BMK-1407-1/2021.

A BUDAPESTI MŰVELŐDÉSI KÖZPONT ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

BUDAPEST

2021.

(hatályos: 2021. július 05 – től)

Jóváhagyom:

Márai László

igazgató

Tárgy: [Tárgy]

	Budapesti Művelődési Központ
Verzió:	**1.0**
Dokumentum típusa:	**Munkautasítás**
Készítette:	**DHG Ügyvédi Iroda**
Ellenőrzésért felel:	**Adatvédelmi Felelős**
Utolsó frissítés dátuma:	2021. június 14.
Frissítés periódusa:	Változáskor, de legkésőbb minden harmadik évben

Dátum	Módosítás leírása
2021. június 14.	Alapdokumentum megnyitása

Tartalomjegyzék

1. Dokumentum célja és hatálya

A Budapesti Művelődési Központ (a továbbiakban: „BMK") *Az információs önrendelkezési jogról és az információszabadságról szóló* 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (3) bekezdésében foglalt kötelezettségének eleget téve elkészítette a jelen adatvédelmi és adatbiztonsági szabályzatát (a továbbiakban: „Szabályzat"), melynek célja, hogy meghatározza a BMK-ban folytatott adatkezelések működésének jogszerű rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek és uniós alapelveinek, továbbá az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

A Szabályzat célja a fentieken túl az ügyintézés során az érintettek személyes adatainak védelme és a közérdekű adatok nyilvánosságának biztosítása.

A Szabályzat hatálya kiterjed a BMK-nál foglalkoztatott valamennyi munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik munkatapasztalat-szerzési, kutatási vagy képzési célból szakmai gyakorlatukat a BMK-nál töltik.

2. Kötelező felülvizsgálat

A BMK az adatkezelés megkezdésétől számított legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét az adatkezelő dokumentálja, a dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) kérésére a NAIH rendelkezésére bocsátja.

3. A szabályozás törvényi alapjai és kapcsolódó dokumentumai

Jelen dokumentum megalkotásakor az alábbi jogszabályokat vettük figyelembe:

- ✓ GDPR (Adatvédelmi Rendelet) - 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;
- ✓ Adatvédelmi törvény - Az információs önrendelkezési jogról, és az információszabadságról szóló 2011. évi CXII. törvény.
- ✓ Az az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény;
- ✓ Ptk. - A Polgári Törvénykönyvről szóló 2013. évi V. törvény;
- ✓ Az adózás rendjéről szóló 2017. évi CL. törvény és végrehajtására kiadott jogszabályok;
- ✓ A számvitelről szóló 2000. évi C. törvény és végrehajtására kiadott jogszabályok;
- ✓ A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény;
- ✓ Mt. - A munka törvénykönyvéről szóló 2012. évi I. törvény;
- ✓ Pp. - A polgári perrendtartásról szóló 2016. évi CXXX. törvény.

4. Fogalmak

„**személyes adat**": az érintettre 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;

„**érintett**": az azonosítható természetes személy, akire az adott személyes adat vonatkozik. (Ilyen pl.: a kamera felvételén látható személy, a megnevezett személy, az e-mailcím tulajdonosa, stb...);

„**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;

„**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;

„**adatfeldolgozás**": az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése;

„**adatfeldolgozó**": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében (megbízásából, utasítására és az adatkezelő döntése alapján) személyes adatokat kezel;

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

„**Adatvédelmi Tisztviselő**": a BMK által megbízott Tisztviselő, aki támogatást nyújt a megfelelő adatkezelési gyakorlat megvalósításában és működtetésében, szükség esetén kapcsolatot tart a felügyeleti hatósággal és az érintettekkel;

„**Adatvédelmi Felelős**": a BMK által megbízott belső felelős, aki biztosítja a megfelelő adatkezelési gyakorlat működtetését;

„**az adatkezelés korlátozása**": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

„**profilalkotás**": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

„**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;

„**nyilvántartási rendszer**": a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető; egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

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

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

„**az érintett hozzájárulása**": az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

„**adatvédelmi incidens**": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

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

5. Adatvédelmi alapelvek

A személyes adatok kezelését az alábbi alapelvek mentén szükséges megtervezni és végrehajtani:

a) A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („**jogszerűség, tisztességes eljárás és átláthatóság**");
b) A személyes adatok 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) A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („**adattakarékosság**");
d) A személyes adatok 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) A személyes adatok 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, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („**korlátozott tárolhatóság**");
f) A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („**integritás és bizalmas jelleg**").

g) Az adatkezelő felelős az alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („**elszámoltathatóság**").

6. A személyes adatok szervezeten belüli védelme

6.1. Általános előírások

A személyes adatok védelméről az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeré-

séről és betartásáról az Adatvédelmi Felelős - amennyiben azonos az Adatvédelmi Tisztviselővel, úgy az Adatvédelmi Tisztviselő - gondoskodik.

A személyes adatok felvétele és a további adatkezelés folyamán ügyelni kell a személyes adatok pontosságára, teljességére és időszerűségére, hogy emiatt az érintett jogai ne sérülhessenek.

Az ügyintézőnél vagy az irattárban lévő iratba az ügyintézőn kívül más személy - az érintett törvény szerinti betekintési jogán túl - csak akkor tekinthet be, ha ezt törvény lehetővé, vagy a munkakörével összefüggő feladatellátás szükségessé teszi.

6.2. Munkavállalók személyes adatainak kezelése

6.2.1. Munkavállalók személyes adatai

A munkaviszonnyal összefüggő adatok kezeléséért a BMK-nál
a) az igazgató,
b) az érintett munkavállaló felettese,
c) a személyzeti feladatot ellátó munkatárs,
d) a munkavállaló - a saját adatainak közlése tekintetében - tartozik felelősséggel.

Az igazgató felel a munkaviszonnyal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok, valamint az e Szabályzatban rögzített előírások megtartásáért, illetve e követelmények teljesítésének ellenőrzéséért.

