A Haladás Sportkomplexum Fejlesztő Nonprofit Kft. (a továbbiakban: Haladás Noprofit Kft., vagy Adatkezelő) adatvédelmi incidenskezelési szabályzata

1. A szabályzat célja, hatálya

A szabályzat célja a természetes személyeket a személyes adataik kezelése kapcsán megillető jogok és szabadságok érvényesülésének, védelmének biztosítása. Mindezek érdekében annak az általános eljárásrendnek, továbbá az ezzel összefüggő feladatoknak meghatározása, amely mentén az Adatkezelő működési körében felmerülő adatvédelmi incidensek (illetve adatvédelmi incidens gyanús események) kivizsgálhatók, kezelhetők, valamint az ezekkel összefüggő - jogszabályban, illetve az Európai Unió kötelező jogi aktusában foglalt - kötelezettségek teljesíthetőek.

A szabályzat hatálya az Adatkezelő minden szervezeti egységére, valamennyi személyesadat-kezelési tevékenységére, és minden abban közreműködőre (munkavállalójára, megbízottjára, az adatfeldolgozóként bevont felekre) kiterjed, azt tevékenysége során mindenki köteles betartani.

1.1. Az adatvédelmi incidensek kezelése kapcsán irányadó legfontosabb normatív szabályozók:

- Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) - amely a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szól
- 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról (Infotv.)

2. Fogalom meghatározások

2.1. 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 azonosíthat

2.2. 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

2.3. 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.

2.4. adatgazda: az Adatkezelő legkisebb olyan önálló szervezeti egységének vezetője, amely szervezeti egység olyan nevesített feladatkörrel rendelkezik, amely végrehajtása személyes adatok kezelésével jár, és amely szervezeti egységnél az ott ellátott feladatokból kifolyóan a felmerülő adatvédelmi incidens elsődleges észlelése a legvalószínűbb. Alapestben adatgazdának minősülnek a Haladás Nonprofit Kft. szervezeti és működési szabályzata szerinti szervezeti egységeinek vezetői.

2.5. Adatkezelő: a Haladás Nonprofit Kft., amennyiben a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

2.6. adatvédelmi incidensről való tudomásszerzés ideje az Adatkezelő részéről: az az időpont, amikor a Haladás Nonprofit Kft. ésszerű mértékben bizonyossággal bír arról, hogy olyan biztonsági sérülés következett be, amely a személyes adatok, illetve az érintettek személyes adataik kezelésével összefüggő jogainak, szabadságának sérüléséhez vezetett

2.7. adatfeldolgozó: az a természetes, vagy jogi személy, közhatalmi szerv, amely a Haladás Nonprofit Kft., mint adatkezelő nevében jogszabályi kijelölés vagy szerződés alapján személyes adatokat kezel.

2.8. felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság.

2.9. érintett: az a természetes személy, akinek személyes adatait a Haladás Nonprofit Kft. kezeli (akinek az adatkezelési művelet, és az ennek kapcsán felmerülő incidens érinti a jogait és szabadságait).

2.10. a személyes adatok „biztonsága": a kezelt személyes adat olyan állapota, amelyben annak védelme a kezelt adatok bizalmassága, integritása (sértetlensége) és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

2.11.A személyes adatok „bizalmassága": a kezelt személyes adat olyan állapota, amikor csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

2.12. A személyes adat „integritása": a kezelt személyes adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, letagadhatatlanságát is, továbbá azt az állapotot, amely esetén a személyes adat rendeltetésének megfelelően használható.

2.13. a bizalmas jelleg sérülése: az Adatkezelő által kezelt személyes adatok jogosulatlan vagy véletlen közzététele vagy az ezekhez való jogosulatlan hozzáférés.

2.14. az integritás sérülése: az Adatkezelő által kezelt személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítása.

2.15. a rendelkezésre állás sérülése: az Adatkezelő által kezelt személyes adatok véletlen vagy jogosulatlan megsemmisítése, a személyes adatok elvesztése, a hozzáférés egyéb okból történő ellehetetlenülése.

