Tájékoztató anyag 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) alkalmazásáról a közlevéltárak számára

Összeállította: Haraszti Viktor és Mikó Zsuzsanna

A tájékoztató anyag a Levéltári Kollégium felkérésére készült a levéltárak felkészülésének segítése céljából

Releváns jogszabályok

Az 1989-es, majd 1990-es alkotmánymódosítás alapjogi szintre emelte az információs jogok magyarországi védelmét. Ezt követően, negyed századdal ezelőtt megszületett az első adatvédelmi és információszabadság törvény, az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. A kelet-európai poszt-szocialista térségben először, de három évvel megelőzve az uniós Adatvédelmi Irányelvet és egyébként több nyugat-európai ország jogalkotását is. A magyar szabályozás kezdettől fogva a két információs alapjog együttes, egymásra ható szabályozási modelljét követi, mely modell napjainkban Európa nagy részén láthatóan egyre inkább teret hódít. A magyar adatvédelmi és információszabadság parlamenti biztosának hivatala a gyakorlatban 1995-ben, az első adatvédelmi ombudsman megválasztásával kezdte meg működését.

2011-től azonban az alkotmányos reform magával hozta az ombudsmani rendszer átalakítását. Mivel az uniós jog megköveteli a teljes függetlenséget, az információs jogok felügyeletéért felelős szervezet a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 2012-től, az Alaptörvényben rögzítetten hatósági keretek között állt fel és folytatta a munkát. Az adatvédelmet és információszabadság alapjait azóta is meghatározó jogszabály az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.

Az Európai Unió adatvédelmi szabályzatának reformja már régóta napirenden volt. Az Európai Parlament és a Tanács **95/46/EK irányelve** (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (a továbbiakban: Irányelv) egyes elemeiben meghaladottá vált és mint irányelv, nem volt közvetlenül alkalmazandó, így az Európai Unió egyes tagállamai más-más szinten és

tartalommal szabályozták egyazon kérdéseket. Az elmúlt tíz évben az információs technológia fejlődésével olyan új innovatív szereplők léptek be a piacra, melyek adatkezelési szabályozásának a meglévő adatvédelmi szabályozások nem tudnak eleget tenni. Az okostelefonok, a közösségi oldalak, és az olyan üzleti modellek, amelyek terméke a személyes adat, veszélyeztetik a magánélethez való jogot az internet világában. Az Európai Bizottság azt remélte, hogy a reform megnöveli a felhasználók bizalmát az online szolgáltatásokban, és ezáltal hozzájárul Európa digitális gazdaságának fellendüléséhez. Mindezek mellett a különböző szabályok az Unió tagállamai között nehezítették a terjeszkedést az innovatív adatkezelő cégek számára. Ezért az Európai Bizottság egyik fő célja egy egységes szabályrendszer az EU tagországainak számára.

Az Európai Parlament és a Tanács 2016. április 27-én fogadta el az új uniós adatvédelmi csomagot, amelynek egyik eleme **a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 Rendelet** (a továbbiakban: Rendelet, általános szóhasználatban a GDPR), a másik a **bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv (2016/680/EU irányelv – bűnügyi irányelv)**.

Míg a GDPR 2018. május 25-től EU-szerte közvetlenül alkalmazandó, addig az irányelvet a tagállamoknak 2018. május 6-ig kell átültetniük nemzeti jogszabályaikba. A Rendelet tehát közvetlen alkalmazandó a nemzeti jogban is, tekintet nélkül az ahhoz kapcsolódó nemzeti deregulációs folyamat állására. Az adatvédelmi szabályozás ezáltal az Európai Unió területén egységessé válik, így annak értelmezésének is egységesnek kell lennie az összes tagállamban. Az egységes alkalmazást elősegítő, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (a továbbiakban: 29-es Munkacsoport) 2017 folyamán iránymutatásokat dolgozott ki, amellyel segíteni kívánta a Rendelet egységes értelmezését.

A Levéltári Kollégium felhasználva a rendelkezésre álló szakmai anyagokat jelen tájékoztató anyaggal kívánja a levéltárak adatvédelmi tudatosságát segíteni. A hazai jogi szabályozás GDPR-megfelelőség szerinti átalakítása megtörténte után jelen tájékoztató is kiegészítésre kerül.

A GDPR által használt elvek, fogalmak, általános szabályok

Az alábbiakban a Rendeletben, illetve annak bevezetőjében szabályozott elvek és fogalmak ismertetésére kerül sor. Az elvek ismertetése kizárólag olyan mélységben és részletezettséggel történik, amely a közlevéltárak működése szempontjából releváns. A fogalmak bemutatása a Rendelet szó szerinti idézésével történik. A fogalmak közül szintén csak a levéltári szempontból releváns meghatározások kiválasztására került sor.

Elvek (II. fejezet)

A személyes adatok kezelésére vonatkozó elvek (5. cikk)

A személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);

b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);

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

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság”);

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok

jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

Az adatkezelő felelős a fenti pontokban ismertetett elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

A bevezetés a Rendeletben szereplő elvekhez részletszabályokat, illetve magyarázatot ad.

Az európai szabályozás deklarálja, hogy a természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Továbbra is arra épül a szabályozás, hogy ez nem jelenti azt, hogy a személyes adatok védelme abszolút jog lenne. A személyes adatok védelmének jogát más alapjogokkal összhangban, az arányosság elvét figyelembe véve lehet érvényre juttatni. Az európai jog szempontjából különösen védendő jogok: a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához és a tájékozódás szabadságához, a vállalkozás szabadságához, a hatékony jogorvoslathoz és a tisztességes eljáráshoz, és a kulturális, vallási és nyelvi sokféleséghez való jog.

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését. A Rendelet a későbbiekben nevesíti is, hogy mely adatok hozhatók közvetlen összefüggésbe, ilyenek: a természetes személyek által használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel. Ezáltal olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyek személyes profiljának létrehozására és az adott személy azonosítására.

Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható. Ez a Rendelet ezért nem vonatkozik az ilyen anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.

A Rendeletet nem kell alkalmazni az elhunyt személyekkel kapcsolatos személyes adatokra. Ez utóbbi adatokra vonatkozó szabályozás tagállami hatáskörbe tartozik.

Új elemként vezeti be a Rendelet az elvek közé az álnevesítés alkalmazását, amelynek a fogalmát is meghatározza. (4. cikk 5. pont)

A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték. Ha az adatkezelés közérdekből elvégzendő feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása érdekében szükséges, uniós vagy tagállami jog meghatározhatja és pontosan leírhatja azokat a feladatokat és célokat, amelyek tekintetében a további adatkezelés jogszerűnek és összeegyeztethetőnek tekintendő. A közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott további adatkezelést összeegyeztethető, jogszerű adatkezelési műveleteknek kell tekinteni.

Az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az alapvető jogokra és szabadságokra nézve a kezelésük körülményei jelentős kockázatot hordozhatnak. Ilyen adatnak minősül a faji vagy etnikai származásra utaló személyes adatok is. A személyes adatok különleges kategóriáira vonatkozó adatkezelési tilalomtól való eltérés szintén megengedhető, ha erről az uniós vagy tagállami jog rendelkezik, és ha arra megfelelő garanciák mellett kerül sor a személyes adatok és más alapvető jogok védelme érdekében, ha ez valamely közérdeken alapul, így különösen több más cél mellett a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból. Eltérés alapján az ilyen személyes adatok kezelése olyan esetekben lehetséges, amikor az jogi igények előterjesztése, érvényesítése, illetve védelme céljából szükséges, függetlenül attól, hogy erre bírósági eljárás, közigazgatási, vagy egyéb, nem bírósági útra tartozó eljárás keretében kerül-e sor.

Alapesetben a **tisztességes és átlátható adatkezelés elvének** megfelelés érdekében az érintetteknek tájékoztatást kell adni az adatkezelés tényéről és céljairól. A tájékoztatás nyújtására vonatkozó kötelezettség előírása nem szükséges, ha az érintettnek ez az információ már a birtokában van, vagy ha a személyes adat rögzítését, illetve közlését valamely jogszabály kifejezetten előírja, vagy ha az érintett tájékoztatása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne. E helyzet állhat elő különösen akkor, ha az adatkezelés közérdekű archiválás célt, tudományos és történelmi kutatási célt vagy statisztikai célt szolgál.

Az érintett jogosult arra, hogy kérhesse a rá vonatkozó személyes adatok helyesbítését és megilleti őt az „elfeledtetéshez való jog", ha a szóban forgó adatok megőrzése sérti a Rendeletet vagy az olyan uniós vagy tagállami jogot, amelynek hatálya az adatkezelőre kiterjed. Az érintett jogosult különösen arra, hogy személyes adatait töröljék és a továbbiakban ne kezeljék, ha a személyes adatok gyűjtése vagy más módon való kezelése az adatkezelés eredeti céljaival összefüggésben már nincs szükség, vagy ha az érintettek visszavonták az adatok kezeléshez adott hozzájárulásukat, vagy ha személyes adataik kezelése egyéb szempontból nem felel meg e Rendeletnek. Ugyanakkor a személyes adatok további megőrzése jogszerűnek tekinthető, ha az a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, valamely jogi kötelezettségnek való megfelelés, illetőleg közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy a népegészségügy területét érintő közérdekből, közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

Az uniós és a tagállami jog olyan mértékig korlátozhat bizonyos elveket, úgy mint a tájékoztatáshoz való jogot, a hozzáférési, helyesbítési és törlési jogot, az adathordozhatósághoz való jogot, a tiltakozáshoz való jogot, a profilalkotáson alapuló döntéseket és az adatvédelmi incidens érintettel történő közlését, valamint az adatkezelők bizonyos kapcsolódó kötelezettségeit, amilyen mértékig ez egy demokratikus társadalomban szükségesnek és arányosnak tekinthető a közbiztonság védelme érdekében. A jogi korlátozásra vonatkozó területek között többek között a Rendeletben szerepel az archivált személyes adatoknak a volt totalitárius államrendszerek alatt tanúsított politikai magatartáshoz kapcsolódó, konkrét információk szolgáltatása érdekében történő további kezelése. Vagyis ezen okra hivatkozás alapot teremthet az elvektől való eltérésre. E korlátozásoknak azonban tiszteletben kell tartaniuk az *Alapjogi Charta (2007. évi CLXVIII.*

törvény az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról szóló lisszaboni szerződés kihirdetéséről), valamint *az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény (1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről* rendelkezéseit.

A Rendelet új szemléletű megközelítése az adatkezelő felelősségének kezelése, az elszámoltathatóság elve. [5. cikk (2) bekezdés] A személyes adatoknak az adatkezelő által vagy az adatkezelő nevében végzett bármilyen jellegű kezelése tekintetében az adatkezelő hatáskörének és felelősségének szabályozását írja elő. A Rendelet alapján az adatkezelőt kötelezni kell különösen arra, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek e Rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is az e Rendelet által előírt szintű. Ezeket az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni. Vagyis az adatkezelőt terheli annak igazolása, hogy körültekintő módon járt el és megtett mindent a személyes adatok védelme érdekében. A Rendelet külön nevesíti az adatkezelő igazolási kötelezettségét. A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát.

Ahhoz, hogy az adatkezelő igazolni tudja az e Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen **a beépített és az alapértelmezett adatvédelem elveit.** Az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket építhessen be és tovább is fejleszthesse azokat. Az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, a szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védeleméhez való

jogot, és a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek. Az igazolási kötelezettség körébe tartozik, hogy az adatkezelő vagy az adatfeldolgozó az e Rendeletnek való megfelelés bizonyítása érdekében nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Minden adatkezelő és adatfeldolgozó köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

Az adatkezelő kötelezettségei körébe tarozik még a kockázatok értékelése is. A biztonság fenntartása és az e Rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például a titkosítás alkalmazásának szükségességét. Ezekkel az intézkedésekkel biztosítani kell a megfelelő szintű biztonságot – ideértve a bizalmas kezelést is –, figyelembe véve a tudomány és a technológia állását, valamint a végrehajtás kockázataival és a védelmet igénylő személyes adatok jellegével összefüggő költségeket. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés – mérlegelni kell abban a tekintetben, hogy mely fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

Az adatkezelők, illetve adatfeldolgozók kategóriáit képviselő egyesületeket vagy egyéb szerveket az e Rendelet által szabott határokon belül, az e Rendelet hatékony alkalmazásának elősegítése érdekében magatartási kódexek létrehozására kell ösztönözni, az adatkezelés sajátosságaira figyelemmel. E magatartási kódexek keretében meg lehet határozni az adatkezelők és az adatfeldolgozók kötelezettségeit, figyelembe véve azt a kockázatot, amellyel az adatkezelés a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően jár.

A Rendelet fontos eleme a kártérítési kötelezettség és a kárért való felelősség szabályozása. Az adatkezelő vagy az adatfeldolgozó az e Rendeletet sértő adatkezelés miatt okozott kárt köteles megtéríteni. Az adatkezelőt vagy az adatfeldolgozót a kártérítési kötelezettség alól abban az esetben mentesíteni kell, ha bizonyítja, hogy a kár bekövetkeztéért őt semmilyen felelősség nem terheli. A szabályozás alapján tehát az adatkezelőt terheli a bizonyítási kötelezettség. A Rendelet egységes kártérítési szabályok alkalmazását írja elő az Európai Unió területén.

A Rendelet bevezetője külön nevesíti a személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő kezelésére vonatkozó szabályozás követelményeit. A Rendelet előírja, hogy az érintettek jogai és szabadságai tekintetében megfelelő garanciák kerüljenek rögzítésre. Ezek a garanciák biztosítják, hogy olyan technikai és szervezési intézkedéseket kell hozni, hogy az adattakarékosság elve érvényesüljön. A személyes adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további kezelésére akkor kerülhet sor, ha az adatkezelő előzetesen felmérte, hogy ezek a célok megvalósíthatók olyan személyes adatok kezelésével, amelyek eleve nem vagy a továbbiakban már nem teszik lehetővé az érintettek azonosítását, feltéve hogy megfelelő garanciák állnak rendelkezésre (mint például a személyes adatok álnevesítése).

A tagállamok számára engedélyezni kell, hogy konkrét feltételekkel és az érintettek számára nyújtott megfelelő garanciák mellett pontosításokat és eltéréseket alkalmazzanak a tájékoztatási követelményekre, a helyesbítéshez való jogra, a törléshez való jogra, az elfeledtetéshez való jogra, az adatkezelés korlátozásához való jogra, valamint az adathordozhatósághoz való jogra, továbbá a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő adatkezeléssel összefüggő tiltakozáshoz való jogra vonatkozóan. A szóban forgó feltételek és garanciák eredményezhetnek egyrészt az említett jogoknak az érintettek általi érvényesítését szolgáló eljárásokat – ha ez megfelelő az adott adatkezelés céljainak fényében –, másrészt az arányosság és a szükségesség elveinek érvényesítése érdekében a személyes adatok kezelésének minimálisra korlátozását célzó technikai és szervezési intézkedéseket. A személyes adatok tudományos célú kezelésének meg kell felelnie az egyéb, például a klinikai vizsgálatokat szabályozó jogszabályoknak is.

A Rendelet bevezetője részletszabályokat tartalmaz az archiválási célokat szolgáló személyes adatok kezelésére azzal a megkötéssel, hogy a Rendelet nem alkalmazható elhunyt személyek személyes adataira. [Preambulum (27) bekezdés] A közérdekű adatokat tároló közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek vagy magánfél szervezetek olyan szolgálatok kell, hogy legyenek, amelyek uniós vagy a tagállami jog szerint kötelesek az általános közérdek szempontjából tartós értéket képviselő adatokat beszerezni, megőrizni, értékelni, rendezni, leírni, közölni, előmozdítani, terjeszteni, illetve azokhoz hozzáférést biztosítani. A tagállamok számára továbbá lehetővé kell tenni, hogy rendelkezzenek a személyes adatok archiválási célokat szolgáló további kezeléséről, például a volt totalitárius államrendszerek

alatt tanúsított politikai magatartáshoz, népirtáshoz, az emberiesség elleni bűncselekményekhez, különösen a holokaussthoz és a háborús bűncselekményekhez kapcsolódó konkrét információk szolgáltatása érdekében.

E Rendeletet a történelmi kutatási célokból kezelt személyes adatok esetében is alkalmazni kell. Ide kell sorolni a történelmi kutatásokat és a genealógiai célú kutatást is, szem előtt tartva, hogy e rendelet elhunyt személyre nem alkalmazandó.

A levéltári gyakorlat szempontjából néhány fontos fogalommeghatározás (4. cikk)

- „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható (1. pont);

- „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés (2. pont);

- „álnevesítés”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni (5. pont);

- „nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető (6. pont);

- „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a

tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja (7. pont);

- „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel (8. pont);

A személyes adatok kezelésének jogszerűsége (6. cikk)

A Rendelet összesen hat feltételt határoz meg az adatkezeléssel összefüggésben, amelyek közül legalább egynek meg kell felelni annak érdekében, hogy az adatkezelés jogszerű legyen. A jogalapok teremtik meg az adatkezelő és az adatalany, az érintett érdekeinek egyensúlyát.

A személyes adat jogszerű kezelésének feltételei [6. cikk (1) bekezdés a)-f) pontok]:

1. Hozzájárulás [6. cikk. (1) bek. a) pont]

Az érintett adatkezeléshez történő hozzájárulása továbbra is a legfőbb jogalap. Evidensnek tűnik, hogy ha az a személy, akinek az adatait kezeljük (vagyis az „érintett”) az adatkezeléshez hozzájárul, akkor nem lehet vitás az adatkezelés jogszerűsége. A Rendelet szerint az adatkezelés jogszerű, ha az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Az érintett hozzájárulása akkor megfelelő, ha az 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. Ennek megfelel az aláírás vagy az elektronikus felületen kipipált „checkbox” négyzet is, a lényeg, hogy a hozzájárulásnak aktív cselekménynek kell lennie.

Személyes adat tehát elsődlegesen akkor kezelhető, ha ahhoz az érintett – önkéntesen, megfelelő tájékoztatást követően, határozottan, félreérthetetlenül – hozzájárul. A hozzájárulás megadható szóban, írásban vagy ráutaló magatartással, de a hallgatás itt nem beleegyezés. Így pl. kamerás megfigyelés esetén, ha az érintett a kellő előzetes tájékoztatást megkapta, azzal, hogy a területre belép, az adatkezeléshez hozzájárulását adja. Az érintett minden esetben tisztában kell legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy azt milyen mértékben tette. Különleges adat kezelése esetén kizárólag írásban lehet az

adatkezeléshez hozzájárulni. Az érintettet minderről előzetesen tájékoztatni kell egy adatkezelési tájékoztató keretében.

