A Nyíregyházi Élsport Nonprofit Korlátolt Felelősségű Társaság Adatvédelmi és Adatbiztonsági Szabályzata

A szabályozó dokumentumot jóváhagyom, alkalmazását 2021. 01. 01. napjától elrendelem.

Nyíregyházi Élsport Nonprofit Kft.
4400 Nyíregyháza Géza u. 8-16.
Cégj.sz.:15-09-082797
Adószám:25313907-2-15

.....

Nyíregyházi Élsport Nonprofit Kft. ügyvezetője

TARTALOMJEGYZÉK

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

1. ÁLTALÁNOS RENDELKEZÉSEK

Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, hogy a Nyíregyházi Élsport Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: Adatkezelő) a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítsa a személyes adatok védelmét az Európai Parlament és a Tanács (EU), 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 szóló 2016/679 számú rendelete (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) szerint.

A Szabályzat célja annak biztosítása, hogy az Adatkezelő adatvédelmi szempontból megfeleljen a hatályos hazai és közvetlenül alkalmazandó nemzetközi jogszabályi előírásoknak. Az Adatkezelő jelen Szabályzatban leírtak szerint gyűjti, rögzíti, rendszerezi és tárolja a személyes adatokat.

Alkalmazott jogszabályok:

- Magyarország Alaptörvénye (a továbbiakban: Alaptörvény)
- Általános Adatvédelmi Rendelet – GDPR,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény – Infotv.,
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.),
- a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Munka tv.),
- a munkavédelemről szóló 1993. évi XCIII. törvény (a továbbiakban: Mvt.),
- a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.)
- a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályaitól szóló 2005. évi CXXXIII. törvény,
- az adózás rendjéről szóló 2017. évi CL. törvény (a továbbiakban: Art.)
- a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Szám. tv.),
- a sportról szóló 2004. évi I. törvény,
- további jogi szabályozók: a Nemzeti Adatvédelmi és Információszabadság Hatóság ("NAIH") ajánlásai és az általa kialakított adatvédelmi gyakorlat, valamint az Adatkezelő számos egyéb szabályzata, szerződése, utasítása.

2. A SZABÁLYZAT HATÁLYA

2.1. Személyi hatály

A Szabályzat személyi hatálya kiterjed:

- az Adatkezelőre,
- az Adatkezelő valamennyi szervezeti egységére, intézményére,
- az Adatkezelőnél foglalkoztatott valamennyi vezető tisztségviselőre és munkavállalóra,
- illetve az Adatkezelővel olyan egyéb jogviszonyban álló valamennyi személyre, aki felelősséggel tartozik az előírt adatvédelmi szabályok betartásáért és betartatásáért,
- azon személyekre, akik jogait vagy jogos érdekeit az adatkezelés érinti.

2.2. Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed az Adatkezelő valamennyi szervezeti egysége, intézménye, munkavállalója által folytatott minden olyan adatkezelésre, amely az érintettek személyes adataira vonatkozik, beleértve a papíralapú és az elektronikus adatkezelést is.

2.3. Időbeli hatály

Jelen Szabályzat 2021. január 01. napjától visszavonásig, vagy az Adatkezelő által történő egyoldalú módosításáig hatályos.

3. AZ ADATKEZELŐ ADATAI

Neve	Nyíregyházi Élsport Nonprofit Korlátolt Felelősségű Társaság
Székhelye	4400 Nyíregyháza, Géza u. 8-16.
Telefonszáma	06 42 411-411
Honlapja	www.nyiregyhazielsport.hu
Képviselő	Dr. Mohácsi Máté, ügyvezető
Adatvédelmi tisztviselő neve, elérhetősége	Dr. Kiss Géza adatvedelem@nyiregyhazielsport.hu

4. ÉRTELMEZŐ RENDELKEZÉSEK

Az értelmező rendelkezések tekintetében a GDPR., valamint az Infotv. rendelkezései irányadóak.

4.1. Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy.

4.2. Személyes adat: az érintettre vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

4.3. 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.

4.4. Biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.

4.5. Egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

4.6. Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.

4.7. Hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.

4.8. Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

4.9. Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

4.10. Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

4.11. Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

4.12. Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja

4.13. Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

4.14. Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

4.15. Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

4.16. 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.

4.17. Címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz.

4.18. Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

4.19. Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

4.20. Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek.

Amennyiben a mindenkori hatályos adatvédelmi jogszabályok (jelen Szabályzat megalkotásakor a GDPR., valamint az Infotv.) fogalom meghatározásai eltérnek jelen Szabályzat értelmező rendelkezéseitől, akkor a hatályos jogszabályok által meghatározott fogalmak az irányadóak.

5. AZ ADATKEZELŐ ADATVÉDELMI SZERVEZETI HÁTTERE

Az Adatkezelő elkötelezett az adatvédelem iránt, ezért folyamatosan – a jogszabályi és működésbeli változásnak megfelelően – módosítja a jelen Szabályzatot és általában az egész adatvédelmi szabályozását.

Az Adatkezelő a sajátosságok figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre és az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, valamint kijelöli az adatkezelés felügyeletét ellátó személyt.

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

Az Adatkezelő adatvédelemmel, adatkezeléssel, adatbiztonsággal és információbiztonsággal kapcsolatos vezetését elsődlegesen az Adatkezelő irányítását ellátó képviselő önállóan látja el.

5.1. Az Adatkezelő ügyvezetőjének feladata különösen:

- a személyes adatok védelmét szolgáló jelen Szabályzat jóváhagyása;
- az Adatkezelő adatvédelmi tevékenységének irányítása, felügyelete;
- a személyes adatok védelmével kapcsolatos alapelvek betartása és Adatkezelő szervezetén belüli betartatása;
- a személyes adatok kezelésével érintett személyek jogai gyakorlásának elősegítése;
- a személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítása;
- az adatfeldolgozási szerződések tartalmának meghatározása és jóváhagyása;
- az Adatkezelő adatvédelmi működésének, a Munkatársak adatkezelésének, valamint az adatvédelmi/adatkezelési nyilvántartások vezetésének rendszeres ellenőrzése;
- a munkatársak munkakör ellátásához szükséges informatikai alkalmazásokhoz való hozzáférési jogosultságának megállapítása és engedélyezése;
- a hozzá beérkező adatkezeléssel kapcsolatos kérelmek adatvédelmi tisztviselőnek való továbbítása;
- az adatvagyon leltár elkészítéséért adott területen felelős személyek kijelölése;
- együttműködés és kapcsolattartás a felügyeleti hatósággal;
- az Adatkezelő adatvédelemmel kapcsolatos belső szabályainak kiadása;
- továbbá ellát egyéb olyan feladatokat, amelyet a jelen Szabályzattól formailag eltérő más szabályzat vagy eljárásrend, utasítás, vagy jogszabály meghatároz.

5.2. A szervezeti egységeket vezetők feladata különösen:

- jelen Szabályzatban foglaltak megismerése, alkalmazása;
- a Szabályzatban foglaltak szervezti egységében dolgozókkal történő megismertetése és betartatása;
- jogszabályváltozás, vagy más fontos okból javaslattétel a Szabályzat módosítására, kiegészítésre.

5.3. Az adatvédelmi tisztviselő

Az Adatkezelő képviselőjének közvetlenül felelő Munkatárs, aki ellátja a következőkben meghatározott feladatokat:

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- tájékoztat és szakmai tanácsot ad az Adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző Munkatársak részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- ellenőrzi az adatkezelésre vonatkozó jogszabályok (Infotv., GDPR), valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek teljesülését, megtartását;
- kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az Adatkezelőt vagy az adatfeldolgozót;
- elkészíti és rendszeresen felülvizsgálja, aktualizálja a belső adatvédelmi és adatbiztonsági szabályzatot;
- vezeti a belső adatvédelmi nyilvántartásokat;
- együttműködik, valamint az adatkezeléssel összefüggő ügyekben kapcsolatot tart a felügyeleti hatósággal, szükség esetén konzultációt folytat vele;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését.

