

FEHÉRVÁR MÉDIACENTRUM KFT.
ADATKEZELÉSI, ADATVÉDELMI
SZABÁLYZATA

Hatályos: 2026.08.26.

Tartalom

I. RÉSZ: ÁLTALÁNOS RENDELKEZÉSEK	5
A szabályozás célja és hatálya	5
A Szabályzat személyi hatálya kiterjed:	5
A Szabályzat tárgyi hatálya kiterjed:	5
A Szabályzat időbeli hatálya:	6
II. RÉSZ: ADATVÉDELEM FELELŐSSÉGI RENDSZERE	6
Az adatkezelő vezetőjének felelősségi rendszere	6
A társaság ügyvezetőjének a feladat- és hatásköre	6
A társaság adatvédelmi tisztviselője	7
Adatfeldolgozókkal szemben támasztott követelmények	7
III. RÉSZ: A SZEMÉLYES ADATOK VÉDELME A TÁRSASÁGNÁL	8
Az adatkezelés alapvető szabályai	8
A társaság adatkezelési tájékoztatója	9
A társaság egyéniesített adatkezelési tájékoztatása és annak rendje	9
IV. RÉSZ: AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI	9
Hozzájáruláson alapuló adatkezelések	9
Szerződésen alapuló adatkezelések	10
Jogi kötelezettségen alapuló adatkezelések	10
Jogos érdeken alapuló adatkezelések	10
Az utánközlés, másodközlés és sajtószemlézés önálló adatkezelési felelőssége („szemlézői felelősség”)	11
Nem közszereplők magánszférája és különleges (bűnügyi) adatok kezelése a sajtóban	11
Drónfelvételek készítéséhez kapcsolódó eljárásrend	12
Gazdasági újságírás, nyilvános cégadatok és vagyonlisták adatkezelési garanciái	12
A vagyonbecslések és gazdasági toplisták eljárási garanciái	13
Kiskorúak és kiszolgáltatott személyek adatkezelésére vonatkozó eljárásrend	13
Olvasói fotók beküldésére irányuló felhívások eljárásrendje	13
Kiemelt figyelemmel bíró felvételek készítése	14
Egészségügyi adatok közzétételi tilalma	14
Személyes adatok gyűjtési céltól eltérő kezelése	14
V. RÉSZ: MUNKAVISZONNYAL KAPCSOLATOS ADATKEZELÉSEK	15

Személyügyi nyilvántartás	15
VI. RÉSZ: ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK ELJÁRÁSRENDJE	15
Az adatvédelmi incidens fogalma és példái	16
Az incidensek észlelése és belső jelzésének rendje	16
Kivizsgálás és kockázatértékelés	17
Intézkedések az incidensek orvoslására és dokumentálása	17
Jelentéstétel a Hatóság (NAIH) felé.....	18
Az érintettek tájékoztatásának rendje	18
VII. RÉSZ: ADATVÉDELMI HATÁSVIZSGÁLAT	18
Adatvédelmi hatásvizsgálat és előzetes konzultáció.....	18
VIII. RÉSZ: AZ ADATTOVÁBBÍTÁS SZABÁLYAI.....	20
Adatkezeléssel, adattovábbítással megbízott dolgozók.....	20
Hatósági megkeresések	20
Külföldi adattovábbítás	20
IX. RÉSZ: AZ ÉRINTETT JOGAI ÉS JOGGYAKORLÁSÁNAK ELŐSEGÍTÉSE	21
Tájékoztatás az érintett jogairól.....	21
A kérelmek fogadásának és azonosításának eljárása	22
A kérelmek vizsgálatának és pontosításának rendje	22
Egyes érintetti jogok teljesítésének és intézésének eljárásrendje	23
Hozzáféréshez való jog	23
Helyesbítéshez és kiegészítéshez való jog	23
A törléshez való jog (elfeledtetéshez való jog) különös eljárásrendje.....	23
Az adatkezelés korlátozásához való jog.....	25
Adathordozhatósághoz való jog	25
Tiltakozáshoz való jog	25
A kérelmek teljesítésével és elutasításával kapcsolatos eljárási szabályok	25
Az eljárás lezárását követő intézkedések	26
A Szabályzat megállapítása, módosítása és felülvizsgálata.....	26
Korábbi különálló szabályzatok hatályon kívül helyezése és záró rendelkezések	26

A Fehérvár Média centrum Kft. (továbbiakban: társaság vagy Társaság) tevékenysége során elkötelezett az adatvédelmi és adatbiztonsági előírások betartása iránt. 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 (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) mindenkor hatályos szabályain túl a társaság vezetője kiadja jelen egységes adatkezelési, adatvédelmi és adatbiztonsági szabályzatot (továbbiakban: Szabályzat).

A jelen Szabályzat egyúttal magában foglalja és egységes szerkezetbe foglalja a korábban különálló Érintetti joggyakorlást elősegítő szabályzatot, valamint a különálló Adatvédelmi incidenskezelési Szabályzatot is. Ezen szabályozások beépítésével a különálló szabályzatok a jelen egységes szabályzat hatálybalépésének napjával hatályukat veszítik, és helyükbe minden tekintetben a jelen egységes Szabályzat rendelkezései lépnek.

A társaság kiadói és médiaszolgáltatási, tömegtájékoztatási, reklám tevékenységet végez. A társaság a Szabályzat elfogadása idején munkavállalókat foglalkoztat, így a kapcsolódó adatkezelésekről is jelen Szabályzat rendelkezik. A társaság papír alapú adatkezeléseken, nyilvántartásokon túl, elektronikus formában is kezel és tart nyilván adatokat, az adatbiztonsági követelményeket jelen Szabályzat, illetve az információbiztonsági szabályzata (IBSZ) szerint teljesíti.

A Társaság kiadói és médiaszolgáltatási tevékenységéből adódóan kiemelten fontos feladatának tekinti a véleménynyilvánítás szabadságához, valamint a sajtószabadságból fakadó tájékozódáshoz és tájékoztatáshoz való alapjogok érvényesülését. Ezen alapjogok gyakorlása azonban szoros és elválaszthatatlan kölcsönhatásban áll az érintett természetes személyek személyes adatainak védelméhez fűződő jogaival. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) és a bíróságok (különösen a Kúria és a Fővárosi Törvényszék) legújabb határozataiban megnyilvánuló szigorú jogalkalmazási elvárások szükségessé teszik a Társaság belső adatkezelési szabályzatának érdemi kiegészítését, finomhangolását és a gyakorlatba ültethető garanciák írásbeli rögzítését a szerkesztőségi és újságírói folyamatok NAIH-megfelelőségének biztosítására.

A társaság ügyfeleit, munkatársait, illetve a vele bármilyen jogviszonyban álló személyeket nem kategorizálja, nem minősíti, ilyen célból adatot nem kezel. Az adatvédelmi elveknek a GDPR 25. cikk alapján a társaság valamennyi tevékenysége, döntése során érvényesülnie kell. A társaság törekszik arra, hogy a lehetőségekhez képest olyan adatvédelmi informatikai megoldást, szervezeti szabályozást alkalmazzon, amely az adatok védelmét a tudomány és technika állása szerint a leghatékonyabban biztosítja. A társaság valamennyi adatvédelmi folyamatának szabályozottnak, átláthatónak, nyomon követhetőnek, konkrét munkakörhöz rendelhetőnek kell lennie. A társaság törekszik arra, hogy amennyiben meghatározott cél elérése személyes adat kezelése nélkül is elérhető, úgy ne kezeljen személyes adatot. A társaság a munkavállalói tevékenységét úgy szervezi meg, hogy lehetőleg minél kevesebb munkavállaló kezeljen

személyes adatokat, a személyes adatot kezelő munkavállaló pedig a személyes adatok egy konkrét csoportját kezelje.

I. RÉSZ: ÁLTALÁNOS RENDELKEZÉSEK

A szabályozás célja és hatálya

A társaság Szabályzatának kibocsátási célja, hogy tevékenysége során a személyes adatok védelméhez fűződő adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározásra kerüljenek az adatkezelési és adatvédelmi előírások, továbbá az érintettek jogai megfelelően biztosítva legyenek.

A szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy a társaság adatkezelő és adatfeldolgozó tevékenysége megfeleljen a GDPR és az Infotv. rendelkezéseinek, továbbá, hogy a napi szerkesztőségi munka során is egyértelmű, jogilag megalapozott és a hatósági elvárásoknak maradéktalanul megfelelő eljárási utat jelöljön ki az újságírók, szerkesztők és a belső munkatársak számára.

Jelen szabályzatban nem szereplő kérdésekben a GDPR and az Infotv. szabályai szerint kell eljárni.

