GH/57/2026

Móricz Zsigmond Színház Nonprofit Kft.

Adatvédelmi incidensek kezelésének szabályzata

Tartalom:

A **Móricz Zsigmond Színház Nonprofit Kft.** (a továbbiakban: Társaság) belső adatkezelésével kapcsolatosan érintettek jogainak biztosítása céljából az alábbi Adatvédelmi incidensek kezelésének szabályzatát alkotja.

Adatkezelő:

Adatkezelő megnevezése:	**Móricz Zsigmond Színház Nonprofit Kft**
Adatkezelő cégjegyzékszáma:	15-09-080692
Adatkezelő székhelye:	4400 Nyíregyháza, Bessenyei tér 13.
Adatkezelő képviselője:	**Kirják Róbert**
Adatkezelő e-elérhetősége:	kirjak@moriczszinhaz.hu
Adatvédelmi tisztviselő:	dr. Lengyel Levente Lajos
E-mail cím:	mzs.szinhaz.adatvedelem@gmail.com

Az adatvédelmi tisztviselő:

- neve:	**dr. Lengyel Levente Lajos**
- elérhetősége:	mzs.szinhaz.adatvedelem@gmail.com +36 30/180 62 63

Jelen rendelkezéseket a Társaság többi, az adatvédelemmel kapcsolatos szabályzatának előírásaival összhangban kell értelmezni.

Vonatkozó jogszabályok

Infotv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII.törvény
Mt.	a munka törvénykönyvéről szóló 2012. évi I. törvény
Mvt.	a munkavédelemről szóló 1993. évi XCIII. törvény
Ptk.	a polgári törvénykönyvről szóló 2013. évi V. törvény
Sztv.	a számvitelről szóló 2000. évi C. törvény
GDPR vagy Rendelet	az Európai Parlament és a Tanács (EU) 2016/679 rendelete
NAIH vagy Hatóság	Nemzeti Adatvédelmi és Információszabadság Hatóság

1. A szabályzat célja és hatálya

A Társaság jelen szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja a GDPR. 12. cikkében meghatározott érintetti tájékoztatáshoz való jog megvalósulását.

A szabályzat célja, hogy

- az érintettek megfelelő tájékoztatást kaphassanak adatvédelmi incidens előfordulása esetén annak eljárás rendjéről
- garanciát adjon a bejelentő védelmére, személyes adatainak biztonságos kezelésére

A szabályzattal a Társaság biztosítani kívánja az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését

A szabályzat tárgyi hatálya kiterjed a Társaságnál folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

Személyi hatály kiterjed:

- ügyvezető igazgatóra
- a Társaság valamennyi dolgozójára
- a feladatellátás érdekében szerződéses, megbízásos jogviszonyban álló foglalkoztatottakra
- a Társaság által nyújtott szolgáltatást igénybe-vevőkre (nézőkre, látogatókra)
- a Társaság valamennyi beszállítójára/szerződő partnerére a vállalkozás érdekében vagy képviseletében a vállalkozás kifejezett írásbeli engedélye szerint eljáró bármely más személyre
- bejelentő személyre.

Időbeli hatály: 2026. január 1-től visszavonásig tart.

2. Az adatkezelések szabályai

Mivel az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így a Társaság eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést.
Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség.
A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.
A Társaság személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig.
Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről a Társaságnak az adatot ténylegesen kezelő munkavállalója gondoskodik. A törlést az ügyvezető és az adatvédelmi tisztviselő ellenőrizheti.

A Társaság személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli –hozzájárulása vagy törvény, illetve törvényi felhatalmazás alapján kezel.

A Társaság az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.
A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak és a Társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni.

Ha a szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.
A Társaság megbízásából adatfeldolgozói tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségeket az adatfeldolgozóval kötött megbízási szerződésben érvényesítendők. Az adatfeldolgozóval a Társaság a GDPR által előírt Adatfeldolgozói szerződést köt.

3. A Társaság adatvédelmi rendszere

3.1. A személyes adatok kezelésével kapcsolatos felelősségek

3.1.1. Ügyvezető felelőssége:

- a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket;
- szabályzatok és kötelező utasítások útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról;
- gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról;
- írásban kijelöli az adatvédelmi tisztviselőt;
- meghozza az adatvédelmi incidensek kezelésére vonatkozó döntéseket;
- felel az adatkezelési tevékenységgel kapcsolatos közzétételi kötelezettség teljesítéséért.

