Adatvédelmi és Adatbiztonsági Szabályzat

Hatályos: 2025. szeptember 11.

Tartalom

1. Általános rendelkezések

1.1 A **Magyar Kultúráért Alapítvány** /rövidített neve: MKA; székhelye: 1053 Budapest, Károlyi utca 16.; adószáma: 19311621-2-41; nyilvántartási száma: 01-01-0013184, a továbbiakban: Adatkezelő) mint adatkezelő az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján az adatkezelés rendjére az alábbi Adatvédelmi és Adatbiztonsági Szabályzatot (a továbbiakban: Szabályzat) alkotja.

1.2 Jelen Szabályzat célja, hogy meghatározza az Adatkezelő által a személyes adatok kezelése és feldolgozása törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, továbbá meghatározza azokat az információkat, adatokat, amelyeket az Adatkezelő a természetes személyekre vonatkozóan kezelhet, illetve hogy azokat milyen célokra használhatja fel. A jelen Szabályzat célja továbbá az Adatkezelő tevékenységével összefüggésben a személyes adatok kezelésével kapcsolatos belső működés meghatározása.

A Szabályzatban foglaltak értelmezése, alkalmazása és végrehajtása során minden esetben irányadó a vonatkozó szabályozási környezet, így különösen:

- az Európai Parlamentnek és a Tanácsnak a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló 2016/679 (2016. április 27.) számú rendelete;
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;

A mindenkor hatályos jogszabályok tartalma a személyes adatokkal kapcsolatos valamennyi tevékenységre vonatkozóan irányadó.

1.3 <u>Az adatkezelő megjelölése</u>

1.3.1. Az adatkezelő neve: **Magyar Kultúráért Alapítvány**
1.3.2. Az adatkezelő székhelye: 1053 Budapest, Károlyi utca 16.

1.4 Amennyiben egy adatról nem eldönthető annak személyes adat jellege, vagy különleges személyes adat jellege, úgy az azzal kapcsolatos belső döntésig azt úgy kell tekinteni mintha ezen minősége/jellege fennállna. Az adat személyes adatként vagy különleges személyes adatként való minősítéséről az Adatkezelő vezető tisztségviselője dönt.

1.5 A személyes adatok kezelése során a jogszabályok, valamint a jelen Szabályzat maradéktalan betartása mellett úgy kell eljárni, hogy a tevékenység:

a) személyes adatok kezelését csak az adott cél elérésére nézve feltétlenül indokolt mértékben és ideig eredményezze;
b) a személyes adatok biztonságát, az érintett természetes személyek jogait és szabadságait ne veszélyeztesse;
c) kockázatainak számbavétele során az adatvédelem kiemelt prioritást kapjon, az azokkal kapcsolatos hatások vizsgálata során pedig mindenkor a lehető legnagyobb potenciális hatásokat kell figyelembe venni és kerülni kell a kockázatok alulértékelését.

1.6 Jelen Szabályzat hatálya kiterjed az Adatkezelő valamennyi munkavállalójára, valamint tevékenységében részt vevő minden személyre – így különösen az alvállalkozókra és szerződéses partnerekre is.

1.7 Az Adatkezelő valamennyi releváns szerződés esetében köteles gondoskodni arról, hogy az Adatkezelővel szerződést kötő fél a jelen Szabályzatban, valamint a mindenkor hatályos vonatkozó adatkezelési tájékoztatóban foglaltakat megismerhesse.

2. Értelmező rendelkezések

- **Személyes adat:** azonosított vagy azonosítható természetes személyre (a továbbiakban: érintett) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Személyes adatnak minősül pl. a név, a telefonszám, a bankszámlaszám, a lakóhelyre vonatkozó adat, az e-mail cím, az IP-cím 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;

- **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;

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

- **Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

- **Munkavállaló:** munkavégzésre irányuló munkajogi vagy polgári jogi jogviszonyban álló személy;

- **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;

- **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik;

- **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

- **Adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

- **Kiskorú:** az a természetes személy, aki tizennyolcadik életévét nem töltötte be;

- **Cselekvőképtelen kiskorú:** az a kiskorú, aki a tizennegyedik életévét nem töltötte be;

- **Korlátozottan cselekvőképes kiskorú:** az a kiskorú, aki a tizennegyedik életévét betöltötte és nem cselekvőképtelen.

- **Nagy mennyiségű személyes adat:** az érintettek nagy száma, a kezelt adatok mennyisége vagy adatfajták köre, az adatkezelés időtartama, földrajzi kiterjedése alapján meghatározott adatmennyiség, de legalább 50 db személyes adat

3. Adatvédelmi alapelvek

3.1. Jogszerűség, tisztességes eljárás és átláthatóság elve: az Adatkezelő a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon köteles kezelni.

3.2. Célhoz kötöttség elve: az Adatkezelő személyes adatokat csak meghatározott, egyértelmű és jogszerű célból gyűjtheti, és azokat nem kezelheti a célokkal össze nem egyeztethető módon.

