SOPRON-FERTŐ
TURISZTIKAI FEJLESZTŐ
NONPROFIT ZRT.

9400 Sopron, Új utca 4.
titkarsag@sopronfertonzrt.hu
+36 99 951 594 | +36 30 337 82 58

SZ-13
Verzió:02

ADATVÉDELMI ÉS ADATKEZELÉSI TÁJÉKOZTATÓ/SZABÁLYZAT

Hatályos: 2021.november 15-től

Sopron, 2021.november 15.

Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zrt.
9400 Sopron, Új u. 4.
25891108-2-08

Kárpáti Béla Imre
vezérigazgató
(munkáltató)

Bevezető

I. A Szabályzat célja

Jelen Szabályzat célja annak biztosítása, hogy a Társaság megfeleljen az adatvédelemmel kapcsolatos hatályos jogszabályoknak, így különösen az alábbiaknak:

- Magyarország Alaptörvénye
- 2011. évi CXII. törvény - az információs önrendelkezési jogról és az információszabadságról;
- 2016/679/EU Általános Adatvédelmi Rendelettel (General Data Protection Regulation, GDPR)
- 2012. évi I. törvény – a munka törvénykönyvéről (Mt.);
- 2013. évi V. törvény – a Polgári Törvénykönyvről (Ptk.);
- 2000. évi C. törvény – a Számvitelről (**Számviteli tv.**);
- 1997. évi CLV. törvény – a fogyasztóvédelemről (**Fogyasztóvédelmi tv**.)
- 2005. évi CXXXIII. törvény – a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól;
- 2009. évi CLV. törvény a minősített adat védelméről
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

II. A Szabályzat hatálya

2.1. Időbeli hatály

Jelen Szabályzat 02 Verzió 2021. november 15-től további rendelkezésig, visszavonásig hatályos.

2.2. Személyi hatály

Jelen Szabályzat hatálya kiterjed a Társaságra, azon személyekre, akik adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon személyekre, akik jogait vagy jogos érdekeit az adatkezelés érinti.

2.3. Tárgyi hatály

Jelen Szabályzat hatálya kiterjed a Társaság minden szervezeti egységében folytatott valamennyi személyes adatokat tartalmazó adatkezelésre ill. az onnan történő adattovábbításra.

III. Fogalmak

Az alábbi fogalmak a jelen Szabályzat alkalmazásában értendők:

adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

személyes adat: azonosított vagy azonosítható természetes személyre („Érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen

valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

adatalany/érintett: bármely információ alapján azonosított vagy egyébként – közvetlenül, vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. A jelen Szabályzat tekintetében Érintettnek minősülnek különösen a Társaság ügyfelei/szerződő partnerei (ezek kapcsolattartói), és vendégei, honlapjainak látogatói, és bármely harmadik személy, akinek a személyes adatát a Társaság kezeli.

különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

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

adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; 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.

adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).

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

az adatkezelés jogalapja: (i) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez, vagy (ii) 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, vagy (iii) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, vagy (iv) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges, vagy (v) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy (vi) 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

hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes, vagy különleges adatok – teljes körű vagy egyes műveletekre kiterjedő –kezeléséhez. Különleges adatok esetében szükséges az írásos forma.

megfelelő tájékoztatás: az érintettel az adatkezelés jogalapját, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről (címzett), az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

adatbiztonság: a Társaság megfelelő intézkedésekkel védi az adatok, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, sérülés ellen és gondoskodik az adatok biztonságáról, melynek keretében megteszi azokat a technikai, műszaki és szervezési intézkedéseket, melyek szükségesek az adatvédelmi szabályok érvényre juttatásához.

az adatkezelés elvei: a Társaság a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi, a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból gyűjti, melyek megfelelőek, relevánsak és a szükségesre kell korlátozódniuk, a személyes adatok pontosak és szükség esetén naprakészek, tárolásuk olyan formában történik, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé és kezelésüket oly módon végzi, 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

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

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

harmadik fél: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az Érintettel, az adatkezelővel vagy az adatfeldolgozóval;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

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;

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.

IV. Az adatkezelések jogalapja, alapelvek az adatkezelés során

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) 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;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) 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.

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak, továbbá az adatok felvételének és kezelésének tisztességesnek kell lennie.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, és csak a cél megvalósulásához szükséges mértékben és ideig.

Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét, naprakészségét, valamint azt, hogy az Érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

Az 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.

A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak kötelesek a megismert személyes adatokat megőrizni.

A Munkáltató teljes mértékben tiltja, hogy a munkaviszony ellátása során a munkavállalók előtt feltárt és a jövőben feltárandó bizonyos információkat, így különösen üzleti terveket, kereskedelmi titkokat, ügyfelek adatait és egyéb tulajdonosi információkat, valamint a személyes adatokat (összefoglalóan: információk) a munkavállaló nem a Munkáltató tulajdonát képező elektronikus eszközön tárolja.

Minden olyan esetben, amely során bármely munkavállaló az Információt nem a jelen Szabályzatban meghatározottak szerint kezel, önálló adatkezelővé válik, az adatkezelésre vonatkozó jogok és kötelezettségek teljesítése során a Munkáltató helyére lép és egyben megvalósítja az Mt. 78. § (1) a) szerinti azonnali hatályú felmondás jogalapját.

A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező munkavállalók titoktartási nyilatkozatot írnak alá (1. számú melléklet), a nem munkaviszonyban álló személyekkel az Adatkezelő **Adatfeldolgozói megállapodást** (2. számú melléklet) köt.

V. A TÁRSASÁG ÁTAL VÉGZETT EGYES ADATKEZELÉSEK

Az Adatkezelő személyes adatot kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel. Az adatkezelés minden szakaszában megfelel az adatkezelés céljának. Az adatok felvétele és kezelése tisztességesen és törvényesen történik. Az Adatkezelő törekszik arra, hogy csak olyan személyes adat kezelésére kerüljön sor, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A Társaság automatikus döntéshozatalt, és profilalkotást nem végez.

Az Érintettek adatainak kezelése során:

(i) Amikor az adatkezelés jogszabályon alapul, a személyes adatok megadásának kötelezettségét a jogszabály írja elő, ilyen esetben az adatokat az Érintettek kötelesek megadni;

(ii) Amikor az adatkezelésre szerződéses kötelezettség teljesítése érdekében kerül sor, úgy az adat szolgáltatása szerződéses kötelezettségen alapul, a szerződésben kötelezően feltüntetendő adatok megadása a szerződéskötés előfeltétele.

(iii) jogos érdeken alapuló adatkezelés esetén az Érintett bármikor tiltakozhat az adatkezelés ellen, mely esetben – ha az adatokat más jogalapon már nem lehet kezelni, és nincs olyan kényszerítő erejű jogos ok, amely elsőbbséget élvezne az érintett érdekeivel, jogaival és szabadságaival szemben – az adatok törlésre kerülnek.

Az adatkezelések során a Társaság adatfeldolgozókat vehet igénybe, az adatfeldolgozók részletes adatait a 3. sz. melléklet tartalmazza és az V. pontban minden egyes adatkezelés esetén a „Címzettek" oszlopban röviden meghatározásra kerül az adott adatkezeléshez kapcsolódó adatfeldolgozó kategóriája (az általa nyújtott szolgáltatás megjelölése útján). Adatfeldolgozó csak olyan személy/vállalkozás lehet, aki írásbeli szerződésben vállalja az adatfeldolgozási feladatok ellátását, és akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására (az adatkezelés célját, jogalapját, az adatkezelési feladatokat és körülményeket, ideértve a szükséges biztonsági intézkedéseket is, a Társaság határozza meg). Az adatfeldolgozó nem jogosult az általa kezelt adatokat saját célra felhasználni.

A Társaság az általa kezelt személyes adatokat szerződéses kötelezettségei teljesítése és jogai érvényesítése során és céljából – annak jellegétől függően – továbbíthatja közreműködő szolgáltatók, hatóságok részére; ezen túlmenően egyes jogszabályi kötelezettségek teljesítése is adattovábbítással járhat (pl. számlák, bizonylatok adattartalmának NAV részére történő továbbítása, pénzmosás gyanú esetén bejelentés, hatósági ellenőrzések során, amennyiben ehhez szükséges.
A Társaság az adatokat saját jogos érdekeinek az érvényesítéséhez jogosult bíróságok, hatóságok részére továbbítani (számlakövetelések, kártérítési igények, bűncselekmények gyanúja esetén a feljelentéshez szükséges adatok stb.).
A Társaság jogosult a kötelezettségei teljesítéséhez és jogai érvényesítéséhez adatfeldolgozókat igénybe venni (tárhely szolgáltató, könyvelő, bérszámfejtő, adminisztratív szolgáltató stb.).
A Társaság EGT térségen kívüli területre kizárólag akkor továbbít személyes adatot, (pl. harmadik országbeli tárhely szolgáltató) ha az érintett ország rendelkezik a Bizottság megfelelőségi határozatával, vagy ha az adattovábbítás megfelelő és alkalmas garanciák mellett történik; ez utóbbiakról az érintettek bármikor információt kérhetnek a Társaságtól és részletes tájékoztatást találhatnak a Bizottság https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en oldalán.

Az érintett a VII. pontban részletezett módon kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, bizonyos esetekben joga van az adathordozhatósághoz.

Hozzájáruláson alapuló adatkezelés esetén a hozzájárulást bármikor, díjmentesen visszavonhatja, a hozzájárulás visszavonása nem érinti a megelőző adatkezelés jogszerűségét. Az érintett jogosult a felügyeleti hatósághoz panaszt benyújtani, illetve igényét bíróság előtt érvényesíteni.

A könnyebb áttekinthetőség érdekében a Társaság által végzett adatkezelésekről az alábbi táblázatos formában nyújtunk tájékoztatást:

V.1. Üzleti partnerek adatainak kezelése

Mint minden gazdasági szereplő, a Társaság az üzleti tevékenységével összefüggésben, szerződések létesítése és teljesítése, valamint az ezekkel összefüggő egyéb kötelezettségek teljesítése (szállítás/beszerzés szervezése, számlázás/számlafizetés, panaszügyek kezelése, jótállási/szavatossági igények intézése stb.), céljából a vele üzleti (beszállítói, szolgáltatói) viszonyban álló, illetve ilyen kapcsolatot létesíteni kívánó személyek (jogi személyek esetén az azokat képviselő személyek) adatait kezeli.

A beszállítókkal, szolgáltató partnerekkel kötött szerződéssel érintett adatok kezelése egyrészről a szerződés példányok, bizonylatok/számlák papír alapú irattározásával (a Társaság székhelyén), másrészről az adatoknak elektronikus mentésével valósul meg. A számviteli bizonylatok kiállítása és kezelése a vonatkozó jogszabályi rendelkezések szerint történik.

Adatkezelés leírása	**Kezelt adatok köre**	**Adatkezelés célja**	**Adatkezelés jogalapja**	**Adatok forrása**	**Adatkezelés címzettjei**	**Adatkezelés időtartama**
Magánszemély szerződéses partner adatainak kezelése	Név Lakcím anyja neve EV nyilvántartási száma, adószáma/ adóazonosító jele) Névjegykártya adatok (ahol felmerül) Bankszámlaszám (ahol szükséges)	Szerződő partner azonosítása, szerződés teljesítése	Szerződéses kötelezettség teljesítése - GDPR 6. cikk (1) b) pont	Érintett	Tárhely szolgáltató, mint adatfeldolgozó	A szerződés tartalmának megállapításához, illetve a teljesítés igazolásához szükséges dokumentumokon feltüntetett személyes adatok esetén a szerződés megszűnését követő 5 év (általános elévülési idő). Egyéb esetben a személyes adatokat a szerződés vagy a képviselői minőség megszűnését követően haladéktalanul töröljük.
	E-mail cím Telefonszám Kapcsolattartó megjelölése esetén: Kapcsolattartó neve E-mail címe Telefonszáma beosztása Névjegykártya adatok (ahol felmerül)	Kapcsolat-tartás a szerződő partnerrel	Szerződéses kötelezettség teljesítése - GDPR 6. cikk (1) b) pont Szerződéses partnertől eltérő kapcsolattartó esetén: jogos érdek a szerződéses kapcsolattartás biztosítása - GDPR 6. cikk (1) f) pont	Érintett Kapcsolattartó megjelölése esetén az adatok forrása a szerződéses partner	Tárhely szolgáltató, mint adatfeldolgozó	A szerződés tartalmának megállapításához, illetve a teljesítés igazolásához szükséges dokumentumokon feltüntetett személyes adatok esetén a szerződés megszűnését követő 5 év (általános elévülési idő). Egyéb esetben a személyes adatokat a szerződés vagy a képviselői minőség megszűnését követően haladéktalanul töröljük.

	Számlázási adatok	Bizonylatok kiállítása	Jogszabály: Számviteli tv. 165-169.§., ÁFA tv. 169.§. - GDPR 6. cikk (1) c) pont	Érintett	Tárhely szolgáltató, mint adatfeldolgozó Számlázási szolgáltató, mint adatfeldolgozó Könyvelő szolgáltató, mint adatfeldolgozó	A bizonylat kiállítása évének utolsó napjától számított 8 év.
Jogi személy szerződéses partner adatainak kezelése	Jogi személy képviseletében eljáró személy neve Beosztása Névjegykártya (ahol felmerül)	Szerződő partner azonosítása, szerződés teljesítése	Szerződéses kötelezettség teljesítése - GDPR 6. cikk (1) b) pont	Érintett	Tárhely szolgáltató, mint adatfeldolgozó	A szerződés tartalmának megállapításához, illetve a teljesítés igazolásához szükséges dokumentumokon feltüntetett személyes adatok esetén a szerződés megszűnését követő 5 év (általános elévülési idő). Egyéb esetben a személyes adatokat a szerződés vagy a képviselői minőség megszűnését követően haladéktalanul töröljük.
	Kapcsolattartó neve E-mail címe Telefonszáma beosztása Névjegykártya (ahol felmerül)	Kapcsolattartás a szerződő partnerrel	Jogos érdek a szerződéses kapcsolattartás biztosítása - GDPR 6. cikk (1) f) pont	Érintett vagy amennyiben nem azonos a képviselővel, akkor az adatok forrása a jogi személy képviselője	Tárhely szolgáltató, mint adatfeldolgozó	A szerződés tartalmának megállapításához, illetve a teljesítés igazolásához szükséges dokumentumokon feltüntetett személyes adatok esetén a szerződés megszűnését követő 5 év (általános elévülési idő). Egyéb esetben a személyes adatokat a szerződés vagy a képviselői minőség megszűnését követően haladéktalanul töröljük.

