Debreceni Jogi Műhely 2018. (XV.) 1-2.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen
(University of Debrecen, Faculty of Law, Debrecen)
DOI 10.24169/DJM/2018/1-2/8

Tóth Fanni

gyámügyi szakügyintéző
Szabolcs-Szatmár-Bereg Megyei Kormányhivatal, Nyíregyházi Járási Hivatal

A GDPR-RÓL – KÜLÖNÖS TEKINTETTEL A KÖNYVTÁRAKRA ÉS LEVÉLTÁRAKRA

Debreceni Jogi Műhely, 2018. évi (XV. évfolyam) 1-2. szám (2018. július 8.)

DOI 10.24169/DJM/2018/1-2/8

About the GDPR – focusing on libraries and archives – Summary

Nowadays data has become one of the most important value which raises the question of protecting personal data. The European Union responds to the challenge by legal instruments: since 25 May 2018 it has been obligatory for the member states to apply GDPR. In the article, first I study the novelties of GDPR. Then I examine to what extent the provisions apply to libraries and archives.

The novelties can be divided into several larger groups. Some of them belong to the data subjects (data portability, right to be forgotten, pseudonymisation), the other parts are principles like data protection by design and by default or the closely related accountability principle. The Regulation also introduces a new legal institution, the data-protection impact assessment and requires the notification of personal data breach. Concerning the expected impacts, it is clear that the Regulation strengthens the rights of the data subjects but imposes new obligations on data controllers and strengthens the role of control. GDPR is a determinative law for the undertakings and business life, and it must also be applied by libraries and archives. For archiving purposes in the public interest, however, the Regulation allows for exemptions concerning libraries and archives. The provisions require libraries and archives to identify the risks that may occur while processing personal data as well as to examine their regulations.

Bevezetés

Szinte naponta érezzük, hogy minden felgyorsult körülöttünk. Nehéz a lépéstartás, nagy a kihívás, egyre sürgetőbbek a határidők, és egyre bonyolultabbak a feladatok. Így van ez az iskolában és a munkahelyen, a vállalkozásokban és a közszférában is. Rettegett dátum, de két éve tudjuk, hogy eljön: 2018. május 25-étől alkalmazni kell az Általános adatvédelmi rendeletet[1] (a továbbiakban: GDPR). Gyakran járok könyvtárba, levéltárba, így hamar bevillan a kérdés: az adatok kimeríthetetlen tárházaira vonatkozik-e a rendelet, mennyiben, és vajon milyen problémákkal kell megküzdeniük? Dolgozatomban áttekintem a GDPR új elemeit, és vizsgálom a könyvtárak, levéltárak helyzetét a rendelet alapján. Az említett intézményekben lehetséges kockázati tényezőket egy konkrét jogeset alapján elemzem.

Az adatvédelemnek abban a korszakában élünk, amelyben meghatározó szerep jut a hatalmas adatmennyiségnek, a változatos adattípusoknak és a gyors adatfeldolgozásnak; ezt a jelenséget összefoglaló néven Big Data[2] névvel is illetik. Mivel a digitalizáció és a globalizáció nem ismer határokat, ezért az adatvédelemnek egységesnek és szilárdnak kell lennie,[3] más megközelítésben a Big Data-jelenséget az EU

[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 irányelv hatályon kívül helyezéséről (Általános adatvédelmi rendelet). Angol nyelven: General Data Protection Regulation, betűszóval: GDPR.
[2] 1998-ban alkotta John Mashey.
[3] Horváth Eszter: Péterfalvi Attila – Egységes európai adatvédelem. http://www.jogiforum.hu/interju/171 (letöltés: 2018. 05. 03.)

DOI 10.24169/DJM/2018/1-2/8

jogérvényesítési, ellenőrzési, betartatási, kikényszerítési problémának tekinti…[4], és a jog eszközeivel válaszol rá. Míg azonban korábban irányelv szabályozta az adatvédelmet, 2016-ban rendelet született, amelyet kötelező alkalmazni. Az irányelv a tagállamok számára határoz meg elérendő szabályozási célokat, de a tagállamok eltérő módon ültethetik át a saját jogrendszerükbe, azaz szabadon választják meg az eszközöket és a módszereket; a rendeletek azonban közvetlenül alkalmazandók, tehát további tagállami aktus nélkül a tagállamok jogának részévé válik. Ez azzal jár, hogy szükséges a kapcsolódó jogszabályokat módosítani, hazánkban például az információs önrendelkezési jogról és az információszabadságról szóló törvényt (a továbbiakban: Infotv.).[5]

1. A GDPR-ról

A GDPR területi hatálya kiterjed minden olyan adatkezelőre, amely az EU területén belül tényleges tevékenységet végez, és személyes adatokat kezel, függetlenül a székhelyétől. Ez azt jelenti, hogy a jogszabály nemcsak az EU-polgárok jogait védi, hanem az EU területén tartózkodó bármely más személy adatait is. Másrészt az olyan adatkezelőkre is kiterjed, amelyek uniós polgárok adatait kezelik bárhol a világon.[6] A GDPR hatálya kiterjed a felhő alapú szolgáltatásokra is, hiszen a rendelkezéseket az adatkezelőkre és az adatfeldolgozókra is alkalmazni kell. A felhőszolgáltatások esetében olyan adatkezelő–feldolgozó közötti kapcsolat jön létre, amelyben a fogyasztó (a szolgáltatás megrendelője) minősül adatkezelőnek, a számításifelhő-szolgáltató pedig adatfeldolgozónak.[7]

A GDPR több új elemet, fogalmat, intézményt vezet be az adatvédelmi szabályozás körébe. Az érintettre vonatkozó új fogalmak: az adathordozhatóság, az elfeledtetéshez való joga, valamint az álnevesítés. Az adathordozhatósághoz való jog az érintett jogainak bővülését jelenti. Ha az érintett hozzájárult például egy szolgáltatónál az adatai kezeléséhez, akkor joga van ahhoz is, hogy a digitális formában kezelt adatát elkérje; vagy kérheti azt is, hogy azt az adatkezelők közvetlenül továbbítsák egymásnak.[8] Ez az átjárhatóság már a modern környezetben, a felhő alapú szolgáltatások és okos eszközök világában ragadja meg az információs önrendelkezés lényegi tartalmát: személyes adatainknak, mint a hozzánk tartozó „csomagnak" az útját mi magunk határozzuk meg.[9]