3.3. Adattakarékosság elve: az Adatkezelő által kezelt személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsak kell lenniük, és a szükségesre kell korlátozódniuk.

3.4. Pontosság elve: az Adatkezelő által kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; az Adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törölje vagy helyesbítse.

3.5. Korlátozott tárolhatóság elve: az Adatkezelő által kezelt 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 a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, a GDPR rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

3.6. Integritás és bizalmas jelleg elve: az Adatkezelő által kezelt 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.

3.7. Adatbiztonság elve: Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az adatkezelésre vonatkozó jogszabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az Adatkezelő köteles gondoskodni az általa adatkezelői, illetve adatfeldolgozói minőségben kezelt személyes adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket, illetve kialakítani azon eljárási szabályokat, amelyek az adatvédelmi jogszabályok és a jelen Szabályzat érvényre juttatásához szükségesek.

3.8. Átláthatóság elve: a nyilvánosságnak vagy az érintettnek nyújtott tájékoztatásnak tömörnek, könnyen hozzáférhetőnek és könnyen érthetőnek kell lennie, valamint azt világosan és közérthető nyelven kell megfogalmazni, illetve – ezen túlmenően – szükség esetén vizuálisan is megjeleníteni; a személyes adatok kezelésével összefüggő tájékoztatásnak, illetve kommunikációnak könnyen hozzáférhetőnek és közérthetőnek kell lennie, valamint azt világosan és egyszerű nyelvezettel kell megfogalmazni. Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról. A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

3.9. Tisztességes és átlátható adatkezelés elve: megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól. Az adatkezelő olyan további információt is az érintett rendelkezésére bocsát, amelyek a tisztességes és átlátható adatkezelés biztosításához szükségesek, figyelembe véve a személyes adatok kezelésének konkrét körülményeit és kontextusát. Az érintettet továbbá a profilalkotás tényéről és annak következményeiről tájékoztatni kell. Ha a személyes adatokat az érintettől gyűjtik, az érintettet arról is tájékoztatni kell, hogy köteles-e a személyes adatokat közölni, valamint, hogy az adatszolgáltatás elmaradása milyen következményekkel jár.

3.10. Dokumentálás elve: az Adatkezelő által kezelt, személyes adatokat is tartalmazó adathordozókkal kapcsolatosan végrehajtott minden tevékenységet dokumentálni kell annak érdekében, hogy a személyes adatok útja és azok fellelhetőségének helye pontosan megállapítható legyen.

3.11. A felelősség elve: A személyes adatok kezelésében közreműködő munkavállalók kötelesek a személyes adatok védelmére vonatkozó jogszabályok és a jelen Szabályzat rendelkezéseit megismerni és maradéktalanul betartani. Az adatvédelmi szabályok megsértői – a vonatkozó jogszabályok rendelkezéseinek megfelelően – munkajogi, szabálysértési, polgári jogi és büntetőjogi felelősséggel tartoznak.

4. Az érintettek jogai és érvényesítésük

4.1. Az adatvédelemre vonatkozó jogszabályok alapján az érintett jogosult arra, hogy:

a) kérelmezze a személyes adataihoz való hozzáférést,
b) kérje a személyes adatainak helyesbítését,
c) kérje a személyes adatainak törlését,
d) kérje a személyes adatok kezelésének korlátozását,
e) tiltakozzon személyes adatainak kezelése ellen,
f) kérje az adathordozhatóságot,
g) tiltakozzon a személyes adatainak kezelése ellen (ideértve a profilalkotás elleni tiltakozást; illetve az automatizált döntéshozatallal kapcsolatos egyéb jogokat),

16

h) visszavonja a hozzájárulását, illetve panaszt nyújtson be az illetékes felügyeleti hatósághoz.

4.2. Hozzáférési jog:
Az érintett jogosult arra, hogy visszajelzést kapjon az Adatkezelőtől arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, kérelmezze a személyes adataihoz való hozzáférést.

Az érintett jogosult arra, hogy másolatot kérjen az adatkezelés tárgyát képező személyes adatairól. Azonosítás céljából további információkat kérhet az Adatkezelő az érintettől, és – az első másolat kiadását kivéve – ügyintézési költség címén indokolt díjat számíthat fel a további másolatokért.

4.3. A helyesbítéshez való jog:
Az érintett jogosult kérni az Adatkezelőtől, hogy a rá vonatkozó pontatlan személyes adatokat helyesbítse. Az adatkezelés céljától függően az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

4.4. A törléshez való jog („az elfeledtetéshez való jog"):
Az érintett jogosult arra, hogy kérje az Adatkezelőtől a személyes adatainak törlését, az Adatkezelő pedig köteles törölni ezeket a személyes adatokat, amennyiben az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat az Adatkezelő gyűjtötte vagy más módon kezelte;
b) az érintett visszavonja a GDPR 6. cikk (1) bekezdésének a) pontja vagy a GDPR 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a GDPR 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
d) a személyes adatokat az Adatkezelő jogellenesen kezelte;
e) a személyes adatokat az Adatkezelő, mint adatkezelőre alkalmazandó uniós vagy magyar jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) személyes adatok gyűjtésére a GDPR 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

4.5. Az adatkezelés korlátozásához való jog:
Az érintett jogosult arra, hogy kérje a személyes adatai kezelésének korlátozását. Ebben az esetben az Adatkezelő megjelöli az érintett személyes adatokat, amelyeket 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.