VI. Nyilvántartott adatok köre és típusai

A Társaság által nyilvántartott adatokat csoportosíthatjuk keletkezésük (forrásuk) szerint, mely a Társasághoz beérkező pályázati anyagoktól kezdve a kilépést követő archiválásig tart. Ezen logika szerint három fázisra bontható a személyes adatok nyilvántartási köre, amelyet az alábbi táblázat foglal össze.

	Adattípusok
Pályázati időszak (munkaviszony előtt)	pályázati anyagok / önéletrajzok
Munkaviszony alatt	- személyes azonosító adatok - jogviszony adatok, a munkáltató általi jogosítások adatai.

	- bérszámfejtéssel, táppénzzel, cafeteriával és egyéb juttatásokkal kapcsolatos adatok, nyugdíjpénztár és más megtakarítási célú adatok, a cég által kötött balesetbiztosítási adatok. - munkavállalók által intranet szerverre feltöltött adatok
Munkaviszony megszüntetése után	archivált adatok, a munkaviszony megszűnésekor keletkező, a következő munkahely számára releváns, Mt.-n alapuló adatok.
Egyéb / ügyfelekkel, szerződő partnerekkel, vendégekkel kapcsolatos adatok	- névjegykártyán megadott adat -képmás

Az adatok forrása minden esetben az Érintett által rendelkezésre bocsátott életrajz (pályázati anyag), képmás, a személyes azonosításra alkalmas hivatalos okmány, bizonyítvány, igazolás, illetve az Érintett által aláírt nyilatkozat, valamint az üzemorvos által szolgáltatott adat, illetve az ügyféllel, szerződő partnerrel kötött szerződés (-tervezet), átadott névjegykártya.

A belépési folyamat részeként az Adatkezelő nyilvántartásba veszi az összes személyes, munkajogviszonyhoz, illetve bérszámfejtéshez szükséges adatot, amelyet a munkaviszony fennállása alatt nyilvántart. A munkaszerződés egy eredeti példányát a pénzügyi vezető tárolja, mely eredeti példány a bérszámfejtés alapja. Az átadott iratokról egy scannelt példány elektronikus formában a tikárságvezető által elmentésre kerül.

A személyes adatokban bekövetkezett változásokat az Érintett 8 napon belül köteles bejelenteni az Adatkezelő felé. A változást igazoló dokumentumot a pénzügyi vezető veszi át, és átvezeti a rendszerekben.

A Társaság, mint Munkáltató, a vonatkozó jogszabályi kötelezettségek teljesítése érdekében az alábbi adatokat kezeli:

Adattípus	Adatkezelés célja	Adatkezelés jogalapja
Személyes azonosító adatok Teljes név Fénykép Születési név Születési hely, idő Nem Állampolgárság Anyja neve Családi állapota Személyi igazolvány száma TAJ szám Adóazonosító jel Bankszámlaszám Lakcím, tartózkodási hely Telefonszám, email cím (céges, ennek hiányában magán) végzettségek nyelvtudás gyermekek adatai (név, születési dátum, hely, adóazonosító, TAJ szám, anyja neve)	munkaviszonnyal kapcsolatos kötelezettségek teljesítése, bérszámfejtés	Érintett önkéntes hozzájárulása, különleges adatok esetén az érintett írásbeli hozzájárulása. (mely azzal történik, amikor az érintett a Társaság részére átadja személyes adatait tartalmazó iratait/ elektronikus fájl-t.) illetve törvényi felhatalmazás (Munka Törvénykönyvéről szóló 2012. évi I. törvény)
<u>Jogviszonyra vonatkozó adatok</u> Jogviszony kód munkaviszony kezdete, vége munkakör	munkaviszonnyal kapcsolatos kötelezettségek teljesítése, bérszámfejtés, jogviszonnyal kapcsolatos adatszolgáltatás (KSH)	törvényi felhatalmazás (Munka Törvénykönyvéről szóló 2012. évi I. törvény)

munkaviszony típusa FEOR szám munkarend, munkaidő költséghely beosztás munkavégzés helye		
Bérszámfejtéssel kapcsolatos adatok alapbér bérek érvényességének kezdete, vége levonások, letiltások ösztönző bér, béren kívüli juttatás, egyéb juttatás és ennek gyakorisága adókedvezmény szabadság, ennek jogcíme, mértéke túlmunka, készenlét, ügyelet szemüveg szükségessége monitorozáshoz tagsági jogviszonyok kezdete, vége	munkaviszonnyal kapcsolatos kötelezettségek teljesítése, bérszámfejtés	törvényi felhatalmazás (Munka Törvénykönyvéről szóló 2012. évi I. törvény)
Adattípus	**Adatkezelés célja**	**Adatkezelés jogalapja**
munkaalkalmassági vizsgálatok eredménye (alkalmas/nem alkalmas)	munkaviszonnyal kapcsolatos kötelezettségek teljesítése	törvényi felhatalmazás (Munka Törvénykönyvéről szóló 2012. évi I. törvény, 33/1998. (VI.24.) NM rendelet 14. sz. melléklete és az 50/1999. (XI.3.) EüM rendelet 1. sz. melléklete)
Céges laptop és telefon, egyéb kiadott műszer leltári száma	vagyonvédelem	az Érintett önkéntes hozzájárulása, mely azzal a cselekedettel történik, amikor átveszi a laptopot, telefont, ill. belépőkártyát, riasztókódot
Névjegykártyán, szerződésekben (tervezetekben) szereplő adatok (név, telefonszám, lakcím, e-mail cím, munkahely, munkahely címe, továbbá a névjegykártyán szereplő egyéb személyes adat).	kapcsolatépítés, a kapcsolattartó személyek közötti érintkezés megkönnyítése.	az Érintett önkéntes hozzájárulása, mely azzal a cselekedettel történik, amikor átadja az Adatkezelő részére a személyes adatait tartalmazó névjegyét.
Munkavállalók által megadott /feltöltött adatok (eddigi munkahely, szakmai előélet, fotó, név, titulus, munkakör, szervezeti egységben elfoglalt helye, hobby stb.)	hírmegosztás, szervezeti eligazodás (vállalti események) összetartás erősítése	az Érintett önkéntes hozzájárulása, mely azzal a cselekedettel történik, amikor feltölti az intranet szerverre a személyes adatait

VII. A nyilvántartás és adatkezelés és a hozzáférés módja

A Munkáltató az adatokat elektronikusan és papír alapon, a munkavállalók személyi anyagában lefűzve tárolja. Az elektronikus adatkezelést HR-szoftverek és Excel táblázatokban kiépített adatbázisok támogatják.

Az alábbi táblázat tartalmazza az adatok nyilvántartásának helyét, valamint az adatokhoz történő hozzáférésre jogosultak megjelölését:

Adattípus	**Nyilvántartás helye**	**Hozzáféréssel rendelkezik**
Pályázat/ önéletrajz papír/ elektronikus	Csak a kiválasztási folyamata során került nyilvántartásra a pénzügyi osztályon, zárható szekrényben, utána törlésre kerül, kivéve, ha az Érintett	pénzügyi vezető, pénzügyes munkatársak

	külön hozzájárul a további adatkezeléshez	
Személyes azonosító adatok	Személyi dossziéban, papír alapon, a pénzügyi osztályon, zárható szekrényben elektronikusan bescannelve /személyi aktába lementve	pénzügyi vezető, pénzügyi munkatársak
Jogviszony adatok	Személyi dossziéban, papír alapon, a pénzügyi osztályon, zárható szekrényben	pénzügyi vezető, pénzügyi munkatársak
Bérszámfejtéshez kötődő adatok	elektronikusan bescannelve /személyi aktába lementve	pénzügyi vezető, pénzügyi munkatársak
Munkaidő adatok (jelenléti ívek)	Személyi dossziéban, papír alapon, a pénzügyi osztályon, zárható szekrényben	pénzügyi vezető, titkárság vezető, pénzügyi munkatársak
Archivált adatok	elektronikusan bescannelve /személyi aktába lementve	pénzügyi vezető, pénzügyi munkatársak
Névjegykártyán megadott adatok (név, email cím, telefonszám, beosztás /munkakör)	Kapcsolattartó személynél, zárható fiókban, elektronikusan titkárságon	titkárság munkatársai és/vagy az a munkavállaló, akinek részére átadásra került
Szerződéses kapcsolattartó személyek, ügyfelek, vendégek adatai (név, email cím, telefonszám, beosztás /munkakör)	Papíralapon (elzárt szekrényben, illetve elektronikusan a titkárságon, szerződéssel érintett területeken)	felhasználói jogosultsághoz kötötten a szerződéssel érintett terület munkatársai
Munkavállalók által megadott /feltöltött adatok (eddigi munkahely, szakmai előélet, fotó, név, titulus, munkakör, szervezeti egységben elfoglalt helye, hobby stb)	Személyi dossziéban, papír alapon, a pénzügyi osztályon, zárható szekrényben	felhasználói jogosultsághoz kötött, pénzügyi osztály kezeli, csak a rendszergazda fér hozzá, önállóan nem végez felhasználói nyilvántartást
Egyéb (chipkártya száma, simkártya leltári számok, riasztókód)	Titkárság vezet külön nyilvántartást a notebook, telefon kiadásról (elektronikusan történik)	rendszergazda, titkárság vezető

Az adatbázisok (informatikai rendszer) mindegyike jelszóval és windows jogosultságkezelési rendszerrel védett, amelynek beállítása megfelel a jelszavak megválasztására vonatkozó biztonsági követelményeknek.

VIII. Az adatok törlése

Az adatok a fentiekben megjelölt időtartamra kerülnek megőrzésre, ezen időtartam elteltét követően külön szabályzat szerint kerülnek törlésre/megsemmisítésre. A papír alapú dokumentumok megsemmisítése jegyzőkönyv felvétele mellett iratmegsemmisítő géppel történik, az elektronikus rendszerben tárolt adatok anonimizálásra ill. jegyzőkönyv felvétele mellett törlésre kerülnek a rendszergazda által.

IX. Adatbiztonság garantálása

A Társaság által kezelt személyes adatokat a Társaság elektronikus formában és/vagy papír alapon is tárolja. Az adatok biztonsága érdekében a Társaság megfelelő szervezeti és technikai intézkedéseket alkalmaz. A

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

A Társaság minden szükséges biztonsági lépést, szervezési és technikai intézkedést megtesz a személyes adatok legmagasabb szintű biztonsága, illetve azok jogosulatlan megváltoztatásának, megsemmisítésének és felhasználásának megakadályozása érdekében.

A Társaság minden szükséges intézkedést megtesz az adatintegritás biztosítása érdekében, azaz az általa kezelt és/vagy feldolgozott személyes adatok pontossága, teljessége, valamint naprakész állapota érdekében.

A Társaság az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés, sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az elektronikus formában tárolt adatok a szerverszolgáltatók, mint adatfeldolgozók szerverén, valamint a Társaság székhelyén található megfelelően védett hardver eszközökön kerülnek rögzítésre. Az elektronikusan tárolt adatok biztonsága érdekében alkalmazott további szervezeti és IT biztonsági intézkedéseket az IT Biztonsági Szabályzat (IBISZ) tartalmazza.

A Társaság a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el az adatvesztést.

A Társaság által használt számítógépek, munkaállomások jelszóval védettek, a dokumentumokhoz a hozzáférés jogosultságkezelési szabályok alapján korlátozott. A Társaság valamennyi számítógépes rendszere a kártékony szoftverek elleni védelemmel van ellátva.

A személyes adatokat tartalmazó papír alapú dokumentumok külön irattári szabályok szerint kerülnek lefűzésre. A személyes adatokat tartalmazó mappákat zárható szekrényben tároljuk. A fizikai irattároló helyiség a víz-, tűz- és behatolásvédelem biztosított. Az irodaterületre való belépések körében alkalmazott biztonsági intézkedéseket a Biztonsági Szabályzat tartalmazza.

Az adatbiztonság követelményének érvényesüléséről az Adatkezelő a jelen Szabályzattal, illetve külön utasításokkal, szabályzatokkal gondoskodik. Az Adatkezelő gondoskodik arról, hogy a jelen Szabályzat, valamint a külön utasítások és szabályzatok mindenkor hatályos tartalmát a munkavállalói, illetve érdekkörében eljáró harmadik személyek (így különösen az adatfeldolgozók) megismerjék, és ezeknek megfelelően járjanak el.

X. Adatfeldolgozók igénybevétele

A Társaság a működése biztosítása érdekében különböző szolgáltatásokat vesz igénybe (pl. szerverszolgáltató, könyvelő, IT szolgáltató stb.). Az ilyen szolgáltatások gyakran járnak együtt személyes adatok kezelésével. Ilyen szolgáltatások igénybevétele esetén a Társaság adatkezelőnek, a szolgáltató pedig adatfeldolgozónak minősül.

A Társaság kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit GDPR, valamint az adatkezelésre vonatkozó külön törvények keretei között az Adatkezelő határozza meg, azaz a Társaság határozza meg az adatfeldolgozó(k) számára, hogy milyen adatokkal milyen műveleteket hajtsanak végre. Az adott utasítások jogszerűségéért az Adatkezelő felel.