A Rendelet azonban kivételeket is megfogalmaz: „*Annak biztosítása érdekében, hogy hozzájárulást önkéntesen adták, a hozzájárulás olyan egyedi esetekben nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez, amelyekben az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn, különösen ha az adatkezelő közhatalmi szerv, és az adott helyzet valamennyi körülményét figyelembe véve ezért valószínűtlen, hogy a szóban forgó hozzájárulás megadása önkéntesen történt*.” [Preambulum (43) bekezdés.]

A hozzájárulás jogalapjának legfontosabb feltétele, hogy annak önkéntesnek, azaz mindenfajta külső befolyástól mentesnek kell lennie. Az ún. 29-es (Adatvédelmi) Munkacsoport több dokumentumában kifejtett álláspontjára támaszkodva a NAIH gyakorlata szerint is a hozzájárulás jogalapként csak akkor jöhet szóba, ha valódi választási lehetőség áll az érintett rendelkezésére, és nem áll fenn a megtévesztés, a megfélemlítés, a kényszerítés vagy más jelentős negatív következmény veszélye a hozzájárulás megtagadása esetén. Az önkéntesség hiányában az adatkezelő nem rendelkezik megfelelő jogalappal az adatkezeléshez.

A munkavégzésre irányuló jogviszonyokban épp ezért nem értelmezhető a hozzájárulás önkéntessége: a munkáltató és a munkavállaló közötti alá-fölérendeltségi viszonyban, ha az alkalmazott a hozzájárulását megtagadja, ez anyagi vagy nem anyagi természetű hátrányt okozhat neki. Az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében tehát csak kivételesen lehet hivatkozni, alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli „előnyöket” szerez a munkavállaló, és nem érheti őt semmilyen hátrány az adatkezelés megtagadása esetén. A hozzájárulás megfelelő jogalap lehet, ha az adatkezelésre nem a munkaviszonnyal összefüggésben kerül sor, vagyis ha az adatkezelés a munkáltatói jogok gyakorlásával nem áll kapcsolatban.

Például egy munkáltató egy labdarúgó tornára csapatot szervez, amelyhez a munkáltatónak továbbítania kell a szervezők részére azon munkavállalóinak az adatait, akik részt vennének a versenyen, mivel a munkáltató állja a nevezés költségeit. Emellett a munkáltató mezeket is biztosít a versenyre, ezért a munkavállalók pólóméretét továbbítania kell a pólót készítő vállalkozás részére. Ez két különböző adattovábbítást jelent, és mindkettőhöz egymástól függetlenül önkéntes hozzájárulást tud adni a munkavállaló anélkül, hogy ennek bármilyen következménye lenne a munkaviszonyára nézve.

2. Szerződés teljesítése [6. cikk (1) bek. b) pont]

A Rendelet által rögzített új jogalap a szerződéses jogalap, mi szerint az adatkezelés jogszerűnek minősül, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség.

Jogszerű az adatkezelés a Rendelet szerint akkor is, ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. Tipikus példa erre a levéltárban is a munkaszerződés vagy egyéb, a munkaviszonyhoz kötődő megállapodás (pl. tanulmányi szerződés, a tanulmányok eredménye).

3. Jogi kötelezettség teljesítéséhez szükséges [6. cikk (1) bek. c) pont]

A GDPR fogalmi rendszerében az adatkezelés jogalapja valamely jogi kötelezettség teljesítéséhez szükséges előírás, ami alapvetően törvény, illetve önkormányzati rendelet által közérdekből elrendelt adatkezelést jelent. Ami az Info tv. korábban meghatározott fogalmi rendszerében a kötelező adatkezelés. Ilyenkor akár az érintett kívánsága ellenére is kezelhetők a személyes adatai. Az adatkezelés feltételeit az adott jogszabály határozza meg.

A kötelező adatkezelések egy jelentős része törvényi rendelkezésen alapul vagy olyan törvényi előíráson, amely kötelezővé teszi az adatkezelést, vagy olyan jogszabályon, amely csupán lehetővé teszi az adatkezelést. Mindkét esetben előfordul, hogy az adott törvény az adatkezelés valamennyi körülményét szabályozza, de olyan jogszabály által nevesített adatkezelés is létezik, amelynél a törvény az adatkezelés részleteit, körülményeit nem határozza meg, azokat az adatkezelőre bízza.

A levéltári feladatellátás, tevékenység körében végzett adatkezelés jogalapja a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. tv. (Ltv.) Adatvédelmi tekintetben a lex generalis az Info. tv., a lex specialis az Ltv. A Rendelet sok esetben az adatkezelési korlátok alóli kivételként említi a „közérdekű archiválás” céljából történő adatkezelést, mely fogalmi idegensége ellenére a levéltári célú adatkezelési kivételeket foglalja magában.

Törvényen alapuló, kötelező adatkezelést széles körben rendelnek el az adókötelezettségre, társadalombiztosításra vonatkozó jogszabályok. Ezen jogszabályok rendelkezései a

munkáltatók és a munkavállalók számára kötelezettségként jelennek meg, vagyis ezek ténylegesen kötelező adatkezelések. Ezen túlmenően a munkaviszonyra is irányadóak lehetnek olyan törvények, amelyek az adatkezelést a munkáltató számára lehetővé teszik. Ebbe a körbe tartozik például a munkáltatói visszaélés-bejelentési rendszerrel (integritás ügyek), illetve a munkáltató ellenőrzési jogosultságával összefüggő adatkezelés a munkavégzés tekintetében. Ilyen még a kötelező munkaköri alkalmassági vizsgálat (üzemorvosi vizsgálat), mely körben a jogszabály különleges adatok kezelésére is feljogosít, de nem a munkáltatót, hanem az egészségügyi szolgáltatót.

Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

4. Az érintett létfontosságú érdeke [6. cikk (1) bek. d) pont]

A Rendelet megfelelő jogalapként elfogadja azt az esetet is, amikor az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. Létfontosságú érdek lehet szükséghelyzet (pl. hegyen eltűnt személy megkereséséhez a telefonja cellainformációinak ismerete). Az Info tv. 6. § (2) bekezdése így fogalmaz: *„Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetőek.”*

Levéltári esetkör ritkán merülhet fel erre a jogalapra hivatkozással történő adatkezelésre, de ügyfélszolgálati tevékenység körében elméletben nem zárható ki.

5. Közhatalmi jogosítvány gyakorlása [6. cikk (1) bek. e) pont]

Jogszerű az adatkezelés, ha az közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, azaz ha az adatkezelésre az adatkezelőre vonatkozó jogi kötelezettség teljesítése keretében kerül sor vagy ha az közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges. A felsorolt esetekben az adatkezelésnek az uniós jogban vagy valamely tagállam

jogában foglalt jogalappal kell rendelkeznie. A Rendelet nem követeli meg, hogy az egyes konkrét adatkezelési műveletekre külön-külön jogszabály vonatkozzon. Elegendő lehet az is, ha egyetlen jogszabály szolgál jogalapul több olyan adatkezelési művelethez is, amely az adatkezelőre vonatkozó jogi kötelezettségen alapul, illetve amelyre közérdekből végzett feladat ellátásához vagy közhatalmi jogosítvány gyakorlásához van szükség. Az adatkezelés célját is uniós vagy tagállami jogban kell meghatározni.

6. Jogos érdek [6. cikk (1) bek. f) pont]

Végül jogszerű az adatkezelés, ha az az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az általános előírás tehát az, hogy az adatkezelőnek vagy egy harmadik félnek legyen egy jogos érdeke, aminek az érvényesítéséhez szükséges az adatkezelés. Adatkezelőnek az minősül, aki a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza, harmadik személynek pedig gyakorlatilag bárki, aki nem azonos az adatkezelés szereplőivel (nem adatkezelő, adatfeldolgozó, érintett vagy ezek irányítása alatt álló, személyes adatot kezelő személy), így például az adatkezelő szerződéses partnere, beszállítója, hitelezője. A jogos érdek lehet tágabban meghatározott (pl. tudományos kutatás folytatása), de egészen specifikusan is megfogalmazott (pl. levéltár IT-rendszereinek biztonsága, munkavállalók megfigyelése).

Ha a levéltár megállapította a jogos érdeket, számba kell vennie az érintett olyan érdekeit vagy alapvető jogait és szabadságait is, amelyek a személyes adatok védelmét szükségessé teszik. Amennyiben ugyanis ezek elsőbbséget élveznek az adatkezelő vagy harmadik személy fenti jogos érdekével szemben, az adatok nem kezelhetőek a jogos érdekre történő hivatkozással. Ilyen alapvető érdek lehet a jó hírnév védelme vagy a magánélethez való jog.

Ahogyan az a fentiekből is kitűnik és az Európai Unió Adatvédelmi Munkacsoportja 6/2014. sz. véleményében is kifejti, az adatkezelőnek egy háromlépcsős tesztet kell végrehajtania. A teszt keretében 1) azonosítani kell az adatkezelő jogos érdekét, 2) meg kell állapítani az érintett érdekét/alapjogát és végül 3) súlyozni kell a két ellenpontot és megállapítani, hogy kezelhet-e az érdekmérlegelés eredménye alapján személyes adatot. Az érdekmérlegelést az adott adatkezelésre kell szabni és körültekintően eljárni, még a nyilvánvalónak tűnő esetekben is. Például, ha egy kutató szándékosan megrongál avagy eltulajdonít iratokat, akkor sem

helyezheti ki a levéltár a kutatóteremben vagy az interneten az elkövető arcképét, mert jogos érdeke nem fogja megelőzni a magánszemély alapvető jogait.

Ne felejtsük azt, hogy hiába volt jogalapunk egy adat kezelésre, ha annak célja már nem létezik – ilyen esetben az adat nem kezelhető tovább. A levéltári iratanyag tekintetében az adatkezelés célja a hosszú távú megőrzés, (ami jogszerű cél és megfelel a GDPR (65). Preambulum bekezdésében és a 17. cikkében megfogalmazott közérdekű archiválási célú kivételnek.)

A levéltár működési körében, ügyviteli iratai közt azonban már található olyan adat (irat), mely az irattári őrzési idő után selejtezhető. Például az álláspályázat során megszerzett önéletrajz – kifejezett, meghatározott ideig történő megőrzésre adott érintetti hozzájárulás hiányában – törlendő, ha nem az illető pályázót vesszük fel.

Az adattakarékosság és adatminimalizálás elvének a személyes adatokat tartalmazó iratok megőrzésénél, tárolásánál komoly hatása lehet, mivel az irattári őrzési időn túli őrzés már jogalap nélküli lesz és így akár a Hatóság bírságát is maga után vonhatja.

Az érintettek jogai

A Rendelet különös gondot fordít az érintettek, az adatalanyok joggyakorlásának szabályozására. Az érintettek jogait a Rendelet III. fejezete tartalmazza, az alábbiak szerint:

1. Tájékoztatás az adatkezelés megkezdésekor
2. Az érintett hozzáférési joga
3. Helyesbítéshez való jog
4. Törléshez való jog (az elfeledtetéshez való jog)
5. Az adatkezelés korlátozásához való jog
6. Az adathordozhatósághoz való jog
7. A tiltakozáshoz való jog
8. Automatizált döntéshozatallal és a profilalkotással kapcsolatos jogok

Az egyes területek részletes kifejtése:

1. *Tájékoztatás az adatkezelés megkezdésekor (12. cikk, 13-14. cikk)*

A Rendelet 12. cikke szabályozza az átlátható tájékoztatásra, kommunikációra és az érintett jogainak gyakorlására vonatkozó intézkedéseket. Az előzetes tájékoztatás megléte minden

adatkezelés alapja. Az adatkezelés megkezdése előtt tájékoztatást kell adni levéltári területen a kutatás megkezdése előtt, a látogatói jegy kiállításakor; az ügyfélszolgálaton az ügyintézés megkezdése előtt és a levéltár saját ügymenetében a munkavállalók és esetleg az ügyfelek (egyszerűbben minden adatkezelés megkezdése előtt az érintettek) felé, így pl. a munkahelyi adatkezelés vagy a kamerás adatkezelés esetében.
A tájékoztatónak tömör, átlátható, érthető és könnyen hozzáférhető formában, kell elkészülnie, világosan és közérthetően megfogalmazva. Írásban vagy más módon, ideértve adott esetben az elektronikus utat is. Kérésre szóbeli tájékoztatás is adható, feltéve, hogy az érintett igazolta személyazonosságát.

Az adatfelvétel előtti tájékoztatás (13-14. cikk) az alábbiakat kell tartalmazza:

- Az adatkezelő és képviselője neve és elérhetőségei
- Ha van, az adatvédelmi tisztviselő elérhetőségei
- Az adatkezelés célja és jogalapja
- Az adatszolgáltatás elmaradásának következményei
- Érdekmérlegelésen alapuló jogalap esetén a jogos érdekek megnevezése
- Adatátvételnél a személyes adatok kategóriái és azok forrása
- Az automatizált döntéshozatallal, profilalkotással kapcsolatos információk
- Adattovábbítás esetén címzettek, címzettek kategóriái
- Harmadik országba történő adattovábbítással kapcsolatos információk, garanciák
- A tárolás időtartama, annak szempontjai
- Az érintett jogai (ideértve a hozzájárulás visszavonásának jogát is)
- Hatósághoz fordulás joga

Nagyon fontos, hogy a tájékoztatás az adatalanyok „nyelvén” szóljon, közérthető legyen. Formailag ugyan teljesítettnek tűnhet a tájékoztatás a Rendelet vonatkozó szövegrészleteinek átemelésével, azonban vélhetően a bonyolult szöveg nem minden érintett számára lesz közérthető, így tartalmilag a tájékoztatás nem lesz a Rendelet elvárásainak megfelelő.

A tájékoztatás időpontjára vonatkozóan is a 13-14. cikkben találunk szabályokat. A tájékoztatás időpontja, amennyiben az érintettől származik az adat, az adatfelvételkor kell megtörténjen.

Egyes adatkezelésekre vonatkozóan a Rendelet felmentést ad a tájékoztatási kötelezettség alól. Nem kell előzetes tájékoztatást adni jogszabály által elrendelt adatkezelés esetén. A 14. § (5) bekezdés b) pontja alapján a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a Rendelet 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében is lehetőség van a tájékoztatás mellőzésére. A jogalkotó felismerte, hogy ezekben az esetekben a korábban említett tájékoztatás megadása, azaz a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne az adatkezelő részéről
További kimentést ad, amennyiben a fent felsorolt tájékoztatási kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelés céljainak elérését.
Ilyen esetekben azonban adatkezelőnek, a levéltáraknak megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében.

2. Az érintett hozzáférési joga (15. cikk)

A Rendelet 15. cikke rögzíti az érintett hozzáférési jogait. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- A személyes adatai másolata
- Az adatkezelés céljai
- Az adatok kategóriái
- Automatizált döntéshozatallal, profilalkotással kapcsolatos adatok
- Adatátvételnél a forrásra vonatkozó információk
- Címzettek, akik részére az adatokat közölték vagy közölni fogják
- Harmadik országba történő adattovábbítással kapcsolatos információk, garanciák
- A tárolás időtartama, ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai
- Az érintett jogai (kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen)
- Hatósághoz fordulás joga

Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

3. *Helyesbítéshez való jog (16. cikk.)*

Az érintett jogosult pontatlan adatainak indokolatlan késedelem nélküli helyesbítésére, kiegészítésére. A jogosultság ingyenesen gyakorolható és alkalmazható az eredetileg is pontatlanul rögzített vagy később megváltozott adatnál is. A helyesbítéshez való joggyakorlása is tartozhat a közérdekű archiválási kivételekhez, ám ezt a tagállami jognak kell szabályoznia.

Ha a levéltár felé a már levéltárban lévő iratanyag tekintetében egy érintett jogának gyakorlásával élni kíván, az nyilván nem jelentheti az eredeti irat tartalmának megváltoztatását, de – amennyiben a konkrét irat előkereshető – az irat mellé elhelyezhető az érintetti nyilatkozat, ami egy jövőbeni kutatás részére segítséget is nyújthat.

Ügyfélszolgálati ügyben ezen jog gyakorlásának akadálya nincs.

4. *Törléshez való jog (az elfeledtetéshez való jog) (17. cikk)*

Levéltári berkekben legnagyobb vitát kiváltó rendelkezés – a levéltárakban őrzött óriási adatmennyiség és az iratok hosszú távú megőrzése okán – az elfeledtetéshez való jog (right to be forgotten). A Rendelet alapján 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, ha az alábbi indokok valamelyike fennáll:

1. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
2. az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
3. az érintett a tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
4. a személyes adatot jogellenesen kezelték;

a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

Ebben az esetben is nagyon fontos, hogy az elfeledtetéshez való jog nem abszolút jog, pl. korlátozható közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, ill. amennyiben valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné a közérdekű archiválási célú adatkezelést. [17. cikk (3) bekezdés d) pont.] Ebből kiindulva a levéltárban lévő iratanyag esetében az elfeledtetéshez való jog nem érvényesíthető. Felmerül ugyanakkor, hogy mi a teendő abban az esetben, ha – és ez sokkal valószínűbb lehetőség – az iratot őrző szervnél kéri az érintett valamely olyan adatának törlését, amely a későbbiekben a levéltárba kerülne. A 17. cikk (3) bekezdés d) pontjának második tagmondata alapján amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő adatkezelést, a szervnek ezt joggal meg kell tagadnia.

Gyakorlatban ez azt jelentheti, hogy mindazon irattári tételek esetében, melyeknél a végső cél a levéltárba kerülés, azaz maradandó értékű iratot képeznek, azokban az esetekben a törléshez való jog nem alkalmazható.