3.1.2. Szervezeti egység vezetők felelőssége

- a szervezeti egységnél dolgozók felügyelete, az adatvédelmi és adatbiztonsági szabályok betartása tekintetében;
- a területen dolgozók által jelentett adatvédelmi incidensek felülvizsgálata és indokolt esetben a szükséges intézkedések meghozatala;
- a saját hatáskörön túlmutató esetekben az adatvédelmi tisztviselő tájékoztatása;
- közreműködés a kivizsgálás során.

3.1.3. Dolgozók felelőssége

A Társaság munkatársai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.
Kötelesek

- betartani a személyes adatok kezelésére előírt szabályokat;
- amennyiben illetéktelen hozzáférést, adatszivárgást tapasztal a személyes adatokkal kapcsolatosan az köteles bejelenteni a közvetlen felettesének (szervezeti egység vezetőjének), vagy az adatvédelmi tisztviselőnek.

3.1.4. Adatvédelmi tisztviselő

- az adatvédelmi szabályzatok, adatkezelési tájékoztatók felülvizsgálata;
- a bejelentett adatvédelmi incidens kivizsgálása;
- javaslattétel az incidens kezelésére;
- a NAIH-al kapcsolattartás, bejelentés teljesítése.

Az adatvédelmi tisztviselő feladat- és hatáskörére vonatkozó részletes előírásokat a Társaság ***Adatvédelmi és adatbiztonsági szabályzata*** részletesen tartalmazza.

4. Adatvédelmi incidens kezelése

A GDPR 4. cikk 12. pontja szerinti **„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.

4.1. Adatvédelmi incidens észlelése és jelentése

Amennyiben a Társaság foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja a szervezeti egység vezetőjét.
A szervezeti egység vezetője az észlelt adatvédelmi incidens kapcsán saját hatáskörben jár el. A jelzést követően azonnal tájékozódik az eset lényeges körülményeiről.
Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, soron kívül megkezdi az incidens érintettekre nézve megjelentő hatásainak csökkentését és arról haladéktalanul értesíti az adatvédelmi tisztviselőt.

Az értesítés tartalmazza:

- az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;
- a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;
- az általa megtett halaszthatatlan intézkedéseket;
- megítélés szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyát;
- az általa tervezett további intézkedések leírását.

A szervezeti egység vezetője haladéktalanul értesíti az adatvédelmi tisztviselőt a bekövetkezett eseményről és a nála rendelkezésre álló információkról, ha

- az adatvédelmi incidens bekövetkezte vagy annak a szervezeti egységre vonatkozó jellemzői számára nem állapíthatók meg egyértelműen és legfeljebb az észlelését követő 24 órán belül,
- az adatvédelmi incidens megítélés szerint elsősorban más szervezeti egység tevékenységét érinti, illetőleg
- az adatvédelmi incidens több szervezeti egységet is érinthet.

Az adatvédelmi tisztviselő megvizsgálja az értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja az informatikai biztonságért felelőst, a szervezeti egység vezetőjét is.

Amennyiben az adatvédelmi incidens érinti a Társaság által üzemeltetett elektronikus információs rendszerének biztonságával összefüggésben következett be, az adatvédelmi tisztviselő a Társaság informatikai biztonságáért felelős (IBF) felé is köteles jelezni a bejelentést. Az IBF a jelzést követően köteles haladéktalanul véleményt összeállítani az adatvédelmi tisztviselő részére arról, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javasolt megtett intézkedéseket.

Amennyiben az adatvédelmi incidens a Társaság által igénybe vett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó adatvédelmi tisztviselőjét is be kell vonni.

4.2. Adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő az adatvédelmi incidens vizsgálata keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat. Ennek során legalább a következőket veszi figyelembe:

- az adatvédelmi incidens jellegét;
- az érinetetek körét, hozzávetőleges számukat;
- az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és a GDPR preambulumának (75) bekezdése szerinti szenzitív adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;
- az elektronikus információbiztonságot is érintő incidensek esetén az elektronikus információbiztonságért felelős által azonosított további kockázatot;
- az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adtavédelmi Testület által elfogadott – agy a GDPR alkalmazandóvá válását követően fenntartott – iránymutatást;
- az adatkezelés kapcsán korábban lefolytatott adatvédelmi hatásvizsgálat dokumentációját.

A Társaság az adatvédelmi incidenseket három kategóriába sorolja:

- 1. kategória: valószínűsíthetően kockázattal járó incidens
- 2. kategória: valószínűsíthetően alacsony kockázattal járó incidens
- 3. kategória: valószínűsíthetően magas kockázattal járó incidens

<u>Érékelési szempontok:</u>

- az incidens típusa (bizalmassági, integritási vagy elérhetőségi)
- a személyes adatok jellege (személyes adat/különleges adat)
- a személyes adatok száma
- az érintett személyek száma

- az érintett természetes személyek azonosíthatósága
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága
- az érintett adatkezelés jogalapja.