Az adatfeldolgozó az Adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót.

Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni, illetve szükség esetén törölni.

Az adatfeldolgozásra vonatkozó megállapodást írásba kell foglalni, melyben meg kell határozni legalább adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő GDPR szerinti kötelezettségeit és jogait, valamint felelősségét. Az adatfeldolgozói megállapodás mintát a jelen Szabályzat 2. számú melléklete tartalmazza.

A vonatkozó jogszabályi rendelkezés szerint adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

A Társaság által igénybe vett adatfeldolgozók részletes adatait a 3. sz. melléklet tartalmazza és az V. pontban minden egyes adatkezelés esetén a „Címzettek" oszlopban röviden meghatározásra kerül az adott adatkezeléshez kapcsolódó adatfeldolgozó kategóriája (az általa nyújtott szolgáltatás megjelölése útján).

XI. Ellenőrzés

1.1. Az adatvédelemmel kapcsolatos előírások, így különösen ezen szabályzat rendelkezéseinek betartását a Társaságnál adatkezelést végző szervezeti egység vezetői folyamatosan kötelesek ellenőrizni.

1.2. A Társaságnál a kezelt adatok ellenőrzését a vezérigazgató és az általa megbízott adatvédelmi tisztviselő minimum évente egyszer ellenőrzi.

XII. Az adatvédelmi incidens

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidens megfelelő tartalmú és megfelelő időben történő intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek (és ezzel közvetve az Adatkezelőnek). Ilyen károk lehetnek többek között a személyes adataik feletti rendelkezés elvesztése (arra jogosulatlanok hozzáférnek az adatokhoz, és nem lehet tudni, hogy később mire használják fel), a pénzügyi veszteség (pl. bankkártya adatok lopása), a jó hírnév sérelme, védett üzleti információk kiszivárgása stb.

A Társaság mindenkor a megfelelő eljárásokat alkalmazza a Társaság a személyes adatok kiszivárgásának kiszűrésére, jelentésére és kivizsgálására, az adatvédelmi incidensek esetén való eljárást külön belső szabályzat rögzíti.

Az Adatkezelő - az adatvédelmi tisztviselő útján - az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az Érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett

személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatvédelmi incidens esetén a Társaság a felügyeleti hatóságot, illetve az Érintetteket a jogszabályban előírtak szerint értesíti.

XIII. Az Érintettek jogai

Az Érintettek jogai a következők:

1) az érintettek hozzáférési joga

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- az adatkezelés céljai;
- az érintett személyes adatok kategóriái;
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- történik-e automatizált döntéshozatal, illetve profilalkotás;
- ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozó megfelelő garanciákról.

Amennyiben tehát Ön szeretné tudni, hogy a Társaság kezeli-e a személyes adatát, és ha igen akkor milyen körülmények között, akkor erről tájékoztatást kérhet.

A Társaság az adatkezelés tárgyát képező személyes adatok másolatát igény esetén az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért adminisztratív díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

2) a helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Kérjük, amennyiben bármilyen személyes adata megváltozik, ezt jelezze, hogy az adatot javíthassuk a nyilvántartásunkban.

Az Adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatást ad ezen címzettekről.

3) a személyes adat törléséhez való jog (elfeledtetéshez való jog)

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték (megvalósult az adatkezelés célja);
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az adatkezelés jogalapja az adatkezelő jogos érdeke és az érintett tiltakozik az adatkezelések ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett tiltakozik a közvetlen üzletszerzést célzó adatkezelés ellen;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell (pl. ha hatóság előírja).

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt a fentiek szerint azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az Adatkezelő nem köteles az adatokat törölni, ha az adatkezelés szükséges

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

Az Adatkezelő minden olyan címzettet tájékoztat a törlésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatást ad ezen címzettekről.

Amennyiben tehát Ön úgy gondolja, hogy a törlés feltételei fennállnak, úgy bármikor kérheti az adatai törlését.

4) adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát (tehát amíg nem nyer bizonyosságot, hogy a kezelt adatok helyesek);

- az adatkezelés jogellenes, az érintett azonban ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását (mert utóbb esetleg az adatkezelés jogszerűvé tehető és akkor nem kell újra felvenni az adatokat);
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett tiltakozott a jogos érdeken alapul adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az Adatkezelés a fentiek szerint korlátozásra kerül, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy fontos közérdekéből lehet kezelni. Az adatkezelés korlátozásának feloldásáról az adatkezelő az érintettet előzetesen tájékoztatja.
Az Adatkezelő minden olyan címzettet tájékoztat a korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatást ad ezen címzettekről.

Ha Ön kéri az adatkezelés korlátozását, úgy a kérelmének helyt adó döntés esetén az adatkezelési jog kizárólag arra terjed ki, hogy tároljuk az Ön adatait, és azokat csak az Ön hozzájárulásával, vagy jogi igény érvényesítése céljából kezeljük.

5) <u>tiltakozáshoz való jog</u>

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekből történő, vagy érdeken alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.
Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik (pl. marketing, hírlevél stb.) az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Ha tehát az adatkezelés jogalapja a Társaság jogos érdeke, akkor Ön bármikor tiltakozhat az adatai kezelése ellen.

6) <u>az automatizált döntéshozatal és profilalkotás megakadályozása</u>

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.
A fentiek nem alkalmazandók abban az esetben, ha a döntés:
- az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- az érintett kifejezett hozzájárulásán alapul.

7) <u>az adathordozhatósághoz való jog</u>

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha az adatkezelés jogalapja az érintett hozzájárulása vagy szerződés teljesítése, és az adatkezelés automatizált módon történik.
Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

Ha tehát az adatkezelésre az Ön hozzájárulása alapján, vagy szerződés teljesítése érdekében kerül sor, és az adatok automatizáltan kerülnek feldolgozásra, úgy Ön kérheti, hogy elektronikusan bocsássuk az Ön vagy az Ön által meghatározott személy rendelkezésére az adatokat.

Az Érintettek fenti jogaik gyakorlására vonatkozó nyilatkozatukat az alábbi módokon terjeszthetik elő:

- **postai úton a 9400 Sopron, Új utca 4. címen, vagy**
- **e-mail útján a titkarsag@sopronfertonzrt.hu email címen.**

A Társaság nem számol fel költséget a kérelmek teljesítése után, és általánosságban véve egy hónap áll rendelkezésre a kérelmek elbírálására és teljesítésére. A megalapozatlan vagy túlzó kérelmek után a Társaság díjat számolhat fel vagy elutasíthatja őket.

Ezenkívül, a Társaságnak egyéb információkkal is kiszolgálja azokat, akik kérelmet nyújtanak be, például az adattárolás időtartamáról, vagy a pontatlan adatok helyesbítésére vonatkozó jogokról.

Az Adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel bizonyos esetekben korlátozhatja az érintettek fentiek szerint meghatározott jogait.

Az érintettek megkereséseiről, és az azokra adott reakciókról az adatkezelő nyilvántartást vezet.

8) <u>A felügyeleti hatósághoz címzett panasz benyújtásának joga</u>

Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR rendelkezéseit.
A panasz tárgyát a felügyeleti hatóság kivizsgálja és ésszerű határidőn belül tájékoztatja a panaszost a vizsgálattal kapcsolatos fejleményekről és eredményekről, különösen, ha további vizsgálat vagy egy másik felügyeleti hatósággal való együttműködés válik szükségessé. A panasz nyomán a felügyeleti hatóság jogosult eljárást kezdeményezni az adatkezelővel szemben.

Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A magyar felügyeleti hatóság pontos elérhetősége a jelen Szabályzat végén kerül feltüntetésre.

9) **Bírósági igényérvényesítés, kártérítés és sérelemdíj**

Az Érintett az adatkezelő, illetve - az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben - az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.
Azt, hogy az adatkezelő (adatfeldolgozó) az előírásoknak megfelel, az adatkezelő, illetve az adatfeldolgozó köteles bizonyítani.

A pert az Érintett - választása szerint - a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja. A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. A perbe az Adatvédelmi Hatóság az érintett pernyertessége érdekében beavatkozhat.

Ha az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni.

Ha az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az Adatkezelőtől sérelemdíjat követelhet.

Az érintettel szemben az Adatkezelő felel az adatfeldolgozó által okozott kárért, és az Adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is.

Az Adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj annyiban, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

XIV. Az adatvédelmi tisztviselő

Mivel a Társaság állami tulajdonban álló, illetve az állami szervek által alapított gazdasági társaságok közfeladatot ellátó szervnek minősül, kötelezett adatvédelmi tisztviselő alkalmazására.

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint az alábbiakban felsorolt feladatok ellátására való alkalmasság alapján a Vezérigazgató jelöli ki.

Az adatvédelmi tisztviselő az Adatkezelő alkalmazottja.

Az Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

Az Adatkezelő támogatja az adatvédelmi tisztviselőt az alábbiakban felsorolt feladatok ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

Az Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai

ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő legfelső vezetésének, azaz a Vezérigazgatónak tartozik felelősséggel.

Az Érintettek a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Az adatvédelmi tisztviselő feladatai, különösen:

a. tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

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

c. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat megfelelő elvégzését;

d. együttműködik a felügyeleti hatósággal;

e. az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,

f. közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

g. ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

h. kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

i. elkészíti és folyamatosan aktualizálja a jelen adatvédelmi és adatbiztonsági szabályzatot;

j. vezeti az adatvédelmi incidensek nyilvántartást;

k. gondoskodik az adatvédelmi ismeretek oktatásáról.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

Az adatvédelmi tisztviselő neve és elérhetőségei:
Kulcsár János, +36/99/951-594, +36/30/887-8566, dpo@sopronfertonzrt.hu

Az adatvédelmi tisztviselő nevét és elérhetőségét az Adatkezelő a felügyeleti hatósággal is közli.

XV. FONTOS ADATOK

ADATVÉDELMI HATÓSÁG ELÉRHETŐSÉGEI

Nemzeti Adatvédelmi és Információszabadság Hatóság
1055 Budapest, Falk Miksa utca 9-11.
Levelezési cím: 1363 Budapest, Pf.: 9.
Telefon: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

A TÁRSASÁG ADATAI ÉS ELÉRHETŐSÉGEI

Elnevezés: Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság
Székhely: 9400 Sopron, Új utca 4.
Adószám: 25891108-2-08
Cégjegyzékszáma: 08-10-001916
Nyilvántartó hatóság: Győr-Moson-Sopron Megyei Törvényszék Cégbírósága
Telefonos elérhetőség: +36 99/951-594
Elektronikus elérhetőség: titkarsag@sopronfertonzrt.hu
Adatkezelő képviselője: Kárpáti Béla Imre
Telefonos elérhetőség: +36 99/951-594
Elektronikus elérhetőség: titkarsag@sopronfertonzrt.hu

Adatvédelmi tisztviselőnk adatai:
Név: Kulcsár János
Postai cím: 9400 Sopron, Új utca 8.
E-mail: dpo@sopronfertonzrt.hu
Telefon: +36/99/951-594; +36/30/887-8566

Mellékletek:

1. Adatfeldolgozók adatai és elérhetőségei nyilvántartása (minta)
2. Adatkezelési hozzájárulás (általános) (minta)
3. Munkavállalói titoktartási nyilatkozat (minta)
4. Titoktartási nyilatkozat (külső szerződő fél) (minta)
5. Adatfeldolgozói megállapodás (minta)
6. Érdekmérlegelési teszt (minta)
7. Adatvédelmi incidensek bejelentésének rendje (útmutató)
8. Adatvédelmi incidens bejelentő formanyomtatvány (minta)

ADATKEZELO MEGNEVEZESE

Cég rövidített neve: Sopron-Fertő Turisztikai Fejlesztő Zrt
Cég székhelye: 9400 Sopron, Új utca 4.
Cégjegyzékszám: 08-10-001916
Adószám: 25891108-2-08
Társaság képviselője: Kárpáti Béla Imre
Telefonszám: +36 99 951-594
E-mail cím:

ÉRINTETTEK KATEGÓRIÁI	ADATKEZELÉS CÉLJA (Munkaügyi, marketing stb..)	SZEMÉLYES ADATOK KATEGÓRIÁI (Név, telefonszám, cím, anyja neve, adóazonosító jele, születési hely és idő stb...)	KEZELT SZEMÉLYES ADATOK FORRÁSA (Érintettől vagy harmadik személytől)	ADATKEZELÉS JOGALAPJA (hozzájárulás, szerződéses kötelezettség teljesítése, jogszabályi kötelezettség teljesítése, adatkezelő jogos érdeke)	TÖRLÉSRE ELŐIRÁNYZOTT HATÁRIDŐK	TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK (Utalás releváns belső szabályzatra)	TÖRTÉNIK-E 3. ORSZÁGBA VAGY NEMZETKÖZI SZERVEZETEK FELÉ ADATTOVÁBBÍTÁS? (Igen/Nem)	TOVÁBBÍTOTT ADATOK FAJTÁJA, FELSOROLÁSA	ADATTOVÁBBÍTÁS CÍMZETTJE, INFORMÁCIÓK, GARANCIÁK	ADATTOVÁBBÍTÁS JOGALAPJA (Ügyanaz, mint F oszlop)	TÖRTÉNIK-E ADATOK MEGKÜLDÉSE ADATFELDOLGOZÓ RÉSZÉRE? (Igen/Nem)	ADATFELDOLGOZÓ (Név, cím, kapcsolattartó neve, e-mail címe és telefonszáma)	ADATFELDOLGOZÁS HELYE (Cím vagy webhely)	ADATFELDOLGOZÁS TECHNOLÓGIÁJA (Kézi vagy elektronial rendszer útján)	ADATFELDOLGOZÁS GYAKORISÁGA (napi, heti, havi stb..)