Szintén az érintett jogainak bővülését jelenti az elfeledtetéshez, azaz a törléshez való jog. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje.[10] Alapvetően ez nem újítás, hisz a törléshez való jogot az Infotv. is tartalmazza,[11] de a GDPR szabályozásában szereplő elfeledtetési jog erősebb jogosítvány. Az adathordozhatósággal összefüggésben az adatkezelőnek nemcsak törölnie kell a személyes adatot, hanem – ha azt nyilvánosságra hozta – az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tennie az észszerűen elvárható lépéseket annak érdekében, hogy tájékoztassa a további adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.[12]

Az álnevesítés a személyes adatok olyan módon történő kezelése, amelynek következtében további

[4] Ződi Zsolt: Privacy és a Big Data. In: Fundamentum, 2017. 1–2. sz., 27. o. http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf (letöltés: 2018. 05. 04.)
[5] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
[6] GDPR 3. cikk.
[7] A 29. cikk szerinti adatvédelmi munkacsoport 01037/12/HU WP 196. 05/2012. számú vélemény a számítási felhőről.
[8] GDPR 20. cikk (1)–(2) bekezdés.
[9] Szabó Endre Győző – Révész Balázs: Adataink biztonságban – adatainkban a biztonság? In: Információs Társadalom, 2017 (17. évf.) 1. sz., 53. o.
[10] GDPR 17. cikk (1) bekezdés. A törlés indokait az a)–f) pontok tartalmazzák.
[11] Infotv. 3. § 8. pont.
[12] Póczek Aliz: Kevesebb mint egy év, és alkalmazandó lesz az adatvédelmi rendelet, 3. https://www.drtivadar.hu/adatvedelem/kevesebb-mint-egy-ev-es-alkalmazando-lesz-az-adatvedelmi-rendelet-iii-resz/ (letöltés: 2018. 05. 03.)

DOI 10.24169/DJM/2018/1-2/8

információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik,[13] azaz elszakad egymástól az adat és az érintett. Hogy a köztük lévő kapcsolat ne legyen helyreállítható, annak az a feltétele, hogy az álnevesített adatok feloldásához szükséges további információt a kezelt adatoktól elkülönítve tárolják. Az álnevesítés előnye, hogy csökkentheti az érintettek számára az adatkezeléssel járó kockázatokat, valamint segítheti az adatkezelőket és az adatfeldolgozókat az adatbiztonság garantálásában, így például egy adatvédelmi incidens esetén a jogellenesen nyilvánosságra hozott, de álnevesített adatokból az érintettek kiléte nem lesz megállapítható.[14] Gyakorlati eset az álnevesítésre, ha például egy fogyasztói adatbázisban az egyes adatsorok egyedi kódokhoz vannak hozzárendelve, és ezeknek a kódoknak a kulcsa egy elkülönített adatbázisban (vagy akár más szerveren) kerül tárolásra. Az adatok tehát integráltan megmaradnak, ám ahhoz, hogy egyes valós személyekhez (és ne csak kódnevekhez) lehessen azokat hozzárendelni, szükség van egy biztonságosan és külön tárolt kódra is.[15]

A GDPR talán leghangsúlyosabb újdonságai: a beépített és alapértelmezett adatvédelem, valamint az ezzel szorosan összefüggő elszámoltathatóság elve. Míg korábban a vállalkozások, szervezetek rutinból alkották meg, illetve másolták egymás személyesadat-kezelésre vonatkozó dokumentumait, ez a GDPR kötelező alkalmazása során nem fordulhat elő, hiszen az adatkezelőnek az adott szervezetre kell szabnia, az egyedi sajátosságok, jellemzők alapján kell kidolgoznia az adatkezelés rendszerét. A beépített adatvédelem azt jelenti, hogy az adatkezelő úgy tervezi meg és úgy alakítja ki az adott szervezet adatkezelési módját, hogy egyrészt figyelembe veszi a tudomány, a technológia állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait; másrészt elemzi, azonosítja és figyelembe veszi a természetes személyek jogaira jelentett kockázatokat. Az alapértelmezett adatvédelem elvárása alapján az adatkezelőnek megfelelő intézkedést kell kidolgoznia annak érdekében, hogy a szervezet csak az adott konkrét adatkezelési cél szempontjából szükséges személyes adatot kezeljen, mind mennyiségileg, mind a kezelés mértékére, a tárolás időtartamára és hozzáférhetőségére vonatkozóan. Mindez azt a célt szolgálja, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak meghatározatlan számú személy számára hozzáférhetővé.[16] Egyszerű példaként említhető a vállalat, szervezet által hirdetett állásra a jelentkezők által küldött önéletrajzok, motivációs levelek tárolása. Ha megszűnik a jogalap, vagyis a felvételi eljárás, az adatokat sem szabad tovább tárolni. A GDPR előírásai alapján az adatkezelés teljes folyamata meghatározott rend, tervezés alapján kell történjen, nem pedig esetlegesen.

A GDPR-ban az elszámoltathatóság elve szerint az adatkezelő felelős az adatvédelmi alapelveknek való megfelelésért, és képesnek kell lennie e megfelelés igazolására is.[17] Előzményeként említhető a felelősségre vonhatóság alapelve, amely már az OECD adatvédelmi irányelvben is megjelent,[18] és az Infotv. is utal rá.[19] Ehhez képest a GDPR az elszámoltathatóság elvét alapelvi szintre emelte, és középponti szerepet adott neki, ezért emlegetik szuperalapelvként.[20]

Azok a szervezetek, amelyek nem felelnek meg a GDPR előírásainak, 20 millió euróig vagy a vállalkozás teljes árbevételének 4%-áig terjedő közigazgatási bírságra számíthatnak.[21]

A személyes adatok kezeléséből a természetes személyek jogait és szabadságait érintő – változó

[13] GDPR 4. cikk 5. pont.
[14] Póczek i. m.
[15] Az új uniós Általános Adatvédelmi Rendelet bevezetésének hatásai a magyar adatvezérelt marketing szakma hétköznapjaira. https://adatvezereltmarketing.files.wordpress.com/2016/11/gdpr-gyakorlati-tagi-kerdesek-2016.pdf (letöltés: 2018. 05. 03.)
[16] GDPR 25. cikk (1)–(2) bekezdés.
[17] GDPR 5. cikk (2) bekezdés.
[18] A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvek, 1980. 14. pontja: Az adatellenőrző legyen felelősségre vonható, hogy azon intézkedések szerint jár-e el, melyek a fenti alapelveknek érvényt szereznek.
[19] Infotv. 23. §.
[20] Az adatvédelem „szuperalapelve" – az elszámoltathatóság. http://gdpr.blog.hu/2017/06/14/az_adatvedelem_szuperalapelve_az_elszamoltathatosag (letöltés: 2018. 05. 03.)
[21] GDPR 83. cikk.