Az igazgató e felelősségi körében köteles gondoskodni:
a) a Munkavállalók Adatkezelési Tájékoztatójának kiadásáról, kiegészítéséről, szükség esetén módosításáról,
b) a munkaviszonnyal összefüggő adatok védelmével kapcsolatos követelmények érvényesüléséről,
c) a munkaviszonnyal összefüggő adatok kezelésére vonatkozó szabályok érvényesülésének folyamatos ellenőrzéséről,
d) az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről.

Az Igazgató szükség szerint átfogó, illetve eseti ellenőrzés keretében győződik meg a munkaviszonnyal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok megfelelő érvényesüléséről.

Az érintett munkavállaló felettese, kizárólag a számára nélkülözhetetlen személyes adatok megismerésére jogosult. Érintetti kérés esetén gondoskodik a kérés továbbításáról a személyzeti feladatokat ellátó munkatárs felé.

A személyzeti feladatot ellátó munkatárs felelősségi körén belül köteles gondoskodni arról, hogy:
a) az általa kezelt személyes adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának,
b) a személyi iratra csak olyan adat, illetve megállapítás kerülhessen, amely a jogszabályokban felsorolt adatforráson alapul, vagy egyéb okból igazolható módon feltétlenül szükséges;
c) a munkaviszonnyal összefüggő adat helyesbítését és törlését kezdeményezze, ha megítélése szerint a személyi iraton szereplő adat a valóságnak már nem felel meg. Továbbá az ilyen irányú érintetti kérdések teljesítésében közreműködjön.

A **munkavállaló** felelős azért, hogy az általa átadott, bejelentett adatok hitelesek, pontosak, teljesek és aktuálisak legyenek.

6.2.2. Munkavállalók tájékoztatása az adatkezelésről

A munkába lepés előtt, de legkésőbb a munkába lépés napján a munkavállalók részére át kell adni a **Munkavállalók Adatkezelési Tájékoztatóját** és a **Tájékoztatót Kamerarendszer Üzemeltetéséről**. A tájékoztatók átvételét a munkavállaló aláírásával igazolja. Az átvétel igazolását a munkavállaló személyi anyagában a munkavállaló kilépéséig meg kell őrizni.

Ha a munkavállalók nagy száma miatt a tájékoztatók fizikai átadására és átvételére nincsen mód, úgy megfelelő, a tájékoztatók elektronikus úton történő megküldése a munkavállaló részére. Ebben az esetben az átvételt az olvasási jelentés bizonyítja.

A tájékoztatók elérését a belső rendszerben szintén javasolt biztosítani.

Ha változik valamelyik tájékoztató, úgy a tájékoztató aktualizált példányát az eredeti példánnyal azonos módon kell a munkavállaló részére átadni.

Amennyiben a munkavállalónak kérdése van az adatkezeléssel kapcsolatban azt írásban jelezheti az adatvedelem@bmknet.hu e-mailcímen.

6.2.3. Munkavállalók adatvédelmi oktatása

Fontos, hogy a munkavállalók megismerjék a munkájukhoz kapcsolódó adatvédelmi követelményeket. Ennek érdekében a munkavállalók adatvédelmi tudását folyamatosan frissen kell tartani.

Az Igazgató köteles a felelős vezetőkkel és az érintett szervezeti egységgel egyeztetni annak érdekében, hogy meghatározzák a különböző besorolású munkavállalók számára szükséges személyes, vagy online adatvédelmi tréningeket.

6.2.4. Ellenőrzési jog gyakorlása

A munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja. A munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert - eltérő megállapodás hiányában - kizárólag a munkaviszony teljesítése érdekében használhatja.

A munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnyal összefüggő adatokba tekinthet be. Az ellenőrzési jogosultság szempontjából munkaviszonnyal összefüggő adatnak minősül a korlátozás betartásának ellenőrzéséhez szükséges adat. Ezt akkor is alkalmazni kell, ha a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ.

6.2.5. Állásra jelentkezők kiválasztása

Álláspályázat kiírása során tájékoztatást kell nyújtani a leendő jelentkezők részére a kiválasztást befolyásoló kritériumokról és a lehetséges **háttérkutatás**okról is. Így például ismertetni kell a jelentkezőkkel, hogy a felvételi eljárás folyamata kiterjed arra is, hogy a leendő munkáltató megtekinti a jelentkező közösségi oldalon létrehozott, bárki számára nyilvános információit. A jelentkező közösségi oldalon végzett, nyilvános tevékenysége megismerhető, arról következtetés levonható, de a további adatkezelési műveletek már jogellenesnek

minősülnek. Vagyis arra nincs lehetőség, hogy a jelentkező profiloldalát a munkáltató lementse, tárolja vagy más számára továbbítsa.[1]

Nem tekinthetők meg azonban azok az adatok, amiket a jelentkező nem szeretne mindenki elé tárni, így a zárt csoportban megosztott képek, információk. Ezen információk már nem teljesen nyilvánosak, ezért ezek megismerése már korlátozza a jelentkező magánszférájához való jogát.

Ugyanakkor fontos, hogy csak azok az információk ismerhetők meg, amelyek lényegesek az álláspályázattal vagy a munkakörrel kapcsolatban.[2]

7. Az érintettek jogai és az igények teljesítésének rendje

7.1. Érintetti igények teljesítése

Az érintettek szóban, postai vagy bármilyen elektronikus úton *(e-mail, telefon, fax)* adatvédelmi szempontból az alábbi kérésekkel kérdésekkel fordulhatnak A BMK-hoz:

- hozzájárulás visszavonása;
- tájékoztatás (hozzáférés) kérése;
- helyesbítés kérése;
- adattörlés kérése;
- adatkezelés korlátozásának kérése;
- adatok átadása iránti kérés;
- tiltakozás.

A fenti kéréseket az alábbiak szerint szükséges kezelni:

Valamennyi az érintettekkel közvetlen kapcsolatba kerülő munkavállaló köteles minden tőle elvárhatót megtenni annak érdekében, hogy az érintett panasza a BMK által orvosolható legyen.

1. lépés: Azonosítás

A kérés teljesítése előtt minden esetben azonosítani kell a kérelmező személyazonosságát. Ha nem lehet azonosítani, hogy valóban az érintett nyújtja be a kérést, a kérés nem teljesíthető. Az azonosítást legalább két rendelkezésünkre álló személyes adat bekérésével kell végrehajtani.