1. számú melléklet az Adatvédelmi szabályzathoz

ADATKEZELŐ MEGNEVEZÉSE **Cég rövidített neve: Sopron-Fertő Turisztikai Fejlesztő Zrt** **Cég székhelye: 9400 Sopron, Új utca 4.** **Cégjegyzékszám: 08-10-001916** **Adószám: 25891108-2-08** **Társaság képviselője: Kárpáti Béla Imre** **Telefonszám: +36 99 951-594** **E-mail cím: titkarsag@sopronfertonzrt.hu**				
ADATFELDOLGOZÓ(K) NEVE ÉS ELÉRHETŐSÉGEI **Cégnév:** **Székhely:** **Cégjegyzékszám:** **Adószám:** **Képviselő:** **Telefonszám:** **E-mail cím:** **Adatvédelmi tisztviselő neve és elérhetősége (ha van):**	**ADATKEZELÉSI TEVÉKENYSÉG KATEGÓRIÁJA**	**TÖRTÉNIK-E 3. ORSZÁGBA VAGY NEMZETKÖZI SZERVEZETEK FELÉ ADATTOVÁBBÍTÁS? (Igen/Nem, ha igen akkor milyen országba?)**	**HA TÖRTÉNIK 3. ORSZÁGBA VAGY NEMZETKÖZI SZERVEZETEK FELÉ ADATTOVÁBBÍTÁS TOVÁBBÍTOTT ADATOK FAJTÁJA, FELSOROLÁSA**	**HA TÖRTÉNIK 3. ORSZÁGBA VAGY NEMZETKÖZI SZERVEZETEK FELÉ ADATTOVÁBBÍTÁS ADATTOVÁBBÍTÁS CÍMZETTJE, INFORMÁCIÓK, GARANCIÁK**

HOZZÁJÁRULÁS _____

Alulírott ..... (lakcím:.....; anyja neve:.....; születési helye és ideje:..... – „**Érintett**"), mint a _____ **Korlátolt Felelősségű Társaság** (székhelye: _____., – „**Társaság**") _____ kijelentem, hogy visszavonhatatlanul engedélyezem, hogy a Társaság az alábbiak szerint kezelje a jelen hozzájáruló nyilatkozatomban foglalt személyes adataimat:

_____

Engedélyezem, hogy a Társaság az így kezelt személyes adataimat az alábbi célokból felhasználhassa ellentételezés nélkül:

_____

A Társaság köteles biztosítani, hogy személyes adataim a jelen hozzájáruló nyilatkozatban foglaltaktól eltérő célból ne kerüljenek felhasználásra.

Hozzájárulok ahhoz, hogy a jelen hozzájáruló nyilatkozatomban foglalt személyes adataimat a Társaság és megbízottjai az itt meghatározott céljából az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény rendelkezéseinek, valamint az Európai Parlament és a Tanács (EU) 2016/679 rendeletének megfelelően kezelje, tárolja és adatfeldolgozóhoz továbbítsa.

Kijelentem, hogy a jelen nyilatkozatot megfelelő tájékoztatás után, szabad akaratomból, minden kényszer és fenyegetéstől mentesen írtam alá. Nincs tudomásom olyan körülményről, aminek ismeretében a jelen nyilatkozatot nem, vagy más tartalommal írtam volna alá.

Sopron, 202 _____ napján

_____
Név:
Beosztás

TITOKTARTÁSI NYILATKOZAT

Alulírott, ... (születési hely: ....., születési idő: .....) ..... szám alatti lakos, mint a Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zrt. munkavállalója, (cím: 9400 Sopron, Új utca 4., Cg.08-10-001916) [a továbbiakban: Munkavállalója]

k i j e l e n t e m ,

hogy tudomással bírok a Munkáltatómnál fennálló munkaviszonyommal kapcsolatban engem terhelő **titoktartási kötelezettség**emről, valamint ennek jogkövetkezményeiről.

Kijelentem, hogy a munkáltató adatkezelési szabályzatát és a személyes adatok kezelésére vonatkozó belső utasításokat megértettem, és tudomással bírok arról, hogy köteles vagyok a munkavégzésem során a személyes adatok, az üzleti titok és a bizalmas kezelésű adatok kezelésére alkalmazni és érvényesíteni az adatkezelési szabályzat és utasítások rendelkezéseit.

Erre figyelemmel elismerem, hogy az alábbi kötelezettségek terhelnek:

Tudomásul veszem, hogy a munkavégzésem során tudomásomra jutott **üzleti titok a Munkáltató tulajdonát képezi**. Jelen nyilatkozat vonatkozásában **üzleti titoknak értendő** minden olyan a Munkáltatónál szerzett ismeret, amely publikus forrásból nem beszerezhető (adat, információ, „know how", megoldás, fénykép, felvétel, üzleti kapcsolatok, munkaviszonyra vonatkozó információk (leszámítva saját munkaviszonyomra vonatkozó egyes konkrét adatok speciális esetét), valamint a munkaviszonyom során általam kezelt személyes adatok). Üzleti titoknak minősül továbbá a Munkáltató gazdasági tevékenységéhez kapcsolódó minden olyan információ, vagy adat, amelynek titokban maradásához Munkáltatómnak méltányolható érdeke fűződik. E kötelezettség körébe esik a munkabér és egyéb járandóságok mértéke is, a munkahelyi munkatársakra is kiterjedően. (A megjelölt kompenzációk mértéke titoknak tekintendő, melynek együttes titokgazdája a munkáltató és a munkavállaló. A munkabérre vonatkozó információt a munkáltató kívánságára titokban kell tartani, a munkavállaló azonban egyedi esetben tudomására hozhatja más, egyedileg meghatározott személynek vagy személyek körének, amennyiben az konkrét, jogos érdekének, illetve érdekérvényesítési lehetőségeinek csorbításához vezethetne. Ehhez azonban szükséges, hogy legyen a munkavállalónak olyan konkrét érdeke, amely legitimálja a munkabérére vonatkozó információnak a mások számára való hozzáférhetővé tételét.

Minden olyan tényt bizalmasan kell kezelnem, amely a munkaviszonyommal kapcsolatos működésem során jut tudomásomra, tekintet nélkül arra, hogy erre külön figyelmeztetnének vagy a figyelmeztetés elmaradna. Tudomásul veszem, hogy erre a munkáltatómmal kialakult bizalmi viszony munkaszerződésemnél fogva minden további szabályozás vagy nyilatkozat nélkül is elvárható szinten kötelez.

Fokozott figyelemmel vagyok köteles az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETÉT 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 (általános adatvédelmi rendelet- a továbbiakban GDPR) rendelkezéseinek betartására a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek végzése közben, 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 vonatkozásában.

Kötelezettséget vállalok arra, hogy az informatikai biztonsági, azon belül kiemelten az adatbiztonsági előírásokat betartom; adatokat elektronikusan kizárólag a Munkáltató tulajdonát képező adathordozókon tárolok, azok védelmét biztosítom. Kötelezettséget vállalok arra, hogy adatokat illetéktelen személyek részére sem papíralapon, sem elektronikus formában nem továbbítok. Tudomásul veszem, hogy nem megengedett az elektronikus adatok mentése olyan adattárolóra, mely nem a Munkáltató tulajdonát képezi.

A Munkáltató jogos érdekének védelmében az Mt. 8. § (4) bekezdése alapján a tudomásomra jutott üzleti titkot a Munkáltatóra és üzleti partnereire vonatkozóan ill. minden személyes adatot köteles vagyok bizalmasan kezelni és megőrizni. Az üzleti titok védelme kiterjed a munkaviszony idejére, valamint annak megszűntét követően korlátlan ideig, azaz az üzleti titok voltának megszűnéséig. Felelősséggel tartozom a közeli hozzátartozóimnak (Ptk. 8:1. §) titoksértő magatartásáért is.

Tartózkodom minden olyan magatartás tanúsításától a munkaviszony fennállása alatt, mellyel a Munkáltatóm jogos gazdasági érdekeit veszélyeztetném (Mt.8.§./1-3/bek.).

Tudomással bírok arról, hogy munkaidőmön kívül sem tanúsíthatok olyan magatartást, amely munkáltatóm jó hírnevének, jogos gazdasági érdekének veszélyeztetésére alkalmas lenne.

Véleménynyilvánításhoz való jogomat a munkáltató jó hírnevét, jogos gazdasági érdekét és szervezeti érdekeit súlyosan sértő vagy veszélyeztető módon nem vagyok jogosult gyakorolni (Mt.8. § (1)-(3) bek.).

Tudomással bírok arról is, hogy amennyiben a Munkáltatóm üzleti titkait ill. természetes személyek személyes adatait jogosulatlanul megszerzem, kifürkészem, felhasználom, felfedem, hozzáférhetővé teszem és/vagy nyilvánosságra hozom, az információs rendszer védelmét biztosító technikai intézkedést kijátszom, az információs rendszert vagy adatot megsértem, úgy akár a Btk. 223-224.§. ill. 418.§, 422., 423, 424. § szerinti bűntettet követem el, továbbá, hogy kötelezettségeim megszegése esetén a Munkáltatóm velem szemben kártérítési igény érvényesítésére jogosult.

Minden olyan esetben továbbá, amely során az üzleti titkot és/vagy személyes adatot nem a Munkáltató mindenkor hatályos Adatvédelmi és Adatkezelési Szabályzatában, illetve bármely egyéb belső szabályzatában, továbbá a jogszabályi rendelkezésekben meghatározottak szerint kezelem, önálló

adatkezelővé válok, az adatkezelésre vonatkozó jogok és kötelezettségek teljesítése során a Munkáltató helyére lépek és egyben a legtöbb esetben megvalósítom az Mt. 78. § (1) a) szerinti azonnali hatályú felmondás jogalapját. (Nem objektív a munkavállalói felelősség, nem áll be automatikusan az azonnali hatályú felmondás jogalapja. A munkáltatónak erre külön kell intézkednie, azután, hogy kivizsgálta és elbírálta a munkavállaló magatartását, amelynél a szándékosság és a súlyos gondatlanság tekinthető felmondási alapnak).

Az üzleti titok megsértéséből, illetve a személyes adatkezelésre vonatkozó előírások megszegéséből eredően a Munkáltató minden kárát haladéktalanul és teljes összegben megtéríteni tartozom (Szándékos vagy súlyosan gondatlan károkozás esetén a teljes kárt meg kell téríteni. Gondatlan károkozás esetén a Mt. 4 havi távolléti díj erejéig ír elő kártérítést. A haladéktalanul és teljes összegben kitételnél a munkáltatónak figyelemmel kell lennie a realitásokra, pl. a dolgozó jövedelmi viszonyaira. A kártérítési kötelezettség mértéke jogi kérdés és nem ténykérdés; megállapításának legfőbb célja, hogy a károkozó a kötelezettségének objektíve képes legyen eleget tenni). Amennyiben a Munkáltató az üzleti titok megsértéséből ill. a személyes adatkezelésre vonatkozó előírások megszegéséből eredő kárát nem kívánja tételesen bizonyítani, úgy átalánykárként vélelmezni kell az utolsó havi alapbéremnek három évre vetített összegét, és ezt az összeget tartozom kötbérként megtéríteni. A kötbér mérséklésére bírósági eljárásban van lehetőség.

A jelen nyilatkozat a Munkáltatóm részére, a titokvédelemmel ill. adatvédelemmel kapcsolatos eljárás során történő felhasználás céljából került kibocsátására.

Kelt: Sopron, 202.....

.....

.....

Munkavállaló

Előttünk, mint tanúk előtt:

Név:	Név:
Lakcím:	Lakcím:
Aláírás:	Aláírás: .....

4. számú melléklet az Adatvédelmi nyilatkozathoz

Titoktartási nyilatkozat

Mely alapján

Név/Cégnév:
Lakhely/Székhely:
Személyi igazolványszám/Cégjegyzékszám:
-/Képviselő neve, beosztása:
a továbbiakban mint „**Titoktartásra kötelezett**"

kötelezettséget vállal az

Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zrt. felé
Székhely: 9400 Sopron, Új utca 4.
Cégjegyzékszám: Cg. 08-10-001916
Adószáma 25891108-2-08
továbbiakban mint „**SFTF Nzrt.**"

(Titoktartásra kötelezett és SFTF Nzrt. a továbbiakban együttesen „**Felek**")

az alábbi nyilatkozat tételével

I.
Fogalmak

1. Jelen Titoktartási nyilatkozat alapján Titoktartásra kötelezettnek minősül, a partner, mely hatályos megbízás, szerződés alapján vagy annak előkészítése során, vagy egyéb módon az SFTF Nzrt.-vel együttműködik vagy az SFTF Nzrt. által meghirdetett pályázati eljárásban vesz részt (továbbiakban: „**Együttműködés**").

2. Titoktartásra kötelezett továbbá az is, aki az SFTF Nzrt. valamely szakterületével már fennálló vagy előkészületben lévő üzleti kapcsolat; már megvalósult vagy készülő együttműködés során, az SFTF Nzrt. területén tett látogatás alkalmával, valamint egyéb módon az SFTF Nzrt.-re vonatkozó üzleti titok birtokába jutott.

3. **Üzemi-, ill. üzleti titok** kiterjed különösen minden bizalmas kezelést igénylő, gazdasági és személyekre vonatkozó, valamint fejlesztési-, kutatási-, tervezési- és intézkedésekkel kapcsolatos adatra, ajánlatokra, azokra adott válaszra, dokumentációra, egyéb megkeresésre, ill. minden ezekkel összefüggő eljárásra, így különösen minden szóbeli vagy írásos úton megszerzett bizalmas információra, ismeretre, munkaeredményre, szakvéleményre, mintákra, rajzokra, nem széria járművekre és jármű-alkatrészekre, technikai folyamatokra és egyéb technikai ismeretekre, számítógépes modellezésekre, adatokra, adattárakra, a nem nyilvánosan, csupán meghatározott kör számára (pl. szállítók) hozzáférhető internetoldalakról származó információkra, a SFTF Nzrt.-nél szokásos üzleti, ipari és egyéb eljárásokra, az adattárolás formáira és annak biztosítottságára, továbbá Hardware-, ill. Software adatokra.