DOI 10.24169/DJM/2018/1-2/8

valószínűségű és súlyosságú – kockázatok származhatnak, amelyek fizikai, vagyoni vagy nem vagyoni károkat okozhatnak.[22] Az adatkezelőnek meg kell állapítania, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, a kockázatokat fel kell tárnia, be kell azonosítania, forrásukat, jellegüket, valószínűségüket és súlyosságukat fel kell mérnie, és a mérséklésükre szolgáló intézkedéseket kell tennie.[23] A GDPR különbséget tesz kockázat és magas kockázat között. A kockázat valószínűségét és súlyosságát objektív értékelés alapján kell felmérni,[24] ebben segítséget nyújtanak a jóváhagyott magatartási kódexek, tanúsítási eljárások, az adatvédelmi tisztviselő (ahol van) és a 29. cikk alapján létrehozott adatvédelmi munkacsoport[25] iránymutatása. A magas kockázat kezelésére a rendelet új jogintézményt vezet be, az adatvédelmi hatásvizsgálatot. Az adatvédelmi hatásvizsgálat az adatkezeléssel kapcsolatos döntések meghozatalát segítő eszköz,[26] az adatkezelést megelőzően kell elvégezni,[27] és hozzájárul a beépített és alapértelmezett adatvédelem elvének érvényesüléséhez.

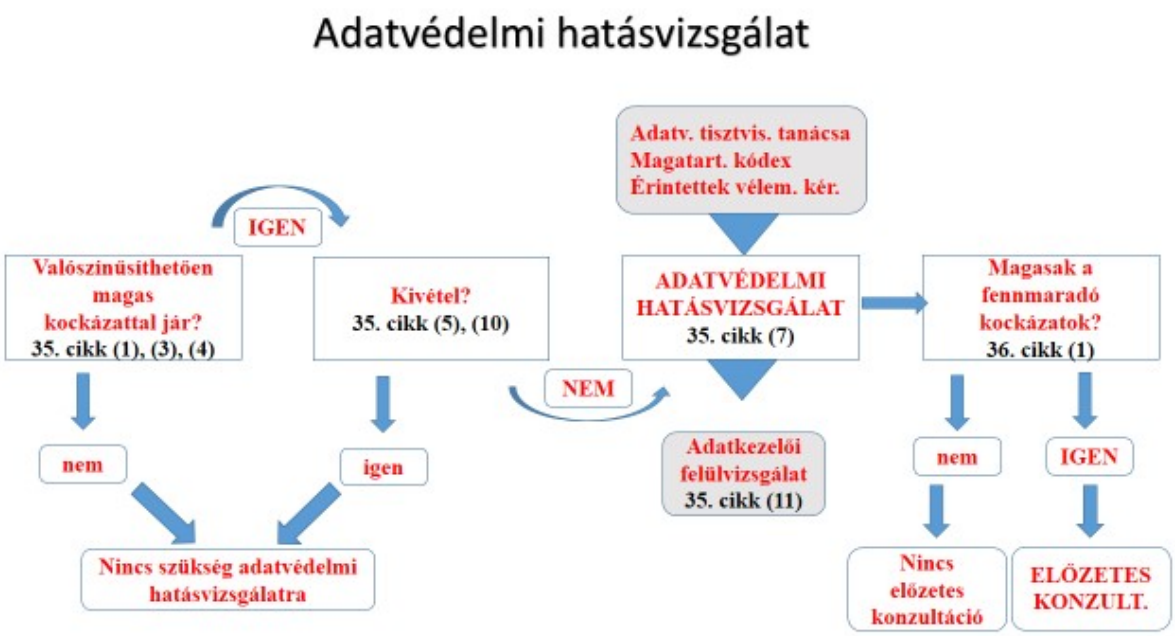
Az adatvédelmi hatásvizsgálat tárgya lehet egyetlen adatkezelési művelet, de az egymáshoz hasonló típusú műveletek egyetlen vizsgálat keretében is értékelhetők. Gazdaságos lehet ez akkor, ha közfeladatot ellátó szervek közös alkalmazást vagy adatkezelési felületet kívánnak létrehozni, de akár valamely ágazat vagy szegmens tekintetében is. Egyetlen vizsgálat elegendő több, a kockázat szempontjából egymáshoz hasonló adatkezelési művelet értékeléséhez is, például egy vasúttársaságnak az összes vasútállomásán végzett videokamerás megfigyelésre vonatkozóan.[28] Mivel a különböző gazdasági ágazatok személyesadat-kezelési műveletei az ágazat jellegéből következően különbözhetnek egymástól, az adatvédelmi munkacsoport szorgalmazza az ágazatspecifikus adatvédelmi hatásvizsgálati keretek kidolgozását.[29]

Az adatkezeléssel összefüggésben – a személyes adatok védelme érdekében – a következő kérdésekre adott válaszok mentén rajzolódnak ki a folyamat lépései.

1. ábra: Az adatvédelmi hatásvizsgálat folyamatának lépései

[22] GDPR (75) preambulumbekezdés.
[23] GDPR (76), (77) és (83) preambulumbekezdés.
[24] GDPR (76) preambulumbekezdés.
[25] A 95/46/EK irányelv 29. cikke alapján létrehozott munkacsoport, amelyet a szélesebb jog- és feladatkörökkel bíró Európai Adatvédelmi Testület fog felváltani.
[26] A 29. cikk alapján létrehozott adatvédelmi munkacsoport WP 248: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e (a továbbiakban: WP 248), 17. o.
[27] GDPR 35. cikk (1) és (10) bekezdés.
[28] WP 248, 8. o.
[29] WP 248, 20–21. o.

Debreceni Jogi Műhely 2018. (XV.) 1-2.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen
(University of Debrecen, Faculty of Law, Debrecen)
DOI 10.24169/DJM/2018/1-2/8



Az ábra forrása: WP 248, 8. o.

Az első két kérdésre (Valószínűsíthetően magas kockázattal jár? és A kivételek közé tartozik-e?) minden adatkezelőnek választ kell adnia. Ezek azok a kérdések, amelyek alapján arról születhet döntés, hogy az adatvédelmi hatásvizsgálatot el kell-e végezni.