A társaság rendelkezésében lévő elektronikus információs rendszerekre (EIR), azok rendszerelemeire, valamint az azokban kezelt személyes adatok technikai és szervezési biztonsági intézkedéseire a jelen Szabályzat mellett a Fehérvári Médiacentrum Kft. Információbiztonsági Szabályzata (IBSZ) kötelezően alkalmazandó. A két szabályzat utasításai egymással teljes összhangban vannak, egymást kiegészítik, és közöttük ellentmondás nem állhat fenn. Az információbiztonsági és adatvédelmi szerepkörök (IBF és DPO) a biztonsági és adatvédelmi folyamatok során szorosan együttműködnek.

A Szabályzat személyi hatálya kiterjed:

- az Adatkezelő valamennyi munkavállalójára;
- az eseti jelleggel munkavégzésre igénybe vett dolgozóra;
- az adatfeldolgozóra, valamint
- a fentiekén kívül mindazon személyre, aki az Adatkezelővel bármilyen szerződéses jogviszonyban áll.

A Szabályzat tárgyi hatálya kiterjed:

- az Adatkezelőnél keletkezett valamennyi személyes és egyéb védendő adatra;
- az informatikai rendszerben kezelt vagy feldolgozott személyes és egyéb védendő adatra;
- az adatkezelés eredményeképpen létrejött személyes és egyéb védendő adatra;
- az Adatkezelőnél alkalmazott valamennyi személyes és egyéb védendő adatot kezelő hardver- és szoftvereszközre;
- az Adatkezelő tevékenységével kapcsolatos, működése során keletkező közérdekű adatra vagy közérdekből nyilvános adatra.

A Szabályzat időbeli hatálya:

- a Szabályzat az alkalmazottakkal való közléstől visszavonásáig hatályos.
- Jelen szabályzat kötelezően felülvizsgálandó:
 - jelentős szervezeti vagy jogszabályi változásokat követően,
 - a hatályossá válását követően két évente, az IBSZ két évenkénti felülvizsgálati ciklusával összehangoltan,
 - az adatkezelések változása, új adatkezelés bevezetése esetén haladéktalanul.

II. RÉSZ: ADATVÉDELEM FELELŐSSÉGI RENDSZERE

Az adatkezelő vezetőjének felelősségi rendszere

Az adatvédelemre vonatkozó előírások alkalmazása során az adatkezelő vezetőjének a társaság ügyvezetőjét kell tekinteni.

A társaság ügyvezetője felelős:

- a) a társaság adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, a szükséges feltételek biztosításáért;
- b) a munkavállalók adatvédelmi oktatásáért és továbbképzéséért;
- c) a társaság tevékenységének rendszeres adatvédelmi ellenőrzéséért, a feltárt hiányosságok megszüntetéséért;
- d) az érintettek jogainak gyakorlásához szükséges feltételek biztosításáért;
- e) az adatvédelmi tisztviselő kiválasztásáért, alkalmazásáért vagy megbízásáért.

A társaság ügyvezetőjének felelőssége nem zárja ki a társasággal kapcsolatban álló személyek kártérítési vagy büntetőjogi felelősségét. Amennyiben a személyes adatokhoz való jog megsértése miatt a társaságnak sérelemdíj- vagy kártérítés-fizetési kötelezettsége keletkezik, a jogsértést ténylegesen elkövető személy kilétének felderítésére mindent meg kell tenni, és vele szemben kártérítési eljárást kell kezdeményezni.

A társaság ügyvezetőjének a feladat- és hatásköre

Az adatkezelő szerv vezetőjének feladat- és hatásköre:

- a) az adatkezelési rendszerek egészének kialakítása, irányítása és rendeltetésszerű működtetése, a törvényes rendelkezések érvényre juttatása;
- b) gondoskodás a jogosulatlan hozzáférés, közlés, megváltoztatás vagy törlés megelőzéséről, a technikai védelemről és az érintettek joggyakorlásáról;
- c) személyes felelősség vállalása a társaság és a munkavállalók, szerződéses partnerek tevékenységéért és az adatvédelmi előírások betartásáért;
- d) a védelmi és biztonsági szabályok érvényesülésének ellenőrzése, intézkedés a hiányosságok felszámolására;
- e) az adatbiztonsági és működési követelmények érvényre juttatása;
- f) az adatkezelések szabályozottságának és dokumentáltságának kialakítása, ellenőrzése;

- g) adatvédelmi kockázatok elemzése és hatásvizsgálat lefolytatása;
- h) az adatkezelési nyilvántartás és az adatvédelmi incidens-nyilvántartás naprakész vezetésének biztosítása.

A társaság adatvédelmi tisztviselője

A társaság az adatvédelmi szabályoknak való megfelelés érdekében adatvédelmi tisztviselőt (DPO) bíz meg. A DPO olyan szakértő, aki az adatvédelmi jogot és gyakorlatot szakértői szinten ismeri. Közvetlenül az ügyvezetőnek tartozik felelősséggel, és feladatának ellátásával összefüggésben nem bocsátható el, és szankcióval nem sújtható.

Az adatvédelmi tisztviselő elsősorban tanácsadó és monitoring szerepkört lát el. Az online médiatartalom-szolgáltatók adatkezelési gyakorlatára vonatkozó hatósági iránymutatások alapján az adatvédelmi tisztviselő pozíciójából és a rá vonatkozó összeférhetetlenségi szabályokból fakadó követelmény, hogy az érintetti joggyakorlás iránti kérelmek kapcsán érdemi döntést nem hozhat – döntést kizárólag a társaság vezetője (ügyvezető) hozhat –, a DPO felkérésre véleményezheti a kérelmeket és tanácsot adhat azok teljesíthetőségéről.

Az adatvédelmi tisztviselő feladatköre:

- a) a társaság adatvédelmi tevékenységének szakmai irányítása, tanácsadás és iránymutatás nyújtása;
- b) közreműködés és segítségnyújtás az adatkezelési döntések meghozatalában és az érintettek jogainak biztosításában;
- c) az adatkezelésre vonatkozó jogszabályok, a Szabályzat és az adatbiztonsági követelmények megtartásának ellenőrzése;
- d) bejelentések kivizsgálása, incidens észlelése esetén a megszüntetésre való felhívás, javaslattevés a károk elhárítására;
- e) szabályzatok, adatvédelmi tájékoztatók tervezeteinek előkészítése és a jogszabályváltozások nyomon követése;
- f) a társasággal jogviszonyban álló személyek adatvédelmi oktatása és továbbképzése;
- g) kapcsolatot tart a NAIH-hal, közreműködik a hatósági vizsgálatokban és megkeresések megválaszolásában;
- h) az érintetti kérelmekre adandó válasziratok tervezetének előkészítése;
- i) az adatvédelmi hatásvizsgálat lefolytatásának segítése és szakmai tanácsadás nyújtása;
- j) szoros együttműködés az IBSZ-ben meghatározott információbiztonsági felelőssel (IBF), a műszaki vezetővel és az IT Üzemeltetővel a biztonsági és adatvédelmi folyamatok során, megosztva a szükséges információkat az adatvédelmi hatásvizsgálatok (DPIA), kockázateértékelések és incidenskezelés hatékony lefolytatása érdekében.

Adatfeldolgozókkal szemben támasztott követelmények

A társaság kapcsolatban áll adatfeldolgozókkal, amelyek kiválasztása körében törekszik a lehető legmagasabb szintű adatvédelmi és adatbiztonsági megoldásokat nyújtó partnerek kiválasztására. Ebből a célból előzetesen megismeri az adatfeldolgozók adatvédelmi és adatbiztonsági

szabályzatát, és az adatfeldolgozói szerződésben rögzíti a vonatkozó szervezeti és informatikai biztonsági rendelkezéseket.

A társaság ügyel arra, hogy az adatfeldolgozók lehetőség szerint ne kerüljenek kapcsolatba a munkavállalók, megbízók személyes adataival. Amennyiben ez nem kerülhető el, úgy azok átadása megfelelő biztonsági intézkedések keretében történhet.

III. RÉSZ: A SZEMÉLYES ADATOK VÉDELME A TÁRSASÁGNÁL

Az adatkezelés alapvető szabályai

A társaságnál kezelt adatállományt 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 társaság köteles a Szabályzatban és más belső szabályozókban, folyamatokban és vezetői intézkedésekben meghatározott technikai és szervezési intézkedéseket érvényre juttatni a biztonság garantálása érdekében.

Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét, jogaik gyakorlásának lehetőségét.

Az adatállományhoz való hozzáférést a társaság elektronikus úton (hálózati meghajtók, jogosultsági szintek) korlátozza.