2.16. a Haladás Nonprofit Kft. informatikai rendszere: a Haladás Nonprofit Kft. informatikai szabályzatában meghatározott rendszer

2.17. a Haladás Nonprofit Kft. informatikai rendszerét érintő biztonsági incidens: a Haladás Nonprofit Kft. informatikai rendszerét érintő olyan esemény, amely felveti a rendszer zavartalan, külső behatástól, illetve beavatkozástól mentes, rendeltetésszerű működésének sérelmét, a rendszerben tárolt adatokhoz való jogosulatlan hozzáférés, azok nyilvánosságra kerülése, illetve megváltozása, vagy megsemmisülése (törlése) lehetőségét, továbbá ezek bekövetkezése.

2.18. Szervezési (adminisztratív) adatvédelmi intézkedések: a kezelt személyes adatok védelme érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá az adatvédelemre, adatbiztonságra vonatkozó oktatás.

2.19. Technikai adatvédelmi intézkedések: a fizikai térben megvalósuló fenyegetések elleni technikai védelem (pl. elektronikai jelzőrendszer, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, klimatizálás és a tűzvédelem) valamint az online térben megvalósuló fenyegetések elleni védelem (pl. határvédelem, vírusvédelem, tűzfal, spamszűrés, jelszómenedzsment)

3. Az adatvédelmi incidensek egyes lehetséges előfordulási esetei

Amennyiben az Adatkezelő működési körében olyan esemény következik be, amely felveti a kezelt személyes adatok biztonságának, bizalmas jellegének, integritásának sérülését, akkor adatvédelmi incidensről beszélhetünk. Ilyen események lehetnek például:

a. a személyes adat elvesztése, vagy végleges hozzáférhetetlenné válása (pl. egy adathordozó olyan jellegű sérülése, amely miatt az azon tárolt személyes adatok, vagy egy részük nem nyerhető ki többé);

b. az Adatkezelő által használt informatikai rendszereket érintő jogosulatlan hozzáférések, vagy azok kísérletei, amelyek személyes adtok szivárgásával, illetéktelen megismerésével járnak;

c. az Adatkezelő informatikai eszközeinek, az általa használt informatikai rendszereknek üzemzavarai, meghibásodása, szolgáltatás kiesése, ezzel kapcsolatos adatvesztés, vagy annak gyanúja;

d. az Adatkezelő mobil informatikai, illetve adattároló eszközeinek elvesztése, sérülése, megsemmisülése, illetéktelen hozzáférése (pl. egy jelszavas védelem nélküli laptop ellopása, elhagyása, amelyen személyes adatok találhatóak);

e. az Adatkezelő digitális vagy papír alapú dokumentumainak elvesztése, sérülése, megsemmisülése, illetéktelen hozzáférése (pl. rossz címre küldött, személyes adatokat tartalmazó levél, vagy a munkavállalók jogosultsági idejével kapcsolatos adatokat tartalmazó iratok megsemmisülése az irattár beázása esetén).

4.Az adatvédelmi incidensekkel kapcsolatos általános kötelezettség

4.1. Az adatvédelmi incidensek megelőzéséhez szükséges technikai és szervezési intézkedések figyelembe vétele az adatkezelési tevékenységek előkészítése, megtervezése során, valamint azok alkalmazása, az adatkezelési tevékenységek végrehajtása során általánosan érvényesítendő szempontok, amelyeket a Haladás Nonprofit Kft. minden munkavállalója köteles betartani.

A munkafolyamatok során a személyes adatok kezelésére vonatkozó jogszabályi, illetve az Európai Unió kötelező jogi aktusaiban foglalt előírások betartásával, valamint a Haladás Nonprofit Kft. szervezeti Integritást sértő események kezelésének eljárásrendjében, továbbá a jelen szabályzatban meghatározottak figyelembe vételével kell eljárni. Gondoskodni kell arról, hogy a kezelt személyes adatok az adatkezelés teljes folyamatában megfelelően védve legyenek az illetéktelen hozzáféréstől, a nyilvánosságra kerüléstől (figyelemmel a közérdekű és közérdekből nyilvános adatokra vonatkozó előírásokra), továbbá hogy a kezelt személyes adatok változatlansága (integritása) biztosított legyen.
A fenti szempontok biztosítását szolgáló szervezési és technikai intézkedések meghatározása tekintetében a Haladás Nonprofit Kft. adatvédelmi tisztviselőjének (a

továbbiakban: adatvédelmi tisztviselő) szakmai tanácsát a Haladás Nonprofit Kft. bármely szervezeti egységnek vezetője, munkavállalója kikérheti.