5.4. Az Adatkezelő adatkezelést végző munkatársainak feladata:

- jelen Szabályzatban meghatározott alapelvek betartása, érvényesítése az adatkezelés során;
- elősegíteni az adatkezeléssel érintett személyeket abban, hogy az adatkezeléssel érintett jogait gyakorolhassák;
- részvétel a személyes adatok kezelésével érintett személyek tájékoztatásában;
- az adatvédelmi tisztviselő kérésére közreműködni a személyes adatok kezelésével érintett személyek részére nyújtandó információk biztosításában;
- közreműködik az adattörlésben, ha az érintett személy adattörlési joga érvényesítésre benyújtott kérelme alapján adattörlésnek van helye;
- közreműködik az adathordozhatósági jog érvényesítésében;
- kijelölés alapján a területére vonatkozóan adatvagyonleltár elkészítése és vezetése, illetve az adatvagyon leltár felülvizsgálata;
- a hozzá érkezett adatkezelésre irányuló kérelmeket továbbítsa az adatvédelmi tisztviselőnek;
- új adatkezelési helyzet jelzése az adatvédelmi tisztviselőnek.

5.5. Általános szabályok

Valamennyi munkatárs köteles az adatok illetéktelen harmadik személyek birtokába kerülésének kockázatát a lehető legkisebbre csökkenteni. Ennek tekintetében a feladata elvégzésével összefüggésben az általa létrehozott, vagy birtokába került, papíron rögzített adatot (pl. manuálisan kitöltött formanyomtatvány, kinyomtatott Word vagy Excel dokumentum stb.) köteles megvédeni a jogosulatlan hozzáféréstől, az elvesztéstől, a fizikai károsodástól és a megsemmisüléstől.

Az adathordozó dokumentumokat minden munkatárs köteles a közvetlen felügyelete alatt, vagy a munkavégzés helyén, illetéktelenek számára nem hozzáférhető, zárt helyen (lezárt fiókban, szekrényben, zárt irodában) tartani.

A munkatársak az adatkezelésre, adat- és titokvédelemre vonatkozó jogszabályi rendelkezések, továbbá mindenkor hatályos Adatvédelmi és Adatbiztonsági Szabályzat, egyéb adatvédelmi vagy más belső szabályzat, munkaköri leírás, munkáltatói utasítás megszegése esetén a magatartás, vagy mulasztás jellegétől függően büntetőjogi és/vagy polgári jogi és/vagy munkajogi felelősséggel tartozhatnak.

5.6. Feladat és felelősség dokumentálása

A munkaköri leírás elkészítéséért felelős személy köteles gondoskodni arról, hogy a munkaköri leírásban meghatározásra kerüljenek:

- legalább a jelen Szabályzatra való hivatkozással a személyes adatok védelmére vonatkozó általános feladatok és felelősségek;
- a konkrét feladat- és felelősségi előírások, ha az érintett munkakör indokolja.

A Szabályzattal kapcsolatos feladat és felelősség dokumentálása megtörténik a Szabályzat megismerési nyilatkozatának aláírásával, mely feltétele a jelen Szabályzatban meghatározott feladatok, tevékenységek ellátásának.

6. AZ ADATKEZELÉS ALAPELVEI

Az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így az Adatkezelő eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezései alapján végez adatkezelést, így különösen betartva az alábbi alapelveket:

6.1. Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelését az Adatkezelő jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi. Az átláthatóság elvének szellemében az Adatkezelő biztosítja, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint azt világos és egyértelmű nyelvezettel fogalmazzák meg.

Jogszerűségi feltételek:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- 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;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (kötelező adatkezelés);
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (kötelező adatkezelés),
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

6.2. Célhoz kötöttség elve

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat az Adatkezelő nem kezeli ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

6.3. Adattakarékosság elve

Az Adatkezelő az adattakarékosság elve érdekében a személyes adatok közül csak annyi és olyan adatot kezelhet, amelyek az adatkezelés céljai szempontjából megfelelőek és relevánsak, és a szükséges mértékre korlátozódnak.

6.4. Pontosság elve

Az Adatkezelő biztosítja a személyes adatok pontosságát, teljességét, sérthetetlenségét, bizalmasságát és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. Az Adatkezelő minden észszerű

intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törölje vagy helyesbítse.

6.5. Korlátozott tárolhatóság elve

A személyes adatok tárolása olyan formában történik, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.

6.6. „Integritás és bizalmas jelleg" elv

A személyes adatok kezelését az Adatkezelő úgy 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.

6.7. Az elszámoltathatóság elve

Az Adatkezelő felelős a személyes adatok kezelésére vonatkozó alapelveknek való megfelelésért, továbbá e megfelelés igazolhatóságáért.

6.8. Beépített és alapértelmezett adatvédelem elve

Ez az elv olyan tudatos gondolkodásmódot jelent, amely szerint mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során (már annak megkezdése előtt is) az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre a fenti elvek hatékony megvalósítása, a kötelezettségek teljesítése, jogi garanciák beépítése céljával, mindezeket pedig szabályozottan és dokumentáltan teszi meg. Ezt a fajta gondolkodásmódot elősegíti a munkatársak adatvédelmi tudatossága, valamint az egyes adatkezelések bevezetése és/vagy rendszeres felülvizsgálata során használt hatásvizsgálat, kockázatelemzés, érdekmérlegelési teszt.

7. AZ ÉRINTETTEK JOGAI

7.1. Előzetes tájékoztatáshoz való jog

Az érintett jogosult a kezelt személyes adatai vonatkozásában az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékozódni. Az Adatkezelő által történő tájékoztatás történhet úgy is, hogy az adatkezelés részleteiről szóló tájékoztatót az Adatkezelő a helyben szokásos módon közzéteszi, és erre az érintett figyelmét felhívja, vagy akár azáltal is, hogy az érintettek figyelmét felhívó jelzések kerülnek elhelyezésre az adatkezelés megkezdése előtt (például az irodák bejáratánál, telefonbeszélgetés elején, elektronikus üzenetben stb.).

Az Adatkezelő törekszik arra, hogy az érintettek az adatkezelést megelőzően tájékoztatást kapjanak az adatkezelés részleteiről. Ennek érdekében az Adatkezelő a honlapján az adatkezeléseiről szóló tájékoztatókat közzéteszi.

Az érintett kérelmére az Adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az esetleges adatvédelmi incidensek körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.

Az Adatkezelő köteles a beadott kérelmet, a benyújtásától számított legrövidebb idő alatt – de legfeljebb 25 napon belül – elbírálni és a döntésről az érintettet írásban, vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíteni. A tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal kell teljesíteni.

Az érintett tájékoztatását az Adatkezelő csak akkor tagadhatja meg, ha azt törvény lehetővé teszi. Ebben az esetben az Adatkezelő tájékoztatja az érintettet a jogorvoslati lehetőségekről.

7.2. Hozzáféréshez való jog

Az érintett bármikor jogosult személyes adatairól és az azok kezelésével összefüggő információkról az Adatkezelőtől tájékoztatást kérni.

7.3. Helyesbítéshez való jog

Az érintett kérheti, hogy a pontatlanul vagy hiányosan rögzített személyes adatait az Adatkezelő helyesbítse, vagy kiegészítse. Abban az esetben, ha a helyesbítendő adatok alapján rendszeres adatszolgáltatás történik, az Adatkezelő szükség esetén a helyesbítésről tájékoztatja az adatszolgáltatás címzettjét, vagy felhívja az érintett figyelmét arra, hogy a helyesbítést más adatkezelőnél is kezdeményeznie kell.

7.4. Törléshez és tiltakozáshoz való jog

Az érintett a jogszabályban elrendelt adatkezelések kivételével kérheti a személyes adatai törlését. Az Adatkezelő az érintettet a törlésről tájékoztatja. Amennyiben a hozzájáruláson alapuló adatkezelés az érintett jogviszonya létesítésének, fenntartásának feltétele, erről, és a várható következményekről az Adatkezelő az érintettet tájékoztatja.