2. lépés: A kérés továbbítása

A szóban elhangzott kérés esetén meg kell kérni az érintettet, hogy kérését írja le, és küldje meg a részünkre.

Az írásban rögzített/átvett kérést azonnal továbbítani kell az Adatvédelmi Felelős és Adatvédelmi Tisztviselő felé. A panaszt/ kérést kezelő munkatárs kijelölése az Igazgató feladta.

---

[1] A NAIH tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről

[2] Mt. 10.§(4) (...)A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.(...)

3. lépés: A panaszt/kérést kezelő munkatárs feladata

A munkatárs összegyűjt minden az adatkezelésre vonatkozó adatot, információt, majd értékelést végez *(ami alapján a panasz elismerhető, részben elismerhető vagy visszautasítandó)*. Ezt követően a panaszkezelő egyezteti az értékelést és az előkészített választ az Adatvédelmi Felelőssel és az Adatvédelmi Tisztviselővel.

4. lépés: A kérés megválaszolása

A kérést vagy kérdést írásban vagy elektronikusan meg kell válaszolni. Ha a megkeresés elektronikus úton érkezett, a választ is elektronikusan kell megküldeni, amennyiben a kérelmező nem kéri más úton a tájékoztatását. A szóban adott tájékoztatást írásban is ki kell adni.

5. lépés: Egyéb intézkedések

Abban az esetben, amennyiben akár az adatkezelések nyilvántartása, akár az Adatkezelési Tájékoztató, vagy bármely más belső szabályzat módosítása szükséges, a panaszkezelő felveszi a kapcsolatot a szakmai terület felelős vezetőjével, valamint az Adatvédelmi Felelőssel és az Adatvédelmi Tisztviselővel a változások átvezetése érdekében.

Adattovábbítás esetén – *amennyiben a kérés törlésre, korlátozásra, helyesbítésre vonatkozik* - tájékoztatni kell azt a felet is, aki felé az adatot továbbítottuk.

Határidők:

- ✓ A panasz beérkezésétől számított legkésőbb 5 (öt) munkanapon belül értesítést kell küldeni a panaszosnak, amelyben tájékoztatni kell, hogy a panasza kivizsgálása folyamatban van.
- ✓ Ha intézkedés meghozatala szükséges, azt legkésőbb 10 (tíz) munkanapon belül el kell végezni.
- ✓ Abban az esetben, ha az üggyel kapcsolatban a két kapcsolatfelvétel közötti idő meghaladja a 15 (tizenöt) napot, a panaszkezelő köteles tájékoztató levelet küldeni az érintettnek, amelyben biztosítja, hogy az ügy elbírálása még tart.
- ✓ A végső választ legkésőbb a kérés beérkezésétől számított egy hónapon belül kell megküldeni a megkeresőnek a kérése nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további kettő hónappal meghosszabbítható, amiről még az egy hónapos ügyintézési határidőn belül tájékoztatni kell a megkeresőt. Az intézkedés elmaradásáról is tájékozást kell nyújtani az egy hónapos ügyintézési határidőn belül.[3]

Az ügyintézés díja:

A kért tájékoztatás és intézkedés díjmentes. Kivételt képez az az eset, ha a kérés egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó. Ebben az esetben díjat számolhatunk fel, vagy megtagadhatjuk a kérés teljesítését. Az ilyen eseteket mindig az Igazgató hagyja jóvá.

7.2. A jogok és jogorvoslati lehetőségek részletes bemutatása

[3] GDPR 12.cikk

7.2.1. Hozzájárulás visszavonása

Kizárólag az érintett hozzájárulása alapján végzett adatkezelések esetén, az érintett bármikor visszavonhatja a hozzájárulását. Ilyen esetben az erről szóló értesítést követően – amennyiben más jogalapon nem kezeljük az adatot - töröljük az érintett személyes adatait. Erről az érintettet tájékoztatjuk, valamint arról, hogy a visszavonás előtt a hozzájárulás alapján végzett adatkezelés jogszerűségét nem érinti.

7.2.2. Tájékoztatás (hozzáférés) kérése

Az érintett tájékoztatása az egyik legfontosabb adatvédelmi alapelv. Azt, hogy pontosan miről kell tájékoztatni az érintettet, a GDPR két külön listában sorolja fel[4] attól függően, hogy az adatokat az érintettől közvetlenül, vagy valaki mástól kaptuk.

A tájékoztatást legegyszerűbben egy általános tájékoztatóval végezhetjük el *(Adatkezelési Tájékoztató, Munkavállalók Adatkezelési Tájékoztatója, Kamerarendszerről szóló Tájékoztató, stb...)*. Lehetnek azonban olyan esetek, amikor esetileg kell tájékoztatni az érintettet. A félreértések elkerülése, és pontos tájékoztatás érdekében törekedjünk az írásos tájékoztatásra, valamint kérjük meg az érintettet, hogy szóban feltett kérdéseit - amennyiben arra az általános tájékoztatókban nem talál választ – írásban, az adatvedelem@bmknet.hu e-mailcímre küldje meg.

Az érintett tájékoztatást kérhet arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen:

- ✓ Mi a célja?
- ✓ Pontosan milyen adatok kezeléséről van szó?
- ✓ Kinek továbbítjuk ezeket az adatokat?
- ✓ Meddig tároljuk ezeket az adatokat?
- ✓ Az érintettnek milyen jogai és jogorvoslati eszközei vannak ezzel kapcsolatban?
- ✓ Kitől kaptuk az adatokat?
- ✓ Hozunk-e automatizált döntést az érintettre vonatkozóan az érintett személyes adatai felhasználásával? Ilyen esetekben arról is kérhető tájékoztatás, hogy milyen logikát (módszert) alkalmazunk, és arról, hogy az ilyen adatkezelés milyen jelentőséggel bír, milyen várható következményekkel jár.
- ✓ Ha az érintett azt tapasztalja, hogy adatait nemzetközi szervezet, vagy harmadik ország (nem uniós tagállam) felé továbbítottuk, úgy kérheti annak bemutatást, hogy mi garantálja személyes adatai megfelelő kezelését.
- ✓ Kérhet másolatot a kezelt személyes adatairól (A további másolatokért az adminisztratív költségeken alapuló díjat számíthatunk fel.)