4.2. Az adatvédelmi incidensek belső bejelentése: az Adatkezelő bármely munkavállalója, megbízottja amennyiben a Haladás Nonprofit Kft. által kezelt személyes adatokkal kapcsolatban adatvédelmi incidenst észlel (vagy erre utaló információ jut tudomására), azt köteles a feladat és hatáskörrel rendelkező szervezeti egység vezetőjének, mint adatgazdának haladéktalanul bejelenteni. Amennyiben a feladat és hatáskörrel rendelkező szervezeti egység nem állapítható meg a bejelentést a Haladás Nonprofit Kft. ügyvezetői irodavezető felé kell megtenni. Amennyiben a bejelentés az ügyvezetői irodavezető felé történik, a bejelentést fogadó késedelem nélkül továbbítja azt a Haladás Nonprofit Kft. ügyvezetője (a továbbiakban: ügyvezető) felé, annak érdekében, hogy a kivizsgálást végző kijelölése megtörténhessen.

A bejelentésnek legalább az alábbiakat kell tartalmaznia:
a) bejelentő neve,
b) munkahelyi telefonszáma és e-mail címe,
c) az érintett szervezeti egység megnevezése,
d) az incidens tárgya (milyen jellegű, és milyen személyes adatokat érint),
e) az incidens bekövetkezésének ideje (amennyiben ismert);
f) a bejelentő tudomására jutás ideje, módja, valamint,
g) hogy az incidens az Adatkezelő informatikai rendszerét érinti-e, és ha igen, milyen formában.

4.2.1. Az adatgazda szervezeti egység vezetője a hozzá érkező bejelentést haladéktalanul ellenőrzi, amelynek során elsődlegesen azt vizsgálja meg, hogy az adatvédelmi incidens ténylegesen megvalósult-e, valamint késedelmet nem tűrő (azonnal végrehajtandó) intézkedések szükségesek-e.

4.2.2. Amennyiben a bejelentett incidens az Adatkezelő informatikai rendszerét, vagy az Adatkezelő által igénybe vett adatfeldolgozó informatikai rendszerében megvalósuló adatkezelését érinti, az adatgazda – haladéktalanul, rövid úton, telefonon - értesíti az Adatkezelő rendszergazdáját, illetve az igénybe vett adatfeldolgozó illetékes vezetőjét.
Az értesítés megtörténtéről – ha az telefonon történt - feljegyzést kell készíteni.

4.2.3. Az adatgazda - a 4.2.1. és 4.2.2. pontokban megjelölt intézkedéseket követően haladéktalanul – köteles, a hivatali út betartásával az ügyvezető felé jelezni, ha adatvédelmi incidens gyanúját észleli, vagy hozzá ilyen bejelentés érkezett.

4.2.4. A felmerült adatvédelmi incidensről, annak gyanújáról, a tett, illetve tervezett intézkedésekről az adatgazda minden esetben az incidens felmerülését követően késedelem nélkül tájékoztatja az adatvédelmi tisztviselőt is az adatvedelem@haladas.eu hivatali e-mail címen, továbbá rövid úton telefonon is.

4.3. Az Adatkezelő által igénybe vett adatfeldolgozók (pl. könyvviteli szolgáltatást nyújtók, tárhely, illetve egyéb informatikai szolgáltatást nyújtó partner, biztonsági/vagyonvédelmi szolgáltató) kötelessége, hogy a saját működési körében felmerült, és az Adatkezelő megbízása folytán kezelt személyes adatokat érintő adatvédelmi incidenseket késedelem nélkül, de legfeljebb azok felmerülését/észlelését követő 24 órán belül bejelentse az Adatkezelő felé.

4.3.1. Amennyiben az adatvédelmi incidens az Adatkezelő által igénybe vett adatfeldolgozónál következik be, azt az Adatkezelő részére történő bejelentését követően – ha az nem az ügyvezető felé történt – az ügyvezető felé haladéktalanul jelezni kell, aki ezt követően dönt az adatfeldolgozónál lefolytatandó estleges helyszíni ellenőrzésről.

4.3.2. Az adatfeldolgozótól származó bejelentést dokumentált formában kell rögzíteni, amelynek minimálisan az alábbiakat kell tartalmaznia:

a) az bejelentés ideje
b) az bejelentést adó, illetve fogadó személye, elérhetősége
c) az adatvédelmi incidens kapcsán addig tett megállapítások
d) az adatvédelmi incidens kapcsán addig tett intézkedések
e) az Adatkezelő utasításai az incidens kapcsán.