Az Adatkezelő a személyes adat törlését megtagadja, ha az adat kezelése jogszabályon alapul, szerződéses vagy jogi kötelezettsége teljesítéséhez kötődik, vagy az adatkezelés az Adatkezelő jogos érdekének érvényesítéséhez szükséges. A törlési kérelem teljesítésének megtagadása esetén az Adatkezelő az érintettet annak okáról tájékoztatja.

Az érintett az Infotv. rendelkezéseinek megfelelően tiltakozhat személyes adatai kezelése ellen:

- ha a személyes adatok kezelése vagy továbbítása kizárólag az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az Adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;
- valamint a törvényben meghatározott egyéb esetekben.

7.5. Az adatkezelés korlátozásához való jog

Az érintett jogosult az adatkezelés korlátozására, ha:

- vitatja a kezelt adatok pontosságát,
- vitatja az adatkezelés jogszerűségét és/vagy szükségességét,
- az érintett tiltakozott az adatkezeléssel kapcsolatban, amíg a vitás kérdés le nem zárul.

A korlátozás ideje alatt az érintett adatot tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, valamint fontos közérdekből lehet kezelni.

A korlátozás feloldásáról az Adatkezelő az érintettet előzetesen értesíti.

7.6. Adathordozhatóság joga

Az érintett kérheti az Adatkezelő által vele kapcsolatban kezelt összes olyan adat átadását, amelyeket az Adatkezelő az érintettől vett fel a nyilvántartásába. Az adathordozhatósági jog érvényesítése során az Adatkezelő az adatokat szöveges, fénykép, mozgókép vagy hanganyag állományban hordozható optikai adathordozón, vagy papír alapú dokumentumban adja át az érintett részére.

7.7. Jogorvoslathoz való jog

Az érintettek a személyes adatkezelésükkel kapcsolatos kifogásaikat, panaszaikat közvetlenül az Adatkezelőhöz nyújthatják be.

Az Adatkezelő intézkedése jogszerűségének vizsgálata céljából az érintettek a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1055 Budapest, Falk Miksa utca 9-11.) eljárás lefolytatását kezdeményezhetik, ha az Adatkezelő jogaik érvényesítését korlátozza vagy ezen jogaik érvényesítésére irányuló kérelmüket elutasítja, valamint akkor, ha megítélésük szerint személyes adataik kezelése során az Adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó megsérti a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat.

A pert az érintett – választása szerint – a lakóhelye vagy tartózkodási helye szerinti illetékes törvényszék előtt is megindíthatja.

8. ADATBIZTONSÁG – ÁLTALÁNOS SZABÁLYOK

Az Adatkezelő gondoskodik a kezelt személyes adatok bizalmasságáról és biztonságáról. Ennek érdekében megteszi a szükséges technikai és szervezési intézkedéseket mind az informatikai eszközök útján tárolt, mind a hagyományos, papíralapú adathordozókon tárolt adatállományok tekintetében. Az Adatkezelő gondoskodik arról, hogy a vonatkozó jogszabályokban előírt adatbiztonsági szabályok érvényesüljenek.

Az Adatkezelő az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az Adatkezelő az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.

8.1. Fizikai védelem

A papíralapon kezelt személyes adatok biztonsága érdekében tett intézkedések:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezik el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- az adatkezelést végző munkatárs a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- az adatkezelést végző munkatárs a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat kell alkalmazni.

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, intézkedni kell a papír megsemmisítéséről. Ebben az esetben az Adatkezelő kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú dokumentumokra vonatkozó megsemmisítési szabályok az irányadóak.

8.2. Informatikai védelem

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében tett intézkedések és garanciális elemek:

- az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehet csak hozzáférni;

- a jelszavak cseréjéről az Adatkezelő rendszeresen, illetve indokolt esetben gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a hálózaton tárolt adatok biztonsága érdekében a szervereket magas rendelkezésre állású infrastruktúrával védik, az adatvesztést mentésekkel és archiválással kerülik el;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végeznek, a mentés a központi szerver teljes adatállományára vonatkozik;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodnak;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozzák illetéktelen személyek hálózati hozzáférését.

Az Adatkezelő az informatikai rendszerben kezelt adatok védelme érdekében az alábbi fizikai és logikai védelmi rendszereket alkalmazza:

- Adatok mentése tükrözött külső Backup eszközökre
- RAID használata a szervereken
- Folyamatos naplózás / monitoring
- Növekményes biztonsági mentés
- Napi mentés
- Active Directory alkalmazása
- NAS / DAS használata
- Vírusvédelem
- Jogosultságkezelés
- Külső hozzáférés CSAK VPN-en szigorított jogosultsággal
- Mappák titkosított kulccsal való ellátása

Szerverek biztonsága

A személyes adatok áramlása elektronikus módon szerverek segítségével, fizikai tárolásuk pedig adattárolók segítségével történik.

Mind az adattárolókat, mind pedig a szervereket külön erre a célra kialakított helyiségben kell elhelyezni. Erre a helyiségre vonatkozóan ki kell alakítani egy hozzáférési jogosultsággal rendelkező munkavállaló bázist, akik engedéllyel férhetnek hozzá ezekhez az eszközökhöz és esetlegesen a rajtuk tárolt

adatokhoz. A szerverszobába való belépési jogosultságot a munkavállalóknak beosztástól függetlenül külön kell igényelnie, amit az IT vezetőnek – az adatvédelmi tisztviselővel egyeztetve – kell elbírálnia.

A személyes adatok tárolásának helyén, a szerverszobákban tárolt szerverek fizikai védelme érdekében tett intézkedések és garanciális elemek:

- a szerverszoba több pontos biztonsági zárral, riasztóval, biztonságos elektromos hálózattal és szünetmentes tápegységekkel ellátott,
- a szerverszobába csak az engedéllyel rendelkező személy rendelkezhet saját kulccsal vagy veheti át a kulcskezelési szabályok alapján a kulcs kezelőjétől a szerverszoba kulcsát,
- amennyiben olyan személynek kell tevékenysége ellátása miatt bemenni a szerverszobába, akinek nincs engedélye, akkor minden esetben tartózkodik vele egy olyan személy, aki engedéllyel rendelkezik.

8.3. A gyermekek személyes adatainak fokozott biztonsága

Az Adatkezelő tevékenysége során kiskorúak személyes adatait is kezeli, ezért kiemelt figyelmet fordít azok speciális védelmére.

A fokozott védelem érdekében különösen az alábbi intézkedéseket teszi:

- Az Adatkezelő különös körültekintéssel jár el és érdekmérlegelési tesztet végez minden olyan esetben, ha az adatkezelése jogalapjaként a jogos érdekét kívánja alkalmazni és az adatkezeléssel érintettek gyermekek vagy gyermekek is vannak (lehetnek) az érintettek között.
- A hozzájáruláson alapuló adatkezelés esetén, a 18. életévét be nem töltött gyermek személyes adatait csak akkor és olyan mértékben kezeli, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló szülő, vagy kirendelt gyám adta meg, illetve engedélyezte.
- Az Adatkezelő mindent megtesz annak érdekében, hogy ellenőrizze, hogy a hozzájárulást valóban a gyermek feletti szülői felügyeleti jog gyakorlója vagy kirendelt gyámja adta meg, illetve engedélyezte.
- A szülői beleegyezést is igénylő esetekben Adatkezelő általánosságban törekszik arra, a lehető legkevesebb adatot kezelje.
- A tájékoztatás nyújtása során az Adatkezelő minden esetben tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően igyekszik megfogalmazni és elérhetővé tenni, ha az információ címzettje gyermek.