A folyamatban lévő munkavégzés, feldolgozás alatt lévő iratokhoz csak az érintett ügyintézők férhetnek hozzá. A bér-, munkaügyi és egyéb személyes adatokat tartalmazó iratokat zárható irodákban és zárható szekrényekben kell tartani.

A társaság a tudomány és technológia állása és a megvalósítás költségei, az adatkezelés jellege, hatóköre, körülményei és céljai alapján megteszi a szükséges technikai és szervezési intézkedéseket.

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 rendelkezők.

Adatbiztonsági szabályok

Az adatállomány kezelésének helyszínéül szolgáló épület megfelelő fizikai és tűzvédelméről gondoskodni kell. Az adatállomány kezelésének zárható helyiségébe csak az arra jogosultak léphetnek be. Az elektronikus informatikai rendszerekre vonatkozó adatbiztonsági előírásokat az IBSZ határozza meg.

A társaság adatkezelési tájékoztatója

A Társaság általános adatkezelési tájékoztatója új adatkezelés bevezetésekor, de legkésőbb évente felülvizsgálatra kerül. Az adatkezelési tájékoztatót a Társaság honlapján kötelező elhelyezni.

Amennyiben a társaság eseti adatkezelést végez (pl. rendezvény szervezése, álláshirdetés), úgy a vonatkozó egyedi tájékoztató kidolgozásáról és az érintettek részére elérhetővé tételéről megfelelően gondoskodik.

A társaság egyéniesített adatkezelési tájékoztatása és annak rendje

Ha a szerkesztőség egy konkrét, azonosítható személy személyes adatait (pl. e-napló adatok, hatósági ügyek részletei, magáningatlan adatai) tervezi felhasználni egy cikkben, a Társaság köteles a cikk megjelenése előtt ésszerű határidőn belül – de legkésőbb a személyes adatok megszerzésétől számított egy hónapon belül, vagy ha az adatok alapján kapcsolatba lép az érintettel, úgy az első kapcsolatfelvételkor – egyediesített tájékoztatást nyújtani az érintett részére.

Az egyediesített tájékoztatónak pontosan tartalmaznia kell: a kezelt személyes adatok kategóriáit, az adatok forrását, az adatkezelés pontos célját és jogalapját (a jogos érdek pontos megjelölésével), a várható megőrzési időt, a címzettek kategóriáit (pl. a nyilvánosság, olvasóközönség), valamint a panasz benyújtásának jogát a NAIH-hoz. Különös figyelmet kell fordítani a GDPR 21. cikk (4) bekezdésének sérelmének elkerülésére: az érintettet a tájékoztatás során világosan, kifejezetten és a többi információtól elkülönítve tájékoztatni kell a tiltakozáshoz való jogáról.

IV. RÉSZ: AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI

Hozzájáruláson alapuló adatkezelések

Amennyiben a személyes adatok kezelése hozzájáruláson alapul, az érintett hozzájárulását úgy kell beszerezni, hogy a Társaság igazolni tudja, hogy a hozzájárulás előtt az érintettet a GDPR-ban előírt módon tájékoztatta az adatkezelésről. A hozzájárulás önkéntességét biztosítani kell.

Hozzájárulásnak minősül az is, ha az érintett a társaság honlapjának megtekintése során bejelöl egy erre létrehozott négyzetet. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

A hozzájárulás visszavonását azonos módon kell lehetővé tenni, mint annak megadását. A hírlevélről történő leiratkozáshoz minden hírlevél végén linket kell biztosítani.

Ráutaló magatartással megadott hozzájárulásnak minősül, ha az érintett (riportalány, interjúalany) önkéntesen olyan körülmények között tesz nyilatkozatot a Médiaszolgáltató részére, amelyekből egyértelműen felismerhető, hogy az Adatkezelő képviselője riporter, illetve sajtómunkatársi minőségben van jelen.

A hozzájárulás az ugyanazon cél vagy célok érdekében történő összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra külön-külön meg kell adni.

Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a hozzájárulás visszavonását követően más jogalap szerint fő szabály szerint nem kezelheti az adatokat.

A társaságnak bármikor igazolnia kell tudni azt, hogy az adatkezelési művelethez az érintett hozzájárult.

Szerződésen alapuló adatkezelések

A szerződés előkészítése során, a tervezet kidolgozásakor, véleményezésre megküldése során személyes adat feltüntetésére nem kerülhet sor.

A szerződésben csak a szerződés érvényességéhez és a teljesítéséhez szükséges személyes adatok kezelhetők.

A szerződésekben külön adatvédelmi záradékot (Adatfeldolgozói vagy közös adatkezelési szerződések szerint) kell alkalmazni, amelyben rögzíteni kell a papír alapú és elektronikus védelmi intézkedéseket.

A szerződésben szereplő adatok kezelése a szerződés hatálya alatt, illetve a megszűnést követő 5 évig (követelések érvényesítése érdekében) jogszerű. 5 éven túli jótállás esetén a jótállási idő leteltét követő 5 évig kezelhetők az adatok.

A társaság a szerződést kötő partnerét tájékoztatja a szerződéskötéshez kapcsolódó lényeges adatkezelési feltételekről.

Jogi kötelezettségen alapuló adatkezelések

A jogi kötelezettségen alapuló adatkezelés szabályaira a vonatkozó jogszabályi rendelkezések irányadók.

Ezen adatkezelés az érintett hozzájárulásától független. Az érintettet az adatkezelés megkezdése előtt tájékoztatni kell az adatkezelés kötelező jellegéről, céljáról, jogalapjáról, az időtartamról és a jogorvoslati lehetőségekről.

Jogos érdeken alapuló adatkezelések

Az újságírási célú adatkezelés jogalapja főszabályként a jogos érdek (GDPR 6. cikk (1) bekezdés f) pont).

A jogos érdek alkalmazásakor az érintett hozzájárulása nélkül történik az adatkezelés, ezért garanciális jelentőségű, hogy az adatkezelő alaposan feltérképezze az adatkezelés hatásait az érintett információs önrendelkezési jogára, különösen online nyilvánosság esetén. Az érdek mérlegelést még az adatkezelés megkezdése előtt el kell végezni, és ha az érintett tiltakozik, egyénre szabott érdek mérlegeléssel kell reagálni.

A sajtótermékek által személyes adatokat tartalmazó cikkek publikálása során az érdekmérlegelésnek a konkrét közlés sajátosságait is figyelembe kell vennie.

Nem fogadható el a túl tágan, általánosságban megfogalmazott jogos érdek. Az érdekmérlegelésnek a konkrét közlés sajátosságait is figyelembe kell vennie, azokra külön és érdemben reflektálnia kell.

Az érdekmérlegelés nem lehet felületes: részletesen elemezni kell, hogy az érintett adatainak nyilvánosságra hozatala mennyiben szükséges és arányos a megjelölt újságírói cél eléréséhez, és az milyen hatással van az érintett magánszférájára. Ha az érintett a GDPR 21. cikke alapján tiltakozik a személyes adatainak kezelése ellen, a Társaság nem utasíthatja el a kérelmet sablonos jogi hivatkozásokkal. Ilyenkor kötelező egy kifejezetten az érintett egyedi élethelyzetére szabott, megismételt egyedi érdekmérlegelést lefolytatni és azt írásban dokumentálni.

Az utánközlés, másodközlés és sajtószemlézés önálló adatkezelési felelőssége („szemlézői felelősség”)

A korábban más sajtóorgánumok által már megjelentetett cikkek, információk és személyes adatok átvétele, szemlézése vagy utánközlése nem mentesíti a Társaságot az adatvédelmi felelősség alól. Az Smtv. 21. § (1) bekezdése és a GDPR 4. cikk 7. pontja alapján a Társaság mint a másodközlő sajtótermék kiadója önálló adatkezelőnek minősül, mivel a személyes adatok (újra)felhasználásának és nyilvánosságra hozatalának célját és eszközeit önállóan határozza meg.

Önmagában az a tény, hogy az információ az interneten már hozzáférhető a nyilvánosság számára, nem vonja ki azt a GDPR és az érintetti jogok védelme alól. Ha az érintett a törlést kéri, a Társaság köteles önállóan megvizsgálni a kérelem megalapozottságát, és nem hivatkozhat arra, hogy "az adatot csak más sajtóorgánumtól vette át".

A szerkesztőség köteles ellenőrizni az átvett információk aktualitását. Ha például egy büntetőeljárással kapcsolatos korábbi híradást veszünk át, kötelező bemutatni a legfrissebb fejleményeket is (pl. ha a vádlottat/tanút időközben jogerősen felmentették vagy felelősségét kizárták), ellenkező esetben az utánközlés megsérti a GDPR 5. cikk (1) bekezdés d) pontja szerinti pontosság és naprakészség elvét.