Minden más esetben azonban igen – ha más kivétel nem érvényesül. Nagyon fontos, hogy a nem selejtezhető, levéltárba adandó tételek esetében erről az irattári anyagot őrző szervek is tudomással bírjanak. Szükségesnek tartjuk a jogi garanciák kidolgozását arra nézve, hogy mind a törlésre vonatkozó esetleges kérelmek elbírálása során, mind pedig a selejtezés során kifejezetten érvényesíthetőek legyenek a Rendelet 17. cikk (3) bekezdése d) pontjában foglaltak. Amiatt is indokolt a Rendelet e cikkének a körültekintő értelmezése és alkalmazása, mert a Rendelet 89. cikk (2) és (3) bekezdése egyedül a törléshez való jog kapcsán nem engedi meg azt, hogy a személyes adatok közérdekű archiválása céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelése vonatkozásában az uniós vagy a tagállami jog a Rendelettől eltérést állapítson meg.

Figyelemmel kell lenni azonban az eredeti adat publikálási célú megjelenítésére. Az Ltv. az iratok megőrzését, kutathatóvá tételét a levéltárak feladatává teszi ugyan, de ez nem egyenlő az adatok, iratok interneten eredeti formájában történő közzétételének törvényi kötelezettségével. Azaz közzététel esetén az érintett élhet a törléshez, elfeledtetéshez való jogával.

Ha ilyen eset előfordul, azaz ha az adatkezelő (a levéltár) interneten nyilvánosságra hozta a korabeli iraton szereplő adatot, és azt kérelem nyomán törölni köteles a nyilvános felületről – az elérhető technológia és a megvalósítás költségeinek figyelembevételével –, ésszerűen elvárható lépéseket is kell tennie annak érdekében, hogy tájékoztasson más adatkezelőket, a szóban forgó linkek, másolatok, másodpéldányok törlése kapcsán.

5. *Az adatkezelés korlátozásához való jog (18. cikk)*

Az adatkezelő az érintett kérésére korlátozza az adatkezelést, ha:
- az érintett vitatja a személyes adatok pontosságát
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését
- az adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez
- az érintett tiltakozott az adatkezelés ellen és az adatkezelő még vizsgálódik.

Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

6. *„A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség (19. cikk)*

Az adatkezelő minden olyan címzettet tájékoztatni kell a 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

7. *Az adathordozhatósághoz való jog (20. cikk)*

Az érintett jogosult az általa az adatkezelő rendelkezésére bocsátott adatait megkapni:
- tagolt, széles körben használt, géppel olvasható formátumban
- jogosult más adatkezelőhöz továbbítani
- kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz – ha ez technikailag megvalósítható

A rendelet ebben az esetben is ismer kivételeket: az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.
Így ebben az esetben a levéltárnak nincs feladata.

8. Tiltakozáshoz való jog (21. cikk)

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges alapuló adatkezelése ellen. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

A tiltakozási jog korlátja a (21) cikk (6) bekezdése, mely szerint, ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Azaz a közérdekű archiválás esetében tiltakozási jog kizárt. Ugyanakkor a tudományos vagy történelmi kutatási célú adatkezelések esetében a tiltakozási jog élő és gyakorolható.

9. Automatizált döntéshozatallal és a profilalkotással kapcsolatos jogok (22. cikk)

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.
Ez a szakasz a levéltári tevékenységi kört egyelőre nem érinti.

Az adatkezelő kötelezettségei

1. Kockázatelemzés

Az integritás és bizalmas jelleg alapelvéből következően a személyes adatokat olyan módon kell kezelni, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek

között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

Már a Rendelet (83) preambulum bekezdése kiemeli, hogy a biztonság fenntartása és a Rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő köteles értékelni az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást kell alkalmaznia.

A szabály az adatbiztonsági követelményeknek való megfelelés általános megfogalmazása. Alapvetően az a kötelezettség jelenik meg tehát, hogy az adatbiztonsági kockázatokat értékelni kell (javasolt dokumentálni is), és a kockázatok alapján kell meghozni a szükséges intézkedéseket.

A Rendelet adatkezelés biztonságával kapcsolatos 32. cikke részleteiben annyit határoz meg az intézkedésekkel kapcsolatban, hogy az adatkezelő a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Az adatkezelő a jóváhagyott magatartási kódexekhez jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy teljesíti a követelményeket. A közlevéltárak számára tehát nyitva áll a lehetőség arra, hogy a kockázatelemzésre vonatkozó előírásokat magatartási kódex segítségével szabályozzák.

A kockázatok értékelésére és a szükséges intézkedésekre alkalmazandó az elektronikus információs rendszerben[1] kezelt adatok tekintetében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.).

Az Ibtv. 5. §-a azt írja elő, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. A védelem megvalósítása során az összes számításba vehető fenyegetést kell figyelembe venni, azzal, hogy a védelem az elektronikus információs rendszer valamennyi elemére kiterjed és folyamatában megvalósul, továbbá költségei arányosak a fenyegetések által okozható károkkal. Ezen védelem biztosítása érdekében az elektronikus információs rendszereket a bizalmasság, sértetlenség és rendelkezésre állás szempontjából biztonsági osztályba kell sorolni és háromévenként vagy szükség esetén soron kívül felül kell vizsgálni.[2]

Mindezek biztosítása érdekében az elektronikus információs rendszernek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, a biztonsági események kezelését.

Ez alapján tehát az elektronikus információs rendszer teljes életciklusában, így már a bevezetésekor is el kell végezni az elektronikus információs rendszernek biztonsági osztályba sorolását és az adott biztonsági osztályhoz tartozó követelményeknek is meg kell felelnie az elektronikus információs rendszernek, továbbá az Ibtv. 9. §-a alapján el kell végezni szervezet biztonsági szintbe sorolását is.

[1] Ibtv. 1. § (1) bekezdés 14b pont - elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;
[2] Ibtv. 7.-8. §-ok

Az elektronikus információs rendszerek besorolásával kapcsolatban a 41/2015. (VII. 15.) BM rendelet[3] (a továbbiakban: BM rendelet) az Ibtv.-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről ad eligazítást. Az alkalmazott védelmi forma lehet adminisztratív, fizikai és logikai védelem, amely védelmi formák intézkedési katalógusa jelenik meg a BM rendeletben (ún. védelmi intézkedés katalógus).

Az idézett BM rendelet az adott elektronikus információs rendszer biztonsági osztályához igazodva felsorolást ad azokról a védelmi intézkedésekről , amelyeket kötelezően meg kell valósítani a zárt, teljes körű, folytonos és kockázatokkal arányos védelem biztosítása érdekében (BM rendelet 3. melléklet)., A BM rendelet 1. melléklet 1. pontja szerint a biztonsági osztályba sorolás során Általánosan figyelembe veendő szempontok többek között:

- Az érintett szervezetnek az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal kell érvényesíteni, amely:
    - a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;
    - a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;
    - a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.
- Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

A biztonsági osztályba sorolás szempontjából elengedhetetlen a fentiek alapján a rendszerbe kerülő adatkörök ismerete.

[3] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet

A biztonsági szinthez tartozó követelményeknek való megfelelésre az adott szerv mindaddig köteles, amíg az elektronikus információs rendszert használja.

Az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, amit az érintett szervezet vezetője hagy jóvá. A kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele.

Az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemzés alapját:

- az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága;
- a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége képezi.

A biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.

Emellett a BM rendelet 2. melléklete szerint az egyes szinteknél figyelembe veendő szempontok az alábbiak:

Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel:

- az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
- nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;

A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel

- személyes adat sérülhet;
- az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;

- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.

A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel

- különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;
- az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
- a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.

A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel

- különleges személyes adat nagy mennyiségben sérülhet;
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
- az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel

- különleges személyes adat kiemelten nagy mennyiségben sérülhet;
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;

- a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

A BM rendelet az egyes biztonsági szintekhez kapcsoltan állapít meg kötelező jellegű szabályokat, amelyeknek meg kell felelni. A szervezet besorolása az Ibtv. 9. § (2) bekezdése alapján a kötelezett szervnek a biztonsági osztálya megegyezik a legmagasabb besorolású elektronikus információs rendszer besorolásával, azonban a központi államigazgatási szervek legalább 3. biztonsági osztályba sorolandók be, a „jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások" tekintetében adatfeldolgozóknak minősülők pedig a legmagasabb, az 5. biztonsági osztályba sorolandók be.

Fentiek alapján tehát a közlevéltáraknak rendszeres időszakonként (az MNL-nek legalább évente, más levéltáraknak legalább 3 évente, illetve a szervezetben bekövetkező jelentős változások esetén) kockázatelemzést kell végeztetnie, melynek eredményeképpen azonosítják, számszerűsítik és a szervezeti célok és kockázatelfogadási kritériumok alapján besorolják a releváns kockázatokat. Az elektronikus levéltári rendszert használóknak a rendszer sajátosságaiból adódóan informatikai kockázatelemzést is kell végezni. A kockázatelemzés során az Ibtv. előírásait kell alkalmazni.

A kockázatelemzés során, az informatikai vagyontárgyak azonosítása után fel kell mérni az egyes alapfenyegetettségeket. A legnagyobb fenyegetést rendszerint az elektronikus információs rendszerek életciklusából adódó kockázatok, adatvesztés, illetéktelen hozzáférés és manipuláció, a tapasztalatlanságból eredő személyi kockázatok jelentik. Jellemzően az alábbi tipikus fenyegetettségekkel szokás számolni:

- a (környezeti) infrastruktúra területén: ellenőrizetlen belépés, betörés, közműellátás zavarai, tűz, vízbetörés;
- az eszközök (hardverek) területén: érzékenység az elektromágneses sugárzással szemben, hibás kezelés, áramellátás zavarai, műszaki jellegű hibák, rendellenességek,
- az adathordozók területén: nem védett tárolás, szakaszos demagnetizálódás hosszabb tárolás esetén, tárolóképesség;

- a szoftverek területén: felhasználói azonosítás hiánya, hozzáférési jogok helytelen odaítélése, szükségtelenül biztosított jogok, hiányzó naplózás, helytelen jelszó-mechanizmus, ártalmas kódok;
- az adatok területén: hiányzó hibakezelési eljárás, hiányzó ellenőrző eljárás, sértetlenség, bizalmasság elvesztése, hitelesség elvesztése, működőképesség elvesztése;
- a (számítógépes) kommunikáció területén: lehetőség az üzenetek lehallgatására, meghamisítására és
- a személyek területén: felmondás, hibás viselkedés az ismeretek hiánya miatt, hiányos biztonságtudat miatt, szándékos hibás viselkedés.

A kockázatelemzés során fel kell mérni és értékelni a kárkövetkezményeket, amelyek a levéltárakban jellemzően adatvesztés, személyes adat megsértése, bizalomvesztés, időhöz kötött adatok idő előtti nyilvánosságra hozatala, károk a törvények megsértése miatt, adatvédelmi törvény megsértése, szerzői jogi törvény megsértése, a közmegbecsülés elvesztése.

Az esetlegesen bekövetkező károk értékelése három meghatározó szempont alapján történhet, úgymint:

- a károk egyedi nagyságrendje (értékskála),
- a károk valószínű bekövetkezési gyakorisága (gyakoriság skála) és
- a kárérték és a gyakoriság által keletkező kockázat (kockázatmátrix).

A kockázatelemzést eredményeképpen biztonsági intézkedéseket kell meghatározni, amelyek biztosítják, hogy a rendszer védelme arányban legyen a kockázatokkal (a maradványkockázat mértékéig).

2. Hatásvizsgálat

A Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján magyarul elérhető az Irányelv 29. cikke szerinti Adatvédelmi munkacsoport hatásvizsgálattal kapcsolatos útmutatása. Lásd: https://naih.hu/files/wp248-rev.01_hu_hatasvizsg.pdf. Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e címmel (a továbbiakban: Iránymutatás). Az alábbi ismertetés ezen az Iránymutatáson alapul.

„Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. Az adatvédelmi hatásvizsgálatok az elszámoltathatóság szempontjából is jelentőséggel bírnak, ugyanis nemcsak az általános adatvédelmi rendelet előírásainak teljesítését könnyítik meg az adatkezelők számára, de a rendelet betartása érdekében hozott megfelelő intézkedések végrehajtásának bizonyítását is. Az adatvédelmi hatásvizsgálat tehát a rendelet betartásának elérésére és bizonyítására szolgáló eljárás.”

Az adatvédelmi hatásvizsgálatot akkor kell elvégezni, ha valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az adatkezelőnek mérlegelnie kell, hogy a meghatározás alapján el kell-e végeznie a hatásvizsgálatot. Az Iránymutatás ehhez mérlegelési szempontokat ad. Ezen szempontok közül a levéltárakat a következők érintik:

- különleges adatok vagy fokozottan személyes jellegű adatok: ide tartoznak a személyes adatok a Rendelet 9. cikkében meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a 10. cikkben meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok.
- Nagy számban kezelt adatok: a Rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a (91) preambulum bekezdés nyújt némi támpontot. Az Irányelv 29. cikke szerinti adatvédelmi munkacsoport ajánlása szerint a következő tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e: a) az érintettek száma konkrét számadatként vagy a lakosság arányában; b) a kezelt adatok mennyisége vagy adatfajták köre; c) az adatkezelési tevékenység időtartama vagy állandó jellege; d) az adatkezelési tevékenység földrajzi kiterjedése.

Fentiek alapján tehát a levéltáraknak mindenképpen szükséges a hatásvizsgálat elvégzése.

Az adatvédelmi hatásvizsgálatot a folyamatban lévő adatkezelési műveletekre is el kell végezni, ha az valószínűsíthetően magas kockázattal jár. Mindenképpen el kell végezni ha pl. a technológia megváltozik vagy a személyes adatok kezelésének célja megváltozik. A hatásvizsgálat megállapításait folyamatosan felül kell vizsgálni és rendszeresen újra kell értékelni. Az adatvédelmi hatásvizsgálatot az adatkezelés megkezdése előtt kell elvégezni.

Ennek elvégzéséért az adatkezelő felelős. Ha van adatvédelmi tisztviselő (a levéltárakban kötelezően lennie kell) akkor az ő véleményét is ki kell kérni. A hatásvizsgálat során ki kell kérni az érintettek vagy képviselőik véleményét. Ha az adatkezelő ezt nem teszi meg, azt indokolnia kell.

A Rendelet meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit [a 35. cikk (7) bekezdése, valamint a (84) és a (90) preambulum bekezdés]:

- „a tervezett adatkezelési műveletek […] [leírása] és az adatkezelés céljainak [ismertetése]";
- „az [adatkezelés] szükségességi és arányossági [vizsgálata]";

- „az érintett jogait és szabadságait érintő kockázatok [vizsgálata]";

- az alábbiakat „célzó intézkedések": „a kockázatok [kezelése]"; „az e rendelettel való összhang [igazolása]".

Az Iránymutatás javasolja ágazatspecifikus szabályok kidolgozását.

Az Iránymutatás összefoglalja a legfontosabb tennivalókat a valószínűsíthetően magas kockázattal járó adatkezelés esetére:

- olyan adatvédelmi hatásvizsgálati módszert választani, amely megfelel az Iránymutatásban felsorolt szempontoknak, vagy olyan módszeres adatvédelmi hatásvizsgálati eljárást meghatározni és végrehajtani, amely összhangban van az Iránymutatásban szereplő szempontokkal; a belső eljárásoknak, körülményeknek és kultúrának megfelelően beépül a meglévő tervezési, fejlesztési, módosítási, kockázati és működési felülvizsgálati eljárásokba; a megfelelő érdekeltek részvételével zajlik, és egyértelműen meghatározza felelősségi körüket (adatkezelő, adatvédelmi tisztviselő, érintettek vagy képviselőik, vállalkozás, műszaki szolgálatok, adatfeldolgozók, információbiztonsági tisztviselő, stb.);

- kérésre az adatvédelmi hatásvizsgálatról szóló jelentést benyújtani az illetékes felügyeleti hatóságnak;

- konzultálni a felügyeleti hatósággal, ha nem sikerült megfelelő intézkedéseket hozni a magas kockázatok csökkentésére;

- rendszeresen, de legalább az adatkezelési művelettel járó kockázat megváltozása esetén felülvizsgálni az adatvédelmi hatásvizsgálatot és a tárgyát képező adatkezelést;

- írásba foglalni a hozott döntéseket.

Az Iránymutatás 2. melléklete tartalmazza az elfogadható adatvédelmi hatásvizsgálatra vonatkozó szempontokat, utalva a Rendelet cikkeire.

a) módszeres leírás készült az adatfeldolgozásról [a 35. cikk (7) bekezdésének a) pontja]:
- figyelembe vették az adatkezelés jellegét, hatókörét, körülményeit és céljait ((90) preambulum bekezdés);
- a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítették;
- funkcionális leírás készült az adatkezelési műveletről;
- a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) azonosították;
- figyelembe vették a jóváhagyott magatartási kódexek előírásainak teljesítését [a 35. cikk (8) bekezdése];

b) értékelték a szükségességet és az arányosságot [a 35. cikk (7) bekezdésének b) pontja]:

- a Rendelet betartására irányuló intézkedéseket meghatározták [a 35. cikk (7) bekezdésének d) pontja és a (90) preambulum bekezdés], figyelembe véve az alábbiakat: az adatkezelés arányosságát és szükségességét előmozdító intézkedések a következők alapján: meghatározott, kifejezett és jogos cél(ok) [az 5. cikk (1) bekezdésének b) pontja]; az adatkezelés jogszerűsége (6. cikk); megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak [az 5. cikk (1) bekezdésének c) pontja]; korlátozott tárolási időtartam [az 5. cikk (1) bekezdésének e) pontja];

- az érintettek jogait támogató intézkedések: o az érintetteknek nyújtott tájékoztatás (12., 13. és 14. cikk); betekintési jog és az adathordozhatósághoz való jog (15. és 20. cikk); a helyesbítéshez és a törléshez való jog (16., 17. és 19. cikk); kifogásolási jog és az adatkezelés korlátozásához való jog (18., 19. és 21. cikk); a feldolgozókkal fennálló kapcsolatok (28. cikk); a nemzetközi adattovábbításhoz kapcsolódó garanciák (V. fejezet); előzetes konzultáció (36. cikk);

c) az érintett jogait és szabadságait érintő kockázatokat kezelik [a 35. cikk (7) bekezdésének c) pontja]:

- a kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték [vö. (84) preambulum bekezdés] vagy konkrétabban mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből: figyelembe vették a kockázatforrásokat [(90) preambulum bekezdés];

az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat beazonosították olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése; az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket beazonosították; felmérték a valószínűséget és a súlyosságot [(90) preambulum bekezdés];

- az említett kockázatok orvoslására irányuló intézkedéseket meghatározták [a 35. cikk (7) bekezdésének d) pontja és a (90) preambulum bekezdés];

d) az érdekelteket bevonták:

- kikérték az adatvédelmi tisztviselő tanácsát [a 35. cikk (2) bekezdése];

- adott esetben kikérték az érintettek véleményét [a 35. cikk (9) bekezdése].