8.4. Titoktartás

Természetes személyek adatai vonatkozásában a személyes adatok védelmére vonatkozó szabályok is alkalmazandók. A titoktartási kötelezettség – időbeli korlátozás nélkül – az Adatkezelő képviselőjére, vezető beosztású munkavállalóira, minden alkalmazottjára, valamint mindazokra vonatkozik, akik az érintettekkel kapcsolatos információkhoz az Adatkezelővel kapcsolatos tevékenységük során bármilyen módon hozzájuthatnak.

Az Adatkezelő titoktartása vonatkozásában megfelelően irányadóak az alábbiak:

- a Ptk. személyhez fűződő jogokkal és azok védelmével kapcsolatos valamennyi rendelkezései, ideértve különösen a levéltitokkal, magántitokkal és üzleti titokkal kapcsolatos szabályokat;
- a Btk. titokvédelemmel kapcsolatos valamennyi rendelkezései,
- az Art. titoktartással, titokvédelemmel kapcsolatos valamennyi rendelkezése, ideértve különösen az adótitokkal kapcsolatos 127. és egyéb paragrafusait;
- a GDPR által előírt adatvédelmi rendelkezései,
- az Infotv. adatkezeléssel kapcsolatos rendelkezései;
- az Adatkezelő SZMSZ-ében, valamint az adatfeldolgozásra irányuló szerződésekben előírt, a titoktartásra vonatkozó rendelkezései.

Az Adatkezelő vezető tisztségviselője (képviselője) és munkatársai vonatkozásában a titoktartási kötelezettség nem áll fenn:

- a hatáskörében eljáró Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH),
- a hagyatéki ügyben eljáró közjegyzővel, valamint a hatáskörében eljáró gyámhatósággal;
- a csődeljárás, felszámolási eljárás, önkormányzatok adósságrendezési eljárása, bírósági végrehajtási eljárás, illetve végelszámolás ügyében eljáró vagyonfelügyelővel, felszámolóval, pénzügyi gondnokkal, végrehajtóval, illetve végelszámolóval;
- a folyamatban lévő büntetőeljárás keretében eljáró, valamint a feljelentés kiegészítését folytató nyomozó hatósággal, valamint a hatáskörében eljáró ügyészséggel;
- a büntető-, valamint polgári ügyben, továbbá csőd-, felszámolási eljárás keretében a bírósággal;
- külön törvényben meghatározott feltételek teljesülése esetén a titkosszolgálati eszközök alkalmazására, titkos információgyűjtésre felhatalmazott szervvel;
- az adó-, vám- és társadalombiztosítási kötelezettség teljesítésének ellenőrzése, valamint az ilyen tartozást megállapító végrehajtható okirat végrehajtása érdekében folytatott eljárás keretében eljáró adóhatósággal, vámhatósággal;
- a gyermekvédelmi észlelő- és jelzőrendszer tagjával szemben, amennyiben az Adatkezelő tevékenysége során jelzés megtételére okot adó körülmény merül fel.

9. ADATBIZTONSÁG – SPECIÁLIS SZABÁLYOK

9.1. Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti az Adatkezelőt az elvárt, illetve elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében tett jogosultságkezelési előírások:

- Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján az IT vezető végzi.
- A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
- El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására igényt nem tartó személyek.
- Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az Adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.
- Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

Jogosultságkezelési folyamata:

Jogosultságigényléshez, jogosultságmódosításhoz, vagy a jogosultság megszüntetéséhez az IT vezetőnek címzett, jelen Szabályzat 1. számú mellékletét képező, aláírt „Jogosultságkezelési megrendelőlap"-ot kell küldeni. A megrendelőlapot papíralapon vagy elektronikus formátumban, az aláírt példányt beszkennelve kell eljuttatni az IT vezetőnek.

A jogosultság kezelésekről az IT vezető a Szabályzat 2. számú melléklet szerinti belső nyilvántartást vezeti.

Az IT vezető minden esetben konzultál a megrendelőlapon szereplő jogosultság megadásáról vagy módosításáról annak indokoltságának tekintetében a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezető tisztségviselőnek és az igénylő feletti munkáltatói jog gyakorlójának vétójoga van.

A megszületett döntést követően az IT vezető által kijelölt munkatárs beállítja a jogosultságokat, amelyről visszaigazolást küld az igénylő felé.

A jogosultság birtokosának munka- vagy egyéb jogviszonya megszűnésével közvetlen felettesének kötelessége értesíteni az IT vezetőt, valamint a munkáltatói jogok gyakorlóját a jogosult eddig birtokolt jogosultságainak törlése érdekében.

A jogosultság megszűnése esetén a jogosult felettese a megszűntetési kérelmet elektronikus módon vagy papíralapon a jogosultságkezelési megrendelőlapon küldi meg az IT vezetőnek, aki gondoskodik a jogosultság törléséről. Ezt követően az IT vezető vagy az általa megbízott munkatárs visszajelzést küld a törlést kezdeményezőnek.

Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes egyetemlegesen kötelesek gondoskodni a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

Az Adatkezelő rendszergazdai tevékenységét külső szolgáltató látja el. A külső szolgáltató a tevékenysége során ráláthat az informatikai rendszerben tárolt személyes adatokra, így adatfeldolgozónak minősül.

Egyéb adatvédelmet és adatbiztonságot érintő kérdésben az Adatkezelő mindenkor hatályos Információ Biztonsági Szabályzata (IBSZ) az irányadó, melyet e Szabályzattal összhangban kell alkalmazni.

9.2. Beépített adatvédelem

Az Adatkezelő alkalmazza az ún. beépített adatvédelem (privacy by design) elvét. Ennek részeként már az adatkezelés tényleges megkezdése előtt – például már a projektelőkészítés időszakában – is figyelemmel van a GDPR előírásaira. A beépített adatvédelem az Adatkezelő olyan saját belső eljárásainak az összessége, amivel – a külső szabályozásoktól függetlenül is – igyekszik megfelelni annak, hogy az érintett személyes adatait minél jobban védje.

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a GDPR követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Az említett intézkedések magukban foglalják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést.
Az adatkezelésnek átláthatónak és felhasználó-központúnak, az adatvédelemnek proaktívnak kell lennie, és az adat teljes életciklusát fel kell ölelnie, vagyis a teljes folyamatnak része kell, hogy legyen.
Az Adatkezelő a tudomány és a 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, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

Adattovábbítás esetén az Adatkezelő a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. A garanciák biztosítják az adatvédelmi követelményeknek való megfelelést és az Európai Unión belüli adatkezelés esetén biztosított jogokkal azonos szintű jogokat, beleértve az érintettek jogainak érvényesíthetőségét és a hatékony jogorvoslat lehetőségét.

9.3. Mobil eszköz menedzsment

A mobil eszköz menedzsment területén az Adatkezelőnek biztosítani kell a mobil eszközökön tárolt, szállított saját, valamint a birtokába kerülő harmadik fél adatainak titkosságát, sérthetetlenség és az ilyen eszközök biztonságot garantáló keretrendszerben való működését.

Az Adatkezelő belső rendszerében mobilmenedzsment szolgáltatásokat tartalmazó informatikai megoldásokat alkalmaz, amely az alábbiakat biztosítja:

- összetett és rendszeresen változó jelszóhasználat kikényszerítése;
- használati eszközök automatikus kiléptetése;
- titkosítás használata a rendszerben levő eszközökön;
- adatok távoli törlésének lehetősége;
- eszköz távoli letiltása;
- eszköz távoli ellenőrzése;
- nyomkövetés és helymeghatározási opció távoli bekapcsolásának lehetősége.

9.4. Oktatás és tréningrendszer

Az Adatkezelő kiemelt területként kezeli a biztonságtudatossági képzést a szervezet informatikai és nem informatikai alkalmazottai részére, hiszen a biztonságtudatos magatartás komoly üzleti károkat okozó hibák és támadások megelőzésében játszhat szerepet.