Amennyiben az adatfeldolgozók által kezelt személyes adatokat érinti az adatvédelmi incidens, a fenti értesítést követően az adatfeldolgozónak a Haladás Nonprofit Kft., mint Adatkezelő utasításaira is tekintettel kell a továbbiakban eljárnia. Utasítás adásra az ügyvezető, vagy az általa erre - írásban - felhatalmazott személy jogosult. **Ilyen esetekben a felügyeleti hatóság felé történő bejelentésről, valamint – annak szükségessége esetén - az érintettek értesítéséről szintén a Haladás Nonprofit Kft. ügyvezetője jogosult dönteni.**

4.3.4. Az Adatkezelő által igénybe vett adatfeldolgozók szerződéseiben a fenti előírások teljesülését biztosító adatvédelmi jellegű kikötések szerepeltetése – beleértve a helyszíni ellenőrzések lehetőségének fenntartását is – a szerződések előkészítése, illetve módosítása során figyelembe veendő feladat.

4.4. Amennyiben az Adatkezelő ellenőrzésre jogosult szervezeti egységei, munkavállalói a feladataik ellátása során adatvédelmi incidenst észlelnek, haladéktalanul kötelesek értesíteni az illetékes adatgazdát (vagyis annak a szervezeti egységnek a vezetőjét, amelynek feladatai ellátása keretében az incidenssel érintett személyes adat kezelése történik).

5. Az adatvédelmi incidensek kivizsgálásának felelősségi rendje

5.1. Az ügyvezető dönt az adatvédelmi incidensek kivizsgálásának/kivizsgáltatásának, illetve a kivizsgálást végző kijelölésének kérdésében.

Az ügyvezető a hozzá érkező jelzést követően dönt az adatvédelmi incidens kivizsgálással megbízott személy - figyelemmel az esetleges összeférhetetlenségre – kijelöléséről. Amennyiben az elsődleges információk alapján nem forog fenn az összeférhetetlenséget megalapozó körülmény (pl. esetleges személyes felelősség) a kivizsgálást az adatgazda szervezeti egység vezetője végzi.

5.2. A kivizsgálást - a 6. pontban foglaltak figyelembe vételével - olyan időkeretekben kell megtenni, hogy az Adatkezelő az adatvédelmi incidensről történő tudomásszerzést követő 72 órán belül adott esetben a felügyeleti hatóság felé fennálló bejelentési kötelezettségének eleget tudjon tenni.

5.3. Amennyiben az adatvédelmi incidens (vagy annak gyanúja) kapcsán adott esetben rendelkezésre álló adatok jellegére, minőségére, mennyiségére tekintettel a szükséges döntés meghozatala, illetve az incidens kivizsgálása érdekében az adatgazda, illetve az ügyvezető szükségesnek tartja, kikéri az adatvédelmi tisztviselő szakmai tanácsát.

6. Az adatvédelmi incidensek kezelésének és kivizsgálásának folyamatszerű lépései

6.1. Az adatvédelmi incidens kezelésének elsődleges lépései:

a) az incidens gyanújának felmerülése →
b) bejelentés az adatgazda szervezeti egység vezetője felé →
c) elsődleges ellenőrzés, késedelmet nem tűrő intézkedések (pl. adathordozó adattartalmának másolása, vagy nyílt hálózatról történő lekapcsolás) megtétele →
d) amennyiben az adatvédelmi incidens az Adatkezelő informatikai rendszerét érintő biztonsági incidens is egyben, a rendszergazda felé is jelzés, (továbbá az adatvédelmi tisztviselő értesítése) →
e) ügyvezető felé jelzés →
f) döntés a kivizsgálást végző személyéről, valamint arról, hogy szükség van-e további késedelmet ne tűrő intézkedésekre (pl. helyszíni ellenőrzés az adatfeldolgozónál)
g) az adatvédelmi incidens körülményeinek, következményeinek feltárása;
h) az írásba foglalt megállapítások, javaslatok felterjesztése az ügyvezető felé.