4. **Bizalmas** minden, az SFTF Nzrt.-vel való együttműködés, annak előkészítése, illetve pályázati eljárás során, vagy az SFTF Nzrt. által adott megbízás alapján létrejövő, vagy annak során keletkezett információ, vagy dokumentum, továbbá az előzetesen a pályázó tudomására jutott ismeret, valamint minden, AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE 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 (általános adatvédelmi rendelet), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII tv. (továbbiakban Adatvédelmi tv.) rendelkezései szerint meghatározott személyes adat.

II.
Titoktartási kötelezettség

1. A Titoktartásra kötelezett köteles a fentiekben meghatározott Üzemi- és üzleti titkot, illetve bizalmas információt szigorúan bizalmasan kezelni.

2. A Titoktartásra kötelezett kötelezettséget vállal arra, hogy üzleti titkot, bizalmas információt nem tesz hozzáférhetővé harmadik személy számára, azt kizárólag a szerződésben, pályázati kiírásban előirányzott cél érdekében, az együttműködéshez szükséges mértékben („need-to-know" alapon) használja fel, és megtesz minden, ezen titoktartási megállapodás előírásainak megfelelő intézkedést, az adatkezelés bizalmas jellegének biztosítására.

   Fenti meghatározás magában foglalja különösen a következőket:
   - nem ad felvilágosítást harmadik fél számára a megszerzett információkról, és/vagy az együttműködés módjáról, ill. körülményeiről;
   - szerződés, pályázat tárgyát képező munkafolyamatban illetéktelen harmadik személy számára nem nyújt betekintést a munkavégzés módjára, ill. körülményeire vonatkozóan;
   - különösen tartózkodik a Társaság médiastratégiájával, reklám-, propaganda-, promóció és marketing ügyeinek kiszivárogtatásától, nyilvánosságra hozatalától, illetéktelenekkel történő részleges és teljes megismertetésétől, médiaszereplésen és interjún keresztül is;
   - adatkezeléshez, ill. adatok elektronikus adathordozón történő megőrzéséhez (pl. PC, Laptop), valamint adattovábbításhoz megfelelő biztonsági előkészületeket kell tenni, a vállalati Informatikai biztonsági irányítási szabályzatot (a továbbiakban: IBISZ), a biztonsági szabályzat vonatkozó fejezeteit ebben a vonatkozásban is be kell tartani, melyek kizárják harmadik személynek az adatokhoz való hozzáférését; SFTF Nzrt. szokásos eljárása esetén ebből a célból az elektronikus leveleket arra alkalmas titkosítással kell ellátni;
   - a székhely és telephely területén csak a kijelölt, ill. az átvett munka teljesítéséhez tervezett út-, terület-, és épületrészekre megengedett a belépés, az adott telephelyrész működéséért felelős dolgozó utasításait figyelembe kell venni és be kell tartani;
   - a vagyonkezelés alatt álló és bérelt terület egészére kiterjedő hang-, ill. képrögzítési tilalom áll fenn (fénykép-, film-, videó- vagy mágneses képrögzítő készülék), és semmilyen arra alkalmas készüléket nem lehet fent említett területekre bevinni. Kivétel gyakorlására az SFTF Nzrt. illetékes vezetőjének írásbeli engedélyével kerülhet sor. E tekintetben illetékes vezetőnek a helyszínen a vezérigazgató vagy a médiaigazgató minősül, kivéve abban az esetben, ha a felvétel készítője érvényes, írásos riportkészítési, illetve felvételkészítési engedéllyel rendelkezik.

3. A Titoktartásra kötelezett kötelezettséget vállal a bizalmasan kezelendő információk biztonságos megőrzésére. Az együttműködés befejeztével az írásos információkat, ill. a titoktartási kötelezettség tárgyát képező információkat, dokumentumokat teljes egészében vissza kell szolgáltatni, ill. át kell adni az SFTF Nzrt. részére, vagy a megegyezés alapján meg kell semmisíteni. A megsemmisítés kizárólag az SFTF Nzrt. székhelyén, a Titkárságvezető jelenlétében történhet meg.

4. A Titoktartásra kötelezett kötelezettséget vállal arra, hogy az SFTF Nzrt. adatait és rendszereit érintő eljárások során az IT biztonsági cselekvéseinek rendszerfejlesztőkre, rendszerüzemeltetőkre és rendszer-adminisztrátorokra, valamint partnercégek IT vonatkozású vezérelveit (melyek a társasági IBISZ-ben találhatók) figyelembe veszi és betartja.

III.
Kívülálló harmadik személyek

A jelen Titoktartási nyilatkozat szerint nem minősül kívülálló harmadik személynek a Miniszterelnöki Kabinetiroda és Államtitkárságai, valamint pályázati támogatás szempontjából a Lechner Tudásközpont Nonprofit Kft, a Magyar Turisztikai Ügynökség, illetve fentiek szervezetileg alárendelt egységei.

IV.
Közismert adatok

Nem vonatkozik titoktartási kötelezettség olyan információkra és titoktartási kötelezettség alá eső olyan bizalmas információkra, amelyek Titoktartásra kötelezett igazolása alapján:

- már az információk átadásakor köztudomásúvá váltak, tehát nyilvánosságra hozták, vagy általánosan hozzáférhetővé tették őket
- már az átadás pillanatában általánosan ismertek voltak
- jogszabályi kötelezettség vagy jogerős bírósági vagy hatósági határozat alapján nyilvánosságra hozandók.

V.
Dolgozók, teljesítési segédek, közreműködők

1. A Titoktartásra kötelezett köteles gondoskodni arról, hogy minden, az együttműködés során foglalkoztatott dolgozója, teljesítési segédje betartsa az SFTF Nzrt. titoktartásra vonatkozó alapelveit, ill. az Adatvédelmi törvény (2011. évi CXII. tv.) rendelkezéseit.
   A Titoktartásra kötelezett munkavállalóival, ill. teljesítési segédekkel kötött megfelelő írásbeli megállapodás alapján kötelezettséget vállal arra, hogy azok jelen titoktartási nyilatkozatban meghatározott rendelkezéseket magukra kötelezőnek ismerik el vagy a velük megkötött szolgáltatási, ill. megbízási szerződés alapján titoktartásra kötelezettek.

2. Titoktartásra kötelezett az SFTF Nzrt. vezérigazgatója igényére köteles megnevezni az általa megbízás keretében foglalkoztatott dolgozóit.

VI.
Alvállalkozók

Amennyiben a Titoktartásra kötelezett a szerződésből eredő kötelezettségei teljesítéséhez jogosan alvállalkozókat vesz igénybe, jelen szerződés rendelkezéseinek megfelelően írásos formában kötelezi őket. A további kötelezettek bevonásáról mindenekelőtt az SFTF Nzrt.-t kell haladéktalanul tájékoztatni. Személyes adatok feldolgozásához az SFTF Nzrt. írásos hozzájárulása és adatfeldolgozói szerződés megkötése szükséges.

VII.
Megsértés következményei

1. A titoktartási kötelezettség megsértése súlyos szerződésszegésnek minősül; a Titoktartásra kötelezett teljeskörűen felel az SFTF Nzrt.-nél ebből eredően keletkezett károk megtérítéséért. A SFTF Nzrt. fenntartja továbbá a jogot, hogy ebben az esetben azonnali hatállyal felmondja a szerződést, ill. megszüntesse az együttműködést, illetve a pályázót a pályázati eljárásból kizárja.

2. A Titoktartásra kötelezett a munkavállalói, teljesítési segédei és alvállalkozói magatartásáért teljes felelősséggel tartozik.

3. Az SFTF Nzrt. kifejezetten felhívja a Titoktartásra kötelezett figyelmét, hogy az SFTF Nzrt. a polgári jogi igényeinek érvényesítése mellett azonnali büntetőfeljelentéssel él abban az esetben, amennyiben a titoktartási kötelezettség be nem tartása büntetőjogi tényállást is megvalósít.

4. A titoktartási kötelezettségnek a Titoktartásra kötelezett általi megsértése esetén – a fentiekben foglalt szankcióktól függetlenül - minden egyes esetben a jelen titoktartási szerződéshez kapcsolódó megállapodásban rögzített díj/szerződésteljesítési összeg 30%-át kitevő összegű szerződésszegési átalány-kártérítés fizetendő a Titoktartásra kötelezett által az SFTF Nzrt. részére. Az SFTF Nzrt. fenntartja a jogot az átalány-kártérítésen felül keletkezett kárának érvényesítésére. A titoktartási kötelezettségnek a Titoktartásra kötelezett általi legalább gondatlan megszegése esetén SFTF Nzrt. jogosult azonnali hatállyal felmondani a szerződést, illetve az Együttműködést megszüntetni.

VIII.
Igazolványok, Kulcsok, Elektronikus aláírások

1. Amennyiben a Titoktartásra kötelezett, ill. teljesítési segédei, közreműködői vagy munkavállalói az együttműködés érdekében az SFTF Nzrt. által kiállított igazoló iratot, belső használatú igazolványt, kulcsot, RFID azonosítót vagy elektronikus kódot kapnak, ezeket az együttműködés befejeztével, ill. a Titoktartásra kötelezett mindenkori munkavállalóinak, teljesítési segédeinek, közreműködőinek a teljesítésből, együttműködésből történő kiválásával haladéktalanul vissza kell juttatni az SFTF Nzrt. részére. Fentiekről az SFTF Nzrt. nyilvántartást vezet, melynek személyi adatait a Titoktartásra kötelezett, illetve teljesítési segédei, közreműködői vagy munkavállalói önként szolgáltatják, a visszajuttatás időtartamáig.

2. Igazolvány, kulcs, elektronikus kód elvesztését haladéktalanul jelenteni kell a Titkárságon a mindenkori Adatvédelmi Tisztviselőnek (DPO). Igazolvány, kulcs stb. elvesztése esetén az SFTF Nzrt. Biztonsági Szabályzata szerinti átalány-kártérítés alkalmazandó. Az átalány-kártérítés összege 10 000 Ft + bekerülési költség.

IX.
Jogok és engedélyek

A rendelkezésre bocsátott dokumentumokkal és a titoktartási kötelezettség alá eső tárgyakkal kapcsolatos minden jog az SFTF Nzrt.-t illeti, különös tekintettel a találmányokkal kapcsolatos szerzői és iparjogvédelmi jogokra. A dokumentumok és tárgyak átadása nem jár együtt a jogok és engedélyek átruházásával.

X.
Hatálybalépés, hatály

A titoktartási nyilatkozat az aláírásával lép hatályba és az együttműködés befejezését, illetve a pályázati eljárás eredményének kihirdetését követő 5 évig marad hatályban.

XI.
Általános rendelkezések

1. A titoktartási nyilatkozatra vonatkozó módosítások és az azzal kapcsolatos kiegészítések írásbeli formában érvényesek. Szóbeli kiegészítő megállapodások megkötésére nem került sor.

2. Amennyiben jelen titoktartási nyilatkozat egyes rendelkezései hatálytalanná/érvénytelenné válnak, vagy érvényességüket/joghatályukat később elvesztik, ez a körülmény nem érinti szerződés fennmaradó rendelkezéseinek hatályát/érvényességét. A hatálytalan/érvénytelen rendelkezések helyett SFTF Nzrt. olyan hatályos/érvényes rendelkezéseket határozhat meg, melyek lehető legközelebb állnak a hatálytalan/érvénytelen rendelkezések céljához.

3. Jelen nyilatkozatban nem szabályozott kérdésekben a magyar jog szabályai irányadóak. Jelen nyilatkozatból eredő bármely jogvita elbírálására a Felek kikötik a tárgyi hatáskörrel rendelkező soproni székhelyű bíróság illetékességét.

Kelt / Sopron, 202_____

.....
Cégnév
Képviselő neve, beosztása

5.számú melléklet az adatvédelmi szabályzathoz

ADATFELDOLGOZÓI MEGÁLLAPODÁS

amely létrejött

Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zrt., (cím: 9400 Sopron, Új utca 4., Cg.08-10-001916, a továbbiakban:" Megbízó" vagy **„Adatkezelő"**) és

[*],([*], Cg. [*] a továbbiakban: „**Szerződő Fél**" vagy **„Adatfeldolgozó"**) között, az alábbiak szerint.