Nem közszereplők magánszférája és különleges (bűnügyi) adatok kezelése a sajtóban

- A büntetőeljárásban történő tanúvallomás tétel állampolgári kötelezettség, az nem minősül közszereplésnek.
- Valamely közszereplő politikus házastársa, hozzátartozója vagy családtagja nem válik automatikusan közszereplővé csupán azáltal, hogy hozzátartozóként segíti a politikus kampánytevékenységét (pl. szórólapozással vagy jelenléttel). E tevékenysége miatt a

magánszemély szakmai munkája vagy magánélete nem válik közérdeklődésre számot tartó közüggé.

Bűnügyi személyes adatok védelme:
Az az információ, hogy egy természetes személy tanúként vagy egyéb módon érintett egy büntetőeljárásban, az Infotv. 3. § 4. pontja alapján bűnügyi személyes adatnak (különleges adatnak) minősül. Ezek nyilvánosságra hozatala a sajtóban szigorú korlátokhoz kötött. Nem megengedett az ilyen adatok szenzációhajhász, egyoldalú bemutatása, ha az az érintett magánszférájának súlyos és aránytalan sérelmét okozza, és nem a közéleti vita érdemi megítélését szolgálja.

Korábbi felvételek eltérő célú felhasználásának tilalma:
Ha a Társaság vagy más sajtóorgánium korábban jogszerűen, az érintett hozzájárulásával készített egy képfelvételt egy pozitív kontextusú cikkhez (pl. szakmai interjú), ezen felvétel hozzájárulás és újabb LIA nélkül nem használható fel egy későbbi, az érintett számára hátrányos, negatív vagy kompromittáló híradás illusztrálásaként. Az EJEK joggyakorlata alapján önmagában az a tény, hogy a kép korábban nyilvánosságra került, nem teszi szükségtelenné a hozzájárulást vagy a kényszerítő erejű jogos érdek igazolását az újabb, eltérő célú adatkezelés során.

Drónfelvételek készítéséhez kapcsolódó eljárásrend

A Társaság munkatársai által végzett drónos és kamerás felvételkedzés során az alábbi eljárási szabályokat kell kötelezően alkalmazni:

- A megfigyelésről és a felvétel rögzítéséről az érintettet a felvétel elkészítése előtt vagy azzal egyidejűleg tájékoztatni kell, biztosítva számára a tiltakozás jogát.
- Magánlakásokról, magáningatlanok belső udvaráról drónfelvétel főszabály szerint nem készíthető, kivéve, ha az elengedhetetlenül szükséges egy kiemelkedő súlyú és bizonyított közügy (pl. súlyos és rendszerszintű hatósági jogsértés vagy közpénz-visszaélés) dokumentálásához, és a cél más módon nem érhető el.
- Ha a drónfelvételen olyan magánszemélyek vagy vagyonelemek (pl. szomszédos házak, gépjárművek rendszámai) is láthatók, amelyek nem kapcsolódnak a híradás tárgyát képező közüghöz, azokat a szerkesztőségi előszűrés során homályosítással vagy kitakarással véglegesen és felismerhetetlenné kell tenni.

Gazdasági újságírás, nyilvános cégadatok és vagyonlisták adatkezelési garanciái

A cégnyilvánosságról szóló 2006. évi V. törvény (Ctv.) 10. §-a alapján a cégjegyzék adatai és a cégiratok teljes körűen nyilvánosak. Azonban a cégadatok nyilvánossága nem jelenti azt, hogy ezen adatok bármilyen körben korlátlanul felhasználhatók lennének. A gazdasági újságírás és a vagyonbecslések során a Társaságnak szigorúan be kell tartania a célhoz kötött adatkezelés (GDPR 5. cikk (1) bekezdés b) pont) és az adattakarékosság elvét.

A vagyonebecslések és gazdasági toplisták eljárásí garanciái

Amennyiben a Társaság helyi vagy regionális üzleti toplistákat, vagyonos magánszemélyeket bemutató összeállításokat készít, a következő szabályok alkalmazandók:

- Az adatok kizárólag hiteles, közhiteles és nyilvánosan elérhető állami/bírósági adatbázisokból (e-beszámoló, BÉT honlapja, cégnyilvántartás) származhatnak.
- A szerkesztőség köteles átlátható és objektív módszertant alkalmazni a vagyonebecslés során, és kizárólag a gazdasági tevékenységgel szorosan összefüggő adatokat (pl. EBITDA, tulajdonrész, osztalékok, ingatlanvagyon) kezelhet.

- Ha az érintett üzletember tiltakozik a listán való szerepeltetés ellen, a Társaság köteles egyedi érdekmérlegelést lefolytatni. Ha az érintett nem minősül közszereplőnek, és cégei nem részesülnek kiemelkedő állami támogatásban vagy közpénz-donációkban, az érintetti tiltakozásnak helyt kell adni, és a személyes adatokat a listáról haladéktalanul törölni kell.

Kiskorúak és kiszolgáltatott személyek adatkezelésére vonatkozó eljárásrend

A kiskorúak és kiszolgáltatott helyzetben lévő személyek személyes adatainak védelme fokozott figyelmet és szigorú eljárásí garanciákat igényel, tekintettel arra, hogy ők kevésbé vannak tudatában a személyes adatok kezelésével járó kockázatoknak és jogaiknak. A NAIH határozatai és a Hatóság iránymutatásai alapján a társaság az alábbi eljárásrendet alkalmazza a hozzájárulások beszerzésére.

- Ha az adatkezelés hozzájáruláson alapul, a 16. életévét be nem töltött gyermek (kiskorú) esetén a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeleti jogot gyakorló személy adta meg vagy engedélyezte. A 16. életévüket be nem töltött érintettek esetén az adatkezelés érvényességének feltétele a szülői felügyeleti jogot gyakorló személy hozzájárulása. A Médiaszolgáltató kifejezetten rögzíti, hogy a sajtó részvételével zajló eseményeken a megfelelő előzetes adatvédelmi tájékoztatás elvégzése, és a szükséges szülői hozzájárulások igazolható módon történő beszerzése a meghívó adatkezelő (eseményszervező)felelőssége.

- A társaságnak az elérhető technológia figyelemmel kísérése mellett ésszerű erőfeszítéseket kell tennie annak érdekében, hogy ellenőrizze a szülői hozzájárulás valódiságát és érvényességét. Ehhez írásbeli, azonosításra alkalmas szülői nyilatkozat beszerzése szükséges.

Olvasói fotók beküldésére irányuló felhívások eljárásrendje

A médiaszolgáltató, valamint a fényképet készítő olvasó egyaránt adatkezelőnek minősül. A technikai publikálást minden esetben meg kell előznie a jogi megalapozottság vizsgálatának.

A felhívás közzététele előtt a szerkesztőség köteles előzetesen értékelni, hogy milyen típusú és témájú képek közzététele jogszerű, és erről az olvasókat részletesen tájékoztatni kell.

A beküldött képeket a közzététel előtt moderálni kell. Tilos közzétenni az alábbi kategóriákat: Az emberi méltóságot sértő, betegségben szenvedők, bódult állapotúak, vagy szociálisan kiszolgáltatott személyek ábrázolását, illetve szülői hozzájárulás nélkül kiskorúakról készült felvételt. Továbbá olyan képeket, amelyekből következtetni lehet az egészségi állapotra, vallási meggyőződésre (pl. vallási szimbólum viselése) vagy szexuális irányultságra.

Az érintettek számára a lehető legnagyobb mértékű autonómiát kell biztosítani személyes adataik felett, és az adatkezelő nem használhatja ki az érintettek sebezhetőségét.

Titokban készült felvétel nem hozható nyilvánosságra. A szerkesztőség minden munkatársa egyéni felelősséggel tartozik a szabályzat betartásáért.

A jogellenesen beküldött fotókat a rendszerből haladéktalanul, véglegesen törölni kell.

Kiemelt figyelemmel bíró felvételek készítése

A GDPR 9. cikke alapján a vallási meggyőződésre utaló adatok különleges személyes adatnak minősülnek, amelyek kezelése főszabály szerint tilos. A templomi közvetítések, szentmisék közvetítése során a hívőkről készült közeli, azonosítható képfelvételek közvetve feltárják az érintettek vallási hovatartozását. Ennek elkerülése érdekében:

- A kamerát úgy kell beállítani, hogy a hívőkről ne készüljenek közeli, azonosításra alkalmas portréfelvételek. A felvételeket hátulról vagy olyan látószögből kell készíteni, amely kizárja az egyedi azonosítást.