A rendelet szerint akkor kötelező adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés valószínűsíthetően magas kockázattal járhat a természetes személyek jogaira és szabadságaira nézve, és felsorolja azokat az eseteket, amikor az adatvédelmi hatásvizsgálatot kötelező elvégezni:

- természetes személyekre vonatkozó személyes jellemzők automatizált adatkezelésen (ideértve a profilozást is) alapuló módszeres és kiterjedt értékelése, és amelyre a természetes személy tekintetében joghatással bíró vagy jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái (faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint az egyedi azonosítást célzó genetikai és biometrikus adatok, az egészségügyi adatok és a szexuális életre vagy szexuális irányultságra vonatkozó személyes adatok) – a jogszabályban meghatározott kivételekkel;
- a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;[30]
- nyilvános helyek nagymértékű, módszeres megfigyelése,
- a tagállami felügyeleti hatóság által nyilvánosságra hozott jegyzékén szereplő adatkezelési művelettípusok esetén.[31]

Az adatvédelmi munkacsoport – az eredendően magas kockázatuk miatt kötelező adatvédelmi

[30] Az Infotv. fogalomhasználatában bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat. A GDPR 10. cikke alapján: A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet.

[31] GDPR 35. cikk (1), (3)–(4) bekezdés.

hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének pontosabb meghatározása érdekében – kilenc mérlegelendő szempontot mutat be: 1. értékelés vagy pontozás; 2. joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal; 3. módszeres megfigyelés; 4. különleges adatok vagy fokozottan személyes jellegű adatok; 5. nagy számban kezelt adatok; 6. adatkészletek egymással való megfeleltetése vagy összevonása; 7. kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok; 8. új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása; 9. amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatást vegyenek igénybe, vagy szerződést érvényesítsenek.[32] Az adatvédelmi munkacsoport úgy véli, hogy minél több szempontnak felel meg az adatkezelés, annál valószínűbb, hogy szükséges adatvédelmi vizsgálatot végezni, ugyanakkor azt is hangsúlyozza, hogy akár egyetlen szempont alapján is szükséges lehet.[33] Abban az esetben, ha nem egyértelmű a vizsgálat szükségszerűsége, a munkacsoport azt ajánlja, hogy végezzék el, mivel segítséget jelenthet az adatvédelmi szabályok betartásában.[34]

A GDPR meghatározza azokat az eseteket is, amikor nem szükséges adatvédelmi hatásvizsgálatot végezni: valószínűsíthetően nem jár magas kockázattal, már készült hasonló adatvédelmi hatásvizsgálat, az adatkezelést 2018 májusa előtt engedélyezték, jogalapja van, vagy szerepel azoknak az adatkezelési műveleteknek a jegyzékében, amelyekre vonatkozóan nem kell hatásvizsgálatot végezni.[35]

Az adatvédelmi hatásvizsgálat szükségességének eldöntése után kerül sor magára a vizsgálatra. A vizsgálat tartalmát a GDPR határozza meg. A tartalmi jellemzők számbavétele egyúttal – mivel a rendelet külön nem definiálja a fogalmat – az adatvédelmi hatásvizsgálat definíciójának is tekinthető:

- a tervezett adatkezelési műveletek módszeres leírása és az adatkezelés céljainak ismertetése,
- az adatkezelési műveletek szükségességi és arányossági vizsgálata,
- az érintett jogait és szabadságait érintő kockázatok vizsgálata,
- a kockázatok kezelését célzó intézkedések bemutatása.[36]

Ha a folyamat végére a fennmaradó kockázatok továbbra is jelentősek, szükséges konzultálni a felügyeleti hatósággal.

Az adatvédelmi hatásvizsgálat végrehajtásáról az adatkezelő gondoskodik, egyúttal felelős a teljesítéséért. Ha van, az adatvédelmi tisztviselő tanácsát ki kell kérnie.[37] A hatásvizsgálatot érdemes folyamatosan felülvizsgálni, erre leginkább az adatkezelés körülményeinek változása vagy az ebből eredő kockázatok megváltozása miatt van szükség;[38] illetőleg ellenőrizni kell azt, hogy a személyes adatok kezelése a hatásvizsgálatnak megfelelően történik-e.[39]

Korunkban szinte semmilyen rendszer nem képes teljes biztonságot garantálni a személyes adatok védelme tekintetében. A GDPR megszabja azokat a lépéseket, amelyeket adatvédelmi incidens esetén – 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[40] – az adatkezelőnek tennie kell. A nyilvántartások és értesítések három szintje különböztethető meg: az adatkezelő házon belüli nyilvántartása az ellenőrzések végett; a hatóság tájékoztatása; és a nyilvánosság tájékoztatása az incidens körülményeiről.[41] Az adatvédelmi incidenst a felügyelő hatóságnak indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órával az után,

[32] WP 248, 10–12. o.
[33] WP 248, 12–13. o.
[34] WP 248, 9. o.
[35] GDPR 35. cikk.
[36] GDPR 35. cikk (7) bekezdés.
[37] GDPR 35. cikk (2) bekezdés.
[38] WP 248, 16. o.
[39] GDPR 35. cikk (11) bekezdés.
[40] GDPR 4. cikk 12. pont.
[41] Szabó Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. Beépített és alapértelmezett adatvédelem – Adatvédelmi incidensek bejelentése. Pázmány Law Working Papers. Pázmány Péter Katolikus Egyetem, 2016/27. sz., 5. o. http://plwp.eu/docs/wp/2016/2016-27_Szabo.pdf (letöltés: 2018. 05. 03.)

Debreceni Jogi Műhely 2018. (XV.) 1-2.
Debreceni Egyetem, Állam- és Jogtudományi Kar, Debrecen
(University of Debrecen, Faculty of Law, Debrecen)
DOI 10.24169/DJM/2018/1-2/8

hogy az adatkezelő tudomására jutott, kell bejelenteni.[42]

Új eleme a GDPR-nak az adatvédelmi tisztviselő funkció. Kijelölése abban az esetben kötelező, ha az adatkezelést közhatalmi szerv vagy közfeladatot ellátó szerv végzi, kivéve a bíróságokat; vagy az adatkezelő fő tevékenysége az érintettek rendszeres, nagymértékű megfigyelését teszi szükségessé; vagy az adatkezelő fő tevékenységei a személyes adatok különleges kategóriáinak és a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagyszámú kezelését foglalják magukban.[43]