3. Incidenskezelés

Az adatvédelmi incidens fogalmát nem a Rendelet vezette be, ugyanakkor a Rendelet számos olyan rendelkezést tartalmaz az adatvédelmi incidensekkel kapcsolatban, amelyekkel az adatkezelőknek (és az adatfeldolgozóknak is) tisztában kell lenniük. Magyarországon 2018. május 25-ig az Info tv. 2015. október 1-től hatályos szabályai tartalmazzák az adatvédelmi incidensekre vonatkozó általános szabályokat és írnak elő az adatkezelőre nézve bizonyos kötelezettségeket incidens bekövetkezése esetén (az incidensekről nyilvántartást kell vezetni és az érintett kérelmére az incidensek körülményeiről tájékoztatást kell adni). Míg az Info. tv. szabályai nem írnak elő bejelentési kötelezettséget a NAIH felé, illetve az érintetteket is csak kérelmükre kell tájékoztatni, addig május 25-e után e téren jelentős változásokra kell számítani.

Az adatvédelmi incidens fogalma szorosan kapcsolódik a személyes adatok integritásának és bizalmas jellegének elvéhez [Rendelet 5. cikk (1) bekezdés f) pont]: "*a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.”*

Az Info. tv. az adatvédelmi incidens fogalmát ekképp összegzi: „*személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás,*

továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés."

A Rendeletben szereplő definíció szerint adatvédelmi incidensnek minősül "*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."*

A fenti tág definíció alapján tehát nagyon sokféle adatvédelmi incidens előfordulhat, ide tartozhat például egy személyes adatokat is tartalmazó laptop elvesztése, egy elektronikus információs rendszert ért fenyegetés[4] vagy biztonsági esemény[5], de akár egy rossz helyre küldött levél vagy e-mail is e körbe tartozik. A biztonsági események kezelésére az adott elektronikus információs rendszer biztonsági osztályba sorolt értékével arányos védelmi intézkedéseket kell a BM rendelet szerint bevezetni. Mivel az elektronikus információs rendszerekben általánosan megvalósul a személyes adatok kezelése, minden biztonsági esemény alkalmával vizsgálni kell az adatvédelmi incidens bekövetkezését is. Nagyon fontos ugyanakkor észben tartani, hogy egyetlen személy, egyetlen személyes adatát érintő incidens is adatvédelmi incidensnek tekinthető!

Az Irányelv 29-es cikke szerinti Munkacsoport 2014-es véleménye (2014/3. sz. vélemény) számos gyakorlati példán keresztül is bemutatja, hogy mi tekinthető adatvédelmi incidensnek és ezek milyen következményekkel járhatnak. (Bár a vélemény még a 2002/58/EK irányelvre, az ún. Elektronikus hírközlési adatvédelmi irányelvre tekintettel született, de tanulmányozása hasznos segítséget nyújt a Rendeletre való felkészüléssel kapcsolatban is.)

A Rendelet (85) preambulum bekezdése rögzíti, hogy "*az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között*

- *a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,*
- *a hátrányos megkülönböztetést,*

[4] Ibtv. 1. § (1) bekezdés 19. pont – fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

[5] Ibtv. 1. § (1) bekezdés 9. pont – biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

- *a személyazonosság-lopást vagy a személyazonossággal való visszaélést,*
- *a pénzügyi veszteséget,*
- *az álnevesítés engedély nélküli feloldását,*
- *a jó hírnév sérelmét,*
- *a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve*
- *a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt."*

Az adatvédelmi incidensek tehát súlyos következményekkel járhatnak az érintettekre nézve, így ha megelőzni nem sikerül ezeket, fontos, hogy nagyon rövid határidőn belül intézkedések történjenek az incidensek következményeinek az elhárítása érdekében.

Az adatkezelőnek több feladata is van adatvédelmi incidens előfordulása esetén (33-34. cikk):

- az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, **legkésőbb 72 órával** a tudomásszerzést követően be kell jelenteni az illetékes felügyeleti hatóságnál (Ha a bejelentés nem történik meg 72 órán belül, akkor mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.);
- ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről;
- az adatkezelő nyilvántartja az adatvédelmi incidenseket;
- az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

„Tudomásszerzésnek" az tekinthető, amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet. A hangsúly azon van, hogy az adatkezelő azonnali vizsgálatot kezdeményezzen annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek, illetve szükséges-e bejelentést tenni az adatvédelmi incidensről.

Azt is mérlegelnie kell ezen idő alatt az adatkezelőknek, hogy kell-e tájékoztatni az érintetteket az adatvédelmi incidensről.

Ha az adatkezelő az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira

és szabadságaira nézve, akkor a bejelentés mellőzhető. (Pl. A levéltár, mint adatkezelő által rossz címre küldött levél, úgy érkezik vissza, hogy nem kerül felbontásra, azaz a személyes adatokhoz nem fért hozzá illetéktelen személy vagy – elektronikus irat esetében – a megfelelő hash algoritmussal és anonimizálási technológiával (salted) védett jelszavak esetében ha történik egy biztonsági incidens, azonban a kulcs és az anonimizálási technológia nem sérül, akkor ez sem jelent kockázatot az érintettekre nézve).

Az érintettet nem kell az adatvédelmi incidensről tájékoztatni az alábbi esetekben:

- ha a levéltár, mint adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta is (különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat);
- a levéltár, mint adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. (Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Pl. sajtóközlemény kiadása).

Az illetékes hatóság egyébként utasíthatja az adatkezelőt, hogy tájékoztassa az érintettet az adatvédelmi incidensről [lásd 58. cikk (2) e) pont]. A levéltárba kerülő iratok esetében is előfordulhat olyan eset – mely egyébiránt büntetőjogi kategória is- hogy valaki tömegesen visszaél személyes adatokkal. Ilyen esetben adatvédelmi incidensről beszélhetünk. De adatvédelmi incidens lehet a levéltárban az is, ha egy állásinterjúra jelentkező önéletrajzát rossz e-mail címre továbbítjuk. Ha a harmadik személy arról értesíti az levéltárat, hogy a jogos címzett helyett az e-mailt ő kapta meg, akkor ez is tudomásszerzésnek tekinthető. Ha egy pendrive eltűnik, amelyen titkosítatlanul személyes adatok (levéltári vagy a levéltár működése körében keletkezett személyes adatokkal, nincs jelentősége ebből a szempontból) találhatóak, akkor ez incidensnek tekinthető, és nincs jelentősége annak, hogy az egyébként nem bizonyított, hogy illetéktelen személy hozzáfért személyes adatokhoz. Természetesen az esetek súlyozása más, de incidensként a nyilvántartásba a kis súlyú incidenseket is be kell vezetni.

A Hatóság felé történő bejelentésnek tartalmaznia kell:

- az adatvédelmi tisztviselő (ha van) nevét és elérhetőségét,

- ismertetni kell az adatvédelmi incidens jellegét,

- az érintettek kategóriáit és hozzávetőleges számát,

- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,

- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket,

- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket.

Tekintettel arra, hogy adatvédelmi incidensek bármelyik levéltárban előfordulhatnak és ilyen esetekben az adatkezelőknek gyorsan kell reagálniuk, fontos, hogy az adatkezelők felkészültek legyenek ebből a szempontból is.

Az alábbi lépések megtétele általában célszerű lehet:

- az adatbiztonsági intézkedések áttekintése (figyelemmel a beépített adatvédelem elvére is);
- ha a levéltár adatvédelmi hatásvizsgálatot végez, akkor ki kell térni az esetleges incidensek kezelésére is;
- belső szabályzatban lehet rendezni az incidensek kezelésével kapcsolatos teendőket, felelősségi köröket (ez tartalmazhatja a hatóság felé történő bejelentéssel kapcsolatos tennivalókat és az érintettek tájékoztatásával kapcsolatos lépéseket is);
- célszerű az adatfeldolgozókkal (munkaügyi adatok adatfeldolgozója, elektronikus levéltári iratok adatfeldolgozója) kötött szerződések áttekintése abból a szempontból is, hogy az adatkezelő haladéktalanul értesüljön az adatfeldolgozónál történt incidensről is;
- és különösen: az incidensek belső nyilvántartási rendjét kell kialakítani.

A Rendelet 33. cikk (5) bekezdése alapján: „*az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.”* A Rendelet alapján a nyilvántartás célja lehetővé tenni a felügyeleti hatóság számára, hogy ellenőrizze az incidensek bejelentésével összefüggő kötelezettségeknek való megfelelést.

Az adatvédelmi incidens-bejelentést követően a NAIH eljárásának alapvető célja az, hogy a Hatóság megállapítsa, hogy az adatvédelmi incidens:

- milyen következményt jelent (jelentett) az érintett számára,

- e hatásokat milyen módon igyekszik orvosolni (vagy már orvosolta) az adatkezelő,

- illetve, megfelelőek-e ezek az intézkedések.

Az adatvédelmi incidensvizsgálat végén a Hatóság többféle intézkedés közül választhat:

1. Elfogadja az incidens során tett intézkedéseket, és az ügy körülményei alapján nem folytat vizsgálatot.

2. Utasítja az adatkezelőt, hogy az incidens következményeinek orvoslására (mérséklésére, csökkentésére) további intézkedéseket tegyen.

3. Vizsgálatot indít az incidens alapján a Rendelet valamely rendelkezésének (adatbiztonsági intézkedések hiányossága, nem megfelelő jogalap alkalmazása) megsértése miatt.

Meg kell említeni, mivel a NAIH anyagaiban hangsúlyosan minden esetben megjelenik, a bírság kérdését. Az adatvédelmi incidensek esetén a bírság összegének terjedelme:

- az adatvédelmi incidens bejelentésével összefüggő kötelezettségek megszegése esetén (például késedelmes bejelentés): 10 millió euró vagy az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-a

- anyagi jogszabály megsértése (például nem megfelelő adatbiztonsági intézkedések): 20 millió euró vagy az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-a.

A fent említett összegek a bírság felső határát jelentik, de annyi bizonyos, hogy az incidenskezelést nem szabad elhanyagolni és a bejelentési kötelezettségekre oda kell figyelni.

4. Az adatvédelmi tisztviselő jogállása és feladatai (37-39. cikk)

Az alábbi leírás az Iránymutatás alapján készült.

A Rendelet értelmében az adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt kijelölni. Ez a kötelezettség a közhatalmi és közfeladatot ellátó szervekre kiterjed, így a levéltárak számára ez az előírás kötelező érvénnyel bír.

A Rendelet alapján az adatvédelmi tisztviselő kulcsszereplő az adatkezelés folyamatában, így a kijelölését, jogállását és feladatait is részletesen szabályozza a jogszabály.

A Rendelet 37. cikk (5) bekezdése úgy rendelkezik, hogy az adatvédelmi tisztviselőt „szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni". A (97) preambulum bekezdés alapján a szakértői ismeretek szükséges szintjét az adatkezelő által végzett adatkezelés, valamint az általa kezelendő személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni. A szükséges szakértelem szintje nincs szigorúan meghatározva, arányosnak kell azonban lennie a szervezet által kezelt adatok érzékenységével, összetettségével és mennyiségével. Ha például az adatkezelési tevékenység különösen bonyolult, vagy nagy mennyiségű érzékeny adatot érint, az adatvédelmi tisztviselőnek adott esetben magasabb szintű szakértelemmel és támogatással kell rendelkezni. A 37. cikk (5) bekezdése nem határozza meg az adatvédelmi tisztviselő kijelölésekor figyelembe veendő szakmai képességeket sem, fontos elem, hogy az adatvédelmi tisztviselőknek szakértelemmel kell rendelkezni a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, valamint alaposan ismernie kell a GDPR-t. Hasznos továbbá, ha a felügyeleti hatóságok elősegítik az adatvédelmi tisztviselők megfelelő és rendszeres képzését. Közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv esetében az adatvédelmi tisztviselőnek alaposan kell ismerni a szervezet igazgatási szabályait és eljárásait. Az adatvédelmi tisztviselő feladatainak teljesítésére vonatkozó képességét úgy kell értelmezni, hogy az mind a személyes tulajdonságaira és ismereteire, mind a szervezeten belüli jogállására vonatkozik. A személyes tulajdonságok közé tartozik például az integritás és a magas szintű szakmai morál; az adatvédelmi tisztviselő elsődleges feladata a GDPR-nak való megfelelés lehetővé tétele. Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában, és elősegíti a GDPR alapvető, például az adatok kezelésére vonatkozó elvekre, az érintett jogaira, a beépített és alapértelmezett adatvédelemre, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek végrehajtását.

Az adatvédelmi tisztviselő foglalkoztatási formája bármilyen lehet, lehet közalkalmazotti jogviszonyban, de ellátható a feladat az adatkezelő szervezetén kívüli magánszeméllyel vagy szervezettel kötött szolgáltatási szerződés keretében is.

A 37. cikk (7) bekezdése előírja, hogy az adatkezelő vagy az adatfeldolgozó: közzéteszi az adatvédelmi tisztviselő elérhetőségét, és közli a felügyeleti hatóságokkal az adatvédelmi tisztviselő elérhetőségét. E követelmények célja annak biztosítása, hogy az érintettek (a szervezeten belül és kívül) és a felügyeleti hatóságok könnyen és közvetlenül tudjanak fordulni az adatvédelmi tisztviselőhöz, anélkül, hogy kapcsolatba kellene lépniük a szervezet más részével. Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti (38. cikk (5) bekezdése). Az adatvédelmi tisztviselő elérhetőségének olyan információkat kell tartalmazni, amelyek révén az érintettek és a felügyeleti hatóságok könnyen el tudják érni az adatvédelmi tisztviselőt (levelezési cím, erre a célra fenntartott telefonszám és/vagy erre a célra fenntartott e-mail cím). Adott esetben a nyilvánosság tájékoztatása céljából más kommunikációs eszközök is alkalmazhatók, például egy erre a célra fenntartott forródrót vagy a szervezet honlapján az adatvédelmi tisztviselőhöz vezető kapcsolatfelvételi űrlap. A 37. cikk (7) bekezdése nem írja elő, hogy a közzétett elérhetőségnek tartalmazni kell az adatvédelmi tisztviselő nevét. Bár ez jó gyakorlat lehet, az adatkezelőnek vagy az adatfeldolgozónak és az adatvédelmi tisztviselőnek kell eldöntenie, hogy ez az adott körülmények között szükségesnek vagy hasznosnak bizonyul-e. A felügyeleti hatóság felé azonban kötelező közölni az adatvédelmi tisztviselő nevét. A Munkacsoport jó gyakorlatként azt is ajánlja, hogy a szervezet tájékoztassa alkalmazottait az adatvédelmi tisztviselő nevéről és elérhetőségéről. Például az adatvédelmi tisztviselő neve és elérhetősége az intraneten, a belső telefonkönyvben és a szervezeti ábrákon is feltüntethető.

Az adatvédelmi tisztviselő jogállását alapvetően meghatározza, hogy a GDPR 38. cikke értelmében az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő „a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon”. Az iránymutatás példálózó jelleggel felsorolja, hogy mivel lehet eleget tenni ezen követelménynek:

- az adatvédelmi tisztviselőt rendszeresen meghívják a közép- és felsővezetés megbeszéléseire.
- az adatvédelmi vonatkozású döntések meghozatalakor ajánlott a részvétele. Minden releváns információt időben kell átadni az adatvédelmi tisztviselőnek annak érdekében, hogy megfelelő tanácsot adhasson.

- az adatvédelmi tisztviselő véleményét mindig kellő súllyal kell figyelembe venni. Nézetkülönbség esetén a Munkacsoport jó gyakorlatként azt ajánlja, hogy rögzítsék annak okát, hogy miért nem az adatvédelmi tisztviselő tanácsa szerint járnak el.
- az adatvédelmi tisztviselővel haladéktalanul konzultálni kell, ha adatvédelmi vagy más incidens következett be.

Az adatkezelő vagy az adatfeldolgozó olyan adatvédelmi iránymutatásokat vagy programokat dolgozhat ki, amelyek meghatározzák, hogy mely esetekben kell az adatvédelmi tisztviselővel konzultálni.

A GDPR 38. cikkének (2) bekezdése értelmében a szervezet támogatja az adatvédelmi tisztviselőt azáltal, hogy „biztosítja számára azokat az forrásokat, amelyek [...] feladat[ai] végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek”. Különösen a következőket kell figyelembe venni:

- Az adatvédelmi tisztviselő tevékenységének aktív támogatása a felsővezetés részéről (például igazgatósági szinten).
- Az adatvédelmi tisztviselő részére elegendő idő biztosítása a feladatai ellátására. Ez különösen fontos abban az esetben, ha részmunkaidős belső adatvédelmi tisztviselőt jelölnek ki, vagy ha a külső adatvédelmi tisztviselő az adatvédelmi tevékenységet más feladatok mellett végzi. Ellenkező esetben az egymásnak ellentmondó prioritások eredményeként az adatvédelmi tisztviselő elhanyagolhatja a feladatait. Jó gyakorlat az adatvédelmi tisztviselő által végzett tevékenység időtartamának százalékos meghatározása abban az esetben, ha a feladatellátás nem teljes munkaidőben történik. További jó gyakorlat a feladat elvégzéséhez szükséges időt, az adatvédelmi tisztviselő által végzett feladatok megfelelő prioritási szintjének meghatározása, valamint az adatvédelmi tisztviselő (vagy a szervezet) számára munkaterv készítése.
- Adott esetben megfelelő támogatás a pénzügyi források, infrastruktúra (helyiségek, berendezések, eszközök) és személyzet tekintetében.
- Valamennyi alkalmazott hivatalos tájékoztatása az adatvédelmi tisztviselő kijelöléséről annak biztosítása érdekében, hogy jelenléte és működése ismertté váljon a szervezeten belül.
- Egyéb, például a személyzeti, jogi, informatikai, biztonsági stb. szolgáltatásokhoz való hozzáférés biztosítása, így az adatvédelmi tisztviselők lényeges támogatást, ráfordítást és információkat szerezhetnek e szolgáltatások részéről.