- A templom bejáratánál és az első padsorokban jól látható, írásos formában jelezni kell, hogy az eseményről sajtónyilvános közvetítés készül, megjelölve a kamerák látószögét, hogy a hívők eldönthessék, kívánnak-e a felvétellel érintett területen tartózkodni, vagy tiltakozási jogukkal élve elkerülik azt.

Egészségügyi adatok közzétételi tilalma

Az egészségügyi állapotára vonatkozó adatok (pl. baleset részletei, sérülések mértéke, kórházi kezelés körülményei) a GDPR 9. cikke szerinti különleges adatok.

A balesetmegelőzési vagy prevenciós cél nem írhatja felül a adatkezeléssel érintett magánéletének és személyes adatainak védelmét.

Személyes adatok gyűjtési céltól eltérő kezelése

Személyes adatok gyűjtési céluktól eltérő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljával.

A közérdekű archiválási, tudományos, történelmi kutatási célból, vagy statisztikai célból történő további adatkezelés megengedett.

V. RÉSZ: MUNKAVISZONNYAL KAPCSOLATOS ADATKEZELÉSEK

Személyügyi nyilvántartás

A társaság megnevezés alatt jelen részben a munkáltatót is érteni kell a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) szerint. A társaság az Mt-ben meghatározott alapelvek szerint kezeli az alkalmazottak adatait.

A társaság az alkalmazottak meghatározott adatait a munkavállalók adatkezelési tájékoztatójában meghatározott jogalap szerint és célból kezeli.

Az adatok pontosságának garantálása érdekében a munkavállaló a változásokat 8 napon belül írásban köteles bejelenteni az ügyvezető.

Az adatok címzettjei: a munkáltató vezetője, a munkáltatói jogkör gyakorlója, a munkaügyi feladatokat ellátó munkavállalók és az adatfeldolgozók. A tulajdonosok részére csak a vezető állású munkavállalók személyes adatai továbbíthatók.

A munkavállaló köteles a munkája során tudomására jutott üzleti, szakmai titkot megőrizni.

A betegségre, üzemi tanácsai, szakszervezeti tagságra vonatkozó adatokat a társaság csak az Mt-ben meghatározott jog vagy kötelezettség teljesítése céljából kezelheti.

A személyes adatok tárolásának maximális időtartama az öregségi nyugdíjkorhatárt követő 5 év lehet. Az adatokat irattárban, védve kell tárolni.

A társaság a munkaszerződés megkötésével egyidejűleg a 'Munkavállalók' mappában található adatkezelési tájékoztató megismertetésével tájékoztatja a munkavállalót.

A személyi iratok kizárólag személyesen vagy meghatalmazott útján vehetők át, illetve tértivevényes ajánlott küldeményként postázhatók.

A társaság foglalkoztatottjai kötelesek a feladatkörükben tudomásukra jutott személyes adatokat, titkokat megőrizni. Ennek érdekében a munkaszerződés kiegészítését aláírják.

A társaság nem jogosult az alkalmazott okmányainak másolására, amennyiben erre jogszabály nem hatalmazza fel.

A személyi anyagba csak az arra jogosultak tekinthetnek be. A betekintést a 'Betekintési napló' mappában található betekintő lapon dokumentálni kell.

VI. RÉSZ: ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK ELJÁRÁSRENDJE

A jelen rész teljes egészében magában foglalja és hatályon kívül helyezi a korábbi különálló Adatvédelmi Incidenskezelési Szabályzatot. A társaság az alábbiak szerint határozza meg az adatvédelmi incidensek bejelentésének, kivizsgálásának, orvoslásának és dokumentálásának kötelező rendjét:

Az adatvédelmi incidens fogalma és példái

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.

Példák adatvédelmi incidensre:

- Pendrive, laptop, mobiltelefon vagy egyéb adattároló eszköz elvesztése vagy ellopása;
- Személyes adatok fizikai megsemmisülése vagy nem biztonságos tárolása (pl. szemetesbe dobott, nem megsemmisített bérlapok);
- Adatok téves továbbítása (pl. személyes adatokat tartalmazó e-mail téves címzettnek történő elküldése);
- Ügyfél-, partner- vagy munkavállalói listák illetéktelen másolása vagy továbbítása;
- Szerverek elleni támadások, honlap feltörése, vagy a személyes adatokat kezelő informatikai rendszerek elérhetetlenné válása (zsarolóvírusos fertőzések);
- Személyes adatok engedély nélküli, jogellenes nyilvánosságra hozatala (pl. azonosítható módon közzétett adatok vagy fotók sajtócikkekben).

Az incidensek észlelése és belső jelzésének rendje

Aki a tevékenysége során a Társaság által végzett adatkezeléssel kapcsolatban adatvédelmi incidens gyanúját – vagyis olyan esemény bekövetkezését, amely személyes adatok sérülését, elvesztését vagy illetéktelen hozzáférését eredményezhette – észleli (ideértve azt is, ha az eseményt ő maga okozta), köteles azt haladéktalanul jelezni a társaság vezetője (ügyvezető) felé. Amennyiben az incidens gyanúja az elektronikus információs rendszerekben (EIR) vagy az azokban kezelt adatok bizalmasságában, sértetlenségében vagy rendelkezésre állásában beállt változásként jelentkezik, és személyes adatok érintettsége áll fenn, az IT Üzemeltető vagy a műszaki vezető az észleléstől számított legfeljebb 8 órán belül köteles azt jelezni az adatvédelmi tisztviselő (DPO) felé az IBSZ szerinti belső jelentéstételi rendnek megfelelően, hogy a DPO haladéktalanul megkezdhesse az adatvédelmi incidens kivizsgálását, kockázatértékelését és előkészíthesse a NAIH felé történő 72 órás bejelentést.

Az észlelő munkatárs a jelzésben köteles feltüntetni az alábbi adatokat:

- a) Az érintett adatkezelés, nyilvántartás vagy informatikai rendszer megjelölése;
- b) Az adatok kezeléséért felelős személy megjelölése;
- c) Az eseményt észlelő munkatárs neve és elérhetősége;
- d) Az észlelés pontos időpontja és körülményei (rövid leírás);
- e) Az érintett személyes adatok kategóriái és köre;
- f) Az incidens jellege (bizalmassági, sértetlenségi vagy rendelkezésre állási sérülés);
- g) Az esemény ismert vagy várható következményei, közvetlen veszélyek.

Az ügyvezető akadályoztatása esetén az észlelő a helyettesítésre kijelölt személyt tájékoztatja. Az ügyvezető szükség esetén haladéktalanul – e-mailen és telefonon – felveszi a kapcsolatot az adatvédelmi tisztviselővel az incidens tisztázása érdekében.

Amennyiben az ügyvezető az eseményt nem minősíti adatvédelmi incidensnek, úgy köteles annak indokairól részletes írásbeli feljegyzést készíteni.

Kivizsgálás és kockázatértékelés

Az incidens tudomásra jutását követően az ügyvezető és az adatvédelmi tisztviselő (vagy az erre kijelölt vizsgálócsoport) haladéktalanul megkezdí a körülmények feltárását. Meg kell határozni az incidens 'tudomásszerzési időpontját', amely az a pillanat, amikor a biztonsági esemény és a személyes adatok érintettsége bizonyossá válik.

A vizsgálat során fel kell tárni az érintett személyes adatok kategóriáit, számát, valamint a kockázattal érintett természetes személyek (érintettek) számát. Meg kell őrizni és rögzíteni kell a kivizsgálás során keletkezett bizonyítékokat.

Értékelni kell az incidens által az érintettek jogaira és szabadságaira jelentett kockázat mértékét, az alábbi kategóriák szerint:

- a) Ha az incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve, azt részletesen indokolva dokumentálni kell, kitérve a megelőző intézkedésekre. Ebben az esetben a Hatóság felé történő bejelentés mellőzhető.
- b) Ha az incidens valószínűsíthetően kockázattal jár, azt indokolással dokumentálni kell, és intézkedni kell a NAIH felé történő bejelentésről a tudomásszerzéstől számított 72 órán belül.
- c) Ha az incidens valószínűsíthetően magas kockázattal jár, a NAIH felé történő bejelentés mellett haladéktalanul gondoskodni kell az érintett természetes személyek közvetlen tájékoztatásáról is.

Intézkedések az incidensek orvoslására és dokumentálása

Az adatvédelmi tisztviselő a vizsgálat alapján írásbeli összefoglalót és javaslatot készít az ügyvezető részére az incidens kezelésére, az orvoslásra irányuló intézkedésekre, a határidőkre és a NAIH/érintettek értesítésének szükségességére.

Az ügyvezető dönt a javasolt intézkedések elfogadásáról. Ha egyetért, aláírásával jóváhagyja az összefoglalót. Ha eltérő döntést hoz, arról indokolással ellátott feljegyzést kell készíteni.