A megfelelően kidolgozott IT biztonsági szabályzat, információbiztonsági rendelkezések és adatvédelmi, adatbiztonsági szabályozás megléte mellett nagy hangsúlyt kell fordítani a munkavállalók rendszeres képzésére, tréningjeire, melyek során tudatosítható, hogy a kialakított szabályrendszer és az IT eszközök önmagukban nem képesek garantálni a szervezet számára az adat- és információbiztonságot, ehhez a napi munkatevékenység során tanúsított felelős magatartással mindenkinek hozzá kell járulni.

A munkavállalók megfelelő képzése kimutathatóan kevesebb biztonsági incidenst eredményez, ami a közvetlen adatvesztésből és esetleges adatvédelmi birságból eredő károkon túl a pénzügyi eredményekben is nyilvánvalóan megmutatkozik.

A munkavállalók általános adatvédelmi-információbiztonsági tréningjére évente egy alkalommal (kapcsolható más rendszeres képzésekhez, tréningekhez pl. tűz- és munkavédelem), egy óra időtartamban kerül sor. Ez vonatkozik az informatikai és nem informatikai munkavállalókra egyaránt.

Az Adatkezelő külön tréningrendet biztosít az informatikai, különösen a rendszergazdai feladatokat ellátók részére. Ennek célja, hogy kizökkentse a képzés alatt állókat a megszokott munkamenetükből és feltárja előttük a rosszindulatú támadások, hekkerek által folyamatosan fejlesztett aktuális támadási szemléletet, rámutasson az aktuális trendek szerint jellemzően keresett gyenge pontokra és segítse őket abban, hogy érzékelt behatolási kísérlet esetén milyen megoldásokat preferáljanak a támadások elhárítására és a vonatkozó kockázatok alacsony szinten tartása érdekében.

10. ADATÁLLOMÁNYOK KEZELÉSE

A jelen Szabályzat szerinti elvek és kötelezettségek az elektronikus és a papíralapú nyilvántartások esetében egyaránt érvényesülnek.

Az Adatkezelő a nyilvántartás rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a személyügyi nyilvántartásban szereplő adatokat csak azok a munkavállalók, és egyéb az Adatkezelő érdekkörében eljáró személyek (könyvelési, bérszámfejtési és informatikai feladatokat ellátó személyek) ismerhessék meg, akiknek erre munkakörük, feladatuk ellátása érdekében szükségük van.

Az Adatkezelő biztosítja, hogy a nyilvántartás módja és adattartalma a mindenkor hatályos jogszabályoknak megfeleljen. A jogszabályon alapuló adatkezelések kötelezőek, azonban azokról az érintettek tájékoztatást kérhetnek. Az Adatkezelő gondoskodik az eltérő célú adatkezelések megfelelő, logikai elkülönítéséről, illetve arról, hogy az egyes adatkezelési célok megvalósítása során kizárólag az ahhoz szükséges adatok kerüljenek felhasználásra.

Az Adatkezelő az elektronikus és a papíralapú nyilvántartásokat egységes elvek alapján, a nyilvántartások adathordozóinak különbözőségéből adódó jellemzők figyelembevételével kezeli.

Az Adatkezelő a nyilvántartás, ellátotti és munkatársi dokumentáció, szerződéses állományhoz tartozó adattartalmak papíralapú dokumentumait az adatbiztonság követelményeire tekintettel tárolja, és gondoskodik azok biztonságos őrzéséről.

Az Adatkezelő az elektronikus nyilvántartásokat külön erre a célra fejlesztett nyilvántartási rendszer útján üzemelteti, amely, illetve amelynek futtatási környezete megfelel az adatbiztonság követelményeinek. A jogszabályok által elrendelt kötelező nyilvántartások, amelyekben történő adatrögzítést az Adatkezelő köteles elvégezni védelmi rendszerét az elektronikus nyilvántartásokat működtető szervezetek garantálják.

Az Adatkezelő lehetőség szerint törekszik az adatminimum elvének érvényesülésére, annak érdekében, hogy az egyes munkavállalók, és egyéb, az Adatkezelő érdekkörében eljáró személyek csak a szükséges személyes adatokhoz férjenek hozzá.

Az Adatállományok kezelésére, azok biztonságos őrzésére, a hozzáférési jogokra, adatok, dokumentációk felhasználására az Adatkezelő szervezetén belül – összhangban a törvényi előírásokkal – hatályos szabályzatok, utasítások megfelelően irányadóak.

A hozzáférési jogosultságok igénylése, jóváhagyása, engedélyezése és beállítása, valamint megvonása és törlése dokumentált eljárások keretében történik. A jogosultságok beállítását az érintett adatvagyon elem adatgazdája engedélyezi. Az elavult, már nem szükséges jogosultságok elkerülése érdekében az Adatkezelő rendszeresen felülvizsgálja, leltározza a domain és a nyilvántartási rendszerben beállított jogokat.

Az Adatkezelő a kiadott jogosultságokról külön nyilvántartást vezet, az informatikai feladatokat ellátó munkatárs, vagy megbízott feladata a nyilvántartás összevetése a tényleges hozzáférési beállításokkal.

Az adatfeldolgozók az adatfeldolgozásra irányuló szerződésben foglalt kötelezettségeik ellátásához Adatkezelőtől csak azokat az adatokat kapják meg, amelyekre a tevékenység ellátásához feltétlenül szükség van. Az Adatkezelő – a feladat jellegétől függően minden olyan esetben, amikor a jogszabály az adat megőrzését a továbbiakban nem írja elő – kötelezi az adatfeldolgozót az átadott adatok adatfeldolgozási tevékenység lezárultát követő megsemmisítésére.

11. ADATÁTADÁS, ADATTOVÁBBÍTÁS

Az Adatkezelő az általa kezelt személyes adatokat kizárólag az érintettnek, törvényes képviselőjének, meghatalmazottjának, valamint törvényes feladatkörében eljáró hatóságnak, bíróságnak, közjegyzőnek adja át. Az Adatkezelő az adatátadásokról nyilvántartást vezet.

Az adatok egyéb továbbítására – az adatfeldolgozási tevékenységet kivéve – minden esetben csak az érintett hozzájárulása, vagy jogszabályi felhatalmazás alapján kerül sor.

A személyes adatot továbbítani csak abban az esetben lehet, ha:

- annak jogalapja egyértelmű,
- célja, és az adattovábbítás címzettjének a személye pontosan meghatározott,
- és az adattovábbítással elérendő cél más módon nem valósítható meg.

Az adattovábbítást minden esetben dokumentálni kell, oly módon, hogy annak menete és jogszerűsége bizonyítható legyen. A dokumentálásra elsősorban az adatszolgáltatást kérő, illetve annak teljesítéséről rendelkező, megfelelően kiadmányozott iratok szolgálnak.

A jogszabály által előírt adattovábbítást az Adatkezelő köteles teljesíteni.

A fentieken kívül személyes adatot továbbítani csak akkor lehet, ha ahhoz az érintett egyértelműen hozzájárult. Annak érdekében, hogy a hozzájárulás utóbb bizonyítható legyen, azt lehetőség szerint írásba kell foglalni. Az írásbeliség mellőzhető, ha az adattovábbítás a címzettjére, céljára, vagy az adatkörre tekintettel csekély jelentőségű. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett a nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

Az Adatkezelő által végrehajtott leggyakoribb adattovábbítások:

- Az Adatkezelő könyvvizsgálójának a szerződéses feladatai ellátása miatt.
- Az Adatkezelő könyvelési feladatait ellátó cég részére kizárólag a könyveléshez szükséges adatok továbbítása.
- Adófizetési, támogatás elszámolási, bevallási, beszámolási kötelezettség keletkezésekor a megfelelő szervek felé (pl. Támogató szervezet, Nemzeti Adó- és Vámhivatal, ellátási szerződésben megjelölt önkormányzati szerv stb.).
- Szerver- és más informatikai szolgáltatást biztosító szerződéses partner.