6.2. Az adatvédelmi incidens kivizsgálása keretében a cél annak tisztázása, hogy:

a) ténylegesen a kezelt személyes adat sérült-e, elveszett-e, jogosulatlan számára hozzáférhetővé vált-e, esetleg nyilvánosságra került-e;
b) szándékos (rosszindulatú) avagy gondatlan (véletlen) eseményről van-e szó, megállapítható-e a felelős;
c) kik az érintettek, és hány érintett adatáról van szó;
d) milyen típusú személyes adatok érintettek az incidens által (pl. személyazonosító adatok, életrajzi adatok, pénzügyi személyes adtok/folyószámla adatok, esetleg un. érzékeny/különleges személyes adatok pl. egészségi állapottal kapcsolatos adatok) és milyen mennyiségű adatról van szó, azokból milyen könnyen lehet az érintetteket egyedileg azonosítani;
f) az incidens milyen következményekkel járt, illetve járhat az érintettekre nézve, amelynek során mindenekelőtt az alábbiakra kell tekintettel lenni:

- az érintett adatok fajtája;
- az érintett személyek azonosíthatóságának lehetősége;
- az incidens körülményei;
- adat biztonságának csökkenése;
- rosszindulatú támadásra és a szándékosságra utaló jelek;
- az érintett adatok érzékenysége, kompromittálásra, károkozásra való alkalmassága;

g) az adatvédelmi incidens milyen kockázattal jár az érintettekre nézve?

Az adatvédelmi incidens kockázati szintjének meghatározása: kockázattal nem járó[1]; kockázattal járó[2]; valószínűsíthetően magas kockázattal járó[3] incidens.

6.3. Az incidens megvalósult, illetve lehetséges következményeinek megállapítását követően a következmények elhárítására, enyhítésére a szükséges intézkedéseket meg kell tenni (pl. az internetre felkerült adatok esetében az érintett oldal üzemeltetőjének soron kívüli megkeresése az adatok eltávolítása érdekében).

6.4. Valamennyi a 6.2.-6.3. pontokban megjelölt tevékenységhez kapcsolódóan a tevékenységet végzők az adatvédelmi tisztviselő szakmai tanácsát kikérik a döntés előkészítése, végrehajtása tekintetében.

6.5. Az adatvédelmi incidensek kezelésével kapcsolatos egyszerűsített tevékenységi folyamatábrát jelen szabályzat **1. számú melléklete** tartalmazza.

7. Az adatvédelmi incidens hatósági bejelentése

7.1. Az adatvédelmi incidens körülményeinek kivizsgálásáról az 5.-6. pontok figyelembe vételével a kivizsgálással megbízott személy- az incidens következményeinek orvoslását célzó intézkedésekre irányuló javaslatot is tartalmazó - írásos összefoglalót készít, és azt az incidens ismertté válását követő 48 órán belül bemutatja az ügyvezetőnek. Az írásos összefoglaló elkészítése kapcsán a kivizsgálással megbízott személy kikéri az adatvédelmi tisztviselő szakmai tanácsát.

7.2 A felügyeleti hatóság felé történő bejelentésről, valamint az érintett tájékoztatásáról az ügyvezető dönt. Ugyancsak az ügyvezető dönt arról, hogy adott esetben a kivizsgálás adatai alapján a felügyeleti hatóság, illetve az érintett értesítése nem szükséges. Ez utóbbi esetben az incidens kivizsgálásáról készült írásos összefoglaló anyagra az erre vonatkozó döntés indokait is kellő részletességgel fel kell vezetni.

7.3. Az adatvédelmi incidenst - kivéve, ha az ügyvezető döntése szerint az kockázattal nem járó incidens - a felügyeleti hatóságnak az Adatkezelő általi tudomásszerzést követő **72 órán belül kell bejelenteni**, a bejelentésben az alábbiakat kell szerepeltetni:

1 Kockázattal nem járó az incidens például, ha az érintett adatok nem teszik lehetővé az érintett azonosítását (pl. csak egy olyan személyes adat került illetéktelen kézbe, ami sok emberhez is köthető lenne), vagy olyan adat vált hozzáférhetővé, amit az érintett egyébként is nyilvánosságra hozott pl. közösségi oldalon), vagy ha az érintett adat egyáltalán nem alkalmas arra, hogy azzal visszaéljenek, hátrányos következményeket idézzenek elő az érintettre nézve;