Az incidensek kezelése során az alábbi adatvédelmi elveket kell betartani:

- Minden megtett intézkedést és azok pontos időpontját dokumentálni kell;
- Ha az incidens bejelentése a 72 órás határidőn túl valósul meg, az adatvédelmi tisztviselő köteles a késedelem okairól igazolást/feljegyzést készíteni az ügyvezető részére;
- Az incidens lezárása után az érintett adatkezelések kockázatértékelését ismételtel el kell végezni, és rögzíteni kell az új biztonsági intézkedéseket.

Adatfeldolgozó igénybevétele esetén a szerződésben kötelezően rendelkezni kell az adatfeldolgozó azonnali, késedelem nélküli értesítési és együttműködési kötelezettségéről incidens esetén.

Jelentéstétel a Hatóság (NAIH) felé

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, de legkésőbb 72 órával azután, hogy az incidens a tudomására jutott, bejelenteni köteles a NAIH részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

A bejelentést a Hatóság elektronikus felületén az adatvédelmi tisztviselő teszi meg az ügyvezető jóváhagyását követően. A bejelentés visszaigazolását és kivonatát meg kell őrizni és az ügyvezető részére át kell adni. A Hatósággal az incidens során a DPO tartja a kapcsolatot.

Az érintettek tájékoztatásának rendje

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az incidensről.

A tájékoztatót az ügyvezető és a DPO közösen készíti el. A tájékoztatót külön, más anyagoktól, reklámoktól vagy egyéb iratoktól elkülönítve, önálló dokumentumként kell megküldeni az érintett részére.

A tájékoztatóban világosan és közérthetően ismertetni kell:

- az adatvédelmi incidens jellegét;
- a DPO nevét és elérhetőségeit;
- a várható, valószínűsíthető következményeket;
- az adatkezelő által az orvoslásra tett vagy tervezett intézkedéseket, a hátrányos következmények enyhítését;
- azon lépések leírását, amelyeket az érintett maga tehet meg a károk elhárítása érdekében.

Az érintettek közvetlen tájékoztatása mellőzhető, ha:

- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket alkalmazott (pl. titkosítás, mely az illetéktelenek számára olvashatatlaná tette az adatokat);
- az adatkezelő az incidenst követően olyan intézkedéseket tett, amelyek biztosítják, hogy a magas kockázat valószínűsíthetően a továbbiakban nem valósul meg;
- a közvetlen tájékoztatás aránytalan erőfeszítést tenne szükségessé (ilyenkor nyilvánosan közzétett információk útján kell tájékoztatni az érintetteket).

VII. RÉSZ: ADATVÉDELMI HATÁSVIZSGÁLAT

Adatvédelmi hatásvizsgálat és előzetes konzultáció

Új szoftver, elektronikus információs rendszer (EIR) vagy digitális szolgáltatás beszerzése, tervezése és fejlesztése során a társaság az IBSZ 12. fejezetével (Rendszer- és szolgáltatásbeszerzés) és (Fejlesztésre vonatkozó szabályok) összhangban jár el.

Ha az adatkezelés jellege, hatóköre, körülménye és céljai alapján valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, különösen, ha a NAIH

által közzétett hatásvizsgálati listában szereplő adatkezelések valósulnak meg, az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez.

A kötelezően hatásvizsgálat alá eső kiemelt esetek (a NAIH listája alapján):

- Természetes személy biometrikus adatainak módszeres megfigyelés céljából történő kezelése;
- Kiszolgáltatót helyzetben lévő érintettek (gyermekek, munkavállalók, idős vagy mentális betegségben szenvedők) biometrikus adatainak kezelése;
- Genetikai adatok összekapcsolása más különleges vagy fokozottan személyes adatokkal;
- Érintettek tulajdonságainak felmérése, pontozása, hitelképesség vagy fizetőképesség módszeres értékelése;
- Profilalkotás, különösen ha az az érintett munkahelyi teljesítményére, egészségi állapotára, személyes preferenciáira vagy mozgására vonatkozik;
- Közterületek vagy nyilvános helyek nagymértékű, módszeres megfigyelése (kamerarendszerek, drónok);
- Gyermekek személyes adatainak kezelése profilozás, automatizált döntéshozatal, marketing vagy közvetlenül nekik kínált információs társadalmi szolgáltatások nyújtása során.

Nem kell hatásvizsgálatot végezni, ha az adatkezelést jogszabály írja elő, és a jogalkotó a jogszabály-előkészítés során már elvégezte a hatásvizsgálatot.

A hatásvizsgálat szükségességének előzetes megállapításához az '1. függelékben' szereplő előzetes kockázatelemzési kérdéssort kell megválaszolni.

Ha a tervezett adatkezelés valószínűsíthetően nem jár magas kockázattal, annak tényét és indokait az ügyvezető rögzíti.

Magas kockázat azonosítása esetén az érintett szakterület vagy a megbízott személy adatvédelmi hatásvizsgálat lefolytatását kezdeményezi.

Az ügyvezető elrendeli a hatásvizsgálat lefolytatását. A vizsgálat lezárásáig az adatkezelésről szóló döntés nem hozható meg.

A hatásvizsgálat lefolytatásában az érintett szakterület vesz részt, az adatvédelmi tisztviselő és az információbiztonságért felelős személy szakmai támogatásával. Az iratok nem nyilvánosak.

A hatásvizsgálatot végző összefoglaló értékelést készít a '2. függelék' szerint, melyet az ügyvezető hagy jóvá.

A hatásvizsgálatot a NAIH honlapján elérhető hatásvizsgálati szoftver (PIA szoftver) alkalmazásával kell elvégezni.

A hatásvizsgálat megrendeléséért a társaság vezetője felelős, a DPO tanácsát ki kell kérni.

Ha a hatásvizsgálat megállapítja, hogy az adatkezelés a tervezett kockázatcsökkentő intézkedések hiányában is magas kockázattal járna, az adatkezelő köteles előzetesen konzultálni a felügyeleti hatósággal (NAIH).

Az előzetes konzultációra a GDPR 35-36. cikkei és az Infotv. rendelkezései irányadók.

VIII. RÉSZ: AZ ADATTOVÁBBÍTÁS SZABÁLYAI

Adatkezeléssel, adattovábbítással megbízott dolgozók

Az adatok kezelésére vonatkozó megbízás nem foglalja magában az adattörlés, adatmódosítás, adattovábbítás vagy közzététel jogának egyedüli gyakorlását. Ezen műveletek teljesítéséhez minden esetben az ügyvezető vagy helyettese előzetes jóváhagyása szükséges.

A munkavállalók adatainak felvételére és nyilvántartására a munkaköri leírásuk alapján az ügyvezető és a kijelölt HR/munkaügyi munkatársak jogosultak.

Az ügyfelek adatainak felvételére, nyilvántartására és továbbítására az ügyvezető és a kijelölt ügyfélkapcsolati munkatársak jogosultak.

A társaság által kezelt adatok szabályszerű megkeresés esetén továbbíthatók a hatóságok és bíróságok részére az ügyvezető jóváhagyása után.

Hatósági megkeresések

Személyes adatot érintő adatszolgáltatást kizárólag az ügyvezető előzetes jóváhagyásával lehet teljesíteni. Személyes adatot hatósági vagy bírósági megkeresésre az ügyvezető, míg a NAIH megkeresése alapján az adatvédelmi tisztviselő jogosult írásban kiadni, feltéve, hogy:

- a) a megkeresés papír alapon hivatalos postai úton, vagy elektronikusan hitelesítve a Céglapra érkezett;

- b) a megkereső szerv pontosan megjelölte az érintett személyt, a kért adatok fajtáját, a célját és a teljesítés határidejét.

Amennyiben a megkeresés nem felel meg a követelményeknek (pl. telefonon vagy nem hitelesített e-mailben érkezik), a megkeresőt fel kell hívni a szabályszerű előterjesztésre. Szükség esetén ellenőrizni kell a megkereső kilétét.

Az adatot ki kell adni, ha a hatóság szabályszerű helyszíni ellenőrzést folytat. Az ellenőrzés akkor szabályszerű, ha az ellenőrök bemutatják a megbízólevelüket és igazolják személyazonosságukat.

Kivételesen, sürgős nyomozati cselekmény esetén (pl. telefaxon érkező megkeresés) is teljesíthető a megkeresés, ha az egyéb törvényi feltételek egyértelműen fennállnak.

A megkeresés teljesítésének feltétele, hogy a kért adatokat a társaság jogszerűen kezelje, a megkereső jogosult legyen azok átvételére, az adatok rendelkezésre álljanak, és a továbbítás biztonságos csatornán valósuljon meg.