7.2.3. Helyesbítés kérése

Az érintett kérheti, hogy javítsuk, illetve egészítsük ki a pontatlanul, vagy hiányosan rögzített személyes adatát. Ilyen kérés esetén a javítást vagy kiegészítést haladéktalanul el kell végezni, és erről az érintettet tájékoztatni kell. Ha az adatot másnak is továbbítottuk, értesíteni kell a továbbítás címzettjét is.

7.2.4. Kérés személyes adatok törlése iránt („elfeledtetés")

Az érintett kérheti, hogy töröljük a személyes adatait:

- ✓ ha a személyes adatokra már nincs szükség abból a célból, amelyből azokat kezeltük;

---

[4] GDPR 13. és 14. cikk

- ✓ pusztán az érintett hozzájárulása alapján végzett adatkezelések esetén;
- ✓ ha megállapításra kerül, hogy a személyes adatokat jogellenesen kezeljük, a tiltakozás eredményes;
- ✓ ha Uniós vagy hazai jogszabály előírja;
- ✓ ha a személyes adatokat uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- ✓ ha a személyes adatok gyűjtésére az információs társadalommal összefüggő, gyermekek részére kínált szolgáltatásokkal kapcsolatosan került sor.

Ha nyilvánosságra hoztuk a személyes adatokat, és azt a fentiek értelmében törölni kell, az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tenni az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassuk az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlünk a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A személyes adatokat nem törölhetjük, amennyiben azokra szükség van:

- ✓ a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- ✓ a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből;
- ✓ a népegészségügy területét érintő közérdek alapján;
- ✓ közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy
- ✓ jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A törlés kérésénél a nagy körültekintéssel kell eljárni a tekintetben, hogy az adat valóban törölhető-e. A törlésről tájékoztatjuk az érintettet és azt, akinek az adatot esetlegesen továbbítottuk. Amennyiben bármilyen okból nem, vagy nem teljesen tudjuk törölni az adatokat, az érintettet értesíteni szükséges, és egyeztetni a mindenki számára megfelelő megoldás megtalálása érdekében.

7.2.5. Kérés az adatkezelés korlátozása iránt

Az érintett kérheti, hogy korlátozzuk az adatkezelést, ha az alábbiak valamelyike teljesül:

- ✓ az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy ellenőrizzük a személyes adatok pontosságát;
- ✓ az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- ✓ már nincs szükségünk a személyes adatokra az adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- ✓ az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Korlátozás esetén a 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.

A korlátozás esetleges feloldásáról előzetesen tájékoztatjuk az érintettet.

7.2.6. Adathordozhatósághoz való jog

Kizárólag hozzájárulás, vagy szerződéses jogalapon automatizált módon végzett adatkezelések estén az érintett jogosult arra, hogy az általunk kezelt személyes adatait géppel olvasható formátumban megkapja.

7.2.7. Tiltakozás

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, ha a közérdekű feladat végrehajtásához szükséges.

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.

Az említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Az érintett akkor is tiltakozhat a személyes adatai kezelése ellen, ha:

- ✓ a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor. Ebben az esetben a személyes adatokat mérlegelés nélkül töröljük.

8. Különleges személyes adatok

A különleges adatok, vagyis 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 kizárólag a GDPR 9. cikk (2) bekezdésben felsorolt esetekben lehetséges**.

A különleges adatok kezelése során is fokozottan kell figyelni arra, hogy az adatokat bizalmasan kezeljük, valamint arra, hogy azokat csak azok a személyek ismerhessék meg, akiknek feladatuk van az adatok kezelése kapcsán.

9. Gyermekekkel kapcsolatos adatok

A GDPR Preambulumában 38. pont szerint:

„A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal. Ezt a különös védelmet főként a gyermekek személyes adatainak olyan felhasználására kell alkalmazni, amely marketingcélokat, illetve személyi vagy felhasználói profilok létrehozásának célját szolgálja, továbbá a gyermekek személyes adatainak a közvetlenül a részükre nyújtott szolgáltatások igénybevétele során történő gyűjtésére. A közvetlenül a gyermek részére nyújtott megelőzési és tanácsadási szolgáltatások esetében nincs szükség a szülői felügyelet gyakorlójának hozzájárulására."

A gyermekekkel kapcsolatos adatok kezelésénél tehát szintén **különös odafigyeléssel kell eljárni**.

A közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások[5] *(pl.: gyermekeknek szóló applikáció, egyedi hozzáférés)* vonatkozásában végzett személyes adatok kezelése akkor jogszerű,

---

[5] *„Információs társadalommal összefüggő szolgáltatás: elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá"*; az elektronikus kereskedelmi

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

Minden egyéb – tehát nem információs társadalommal összefüggő – szolgáltatás (pl.: verseny) esetén a 18 éven aluli személyek személyes adatainak kezeléséhez a törvényes képviselő hozzájárulására is szükség van.

18 éven aluli személy személyes adatinak kezelése esetén a tájékoztatást egyszerűsített, a gyermekek számára is könnyen érthető formában is elérhetővé kell tenni.

Hozzájárulás esetén - a törvényes képviselő hozzájárulása mellett - a 14 éven felüli gyermek hozzájárulását is kérni kell.

10. Közérdekű adatok

Az Infotv. 30.§ (6), 35. § (3), a 32. § - 37/B. § - ban foglaltak alapján, továbbá a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII. 25.) Korm. rendelet 3. §-ában és a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII. 27.) IHM rendeletben foglaltaknak eleget téve a közérdekű adatok igénylésének rendje és a közérdekű és közérdekből nyilvános adatok közzétételének rendjére két külön szabályzat vonatkozik.

11. Adatvédelmi előírások a honlap tekintetében

Az egyik legfontosabb adatvédelmi előírás, az **Adatkezelési Tájékoztató** elhelyezése a honlapon. Ez egyrészről azért fontos, mert a BMK részben ezzel tesz eleget tájékoztatási kötelezettségének, másrészről megkönnyíti a későbbi hivatkozást, amit egy link beszúrásával, vagy egy elérési útvonal feltűntetésével tehetünk meg. Az Adatkezelési Tájékoztató elérését amennyire lehet, egyszerűvé kell tenni, például a címek külön kiemelésével ezáltal rövid elérést biztosítva az egyes fejezetekhez. Biztosítani kell továbbá, hogy a dokumentum PDF formátumban letölthető legyen.