4.6. A tiltakozáshoz való jog:
Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon az Adatkezelőnél személyes adatainak a GDPR 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is, illetve kérheti az Adatkezelőtől, hogy a továbbiakban ne kezelje személyes adatait.

4.7. Az adathordozhatósághoz való jog:
Az érintett jogosult arra, hogy a rendelkezésre bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban (vagyis digitális formátumban) megkapja az Adatkezelőtől, továbbá jogosult arra, hogy – amennyiben a továbbítás technikailag megoldható – kérje ezeknek az adatoknak a továbbítását egy másik adatkezelő részére anélkül, hogy ezt az Adatkezelő akadályozná.

4.8. A hozzájárulás visszavonásához való jog:

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Ha az érintett visszavonja a személyes adatainak kezelésére vonatkozóan az Adatkezelőnek adott hozzájárulását, akkor lehet, hogy egyáltalán nem vagy csak részben tudja az Adatkezelő biztosítani a kért szolgáltatásokat.

5. A személyes adatok kezelhetőségére vonatkozó feltételek

5.1. Személyes adatok kizárólag az alábbi feltételek együttes teljesülése esetén kezelhetők:

a) az **adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének valamely pontját teljesíti**, így:
   aa) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
   ab) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
   ac) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
   ad) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
   ae) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
   af) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.
b) az **adatkezelésre vonatkozóan amennyiben szükséges, úgy adatvédelmi kockázatelemzés, valamint amennyiben szükséges, úgy hatásvizsgálat elkészült** – illetve amennyiben az adatvédelmi hatásvizsgálat alapján az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában is valószínűsíthetően magas kockázattal jár, úgy a felügyeleti hatósággal (Nemzeti Adatvédelmi és Információszabadság Hatósággal, a továbbiakban: NAIH) történt konzultáció megtörtént, és az adtakezelést a NAIH nem tiltotta meg, illetve az általa előírt feltételeket az Adatkezelő teljesítette;

5.2. Különleges adatokat kizárólag abban az esetben lehet kezelni, ammenyiben teljesülnek az 5.1. pontban írt feltételek, valamint az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének valamely pontját, valamint a GDPR 9. cikk (2) bekezdésének valamely pontját is teljesíti.

5.3. Amennyiben az adatkezelés jogalapja 6. cikk (1) bekezdésének a) pontja, úgy – az 5.4. pontban foglalt eset kivételével – cselekvőképtelen kiskorú érintett esetén az adatokat kizárólag a törvényes képviselő adhatja meg az Adatkezelőnek, korlátozottan cselekvőképes kiskorú esetén az Adatkezelőnek be kell szereznie a törvényes képviselő hozzájárulását.

5.4. Ha a 6. cikk (1) bekezdésének a) pontja alkalmazandó, a közvetlenül kiskorúnak kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a kiskorú a 16. életévét betöltötte. A 16. életévét be nem töltött kiskorú esetén, a 16. életévét be nem töltött kiskorú érintett személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a 16. életévét be nem töltött kiskorú törvényes képviselője adta meg, illetve engedélyezte.

5.5. Minden olyan adatkezelés esetén, amelyben az adatkezelés célját és eszközeit nem kizárólag az Adatkezelő határozza meg, úgy az adatkezelés további feltétele, hogy az Adatkezelő a többi

adatkezelővel a GDPR 26. cikke szerinti megállapodást is megkösse, amelyekre az Adatkezelő nevében az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja jogosult.

5.6. Az Adatkezelő jelenlegi adatkezeléseit a jelen Szabályzat 1. sz. melléklete tartalmazza.

5.7. Az adatkezelésért felelős munkavállaló feladata különösen:

a) az adatvédelmi hatásvizsgálathoz szükséges kockázatelemzés, valamint a hatásvizsgálat elkészítése a vonatkozó módszertan alapján,
b) a kockázatelemzés, valamint hatásvizsgálat során javaslattétel
   - az adathoz való hozzáférés (pl. személyi, időbeli) korlátaira,
   - az adattovábbítás szabályaira (kinek, milyen célból, milyen feltételekkel);
   - az adatkezeléssel összefüggésben végrehajtandó egyéb technikai és szervezési intézkedésekre (pl. az adatot tartalmazó file-ok vagy dokumentumok őrzési helyének, az adat tárolására szolgáló eszközök használatával kapcsolatos jelszókezelési szabályoknak, vagy a felhasználásnak az Adatkezelő székhelyére való korlátozása).
c) az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja döntéséhez az adatkezelés szükségességére, céljára és időtartamára vonatkozó javaslatot előkészíti;
d) elvégzi az adatkezelés rendszeres felülvizsgálatát;
e) gondoskodik az adatkezelés jogszerűségét alátámasztó körülmények dokumentálásáról (így különösen hozzájárulás, érdekmérlegelés dokumentálása)
f) amennyiben az adatkezelésbe szervezeten kívüli személy bevonása válik szükségessé, úgy ezt jelzi az igazgatóság elnökének, vagy az igazgatóság önálló aláírási jogosultságú tagjának;
g) az érintetteket tájékoztatja az adatkezelésről.