Külföldi adattovábbítás

A társaság bizonyos szolgáltatások (pl. felhőtárhely) igénybevétele során továbbíthat adatokat az Európai Gazdasági Térségen (EGT) kívüli harmadik országba. Ilyen esetben előzetesen tisztázni kell az adattovábbítás tényét.

Harmadik országba történő adattovábbításra akkor kerülhet sor, ha az Európai Bizottság megállapította, hogy a third ország megfelelő védelmi szintet biztosít (megfelelőségi határozat).

Megfelelőségi határozat hiányában a társaság csak akkor továbbíthat személyes adatot, ha a címzett megfelelő garanciákat nyújt (pl. a Bizottság által elfogadott általános adatvédelmi kikötések – SCC, jóváhagyott magatartási kódex vagy tanúsítási mechanizmus).

Megfelelő garanciák hiányában csak különleges esetekben (pl. az érintett kifejezett, kockázatokról tájékoztatott hozzájárulása, szerződés teljesítése, fontos közérdek, vagy jogi igények érvényesítése esetén) történhet adattovábbítás.

Ha a fenti jogalapok egyike sem alkalmazható, az adattovábbítás csak akkor történhet meg, ha az nem ismétlődő, korlátozott számú érintettet érint, az adatkezelő kényszerítő erejű jogos érdekében szükséges, és az adatkezelő megfelelő garanciákat nyújtott.

Ilyen rendkívüli esetekben a társaságnak tájékoztatnia kell a NAIH-ot az adattovábbításról, valamint az érintettet is tájékoztatni kell a továbbításról és a jogos érdekről.

IX. RÉSZ: AZ ÉRINTETT JOGAI ÉS JOGGYAKORLÁSÁNAK ELŐSEGÍTÉSE

A jelen rész teljes egészében magában foglalja és hatályon kívül helyezi a korábbi különálló Érintetti Joggyakorlást Elősegítő Szabályzatot. A társaság az alábbiak szerint határozza meg az érintetti jogokkal kapcsolatos kérelmek kezelésének, elbírálásának és teljesítésének részletes eljárásrendjét:

Tájékoztatás az érintett jogairól

A GDPR 21. cikk (4) bekezdése alapján az érintett tiltakozáshoz való jogára legkésőbb az első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmet, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

134. A társaság honlapján az érintettek jogairól szóló részletes tájékoztatót kell elhelyezni, amely az 'Ügyfelek' mappában is megtalálható.

Az adatkezeléssel kapcsolatos érintetti igényeket az ügyvezető részére kell előterjeszteni, aki gondoskodik azok határidőn belüli megválaszolásáról.

Minden esetben kétséget kizáróan meg kell győződni arról, hogy a jogait gyakorolni kívánó személy valóban jogosult-e az igény előterjesztésére. Az azonosítás során csak a legszükségesebb adatok kezelhetők.

A jogok gyakorlása során mások jogai és szabadságai nem sérülhetnek, ezért szükség esetén a meg nem ismerhető adatok (pl. harmadik személyek adatai, képmásai) anonimizálásáról gondoskodni kell.

A társaság az érintetti jogok megfelelő gyakorlása érdekében az adatvédelmi tisztviselőt bevonja az érintettnek adandó választervezetek előkészítésébe.

Az érintett jogait díjmentesen gyakorolhatja. Visszaélésszerű vagy ismétlődő kérelem esetén adminisztratív önköltségi díj számítható fel.

Az érintett alapvető jogai a következők:

- a) Átlátható tájékoztatás és kommunikáció;
- b) Hozzáférési jog (adatok másolatának kiadása, tájékoztatás az adatkezelésről);
- c) Helyesbítéshez és kiegészítéshez való jog;
- d) Törléshez való jog (elfeledtetéshez való jog);
- e) Az adatkezelés korlátozásához való jog;
- f) Adathordozhatósághoz való jog;
- g) Tiltakozáshoz való jog;
- h) Adatvédelmi incidensről való tájékoztatás joga;
- i) Hatósági (NAIH) és bírósági jogorvoslathoz való jog.

A kérelmek fogadásának és azonosításának eljárása

Az érintetti kérelem előterjeszthető szóban (személyesen vagy telefonon), írásban postai úton vagy elektronikusan. A kérelem érvényességének nem feltétele a jogi indokolás.

A szóban előterjesztett kérelmet az ügyintéző köteles a '2. mellékletben' meghatározott nyomtatványon rögzíteni. Személyes megjelenés esetén a kérelmezőnek fel kell mutatnia személyazonosító okmányait, és igazolnia kell az érintettel való kapcsolatát (pl. meghatalmazás, szülői minőség).

Az írásbeli vagy elektronikus kérelemben az alábbi adatokat kell megadni:

- A kérelmező és az érintett neve;
- Képviselő esetén a jogosultság igazolása;
- Az érintett személyazonosságának megerősítésére szolgáló azonosító adatok;
- Válaszadásra szolgáló elérhetőség;
- A gyakorolni kívánt jog és az igény pontos meghatározása.

Ha a kérelem nem tartalmazza a szükséges adatokat, az ügyintéző felhívja a kérelmezőt a pontosításra. A beérkezett kérelmet az átvevő köteles haladéktalanul továbbítani az ügyvezető részére.

A kérelmek vizsgálatának és pontosításának rendje

Az ügyvezető által megbízott alkalmazott megvizsgálja a kérelmet a tartalom, a jogosultság és az adatkezelés tényének szempontjából.

Amennyiben a kérelem pontatlan vagy hiányos, az ügyintéző köteles felvenni a kapcsolatot a kérelmezővel, és segítséget nyújtani az igény pontos meghatározásában. Ha a kérelmező a felhívás és figyelmeztetés ellenére sem pontosítja az értelmezhetetlen kérelmet, az adatkezelő jogosult azt visszavontnak tekinteni.

Ha megállapítást nyer, hogy a kért adatok nincsenek a társaság kezelésében, az érintettet az igény teljesíthetetlenségéről értesíteni kell.

Egyes érintetti jogok teljesítésének és intézésének eljárásrendje

Hozzáféréshez való jog

A hozzáféréshez való jog gyakorlása során az érintett jogosult tájékoztatást kapni az adatkezelés körülményeiről és másolatot kérni a kezelt személyes adatokról. Ennek teljesítése során kiemelten ügyelni kell arra, hogy más személyek adatai ne váljanak megismerhetővé; a dokumentumokat, képeket vagy hangfelvételeket anonimizálni kell.

- A tájékoztatás megvalósulhat ügyféltörzs alkalmazása esetén akár az érintettre vonatkozó adatok megnyitását követően a képernyőkép kinyomtatásával (PrintScreen) és átadásával is.

Helyesbítéshez és kiegészítéshez való jog

A pontatlan adatok helyesbítése vagy hiányos adatok kiegészítése előtt meggyőződni kell az újonnan megadott adatok helyességéről (pl. telefonos vagy e-mailes egyeztetéssel). Természetes személyazonosító adatok vagy okmányazonosítók helyesbítése esetén az okmány bemutatása és dokumentálása kötelező.

- A helyesbítést a társaság minden olyan rendszerében és adatbázisában el kell végezni, ahol az adatot tárolják. Kép-, hang- vagy egészségügyi adatok helyesbítésére természetüknél fogva főszabály szerint nincs lehetőség. Ha a helyesbítési kérelemről nem lehet 24 órán belül dönteni, intézkedni kell az adatok korlátozása (zárolása) iránt.

A törléshez való jog (elfeledtetéshez való jog) különös eljárásrendje

Az online médiatartalom-szolgáltatás speciális jellegére tekintettel a társaság az alábbi szigorú eljárásrendet alkalmazza a törlési kérelmek kezelése során, összhangban a NAIH 2025. évi átfogó jelentésének és a hatósági határozatok követelményeivel:

1. Egyedi mérlegelés és kivételek:

- A törlési kérelmeket minden esetben egyedileg és érdemben kell kivizsgálni. A sajtótevékenység során az adatkezelés jogalapja leggyakrabban a jogos érdek (GDPR 6. cikk (1) f) pont) és a lakosság tájékoztatásához fűződő kötelezettség (Smtv. 10. §).
- A GDPR 17. cikk (3) bekezdése alapján a törlési kötelezettség nem alkalmazandó, ha az adatkezelés a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása miatt szükséges. Közszereplők, közéleti vagy bűnügyi eseményekről szóló tudósítások, valamint történelmi/társadalmi jelentőségű események esetén a közérdek megelőzheti az érintett törlési igényét, ha az adatkezelő előzetes, írásban rögzített érdekmérlegelési tesztel (LIA) igazolja a jogos érdek fennállását.