Az adatkezelés jogalapjául főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés szolgálhat, ezek mellett a szerződéskötés és -teljesítés, az adatkezelőre vonatkozó jogi kötelezettség teljesítése, az érintett létfontosságú érdekének védelme, közérdek vagy hivatali hatáskör és az adatkezelő jogos érdekének érvényesítése szolgálhat az adatkezelés alapjául. A GDPR meghatározza az érintett hozzájárulásának definícióját: 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.[44] A gyakorlatban ez azt jelenti, hogy az ügyfél kipipálja az erre vonatkozó check-boksz-ot, és az online szolgáltatás igénybevétele során erre vonatkozó technikai beállítást hajt végre. A hozzájárulás iránti kérelmet egyértelműen megkülönböztethető módon kell előadni más ügyektől. Az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. A hozzájárulás bármikor visszavonható, erről az érintettet tájékoztatni kell.[45] Gyermekek közül csak a 16. évet betöltöttek hozzájárulása fogadható el, fiatalabbak esetében a hozzájárulást a szülői felügyeletet gyakorló adhatja meg.[46]

2. A GDPR – a könyvtárakra és a levéltárakra vonatkozóan[47]

Az információ és a tudás gyűjteményi szintű forrásai és intézményei a könyvtárak és a levéltárak. Működésük kereteit jogszabályok alakítják: a könyvtárakét a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről szóló törvény (a továbbiakban: Kult. tv.);[48] a levéltárakét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló törvény (a továbbiakban: Ltv.).[49] E törvények szabályozzák a használatukat, alakítják szabályzataikat. A könyvtári szolgáltatások egy része regisztrációval vehető igénybe, bizonyos szolgáltatások beiratkozáshoz kötöttek.[50] Aki levéltárban szeretne kutatni, annak kérelmet kell benyújtania, amelyen a személyes adatok mellett fel kell tüntetnie a kutatás témáját, időhatárát (iratanyag évköre), és azt, hogy tudományos vagy nem tudományos jellegű kutatást kíván végezni. Előbbihez csatolni kell a kutatást végző, közfeladatot ellátó szerv – a kutató részletes kutatási terve alapján megadott – támogató állásfoglalását. A kérelem alapján kap a kérelmező látogatói jegyet, illetve a feltüntetett kutatási téma és időhatár alapján kap engedélyt a kutatásra.[51]

A továbbiakban azt vizsgálom, hogy a GDPR mely rendelkezései vonatkoznak a könyvtárakra és a levéltárakra. A könyvtárakban és a levéltárakban kezelt adatok alapvetően kétfélék lehetnek. Egyrészt olyan természetes személyek adatai, akikkel az említett intézmények kapcsolatban állnak, idetartoznak a használók, azaz a regisztrált vagy beiratkozott olvasók és a levéltári kutatók, illetve bármely természetes személyek, akiknek az adatait kezelik (rendezvények, marketing stb.). Ezen adatok kezelését 2018. május 25-étől a GDPR szabályozza. Másrészt az említett intézmények állományában is találhatók személyes adatok. A könyvtárak esetében a különgyűjtemények, például a kézirattár, a folyóirat- és cikkgyűjtemény, a

[42] GDPR 33. cikk (1) bekezdés.
[43] GDPR 37. cikk (1) bekezdés.
[44] GDPR 4. cikk 11. pont.
[45] GDPR 7. cikk.
[46] GDPR 8. cikk (1) bekezdés.
[47] A kérdéskört jelen dolgozat csak a közlevéltárakra, illetve a nyilvános könyvtárakra vonatkozóan vizsgálja.
[48] 1997. évi CXL. törvény a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről.
[49] 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről.
[50] Kult. tv. 56–57. §.
[51] Lvt. 22. §.

DOI 10.24169/DJM/2018/1-2/8

kisnyomtatványtár dokumentumai tartoznak ide. A levéltárak esetében – illetékességi és gyűjtőkörük függvényében[52] – az iratanyag tartalmazhat élő személyekre vonatkozó adatokat.

A könyvtár és a levéltár használói, a regisztrált vagy beiratkozott olvasók és a kutatók, valamint az ezekkel az intézményekkel kapcsolatban állók személyes adatai tekintetében az említett intézményeknek ugyanolyan kötelezettségeik vannak a GDPR betartása kapcsán, mint bármely más szervezetnek, amely személyes adatot kezel. A GDPR-nak való megfelelés miatt három területen vannak kötelezettségeik: 1. Meg kell vizsgálniuk saját adatfeldolgozásukat, és arról módszeres leírást készíteniük; 2. a szükségesség és arányosság elve alapján intézkedéseket kell hozniuk magára az adatkezelésre és az érintettekre vonatkozóan; 3. azonosítaniuk kell az érintettek jogait és szabadságait érintő kockázatokat, és azokat orvosolniuk kell.[53]

A továbbiakban a felsoroltak közül csak azokat az intézkedéseket vázolom, amelyeket a könyvtáraknak és a levéltáraknak is meg kell határozniuk az érintettek, azaz az olvasók és a kutatók jogainak támogatása végett a személyes adataik kezelése kapcsán:

1. az érintettek tájékoztatása (érthető, egyszerű nyelvezet, az adatfelhasználás jogi alapjának ismertetése, adattárolási idő, kivel osztja meg);
2. betekintési jog és adathordozhatósághoz való jog;
3. helyesbítéshez és törléshez való jog;
4. kifogásolási jog és az adatkezelés korlátozásához való jog;
5. a nemzetközi adattovábbításhoz kapcsolódó garanciák (nemzetközi kutatási projektek, felhő alapú szolgáltatások stb. esetén).[54]

Az állományban található dokumentumokban, iratokban található személyes adatok egy részét az élő természetes személyek adatai képezik. A gyűjtőkör, illetve az illetékességi kör függvényében előfordulhat, hogy hatalmas mennyiségű iratanyagról van szó, rengeteg adattal az érintettekre vonatkozóan. Fölmerül a kérdés, hogy milyen szabályok vonatkoznak ezekre a személyes adatokra a GDPR alapján?