Tekintettel arra, hogy a [*] szerződéssel személyes adatok átadása/ továbbítása történik a Szerződő fél irányába, a Szerződő Felek a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló, az **EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE** (a továbbiakban: Rendelet) előírásai alapján az alábbiakról állapodnak meg:

1. A Szerződő Felek rögzítik, hogy szerződéses kapcsolatuk során, a [*] szerződés (a továbbiakban: Szerződés) teljesítése érdekében a Megbízó, mint adatkezelő az alábbi személyes adatokat adja át a Szerződő fél, mint adatfeldolgozó részére:

Érintettek kategóriái	Személyes adatok[1] típusa	Adatkezelés tárgya	Adatkezelés jellege	Adatkezelés célja	Adatkezelés időtartama

Szerződő fél az alábbi adatfeldolgozási műveleteket végzi:

-
-
-

2. Szerződő Fél kötelezi magát, hogy a részére átadott személyes adatokat **jogszerűen és tisztességesen, és egyedül csak a fenti 1. pontban rögzített Szerződéssel összefüggésben a szükséges mértékben; és (ii) a Adatkezelőtől időről időre kapott dokumentált utasításoknak megfelelően kezeli.**
3. Szerződő Fél a Rendeletnek való megfelelés bizonyítása érdekében **nyilvántartást vezet** a hatásköre alapján végzett adatfeldolgozási tevékenységekről és ezeket a nyilvántartásokat az arra jogosult kérésére **hozzáférhetővé tenni** az érintett adatkezelési műveletek ellenőrzése érdekében.
4. Szerződő Fél a Megbízó **előzetesen írásban tett eseti vagy általános felhatalmazása nélkül** további adatkezelőt/adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén a Szerződő Fél tájékoztatja a Megbízót minden olyan tervezett változásról, amely további

[1] Személyes adatnak minősül minden, azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

adatkezelő/adatfeldolgozó igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget a Megbízónak arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

5. Szerződő Fél kötelezi magát, hogy a Megbízó által, a [*] szerződés teljesítése érdekében részére átadott személyes adatokat kizárólag a Megbízó **írásbeli utasításai** alapján kezeli, illetve dolgozza fel – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést/adatfeldolgozást a Szerződő Félre alkalmazandó uniós vagy tagállami jog írja elő. Amennyiben az Adatfeldolgozó bármikor képtelenné válik arra, hogy az Adatkezelőnek a vonatkozó személyes adatok kezeléséről szóló utasításainak megfeleljen (akár az alkalmazandó jogszabály akár az Adatkezelő utasításainak változása miatt), az Adatfeldolgozó köteles azonnal (i) tájékoztatni az Adatkezelőt ennek tényéről, és megfelelő tájékoztatást adni arról, hogy mely utasításoknak milyen okból nem tud a GDPR által előírtaknak megfelelni, és (ii) beszüntetni az összes érintett személyes adat kezelését (kivéve, az érintett személyes adatok tárolását és biztonságának fenntartását szolgáló intézkedéseket) mindaddig, amíg az Adatkezelő nem ad olyan új utasítást, amelyeknek az Adatfeldolgozó meg tud felelni.
6. Szerződő Fél biztosítja azt, hogy a nála személyes adatok kezelésére/Feldolgozására feljogosított személyek **titoktartási kötelezettséget vállalnak** vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
7. Szerződő Fél szavatolja, hogy a szolgáltatás-nyújtásával összefüggésben az adatfeldolgozás természetéből fakadó **kockázatokat**[2] **értékelte**, és az e kockázatok csökkentését szolgáló intézkedéseket megtette. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot – ideértve az adatok bizalmas kezelését is –, figyelembe véve a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés –mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.
8. Szerződő Fél szavatolja, hogy a jelen megállapodás tartama alatt fenntartja az **adatbiztonságra** előírt intézkedéseket, azaz

8.1. 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**[3] **és szervezési**[4] **intézkedéseket** hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

---

[2] Kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, a személyes adataik feletti rendelkezés elvesztése vagy a jogaik korlátozása, az álnevesítés engedély nélküli feloldása, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrány, stb.

[3] A személyes adatokat olyan megfelelő technikai védelmi intézkedésekkel kell védeni, amelyek hatékonyan korlátozzák a személyazonossággal való visszaélés vagy a visszaélés más formái előfordulásának a valószínűségét. A természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. A természetes személyek védelme a személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni.

[4] A hatáskörök egyértelmű meghatározásával és felosztásával.

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

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

8.3. Szerződő Fél a személyes adatokat olyan módon kezeli, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását, valamint, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

8.4. Szerződő Fél köteles – bármely arra jogosult kérésére - mindenkor **igazolni** azt, hogy az adatkezelési tevékenységek a Rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is a Rendelet által előírt szintű.

9. Szerződő Fél köteles megfelelő **garanciákat nyújtani** – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – az adatkezelés Rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő **technikai és szervezési** intézkedések végrehajtására.

10. Szerződő Fél az adatkezelés jellegének figyelembevételével megfelelő **technikai és szervezési** intézkedésekkel a lehetséges mértékben segíti a Megbízót abban, hogy teljesíteni tudja kötelezettségét az érintettek a Rendelet III. fejezetében foglalt **jogainak gyakorlásához kapcsolódó kérelmek** megválaszolása tekintetében, azaz Szerződő Fél köteles az érintettek a Rendeletben biztosított jogainak gyakorlását megkönnyítő intézkedéseket biztosítani, ideértve olyan mechanizmusok biztosítását, amely által többek között az érintettnek lehetősége van díjmentesen kérelmezni, illetve adott esetben megkapni különösen a személyes adatokhoz való hozzáférést, azok helyesbítését és törlését, valamint gyakorolja a tiltakozáshoz való jogát.
Ebben a körben Szerződő Fél köteles a rendelkezésére bocsátott, érintettekre vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban (elektronikus úton) Megbízó részére késedelem nélkül, de legkésőbb 10 napon belül továbbítani, ha az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, illetve, ha az adatkezelés szerződés teljesítéséhez szükséges.

11. Szerződő Fél minden elvárható módon **segíti** a Megbízót a Rendelet 32–36. cikk (adatkezelés biztonsága, adatvédelmi incidens bejelentése, érintett tájékoztatása, adatvédelmi hatásvizsgálat és előzetes konzultáció) szerinti kötelezettségek **teljesítésében**, figyelembe véve az adatkezelés jellegét és a Szerződő Fél rendelkezésére álló információkat. Ennek alapján a Szerződő Fél köteles Megbízót az adatvédelmi incidensről indokolatlan késedelem nélkül, de legkésőbb a tudomására

jutásától számított legkésőbb 12 órán belül **írásban tájékoztatni**. A tájékoztatásnak alkalmasnak kell lenni arra, hogy az Adatkezelő az adatvédelmi incidensből eredő kockázatokat mérlegelni tudja. Felek megállapodnak, hogy a tájékoztatásnak minimálisan a NAIH által közzétett adatvédelmi incidens bejelentőlap kötelező tartalmi elelmeit kell tartalmaznia.

12. Szerződő Fél a Megbízó rendelkezésére bocsát minden olyan információt, amely a Rendelet 28. cikkében meghatározott, fentiekben felsorolt kötelezettségek teljesítésének **igazolásához** szükséges, továbbá amely lehetővé teszi és elősegíti a Megbízó által vagy az általa megbízott más **ellenőr által végzett auditokat**, beleértve a **helyszíni vizsgálatokat** is. A Szerződő Fél köteles haladéktalanul tájékoztatni a Megbízót, ha úgy véli, hogy annak valamely utasítása sérti a Rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.
13. Szerződő Fél kijelenti, hogy az általa végzett adatkezelési/adatfeldolgozási műveletek nem járnak magas kockázattal a természetes személyek jogaira és szabadságaira nézve, ezért **adatvédelmi hatásvizsgálat** elvégzése nem szükséges.
14. Szerződő Fél az adatkezelési szolgáltatás nyújtásának befejezését követően a Megbízó döntése alapján, a Megbízó által közölt határidőn belül, minden személyes adatot töröl vagy visszajuttat a Megbízónak, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő.
15. Jelen megállapodásban foglalt elveket minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell, kivéve az anonim információk kezelését, a statisztikai vagy kutatási célú adatkezelést.
16. Szerződő fél nem jogosult a személyes adatok különleges kategóriáit célzó automatizált döntéshozatalra, valamint a profilalkotásra.
17. Ha Szerződő Fél bizonyos, a Megbízó nevében végzett konkrét adatkezelési/adatfeldolgozási tevékenységekhez további harmadik személy szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további harmadik személyre is ugyanazokat az adatvédelmi kötelezettségeket köteles Szerződő Fél **írásban kötött szerződéssel** telepíteni, mint amelyek a Megbízó és a Szerződő Fél között létrejött jelen megállapodásban vagy egyéb jogi aktusban szerepelnek, különösen úgy, hogy a további harmadik személynek megfelelő és igazolt **garanciákat** kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek. Ha a további harmadik személy nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó Szerződő Fél teljes és korlátlan felelősséggel tartozik a Megbízó felé a további harmadik személy kötelezettségeinek a teljesítéséért.
18. Szerződő Felek rögzítik, hogy a Rendelet 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy Szerződő fél a jelen megállapodásban meghatározott követelményeket teljesíti.
19. Szerződő Fél haladéktalanul kártalanítani és a felelősség alól mentesíteni köteles Megbízót mindennemű olyan követelés, felelősség, kártérítés, veszteség, költség és kiadás tekintetében (ide értve az ügyvédi költségek teljes körű megtérítését is), melyet a Megbízó szenved el közvetve vagy közvetlenül a Szerződő Félnek a jelen megállapodásban meghatározott kötelezettségeinek megsértéséből eredő per, követelés vagy eljárás következtében. Ezen kártalanítási és felelősség alóli mentesítési kötelezettség kiterjed az adatvédelmi hatóság által a Megbízóra kiszabott fizetési kötelezettségekre is.

20. Amennyiben a Szerződő Fél a Rendeletet előírásait és/vagy a jelen megállapodást **megsértve,** maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében önálló adatkezelőnek kell tekinteni.
21. Az, hogy Megbízó késedelmesen vagy egyáltalán nem érvényesíti vagy gyakorolja valamely jogát, hatáskörét vagy jogérvényesítési lehetőségét, nem értelmezhető az adott jog korlátozásaként vagy az adott jogról való lemondásként.
22. Ha a jelen megállapodás bármely rendelkezése jogellenes, érvénytelen, kikényszeríthetetlen vagy azzá válik, az a jelen megállapodásban foglalt többi rendelkezés jogszerűségét, érvényességét vagy kikényszeríthetőségét nem befolyásolja, illetve nem akadályozza.
23. Jelen megállapodás bármely rendelkezése kizárólag írásban módosítható.
24. Jelen megállapodás az 1. pontban rögzített, a Felek között létrejött Szerződés tartamával egyező tartamra jött létre, a Szerződés megszűnésével a jelen megállapodás minden további jogcselekmény nélkül megszűnik, és a Szerződő Fél köteles a birtokában levő Megbízói adatokat a Megbízó utasítása szerint a Megbízó részére visszaszolgáltatni vagy ilyen igény esetén törölni. Az elektronikusan kezelt adatokat, listákat, nyilvántartásokat elektronikusan továbbítja az Adatkezelőnek vagy az Adatkezelő által megjelölt harmadik személynek – amennyiben ezek elektronikus fogadására az Adatkezelő nem képes, az adatokat papír alapon (kinyomtatva) adja át az Adatkezelőnek egyidejűleg az Adatkezelőtől származó minden személyes adatot és ezt tartalmazó másolatot töröl a nyilvántartásából.

Szerződő Felek a jelen megállapodást, mint akaratukkal és tényekkel mindenben megegyezőt, jóváhagyólag aláírják, és aláírásukkal elismerik, hogy a jelen megállapodás megkötéséhez szükséges minden felhatalmazással rendelkeznek.

Kelt: [*]

[*]	[*]
Megbízó	**Szerződő Fél**

Érdekmérlegelési Teszt nyomtatvány

Érdekmérlegelési Teszt ..... adatkezeléshez
Jelen Érdekmérlegelési Teszt annak eldöntése céljából került lefolytatásra, hogy a **Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság** rendelkezik-e jogalappal a .....(érintett)..... (személyes adat) kezelésére, az alábbi célból: ..... A GDPR 6. cikkének (1) f) pontja alapján az adatkezelés jogszerű, ha 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. Jelen Érdekmérlegelési teszt során: a **Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság** jogos érdeke azonosításra és értékelésre került meghatározásra került, hogy az adatkezelés feltétlenül szükséges-e a kívánt érdek eléréséhez mérlegelésre került, hogy az érintettek alapvető jogai vagy érdekei felülírják-e az adatkezelő érdekeit megállapításra került, hogy az adatok kezelhetők-e vagy sem
Jogos érdek
A **Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság** jogos érdekét megalapozza: -
Feltétlenül szükséges-e az adatkezelés? Elérhető-e a kívánt cél más eszközökkel?
Az adatkezelés feltétlenül szükséges, mert .....
Az érintettek alapvető jogai és érdekei
Az érintetteknek alapvető joguk a személyes adataik védelméhez való jog. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A személy adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok 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.
További az adatkezelő által alkalmazott garanciák

- -
Következtetés
A jelen Érdekmérlegelési Teszt alapján megállapításra került az, hogy a ..... ZRt. rendelkezik jogos érdekkel arra, hogy..... (érintett) ..... (személyes adat) kezelje az alábbi célból: .....

Kelt: Sopron, 20 .....

Kárpáti Béla Imre
vezérigazgató

Sopron-Fertő Turisztikai Fejlesztő

Nonprofit Zártkörűen Működő Részvénytársaság

Adatvédelmi incidensek bejelentési rendje

Tartalomjegyzék

1 Bevezető

Jelen eljárásrendet abban az esetben kell alkalmazni, amikor olyan incidens történik, amely ténylegesen vagy feltehetően a **Sopron-Fertő Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság** (a továbbiakban: **Társaság**) által adatkezelőként vagy adatfeldolgozóként kezelt adatok megsemmisülését, vagy illetéktelen személyek számára történő kiszivárgását eredményezi.

Az Európai Unió Általános Adatvédelmi Rendelete 2016 (GDPR) előírja, hogy a személyes adatokra vonatkozó olyan eseményeket, amelyek az érintettek jogait és szabadságait veszélyeztethetik, indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával a tudomásszerzést követően be kell jelenteni a felügyeleti hatóságnak. Ha a bejelentés nem történik meg 72 órán belül, meg kell adni a késedelem igazolására szolgáló indokokat is.

Amennyiben egy esemény a személyes adatokat érinti, döntést kell hozni az érintettekkel való kommunikáció mértékéről, időzítéséről és tartalmáról. A GDPR előírja, hogy a kommunikációnak "indokolatlan késedelem nélkül" meg kell történnie, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve".

Jelen dokumentumban bemutatott műveletek csak iránymutatásként szolgálnak egy adatvédelmi incidensre történő reagálás során. Az incidens pontos jellegét és hatását nem lehet teljes bizonyossággal előrejelezni, ezért fontos, hogy józan és ésszerű mérlegelést alkalmazzunk annak eldöntése során, hogy hogyan cselekedjünk. Azonban meggyőződésünk, hogy az itt leírt lépések hasznosnak bizonyulhatnak a GDPR szerinti kötelezettségeink teljesülésének biztosításában.

