# NYSÜ NYÍREGYHÁZI SPORTLÉTESÍTMÉNYEKET ÜZEMELTETŐ KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

# ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

## 1. ÁLTALÁNOS RENDELKEZÉSEK

Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, hogy a NYSÜ Nyíregyházi Sportlétesítményeket Üzemeltető 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, továbbá egységes szerkezetbe foglalja az adatkezelésben résztvevő dolgozók számára az adatkezelési folyamatokat.

Az Adatkezelő jelen Szabályzatban leírtak szerint gyűjti, rögzíti, rendszerezi és tárolja az ügyfelei, munkavállói, valamint egyéb partnerei személyes adatait.

## 2. AZ ADATKEZELŐ ADATAI

**Név:** NYSÜ Nyíregyházi Sportlétesítményeket Üzemeltető Korlátolt Felelősségű Társaság
**Rövidített név**: NYSÜ Kft.
**Székhelye:** 4400 Nyíregyháza, Géza utca 8-16.
**Képviselője:** Hajnal Gusztáv, ügyvezető
**Elérhetősége**: 42/512-725
**Adószáma:** 10731785-2-15
**Telephely 1:** Nyíregyházai Atlétikai Centrum
**Címe:** 4400 Nyíregyháza, Tiszavasvári út 4.
**Telephely 2:** Eissmann Nyíregyházi Városi Uszoda
**Címe:** 4400 Nyíregyháza, Bujtos utca 4.
**Adatvédelmi tisztviselő neve, elérhetősége:** Kutykó Róbert e-mail: adatvedelem@nysu.hu

## 3. A SZABÁLYZAT HATÁLYA

Személyi hatály
A Szabályzat személyi hatálya kiterjed:

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

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

Időbeli hatály
Jelen Szabályzat időbeli hatálya annak kihirdetésétől, visszavonásáig, vagy az Adatkezelő által történő egyoldalú módosításáig tart.

## 4. FOGALOM MEGHATÁROZÁSOK

A fogalom meghatározások tekintetében a GDPR, valamint az Infotv. rendelkezései irányadóak.

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

**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.

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

**Adatkezelés**: 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.

**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.

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

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

**Nyilvánosságra hozatal**: az adat bárki számára történő hozzáférhetővé tétele.

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

**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.

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

Amennyiben a mindenkori hatályos adatvédelmi jogszabályok fogalom meghatározásai eltérnek jelen Tájékoztató értelmező rendelkezéseitől, akkor a hatályos jogszabályok által meghatározott fogalmak az irányadóak.

## 5. A SZABÁLYZAT ADATKEZELÉSI 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:

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.

**6.1. 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.

**6.2. 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.

### 6.5. 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.

### 6.6. 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.

## 7. 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.

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.

## 8. 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 NYSÜ 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.

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.

## 10. 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.

- 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.

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.

## 11. ADATBIZTONSÁG - SPECIÁLIS SZABÁLYOK

### 11.1. 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.

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.

### 11.2. 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.

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.

## 12. 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.

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 partner.

## 14. 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.

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.

**Hozzáféréshez való jog:** Az érintett bármikor jogosult személyes adatairól és az azok kezelésével összefüggő információkról az Adatkezelőtől tájékoztatást kérni.

**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.

**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 törvényben meghatározott egyéb esetekben.

**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.

### 15.1 AZ ÉRINTETTI JOGOK GYAKORLÁSA

Az érintettek jogaik gyakorlásával kapcsolatos kérelmüket szóban, írásban vagy elektronikus úton is előterjeszthetik. Az Adatkezelő az érintett kérelmét indokolatlan késedelem nélkül, de lekésőbb a beérkezéstől számított 25 napon belül tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazott tartalommal teljesíti. A kérelem megtagadásáról az Adatkezelő szintén ezen határidőn belül dönt és tájékoztatja az érintettet a kérelem megtagadásának okairól, valamint a jogorvoslati lehetőségekről.

Adatkezelő a kérelmek teljesítéséért díjat, költségtérítést nem számít fel. Abban az esetben, ha az érintettől azonos adatkörre vonatkozó újabb kérelem érkezik be az előző, már teljesített kérelmet követő egy éven belül, Adatkezelő fenntartja magának a jogot arra, hogy a kérelem teljesítéséért a teljesítéssel kapcsolatos munkateherrel arányos költségtérítést állapítson meg.

## 16. ZÁRÓ RENDELKEZÉSEK

Jelen Szabályzat 2022. augusztus 30. 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 köteles intézkedni adatvédelmi gyakorlata felülvizsgálatáról és szükség esetén a jelen Szabályzat rendelkezéseinek megfelelő eljárások kialakításáról.

Nyíregyháza, 2022. augusztus 30.

2. SZÁMÚ MELLÉKLET

JOGOSULTSÁGKEZELÉSI NYILVÁNTARTÓLAP

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

.....

informatikai vezető aláírása

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:** .....

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.:

## 6. SZÁMÚ MELLÉKLET

### ADATKEZELÉSI NYILVÁNTARTÁS

Nyíregyházi Sportlétesítményeket Üzemeltető Kft.

1. Az **NYSÜ *Kft.***, mint adatkezelő, az Európai Parlament és a Tanács (EU) 2016/679 RENDELET 30. cikk (1) bekezdése szerint az alábbi ***adatkezelési nyilvántartást vezeti.***

2. Az ***NYSÜ Kft.*** a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

- az adatkezelő neve és elérhetősége, valamint - ha van ilyen - a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés céljai;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
- ha lehetséges, a technikai és szervezési intézkedések általános leírása.

**3. Az adatkezelő adatai:**

| | |
|---|---|
| Az adatkezelő neve, típusa: | Nyíregyházi Sportlétesítményeket Üzemeltető Kft. |
| Címe: | 4400 Nyíregyháza, Géza utca 4-6. |

Adatkezelő informatikai rendszere és hálózata egyaránt védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá a számítógépvírusok, a számítógépes betörések és a szolgálat megtagadásra vezető támadások ellen. Az üzemeltető a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik. A papír alapú, személyes adatokat tartalmazó dokumentumok zárható szekrényben kerülnek tárolásra.