A fenti a) és b) pontok kapcsán tett javaslatokról az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja a kockázatelemzési, illetve hatásvizsgálati lapok jóváhagyásával dönt.

5.8. Amennyiben az 5.7. pontban meghatározott feladatok elvégzése több adatkezelésért felelős munkavállalót érint, úgy az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja kijelölheti a feladatok elvégzéséért felelős adatkezeléséért felelős munkavállalót, illetve meghatározhatja az adatkezelésért felelős munkavállalók által elvégzendő feladatokat. Kijelölés, illetve a feladatok megosztásának hiányában az adatkezelésért felelős munkavállalók együttesen felelősek a hatáskörükbe tartozó feladatok ellátása iránt intézkedni.

5.9. Az adatkezelés céljaként csak olyan ok vagy körülmény jelölhető meg, amely a jogszabályi elvárásokat kielégíti, az Adatkezelő tevékenységével közvetlenül összefügg, ahhoz szükséges vagy arra nézve egyébként célszerű.

5.10. A kezelt adatok köre a minimálisan szükséges, ugyanakkor az Adatkezelő tevékenysége biztonságos és felelős ellátására nézve indokolt mértékben határozandó meg.

5.11. Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

5.12. Az adatvédelmi hatásvizsgálathoz szükséges kockázatelemzést, valamint – amennyiben az indokolt (azaz, ha a kockázatelemzés alapján az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve) – az adatvédelmi hatásvizsgálatot az adatkezelésért felelős munkavállaló köteles az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja által megjelölt határidőig elvégezni.

5.13. Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően továbbra is magas kockázattal jár az érintettekre nézve, a személyes adatok kezelését megelőzően az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja köteles konzultációt kezdeményezni a NAIH-al. A konzultációba az adatkezelésért felelős munkavállalót be kell vonni, aki annak, valamint a konzultáció megállapításai alapján végrehajtott intézkedések eredményei alapján a kockázatelemzést, valamint az adatvédelmi hatásvizsgálatot felülvizsgálja.

5.14. A kockázatelemzési, illetve hatásvizsgálati lapokat az elkészítő munkavállaló az adatvédelmi tisztviselő jóváhagyását követően elektronikus formában köteles elmenteni és azzal egyidejűleg megküldeni az igazgatóság elnökének, vagy az igazgatóság önálló aláírási jogosultságú tagjának elektronikus úton. A kockázatelemzés, valamint hatásvizsgálat információihoz csak az azt készítő munkavállaló (vagy a munkakörét átvett személy) illetve az igazgatóság tagjai, valamint az adatvédelmi tisztviselő számára biztosítható hozzáférés.

6. A személyes adatok kezelésének gyakorlati szabályai

6.1. Személyes adatok kizárólag az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja által meghatározott belső szabályok és jogszabályi előírások maradéktalan betartása mellett kezelhetők. Az igazgatóság számára haladéktalanul jelzendő továbbá minden olyan tevékenység vagy jelenség, amely arra utal, hogy az Adatkezelővel szerződéses viszonyban álló személy az adatkezeléssel összefüggő jogszabályi előírásokat nem tartja meg. Ilyen esetben a szerződés teljesítését az adatkezelés jogszerűségének helyreállításáig fel kell függeszteni olyan módon, hogy a munkavállalókat, partnereket, valamint általában az adatkezelés érintettjeit kár ne érje, vagy az Adatkezelő által nyújtott szolgáltatások szintjének csökkenése a legkevésbé legyen számukra érzékelhető.

6.2. Az érintettel kapcsolatot tartó munkavállaló köteles meggyőződni róla, hogy
- a személyes adatokat az érintett maga adja meg, valamint járul hozzá az adatkezeléshez;
- az Adatkezelő valamely szerződéses partnere adja meg azokat, amely esetben a vonatkozó szerződés alapján az adatkezelés jogszerűségét az Adatkezelő, valamint a partner közötti szerződés biztosítja (amelyben az Adatkezelő és a partner közös adatkezelőként jelennek meg);
- olyan szerződés megkötésével összefüggésben kerül sor az adatkezelésre, ahol az érintett természetes személy az egyik fél.