2 Követelmények az adatvédelmi incidens felderítésére és értesítésekre

2.1 Felderítés és kezdeti elemzés

Egy adatvédelmi incidens kezdetben számos különböző módon és sok forrásból észlelhető, az incidens helyétől és természetétől függően. Némely események önmagukban észlelhetők a Társaságon belül használt szoftvereszközök vagy a szokatlan tevékenységeket észlelő belső ellenőrzési folyamatok által. Más incidensekről harmadik felektől, például ügyféltől, szállítóktól vagy bűnüldöző szervektől értesülhetünk, akik azért értesülhetnek az adatvédelmi incidensről, mert a lopott adatokat valamilyen módon rosszindulatú célokra használják fel.

Nem ritka, hogy az adatvédelmi incidens bekövetkezte és annak észlelése között hosszabb idő teljen el; az információbiztonság proaktív megközelítésének egyik célja ezen időtartam csökkentése. A legfontosabb tényező, hogy az adatvédelmi incidens felismerését követően az incidensre adott válaszfolyamat a lehető leggyorsabban elkezdődhessen, így kellően hatékony válasz szülessen.

Az adatvédelmi incidens részleteiről összegyűjtött információkat amennyire csak lehetséges dokumentálni kell, hogy a felmerülő helyzet tisztázott, időalapú megértése lehetséges legyen az aktuális használatra és egy később felülvizsgálat során is. Amennyiben lehetséges, a hatás mértékének felmérésével együtt létre kell hozni egy listát azokról az információs eszközökről (ideértve a személyes adatokat), üzleti tevékenységekről, termékekről, szolgáltatásokról, csapatokról és támogató folyamatokról, amelyek esetlegesen érintettek lehetnek az incidensben.

2.2 Felelős Tisztségviselő

Ezen kezdeti elemzés eredményeképpen a Társaságon belül bármely személy bármely időpontban jogosult kapcsolatba lépni az Adatvédelmi Tisztviselővel (a továbbiakban: **Vezető**) hogy felkérje őt arra, hogy foglaljon állást a Adatvédelmi Incidens Bejelentési Eljárás megindításáról.

A Vezető - egyeztetve az incidenst észlelő és bejelentő személlyel, a pénzügyi vezetővel, a mindenirányú projektmenedzsmenttel és a hozzá kapcsolódó és a független operációval, az IT szolgáltatóval, a HR feladatokat ellátó személlyel (ha van ilyen), az üzleti folytonosságot és tervezést biztosító titkársággal, a kommunikáció (PR és médiakapcsolatok) vezetőjével és a Társaság jogi és szabályozói csoportjaival (külső tanácsadói csoport(ok)) - köteles

- dönteni arról, hogy megindítja-e az Adatvédelmi Incidens Bejelentési Eljárást
- szükség esetén összegyűjteni a Adatvédelmi Incidens Csapatot
- ellátni a csapat általános irányítását

- elvégezni vagy gondoskodni az e tervben foglalt kötelezettségek teljesítéséről és gondos ellenőrzéséről
- összekötőként működni a vezetőséggel és egyéb magas szintű érdekeltekkel
- kapcsolatot tartani a felügyeleti hatósággal
- kapcsolatot tartani a külső tanácsadókkal és szakértőkkel (pl.: jogászokkal)
- gondoskodni a szükséges értesítések megküldéséről és a megfelelő dokumentációjukról
- megszervezni a helyreállítási intézkedések

Végső döntés meghozatala minden esetben az vezérigazgató joga és kötelezettsége.

3 Adatvédelmi Incidens Bejelentésének Rendje

Miután a Vezető azt állapította meg, hogy adatvédelmi incidens történt a GDPR rendelkezései szerint, amennyiben a Társaság az adatkezelő, az alábbi 2 csoportnak kell értesítést küldeni:

1. A Felügyeleti Hatóság
2. Az érintettek

Az, hogy az Adatvédelmi Incidenst jelenteni kell nem előre eldöntött tény; ez attól függ, hogy az incidens mekkora kockázatot jelent a *"a természetes személyek jogaira és szabadságaira" (GDPR 33. cikk)*. A következő szakaszok azt mutatják be, hogy ezt a döntést mi alapján kell meghozni, és mit kell tenni a bejelentés szükségessége esetén.

Abban az esetben, ha a Társaság adatfeldolgozói pozícióban van és a Vezető azt állapította meg, hogy Adatvédelmi Incidens történt, az adatkezelőt haladéktalanul értesíteni kell.

3.1 A Felügyeleti Hatóság

A Társaság számára a GDPR-re vonatkozó felügyeleti hatóság:

Név:	Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím:	H-1055 Budapest, Falk Miksa u. 9-11.
Telefon:	+36 (1) 391-1400
Fax:	+36 (1) 391-1410
Email:	ugyfelszolgalat@naih.hu

1. táblázat – Felügyeleti Hatóság elérhetőségei

3.1.1 A Felügyeleti hatóság értesítéséről szóló döntés meghozatala

A GDPR rendelkezései előírják az adatvédelmi incidens felügyeleti hatóság részére történő bejelentését, *"kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve." (GDPR 33. cikk).* Ez megköveteli, hogy a szervezet értékelje a kockázat mértékét mielőtt döntést hoz az értesítésről. E célból hasznos lehet az Adatvédelmi Kockázatértékelés és Hatásvizsgálati Eljárás Szabályzata.

A kockázatértékelés során az alábbi tényezőket kell figyelembe venni:

- Titkosították-e a személyes adatokat
- Ha titkosították, a használt titkosítás erőssége
- Milyen mértékben pszeudonimizáltak az adatok (azaz élő egyének ésszerűen azonosíthatóak-e az adatokból)
- Tartalmaznak-e az adatelemek például nevet, címet, banki adatokat, biometrikus adatokat
- Az érintett adatmennyiség
- Az érintettek száma
- Az incidens jellege pl.: lopás, véletlen megsemmisítés
- Bármely egyéb relevánsnak tekinthető tényező

A kockázatértékelésben részt vevő felek az adatvédelmi incidens jellegétől és körülményeitől függően azalábbi területek képviselői lehetnek:

- Felsővezetés
- Üzleti terület(ek) úgy is, mint projektmenedzsment/Tervezés/Kezelés
- Technológia/üzemvitel
- Információbiztonság
- Jog
- Adatvédelmi tisztviselő
- Egyéb

A kockázatértékelésnek az adatvédelmi incidensről történő értesülést követő 48 órán belül meg kell történnie. A kockázatértékelés módszerét, annak okait és megállapításait teljes körűen dokumentálni kell és a Vezetőnek, valamint a Felsővezetésnek bizonyíthatóan el kell fogadnia. A kockázatelemzésnek tartalmaznia kell az alábbi megállapítások egyikét:

1. Az adatvédelmi incidens nem igényel bejelentést

2. Az adatvédelmi incidens csak a felügyeleti hatóság részére igényel bejelentést
3. Az adatvédelmi incidens mind a felügyeleti hatóság mind az érintettek részére igényel bejelentést

Ezen megállapítások változhatnak a Felügyeleti Hatóságtól kapott visszajelzések és az incidens folyamatban lévő vizsgálatából származó további információk alapján.

3.1.2 A Felügyeleti Hatóság értesítése

Ha a Felügyeleti Hatóság értesítéséről született döntés, a GDPR előírja, hogy ennek *"indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásunkra jutott," (GDPR 33. cikk) eleget kell tennünk.* Ha ennek a bejelentési kötelezettségnek az előírt időben törvényes okból nem teszünk eleget mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A bejelentést megfelelő biztonsági intézkedésekkel ellátva az 1. számú táblázatban szereplő szervnek kell elküldeni az Adatvédelmi Incidens Bejelentési Formanyomtatvány minta használatával (lásd: Melléklet 1).

A bejelentés részeként az alábbi információkat kell megadni:

a) Az adatvédelmi incidens jellegét ideértve, ahol lehetséges:

   i. Az érintettek kategóriái és becsült száma

   ii. Az érintett személyes adatok kategóriát és becsült száma

b) Az adatvédelmi tisztviselő vagy más kapcsolattartó személy neve és elérhetőségei, aki bővebb információt tud nyújtani

c) Az adatvédelmi incidens lehetséges következményeinek leírása

d) Az adatvédelmi incidens kezelésére tett vagy javasolt intézkedések leírása, beleértve adott esetben a lehetséges káros hatások enyhítését célzó intézkedéseket

e) Amennyiben a bejelentés túllép a 72 órás kereten a határidő elmulasztásának okai

Az átvétel dátumát és időpontját is tartalmazó írásbeli visszaigazolást kell beszerezni a felügyeleti hatóságtól az adatvédelmi incidens bejelentéséről. Szükség esetén a GDPR lehetőséget biztosít arra, hogy az információk további indokolatlan késedelem nélkül szakaszosan kerüljenek megadásra.

3.2 Érintettek

3.2.1 Az érintettek értesítéséről szóló döntés meghozatala

A GDPR előírja, hogy az adatvédelmi incidensről az érintetteket értesíteni kell, *"ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve" (GDPR 34. cikk).* Megjegyzés: a „magas" szó, a 33. cikkben lévő meghatározásban nem szerepel.

A jelen eljárásban korábban elvégzett kockázatértékelés (2.1.1. szakasz) meghatározza, hogy a kockázat az érintett természetes személyek jogaira és szabadságaira nézve annyira magas-e, ami indokolttá teszi az érintettek értesítését.

Azonban, ha megfelelő technikai és szervezési védelmi intézkedéseket hajtottak végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat, a GDPR alapján az érintettek tájékoztatása nem kötelező.

Ha a későbbiekben olyan további intézkedések megtételére került sor, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg, a GDPR alapján az érintettek tájékoztatása szintén nem kötelező.

A GDPR alapján az érintettek tájékoztatása akkor sem kötelező, ha ez *"aránytalan erőfeszítést tenne szükségessé" (GDPR 34. cikk).* Ebben az esetben azonban a nyilvános kommunikáció valamely formáját használni kell.

Ismét kiemelendő, hogy ezek változhatnak a Felügyeleti Hatóságtól kapott visszajelzés és az incidens folyamatban lévő vizsgálatából származó további információk alapján.

3.2.2 Az érintettek értesítése

Amennyiben az a döntés született, hogy az incidens indokolttá teszi az érintettek értesítését, a GDPR megköveteli, hogy ez indokolatlan késedelem nélkül történjen meg.

Az érintetteknek szóló értesítésében *„világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét"* (GDPR 34. cikk) és közölni kell legalább:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A GDPR által előírtakon túl célszerű lehet az érintettek részére arra vonatkozóan is tanácsot adni, hogy ők milyen további lépéseket tehetnek az adatvédelmi incidenssel kapcsolatos kockázatok csökkentése érdekében.

A legtöbb esetben elegendő az érintetteket postai levél vagy e-mail útján tájékoztatni, hogy bizonyosan megkapják az üzenetet és lehetőségük legyen a szükséges lépések megtételére.

4 Incidensek Elszigetelése, Megszüntetés és Helyreállítás

4.1 Elszigetelés

A fentiekben ismertetett bejelentéshez és értesítéshez kapcsolódó követelmények teljesítése mellett a Társaságon belül a legfontosabb lépés az lesz, hogy megpróbáljuk megállítani az adatvédelmi incidens súlyosabbá válását, azaz elszigeteljük. Vírustámadás esetén ez magában foglalhatja a hálózat érintett részeinek leválasztását, hackertámadás esetén jelentheti a bizonyos profilok vagy portok letiltását a tűzfalon vagy akár az egész belső hálózat lekapcsolását az internetről. Az elvégzendő konkrét intézkedések az esemény körülményeitől függnek.

Megjegyzés: ha úgy ítélik meg, hogy valószínűleg olyan digitális bizonyítékot kell gyűjteni, amelyeket a későbbiekben bíróságon kell felhasználni, óvintézkedéseket kell tenni annak biztosítása érdekében, hogy az ilyen bizonyítékok a továbbiakban is elfogadhatóak maradhassanak. Ez azt jelenti, hogy ezen adatokat tilos akár szándékosan akár véletlenül megváltoztatni, pl.: egy laptop bekapcsolásával. Javasoljuk, hogy ezen ponthoz a Vezető szerezze be adatszakértő véleményét is.

Különösen (de nem kizárólagosan), ha az incidens vonatkozásában szabálytalanság elkövetésének a gyanúja merül fel pontos nyilvántartást kell vezetni a megtett intézkedésekről és a bizonyítékokról, amelyeket a digitális törvényszéki iránymutatások alapján gyűjtöttek össze. Ezen iránymutatások főbb alapelvei az alábbiak:

Alapelv 1 – Ne változtass meg semmilyen adatot. Ha bármi történik, ami az adott rendszerre vonatkozó adatok bármilyen módon történő megváltozását eredményezik, az hatással lesz a későbbi bírósági ügyekre.

Alapelv 2 – Az eredeti adatokat csak kivételes körülmények között lehet megnyitni. Egy képzett szakember a memóriában tárolt adatok egy másolatát fogja használni, legyen szó akár merevlemezről, flash memóriáról vagy SIM-kártyáról. Ezt követően minden vizsgálat a másolaton fog történni és az eredeti fájlt soha nem fogják érinteni, kivéve kivételes körülmények esetén, pl.: az időtényező lényeges és az információszerzés a további bűncselekmények megakadályozására céljából fontosabb, mint a bizonyítékok elfogadhatóságának megőrzése.

Alapelv 3 – Mindig kövessük nyomon, hogy pontosan mi történik. A törvényszéki eszközök ezt automatikusan elvégzik, de ez alkalmazandó a helyszínen tartózkodó első szemtanúkra is. Fénykép és videófelvételek készítése mindaddig javasolt, amíg minden érintetlen.