A Társaságnál az incidens értékelése során az alábbi konkrét szempontok alapján értékeli:

- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett személyes adatok száma meghaladja a 100 darabot,
- az incidensben érintett természetes személyek száma meghaladja a 100 főt,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az incidensben érintett adatkezelés jogalapja az érintett vagy egy másik természetes személy létfontosságú érdeke,
- az incidensben érintett adatkezelés jogalapja közérdekű vagy közhatalmi jogosítvány gyakorlása,
- az incidensben érintett adatkezelés jogalapja a Társaság vagy egy harmadik fél jogos érdeke,
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget okozzanak az érintettjüknek.

Az incidenst a Társaság „1.kategóra: valószínűsíthetően kockázattal nem járó incidens"-nek minősíti, ha:

- a fent felsorolt feltételek közül legfeljebb kettő áll fenn és
- a Társaság képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

Az incidenst a Társaság „2.kategória: valószínűsíthetően alacsony kockázattal járó incidens"-nek minősíti, ha:

- a fent felsorolt feltételek közül egy áll fenn és
- a Társaság nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

Az incidenst a Társaság „3.kategória: valószínűsíthetően magas kockázattal járó incidens"-nek minősíti, ha:

- a fent felsorolt feltételek közül legalább kettő áll fenn és
- a Társaság nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja a Társaság ügyvezető igazgatóját az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószítnűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.
A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.

Amennyiben a Társaság ügyvezető igazgatója a kapott tájékoztatás alapján úgy ítéli meg, hogy adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő a NAIH honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a NAIH által vezetett nyilvántartásba.

Amennyiben a vizsgálatot az adatvédelmi tisztviselő véleménye szerint

- nem lehet 72 órán belül teljeskörűen lefolytatni, vagy
- nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi incidens bekövetkezésének valamennyi más lényeges körülményét,

úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján, szakaszos bejelentésre tesz javaslatot az ügyvezető igazgató részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

Amennyiben az ügyvezető igazgató az adatvédelmi tisztviselő tájékoztatása alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, vagy az esemény egyéb körülményei alapján azt szükségesnek látja, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével elrendeli az érintettek tájékoztatását az adatvédelmi incidens kapcsán.

Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – ésszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi a Társaság honlapján.

5. Kockázati tényezők, amelyek adatvédelmi incidens bekövetkezését eredményezhetik

Adatvédelmi incidens bekövetkezését eredményezhetik az alábbi kockázati tényezők:

- informatikai eszközt elvesztik, ellopják (személyes adatok voltak rajta),
- feltörik az informatikai rendszert,
- levél, irat elvesztése vagy jogosulatlan felnyitása,
- papír alapú dokumentumot elvesztik, ellopják vagy nem biztonságos helyen tárolják,
- rosszindulatú (zsaroló) programok vannak a számítógépeken,
- személyes adatok jogosulatlan megismerése,
- személyes adatok jogosulatlan szóbeli közlése,

- személyes adatok nagy nyilvánosság előtti jogellenes közzététele,
- személyes adatok téves címzett részére történő elküldése stb.

6. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó elektronikus nyilvántartást vezet.

A nyilvántartás tartalmazza:

- az adatvédelmi incidensről készült feljegyzés iktatószámát;
- az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;
- az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;
- az érintett személyes adatok körét;
- az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;
- a bejelentés időpontját – amennyiben az adatvédelmi incidenst a Társaság részére bejelentették, vagy annak rövid indoklását, ami miatt az adatvédelmi incidenst nem jelentették be.

Az adatvédelmi incidens nyilvántartás (*1. számú melléklet*) pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

7. Az adatvédelmi incidens bejelentése a Hatóság részére

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Amennyiben a Társaság az adatvédelmi incidenst 2. kategóriába vagy a 3. kategóriába tartozónak minősíti, úgy az adatvédelmi tisztviselő az értékelés megtörténtét követően, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens a Társaság tudomására jutott, az adatvédelmi incidenst be kell jelenti a NAIH-nak.

Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére.

A hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

8. Az érintettek tájékoztatása az adatvédelmi incidensről

Az incidens kivizsgálása során vizsgálni kell, hogy

- az adatvédelmi incidens okait (külső vagy belső, rosszhiszemű vagy rosszhiszeműnek nem minősülő cselekmény),
- milyen adatkört érintett (személyes adatok, különleges adatok), kik az érintettek (alkalmazottak, felhasználók, ügyfelek),
- mik a következmények (mi sérült):
  - bizalmas jelleg (szélesebb körű hozzáférés történt, mint amihez az érintett hozzájárult, az adat összekapcsolhatóvá vált az érintett adatával, más célból, tisztességtelen módon történő kezelés),
  - integritás sérülése (az adat módosíthatóvá vált, valószínű, hogy módosították, eltérő célra használták),
  - az érintettet ért fizikai vagy nem anyagi károk, egyéb jelentős következmények (érintetti jogok korlátozása, hátrányos megkülönböztetés, jó hírnév sérelme, pénzügyi veszteség, személyes adatok feletti rendelkezés elvesztése, személyazonossággal való visszaélés).

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről az ügyvezető igazgatót is.

<u>Nem kell az érintetteket tájékoztatni:</u>

- ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét,
- ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg,
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

9. Rendszeres tréningek

Az adatvédelmi tisztviselő az adatvédelmi tudatosság növelése céljából gondoskodik adatvédelmi incidensekkel kapcsolatos oktatásról (személyesen, vagy általa megbízott személy közreműködésével), mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad legalább évente egy alkalommal.
Az adatvédelmi tisztviselő az oktatás időpontját az ügyvezetővel köteles egyeztetni, de évente legalább egy alkalommal köteles megtartani, melyen az ügyvezető által kijelölt dolgozók kötelesek részt venni.

A tréningek formáját, módját (kontakt képzés vagy ppt. anyag) az adatvédelmi tisztviselő határozza meg, melyről az ügyvezetőt tájékoztatja.

Az adatvédelmi oktatásnak legalább az alábbi témákra kell kiterjednie:

- az előző oktatás óta eltelt időszak tapasztalatai az adatvédelem területén,
- amennyiben az előző oktatás óta módosult a Szabályzat, a módosítással kapcsolatos legfontosabb tudnivalók,
- az esetlegesen megtörtén adatvédelmi incidens bemutatása, értékelése, a helyesbítő, megelőző intézkedések ismertetése,
- az adatvédelem területén történt általános változások, jogszabály módosítások.

Az adatvédelmi tisztviselő rendkívüli oktatást tart – amennyiben az indokolt – az alábbi esetekben:

- adatvédelmi incidens megtörténte,
- marasztalással zárul NAIH-eljárás lefolytatás a Társasággal szemben,
- adatvédelmi bírság kiszabása bármely, hasonló vagy azonos feladatot ellátó jogi személy ellen, ha eltérő gyakorlatot igényel a Társaság adatvédelmi rendszerében.

A belső adatvédelmi oktatásokról az adatvédelmi tisztviselő nyilvántartást köteles vezetni. Részletes szabályokat a Társaság „Adatvédelemmel és adatkezeléssel kapcsolatos nyilvántartások vezetésének szabályzata" rögzíti.

10. Hatásvizsgálat

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően a Társaság hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlen egy hatásvizsgálat keretében is elvégezhetők.
A hatásvizsgálatot az adatvédelmi tisztviselő végzi. Amennyiben nem ő végzi, úgy a Társaság köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén gondoskodik a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra elvégzi. A kockázatok felülvizsgálatát legalább 3 évente el kell végezni.

Záró rendelkezés

A szabályzat **2026. január 01**.-től hatályos.
E Szabályzat rendelkezéseit meg kell ismertetni a Társaság valamennyi munkavállalójával (foglalkoztatottjával), és a munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden munkavállaló (foglalkoztatott) lényeges munkaköri kötelezettsége. Felelős a munkáltatói jogkör gyakorlója.
A „Munkaszerződés kikötés" a dolgozók személyi anyagában kerül elhelyezésre.

A szabályzat felülvizsgálatát általános szabályok szerint évente, tárgyévet követő év január 31-ig kell elvégezni. Amennyiben jelentős változás következik be az adatkezelési folyamtokban, akkor a változást követő 30 napon belül kell elvégezni a szabályzat aktualizálását.
A szabályzat felülvizsgálatáért, aktualizálásáért az adatvédelmi tisztviselő a felelős.

Nyíregyháza, 2026. január 05.

jóváhagyta:

Kírják Róbert
ügyvezető igazgató

1.számú melléklet

Nyilvántartás adatvédelmi incidensekről

Iktatószám	adatvédelmi incidenssel érintett irat vagy nyilvántartás	adatvédelmi incidens észlelésének időpontja	érintett személyes adatok köre	az incidens hatásai, következményei	az adatvédelmi incidens orvoslására tett intézkedések	az incidens bejelentésének időpontja	a bejelentés mellőzésének rövid indoklása