A GDPR rögzíti, hogy a közérdekű archiválás céljából folytatott további adatkezelés összeegyeztethető, jogszerű adatkezelési művelet.[55] A célhoz kötöttség elve alapján az adatok gyűjtése csak meghatározott és jogszerű célból történhet. A további adatkezelés azonban megengedett közérdekű archiválás céljából, vagyis az egyszer már jogszerűen felvett adatoknak az eredeti célon túli, közérdekű archiválási célú kezelése. Magyarországon a levéltárak és a könyvtárak működését törvényben szabályozzák, mely jogalapot képez a közérdekű archiváláshoz. A közérdekű archiválási célokat szolgáló személyesadat-kezelés során a könyvtáraknak és a levéltáraknak is alkalmazni kell a GDPR-t.[56]

A levéltárban és a könyvtárban a közérdekű archiválási célból kezelt adatokat nem az érintettől szerzik meg, nem az érintett önkéntes hozzájárulása alapján válnak kezelendő adattá, ebből következően a rendelet a közérdekű archiválási célú adatkezelésre vonatkozóan mentességek, eltérések megállapítását teszi lehetővé tagállami szinten.[57] Az eltérések többnyire az érintett jogait korlátozzák: hozzáférési jogát, helyesbítéshez való jogát, az adatkezelés korlátozásához való jogát, adathordozhatósághoz való jogát és tiltakozáshoz való jogát. Ezek mellett – a személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség tekintetében – az adatkezelőre vonatkozó mentességet is lehetővé tesznek. Abban az esetben állapítható meg a felsoroltak vonatkozásában eltérő szabályozás, ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához szükség van ilyen eltérésre.[58] A jogalkotók valószínűleg élni fognak ezzel a lehetőséggel, hiszen az említett intézmények nagy mennyiségű adatot, a könyvtárak egész

[52] Ltv. 3 § r)–s) pontok.
[53] WP 248, 26–27. o.
[54] ua.
[55] GDPR (50) preambulumbekezdés.
[56] GDPR (158) preambulumbekezdés.
[57] GDPR 89. cikk.
[58] GDPR 89. cikk (3) bekezdés.

DOI 10.24169/DJM/2018/1-2/8

gyűjteményeket, a levéltárak pedig több száz, több ezer iratfolyóméternyi anyagot kezelnek, illetve az iratok is különböző szinten rendezettek.

A közérdekű archiválási célú adatkezelés során garanciákkal kell védeni az érintett jogait és szabadságait. E garanciák közé tartoznak a megfelelő technikai, szervezési intézkedések,[59] amelyekkel elősegíthető az adatok védelme a jogosulatlan vagy jogellenes felhasználás ellen, a véletlen elvesztés, megsemmisítés és károsodás ellen.

Hazai és nemzetközi könyvtárak, levéltárak, szervezetek is szólnak a GDPR okozta változásokról. A Magyar Nemzeti Levéltár az idei év munkatervében jegyezte meg: a jogszabályi változásokra fel kell készülni, a GDPR szervezeti és szabályozási szinten is feladatot jelent.[60] A közgyűjtemények vonatkozásában azonban sok a bizonytalanság: vannak még kérdések jócskán, melyeknek még nem tudni előre a pontos koreográfiáját.[61] A Könyvtári Egyesületek és Szervezetek Nemzetközi Szövetsége (IFLA) mind a könyvtárak, mind a levéltárak vonatkozásában leszögezte: kimagaslóan fontos a GDPR-nak való megfelelés, hiszen ezen rendelet értelmében kötelezettségük keletkezik az általuk kezelt személyes adatok felelősségteljes védelmére és felhasználására vonatkozóan. A leglényegesebb változásokra öt pontban hívta fel a figyelmet: magasabb bírságok; a beépített és alapértelmezett adatvédelmi elvek alkalmazásának módszertana; adatvédelmi incidens bejelentése; a könyvtári vendégek joga; adatvédelmi tisztviselő kinevezése.[62]

Az európai országok többségében a levéltárak és a könyvtárak a személyesadat-kezelést közérdekű archiválási célból végzik, tehát vonatkoznak rájuk a felsorolt mentességek. Az Egyesült Királyságban azonban hiányos az ezzel kapcsolatos törvényi szabályozás. Az ARA – az Egyesült Királyság és Írország levéltárosainak egyesülete – azon túlmenően, hogy ágazati kódexet kíván kidolgozni, azonosította a közérdekű archiválás területeit, amelyeket a GDPR-megfelelőség érdekében jogszabályba kell foglalniuk.

- Az adatkezelés célja az általános közérdek szempontjából tartós értéket képviselő adatok gyűjtése, megőrzése, értékelése, rendezése, leírása, közlése, előmozdítása, terjesztése, illetve azokhoz hozzáférés biztosítása.
- Megfelelés a szakmai szabványoknak, annak érdekében, hogy az archivált adatok megfelelő védettsége, hitelessége és integritása biztosított legyen.
- Nyilvános hozzáférés biztosítása a közérdekű adatokhoz későbbi kutatás céljából vagy bármely közérdekű adatkezelési célból.[63]

Az Egyesült Királyság és Írország legjelentősebb kutatási könyvtárait képviselő szervezet, az RLUK tíz pontból álló gyakorlati ellenőrzőlistát állított össze, amely segítséget nyújthat a könyvtáraknak a GDPR-nak való megfelelés teljesítésében.[64]

3. A közérdekű archiválási célú adatkezelés kockázatai – egy konkrét jogeset kapcsán

2016-ban korabeli bűnügy témájú, 1959–61. években keletkezett, konkrét nevekhez köthető iratokra vonatkozóan kértek kutatási engedélyt az egyik levéltárban. Mivel a kérelmező kutatása nem tudományos

[59] GDPR 89. cikk (1) bekezdés.
[60] A Magyar Nemzeti Levéltár 2018. évi munkaterve.
[61] Aczél-Partos Adrienn: Szakmai nap az adatvédelemről. In: EKE Hírlevél, 2017 (14. évf.) 4. sz., 19. o.
[62] Briefing: Impact of the General Data Protection Regulation 2018 https://www.ifla.org/files/assets/clm/publications/briefing_general_data_protecti on_regulation_2018.pdf (letöltés: 2018. 05. 03.)
[63] Data Protection and 'Archiving purposes in the public interest'. https://www.whatdotheyknow.com/request/425084/response/1035207/attach/html/5/20170105%20ARA%20position%20paper%20Archiving%20purposes%20in%20the%20public%20interest%20final.pdf.html (letöltés: 2018. 05. 03.)
[64] General Data Protection Regulation 2018 – Ready? Set? Go? http://www.rluk.ac.uk/about-us/blog/general-data-protection-regulation-is-it-important-for-a-library-or-archive/ (letöltés: 2018. 05. 03.)