Az **egyes űrlapok, vagy regisztrációs adatlapok** végén egy külön jelölő négyzettel kell az Adatkezelési Tájékoztató megismerését és tudomásulvételét kialakítani. Az egyszerűbb űrlapokon *(pl.: regisztráció, üzenetküldés)*, ahol az adott űrlapon kizárólag az Adatkezelési Tájékoztató elfogadását kell kialakítani *(ahol nincs több célja az adatkezelésnek)* ott elhagyható a jelölő négyzet, kizárólag a tájékoztató szöveget és linket kell feltüntetni. Ebben az esetben ugyanis pl.: az *„Elküldöm"* gombra történő klikkelés az a tevőleges magatartás, amivel az érintett az Adatkezelési Tájékoztató elolvasása után az adatkezeléshez hozzájárul.

A legtöbb honlap sütiket *(cookiekat)* használ.

A cookie egy olyan kisméretű szövegfájl, amely a számítógép vagy a mobil eszköz merevlemezén tárolódik a cookie-ban beállított lejárati ideig és a későbbi látogatásokkor aktiválódik *(pl. visszajelez a webkiszolgálónak)*. A honlapok cookiek-at használnak azzal a céllal, hogy rögzítsék a látogatással kapcsolatos információkat *(pl. meglátogatott oldalak, az oldalakon töltött idő, böngészési adatok, kilépések stb.)*, illetve a személyes beállításokat. Ez az eszköz segít a felhasználóbarát honlap kialakításában, a látogatók online élményének fokozása érdekében.

---

szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2.§ f) pont

A cookie-k két típusát különböztetjük meg: *"munkamenet sütik"* és *"maradandó sütik"*. Mindkét süti típus esetén azok addig kerülnek tárolásra a böngészőben amíg a felhasználó nem törli azokat.

- ✓ A "munkamenet sütik" *(session cookie)* a számítógép, notebook vagy mobileszköz csak ideiglenesen tárolja, mindaddig, amíg a látogató el nem hagyja az adott honlapot; ezek a sütik segítenek a rendszernek, hogy információt jegyezzen meg, így nem kell ismételten megadni vagy kitöltenie az adott információt. A munkamenet sütik érvényességi ideje kizárólag a felhasználó aktuális munkamenetére korlátozódik, céljuk az adatvesztés megakadályozása *(például egy hosszabb űrlap kitöltése során)*. A munkamenet végeztével, illetve a böngésző bezárásával a sütik e fajtája automatikusan törlődik a látogató számítógépéről.

- ✓ A "maradandó sütik" *(persistent cookie)* a honlap elhagyását követően is tárolódnak a számítógépen, notebookon vagy mobileszközön. Ezen cookie-k segítségével a honlap felismeri a visszatérő látogatót. A maradandó sütik a kiszolgáló oldali azonosító – felhasználó összerendelés révén alkalmasak az azonosítására, így minden olyan esetben, ahol a felhasználó hitelesítése elengedhetetlen – pl. webáruház, netbank, webmail – a helyes működés szükséges feltételei.

Mivel a süti kezelés, adatkezelésnek minősül, az általunk használt sütikről tájékoztatást kell nyújtani. Tájékoztatni kell a honlap látogatóját, hogy milyen sütit használunk, a sütinek mi a feladata, és meddig tárolja a látogató eszköze az adott sütit. Arról is tájékoztatást kell nyújtani, hogy a süti alkalmazása szükséges-e a honlap működéséhez, esetleg statisztikai adatokat tárol, vagy marketing sütiről van szó.

A hozzájárulást nem igénylő sütik esetén honlap első látogatása során kell tájékoztatást nyújtani.

Elegendő, ha egy látogató esetében egy alkalommal jelenik meg a tájékoztatás, és amíg a sütik alkalmazásának körülményei nem változnak, a honlapon nem jelenik meg újabb tájékoztatás az adott látogató számára. De tájékoztatást később is könnyen elérhetővé kell tenni.

A hozzájárulást igénylő sütik esetében a tájékoztatás kapcsolódhat a honlap első látogatásához is, abban az esetben, ha a sütik alkalmazásával együtt járó adatkezelés már az oldal felkeresésével megkezdődik. Amennyiben a süti alkalmazására a látogató által kifejezetten kért funkció igénybevételéhez kapcsolódik, akkor a tájékoztatás is megjelenhet e funkció igénybevételéhez kapcsolódóan. A látogatók hozzájárulásán alapuló sütik nem települhetnek addig, amíg nem szereztük meg a hozzájárulást. Ez a látogatók oldaláról nézve magában foglalja azt is, hogy a látogatók addig nem férhetnek hozzá a honlaphoz vagy valamely tartalmához, funkciójához, amíg nem nyilatkoztak a hozzájárulásukon alapuló sütik elfogadásáról vagy tiltásáról.

A hozzájárulást ugyanakkor sütinként – de legalább kategóriánként - külön-külön kell beszerezni. Nem fogadható el az a megoldás, ha valamennyi, a látogató hozzájárulását igénylő sütihez egyszerre kérünk egyetlen hozzájárulást.

Az alábbi felsorolás a szükséges sütiket tartalmazza a WP29 iránymutatása alapján, használatukhoz tehát **nem kell hozzájárulást kérni**:[6]

- a felhasználó által rögzített adatokat tároló sütik *(„user-input cookies");*
- hitelesítési munkamenet-sütik *(„authentication cookies");*
- felhasználóközpontú biztonsági sütik *(„user centric security cookies");*
- multimédia-lejátszó munkamenet-sütik *(„multimedia player session cookie");*
- terheléskiegyenlítő munkamenet-sütik *(„load balancing session cookies");*

---

[6] a WP29 munkacsoport 2012/4 sz- véleménye. Ezzel kapcsolatban azonban meg kell jegyeznünk, hogy ez egy korábbi uniós irányelv elemzésén alapul, amit a most tárgyalás alatt lévő E-pivacy rendelet fel fog váltani, így változás is elképzelhető.