- Folyamatos képzés. Az adatvédelmi tisztviselőknek lehetőséget kell adni arra, hogy naprakészek maradjanak az adatvédelem terén elért fejlődések tekintetében. A cél az, hogy folyamatosan növeljék az adatvédelmi tisztviselők szaktudásának szintjét, és ösztönözni kell őket arra, hogy vegyenek részt adatvédelmi tanfolyamokon és a szakmai fejlődés egyéb formáiban, például a magánélet védelmével foglalkozó fórumokon, műhelyekben stb.
- Tekintettel a szervezet méretére és szerkezetére, előfordulhat, hogy létre kell hoznia egy – az adatvédelmi tisztviselőből és alkalmazottaiból álló – adatvédelmi tisztviselői csoportot. Ilyen esetekben világosan meg kell határozni a csoport belső struktúráját, valamint az egyes tagok feladatait és felelősségét. Hasonlóképpen, ha az adatvédelmi tisztviselő tevékenységét külső szolgáltató végzi, az ennél a szervezetnél dolgozó személyek csoportja az ügyfél számára kijelölt vezető kapcsolattartó felelőssége mellett csoportként ténylegesen elláthatja az adatvédelmi tisztviselő feladatait. Általában véve, minél összetettebbek és/vagy érzékenyebbek az adatkezelési műveletek, annál több forrást kell biztosítani az adatvédelmi tisztviselőnek. Az adatvédelmi tevékenységnek hatékonynak kell lennie és megfelelő forrásokkal kell rendelkeznie az elvégzendő adatkezelés tekintetében.

A 38. cikk (3) bekezdése bizonyos alapvető garanciákat biztosít annak érdekében, hogy az adatvédelmi tisztviselők képesek legyenek a szervezetükön belül megfelelő szintű önállósággal ellátni feladataikat. Mindenekelőtt, az adatkezelő és az adatfeldolgozó köteles biztosítani, hogy az adatvédelmi tisztviselő „a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el”. A (97) preambulum bekezdés ezt kiegészíti azzal, hogy az adatvédelmi tisztviselők „ – függetlenül attól, hogy az adatkezelő alkalmazásában állnak-e – módjában kell, hogy álljon kötelezettségeik és feladataik független ellátása”. Ez azt jelenti, hogy a 39. cikk szerinti feladataik teljesítése során az adatvédelmi tisztviselők nem utasíthatók arra, hogyan kezeljenek egy ügyet, például milyen eredményeket kell elérni, hogyan kell kivizsgálni egy panaszt, vagy kell-e konzultálni a felügyelő hatósággal. Ezenkívül nem utasíthatók arra, hogy az adatvédelmi joggal kapcsolatos valamely ügyben – például a jogszabály egy adott értelmezését illetően – egy bizonyos álláspontot képviseljenek. Ehhez kapcsolódó előírás a 38. cikk (3) bekezdése, amely úgy rendelkezik, hogy az adatvédelmi tisztviselő „közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel”. Az ilyen közvetlen jelentéstétel biztosítja, hogy a felső vezetés ismerje – az adatvédelmi tisztviselőnek az adatkezelő vagy adatfeldolgozó tájékoztatására és tanácsadására

irányuló küldetése részeként – az adatvédelmi tisztviselő tanácsát és ajánlásait. A közvetlen jelentéstétel másik példája a legfelső vezetés részére éves jelentés készítése az adatvédelmi tisztviselő tevékenységeiről.

A függetlenség erősítésére szolgál a 38. cikk (3) bekezdése, melynek értelmében az adatvédelmi tisztviselőket „feladatai[k] ellátásával összefüggésben nem bocsáthatj[ák] el és szankcióval nem sújthatj[ák]".

A 38. cikk (6) bekezdése alapján az adatvédelmi tisztviselő „más feladatokat is elláthat". A rendelkezés előírja, hogy a szervezetnek biztosítani kell, hogy „e feladatokból ne fakadjon összeférhetetlenség". Az összeférhetetlenség hiánya szorosan kapcsolódik a független működéshez fűződő követelményhez. Bár az adatvédelmi tisztviselőknek lehetnek más feladataik, csak olyan egyéb feladatokkal bízhatók meg, amelyek nem okoznak összeférhetetlenséget. Ez különösen azt jelenti, hogy az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit. Az egyes szervezetek sajátos szervezeti felépítése miatt ezt eseti alapon kell megállapítani. Az összeférhetetlenséget okozó szervezeten belüli pozíciók lehetnek a felsővezetői pozíciók (pl. humán erőforrás vezető vagy informatikai osztályvezetők), de más, a szervezeti struktúrában alacsonyabb szinten lévő pozíciók is, ha ezek a pozíciók az adatkezelés céljainak és eszközeinek meghatározásával járnak. Ezenkívül összeférhetetlenség merülhet fel például, ha a külső adatvédelmi tisztviselőt az adatkezelő vagy az adatfeldolgozó bíróság előtti képviseletére kérik fel adatvédelmi kérdéseket érintő ügyekben. A szervezet tevékenységeitől, méretétől és szerkezetétől függően jó gyakorlat lehet az adatkezelők vagy az adatfeldolgozók számára:

- azon pozíciók meghatározása, amelyek összeegyeztethetetlenek az adatvédelmi tisztviselő tevékenységével
- e célból belső szabályok megállapítása az összeférhetetlenség elkerülése érdekében
- általánosabb magyarázat nyújtása az összeférhetetlenségről
- e követelmény tudatosításának módjaként nyilatkozat arról, hogy az adatvédelmi tisztviselő nem összeférhetetlen az adatvédelmi tisztviselőként végzett feladatai tekintetében
- a szervezet belső szabályaiban biztosítékok szerepeltetése, és annak biztosítása, hogy az adatvédelmi tisztviselői pozíció betöltésére vagy szolgáltatási szerződés megkötésére vonatkozó felhívás kellően pontos és részletes az összeférhetetlenség elkerülése érdekében.

Az adatvédelmi tisztviselő feladatai:

a) A GDPR-nak való megfelelés ellenőrzése

A megfelelés ellenőrzésére vonatkozó feladatai részeként az adatvédelmi tisztviselők különösen az alábbiakat tehetik:

- információt gyűjt az adatkezelési tevékenységek meghatározása érdekében
- elemzi és ellenőrzi az adatkezelési tevékenységek megfelelőségét
- tájékoztatást, szakmai tanácsadást nyújt és ajánlásokat bocsát ki az adatkezelő vagy az adatfeldolgozó részére.

A megfelelés ellenőrzése nem jelenti azt, hogy az adatvédelmi tisztviselő személyesen felelős a rendelkezések be nem tartásáért. A GDPR egyértelművé teszi, hogy nem az adatvédelmi tisztviselő, hanem az adatkezelő köteles „megfelelő technikai és szervezési intézkedéseket [...] végre[hajtani] annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik” (24. cikk (1) bekezdése). Az adatvédelmi rendelkezések betartása nem az adatvédelmi tisztviselő, hanem az adatkezelő szervezeti felelőssége.

b) adatvédelmi hatásvizsgálat segítése

A beépített adatvédelem elve értelmében a 35. cikk (2) bekezdése kifejezetten előírja, hogy az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő „szakmai tanácsát köteles kikérni”. A 39. cikk (1) bekezdésének c) pontja pedig azt a feladatot írja elő az adatvédelmi tisztviselő részére, hogy „kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését”. A Munkacsoport azt ajánlja, hogy az adatkezelő az adatvédelmi tisztviselő szakmai tanácsát különösen az alábbi kérdésekben kérje ki:

- kell-e adatvédelmi hatásvizsgálatot végezni
- milyen módszereket kell követni az adatvédelmi hatásvizsgálat elvégzésekor
- az adatvédelmi hatásvizsgálatot szervezeten belül végezzék-e el, vagy kiszervezzék-e azt
- milyen biztosítékokat (beleértve a technikai és szervezési intézkedéseket) kell alkalmazni az érintettek jogait és érdekeit érintő kockázatok enyhítésére
- az adatvédelmi hatásvizsgálatot megfelelően végezték-e el, és a következtetései (lehet-e folytatni az adatkezelést, és milyen biztosítékokat kell alkalmazni), megfelelnek-e a GDPR-nek.

c) együttműködés a felügyeleti hatósággal és kapcsolattartóként való eljárás

A 39. cikk (1) bekezdés d) és e) pontja alapján az adatvédelmi tisztviselő „együttműködik a felügyeleti hatósággal”, és „az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

d) kockázatalapú megközelítés

A 39. cikk (2) bekezdése értelmében az adatvédelmi tisztviselő feladatait „az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi”. A rendelkezés lényegében azt írja elő, hogy az adatvédelmi tisztviselők rangsorolják a tevékenységeiket, és a magasabb adatvédelmi kockázatot jelentő ügyekre összpontosítsanak. Ez nem jelenti azt, hogy nem kell ellenőrizniük az olyan adatkezelési műveletek megfelelését, amelyek viszonylag alacsonyabb kockázati szintet jelentenek, hanem arra utal, hogy elsősorban a magasabb kockázatú területekre kell összpontosítaniuk. Ez a szelektív és gyakorlatias megközelítés segíti az adatvédelmi tisztviselőt az adatkezelő részére az azzal kapcsolatos tanácsok nyújtásában, hogy milyen módszereket alkalmazzon az adatvédelmi hatásvizsgálat elvégzésekor, mely területeket kell belső vagy külső adatvédelmi auditnak alávetni, milyen belső képzéseket kell biztosítani az adatkezelési tevékenységekért felelős alkalmazottaknak vagy vezetésnek, és mely adatkezelési műveletek igényelnek több időt és forrást.

e) nyilvántartás vezetése

A Rendelet 30. cikk (1) és (2) bekezdése az adatkezelő felelősségeként írja elő a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartás vezetését. A gyakorlatban célszerű ezt a feladatot is az adatvédelmi tisztviselőre bízni. Ezt a nyilvántartást az egyik olyan eszköznek kell tekinteni, ami lehetővé teszi az adatvédelmi tisztviselő számára, hogy teljesítse a megfelelés ellenőrzését, a tájékoztatást és az adatkezelő vagy az adatfeldolgozó részére végzett tanácsadást.

5. Az adatkezelési tevékenységek nyilvántartása (30 cikk)

A Rendelet alapján minden adatkezelő köteles lesz nyilvántartást vezetni a következő információkról:

- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés céljai;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

- olyan 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;
- ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
- ha lehetséges, az adatbiztonsági technikai és szervezési intézkedések általános leírása.

A levéltárak számára javasolt megoldás a 27/2015. (V. 27.) EMMI rendelet által előírt kötelező nyilvántartások adatvagyon nyilvántartásként történő kezelése kiegészítve a fenti, Rendelet által előírt adatokkal.

4. Belső szabályzatok

Az adatvédelem területén rendkívül sokrétű szabályozási rendszert különböztetünk meg attól függően, hogy ki a szabályozás címzettje, valamint min a szabályozás tárgyköre. Az adatvédelmi szabályzatok készítése esetén ezért tipikus gyakorlati probléma, hogy ténylegesen több szabályzat és legalább egy átfogó tájékoztató elkészítése szükséges az adatkezelők részéről, ha egy adatkezelő minden adatkezelési esetet az előírásoknak megfelelően le kíván szabályozni, de úgy, hogy az egyes címzettek csak a számukra releváns információkat kapják meg. A szabályzatokkal szembeni fő elvárás, hogy világosan rögzítse azt, hogy a külső megkeresések és a belső folyamatok alapján keletkezett ügyeket kinek és milyen eljárás keretében kell kezelnie az adatkezelő szervezetén belül.

A levéltárak esetében a GDPR alapján minimálisan az alábbi releváns szabályozási területeket kell kialakítani és szabályzatot alkotni:

Javasolt szabályzat megnevezése	Tartalmi javaslat
Általános belső adatkezelési szabályzat	A belső adatkezelési szabályzat azokat az eseteket szabályozza, amely a Rendelet szerinti általános kötelezettségek teljesítésének eljárásrendjét írja le.
Az adatigények teljesítésére vonatkozó belső adatkezelési szabályzat	Terjedelmét és fontosságát tekintve külön javasoljuk szabályozni az adatigények teljesítésével kapcsolatos adatvédelmi kérdéseket.
Külső adatkezelési szabályzat	A közfeladatot ellátó szerveknek

Javasolt szabályzat megnevezése	Tartalmi javaslat
	adatvédelmi szabályzatot kell közzétenniük. Ennek, a gyakorlati tapasztalatok alapján, tartalmában inkább az adatkezelési tájékoztató tartalmi elemeit kell követni, az érintettek számára az adatkezeléssel kapcsolatos alapvető információkat, jogorvoslati lehetőségeket kell tartalmaznia.
Informatikai fejlesztések adatvédelmi garanciáit leíró szabályzat	Az informatikai fejlesztések szinte minden esetben adatkezeléssel is járnak, ezért szabályozni szükséges, hogy az adatkezelési garanciák biztosítása érdekében milyen eljárásrendet kell követni a fejlesztések tervezése során. Azért került külön szabályzatba ez a téma, mivel tartalmát tekintve, egyaránt az informatikai biztonsági, informatikai fejlesztési és az adatvédelmi szabályzat részét is képezheti.
Adatkezelési tájékoztató a kutatói adatkezelésekre	A levéltárakban jelenleg is használatos kutatási szabályzat keretei között kell szabályozni a személyes adatokat tartalmazó iratok kutatásának és nyilvánosságra hozatalának feltételeit és lehetőségeit.
Magatartási kódex	A GDPR 4. cikke ösztönzi a tisztességes és átlátható adatkezelés érdekében magatartási kódexek megalkotását. A magatartási kódex az ágazat sajátosságainak megfelelően tartalmazhatja a speciális szabályokat. Alkalmazásához a NAIH jóváhagyása szükséges.

6. Adatfeldolgozási szerződés

Mivel személyes adatot kezelni csak valamely, korábban ismertetett jogalap megléte esetén lehet és az egyes feladatok kiszervezése révén lehetővé vált, hogy az adatkezeléssel kapcsolatos döntések meghozatala, és azok technikai végrehajtása elkülönüljön, szükségessé vált az adatfeldolgozás fogalmának megalkotása, melyhez eltérő felelősségi szabályok társulnak, a hozzájárulás helyett csak a tájékoztatási kötelezettségnek kell eleget tenni.

A Rendelet is elhatárolja a két fogalmat a 4. cikkében:

„adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

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

Adatkezelőnek nevezzük tehát azt, aki az adatkezelés célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza. Adatfeldolgozó, aki az adatkezeléshez kapcsolódó technikai műveleteket elvégzi. Az adatkezelésre vonatkozó döntéseket az adatkezelő maga is végrehajthatja (ekkor csak adatkezelőről beszélünk, és nincs adatfeldolgozó), de adatfeldolgozó megbízottjával is végrehajtathatja.

A jelenleg hatályos Info. tv. megfogalmazásában:
adatkezelő: „*az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja*.”
adatfeldolgozás: „*az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik*.”
Az Info tv. az adatkezelő-adatfeldolgozó közti viszonyt is meghatározza:
A 10. § (3) bekezdése alapján „*az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját célra adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni*”.

Tipikus esete az adatfeldolgozásnak, amikor egy szolgáltató szeretne minden hónap elsején néhány tízezer számlát kinyomtatni. Sem technikai, sem humán erőforrással nem rendelkezik, és nem is lenne gazdaságos, ha havi egy napi kihasználtsággal tartaná fenn a kiszolgáló egységet. Ezért átadja ügyfelei nevét, címét, a számla tartalmát egy nyomdának, aki a számlákat kinyomtatja és postára adja. Levéltári területen egy digitalizálás során történő adatrögzítés kerülhet ebbe a körbe vagy egy olyan, szolgáltató kezelésében lévő honlap, melyre a levéltár tartalmakat tesz fel, vagy ha az elektronikus levéltári iratanyagot nem a levéltár, hanem külső szolgáltató tárolja. Természetesen mindegyik esetben csupán akkor, ha személyes adatok kezelése történik.

Az adatfeldolgozónak a személyes adatokon végzett tevékenységére vonatkozó érdemi döntéseket az adatkezelő hozza meg. Az adatfeldolgozó döntéshozatalát a Rendelet ki is zárja. Ha a megbízott döntést hoz, akkor ő nem adatfeldolgozó, hanem adatkezelő lesz, így a részére történő adattovábbításhoz az érintett hozzájárulására van szükség. Ebből következik az is, hogy az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felelős.

Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe. Az adatfeldolgozó az adatokat csak az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára nem használhatja fel az adatokat.

Már az Info. tv. is előírta, hogy az adatfeldolgozásra irányuló megbízást írásba kell foglalni. A megbízott adatfeldolgozó további alvállalkozót nem vehet igénybe. A Rendelet sematározza meg az adatfeldolgozói szerződés kötelező formáját, tartalmi elemeit. Egy adatfeldolgozói szerződés javasolt tartalmi elemei az alábbiak:

- adatkezelő és adatfeldolgozó megnevezése
- adatfeldolgozói feladat
- a feldolgozásra átadott adatbázis, az adatok köre
- rendelkezés a szerződés teljesítése, megszűnése esetére
- felelősségi kérdések, illetve helytállás harmadik személy irányába.

Fontos, hogy amennyiben bármely olyan feladat kiszervezésre kerül, ami esetében a levéltár adatkezelő és egy adott másik szerv adatfeldolgozói szerepkörbe kerül, úgy készüljön adatfeldolgozói szerződés is.

Információbiztonságra vonatkozó szabályozási és szervezetfejlesztési feladatok

Az informatikai védelem az informatikai biztonság megteremtésének eszköze, az informatikai biztonság pedig az informatikai védelem eredménye. Az adatvédelem az informatikai védelemnek az embert, az adatalanyt a középpontjába állító vetülete (data protection). Ez azonban valójában nem az adat, hanem az adatalany védelmét jelenti (tehát a jogi oldalról szól). Az informatikai védelemnek az adatot a középpontjába állító vetülete az adatbiztonság (data security). Ez azonban valójában nem biztonsági, hanem védelmi kategória, nem cél, hanem eszköz: az adatalany védelme érdekében az adat védelmének műszaki, technikai eszköze.