DOI 10.24169/DJM/2018/1-2/8

célú volt, támogatói állásfoglalást nem mutatott fel, így anonimizált másolatot kapott. Pár héttel később több weboldalon és médiafelületen hozták nyilvánosságra az 1962-es ítéletben szereplő bűnügyet és az érintett személy nevét is, aki – bűnügyi személyes adatainak engedély nélküli közzététele miatt – a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: NAIH) fordult. A NAIH hivatalból indított adatvédelmi hatósági eljárást annak megállapítására, hogy a levéltár jogszerűen biztosított-e hozzáférést az 1962-es ítélethez. Az eljárás során megállapította, hogy a levéltár nem alkalmazta helyesen az Ltv. 24. § (2) bekezdés a) pontját, s ezzel megsértette az Infotv.-t: az ítélet – mint bűnügyi személyes adat[65] – csak az érintett írásbeli hozzájárulásával vagy törvényi felhatalmazás alapján kezelhető, továbbítható.[66] Harmadik személy részére jogalap nélküli hozzáférés biztosítása miatt a levéltárat adatvédelmi bírság megfizetésére kötelezte.[67] A levéltár bírósághoz fordult, amely hatályon kívül helyezte a határozatot.[68]

Jelen írásnak nem feladata és nem célja annak vizsgálata, hogy jogszerűen bocsátotta-e a levéltár a kutató rendelkezésére az adatokat, sem a vonatkozó törvények és eljárások bemutatása. Az említett jogeset azért figyelemre méltó, mert a levéltárban őrzött, bűnügyi adatot tartalmazó 1962-es ítélet nyilvánosságra került. A jogszerű állapot már nem állítható helyre, az érintett személyes adatainak védelméhez fűződő joga sérült. Az adott levéltári kutatás 2016-ban történt, amikor a levéltári iratanyagból megismert és kigyűjtött személyes adatokra vonatkozóan az Infotv. rendelkezései vonatkoztak; 2018. május 25-étől azonban alkalmazni kell a GDPR-t. Vajon a levéltárakban kezelt személyes adatok védelmét hatékonyabban biztosítja-e majd ez a rendelet?

A GDPR rendelkezéseinek értelmében a levéltáraknak azonosítaniuk és kezelniük kell azokat a kockázatokat, amelyek az érintett jogaira és szabadságaira hatással lehetnek. Ehhez szükséges felmérni a levéltár iratállományában található, élő személyekre vonatkozóan kezelt adatokat a következő szempontokból:

1. Kezel-e érzékeny személyes adatokat?

- a személyes adatok különleges kategóriáiba tartozó adatok (9. cikk),
- bűncselekményekre vonatkozó adatok (10. cikk),
- kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok (75) preambulumbek.,
- személyes jellemzők értékelésére vonatkozó személyes adatok (75) preambulumbek.

2. Nagy számban kezeli-e ezek közül valamelyiket?

A felsoroltak kockázatot jelenthetnek a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése vonatkozásában. Vizsgálni kell azt is, hogy ezek milyen hatással lehetnek az érintett jogaira és szabadságaira, milyen intézkedések alkalmazhatók a kockázatok orvoslására, illetve hogy a kockázatok mennyire valószínűek és súlyosak.

Ezek a szempontok relevánsak lehetnek a levéltárban kezelt papír alapú iratokban található személyes adatokra és az elektronikusan feldolgozott adatokra vonatkozóan is. (Az elektronikusan kezelt adatokra vonatkozóan a kockázatokkal összefüggésben figyelembe kell venni az informatikai biztonsággal kapcsolatos elemeket is.) Az említett jogesetre fókuszálva: a bűncselekményekre vonatkozó adatok kezelése kockázatot hordozhat, mert az érintettre vonatkozóan nem vagyoni kárhoz vezethet az, ha az adataihoz jogosulatlanul fér hozzá harmadik személy.[69] Mit tehet a levéltár, hogyan tudja elkerülni azt, hogy a jogesetben ismertetett esethez hasonló ne fordulhasson elő újra? A GDPR intézkedési lehetőségként az álnevesítést említi, amennyiben a közérdekű archiválási célok ily módon

[65] Infotv. 3. § 3. pont (b) alpont és 3. § 4. pont.
[66] Infotv. 5. § (2) bekezdés a)–c) pont.
[67] NAIH/2016/2504/27/H. A NAIH a levéltártól független adatkezelők adatkezelésével kapcsolatban tovább folytatta az eljárást, és külön határozatot hozott: NAIH/2017/491/H.
[68] Fővárosi Közigazgatási és Munkaügyi Bíróság: 13.K.32.793/2016/15. A per tárgya: a levéltár megszegte-e az Ltv. 24. § (2) bekezdés a) pontjában foglaltakat, tehát nem érintette a bűnügyi személyes adatok jogellenes nyilvánosságra hozatalát és ezzel kapcsolatban a kutató felelősségét.
[69] GDPR (75) és (90) preambulumbekezdés.

DOI 10.24169/DJM/2018/1-2/8

megvalósíthatók.[70] A személyes adat eltávolítása azonban olyan, mintha az ember elveszítené a DNS-ét.[71] Értelmezhetetlenné válik a lényeg, az összefüggések. A levéltárak jelenlegi gyakorlata az Ltv. alapján az anonimizálás. Mivel a GDPR alapján követelmény az, hogy a közérdekű archiválás céljából végzett személyesadat-kezelés során megfelelő technikai és szervezési intézkedéseket vezessenek be,[72] ez a kutatási kérelmek elbírálására vonatkozó belső szabályozók átgondolását teheti szükségessé. Ha adott jogeset kapcsán gondolkodunk, az anonimizálással kapcsolatban elvileg több összetevő körvonalazódhat: 1. ki értelmezi, elemzi, értékeli a bűncselekményre vonatkozó adatot tartalmazó iratot; 2. az 1. pontban említett levéltári dolgozó ugyanaz-e, aki az adott kutatási kérelmet kezeli (hogy az anonimizálás hatékonyságát meg tudja ítélni, az esetleges összefüggést észrevegye); 3. ki végzi technikailag az anonimizálást; 4. felelősségi kérdések.

A bűncselekményekre vonatkozó adatokon kívül a többi érzékeny adat vonatkozásában is meg kell találni azokat a pontokat, amelyek kockázatot, veszélyforrást jelenthetnek az érintett jogai és szabadságai tekintetében. A levéltári munka és a könyvtári munka sajátosságainak figyelembevétele a szakma, a jogászok és az informatikusok együttműködését igényelheti, olyan keretek kidolgozását kívánva, amelyek segítenek a GDPR-nak való megfelelésben.