- a felhasználói felület testreszabását segítő munkamenet-sütik *(„user interface customization cookies")*.

A marketing célú sütiket kizárólag a honlap látogatójának hozzájárulását követően lehet alkalmazni. Mivel a látogatónak hozzájárulást még a honlap böngészését megelőzően kell megadnia, javasolt a tájékoztatást és a beállításokat lehetővé tevő panelt egy „felugró ablakban" elhelyezni a honlapon.

Tekintettel arra, hogy a marketing és statisztikai sütiket csak hozzájárulás alapján lehet kezelni, az alapbeállítás kizárólag a szükséges sütik elhelyezését engedélyezheti!

A közérdekű és közérdekből nyilvános adatok közzétételi kötelezettségére vonatkozó előírásokat az erre vonatkozó külön szabályzat tartalmazza. (18.5.)

12. Adatbiztonsági előírások

A BMK munkatársa a nála lévő, személyes adatnak minősülő adatokat tartalmazó iratokat köteles munkaidőn túl - és amelyeket lehetséges munkaidőben is - szekrényébe zárva tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt tárolhatók. Az ilyen iratok elzárásáért az az ügyintéző felelős, akinél azok a munkaidő befejezésekor találhatók.

Azokat a helyiségeket, ahol közös használatú nyomtató vagy másológép üzemel, az adatbiztonsági követelmények figyelembevételével kell használni.

Azokat a szobákat, helyiségeket, ahol számítógép, munkaállomás üzemel, úgy kell használni, hogy az megfeleljen az adatvédelmi, tűzrendészeti és informatikai biztonsági követelményeknek.

A BMK munkatársa köteles a számítógépet és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a munkaállomást kikapcsolni, az ajtót bezárni.
A tűzrendészeti előírásokat be kell tartani. A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a BMK Tűzvédelmi szabályzata tartalmazza.

Személyes adatokat is tartalmazó iratot a BMK épületéből kivinni - munkaköri feladat ellátásának kivételével - csak a közvetlen felettes vezető engedélyével lehet. Az ügyintéző ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg, és tartalma illetéktelen személy tudomására ne jusson. Az ügyintéző harmadik személlyel személyes és különleges adatot nem közölhet, illetve ilyen adatot harmadik szermélynek nem adhat át.

Az iratok telefaxon, az adatok telefonon, illetve egyéb elektronikus úton csak kellő körültekintéssel, legalább jelszóval védett fájlban továbbíthatók. Külső adathordozó esetén az adathordozót szintén legalább jelszavas védelemmel kell ellátni.

Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot az önálló szervezeti egységek vezetőjének személyre lebontottan meg kell határoznia, és az időszerű állapotnak megfelelő nyilvántartásukról gondoskodnia kell.

A személyes adatokat tartalmazó számítógépes információs rendszer védelme érdekében gondoskodni kell az információs rendszerben az adatkezelés biztonságáról, a működtetés rendjéről.

Bár a kézi, azaz nem automatizált (más kifejezéssel: papír alapú) adatkezelések esetében a GDPR hatálya csak azokra az adatokra terjed ki, amelyek valamely nyilvántartási rendszer részei, vagy amelyek kezelése nyilvántartási céllal történik (annak minősülhet bármilyen jegyzék, lista, amelyben az adatok bármilyen szempont szerint kereshetők, illetve csoportosításra kerülnek), az Info tv. alapján a GDPR-ban foglalt szabályokat ezen

adatkezelésekre is alkalmazni kell majd.

Nem lehet tehát különbséget tenni a papír alapú vagy a számítógépes adatkezelés között a védelmi szint tekintetében.

A GDPR nem határozza meg pontosan, hogyan járjunk el az adatok biztonságos kezelése során, milyen technológiát alkalmazzunk, ahogy az Info tv. sem teszi. Az elvárás viszont, hogy a tudomány és 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 hajtsanak végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Egyszerűbben kifejezve, meg kell tenni minden tőlünk telhetőt a biztonság garantálására. Papír alapú adatkezelésnél főként azt kell biztosítanunk, hogy illetéktelenek ne férhessenek hozzá az adatokhoz, ideértve az olyan munkavállalókat is, akiknek nincs feladatuk az adott dokumentummal kapcsolatban.

Ennek eszközei lehetnek:

- ✓ kategorizálás;
- ✓ anonimizálás másolatok készítésével;
- ✓ elzárt tárolás (pl. széf, zárható szekrény, zárható fiók);
- ✓ felesleges (személyes adatokat tartalmazó), vagy olyan dokumentumok megsemmisítése iratmegsemmisítővel, amelyek adattárolási ideje lejárt;
- ✓ elektronikus adatok törlése esetén a dokumentum nyomtatott példányait is törölni kell.

A papír alapú iratok adminisztratív szempontú kezelésének pontos módjáról az Iratkezelési Szabályzat rendelkezik. (18.2.)

13. Biztonsági rendszerek használata

A BMK által alkalmazott kamerák beállításának és használatának részletes szabályozását a Kamerarendszer Üzemeltetési Szabályzat tartalmazza. (18.1.)

14. Szerződések

14.1. Adatfeldolgozói szerződések

Az alvállalkozói szerződésekhez **rendelkezésre áll az adatfeldolgozói szerződések mintája**. Adatfeldolgozónak számít az a cég vagy személy, amely vagy aki kizárólag technikai végrehajtást végez a mi utasításaink alapján, önálló döntést az adatkezelés kapcsán sosem hoz.

Az ilyen cégeket az együttműködő cégek nyilvántartásában fel kell tüntetni. (18.7.)

14.2. Közös adatkezelői szerződés

A BMK több tekintetben közös adatkezelést végez a Fővárosi Szabó Ervin Könyvtárral (FSZEK). A közös adatkezelők a GDPR. 26. cikke alapján feladataikat és a felelősség megosztását megállapodásban rögzítik. A két intézmény között tehát ilyen megállapodás aláírása és szükség esetén módosítása szükséges az alábbiak szerint.