Az adatbiztonság nem biztonsági, hanem védelmi kategória, azon védelmi módszerek összessége, amelyeket az adatokon hajtanak végre az adatalany, illetve az érintett, valamint az adatkezelő védelme érdekében.

Az adatbiztonság fogalmát az Info tv. határozza meg:

„7. § (1) *Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét*. „

A 7. § (1) bekezdése deklarálja a célt, illetve azt is, hogy kik kötelesek megtervezni és végrehajtani az adatkezelési műveleteket oly módon, hogy ezt a célt elérjék. Nevezetesen: az adatkezelő, jelen esetben a levéltár felelős azért, hogy úgy legyenek megtervezve és végrehajtva az adatkezelési cselekmények, hogy biztosítva legyen az adatalanyok magánszférájának védelme, tehát a személyes adatok védelme.

„(2) *Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*”

A (2). bekezdés rögzíti, kik kötelesek gondoskodni az adatbiztonságról, kiknek kell megtenniük az adat védelmével kapcsolatos intézkedéseket a célból, hogy ezek az intézkedések megfeleljenek az Info tv.-nek, a Rendeletnek illetve az egyéb adat- és titokvédelmi szabályoknak. Tehát az adatkezelőnek és tevékenységi körében az adatfeldolgozónak – a jogszabályok és az adatkezelő által meghatározott keretek között – kell gondoskodnia az adatok biztonságáról. Fontos szófordulat – főképp az elszámoltathatóság

elve alkalmazásánál -, hogy a levéltár **köteles** a védelmi intézkedések lehetséges irányait: technikai és szervezési intézkedéseket, eljárási szabályokat kialakítani.

„(3) *Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen*."

A (3). bekezdés példálózó felsorolás arra, milyen veszélyek ellen kell adatainkat megvédeni. Lényeges, hogy a védelem megfelelő szintjének eléréshez valamilyen tervvel, szabályozással a levéltárnak rendelkeznie kell.

(4) *A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. …….. (6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.*'

A (4). bekezdés egy egyértelmű előírást tartalmaz, az (5). bekezdés a személyes adatok automatizált feldolgozásával foglalkozik, ez a levéltárban nem releváns és a (6). bekezdés arra utal, hogy a jog mindig a technikai fejlődés után „kullog", a jog csak a meglévőt tudja szabályozni. A védelemnek tehát a technika előre meg nem fogalmazható mindenkori fejlettségéhez kell igazodnia.

A jogszabály mind a kereteket, mind a feladatokat egyértelműen kijelöli. Az informatikai biztonság fogalmából és az Info tv. rendelkezéseiből kiindulva összefoglalhatóak azok a védelmi módszerek, amelyekkel az adat biztonsága megvalósítható: ezek az adatbiztonság összetevői.

A Közigazgatási Informatikai Bizottság (KIB) 25. számú ajánlása a következőképp definiálja az informatikai biztonságot. Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a

rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Az elektronikus információbiztonsághoz kapcsolódó alapfogalmakat – melyeket már a fent említett KIB ajánlás is használt az informtikai biztonság témakörében az Ibtv. jogi norma szintjére emelte. Az Ibtv. értelmező rendelkezései között rögzíti, hogy az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos[6].

A felsorolt fogalmakat az IBtv. értelmező rendelkezései az alábbiak szerint definiálják:

- Bizalmasság[7]: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
- Sértetlenség[8]: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
- Rendelkezésre állás[9]: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
- Zárt védelem[10]: az összes számításba vehető fenyegetést figyelembe vevő védelem;
- Teljes körű védelem[11]: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
- Folytonos védelem[12]: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

[6] Ibtv. 1. § (1) bekezdés 9. pont
[7] Ibtv. 1. § (1) bekezdés 8. pont
[8] Ibtv. 1. § (1) bekezdés 39. pont
[9] Ibtv. 1. § (1) bekezdés 38. pont
[10] Ibtv. 1. § (1) bekezdés 48. pont
[11] Ibtv. 1. § (1) bekezdés 44. pont

- Kockázattal arányos védelem[13]: kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

Ha az elektronikus információs rendszer környezete vagy valamely eleme olyan állapotban van, hogy fennáll a bizalmasság, a sértetlenség vagy a rendelkezésre állás sérülése, akkor az adott elem a fenyegetettség állapotába került, amely mindig valamilyen veszélyforrásból kiindulva következik be. A veszélyforrás jelentkezhet a környezeten belül, például lehet valamilyen nem kellően megszervezett vagy végrehajtott védelmi intézkedés, cselekmény, hibásan működő hardver vagy szoftver, a valóságnak meg nem felelő (esetleg módosított) adat, az adatkezelési tevékenység ellátására alkalmatlan objektum vagy helyiség, bizalmasságában sérült humán erőforrás. A veszélyforrás azonban eredhet a környezeten kívülről is, így lehet valamilyen külső ráhatás, természeti csapás, robbanás a szervezet működési környezetében stb. Ezek a külső veszélyforrások általában a vis maior kategóriájába tartoznak ugyan, az adatbiztonság azonban éppen arra irányul, hogy az adatokat ezek egy része ellen is védje.

Ha az elektronikus információs rendszer sérül és személyes adatok harmadik, illetéktelen személy tudomására jutnak, akkor adatvédelmi incidensről is szó van.

Az elektronikus információs rendszert érintően a humán veszélyforrások két irányból jelentkezhetnek: Egyrészt belülről, amely esetben a humán erőforrások bizalmassága, sértetlensége és rendelkezésre állása sérül. Másrészt viszont humán veszélyforrásnak tekinthetjük a kívülről eredő, az informatikai biztonság kedvező állapotának megváltoztatását célul kitűző szándékos emberi magatartásokat, cselekményeket. A belülről jelentkező veszélyforrások alapja általában a nem megfelelő szintű adatvédelmi és adatbiztonsági tudatosság, amelynek következményei az adatvédelmi és adatbiztonsági szabályok be nem tartása, a veszély túlzott lekicsinylése, ilyen módon a túlzott biztonságérzet kialakulása

A sérülésből eredő adatvédelmi kockázatot megfelelő szabályzatok létrehozásával, azok betartásával, a munkatársak folyamatos oktatásával lehet csökkenteni. Amiképp az elektronikus iratok mennyiség nő, úgy válik a levéltárakban mind fontosabbá az információbiztonság megteremtése, fenntartása, védelme.

---

[12] Ibtv. 1. § (1) bekezdés 21. pont
[13] Ibtv. 1. § (1) bekezdés 31. pont

A téma bővebb kifejtésére jelen tájékoztató keretében nincs lehetőség, de további tanulmányozásra a fejezet tartalmához felhasznált egyetemi jegyzet, Törley Gábor: Adatbiztonság a közigazgatásban c. műve ajánlható.

Archiválási célú kivételek szabályozása

A Rendelet szigorú szabályok közt korlátozza a személyes, kivált a különleges adatok körének az érintetten kívüli megismerhetőségét. Ez ugyanakkor nem újdonság, hisz az Info. tv. is szigorú korlátokat alkalmazott és a szektorális törvénnyel, az Ltv.-vel az eltelt évek tanúsága szerint az összhangot is sikerült megteremteni.

A Rendelet két nagy újdonságáról már esett szó, az egyik az álnevesítés, a másik az elfeledtetéshez való jog. Amennyiben a személyes adatok védelménél az érintetti jogok mindent megelőznének, úgy a történeti múlt kutatása jelentősen megnehezülne, egyes esetekben ellehetetlenülne.

A Rendelet alkotói ezért több kivételt is megállapítottak, amikor az adatok (iratok) megőrzése, adott esetben megismerhetővé tétele az érintetti jogokat megelőzi. A Rendelet szövege alapján a **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott további adatkezelést összeegyeztethető, jogszerű adatkezelési műveleteknek kell tekinteni. Bár a közérdekű archiválás fogalma a magyar jogban nem definiált, mégis nyilvánvaló, hogy a levéltárak tevékenysége a Rendelet fogalomkörébe tartozik. A Rendelet kivételekkel foglalkozó szakaszait kiemeltük, mint a levéltári adatvédelmi tudatosság alapelveit.

Már a Rendelet preambulum bekezdései is foglalkoznak a kivételi körrel, melyet minden esetbe félkövérrel jelölünk:

A (160). preambulum bekezdés egyértelműen leszögezi:

> „*E rendeletet a **történelmi kutatási** célokból kezelt személyes adatok esetében is alkalmazni kell. Ide kell sorolni a történelmi kutatásokat és a genealógiai célú kutatást is, szem előtt tartva, hogy e rendelet elhunyt személyre nem alkalmazandó*."

A Polgári Törvénykönyv (2013. évi V. törvény 2:50. §) a kegyeleti jogot a személyiségi jogok között sorolja fel. A levéltárakban fokozottan kell tekintettel lenni a kegyeleti jogra is, hisz az elhunyt ember emlékének megsértése miatt bírósághoz fordulhat a hozzátartozó vagy az, akit az elhunyt végrendeleti juttatásban részesített.

Az (50) preambulum bekezdés az első, melyben a személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelésének elveit rögzítik:

„A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését. Ha az adatkezelés közérdekből elvégzendő feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása érdekében szükséges, uniós vagy tagállami jog meghatározhatja és pontosan leírhatja azokat a feladatokat és célokat, amelyek tekintetében a további adatkezelés jogszerűnek és összeegyeztethetőnek tekintendő. A ***közérdekű archiválás*** *céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott további adatkezelést összeegyeztethető, jogszerű adatkezelési műveleteknek kell tekinteni. Az uniós vagy tagállami jogban foglalt, a személyes adatok kezelésére vonatkozó jogalap a további adatkezeléshez is jogalapul szolgálhat. Annak megállapításához, hogy a további adatkezelés célja összeegyeztethető-e a személyes adatok gyűjtésének eredeti céljával, az adatkezelő – az eredeti adatkezelés jogszerűségére vonatkozó valamennyi előírás teljesítését követően – figyelembe veszi többek között minden, az említett eredeti célok és a tervezett további adatkezelési célok között fennálló összefüggést, az adatgyűjtés körülményeit, ideértve különösen az érintettnek a további adatfelhasználásra vonatkozó, az adatkezelővel fennálló kapcsolatán alapuló észszerű elvárásait is, továbbá a személyes adatok jellegét, a tervezett további adatkezelés következményeit az érintettekre nézve, valamint a megfelelő garanciák meglétét mind az eredeti, mind a tervezett további személyesadat-kezelési műveletek során. Ha az érintett hozzájárulását adta, illetve ha az adatkezelés uniós vagy tagállami jogon alapul, és egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül bizonyos fontos közérdekek védelme szempontjából, a célok összeegyeztethetőségétől függetlenül az adatkezelő jogosult a szóban forgó adatokon további adatkezelést végezni. Minden esetben biztosítani kell az e rendeletben rögzített elvek érvényesülését, valamint különösen az érintett tájékoztatását ezen egyéb célokról és a jogairól, ideértve a tiltakozáshoz való jogról.*”

A közérdekű archiválás tehát teljesen törvényes jogalap a személyes adatok kezeléséhez, de ebben az esetben is figyelembe kell venni a nemzeti jog szabályait.

A különleges adatok a rendelet szerint alapesetben nem kezelhetőek, ezt rögzíti az (51) preambulum bekezdés. Ehhez képest állapít meg kivételeket a Rendelet. Fontos szabály, hogy a személyes adatok különleges kategóriáinak kezelésére vonatkozó általános tilalomtól való eltérésről kifejezetten rendelkezni kell, még az érintett egyértelmű hozzájárulása esetén is. A kivételeket az (52) preambulum bekezdés rögzíti:

„*A személyes adatok különleges kategóriáira vonatkozó adatkezelési tilalomtól való eltérés szintén megengedhető, ha erről az uniós vagy tagállami jog rendelkezik, és ha arra megfelelő garanciák mellett kerül sor a személyes adatok és más alapvető jogok védelme érdekében, ha ez valamely közérdeken alapul, így különösen a foglalkoztatási jog és a szociális védelmi jog területén, a nyugdíjakat is beleértve, valamint a népegészség-védelem, a nyomonkövetési és riasztási célok, a fertőző betegségek és más súlyos egészségügyi veszélyek megelőzése, valamint az ellenük való védekezés érdekében végzett személyesadat-kezelés esetében. Ezekre az eltérésekre egészségügyi célokból – köztük a népegészségüggyel és az egészségügyi szolgáltatások irányításával kapcsolatos célokból – kerülhet sor, különösen annak biztosítása érdekében, hogy az egészségbiztosítási rendszer szolgáltatásaival és juttatásaival kapcsolatos igények rendezésére szolgáló eljárások magas szintűek és költséghatékonyak legyenek, továbbá a* ***közérdekű archiválás*** *céljából, tudományos és történelmi kutatási célból vagy statisztikai célból. Eltérés alapján az ilyen személyes adatok kezelése olyan esetekben lehetséges, amikor az jogi igények előterjesztése, érvényesítése, illetve védelme céljából szükséges, függetlenül attól, hogy erre bírósági eljárás, közigazgatási, vagy egyéb, nem bírósági útra tartozó eljárás keretében kerül-e sor.”*

Az egészségügyi adatok védelméről, kezeléséről és a kivételekről az (53) preambulum bekezdés rendelkezik:

„*A különleges kategóriába tartozó, magasabb szintű védelmet igénylő személyes adatokat kizárólag abban az esetben lehet az egészséggel kapcsolatos célokból kezelni, ha az az említett céloknak a természetes személyek és a társadalom egészének érdekében történő eléréséhez szükséges, különösen az egészségügyi és szociális szolgáltatások és rendszerek irányításának összefüggésében, beleértve azt is, amikor az irányító és központi nemzeti egészségügyi hatóságok a következő célokból végzik az ilyen adatok kezelését: minőségellenőrzés, információkezelés, valamint az egészségügyi és szociális rendszer általános országos és helyi felügyelete, továbbá az egészségügyi és szociális ellátás, a határokon átnyúló egészségügyi ellátás, valamint a népegészség-védelem*

folytonosságának biztosítása, nyomonkövetési és riasztási célok, a ***közérdekű archiválás céljából****, tudományos és történelmi kutatási vagy statisztikai célból közérdekű célt szolgáló uniós vagy tagállami jog alapján, illetve a népegészség területén közérdekből készített tanulmányok céljából. Ebből kifolyólag a sajátos adatkezelési szükségletek tekintetében ebben a rendeletben harmonizált feltételeket kell meghatározni az egészségügyi személyes adatok különleges kategóriáinak kezelésére vonatkozóan, különösen azt illetően, ha ezen adatok kezelését bizonyos egészséggel kapcsolatos célokból olyan személyek végzik, akikre jogszabályban megállapított szakmai titoktartási kötelezettség vonatkozik. Az uniós vagy tagállami jogban rendelkezni kell olyan célzott és megfelelő intézkedésekről, amelyek a természetes személyek alapvető jogainak és személyes adatainak védelmére irányulnak. A tagállamok további feltételeket – például korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan. Ez azonban nem akadályozhatja a személyes adatok Unión belüli szabad áramlását azokban az esetekben, amikor az említett feltételek az ilyen adatok határokon átnyúló kezelésére vonatkoznak*."

A nemzeti jognak tehát követnie kell a Rendelet szabályait, igazodnia kell hozzá és a Rendelet szellemiségének megfelelően kell a tagállami jogszabályokat meghozni. (Ezek még Magyarországon nem történtek meg).

A (62) preambulum bekezdés külön kiemeli a tájékoztatás nyújtására vonatkozó kötelezettségre vonatkozó kitételeket, amelyek nagyon fontosak a levéltárba kerülő iratanyag szempontjából, hiszen ha az általános tájékoztatási kötelezettség minden személyes adatot tartalmazó, levéltárba került vagy kerülő iratanyagnál fennállna, úgy a levéltári alapfeladat ellátás ellehetetlenülne. De a tájékoztatás elmaradása esetén az érintettek számát, az adatok korát, valamint az elfogadott megfelelő garanciákat figyelembe kell venni. Feltehető, hogy ez utóbbi mondatnak a pontosítása a tagállami jogalkotás feladata lesz. A Rendelet így fogalmaz:

„*Mindazonáltal a tájékoztatás nyújtására vonatkozó kötelezettség előírása nem szükséges, ha az érintettnek ez az információ már a birtokában van, vagy ha a személyes adat rögzítését, illetve közlését valamely jogszabály kifejezetten előírja, vagy ha az érintett tájékoztatása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne. E helyzet állhat elő különösen akkor, ha az adatkezelés* ***közérdekű archiválás célt****, tudományos és történelmi kutatási célt vagy statisztikai célt szolgál. E tekintetben az érintettek számát, az adatok korát, valamint az elfogadott megfelelő garanciákat figyelembe kell venni."*

A (65) preambulum bekezdés az *„elfeledtetéshez való jog”*-gal kapcsolatos rendelkezéseket tartalmazza:

*„Az érintett jogosult arra, hogy kérhesse a rá vonatkozó személyes adatok helyesbítését és megilleti őt az „elfeledtetéshez való jog”, ha a szóban forgó adatok megőrzése sérti e rendeletet vagy az olyan uniós vagy tagállami jogot, amelynek hatálya az adatkezelőre kiterjed. Az érintett jogosult különösen arra, hogy személyes adatait töröljék és a továbbiakban ne kezeljék, ha a személyes adatok gyűjtése vagy más módon való kezelése az adatkezelés eredeti céljaival összefüggésben már nincs szükség, vagy ha az érintettek visszavonták az adatok kezeléshez adott hozzájárulásukat, vagy ha személyes adataik kezelése egyéb szempontból nem felel meg e rendeletnek. Ez a jog különösen akkor lényeges, ha az érintett gyermekként adta meg hozzájárulását, amikor még nem volt teljes mértékben tisztában az adatkezelés kockázataival, később pedig el akarja távolítani a szóban forgó személyes adatokat, különösen az internetről. Az érintett e jogát gyakorolhatja akkor is, ha már nem gyermek. Ugyanakkor a személyes adatok további megőrzése jogszerűnek tekinthető, ha az a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, valamely jogi kötelezettségnek való megfelelés, illetőleg közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy a népegészségügy területét érintő közérdekből, **közérdekű archiválás céljából**, tudományos és történelmi kutatási célból vagy statisztikai célból, vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges*.”

