikk.
[98] GDPR 46. cikk (2) bekezdés *a)* pont.

koztatását szolgálja. Megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozhatja bizonyos kategóriákba tartozó személyes adatok továbbítását valamely harmadik országba vagy nemzetközi szervezethez.[99]

Az érintett adatalany *jogorvoslattal* élhet az adatkezeléssel szemben, amely magában foglalja egyrészről a panasztételi jogot, másrészről amennyiben az adatkezelő vagy az adatfeldolgozó közhatalmi szerv, úgy annak tevékenységi helye szerinti tagállam bírósága előtti eljárás megindításának jogát.[100] A GDPR-t sértő adatkezelés és a felelősség megállapítása esetén az adatkezelőt kártérítési kötelezettség terheli. A *közigazgatási bírságok* tekintetében a GDPR szintén tartalmaz kivételt, ugyanis minden tagállam megállapíthatja az arra vonatkozó szabályokat, hogy az adott tagállami székhelyű közhatalmi vagy egyéb, közfeladatot ellátó szervvel szemben kiszabható-e közigazgatási bírság, és ha igen, milyen mértékű.[101] A magyar Infotv. szerint a bírság mértéke százezertől húszmillió forintig terjedhet, ha költségvetési szerv a bírság megfizetésére kötelezett, tehát a magyar jogalkotó rendelkezése szerint a költségvetési szervekkel szemben is kiszabható bírság.

A NAIH mindezidáig két alkalommal szabott ki adatvédelmi bírságot a közszférába tartozó szervvel szemben, mindkettőt adatvédelmi incidens miatt: 2019. február 28-án kelt határozatában Kecskemét Megyei Jogú Város Polgármesteri Hivatalával szemben egymillió forint összegben, 2019. június 25-én kelt határozatában a Budapesti Rendőr-főkapitánysággal[102] szemben ötmillió forint összegben. Az első esetben a NAIH megállapítása szerint az adatkezelő jogellenesen járt el, mivel jogalap nélkül adta át az érintett személyes adatait tartalmazó közérdekű bejelentését harmadik személy részére, aki így jogosulatlanul fért hozzá azokhoz.[103] A második esetben a rendőr-főkapitányság nem tett eleget egy személyes adatokat tartalmazó pendrive elvesztésével okozott adatvédelmi incidens határidőn belüli bejelentési kötelezettségének.[104]

6. Összegzés

Az új uniós adatvédelmi rendelet, a GDPR kiemelt figyelmet szentel a közszférában megvalósuló adatkezelésnek. A magánszektorhoz képest több eltérést és kivételi lehetőséget is tartalmaz, így a közhatalmi tevékenységet ellátó szerveknek és testületeknek tudatában kell lenniük ezeknek a speciális szabályoknak, mielőtt az általános szabályokat alkalmaznák. Az új uniós adatvédelmi rezsim célja az adatalany középpontba helyezése a személyes adatai feletti ellenőrzési joga hangsúlyozásával. Noha az ezt biztosító jogok közül több nem alkalmazható a közhatalmi szervek-

[99] GDPR 49. cikk.

[100] GDPR 77. és 79. cikkek.

[101] GDPR 83. cikk (7).

[102] A BRFK is költségvetési szerv, amelyre az Infotv. 61. § (4) bekezdés *b)* pontja alapján legfeljebb 20 millió forintig terjedő bírság szabható ki a GDPR 83. cikkével összhangban.

[103] NAIH/2019/596. számú határozat.

[104] NAIH/2019/2471/6. számú határozat.

re, azoknak mégis az adatalany érdekeinek szem előtt tartásával és az adatbiztonság garantálásával kell ellátniuk tevékenységüket. Az új szabályozás új esélyt jelent a közszféra számára is, hogy felülvizsgálja adatkezelési folyamatait, technológiáit és erőforrásait, és hatékonyabb, megbízhatóbb és egyben biztonságosabb közszolgáltatást nyújtson. Nem kétséges, a GDPR nagy kihívást jelentett minden szervezet számára, és nyugodtan mondhatjuk, hogy mind a mai napig vannak még teendők a rendeletnek való megfelelés érdekében.

Abstract

The European Union has finished the reform of the European data protection rules, and the main result is the General Data Protection Regulation (GDPR),[105] which entered into force after a two-year period on 25 May 2018. The GDPR draws special attention to the protection of personal data not only in the private, but also in the public sector. It introduces several significant changes and restrictions, but after almost a year of being in force, there are still some uncertainty how we can apply its provisions, especially for public authorities and bodies. Therefore, the aim of this paper is to explore the relevant data protection provisions of GDPR regarding the public sector and to clarify any misunderstandings in this field.

[105] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4.5.2016, 1–88.