12. ADATFELDOLGOZÁS

Az Adatkezelő fenntartja magának a jogot, hogy tevékenysége során adatfeldolgozót vegyen igénybe, állandó vagy eseti megbízás, vagy vállalkozói szerződés alapján. Állandó jellegű adatfeldolgozásra elsősorban a könyvelési feladatok ellátása, az iratmegsemmisítés, selejtezés, valamint az informatikai rendszer fenntartása érdekében kerülhet sor.

Az adatfeldolgozó igénybevétele során a vonatkozó jogszabályok, elsősorban az Infotv. és a GDPR rendelkezései az irányadók. Adatfeldolgozó igénybevételére kizárólag írásbeli szerződés alapján kerülhet sor.

Az Adatkezelő kérésre az érintettet tájékoztatja az adatfeldolgozó személyéről, valamint adatfeldolgozási tevékenységének részleteiről, így különösen az elvégzett műveletekről, valamint az adatfeldolgozónak adott utasításokról.

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a vonatkozó jogszabályok keretei között az Adatkezelő határozza meg.

Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az Adatkezelő felel.

Az adatfeldolgozó tevékenységi körén belül, illetőleg az Adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót csak az Adatkezelő előzetes írásbeli hozzájárulásával vehet igénybe.

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.

Az Adatkezelő garanciákat nyújtó szerződési feltételek kialakításával és megfelelő szervezeti, technikai intézkedésekkel biztosítja, hogy az adatfeldolgozó tevékenysége során az érintettek jogai ne sérülhessenek, és az adatfeldolgozó személyes adatokat csak akkor ismerhessen meg, ha az feladata ellátásához elengedhetetlenül szükséges.

13. ÉRDEKMÉRLEGELÉS

Az adatvédelemre vonatkozó jogszabályhelyek értelmében lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy az Adatkezelő eleget tesz tájékoztatási kötelezettségének.

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az egyik jogszerűségi feltétel teljesül. Ebben az esetben az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben 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.

Az adatkezelés jogszerűségének vizsgálatához az Adatkezelő elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során azonosítani kell a jogos érdeket az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel kell vizsgálni.
Az Nyíregyházi Élsport Nonprofit Kft. a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is el kell végezni, amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján az Adatkezelő megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy az Adatkezelő a beleegyezésük nélkül kezeli a személyes adatokat. A tájékoztatásnak tartalmaznia kell a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákat és az adatkezelés elleni tiltakozás lehetőségeit.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé az Adatkezelő az adott eset sajátos körülményeire tekintettel, ezért az Adatkezelő minden egyes esetben külön érdekmérlegelési tesztet végez el.

Az érdekmérlegelés folyamatának lépései:

1. A tervezett adatkezelés megkezdése előtt az Adatkezelő áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.
2. A jogos érdek lehető legpontosabb meghatározása.
3. Meg kell határozni az adatkezelés célját, valamint azt, hogy milyen személyes adatokról van szó és azok mennyi ideig tartó adatkezelést igényelnek.
4. Az érintettek érdekeinek meghatározása.

5. Az Adatkezelő elvégzi a jogos érdek és az érintettek érdekeinek és alapvető jogainak súlyozását és megállapítja, hogy a személyes adat kezelhető-e.
6. Az Adatkezelő meghatározza azokat az adatkezelési garanciákat, melyek biztosítják az adatkezelés szükségességét és arányosságát.

Az Adatkezelő jelen Szabályzat 3. számú mellékletében leírt szempontrendszer figyelembevételével végzi el az érdekmérlegelést.

14. ADATVÉDELMI HATÁSVIZSGÁLAT

Az Adatkezelőnek új adatkezelési művelet bevezetését megelőzően hatásvizsgálatot kell végezni arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. A hatásvizsgálat abban az esetben kötelező, ha az adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Az adatvédelmi hatásvizsgálatot el kell végezni az alábbi esetekben:

- azon adatkezelések során, ahol cél, hogy a természetes személyekkel kapcsolatban döntést lehessen hozni azt követően, hogy elvégzik a természetes személyek személyes jellemzőinek szisztematikus és kiterjedt értékelését;
- személyes adatok különleges kategóriái, biometrikus adatokra vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése;
- nyilvános helyek nagymértékű, nyilvános megfigyelése.

Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatot jelentenek egy hatásvizsgálat keretében is elvégezhetők.

Az adatvédelmi hatásvizsgálat elvégzését az adatvédelmi tisztviselőnek szakmailag véleményezni kell.

A hatásvizsgálatnak ki kell terjednie:

- a tervezett adatkezelési műveletek módszeres leírására, az adatkezelés céljainak ismertetésére, beleértve az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintettek jogait és szabadságait érintő kockázatok vizsgálatára;

- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az Infotv.-el való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

Az adatkezelés során, a kockázatok változása esetén, illetve szükség szerint ellenőrzést kell lefolytatni annak érdekében, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A GDPR hatályba lépése előtt megkezdett adatkezelésekre nem szükséges azonnali hatásvizsgálatot végezni, de felülvizsgálat keretében valamennyi kockázatosnak ítélt adatkezelést felül kell vizsgálni. Amennyiben az adatvédelmi hatásvizsgálat azt állapítja meg, hogy az adatkezelési folyamat valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően konzultálni kell a felügyeleti hatósággal.

A felügyeleti hatóságot tájékoztatni kell az elvégzett hatástanulmányról, az adatkezelési folyamatban résztvevő adatkezelő, adatfeldolgozó feladatköreiről, a tervezett adatkezelés céljairól és módjairól, az érintettek jogainak, szabadságainak védelmében hozott intézkedésekről, garanciákról.

Az Adatkezelő jelen Szabályzat 4. számú mellékletében meghatározott szempontrendszer figyelembevételével végzi el az adatvédelmi hatásvizsgálatot.

15. ADATVÉDELMI INCIDENS

Az adatvédelmi incidens az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

A természetes személyeknek fizikai, vagyoni vagy nem vagyoni károkat okozhat az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában. Többek között: a személyes adataik feletti rendelkezés elvesztését, vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság lopást, vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Az Adatkezelő az adatvédelmi incidensek megelőzése és felderítése érdekében a következő technikai és szervezési intézkedéseket tette meg és ezen intézkedések megtételét rendszeresen ellenőrzi:

- Adatvédelmi szabályozási rendszert hozott létre és tart naprakészen.
- Az Adatvédelmi és Adatbiztonsági Szabályzatban meghatározta az adatvédelem szervezetét.
- Adatvédelmi tisztviselőt nevezett ki.
- Munkavállalóit folyamatosan informálja, oktatja az adatvédelmi szabályozásról, annak változásáról.
- A munkavállalók megismerik és nyilatkozatban fogadják el az adatvédelmi szabályozási rendszer rendelkezéseit.
- Az Adatkezelő az adatvédelmi incidensek megelőzése és felderítése céljából naplózási rendet vezet be és folyamatosan ellenőriz.

15.1. Az adatvédelmi incidenskezelés eljárásrendje

A Szabályzat hatálya alá tartozó személyek, bármely, az adatkezelő által működtetett informatikai rendszer, vagy manuális adatkezelés esetében haladéktalanul, de legkésőbb 24 órán belül kötelesek jelenteni az adatvédelmi tisztviselő felé, ha adatvédelmi incidens történt, vagy annak gyanúja merül fel.

Az adatvédelmi tisztviselő a bejelentés megtörténte után haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. Amennyiben az adatvédelmi incidens érinti az Adatkezelő informatikai rendszerét is, akkor a bejelentést a rendszergazda részére is meg kell küldeni.

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén a rendszergazdával együttműködve – megvizsgálja a bejelentést és amennyiben szükséges a bejelentőtől további adatokat kér az incidensre vonatkozóan.
A bejelentő köteles megadni az adatvédelmi incidens bekövetkezésének:

- időpontját, helyét,
- egyéb körülményeit,
- az érintett adatok körét,
- az érintett adatok mennyiségét,
- az érintett személyek körét, számát,
- az adatvédelmi incidens várható hatásait,
- a megelőzésre, következményeinek enyhítésére megtett intézkedések felsorolását.