Alapelv 4 – A Vezetőknek biztosítaniuk kell, hogy betartsák ezen iránymutatásokat.

A szakértő megérkezése előtt az alapvető információkat össze kell gyűjteni.

Ezek magukban foglalhatják:

- Releváns üzenetekről vagy információkról készült fénykép vagy videófelvételeket
- Az incidens időrendjéről szóló írásos feljegyzést
- Eredeti dokumentumokat, beleértve azon nyilvántartásokat, hogy ki találta őket, hol és mikor
- Bármely szemtanú adatait

Miután összegyűjtötték őket, a bizonyítékokat biztonságos helyen kell tartani, ahol ezek nem manipulálhatók és a formális felügyeleti lánc biztosított.

A bizonyítékok szükségesek lehetnek:

- Az incidens okának későbbi elemzéséhez
- Büntető vagy polgári peres eljárásokban bizonyítékként való felhasználáshoz
- Szoftver vagy szervizszolgáltatókkal folytatott kompenzációs tárgyalások támogatásához.

Ezután világos képet kell alkotni a történtekről. Mindennemű feltartóztatásra irányuló intézkedés megtétele előtt meg kell állapítani a az incidens mértékét és a lehetséges következményeket.

Az eseménysorozat rekonstruálása érdekében az ellenőrzési naplókat meg lehet vizsgálni; ügyelni kell arra, hogy csak a nem manipulált naplók biztonságos másolatai kerüljenek felhasználásra.

4.2 Megszüntetés

Az incidens által okozott károk helyreállítása iránt tett intézkedések, pl.: a malware-ek törlését minden esetben a Társasággal szerződéses kapcsolatban álló IT-szolgáltató, mint szakmai tanácsadó bevonása mellett, a központi IT irányelvek alkalmazásával történik. Ezeknek az intézkedéseknek az incidens előtti helyzet és állapot helyreállítására és az incidens prevenciójára kell irányulniuk. Minden olyan sérülékenységet, amelyet az incidens során kihasználtak, azonosítani kell.

Az incidens típusától függően néha feleslegessé válik a megszüntetés.

4.3 Helyreállítás

A helyreállítási szakaszban a rendszert vissza kell állítani az incidens előtti állapotába, bár az incidens részeként kihasznált sérülékenységek felszámolásához szükséges intézkedéseket meg kell tenni. Ez magában foglalhat olyan intézkedéseket, mint javítások telepítése, kódok-jelszavak megváltoztatása, szerverek javítása és eljárások módosítása.

5 Az Incidenst követő tevékenységek

A Vezető határozza meg az intézkedések megszüntetését és a tevékenységek leállítását. Figyelembe véve azt, hogy a helyreállítás és a végrehajtási tervek folytatódhatnak ezen a ponton túl is de kevésbé formális vezetői kontrol alatt.

MELLÉKLET 1 - Adatvédelmi Incidens Bejelentési Formanyomtatvány

A Hatóság kérdései	A kitöltő válaszai
0. Adatvédelmi incidens jelentése	
Bejelentés típusa	☐ teljes bejelentés ☐ szakaszos bejelentés ☐ bejelentés módosítása
A korábban bejelentett incidens azonosítója	
A korábbi bejelentés időpontja	

1. A bejelentő adatai

1.1 Kapcsolati

A bejelentő adatkezelő cégjegyzékszáma	
A bejelentő adatkezelő adószáma (magánszemély bejelentése esetén nem kell)	
Szervezet száma	
A bejelentő adatkezelő elnevezése	
Az incidenssel érintett igazgatási/szervezeti egység megnevezése és elérhetőségei	

A bejelentő adatkezelő címe és egyéb elérhetőségei	
A bejelentő természetes személy neve és beosztása	
A bejelentő természetes személy elérhetőségei	
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és beosztása	

Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó email elérhetősége	
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó telefonszáma	
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó levelezési címe	

Az adatkezelő az alábbiak közül melyik szektorba tartozik		Adminisztratív és szolgáltatást támogató tevékenység
		Bányászat, kőfejtés
		Büntetés-végrehajtás
		Bűnüldözés
		Egészségügy, szociális ellátás
		Egyéb közhatalmi tevékenység
		Építőipar
		Helyi önkormányzati igazgatás
		Honvédelem
		Információ, kommunikáció, hírközlés
		Ingatlanügyletek
		Kereskedelem
		Könnyűipar, feldolgozóipar
		Közlekedés, közlekedésbiztonság
		Központi közigazgatás
		Közrend és közbiztonság védelem
		Média
		Mezőgazdaság, erdőgazdálkodás, halászat
		Munkaügy
		Művészet, szórakoztatás
		Nehézipar, gépgyártás
		Nemzetbiztonság
		Oktatás, kutatás
		Pénzügyi, biztosítási tevékenység
		Rendvédelem
		Szakmai, tudományos, műszaki tevékenység

		Szálláshely-szolgáltatás, vendéglátás
		Szállítás, raktározás
		Személy- és vagyonvédelem
		Társadalmi szervezetek által végzett tevékenység
		Társadalombiztosítás
		Villamosenergia-, gáz-, gőzellátás, légkondicionálás
		Vízellátás, szennyvíz gyűjtése, kezelése, hulladékgazdálkodás, szennyeződésmentesítés
		Egyéb

1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban	
Az adatkezelőn kívül részt vesz-e más személy/szervezet az adatvédelmi incidenssel érintett adatkezelés folyamatában?	Igen/Nem
Az adatkezelőn kívüli fél megnevezése és minősége	

2. Időpontok

Adatvédelmi incidens időpontja	
Adatvédelmi incidens kezdő időpontja	
Adatvédelmi incidens záró időpontja	
Az adatvédelmi incidens továbbra is fennáll	Igen/Nem
Az incidensről való tudomásszerzés időpontja	
Az incidens észlelésének módja	
Az adatfeldolgozó általi értesítés időpontja	
A késedelmes tájékoztatás indokai	
Egyéb megjegyzések az incidens időpontját érintően	

3. Az adatvédelmi incidensről

Bizalmas jelleg	Sérült/Nem sérült	
Integritás	Sérült/Nem sérült	
Rendelkezésre állás	Sérült/Nem sérült	
Adatvédelmi incidens jellege (több válasz is elfogadható)	☐	adathalászat
	☐	elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön)
	☐	eszköz elvesztése vagy ellopása
	☐	informatikai rendszer feltörése (hackelés)
	☐	levél elvesztése vagy jogosulatlan felnyitása
	☐	papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak
	☐	papír alapú dokumentum nem megfelelő módon történő megsemmisítése
	☐	rosszindulatú számítógépes programok pl. Zsarolóprogram
	☐	személyes adatok jogosulatlan megismerése
	☐	személyes adatok jogosulatlan szóbeli közlése
	☐	személyes adatok nagy nyilvánosság előtti jogellenes közzététele
	☐	személyes adatok téves címzett részére történő elküldése
	☐	egyéb
Egyéb megjegyzés az adatvédelmi incidens részletes leírásához		

Adatvédelmi incidens okai (több válasz is elfogadható)		külső, rosszhiszemű cselekmény
		külső, rosszhiszeműnek nem minősülő cselekmény
		szervezeten belüli, rosszhiszemű cselekmény
		szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény
		egyéb
Adatvédelmi incidens egyéb okainak leírása		

4. Az adatvédelmi incidenssel érintett személyes adatok

4.1 Személyes adatok

Személyazonossághoz kapcsolódó adatok	Érintett/Nem érintett
Személyi szám	Érintett/Nem érintett
Elérhetőségi adatok	Érintett/Nem érintett
Azonosító adatok	Érintett/Nem érintett
Gazdasági, pénzügyi adatok	Érintett/Nem érintett
Képfelvétel	Érintett/Nem érintett
Hangfelvétel	Érintett/Nem érintett
Hivatalos okmányok	Érintett/Nem érintett
Helymeghatározó adatok	Érintett/Nem érintett
Biometrikus adatok	Érintett/Nem érintett
Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok	Érintett/Nem érintett

4.2 Különleges adatok	
Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok	Érintett/Nem érintett
Politikai véleményre vonatkozó adatok	Érintett/Nem érintett
Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok	Érintett/Nem érintett
Érdek-képviseleti szervezeti tagságra vonatkozó adatok	Érintett/Nem érintett
Szexuális életre vonatkozó adatok	Érintett/Nem érintett
Egészségügyi adatok	Érintett/Nem érintett
Genetikai adatok	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb személyes adatok leírása	
Az adatvédelmi incidenssel érintett személyes adatok becsült száma	

5. Az érintettek

Alkalmazottak	Érintett/Nem érintett
Felhasználók	Érintett/Nem érintett
Feliratkozók	Érintett/Nem érintett
Diákok	Érintett/Nem érintett
Katonai állomány tagjai	Érintett/Nem érintett
Ügyfelek (jelenlegi és potenciális)	Érintett/Nem érintett
Páciensek	Érintett/Nem érintett
Kiskorúak	Érintett/Nem érintett
Kiszolgáltatott személyek	Érintett/Nem érintett
Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb leírása	

Az incidenssel érintett adatalanyok részletes leírása	
Az adatvédelmi incidenssel érintettek becsült száma	

6. Az incidens ELŐTT alkalmazott intézkedések

Az adatvédelmi incidens előtt alkalmazott intézkedések leírása	

7. Következmények

7.1 Bizalmas jelleg sérülése

Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult	Igen/Nem
Az adat összekapcsolhatóvá vált az érintett egyéb adatával	Igen/Nem
Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges	Igen/Nem
Egyéb	Igen/Nem
Az egyéb bizalmas jelleget érintő következmény leírása	

7.2 Intergritás sérülése	
Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt	Igen/Nem
Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták	Igen/Nem
Egyéb	Igen/Nem
Az egyéb integritást érintő következmény leírása	

7.3 Rendelkezésre állás sérülése	
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése	Igen/Nem
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása	Igen/Nem
Egyéb	Igen/Nem
Az egyéb rendelkezésre állást érintő következmény leírása	

7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények		
Az incidens valószínűsíthető hatásai az érintettekre (több válasz is elfogadható)		álnevesítés engedély nélküli feloldása
		érintett jogainak korlátozása
		hátrányos megkülönböztetés
		jó hírnév sérelme
		pénzügyi veszteség
		szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése
		személyazonosság-lopás
		személyazonossággal való visszaélés
		személyes adatok feletti rendelkezés elvesztése
		egyéb
Az egyéb valószínűsíthető hatások leírása		
A valószínűsíthető következmények súlyossága		elhanyagolható
		korlátozott
		jelentős
		maximális

8. Megtett intézkedések

8.1 Érintettek tájékoztatása

Érintettek tájékoztatása		a, Az érintetteket tájékoztatta
		b, Az érintettek tájékoztatását tervezi
		c, Az érintettek tájékoztatását NEM tervezi
		d, Nem tudja
Tájékoztatás időpontja („a" válasz esetén)		
Tájékoztatás tervezett időpontja („b" válasz esetén)		

A tájékoztatás tervezett időpontja még nincs eldöntve („b" válasz esetén		El van döntve/Nincs eldöntve
Tájékoztatás hiányának indokai („c" válasz esetén)		I, Az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat
		II, Az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg
		III, Az érintettek egyenkénti tájékoztatása aránytalan erőfeszítést tenne szükségessé az adatkezelő számára
Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor („c" válasz esetén)		
Tájékoztatott érintettek száma („a" válasz esetén)		

Az érintett tájékoztatásának formája („a" válasz esetén)	
Az érintetteknek szóló tájékoztatás tartalma („a" válasz esetén)	
Nyilvánosan közzétett információk, vagy hasonló intézkedés („c" illetve „III" válasz esetén)	

8.2 Az adatvédelmi incidens orvoslására tett intézkedések

Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések	

8.3 Egyéb bejelentések

A vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens	Igen/Nem	
Az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet (több válasz is elfogadható)		Ausztria
		Belgium
		Bulgária
		Ciprus
		Csehország
		Dánia
		Egyesült Királyság
		Észtország
		Finnország
		Franciaország
		Görögország
		Hollandia
		Horvátország
		Írország
		Izland
		Lengyelország
		Lettország
		Liechtenstein
		Litvánia
		Luxemburg
		Magyarország

	☐ Málta ☐ Németország ☐ Norvégia ☐ Olaszország ☐ Portugália ☐ Románia ☐ Spanyolország ☐ Svájc ☐ Svédország ☐ Szlovákia ☐ Szlovénia
Az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának?	

Az EU felügyeleti hatóságok listája, amelyeknek az adatkezelő közvetlenül bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst (több válasz is elfogadható)	☐	Ausztria
	☐	Belgium
	☐	Bulgária
	☐	Ciprus
	☐	Csehország
	☐	Dánia
	☐	Egyesült Királyság
	☐	Észtország
	☐	Finnország
	☐	Franciaország
	☐	Görögország
	☐	Hollandia
	☐	Horvátország
	☐	Írország
	☐	Izland
	☐	Lengyelország
	☐	Lettország
	☐	Liechtenstein
	☐	Litvánia
	☐	Luxemburg
	☐	Magyarország
	☐	Málta
	☐	Németország
	☐	Norvégia
	☐	Olaszország
	☐	Portugália

	☐ Románia ☐ Spanyolország ☐ Svájc ☐ Svédország ☐ Szlovákia ☐ Szlovénia
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta?	Igen/Nem
Azon más EGT-tagállami adatkezelő megnevezése és elérhetőségei, amelynek az incidenst bejelentette vagy be fogja jelenteni.	
Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst EU-n kívüli adatvédelmi hatóságnak?	Igen/Nem

Az EU-n kívüli felügyeleti hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette, vagy be fogja jelenteni az adatkezelő	
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb EU-s hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján? (NIS Irányelv, eIDAS Rendelet)?	Igen/Nem
Egyéb EU hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette vagy be fogja jelenteni az adatkezelő.	