6.3. Az Adatkezelő valamennyi munkavállalója köteles a személyes adatok kezelése vonatkozásában az alábbi gyakorlati szabályokat megtartani:

a) a munkavégzés során csak az ahhoz elengedhetetlenül szükséges személyes adatok kezelhetők, továbbíthatók, az adott feladatot ellátó szervezeti egység vezetőjének felelőssége a munkafolyamatok ennek megfelelő kialakítása (szükségtelen adathalmozás elkerülése);

b) az informatikai jogosultságok engedélyezésekor figyelemmel kell lenni arra, hogy személyes adathoz csak az a személy és csak annyi ideig férhessen hozzá, akinek a munkavégzéséhez az az adat, adatkör elengedhetetlenül szükséges;

c) személyes adatot tartalmazó papír alapú dokumentum csak zárt borítékban, vagy dokumentum-továbbításra alkalmas, zárt eszközben továbbítható;

d) e-mailben nagy mennyiségű személyes adatot tartalmazó, különleges adatokat tartalmazó, vagy kiskorúak személyes adatát tartalmazó dokumentum nem továbbítható. Amennyiben a munkavállalónak ilyen adatokat tartalmazó dokumentumot, iratot stb. kell más személynek elektronikus úton megküldenie, úgy a küldő személy köteles az Adatkezelő saját (file)szerverére, vagy más, megfelelő biztonságú tárhelyre feltölteni, és a dokumentum elérési módját (linkjét) megküldeni, és emellett intézkedni az adott dokumentum elérését lehetővé tévő külön jogosultság biztosításáról a személyes vagy különleges adat megismerésére jogosult személynek;

e) a szervezeti egységek által használt közös meghajtókon személyes adatot tartalmazó dokumentum csak akkor tárolható, ha biztosított, hogy azt csak az arra jogosultak tekintik meg, a közös meghajtók esetében a meghajtóért felelős szervezeti egység vezetője a felelős a jelen pontban írt kötelezettség tekintetében.

6.4. Ha a személyes adatok nem az érintettől kerültek megszerzésre, az adott érintett számára az adatvédelmi tisztviselő elkészíti a GDPR 14. cikke szerinti tájékoztatást az érintett felé, amelyben feltünteti:

a) az Adatkezelőt és annak elérhetőségeit,
b) az adatvédelmi tisztviselő elérhetőségeit,
c) a személyes adatok tervezett kezelésének célját, valamint az adatkezelés jogalapját,
d) a kezelt személyes adatok kategóriáit,
e) a személyes adatok címzettjeit (pl. hogy az adatok milyen típusú cégeknek, partnereknek kerülnek továbbításra),
f) adott esetben annak ténye, hogy az Adatkezelő valamely harmadik országba kívánja továbbítani a személyes adatokat, továbbá, hogy az adattovábbításra milyen garanciák alapján kerül sor (6.17-6.20-es pontok),
g) a személyes adatok tárolásának időtartamát,
h) az érintett azon jogát, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogát,
i) az érintett azon jogát, hogy az adatkezeléssel összefüggő hozzájárulását bármely időpontban visszavonhatja, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
j) a valamely felügyeleti hatósághoz címzett panasz benyújtásának jogát,
k) a személyes adatok forrását (azaz azt, hogy hogyan kapta meg az Adatkezelő a vonatkozó adatokat).

6.5. Az adatvédelmi tisztviselő:

a) részt vesz az Adatkezelő által alkalmazott módszertanok szerinti értékelésekben (incidens, kockázatelemzés, hatásvizsgálat), valamint szakmai tanácsokkal segíti a módszertanok elkészítését, valamint figyelemmel kíséri azok dokumentálását és az azokhoz kapcsolódó kötelezettségek teljesítését;
b) tájékoztatást és szakmai tanácsot ad az igazgatóság és más munkavállalók részére a GDPR, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
c) részt vesz és koordinálja az adatkezelési műveletekben érintett munkavállalók tudatosság-növelését és képzését;
d) részt vesz és felügyeli az információbiztonsági, adatbiztonsági ellenőrzéseket és a kapcsolódó auditokat;
e) együttműködik az adatvédelmi felügyeleti hatósággal;
f) feladatai ellátása során figyelembe veszi az adatkezelési műveletekhez fűződő kockázatokat, továbbá az adatkezelés jellegét, hatókörét, körülményeit és célját;
g) kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az Adatkezelőt;
h) részt vesz az adatvédelmi incidensek kezelési eljárásrend továbbfejlesztésében és működtetésében;
i) kapcsolatot tart a külső hatóságokkal, szervezetekkel adatvédelmet érintő kérdésekben, megadja részükre a szükséges felvilágosítást, külső vizsgálatok esetén együttműködik a vizsgálatot lefolytató hatóságokkal, szervezetekkel
j) vezeti az adatvédelmi incidens nyilvántartást.

IK

6.6. Amennyiben az adatkezelési szabályok megsértését észleli, azt valamennyi munkavállaló köteles haladéktalanul jelezni az igazgatóság vagy az adatvédelmi tisztviselő részére. A jelzések alapján az igazgatóság a kérdéses adatkezelési gyakorlatokat kivizsgálja vagy kivizsgáltatja, majd annak eredményei alapján megteszi a szükséges intézkedéseket a biztonságos, az érintettek jogait és szabadságait biztosító adatkezelés megteremtése érdekében.