Az adatvédelmi tisztviselő a felderítés során az alábbi kategóriák valamelyikébe sorolja az adatvédelmi incidenst:

1. Magas szintű adatvédelmi incidens:

- az adatvédelmi incidenssel érintett adatok köre: különleges adat vagy személyes adat;
- az adatvédelmi incidenssel érintettek száma: személyes adat esetén 100 vagy ennél több érintett, adatvédelmi incidenssel érintett különleges adat esetén legalább 1 érintett;
- azonnali intézkedést igényel;
- partner adatait érinti, függetlenül attól, hogy hány partnerről, vagy adatról van szó;
- hatás: jelentős vagy visszafordíthatatlan következmények;
- jelentős reakciót igényel a normális működésen túl;
- büntetőjogi következményei lehetnek;
- az adatvédelmi incidens és/vagy körülménye elektronikus vagy nyomtatott médiában elérhető.

Intézkedések:

Haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, melyben részt vesz az adatvédelmi tisztviselőn kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és az Adatkezelő vezetője. A munkacsoport meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre, továbbá – amennyiben szükséges – meghatározza az érintettek értesítésének módját és tartalmát. Az adatvédelmi tisztviselő rögzíti az incidenst az incidensek nyilvántartásában és értesíti a felügyeleti hatóságot 72 órán belül.

2. Közepes szintű adatvédelmi incidens:

- az adatvédelmi incidenssel érintett adatok köre: személyes adat;
- az adatvédelmi incidenssel érintettek száma: 100 érintettnél kevesebb;
- hatás: közepes, érintettek kényelmetlenségeket tapasztalhatnak;
- az észlelés napján igényel intézkedést, de azonnali intézkedést nem igényel (függetlenül attól, hogy az intézkedés az észlelést követően azonnal megtörténik);
- büntetőjogi következmény nem merülhet fel, de más jogi következmény felmerülhet (pl.: polgári jogi).

Intézkedések:

Haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre. Rögzíti az incidenst az incidensek nyilvántartásában és értesíti a felügyeleti hatóságot 72 órán belül.

3. Alacsony szintű adatvédelmi incidens:

- az adatvédelmi incidenssel érintett adatok köre: olyan adat, amely segítségével nem azonosítható be az érintett;
- az adatvédelmi incidenssel érintettek száma: nem értelmezhető, mert érintett nem beazonosítható;
- hatás: minimális (pl.: informatikai leállás tapasztalható);
- az adatok visszaállítása egyszerűen kivitelezhető.

Intézkedések:
A tudomásszerzéstől számított 2 napon belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre. Rögzíti az incidenst az incidensek nyilvántartásában.

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

15.2. Az adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet, melynek aktualizálásáról gondoskodik.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárításra megtett intézkedéseket.

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezést követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől számított 72 órán belül bejelenti a Hatóság részére (5. sz. melléklet), kivéve, ha az incidens valószínűsítve nem jár kockázattal a természetes személy jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére.

A hatósági bejelentés az alábbi adatokat tartalmazza:

- az adatvédelmi incidens bekövetkezésének, valamint a tudomásszerzés időpontját,
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét, elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit,
- a megtett vagy tervezett intézkedéseket.

Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

16. ZÁRÓ RENDELKEZÉSEK

Jelen Szabályzat 2021. január 01. 16. napján lép hatályba.

Az Adatkezelő köteles jelen Szabályzatban foglaltakat a munkavállalóival megismertetni, valamint gondoskodni arról, hogy az előírásait munkavégzésük során alkalmazzák.

Az Adatkezelő jelen Szabályzat hatályba lépéstől számított 60 napon belül intézkedik adatvédelmi gyakorlata felülvizsgálatáról és szükség esetén a jelen Szabályzat rendelkezéseinek megfelelő eljárások kialakításáról.

Nyíregyháza, 2020. december 10.

MELLÉKLETEK

1. SZÁMÚ MELLÉKLET

JOGOSULTSÁGKEZELÉSI MEGRENDELŐLAP

Igénylő/Felhasználó neve:

Szervezeti egység:

Szervezeti egység vezetője:

Az igény:

- ☐ jogosultságigénylés
- ☐ meglévő jogosultság módosítása
- ☐ összes jogosultság törlése munkaviszony megszűnése miatt

Az igény indoklása:

- ☐ új munkavállaló
- ☐ jelenlegi munkavállaló pozícióváltása

A meglévő jogosultság leírása:

Az igényelt jogosultság, a jogosultság jóváhagyásához szükséges információ leírása:

Kelt: .....

igénylő aláírása

Az igény:

- ☐ indokolt
- ☐ indokolatlan

.....

informatikai vezető aláírása

Az igény:

- ☐ indokolt
- ☐ indokolatlan

.....

vezető tisztségviselő aláírása

Teljesülés dátuma:

.....

informatikai vezető aláírása

2. SZÁMÚ MELLÉKLET

JOGOSULTSÁGKEZELÉSI NYILVÁNTARTÓLAP

dolgozó neve	munkaköre	jogosultág megadásának napja	jogosultság megszűnésének napja	jogosultság típusa	jóváhagyó vezető aláírása

.....

informatikai vezető aláírása

3. SZÁMÚ MELLÉKLET

ÉRDEKMÉRLEGELÉSI TESZT

1. Az érdekmérlegelés elvégzésének oka:

Amennyiben az adatkezelés jogalapját a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben 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.

Az adatkezelés jogszerűségének vizsgálatához el kell végezni egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását kell vizsgálni és megfelelően alátámasztani.

Az érdekmérlegelési teszt során az Adatkezelő:

- azonosítja az érdekmérlegelési teszt tárgyát képező személyes adat kezeléséhez fűződő jogos érdekét, és
- a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél, és
- megállapítja az Érintetteknek az érdekmérlegelési teszt tárgyát képező személyes adataival kapcsolatos érdekeit, az érintett alapjogokat, mint az Adatkezelő jogos érdekeinek ellenpontját, és
- elvégzi az Adatkezelő jogos érdekeinek és az Érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e.

2. Az Adatkezelő jogos érdeke:

3. Az adatkezelés célja, a kezelt személyes adatok köre, az adatkezelés időtartama:

- az adatkezelés célja:
- a kezelt személyes adatok köre:
- az adatkezelés időtartama:

4. Az érintett érdekei, alapjogok:

Az Alaptörvény rendelkezései értelmében mindenkinek joga van személyes adatai védelméhez. A GDPR kifejezett célja az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák. A GDPR továbbá alapelvi szinten rögzíti, hogy személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető.

Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. A személyes adatok jogosulatlan vagy céltól eltérő kezelését, illetve az adatok biztonságát szolgáló intézkedések elmulasztását a Büntető Törvénykönyv is büntetni rendeli.

Az Érintettnek, mint természetes személynek az előbbiek szerinti védelmet élvező érdeke fűződik ahhoz, hogy:

- információs önrendelkezési jogát gyakorolhassa,
- saját személyes adatainak mások általi kezeléséről maga rendelkezhessen,
- magánszféráját az adatkezelők tiszteletben tartsák,
- az információs önrendelkezési jog érvényesítését elősegítő, illetve a személyes adatok és ezen keresztül a magánszféra védelmét biztosító jogszabályi rendelkezések érvényesüljenek.

5. Az Adatkezelő jogos érdekének és az érintett érdekeinek, alapjogainak súlyozása:

6. Adatbiztonság, garanciák:

Az adatfelvételkor kötelezően nyújtott tájékoztatáson túl az Érintett bármikor információt kérhet az adatkezelés lényeges körülményeiről, melyről az Adatkezelő a lehető legrövidebb idő, maximum a kérelem beérkezésétől számított 25 napon belül írásban tájékoztatja. Az Adatkezelő honlapján elérhető az Adatvédelmi és Adatbiztonsági Szabályzat, mely részletes leírást tartalmaz az adatkezelés céljáról, jogalapjáról, időtartamáról, azok egyéb jogszabályi előírásoknak megfelelő jellemzőiről.