Az államháztartásról szóló 2011. évi CXCV. törvény 10. § (4a) bekezdés b) pontja értelmében a BMK gazdasági szervezetének gazdasági, pénzügyi és műszaki feladatait a FSZEK látja el

A közös adatkezelők az itt felsorolt adatkezelések során a természetes személyek adatai vonatkozásában közös adatkezelést végeznek, az adatkezelés céljait és eszközeit közösen határozzák meg.
1. Pénzügyi kötelezettségvállalás
2. Munkavállalókkal kapcsolatos adatkezelés
3. Működtetési és üzemeltetési feladatok
4. Felnőttképzési szerződések

Felek közös adatkezelés során betöltött szerepe

1. Pénzügyi kötelezettségvállalás
A BMK kiadási előirányzatai tekintetében a BMK igazgatója kötelezettségvállalási jogkörrel rendelkezik. A személyi kifizetéseket érintően a FSZEK készíti el a kötelezettségvállalások dokumentumait.

2. Munkavállalókkal kapcsolatos adatkezelés
A munkavállalók kiválasztását, felvételét és utasítását a BMK végzi, míg a foglalkoztatáshoz kapcsolódó minden egyéb tevékenység a FSZEK feladata különös tekintettel a következőkre: adminisztráció, bérelszámolás, utalás.

3. Működtetési és üzemeltetési feladatok
Felek által közösen használt épülethez tartozó berendezések, így a BMK székhelyén található kamerarendszer működtetése és üzemeltetése a FSZEK feladata.

4. Felnőttképzési szerződések
A képzéseket a BMK szervezi és tartja, míg a FSZEK a gazdasági jellegű feladatokban működik közre.

Az érintett tájékoztatása

Felek az adatkezelésekről az alábbiak szerint nyújtanak tájékoztatást:
1. Pénzügyi kötelezettségvállalás - Adatkezelési Tájékoztató
A tájékoztató az alábbi helyeken érhető el:
- BMK honlapján;
- FSZEK honlapján.

2. Munkavállalókkal kapcsolatos adatkezelés – Munkavállalók adatvédelmi tájékoztatója
A tájékoztató az alábbi helyeken érhető el:
- BMK belső hálózatán (intranet);
- FSZEK belső hálózatán (intranet).

3. Működtetési és üzemeltetési feladatok – Kamerarendszer adatkezelési tájékoztató
A tájékoztató az alábbi helyeken érhető el:
- BMK honlapján;
- FSZEK honlapján.

4.Felnőttképzési szerződések – A szerződéshez kapcsolódó adatkezelési tájékoztató
A tájékoztató az alábbi helyeken érhető el:
- A szerződések mellékletében;
- A képzés leírását tartalmazó online felületeken.

15. Nyilvántartási kötelezettség

A GDPR 30. cikke – az abban meghatározott tartalommal és kivételekkel - előírja, hogy a végzett adatkezelési tevékenységekről **nyilvántartást kell vezetni (18.6.), melyet megkeresésre a felügyeleti hatóság (NAIH) rendelkezésére kell bocsátani és az adatkezelés jogszerűségét ezáltal is igazolni.**

A nyilvántartást legalább évente felül kell vizsgálni és aktualizálni. Valamennyi szervezeti egység feladta, hogy felülvizsgálja a saját területén alkalmazott eljárásokat és rendszereket és ahol szükségesnek látja módosításokat javasoljon.

Azonban a mennyiben a nyilvántartás módosítása évközben is szükségessé válik, azt az Adatvédelmi Felelős és az Adatvédelmi Tisztviselő felé jelezni kell.

16. Hatásvizsgálat

Az adatvédelmi hatásvizsgálatok azoknak az új helyzeteknek a módszeres elemzésére irányulnak, amelyek a természetes személyek jogaira és szabadságaira nézve magas kockázattal járhatnak. Csak akkor kötelező adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve".[7] Ez különösen új adatkezelési technológiák bevezetésekor lényeges.

Az adatkezelési művelet *„valószínűsíthetően magas kockázattal jár"* többek között:

a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;

b) a személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;

c) nyilvános helyek nagymértékű, módszeres megfigyelése.

Ezzel szemben előfordulhat, hogy egy adatkezelési művelet ugyan megfelel a fent ismertetett esetek egyikének, az adatkezelő azonban mégsem úgy ítéli meg, hogy „valószínűsíthetően magas kockázattal jár". Ilyenkor az adatkezelőnek indokolnia és dokumentumokkal igazolnia kell az adatvédelmi hatásvizsgálat mellőzésének okait, és ezzel összefüggésben az adatvédelmi tisztviselő álláspontját is közölnie/rögzítenie kell.[8]

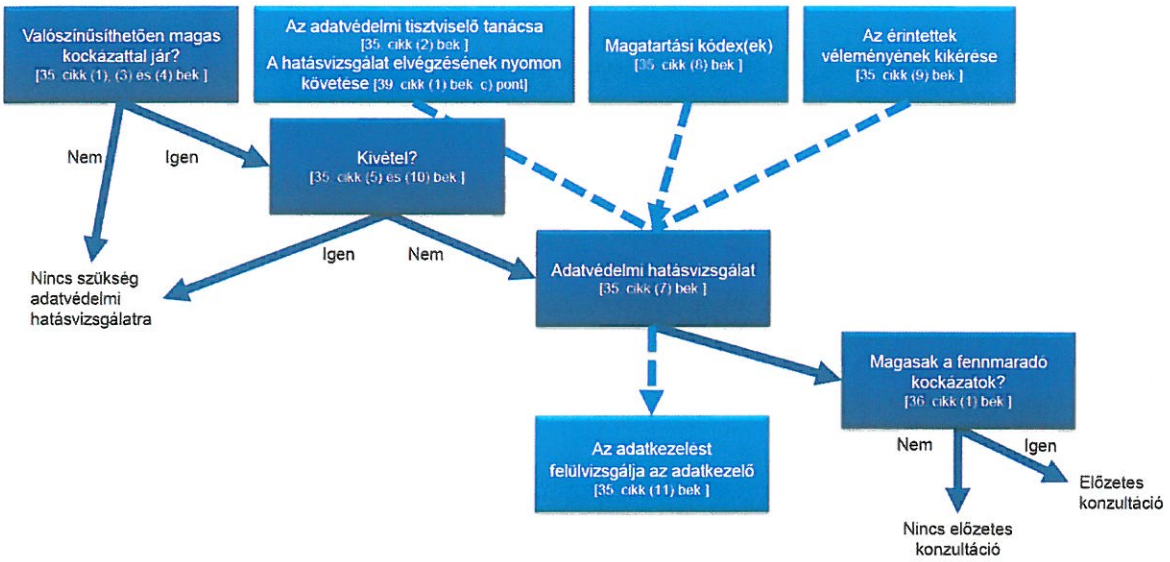
Annak megítéléséhez, hogy javasolt-e a hatásvizsgálatot elvégezni az alábbi ábra nyújt segítséget[9]. Ugyanakkor a NAIH honlapján található lista segítségével pontosan megállapítható, hogy mikor kötelező mindenképp a hatásvizsgálat elvégzése.