2 Kockázattal járó az incidens például, ha az érintett adatok könnyen lehetővé teszik az érintett azonosítását, de az eset körülményei (pl. vétlen incidens), és/vagy az adatok jellege miatt, észszerűen nem kell az érintettre nézve hátrányos következményekkel számolni (pl. név vagy szakmai tapasztalat, vagy olyan adatok érintettek az incidens által, amelyek rosszindulatú felhasználása az adott körülmények szerint nem életszerű pl. az érintett járművezetői engedélyének kategóriái);

3 Valószínűsíthetően magas kockázattal járó az incidens például, ha olyan adatok érintettek a incidensben, amelyek rosszindulatú felhasználásával az adott körülmények szerint, vagy az általános tapasztalatok szerint számolni lehet (pl. személyes adatok, plusz pénzügyi személyes adatok, egészségügyi adatok), vagy ha az érintett adat(ok) „érzékeny" jellege miatt valószínűsíthető, hogy az incidens hátrányos következményekkel járhat az érintettre nézve (pl. olyan adatok, amelyek rosszindulatú felhasználásával az érintett kompromittálható, vagyoni érdekei, személyiségi jogai támadhatóak, betegséggel, gyógykezeléssel kapcsolatos adatok, jelszavak, belépési azonosítók).

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az illetékes felügyeleti hatóság adatai:

megnevezés:	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
cím:	1055. Budapest, Falk Miksa utca 9-11
e-mail:	ugyfelszolgalat@naih.hu
telefon:	(1) 391 1400

A bejelentést on-line bejelentő felületen a hatóság *www.naih.hu* internetes oldalán, az „Adatvédelmi Incidensbejelentő Rendszer" menüpontban, az ott elérhető elektronikus űrlapok kitöltésével és megküldésével kell megtenni.

Az adatvédelmi incidens felügyeleti hatóság felé történő bejelentését – az ügyvezető eltérő döntése hiányában – az adatvédelmi tisztviselő végzi, ennek érdekében az ügyvezető által jóváhagyott írásos összefoglalót a rendelkezésére kell bocsátani.

Amennyiben az adatvédelmi incidens észlelését követő 72 órán belül az Adatkezelőnek nem áll rendelkezésére valamennyi a bejelentésben részletezendő – fent megjelölt – információ, a bejelentést ebben az esetben is 72 órán belül meg kell tenni a felügyeleti hatóság felé, azonban abban jelezni kell, hogy a további információkat szakaszosan – az azokról való tudomásszerzést követően – jelenti be az Adatkezelő.

7.4. Amennyiben az adatvédelmi incidens valószínűsíthetően **magas kockázattal** jár a természetes személyek jogaira és szabadságaira nézve, **az Adatkezelő** (a felügyeleti hatóság felé történő bejelentése mellett) indokolatlan késedelem nélkül **tájékoztatja az érintettet is** az adatvédelmi incidensről. Ha az Adatkezelő olyan védelmi intézkedéseket alkalmazott – mint például a titkosítás –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat, úgy az érintettet nem kell tájékoztatni.

7.5. Nem kell a felügyeleti hatóság felé **az adatvédelmi incidenst bejelenteni (és az érintettet sem kell tájékoztatni)**, ha az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az Adatkezelő saját nyilvántartásában ebben az esetben is szerepeltetni kell az incidenst.

8. Az adatvédelmi incidens kivizsgálásával összefüggő további teendők

8.1. Meg kell vizsgálni, hogy az incidenssel érintett adatok, illetve folyamatok tekintetében az Adatkezelő (illetve az általa bevont adatfeldolgozó) milyen szervezési, technikai védelmi intézkedéseket tett, és azok megfelelőek voltak-e, milyen további intézkedésekre van lehetőség/szükség. Ennek során a Haladás Nonprofit Kft. szervezeti integritást sértő

események kezelésének eljárásrendjében meghatározott feladatok végrehajtása érdekében az integritás felelős tájékoztatását is el kell végezni.

8.2. A kivizsgálás során keletkezett adatok felhasználásával az Adatkezelőnél felmerült adatvédelmi incidensek nyilvántartását - a jelen szabályzat **2. számú mellékletét képező űrlap szerinti tartalommal** - vezetni kell. Az ügyvezető által az incidens kivizsgálására kijelölt személy köteles gondoskodni az adatvédelmi incidens nyilvántartás adatainak feltöltéséről. A nyilvántartásba bejegyezni tervezett adatokat előzetesen az adatvédelmi tisztviselő részére meg kell küldeni, aki arra 24 órán belül észrevételt tehet.