A GDPR vonatkozó rendelkezései fölvetik annak szükségességét is, hogy megvizsgálják az Ltv. rendelkezéseit. Ez az igény már az ismertetett jogeset kapcsán is megfogalmazódott: A NAIH elnöke és a levéltár vezetője egyaránt úgy véli, hogy az Ltv. és a hozzá kapcsolódó jogszabályok helyenként ellentmondásosak. Sok esetben nem egyértelmű, hogy a régi bírósági aktákban szereplő személyes adatokat – a bíróságon, illetve a levéltárban – ki, hogyan és milyen feltételekkel ismerheti meg.[73]

Összegzés

Korunkban az adat lett az egyik legfontosabb érték, ami újra és újra fölveti annak kérdését, hogyan lehet biztosítani a személyes adatok védelmét. Az Európai Unió jogi eszközökkel válaszol a kihívásra: 2018. május 25-étől kell alkalmazni a GDPR-t. A GDPR újdonságainak számbavétele után azt vizsgáltam, hogy a rendelkezések mennyiben vonatkoznak a könyvtárakra és a levéltárakra.

Az újdonságok több nagyobb csoportba sorolhatók. Egy részük az érintettekre vonatkozik (adathordozhatóság, elfeledtetéshez való jog, álnevesítés), más részük alapelv, mint a beépített és alapértelmezett adatvédelem, valamint az ezzel szorosan összefüggő elszámoltathatóság elve. A GDPR új jogintézményt is bevezet, az adatvédelmi hatásvizsgálatot, illetve előírja az adatvédelmi incidens bejelentési kötelezettségét is. Ha mérlegre tesszük a várható hatásokat, azt látjuk, hogy a rendelet erősíti az érintettek jogait, de az adatkezelőkre újabb kötelezettségeket ró, illetve erősíti az ellenőrzés szerepét.

A GDPR nemcsak a vállalkozások és az üzleti élet meghatározó adatvédelmi jogszabálya, alkalmazni kell a könyvtárakban és a levéltárakban is. A közérdekű archiválási célú adatkezelésre vonatkozóan azonban – a levéltárak, könyvtárak sajátosságainak figyelembevételével – mentességeket, eltéréseket engedélyez. A rendelkezések fölvetik annak szükségességét, hogy a könyvtárak és a levéltárak is azonosítsák a személyes adatok kezelése során felmerülő kockázatokat és értékeljék a szabályzataikat.

Felhasznált irodalom

A Magyar Nemzeti Levéltár 2018. évi munkaterve

ACZÉL-PARTOS Adrienn: Szakmai nap az adatvédelemről. In: EKE Hírlevél, 2017 (14. évf.) 4. sz., 18–19. o.

[70] GDPR 89.cikk (1) bekezdés.
[71] Briefing: Impact of the General Data Protection Regulation 2018.
[72] GDPR 89. cikk (1) bekezdés.
[73] Kulcsár Anna: Per indul a bűnügyi adatok megismeréséről. https://magyaridok.hu/belfold/per-indul-bunugyi-adatok-megismereserol-893599/ (letöltés: 2018. 05. 03.)

Az adatvédelem „szuperalapelve" – az elszámoltathatóság. http://gdpr.blog.hu/2017/06/14/az_adatvedelem_szuperalapelve_az_elszamoltathatosag (letöltés: 2018. 05. 03.)

Az új uniós Általános Adatvédelmi Rendelet bevezetésének hatásai a magyar adatvezérelt marketing szakma hétköznapjaira. https://adatvezereltmarketing.files.wordpress.com/2016/11/gdpr-gyakorlati-tagi-kerdesek-2016.pdf (letöltés: 2018. 05. 03.)

Briefing: Impact of the General Data Protection Regulation 2018. https://www.ifla.org/files/assets/clm/publications/briefing_general_data_protection_regulation_2018.pdf (letöltés: 2018. 05. 03.)

Data Protection and 'Archiving purposes in the public interest'. https://www.whatdotheyknow.com/request/425084/response/1035207/attach/html/5/20170105%20ARA%20position%20paper%20Archiving%20purposes%20in%20the%20public%20interest%20final.pdf.html (letöltés: 2018. 05. 03.)

Felkészülés az Adatvédelmi Rendelet alkalmazására 12 lépésben. https://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html (letöltés: 2018. 05. 04.)

General Data Protection Regulation 2018 – Ready? Set? Go? http://www.rluk.ac.uk/about-us/blog/general-data-protection-regulation-is-it-important-for-a-library-or-archive/ (letöltés: 2018. 05. 03.)

HORVÁTH Eszter: Péterfalvi Attila – Egységes európai adatvédelem. http://www.jogiforum.hu/interju/171 (letöltés: 2018. 05. 03.)

KULCSÁR Anna: Per indul a bűnügyi adatok megismeréséről. https://magyaridok.hu/belfold/per-indul-bunugyi-adatok-megismereserol-893599/ (letöltés: 2018. 05. 03.)

LUKÁCS Adrienn: Adatvédelmi irányelv és rendelet, avagy hogyan változott a közösségi oldalakra vonatkozó szabályozás az Európai Unió adatvédelmi reformjával? In: Ünnepi kötet dr. Zakar András c. egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis. Acta Juridica et Politica (Tom. 80). Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2017, 125–139. o.

PÓCZEK Aliz: Kevesebb mint egy év, és alkalmazandó lesz az adatvédelmi rendelet, 3. https://www.drtivadar.hu/adatvedelem/kevesebb-mint-egy-ev-es-alkalmazando-lesz-az-adatvedelmi-rendelet-iii-resz/ (letöltés: 2018. 05. 03.)

SZABÓ Endre Győző – RÉVÉSZ Balázs: Adataink biztonságban – adatainkban a biztonság? In: Információs Társadalom, 2017 (17. évf.) 1. sz., 45–54. o.

SZABÓ Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. Beépített és alapértelmezett adatvédelem – Adatvédelmi incidensek bejelentése. Pázmány Law Working Papers. Pázmány Péter Katolikus Egyetem, 2016/27. sz. http://plwp.eu/docs/wp/2016/2016-27_Szabo.pdf (letöltés: 2018. 05. 03.)

ZŐDI Zsolt: Privacy és a Big Data. In: Fundamentum, 2017. 1–2. sz., 18–30. o. http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf (letöltés: 2018. 05. 04.)

NAIH-határozatok: NAIH/2017/491/H.; NAIH/2016/2504/H

Fővárosi Közigazgatási és Munkaügyi Bíróság. 13.K.32.793/2016/15.

Jogszabályok:

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (Általános adatvédelmi rendelet)

A 29. cikk alapján létrehozott adatvédelmi munkacsoport WP 248: Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e

DOI 10.24169/DJM/2018/1-2/8

A 29. cikk szerinti adatvédelmi munkacsoport 01037/12/HU WP 196. 05/2012. számú vélemény a számítási felhőről

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

1997. évi CXL. törvény a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvek, 1980