---

[7] 35. cikk (1) bekezdése, részletesen kifejti a 35. (3) bekezdése, és kiegészíti 35. cikk (4) bekezdése

[8] WP29 Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e 14. old.

[9] WP29 Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e 8. old.



Az adatvédelmi hatásvizsgálatot *„az adatkezelést megelőzően"* kell elvégezni, az alábbiak szerint.[10]

A hatásvizsgálat lefolytatására **a NAIH honlapjáról letölthető hatásvizsgálati szoftvert kell használni.**

A hatásvizsgálat lefolytatását követően[11]:

- ✓ A NAIH kérésére - az adatvédelmi hatásvizsgálatról szóló jelentést be kell nyújtani a NAIH felé;
- ✓ Konzultálni kell a NAIH-hal, ha nem sikerült megfelelő intézkedéseket hozni a magas kockázatok csökkentésére;

---

[10] WP29 Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e 19. old.

[11] WP29 Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e 23.old.

- ✓ Rendszeresen, de legalább az adatkezelési művelettel járó kockázat megváltozása esetén felül kell vizsgálni az adatvédelmi hatásvizsgálatot és a tárgyát képező adatkezelést;
- ✓ Írásba kell foglalni a hatásvizsgálat alapján hozott döntéseket.

17. Adatvédelmi incidens

Az adatvédelmi incidens akkor következik be, amikor az adat biztonsági előírásokat valaki szándékosan, vagy véletlenül nem tartja be és ennek eredményeképpen sérül a titoktartási kötelezettség, a hozzáférhetőség vagy az integritás. *(pl. nyilvánosságra kerülnek e-mailcímek, telefonszámok vagy bankkártya adatok; elvesznek merevlemezek, akták, amelyeken személyes adatok szerepelnek; valaki feltöri az online rendszert, stb...)*

Ha ez bekövetkezik és az incidens feltehetően kockázatot jelent az érintettek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül, legkésőbb 72 (Hetvenkettő) órával azután, hogy az adatvédelmi incidens a tudomásunkra jutott, azt jelenteni kell a NAIH felé és általában értesíteni kell az érintetteket is.

Ha nem jelent nagy kockázatot, nem kell jelenteni és nem kell értesíteni az érintetteket, de a hibát azonnal helyre kell hozni és fel kell vezetni az incidensek nyilvántartásába (18.8.).

Az adatvédelmi incidensek kezeléséről az Incidenskezelési Terv részletesen rendelkezik. (18.3.)

18. Adatvédelmi tisztviselő

A GDPR 37. cikke alapján az adatkezelő adatvédelmi tisztviselőt köteles kijelölni minden olyan esetben, amikor az adatkezelést közfeladatot ellátó szerv végzi. A BMK esetén tehát **indokolt az adatvédelmi tisztviselő kinevezése.**

Az adatvédelmi tisztviselő az alábbi feladatok ellátására köteles:
- ✓ Tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

- ✓ Ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

- ✓ Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR. 35. cikk szerinti elvégzését;

- ✓ Együttműködik a felügyeleti hatósággal;

- ✓ Az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

A feladatkörök bővíthetők.

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

Releváns készségek és szakértelem például:
- ✓ szakértelem a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, beleért-ve a GDPR alapos

ismeretét;
- ✓ az elvégzett adatkezelési műveletek ismerete;
- ✓ az információs technológiák és az adatbiztonság ismerete;
- ✓ az üzletág és a szervezet ismerete;
- ✓ a szervezeten belül az adatvédelmi kultúra előmozdításának képessége.

Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait. Bár az adatvédelmi tisztviselőknek lehet más feladatuk, csak olyan egyéb feladatokkal bízhatók meg, amelyek nem okoznak összeférhetetlenséget. A GDPR 38. cikk (3) bekezdése szerint az adatvédelmi tisztviselőt úgy kell kijelölni, hogy senkitől ne fogadhasson el utasításokat a tisztviselői feladatának ellátásával kapcsolatban. Az adatvédelmi tisztviselő közvetlenül az adatkezelő legfelső vezetésének tartozik felelősséggel. Ugyanakkor az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit, vagyis nem lehet vezető sem.

Az adatvédelmi tisztviselő elérhetőségét közzé kell tenni és a személyét a NAIH felé be kell jelenteni az erre kialakított online felületen.

Záró rendelkezések

Jelen szabályzat 2021. július 05-ével lép hatályba. A tárgyra vonatkozó minden korábbi szabályozás hatályát veszti.

Budapest, 2021. július 05.

Jóváhagyja és hatályba lépteti

Marsi László

igazgató

MELLÉKLETEK:

Jelen Szabályzat elválaszthatatlan részét képezik az alábbi belső szabályzatok és nyilvántartások:

18.1. **Kamerarendszer Üzemeltetési Szabályzat**

18.2. **Iratkezelési Szabályzat**

18.3. **Incidenskezelési Terv**

18.4. **Szabályzat a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről**

18.5. **Szabályzat a közérdekű és közérdekből nyilvános adatok elektronikus közzétételének rendjéről**

18.6. **Adatkezelések nyilvántartása**

18.7. **Az együttműködő cégek nyilvántartása**

18.8. **Adatvédelmi incidensek nyilvántartása**