9. A kivizsgálást követő teendők

9.1. Az adatvédelmi incidens kivizsgálása kapcsán készült írásos összefoglalót, és mellékleteit az Adatkezelő az incidenssel érintett személyes adatot tartalmazó dokumentum selejtezését, illetve levéltárba adását követő 5 évig megőrzi, majd az Adatkezelő mindenkori hatályos iratkezelési szabályzatának megfelelően selejtezi, vagy az illetékes levéltárnak átadja.

Amennyiben az adott adatvédelmi incidens kapcsán hatósági eljárás, vagy egyéb jogi igény (pl. kártérítés, sérelemdíj) érvényesítésére irányuló eljárás indul, a megőrzés ideje az adott eljárással kapcsolatos kötelezettség, vagy jogi igény elévülésének idejéhez igazodik.

9.2. Az Adatkezelőnél előforduló adatvédelmi incidensek jellemzőit rendszeresen (legalább félévente) át kell tekinteni. Amennyiben az előforduló adatvédelmi incidensek feltárt sajátosságai, okai az Adatkezelő által alkalmazott technikai vagy szervezési adatvédelmi intézkedések elégtelen voltára vagy nem megfelelő működésére engednek következtetni, a technikai, illetve szervezési intézkedések megfelelő módosítására az illetékes adatgazda, valamint az adatvédelmi tisztviselő javaslatot tehet az ügyvezető felé.

9.3. Amennyiben az adatvédelmi incidens bekövetkezéséhez vezető hiányosságok az Adatkezelő által bevont adatfeldolgozó működési körében felmerülő okra vezethetők vissza, ezek megszüntetésére – megfelelő határidő kitűzésével – az adatfeldolgozót írásban fel kell szólítani. A hiányosságok orvoslásának megtörténtét az ügyvezető döntésének megfelelően az adatfeldolgozónál ellenőrizni kell. Az adatfeldolgozó esetleges kárfelelősségének érvényesítéséről, illetve indokolt esetben az adatfeldolgozás alapjául szolgáló szerződés megszüntetéséről szintén az ügyvezető dönt. A döntése kialakítása kapcsán az ügyvezető szükség esetén az adatvédelmi tisztviselő szakmai tanácsát kikéri.

10. Záró rendelkezések

Jelen szabályzat jóváhagyása napján lép hatályba és visszavonásig érvényes, rendelkezéseit ismertetni kell a Haladás Nonprofit Kft. teljes személyi állományával, valamint – a rájuk vonatkozó részben – a Haladás Nonprofit Kft. által bevont adatfeldolgozókkal.