Az utolsó tagmondatban felsorolt kitételek teremtik meg a levéltári adatkezelés, feldolgozó munka, kutatásra történő előkészítés alapjait. A (156) preambulum bekezdés a kivételek, így a közérdekű archiválás tekintetében az érintettek jogai és szabadságai tekintetében megfelelő garanciákat fogalmaz meg:

„*E rendelet alapján a személyes adatok **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő kezelésére az érintettek jogai és szabadságai tekintetében megfelelő garanciák vonatkoznak. Ez említett garanciák biztosítják, hogy technikai és szervezési intézkedéseket hoztak különösen annak érdekében, hogy az adattakarékosság elve érvényesüljön. A személyes adatok **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további kezelésére akkor kerülhet sor, ha az adatkezelő előzetesen felmérte, hogy ezek a célok megvalósíthatók olyan személyes adatok kezelésével, amelyek eleve nem vagy a*

*továbbiakban már nem teszik lehetővé az érintettek azonosítását, feltéve hogy megfelelő garanciák állnak rendelkezésre (mint például a személyes adatok álnevesítése). A tagállamok megfelelő garanciákról kell rendelkezniük a személyes adatok **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő kezelése tekintetében. A tagállamok számára engedélyezni kell, hogy konkrét feltételekkel és az érintettek számára nyújtott megfelelő garanciák mellett pontosításokat és eltéréseket alkalmazzanak a tájékoztatási követelményekre, a helyesbítéshez való jogra, a törléshez való jogra, az elfeledtetéshez való jogra, az adatkezelés korlátozásához való jogra, valamint az adathordozhatósághoz való jogra, továbbá a **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő adatkezeléssel összefüggő tiltakozáshoz való jogra vonatkozóan. A szóban forgó feltételek és garanciák eredményezhetnek egyrészt az említett jogoknak az érintettek általi érvényesítését szolgáló eljárásokat – ha ez megfelelő az adott adatkezelés céljainak fényében –, másrészt az arányosság és a szükségesség elveinek érvényesítése érdekében a személyes adatok kezelésének minimálisra korlátozását célzó technikai és szervezési intézkedéseket. A személyes adatok tudományos célú kezelésének meg kell felelnie az egyéb, például a klinikai vizsgálatokat szabályozó jogszabályoknak is."*

A (158) preambulum bekezdés azon személyes adatok kezelésére vonatkozó garanciákat rögzíti, melyek személyes adatokat tartalmaznak:

„E rendeletet az archiválási célokat szolgáló személyes adatok kezelésekor is alkalmazni kell, szem előtt tartva, hogy e rendelet nem alkalmazható elhunyt személyek személyes adataira. A közérdekű adatokat tároló közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek vagy magánfél szervezetek olyan szolgálatok kell, hogy legyenek, amelyek uniós vagy a tagállami jog szerint kötelesek az általános közérdek szempontjából tartós értéket képviselő adatokat beszerezni, megőrizni, értékelni, rendezni, leírni, közölni, előmozdítani, terjeszteni, illetve azokhoz hozzáférést biztosítani. A tagállamok számára továbbá lehetővé kell tenni, hogy rendelkezzenek a személyes adatok archiválási célokat szolgáló további kezeléséről, például a volt totalitárius államrendszerek alatt tanúsított politikai magatartáshoz, népirtáshoz, az emberiesség elleni bűncselekményekhez, különösen a holokauszthoz és a háborús bűncselekményekhez kapcsolódó konkrét információk szolgáltatása érdekében."

Az alapelveket rögzítő preambulum bekezdések után következik maga a Rendelet jogi szövege. A fogalommeghatározásokról már szóltunk, a 9. cikk szabályozza a személyes

adatok különleges kategóriáinak kezelését, mégpedig alapesetben igen egyszerűen és határozottan: a felsorolt adatfajták kezelését megtiltja.

A következő szakaszban jönnek a kivételek, melyek fennállása esetén mégis – jól körülhatárolt módon – kezelhetők az ún. különleges adatok is.

„*(1) A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.*

(2) Az (1) bekezdés nem alkalmazandó abban az esetben, ha:

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

……

(4) A tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.”

A 9. cikk (2) bekezdése az itt idézetnél több kivételt enged meg a különleges adatok kezelése terén, lényegesnek a közérdekű archiválással kapcsolatos kitételek pontos közzétételét tartjuk. A kérdéskör pontos szabályozását a tagállami jogalkotás körébe utalja a Rendelet, mely még készülőben van. A (4) bekezdés levéltári szempontból nagyon fontos, hisz a sok szempontból jelenleg is neuralgikus egészségügyi adatok kezelésére vonatkozóan lehetőséget biztosít a tagállami jogalkotásnak további korlátozások bevezetésére. Ezek még nem ismertek.

Az immáron többször hivatkozott 89. cikket az alábbiakban teljes terjedelmében közöljük:

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

*(1) A személyes adatok **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelését e rendelettel összhangban az érintett jogait és szabadságait védő megfelelő garanciák mellett kell végezni. E garanciáknak biztosítaniuk kell, hogy olyan technikai és szervezési intézkedések legyenek érvényben, melyek biztosítják különösen az adattakarékosság elvének betartását. Ezen intézkedések közé tartozhat az álnevesítés, amennyiben az említett célok ily módon megvalósíthatók. Amennyiben e célok megvalósíthatók az adatok oly módon történő további kezelése révén, amely nem vagy már nem teszi lehetővé az érintettek azonosítását, a célokat ilyen módon kell megvalósítani."*

Figyelmesen olvasva egyértelműen megállapítható, hogy a kivételek csak akkor lépnek életbe, ha az érintettek jogait és szabadságát védő megfelelő garanciák is életbe léptek. Ezek egy része konkrét jogszabályokon alapul, más része jelen tájékoztató korábbi részeiben említett intézkedések, szabályozások sora.

„Az adatminimalizálás (adattakarékosság) elve lényegében megegyezik az Info tv.-ben szereplő alapelvvel. Az általános adatvédelmi rendelet szerint a személyes adatok kezelésének az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és az adatkezelésnek az elengedhetetlenül szükségesre kell korlátozódniuk. Az általános adatvédelmi rendelet elválasztja egymástól a célhoz kötött adatkezelés elvét, illetve azt az alapvető kötelezettséget, hogy a személyes adat csak a cél megvalósulásához szükséges ideig kezelhető. A rendelet ezt az elvet „korlátozott tárolhatóság" alapelveként ismeri el. A rendelet kimondja, hogy a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Ezen főszabály alól a közérdekű archiválási, tudományos és történelmi kutatási, illetve statisztikai célú adatkezelések jelenthetnek kivételt, feltéve, hogy az adatkezelők megfelelő technikai és szervezési intézkedésekkel biztosítják az érintettek személyes adatok védelméhez fűződő jogát. Ilyen intézkedés lehet az adatkezelők részéről a már korábban említett álnevesítés, amely alkalmas lehet arra, hogy például az érintett személyes adataira is kiterjedő tudományos kutatás úgy valósuljon meg, hogy a kutató előtt az érintett kiléte nem lesz ismert, minthogy az azonosításához szükséges adatokat külön tárolják." – írja a NAIH a 2016-os évről készült beszámolójában.Az álnevesítés gyakorlati megvalósítása lehet a Rendelet és az átalakítandó levéltári jogi szabályozás „ütközőköve". A személyes adat fogalmának egyik kulcseleme, hogy csak természetes személyre vonatkozó információ lehet (azaz például egy jogi személyre vonatkozó információk, pl. a cég neve,

cégjegyzékszáma, székhelye nem minősülnek személyes adatnak). A másik kulcselem pedig, hogy azonosított vagy azonosítható természetes személyre (az érintettre) kell vonatkoznia. Nem kell tehát az azonosításnak feltétlenül megtörténnie, elegendő, ha a lehetőség adott az azonosításra ("azonosít*ható*").

Az anonimizálással és az álnevesítéssel kapcsolatban a (26) preambulum bekezdés ad útmutatást:

> *„Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni. Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését. Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható. Ez a rendelet ezért nem vonatkozik az ilyen anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.”*

A levéltári kutatások során az anonimizálás az a lehetséges mód, mely a személyiségi jogok teljes körű védelmét garantálhatja és amint a fentebbi sorokból kitűnik, az anonim információkra nem kell alkalmazni a Rendelet előírásait, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.

Fontos szempont és elvárás az anonimizációval kapcsolatban, hogy a kapcsolat ne legyen többé helyreállítható, azaz a természetes személy már nem azonosítható. Ez elsőre talán

egyszerűnek tűnik, a gyakorlatban azonban számos kihívással találhatjuk szemben magunkat, hiszen a fejlődő technológiának is köszönhetően sokszor nem is olyan egyszerű feladat, hogy az adat és a természetes személy közötti kapcsolatot végérvényesen megszüntessük.

Az Irányelv 29. cikke szerinti Munkacsoport (WP29) 2014-ben kiadott egy véleményt az anonimizálási technikákról (Opinion 05/2014 on Anonymisation Techniques). A szingapúri adatvédelmi hatóság (Personal Data Protection Commission of Singapore) pedig 2018. januárjában adott ki egy összefoglalót az alapvető anonimizálási technikákról (Guide To Basic Data Anonymisation Techniques). Hasznos segítségnek bizonyulhat az angol adatvédelmi hatóság (ICO) 2012-es iránymutatása is (Anonymisation Code of Practice). Az Egyesült Királyságban egy külön szerveződés is létrejött arra, hogy a személyes adatok hatékony anonimizálásában segítséget nyújtson (UK Anonymisation Network).

A szakszerűen anonimizált adatra (iratra) nem alkalmazandók a személyes adatok védelmére vonatkozó szabályok. Ezzel szemben az álnevesített adatok továbbra is a személyes adatok védelmére vonatkozó szabályok hatókörében maradnak. Az álnevesítés lényege, hogy a személyes adatok védelme során ez az adatok magas szintű védelmének egyik eszköze. A Rendelet meghatározza az álnevesítés fogalmát és számos ponton ajánlja az adatkezelőknek az álnevesítés alkalmazását. A Rendelet (28) preambulum bekezdése szerint „*a személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint segíthet az adatkezelőknek és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek*.”

A Rendelet alapján az ***álnevesítés (pszeudonimizáció)*** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni. Nagyon fontos azonban tudni, hogy az álnevesített adatokra továbbra is alkalmazandóak az adatvédelmi szabályok, mert azok személyes adat jellegüket nem veszítik el.

A jogszabályok ismertetésén túl jelen tájékoztató az álnevesítés gyakorlatával kapcsolatban annak kialakulatlansága miatt állást foglalni nem tud. Annyi bizonyos, hogy a szerveknél történő álnevesítés, a személyes adatok külön történő tárolása, mely a NAIH álláspontja is, még jelentős problémákat okozhat az ilyen típusú adatok levéltári átvételénél, megőrzésénél

és főképp kutathatóságánál. Kérdésként merülhet fel, hogy egy, a szervnél meglévő speciális szoftver segítségével történő álnevesítés miképp lesz visszaállítható a levéltári átadáskor, tekintettel a technika gyors fejlődésére. (Vö. az elektronikus iratnyilvántartás élő problematikáját.) Annyi bizonyos, hogy a hazai jogszabályi környezet kialakításánál a rendelet előírásainak betartásával ugyan, de figyelni kell az álnevesítés közérdekű archiválás és a későbbi történeti kutatások érdekével egybeeső szabályozására.

A 89. cikk (2) és (3) bekezdése további kivételek lehetőségét tartalmazza a közérdekű archiválás tekintetében. Ezek egy részéről már volt szó (pl. az elfeledtetéshez való jognál), azon jogszabály-helyét a rendeletnek, melyekhez a tagállami jog átalakítása szükséges, részletesen nem tagaljuk, mivel ezek még nem születtek meg, így eltérést sem állapíthattak meg. A két bekezdés szövege az alábbi:

> *(„2) A személyes adatok **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott kezelése vonatkozásában az uniós vagy a tagállami jog – az e cikk (1) bekezdésében említett feltételekre és garanciákra is figyelemmel – **eltérést állapíthat meg** a 15., 16., 18. és 21. cikkben említett jogokat illetően, ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához szükség van ilyen eltérésre.*
>
> *(3) A személyes adatok közérdekű archiválás céljából való kezelése vonatkozásában az uniós vagy a tagállami jog – az e cikk (1) bekezdésében említett feltételekre és garanciákra is figyelemmel – **eltérést állapíthat meg** a 15., 16., 18., 19., 20. és 21. cikkben említett jogokat illetően, ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják az adott célok elérését, és azok megvalósításához szükség van ilyen eltérésre.*
>
> *(4) Ha a (2), illetve (3) bekezdésben említett adatkezelés egyidejűleg más célokat is szolgál, az eltérést kizárólag az érintett bekezdésben említett adatkezelési célokra kell alkalmazni.”*

Zárszó

Fenti összefoglalás a jelenleg ismert jogszabályi rendelkezéseken alapul. A Rendelet kötelező a tagállamokra nézve és rendelkezései 2018. május 25-től közvetlenül alkalmazandók a tagállami jogban, azonban mindenképpen szükséges a magyar jogszabályi környezet megalkotása is. A magyar jogszabályok elfogadása után mindenképpen szükséges aktualizálni a levéltárak előtt álló feladatokat.

A jelenlegi jogi környezetben a következő feladatokat kell a legsürgősebben elvégezni:

1. Adatvédelmi tisztviselő jelölése
2. Hatásvizsgálat elvégzése
3. Adatvagyon nyilvántartás elkészítése
4. Belső szabályzatok elkészítése
5. Érintettek jogai érvényesítéséhez szükséges tájékoztató(k) elkészítése.
6. Elektronikus információs rendszerek védelmének megteremtése

Mellékletek

1. számú melléklet

A személyi anyag és a személyi anyaggal együtt őrzött személyi irat kezelésére vonatkozó adatvédelmi tájékoztató és nyilatkozat dolgozók részére

Az Adatkezelő megnevezése:
Adatkezelő székhelye:
Tájékoztatjuk, hogy közalkalmazotti jogviszonyával [a továbbiakban: jogviszony] kapcsolatos személyes adatait jelen iratban foglaltak alapján kezeljük.
Az adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása.
A kezelt adatok köre:
A levéltár munkavállalóiról személyzeti, illetve bér- és munkaügyi nyilvántartást vezet. [14]
A munkaügyi nyilvántartás az xy rendszerrel történik, mely a levéltár saját szerverén fut. A munkaügyi nyilvántartás bérszámfejtéshez szükséges adatai a …..alapján a Magyar Államkincstárnak átadásra kerülnek.[15]
A bérszámfejtést a Magyar Államkincstár végzi, ….alapján. A bérszámfejtéshez az XY programot alkalmazza, a rendszerre és az adatokra adatfeldolgozóként rálát.[16]
A közalkalmazott
neve,
születési neve
születési helye és ideje
állampolgársága
törzsszáma
anyja születési neve
lakóhelyének címe
tartózkodási helye (amennyiben eltérő a lakóhelytől)
magán-nyugdíjpénztári tagság ténye, belépés ideje (év, hó, nap), bank neve és kódja
adóazonosító jele
társadalombiztosítási azonosító jele (TAJ szám)
nyugdíjas törzsszám (nyugdíjas munkavállaló esetén)
folyószámla száma
jogviszony kezdő napja
biztosítási jogviszony típusa
heti munkaórák száma
telefonszáma
családi állapota
végzettséget igazoló okmány másolati példánya
munka-alkalmassági egészségügyi igazolás
munkaköre
orvosi alkalmasság ténye
erkölcsi bizonyítványának kiállításának dátuma, okmányszáma

[14] Ha másmilyet is, akkor itt felsorolandó.

[15] Értelemszerűen saját adatokkal kitöltendő

[16] Ha a MÁK az adatfeldolgozó. Más esetben értelemszerűen kitöltendő. Ha a levéltár a bérszámfejtést stb. maga végzi, akkor nincs adatfeldolgozó.

meghatározott munkakörben vezetői engedély kategóriánkénti egészségügyi alkalmasságának lejártának időpontja,
főálláson kívüli munkavégzés esetén a jogviszony jellege, munkáltató neve és székhelye
a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő, elvégzendő tevékenység
a pótszabadság igénybevételével kapcsolatos okmányok
a dolgozó 16. életévét be nem töltött gyermekének neve, születési helye és ideje, lakcíme, anyja neve, társadalombiztosítási azonosító jele (TAJ szám), adóazonosító jele.[17]

Az adatkezelés jogalapja:
- a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény
- a Munka Törvénykönyvéről szóló 2012. évi I. törvény
- az egyes vagyonnyilatkozat-tételi kötelezettségekről szóló 2007. évi CLII. törvény
- a közfoglalkoztatásról és a közfoglalkoztatáshoz kapcsolódó, valamint egyéb törvények módosításáról szóló 2011. évi CVI. törvény [18]
- a statisztikáról szóló 1993.évi XLVI. törvény.

Az adattárolás határideje:
Az adatkezelés céljának megvalósulásáig, főszabály szerint a jogiszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a jogviszony megszűnéséig, a jogviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig ill. közérdekű archiválás céljából a levéltár hatályos irattári tervében rögzítettek szerint.
Az adatkezelés módja: papíralapon és elektronikusan.
Tájékoztatjuk, hogy amennyiben a jogviszony létesítéséhez, fenntartásához, megszüntetéséhez, az ezekkel kapcsolatos jogosultságok bizonyításához vagy kötelezettségek elismeréséhez nyilatkozat beszerzése szükséges a dolgozótól, úgy a nyilatkozat beszerzése során minden esetben felhívja a dolgozó figyelmét az a nyilatkozaton megadott adatokkal kapcsolatosan az adatkezelés tényére, jogalapjára, céljára. Amennyiben a nyilatkozat érvényességéhez okmány bemutatása szükséges (személyi igazolvány, diákigazolvány), úgy a levéltár semmilyen módon nem kezeli az okmány adatait és/vagy képét, hanem arra jogosult dolgozója aláírásával tanúsítja az okmány bemutatását és annak érvényességét.
Ön mint érintett az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján
a) kérelmezheti az adatkezelő levéltárnál tájékoztatását személyes adatai kezeléséről, személyes adatainak helyesbítését, valamint személyes adatainak törlését vagy zárolását,
b) élhet tiltakozási jogával,
c) a Nemzeti Adatvédelmi és Információszabadság Hatóságnál bejelentést tehet, továbbá bírósághoz fordulhat.
Az adatkezelésre vonatkozó további részletes szabályokat levéltár Adatvédelmi és adatbiztonsági szabályzata és a levéltár Munkahelyi kamerarendszer üzemeltetéséről szóló szabályzata tartalmazza.[19]

[17] Nem teljes körű felsorolás.