6.7. Az Adatkezelő 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 hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve többek között, adott esetben:

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

6.8. Az érintettnek a személyes adatai kezelésére vonatkozó kéréseit (így különösen a GDPR III. fejezetének 3. szakasza szerint megfogalmazott nyilatkozatait az adatok helyesbítésére, törlésére, a kezelt adatok körére vonatkozó információkérésre vonatkozóan) az Adatkezelő adatvédelmi tisztviselője kezeli, amelynek keretében – a kérelem hozzá érkezésétől számított – legfeljebb 5 munkanapon belül köteles

a) amennyiben a kérés nem teljesíthető, úgy azt indokolással együtt az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja válaszaként kiküldhető levéltervezetként előkészíteni;
b) a nyilatkozatban foglaltakat – az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja értesítése mellett – az adatkezelésért felelős munkavállalóval közösen végrehajtani és az érintettet, továbbá szükség esetén minden olyan címzettet értesíteni, amellyel a megváltozott személyes adatot közölték.

6.8.1. Az érintett kérelmének teljesítéséről vagy annak elmaradásáról (az elmaradás okainak megjelölésével, valamint a NAIH-hoz vagy bírósághoz fordulás jogáról szóló tájékoztatással együtt) az érintettet legkésőbb a kérelemnek az Adatkezelőhöz érkezésétől számított 1 hónapon belül írásban kell értesíteni. Ez a határidő különösen indokolt esetben (figyelemmel a kérelmek számára, illetve összetettségére) további 2 hónappal meghosszabbítható; erről az érintettet legkésőbb az említett 1 hónapos határidőben tájékoztatni kell.

6.8.2. Az érintett kérelmeinek intézését díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a kért tájékoztatás vagy intézkedés teljesítésével járó adminisztratív költségek (pl. másolat, adathordozó költségei) felszámíthatók, indokolt esetben az intézkedés megtagadható. A kérelem egyértelműen megalapozatlanság vagy túlzó jellegének okairól írásban jegyzetet, emlékeztetőt kell készíteni.

6.9. A személyes adatokat törölni kell, ha

a) az adatkezelésre meghatározott időtartam eltelt, vagy az adatkezelés egyébként céltalanná, illetve indokolatlanná vált,
b) az érintett kéri,
c) arra az Adatkezelőt jogszabály, bírósági vagy hatósági határozat kötelezi.

Nem törölhető olyan adat, amely az Adatkezelő jogszabályi kötelezettségeinek teljesítése érdekében szükséges lehet. Az adatok törléséhez minden esetben az igazgatóság vagy az adatvédelmi tisztviselő

10

előzetes jóváhagyását kell beszerezni – ide nem értve azon automatizált adattörléseket, amelyek elektronikus adatbázisokat vagy dokumentumokat érintenek, és amelyekkel kapcsolatosan a törlési rutinokat az igazgatóság már korábban jóváhagyta.

6.10. A személyes adatok törlése során úgy kell eljárni, hogy az a törölt adat megismerhetőségét kizárja. Így:

a) a személyes adatot tartalmazó papír alapú dokumentum
   - teljes egészében megsemmisítendő (pl. iratmegsemmisítővel),
   - ha a dokumentum teljes megsemmisítése nem indokolt, úgy a személyes adatok olvashatatlanná tételével biztosítandó a törlés

   oly módon, hogy a papír alapú dokumentumról készített elektronikus másolat is törlendő, vagy az olvashatatlanná tett változattal váltandó fel;

b) a személyes adatot tartalmazó elektronikus dokumentum
   - teljes egészében törlendő, vagy
   - amennyiben annak teljes törlése nem indokolt, úgy abból a törlendő adatok távolítandóak el

   oly módon, hogy az elektronikus dokumentum személyes adatot tartalmazó változata ne legyen helyreállítható.

Az elektronikus dokumentumokat, adatbázisokat a biztonsági mentésekből is törölni szükséges, vagy olyan visszaállítási protokoll biztosítandó, amely a kérdéses file-okat nem állítja vissza, és a biztonsági másolatok tartalmához nem (akár harmadik személyek, mint pl. rendszergazdai feladatokat ellátók irányában sem) teszi lehetővé.

6.11. Az adatok törléséért az adatot közvetlenül kezelő munkavállaló felelős.

6.12. Az adatvédelmi incidenseket valamennyi munkavállaló köteles haladéktalanul, de legkésőbb a tudomásszerzést követő 12 órán belül jelezni az igazgatóságnak, valamint az adatvédelmi tisztviselőnek.

6.13. Az adatvédelmi incidenst az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja által kijelölt munkavállaló köteles haladéktalanul kivizsgálni, és az azzal kapcsolatos kockázatokat értékelni, és az értékelésbe az adatvédelmi tisztviselőt bevonni. A kockázatértékelés eredményéről az igazgatóságot tájékoztatni kell.