Az Érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését az adat felvételénél jelzett módon, illetve az Adatkezelő elérhetőségein.

Jogorvoslat lehetőséggel, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (a továbbiakban: NAIH) lehet élni. (székhely: 1055 Budapest, Falk Miksa utca 9-11. honlap: http://www.naih.hu)

Az adatkezelés a telefonszám kapcsolatfelvétel és esetlegesen kapcsolattartás céljából történő felhasználásáig, ellenőrzéséig terjed ki, annak jogosulatlan harmadik személyek felé történő kiadása, profilalkotás céljára történő felhasználása nem valósulhat meg. A valóságnak nem megfelelő személyes adat módosítása bármikor kérhető. Az Érintett kérheti személyes adatainak törlését, amennyiben véleménye szerint annak kezelése nem indokolt. Az Adatkezelő a kérelem beérkezését követő 15 napon belül írásban értesíti az Érintettet a kérelem kivizsgálásának eredményéről, illetve a jogorvoslati lehetőségekről.

Az adat törlésre kerül, ha az Adatkezelő megállapítása szerint a tárolt adat kezelése jogellenes, a törlést elrendelte a bíróság, a NAIH, az adat hiányos vagy téves, és ezen állapot nem kiküszöbölhető, vagy az adatkezelés célja megszűnt, illetőleg az adat tárolásának törvényi határideje lejárt. Az Adatkezelő az adatbiztonság érvényesülése okán, a GDPR, illetve az egyéb adat- és titokvédelmi szabályoknak megfelelve minden olyan technikai, szervezeti, szervezési és egyéb olyan műszaki feltételt biztosít, amely a kezelt adatok jogellenes nyilvánosságra hozatalát, jogosulatlan adattovábbítását, hozzáférését, módosítását, megsemmisülését megakadályozza. Előbbiekre tekintettel az Adatkezelő által kezelt adatok sérthetetlensége és titkossága teljeskörűen biztosított.

7. Az érdekmérlegelési teszt eredménye:

Kelt.:

Készítette: .....

4. SZÁMÚ MELLÉKLET

ADATVÉDELMI HATÁSVIZSGÁLAT (SEGÉDANYAG)

Az Adatkezelő tevékenységének ellátásához kapcsolódóan az alábbi adatkezelési eljárást kívánja bevezetni:

1. A bevezetni kívánt adatkezelési folyamat leírása:
2. Az adatkezelési műveletek módszeres leírása:
3. Az Adatkezelő és az adatkezelési folyamatban egyéb résztvevők megnevezése (a résztvevők státuszának és adatkezeléssel összefüggő tevékenységének leírása):
4. Az adatkezelés bevezetésének várható dátuma:

Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a)- f) pontjai az irányadók. Amennyiben a jogalapot a 6. cikk (1) bekezdés f) pontja jelenti: az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben 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. Az adatkezelés jogszerűségének vizsgálatához el kell végezni egy érdekmérlegelési tesztet, amelynek során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását kell vizsgálni és megfelelően alátámasztani.

Az Adatkezelő a GDPR 35. cikkének felhatalmazása alapján az alábbi hatásvizsgálatot végzi el:

1. Az adatkezelés jogalapja:

2. Az adatkezelés célja/ az Adatkezelő jogos érdekének leírása:

Az adatkezelés céljainak, indokainak leírása, különös tekintettel az adatkezelés szükségességének, alátámasztása:

A kezelt adatok körének pontos meghatározása. Annak meghatározása, hogy az egyes adatok tekintetében fennáll-e az adatkezelési cél, az adat a cél elérésére alkalmas-e, szükséges-e?

3. Az érintettek köre:

4. Az adatkezelés egyéb körülményei:

Az adatkezelés specialitásai, esetleges különleges személyes adatok, adattovábbítások megnevezése és indoka:

- adattovábbítás címzettje:
- adattovábbítás célja:
- adattovábbítás jogalapja:

5. Várható hatások, kockázatok:

1. Milyen lehetséges kockázatokkal jár az adatkezelés az érintettek jogainak esetleges sérelme szempontjából? Adatbiztonsági kockázatok vizsgálata. Az esetleges adatvesztések, jogosulatlan hozzáférések, vagy egyéb adatvédelmi incidensek bekövetkezésének lehetséges esetei, az incidens- bekövetkezés valószínűségének vizsgálata.

2. Melyek az érintettek érdekei az adatkezeléssel kapcsolatban?

3. Alternatíva keresése. Létezik-e más módszer a cél elérésére, amely az érintettek jogait kevésbé korlátozza? Ha létezik, ugyanolyan hatékonyan szolgálja-e a cél elérését?

4. Arányos-e az érintettek jogainak korlátozása az elérendő céllal? Csak annyiban korlátozza-e az érintettek jogait, amennyire a cél elérése érdekében szükséges?

6. A kockázatok elhárítására tett intézkedések, garanciák, a felek együttműködése

1. A megtett intézkedések leírása. Az egyes intézkedések mennyiben csökkentik az adatkezelési kockázatokat. Adatbiztonsági intézkedések leírása (fizikai, logikai, adminisztratív intézkedések megtétele).

2. Az érintettekkel való együttműködés biztosítása (panaszkezelés, jogorvoslati lehetőségek, kérelemre történő tájékoztatásadás lehetősége, adatvédelmi szabályzat megléte, adatvédelmi tisztviselő kinevezése, stb.).

7. **A hatásvizsgálat eredmények megállapítása, a kockázatok mértékének, jellegének leírása, további intézkedések megtételének szükségessége, előzetes konzultáció szükségessége:**

   A kockázat mértékének, jellegének leírása, következtetés levonása (miért jogszerű az adatkezelés, miért fűződik magasabb érdek a cél eléréséhez, illetve az érintettek jogainak korlátozása mitől arányos).

8. **Érintettek jogai:**

   - tájékoztatáshoz való jog
   - helyesbítéshez való jog
   - törléshez való jog
   - adathordozhatósághoz való jog
   - tiltakozáshoz való jog

Az Érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve - a jogszabályban elrendelt adatkezelések kivételével - törlését az adat felvételénél jelzett módon, illetve az Adatkezelő elérhetőségein. Jogorvoslat lehetőséggel, panasszal a **Nemzeti Adatvédelmi és Információszabadság Hatóságnál** (a továbbiakban: NAIH) lehet élni. Székhely: 1055 Budapest, Falk Miksa utca 9-11. honlap: http://www.naih.hu

Kelt.:

5. SZÁMÚ MELLÉKLET

ADATVÉDELMI INCIDENS BEJELENTÉSE

Iktatószám: Tárgy: adatvédelmi incidens bejelentése

Nemzeti Adatvédelmi és Információbiztonsági Hatóság

Budapest

Budapest, Pf. 9.

1363

Tisztelt Nemzeti Adatvédelmi és Információbiztonsági Hatóság!

A Nyíregyházi Élsport Nonprofit Korlátolt Felelősségű Társaság az Infotv. 25/J. §-a alapján a bekövetkezett adatvédelmi incidenssel kapcsolatosan az alábbi bejelentést teszi:

1. Az incidens bekövetkezésének időpontja:
2. Az incidensről való adatkezelői tudomásszerzése időpontja és módja:
3. Az adatvédelmi incidens jellege, körülményei:
4. Az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát:
5. Az adatvédelmi incidenssel érintett személyek köre és hozzávetőleges száma:
6. Az adatvédelmi tisztviselő neve, elérhetősége:
7. Az adatvédelmi incidens valószínűsíthető következménye:
8. A megtett intézkedések:

Kelt:

Tisztelettel:

.....

az Adatkezelő képviselője