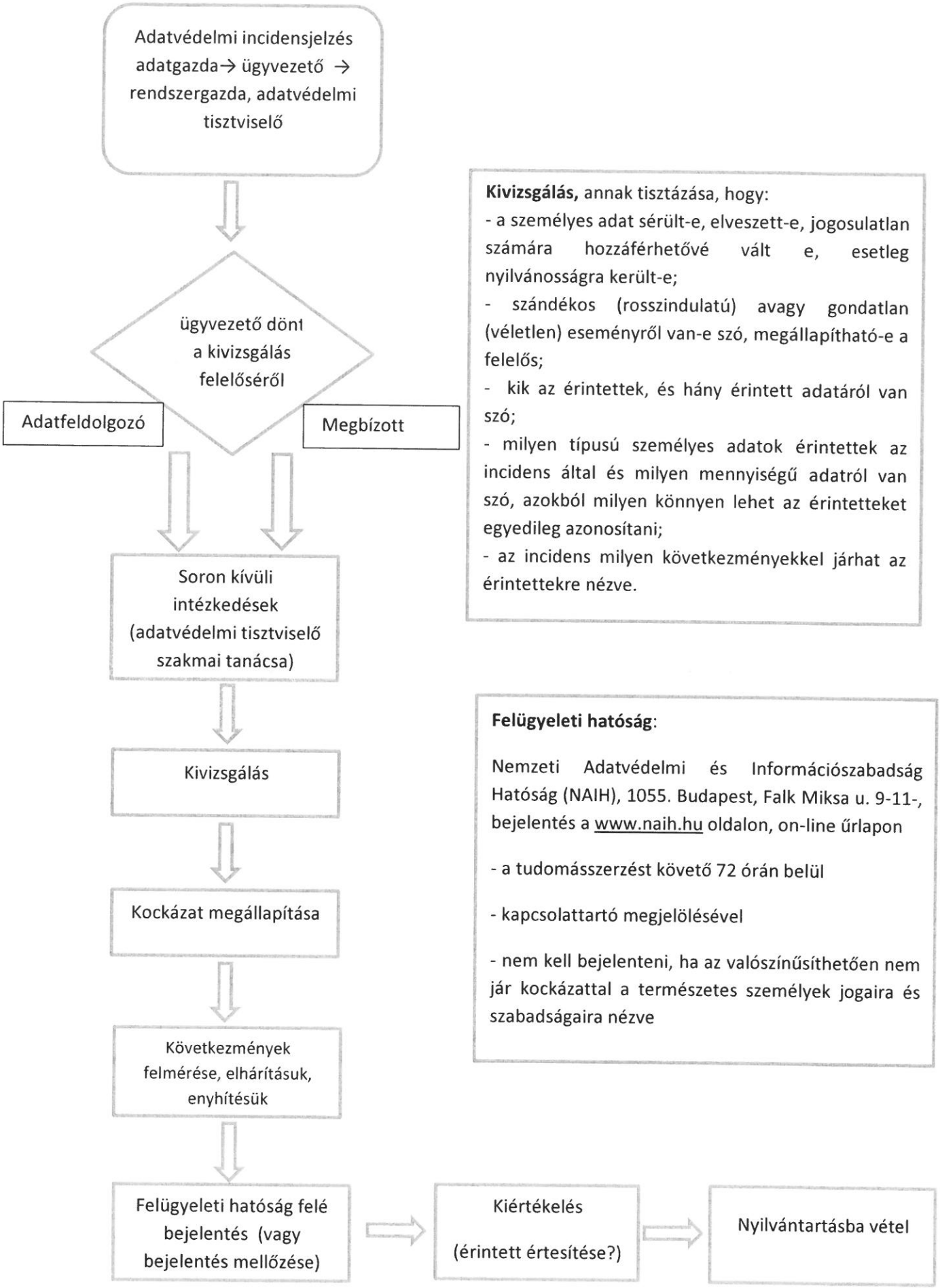
Szombathely, 2022. június 30.

Haladás Sportkomplexum Fejlesztő Nonprofit Kft.
9700 Szombathely, Rohonci út 3.
Adószám: 24827373-2-18

.....

ügyvezető

Adatvédelmi incidens kezelésének, kivizsgálásának tevékenységi folyamatábrája ***1. sz. melléklet***



2. sz. melléklet

ADATVÉDELMI INCIDENS NYILVÁNTARTÁS

adatkezelő megnevezése: Haladás Sportkomplexum Fejlesztő Nonprofit Kft.;
székhely: 9700 Szombathely, Rohonci út 3.
tel: +36 94 900 138
e-mail: office@haladas.eu
adatvédelmi tisztviselő elérhetősége: adatvedelem@haladas.eu

1. Az adatvédelmi incidens jellegének leírása (Mi történt? Miért valószínűsíthető/állapítható meg a személyes adatok biztonságának, bizalmas jellegének, épségének a sérülése?)
2. Kik az érintettek, és hány érintett van (azok a természetes személyek, akiknek az adatairól szó van) **szükséges- e az érintett tájékoztatása**, ha igen a megtörténtének ideje, amennyiben nem annak okai
3. Milyen, és mennyi személyes adatot érint az incidens (az adatok típusát kell megadni pl. név, születési adtok, bankszámlaszám)
4. Az incidensből eredő valószínűsíthető következmények (milyen konkrét adatok utalnak arra, hogy valamely érintett(ek) hátrányos következményekkel kell számoljanak, és mik ezek a következmények)
5. A következmények orvoslására tett, vagy tervezett intézkedések (ide értve a már bekövetkezett hátrányos következmények enyhítését célzó intézkedéseket is)
6. Felügyeleti hatóság felé a bejelentés szükséges-e, ha igen a megtörténtének időpontja, az adatkezelő részéről kapcsolattartásra kijelölt személy megjelölése; **ha nem, annak indokai** (kockázat nélküli az incidens)