„Az adatvédelmi incidensek értékelését célzó dokumentumokat az elkészítő munkavállaló az adatvédelmi tisztviselő jóváhagyását követően elektronikus formában köteles elmenteni, és azzal egyidejűleg megküldeni az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja részére elektronikus úton. Az incidensekkel kapcsolatos információihoz csak az incidenseket kivizsgáló munkavállaló (vagy a munkakörét átvett személy) illetve az igazgatóság, valamint az adatvédelmi tisztviselő számára biztosítható hozzáférés.

6.14. A kockázatértékelés eredményei alapján az igazgatóság – az adatvédelmi tisztviselővel való egyeztetést követően – megteszi a szükséges intézkedéseket a további incidensek elkerülése érdekében.

Az intézkedéseket az adatvédelmi tisztviselővel, az adatkezelést közvetlenül végző munkavállalókkal, valamint szükség esetén a többi munkavállalóval vagy az Adatkezelővel szerződéses jogviszonyban álló harmadik személlyel is közölni kell. Mellőzendő a többi munkavállaló vagy Adatkezelővel szerződéses jogviszonyban álló harmadik személy értesítése, ha a közlés feltehetően újabb adatvédelmi incidenseket alapozna meg.

6.15. Az érintett jogaira és szabadságaira kockázatot jelentő incidenseket az adatvédelmi tisztviselő – az adatszolgáltatásnak az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja általi

jóváhagyása alapján – köteles haladéktalanul, de legkésőbb az incidens bekövetkezte vagy az arról való tudomásszerzést követő 72 órán belül jelezni a NAIH felé a GDPR 33. cikke alapján, amely adatszolgáltatás tartalmát az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja által erre kijelölt munkavállaló készíti elő. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintett(ek) jogaira és szabadságaira nézve, az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja által kijelölt munkavállaló haladéktalanul elkészíti az érintettet az adatvédelmi incidensről tájékoztató felhívást is, amelyet az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja hagy jóvá.

6.16. A GDPR 33. cikk (5) bekezdése szerint az Adatkezelő az adatvédelmi incidensekről nyilvántartást vezet, amelyet az adatvédelmi tisztviselő állít össze. Ezen nyilvántartásban egyaránt rögzíteni kell a NAIH, valamint az érintett értesítését nem igénylő incidenseket is.

6.17. Személyes adatok harmadik országba (nem Uniós tagállamba) kizárólag a GDPR 45, 46, valamint 48-49. cikkelye alapján továbbíthatók.

6.18. Az EGT tagállamok mellett szabadon továbbíthatók a személyes adatok a Bizottság által jóváhagyott országokba. A GDPR 45. cikke alapján a Bizottság által jóváhagyott országnak tekintendő Andorra, Argentína, Dél-Korea, Egyesült Királyság, Feröer Szigetek, Guernsey, Izrael, Jersey, Japán, Kanada, Man-sziget, Svájc, Uruguay, valamint Új-Zéland. Ezen országokba személyes adatok továbbíthatók.

6.19. Minden olyan esetben, amelyben a 6.18-as pont által nem lefedett országba továbbítandó adat, kötelező megbizonyosodni róla, hogy az adott adatkezelő a GDPR 46. cikkelyének megfelelő garanciákat nyújtott-e az adatkezelésének megfelelőségére vonatkozóan, azaz az adatkezelő igazolja, hogy

- kötelező erejű vállalati szabályokat alkalmaz, vagy
- a Bizottság által elfogadott általános adatvédelmi kikötéseknek felelés meg, vagy
- az Unióban elfogadott magatartási kódexnek vetette alá magát, vagy az Unióban jóváhagyott tanúsítási mechanizmussal került ellenőrzésre

6.20. Amennyiben a harmadik országba történő adattovábbítás a GDPR 45-46. cikke szerint nem lehetséges, úgy az adat továbbítása kizárólag a GDPR 49. cikke alapján történhet.

7. Különleges adatok kezelése

7.1. A különleges adatokhoz hozzáférés kizárólag az igazgatóságnak, az adatkezelést közvetlenül végző munkavállalónak, a munkakörét helyettesítő munkavállalónak adható. Más munkavállalónak jogosultság, vagy külső, más az Adatkezelővel szerződéses jogviszonyban álló harmadik személynek hozzáférés csak különösen indokolt esetben biztosítható.

7.2. Különleges adatok esetében az adatkezeléssel kapcsolatos kockázatok sem az adatvédelmi hatásvizsgálat, sem az adatvédelmi incidensek keretében nem zárhatók ki, és nem értékelhetők az azokkal kapcsolatos tevékenységek valószínűsíthetően kockázatmentesnek.

7.3. Különleges adatok esetében az azok jellegére és formájára, valamint az adatkezelés kockázataira nézve figyelemmel indokolt technikai és szervezési intézkedések elrendelése nem mellőzhető.