[18] Amennyiben ilyen adatkezelés történik.

[19] Amennyiben van ilyen.

NYILATKOZAT

Alulírott név: …….,

születési helye és ideje: ……

anyja neve: ……,

kijelentem, hogy a fenti tájékoztatást tudomásul vettem, személyes adataim kezelését tudomásul vettem, illetőleg ahhoz hozzájárulok.

Budapest, ……év ……..hó ……..-n.

……..

A közalkalmazott aláírása

2. számú melléklet

KUTATÓSZOLGÁLATI ADATKEZELÉSI TÁJÉKOZTATÓ

XY Levéltár (továbbiakban Levéltár) kutatószolgálati eljárás keretében személyes adatoknak a LEVÉLTÁR által történő adatkezeléséről.

A LEVÉLTÁR, mint személyes adatok kezelője (a továbbiakban úgyis, mint: Adatkezelő) a jelen nyilatkozatával tájékoztatja az érintetteket a kutatószolgálati tevékenysége során követett adatkezelési gyakorlatáról, a kezelésébe került személyes adatok védelme érdekében megtett intézkedéseiről és az érintettek jogorvoslati lehetőségeiről.

A jelen adatkezelési tájékoztató az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 20.§ (2) bekezdésén alapul, amely szerint az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő az Infotv. 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Az Infotv. 4. § (1) bekezdése értelmében személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Az Infotv. 4. § (2) bekezdése értelmében csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

1. Adatkezelő azonosító adatai:

XY Levéltár (rövidített neve: LEVÉLTÁR, székhelye: …… képviseli: ……..)

Releváns kapcsolattartási adatok:

Telefonszám:

E-mail cím: Levéltár@

Adatkezelő honlapjának elérhetősége:

2. Adatkezelés célja:

Jelen adatkezelés célja a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. tv. által a Levéltár részére előírt személyes adatokat tartalmazó adatkör kezelése.

3. Az adatkezelés jogalapja:

Az 1995. évi LXVI. tv. 22. § (3) bekezdése:

„A látogatói jegy kiadásakor a közlevéltár nyilvántartásba veszi a kutató természetes személyazonosító adatait és lakcímét.”

Az 1995. évi LXVI. tv. 24. (4) bekezdése:

„A kutatónak ……írásos nyilatkozatban meg kell jelölnie az adatkezelés helyét.”

A 27/2015. (V. 27.) EMMI rendelet (a közlevéltárak és a nyilvános magánlevéltárak tevékenységével összefüggő szakmai követelményekről) által előírt adatkör:

***„46. §** (1) A közlevéltár a kutatószolgálat menetének áttekintése és ellenőrzése, valamint a statisztikai adatszolgáltatás érdekében nyilvántartja*
a) az általa kiadott látogatói jegyet, annak nyilvántartási számát és az abban foglalt adatokat az Ltv.-ben foglaltak szerint,
b) a kutatótermi kutatási eseteket és azok időpontját,
c) a levéltári anyag igényléséről szóló kutatói kérőlapok azonosítóját, valamint
d) a 41. § (3) bekezdésében meghatározott elektronikus tárhely útján történő teljesítésre irányuló kutatói kérőlapok számát és azok teljesítését.
(2) Az (1) bekezdés szerinti nyilvántartást év végén le kell zárni, és összesítve rögzíteni kell a kutatók, a kutatási esetek, valamint a kutatói kérőlapok számát.”

Az érintett, mint kutató, a látogatói jegy kiadásakor írásban ill. az Elektronikus Levéltári Portálon (www.eleveltar.hu) keresztül történő internetes beiratkozás esetén hozzájárul személyes adatai kezeléséhez. Az 1995. évi LXVI. tv. által előírt adatok a kötelező adatkezelés körébe tartoznak, az azon felül kért személyes adatok a kutatóval történő kapcsolattartás megkönnyítését szolgálják, megadásuk hozzájárulás alapján történik, nem kötelező.[20]

4. Az Adatkezelő által kezelt személyes adatok köre:

A kutató neve;*
A kutató születési neve;*
Anyja születési neve;*
A kutató születési helye;*
A kutató születési ideje (év, hónap, nap);*
A kutató állandó lakhelye;*
Az 1995. évi LXVI. tv. 24. §-a alapján végzett kutatásnál az adatkezelés helye;*
Levelezési cím (amennyiben eltér);
Telefon;
E-mail;
Kutatás tárgya/témája;
Kérőlap adatai
(* = kötelező adatkezelés körébe tartozó adatok)[21]

5. Az adatkezelés időtartama:

Az adatkezelés időtartama az adatkezelési célokhoz kapcsolódik, az adatok (iratok) a LEVÉLTÁR hatályos Iratkezelési Szabályzat és Irattári terve alapján xx év[22] után kerülnek kiselejtezésre.

6. Adatfeldolgozó igénybevételéről szóló tájékoztatás:

Adatkezelő adatfeldolgozót nem vesz igénybe.[23]

---

[20] 1996. évi XX. törvény (a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról) 4. §-a szerint: „(4) Természetes személyazonosító adat a polgár a) családi és utóneve, születési családi és utóneve, b) születési helye, c) születési ideje és d) anyja születési családi és utóneve.”

[21] Amennyiben a levéltár érintetti hozzájárulás alapján más személyes adatot is kezel, azzal kiegészítendő.

[22] A tényleges megőrzési idő alapján töltendő ki.

[23] Ha mégis, akkor itt meg kell nevezni az adatfeldolgozót.

7. Az adatok megismerésére jogosult személyek köre:

Az érintettek által megadott személyes adatokhoz kizárólag az Adatkezelő arra kifejezetten feljogosított munkatársai férhetnek hozzá.

8. Adatbiztonsági intézkedésekről szóló tájékoztatás:

Adatkezelő állami/önkormányzati[24] költségvetési szerv, amelynek működése szabályozott, az irattározás rendjére és az informatikai rendszer(ek) működésére belső szabályozásokat és kontrollokat alkalmaz.

Adatkezelő gondoskodik a birtokába kerülő személyes adatok biztonságáról, megteszi továbbá azokat a technikai és szervezési intézkedéseket és kialakította azokat az eljárási szabályokat, amelyek az Infotv., a Rendelet[25], valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Adatkezelő informatikai rendszere és hálózata egyaránt védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá a számítógépvírusok, a számítógépes betörések és a szolgálat megtagadásra vezető támadások ellen. Az Adatkezelő a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.[26]

9. Az Infotv. 6. § (5) bekezdésén alapuló adatkezelésről szóló tájékoztatás:

Az Infotv. 6.§ (5) bekezdése szerint, ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában rá vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

Adatkezelő tájékoztatja az érintetteket, hogy az Infotv. fenti rendelkezését a Rendelet személyes adatok kezelésére vonatkozó előírásaival összhangban alkalmazzam az Adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából, vagy az Adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából.

10. Az érintettek jogai és jogérvényesítési lehetőségei:

Kérjük az érintettet, hogy ha úgy érzi, hogy az Adatkezelő megsértette a személyes adatok védelméhez fűződő jogát, akkor vegye fel velünk a kapcsolatot, hogy az esetleges jogsértést orvosolhassuk. Tájékoztatjuk az érintetteket, hogy igényüket polgári bíróság előtt is érvényesíthetik, vagy kérhetik a Nemzeti Adatvédelmi és Információszabadság Hatóság segítségét is. Erre, valamint az Adatkezelő kötelezettségeire vonatkozó részletes törvényi rendelkezéseket az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) tartalmazza.

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. Az érintett dönthet úgy, hogy a pert a lakóhelye vagy tartózkodási helye szerinti törvényszék előtt indítja meg.

---

[24] Értelemszerűen töltendő ki.

[25] 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)

[26] Példálózó felsorolás, a tényleges védelmi szint alapján töltendő ki.

Jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál lehet élni:

Név: Nemzeti Adatvédelmi és Információszabadság Hatóság

Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Honlap: http://www.naih.hu

Telefon: +36 (1) 391-1400

Telefax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu

Az Adatkezelő fenntartja a jogot, hogy a jelen adatvédelmi nyilatkozatát megváltoztassa. Az adatkezelés megváltozása nem jelentheti a személyes adatok céltól eltérő kezelését. Az erre vonatkozó tájékoztatást az Adatkezelő honlapján közzéteszi.

NYILATKOZAT

Alulírott név: …….,

születési helye és ideje: ……

anyja neve: ……,

kijelentem, hogy a fenti tájékoztatást tudomásul vettem, személyes adataim kezelését tudomásul vettem, illetőleg ahhoz hozzájárulok.

Budapest, ……év ……..hó ……..-n.

……..

kutató aláírása

Megj.: Elektronikus beiratkozás esetén a beiratkozáskor a tájékoztató elfogadható a beiratkozás során a tájékoztató elolvasása után egy négyzetbe tett „pipa” jellel, mely a beiratkozási továbbhaladás feltétele. A kutatói adatlap is tartalmazhatja ezt a megismerő nyilatkozatot s abban az esetben nem kell külön nyomtatványt aláírni a kutatónak.

3. számú melléklet

ÜGYFÉLSZOLGÁLATI ADATKEZELÉSI TÁJÉKOZTATÓ

XY Levéltár (továbbiakban Levéltár) egyedi adatról ügyfélszolgálati eljárás keretében történő tájékoztatás során a személyes adatoknak a LEVÉLTÁR által történő adatkezeléséről.

A LEVÉLTÁR, mint személyes adatok kezelője (a továbbiakban úgyis, mint: Adatkezelő) a jelen nyilatkozatával tájékoztatja az érintetteket az ügyfélszolgálati tevékenysége során követett adatkezelési gyakorlatáról, a kezelésébe került személyes adatok védelme érdekében megtett intézkedéseiről és az érintettek jogorvoslati lehetőségeiről.

A jelen adatkezelési tájékoztató az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 20.§ (2) bekezdésén alapul, amely szerint az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő az Infotv. 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Az Infotv. 4. § (1) bekezdése értelmében személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Az Infotv. 4. § (2) bekezdése értelmében csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

1. Adatkezelő azonosító adatai:

XY Levéltár (rövidített neve: LEVÉLTÁR, székhelye: …… képviseli: ……..)

Releváns kapcsolattartási adatok:

Telefonszám:

E-mail cím: Levéltár@

Adatkezelő honlapjának elérhetősége:

2. Adatkezelés célja:

Jelen adatkezelés célja az 1995. évi LXVI. tv. által a Levéltár részére előírt egyedi adatról ügyfélszolgálat keretében történő adatszolgáltatás igénybe vevőinek egyértelmű azonosítása.

3. Az adatkezelés jogalapja:

Az adatkezelés az érintett hozzájárulásával történik, figyelemmel a GDPR 6. cikk (1) bek a) pontjára és az Infotv. 5. § (1) bekezdés a.) pontjára. Az érintett, mint tájékoztatást kérő ügyfél, írásban hozzájárul személyes adatai kezeléséhez.

4. Az Adatkezelő által kezelt személyes adatok köre:

Az ügyfélszolgálati űrlapok esetében általában: adatot kérelmező neve, anyja neve, születési helye, ideje, állandó lakcíme, e-mail címe, személyazonosságot igazoló okmány száma, telefonszáma, megbízás esetén a megbízott adatai: (név, személyigazolvány szám) és a keresett igazolás tárgyát képező adat (munkaviszony esetén a munkahely, iskolai jogviszony esetén az iskola).

Hagyatéki ügy esetében: a kérelmező neve, az ügyben szereplő személlyel való rokoni fok megjelölése, a kérelmet benyújtó állandó lakcíme, telefonszáma, személyazonosságot igazoló okmány száma, megbízás esetén a megbízott adatai. A kérelmező által megadottan: az elhunyt neve, az elhunyt anyjának neve, az elhunyt elhalálozásának pontos dátuma, az elhunyt utolsó állandó lakcíme, végrendelet esetén az ügyben szereplő személyek neve.

Földhivatali iratokkal kapcsolatos megkeresés esetében a kérelmező személyes adatait kiegészítve a keresett ingatlan adatai, kérelmező által megadottan.

Hadigondozási eljárás esetében a kérelmező személyes adatait kiegészítve az elesett vagy hadifogságban elhunyt személy adataival. [27]

5. Az adatkezelés időtartama:

Az adatkezelés időtartama az adatkezelési célokhoz kapcsolódik, az adatok (iratok) a LEVÉLTÁR hatályos Iratkezelési Szabályzat és Irattári terve alapján xx év[28] után kerülnek kiselejtezésre.

6. Adatfeldolgozó igénybevételéről szóló tájékoztatás:

Adatkezelő adatfeldolgozót nem vesz igénybe.[29]

7. Az adatok megismerésére jogosult személyek köre:

Az érintettek által megadott személyes adatokhoz kizárólag az Adatkezelő arra kifejezetten feljogosított munkatársai férhetnek hozzá.

8. Adatbiztonsági intézkedésekről szóló tájékoztatás:

Adatkezelő állami/önkormányzati[30] költségvetési szerv, amelynek működése szabályozott, az irattározás rendjére és az informatikai rendszer(ek) működésére belső szabályozásokat és kontrollokat alkalmaz.

Adatkezelő gondoskodik a birtokába kerülő személyes adatok biztonságáról, megteszi továbbá azokat a technikai és szervezési intézkedéseket és kialakította azokat az eljárási szabályokat, amelyek az Infotv., a Rendelet,[31] valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Adatkezelő informatikai rendszere és hálózata egyaránt védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá a számítógépvírusok, a számítógépes

[27] Példálózó felsorolás, a ténylegesen kezelt adatok körével kiegészítendő ill. csökkentendő.

[28] A tényleges megőrzési idő alapján töltendő ki.

[29] Ha mégis, akkor itt meg kell nevezni az adatfeldolgozót.

[30] Értelemszerűen töltendő ki.

[31] 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)

betörések és a szolgálat megtagadásra vezető támadások ellen. Az Adatkezelő a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.[32]

9. Az Infotv. 6. § (5) bekezdésén alapuló adatkezelésről szóló tájékoztatás:

Az Infotv. 6.§ (5) bekezdése szerint, ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában rá vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

Adatkezelő tájékoztatja az érintetteket, hogy az Infotv. fenti rendelkezését a Rendelet személyes adatok kezelésére vonatkozó előírásaival összhangban alkalmazzam az Adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából, vagy az Adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából.

10. Az érintettek jogai és jogérvényesítési lehetőségei:

Kérjük az érintettet, hogy ha úgy érzi, hogy az Adatkezelő megsértette a személyes adatok védelméhez fűződő jogát, akkor vegye fel velünk a kapcsolatot, hogy az esetleges jogsértést orvosolhassuk. Tájékoztatjuk az érintetteket, hogy igényüket polgári bíróság előtt is érvényesíthetik, vagy kérhetik a Nemzeti Adatvédelmi és Információszabadság Hatóság segítségét is. Erre, valamint az Adatkezelő kötelezettségeire vonatkozó részletes törvényi rendelkezéseket az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) tartalmazza.

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. Az érintett dönthet úgy, hogy a pert a lakóhelye vagy tartózkodási helye szerinti törvényszék előtt indítja meg.

Jogorvoslati lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál lehet élni:

Név: Nemzeti Adatvédelmi és Információszabadság Hatóság

Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Honlap: http://www.naih.hu

Telefon: +36 (1) 391-1400

Telefax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu

Az Adatkezelő fenntartja a jogot, hogy a jelen adatvédelmi nyilatkozatát megváltoztassa. Az adatkezelés megváltozása nem jelentheti a személyes adatok céltól eltérő kezelését. Az erre vonatkozó tájékoztatást az Adatkezelő honlapján közzéteszi.

[32] Példálózó felsorolás, a tényleges védelmi szint alapján töltendő ki.

NYILATKOZAT

Alulírott név: ……,

születési helye és ideje: ……

anyja neve: ……,

kijelentem, hogy a fenti tájékoztatást tudomásul vettem, személyes adataim kezelését tudomásul vettem, illetőleg ahhoz hozzájárulok.

Budapest, ……év ……..hó ……..-n.

……..

ügyfél aláírása

Megj.: Elektronikus ügyfélszolgálati ügyintézés esetében a tájékoztató elfogadható az adatlap kitöltése során a tájékoztató elolvasása után egy négyzetbe tett „pipa” jellel, mely az adatlap kitöltése ill. a továbbhaladás feltétele. Az ügyfélszolgálati adatlap is tartalmazhatja ezt a megismerő nyilatkozatot s abban az esetben nem kell külön nyomtatványt aláírni az ügyfélnek.

4. sz. melléklet

Adatkezelési nyilvántartás

Az adatkezelési nyilvántartás célja:

A …..Levéltár (cím) szervezeti egységeinél történő a GDPR és a 2011. évi CXII. tv. hatálya alá tartozó adatkezelésekkel kapcsolatban a következőeket tartalmazza:

- adatkezelés célját
- adatok fajtáját, kezelésének jogalapját
- érintettek körét
- adatok forrását
- adatra vonatkozó esetleges továbbításának fajtáját, címzettjét és jogalapját
- az adott adatfajta törlésének határidejét
- amennyiben az adattal kapcsolatosan adatfeldolgozás történik, az
- adatfeldolgozó adatait, adatfeldolgozás helyét, az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét.

1. adatcsoport

1.	Az adat fajtája:	
2.	Adakezelés célja:	
3.	Az adatkezelésére vonatkozó jogalap:	
4.	Az érintettek köre:	
5.	Az adatok forrása:	
6.	Adatkezelést végzők:	
7.	Adattovábbítás:	
8.	Adatok fizikai és/vagy elektronikus tárolási helye:	
9.	Adattörlés határideje:	

2. adatcsoport

1.	Az adat fajtája:	
2.	Adakezelés célja:	
3.	Az adatkezelésére vonatkozó jogalap:	
4.	Az érintettek köre:	
5.	Az adatok forrása:	
6.	Adatkezelést végzők:	
7.	Adattovábbítás:	
8.	Adatok fizikai és/vagy elektronikus tárolási helye:	
9.	Adattörlés határideje:	

…….

Tartalom