2. Kivétel nélküli törlési kötelezettség jogellenesség esetén:

- Amennyiben a személyes adatok közzétételének jogellenességét a Hatóság (NAIH) vagy a bíróság (sajtóhelyreigazítási vagy egyéb perben) megállapította, a GDPR 17. cikk (1) bekezdés d) pontja alapján a személyes adatok törlésére az adatkezelő kötelezően köteles. Ezen esetekben a törlési kötelezettség alól nincs kivétel, és a sajtószabadságra vagy tájékoztatásra való hivatkozással a törlés nem tagadható meg.

3. A törlés teljes körűsége és véglegessége:

- A törlésnek véglegesnek és visszaállíthatatlannak kell lennie (fizikai vagy végleges logikai törlés, nem pedig egyszerű anonimizálás, mely utóbbi csak kivételes, történelmi/sajtóarchívumi okokból alkalmazható).

- Az érintett kérésére vagy jogellenesség esetén a törlést el kell végezni nemcsak a nyilvános honlapról (a cikkből), hanem a kiadó valamennyi éles adatbázisából, belső nyilvántartásából, adattárolási eszközéről és a biztonsági mentésekből is. Meg kell győződni arról, hogy a törlés a nyilvános tartalomból valóban megtörtént, és intézkedéseket kell tenni a keresőmotorok találati listájából való eltávolításra (deindexelés) is.

4. Másodközlés és szemlézés (szemléző felelősség):

- A társaság önálló adatkezelői felelősséggel tartozik a más sajtószervek által megjelentetett cikkek személyes adatainak átvételével, másodközlésével (szemlézésével) összefüggő adatkezelésért. Az elszámoltathatóság, a jogalap igazolása és az érintetti jogok biztosítása (így a törlési kötelezettség) a társaságot is önállóan terheli, amennyiben az átvett adatok kezelése jogellenes vagy a kérelem megalapozott.

5. Átmeneti intézkedések:

- Ha a jogi helyzet még nem tisztázott (pl. folyamatban lévő peres eljárás van), a végleges törlés helyett átmeneti intézkedésként az adatok kezelését korlátozni (zárolni) kell, és erről az érintettet írásban tájékoztatni kell.

6. Kommunikáció az érintettel:

- A törlési kérelem beérkezésekor haladéktalanul írásos (e-mailes) visszaigazolást kell küldeni az érintettnek a kérelem befogadásáról, az eljárás menetéről, a válaszadás várható határidejéről (mely maximum 1 hónap) és a jogorvoslatról.

- Ha a kérelem elutasításra kerül, az elutasítás okairól és a jogorvoslatról a kérelmezőt legkésőbb

1 hónapon belül írásban tájékoztatni kell. A kérelem elutasításáról szóló értesítés elmaradása (mint a NAIH-359-10/2026 sz. határozatban megállapítottan) súlyos, bírsággalható jogsértésnek minősül.

Az adatkezelés korlátozásához való jog

Korlátozás esetén az adatkezelő főszabály szerint csak tárolhatja az adatokat. Intézkedni kell az adatokhoz való hozzáférés megszüntetéséről és a honlapról való ideiglenes eltávolításról.
- Ha az adatkezelés jogellenessége merül fel, vagy a törlési/helyesbítési kérelem 24 órán belül nem bírálható el, az adatok korlátozása (zárolása) iránt kötelező intézkedni.

Adathordozhatósághoz való jog

Csak hozzájáruláson vagy szerződésen alapuló adatkezelés esetén gyakorolható, és kizárólag az érintett által rendelkezésre bocsátott adatokra terjed ki (származtatott adatokra nem). Az adatokat .csv vagy .xml fájlformátumban kell átadni.

Tiltakozáshoz való jog

Jogos érdeken alapuló adatkezelés esetén az érintett tiltakozhat a személyes adatok kezelése ellen. Ilyenkor a társaságnak az érdekmérlegelési tesztet az érintett egyedi helyzetére szabva azonnal felül kell vizsgálnia, és az adatkezelést meg kell szüntetnie, kivéve, ha bizonyítja, hogy kényszerítő erejű jogos okok állnak fenn, amelyek elsőbbséget élveznek.

A kérelmek teljesítésével és elutasításával kapcsolatos eljárási szabályok

Az érintett részére a kért adatokról, dokumentumokról vagy kép-/hangfelvételekről készített másolatot első alkalommal ingyenesen kell biztosítani.

Ha a kérelem egyértelműen megalapozatlan vagy ismétlődő jellege miatt túlzó, az adatkezelő ésszerű, az adminisztratív költségeken alapuló díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést. A bizonyítási kötelezettség az adatkezelőt terheli.

A kérelem elbírálásáról az érintettet a kérelem beérkezésétől számított legfeljebb 1 hónapon belül írásban vagy az érintett által igénybe vett elektronikus úton értesíteni kell, a '4. melléklet' szerinti választervezet alapulvételével.

Ha az érintett személyesen veszi át a döntést, az ügyvezető által megbízott személy átadja a tájékoztató levelet, és az érintett aláírásával elismeri az átvételt. Aláírás hiányában a döntés tanulmányozása nem kezdhető meg.

A megtett intézkedések személyes ellenőrzése során az ügyintéző köteles végig jelen lenni, válaszolni a kérdésekre és ügyelni az adatok biztonságára.

Az érintett jogosult az iratokról jegyzeteket készíteni vagy másolatot kérni. Postai teljesítés esetén a döntést és a másolatokat ajánlott, tértivevényes küldeményként kell megküldeni.

Az eljárás lezárását követő intézkedések

A kérelem teljesítését, elutasítását vagy visszavonását követően az ügyintézés befejeződik.

A kérelem teljesítése után a kérelmező (mint joggyakorló) kizárólag ezen eljárás céljából rögzített személyes adatai haladéktalanul törlésre kerülnek.

Ha a kérelem alapján adatmódosításra, törlésre vagy korlátozásra került sor, erről haladéktalanul értesíteni kell mindazon címzetteket (pl. adatfeldolgozók, partnerek), akikkel a személyes adatot korábban közölték, kivéve, ha ez lehetetlen vagy aránytalan erőfeszítést igényel.

157. Az érintetti kérelmek kezelése során szerzett tapasztalatokat és az esetleges hiányosságokat be kell építeni a jövőbeli adatvédelmi hatásvizsgálatokba és kockázatértékelésekbe a folyamatok folyamatos fejlesztése érdekében.

X. RÉSZ: ZÁRÓ RENDELKEZÉSEK

A Szabályzat megállapítása, módosítása és felülvizsgálata

A Szabályzat megállapítására és módosítására a társaság vezetője (ügyvezetője) jogosult.

Jelen szabályzatot a társaságnál helyben szokásos módon (vezetői értekezleten és belső hálózaton történő közzététellel) ismertetni kell a munkavállalókkal. A szabályzat az alkalmazottakkal történő közléssel válik hatályossá.

A társaság vezetője gondoskodik arról, hogy a Szabályzat előírásai a mindennapi folyamatokban érvényre jussanak. A szabályok betartása minden munkavállaló lényeges munkaköri kötelezettsége. Ennek érdekében a munkaszerződések mellékletét képező titoktartási és adatvédelmi nyilatkozatokat ('Munkaszerződés kiegészítés') minden munkavállaló köteles aláírni.

A szabályok súlyos megszegése esetén a társaság fegyelmi eljárást kezdeményez, vagy indokolt esetben büntető feljelentést tesz.

Az új munkatársakat a belépést követő 1 héten belül (online teszt formájában), a személyes adatokat kezelő meglévő állományt pedig évente legalább egyszer adatvédelmi oktatásban kell részesíteni, amelyet a DPO tart.

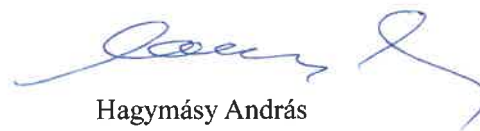
Korábbi különálló szabályzatok hatályon kívül helyezése és záró rendelkezések

Jelen egységes Szabályzat hatálybalépésével egyidejűleg a Fehérvár Médiacentrum Kft. korábbi különálló, 2024. augusztus 31-én kelt 'Érintetti Joggyakorlást Elősegítő Szabályzata', a 2026. július 7-én kelt 'Adatvédelmi Incidenskezelés Szabályzata', hatályát veszti és hatályon kívül

helyeztetik. Ezen szabályzatok rendelkezései átdolgozott, kiegészített és integrált formában a jelen egységesített Szabályzat szerves részét képezik.

Jelen szabályzat és annak mellékletei dr. Kozma-Egeresi Gabriella egyéni vállalkozó szellemi terméke, aki minden jogot fenntart.

Székesfehérvár, 2026.08.26.



Hagymásy András
Ügyvezető