8. Az adatkezelések technikai háttere

8.1. Személyes adatot tartalmazó papír alapú dokumentumok kizárólag az iratkezelési szabályzatban meghatározott tárolási rendben, illetve eszközökben őrizhetők, és azok az Adatkezelő székhelyéről kizárólag az igazgatóság elnöke, vagy az igazgatóság önálló aláírási jogosultságú tagja engedélyével vihetők ki.

8.2. Elektronikus formában tárolt személyes adatok, vagy személyes adatokat tartalmazó dokumentumok kizárólag jelszóval védett számítógépeken kezelhetők. Ilyen dokumentumok vagy adatbázisok külső tárhelyre vagy levelezőrendszerre történő továbbítása, illetve más, harmadik személy által potenciálisan hozzáférhető eszközökön való használata, megnyitása, tárolása tilos.

8.3. A 8.2-es pontban foglalt számítógépekre olyan biztonsági megoldások telepítendők fel, amelyek az informatikai biztonsági igényeket az adatkezelés tárgyával, valamint a kezelés jellegével összefüggésben biztosítják. A konkrét igények az adatvédelmi kockázatelemzés, illetve szükség szerinti hatásvizsgálat eredményei alapján határozandók meg.

8.4. Törekedni kell arra, hogy különleges személyes adatokat tartalmazó elektronikus dokumentumok vagy adatbázisok kizárólag az Adatkezelő saját eszközein kerüljenek tárolásra, illetve kezelésre. Ezen eszközökre az 8.2-es pontban foglaltak megfelelően irányadók.

8.5. Személyes adatokat tartalmazó dokumentumokról vagy adatbázisokról készített biztonsági mentések (vagy ilyen dokumentumokat illetve adatbázisokat is tartalmazó biztonsági mentések) megfelelő titkosítás mellett is kizárólag olyan környezetben tárolhatók, amelyek magas szinten támogatják az adatkezeléssel kapcsolatos garanciák megtartását, valamint nem jelentenek kockázatot az adatok biztonságára vonatkozóan.

9. Vegyes rendelkezések

9.1. Az adatkezeléssel kapcsolatos nyilatkozatokat és utasításokat írásban kell megtenni. Amennyiben az eset összes körülménye sürgős szóbeli közlést indokol, úgy az azzal kapcsolatosan tett nyilatkozatok és utasítások a szóbeli közlésre okot adó körülmény elmúltát követően haladéktalanul írásba foglalandóak. Az e-mailben, sms-ben és egyéb üzenetküldő alkalmazásban, illetve szolgáltatással történt közlés az Adatkezelő szervezetén belül írásbelinek minősül, ha az a szükséges ideig visszakövethetően változatlan formában rendelkezésre áll.

9.2. Az adatvédelemmel kapcsolatos működés során mindenkor a legteljesebb mértékben törekedni kell rá, hogy a jelen Szabályzatnak, valamint a jogszabályi elvárásoknak való megfelelés igazolható legyen, különösen:

a) az érintettnek az adatkezeléshez történő hozzájárulására,
b) az érintettnek a különleges adatok kezelésére tett kifejezett hozzájárulására,
c) az érintett által az egyes adatok törlésére, helyesbítésére, az adatkorlátozás teljesítéséről szóló teljesítés igazolására,
d) az adatvédelmi incidensekről szóló érintetti értesítésre,
e) harmadik országba történő adattovábbításra,
f) a jogos érdeken alapján történő adatkezelés érdekmérlegelési tesztjének elvégzésére vonatkozóan.

Ezen fenti esetekben az igazolhatóságot biztosító írásbeli (vagy annak minősülő) forma sürgős esetekben sem mellőzhető. Az online rendszerekkel kapcsolatos működési háttér úgy alakítandó ki, hogy ezen igények teljesítését biztosítsa – így pl. abban az adatkezeléshez történő, az azonosított érintett által tett hozzájárulás egyértelműen megállapítható legyen.

9.3. Harmadik személyektől nem fogadható el olyan teljesítés, amely olyan személyes adatot tartalmaz, melynek jogszerű kezelhetősége az Adatkezelő vagy a harmadik személy által nem biztosított. Ezen rendelkezést a harmadik személyekkel kötött valamennyi szerződéses megállapodásban rögzíteni kell.

9.4. Az adatvédelmi szabályok megtartásáért az Adatkezelő munkavállalói, valamint szerződéses partnerei egyedileg és közvetlenül felelősek. Az adatkezeléssel összefüggésben felmerült károkért (így különösen hatósági bírságokért, az adatkezeléssel összefüggésben az érintettnek fizetett

sérelemdíjakért, valamint reputációs veszteségekért és elmaradt hasznokért) utóbbiak korlátlan felelősséggel tartoznak. A munkavállalók a károkért a Munka Törvénykönyvéről szóló 2012. évi I. törvény 179.§-ában foglaltak szerint felelnek.

9.5. Jelen Szabályzat szükség esetén, de legalább kétévente az igazgatóság által felülvizsgálandó.