Magyar Kézilabda Utánpótlásért Alapítvány

Adatvédelmi és Adatbiztonsági Szabályzat

Tartalom

I. Bevezető rendelkezések 3
1. Az Adatvédelmi és Adatbiztonsági Szabályzat célja, hatálya 3
2. Jogszabályi hivatkozás, kapcsolat az adatkezelő belső szabályzataival 4
3. Értelmező rendelkezések 5
4. Az adatkezelők adatai 7
II. Adatvédelem 8
5. Adatkezelőre és adatkezelésre vonatkozó szabályok, alapelvek 8
6. Az adatkezelések jogalapjai 9
7. A GDPR 9. cikk szerinti személyes adatok különleges kategóriáinak kezelése 10
8. Szervezeten belüli feladatok és felelősségek 11
9. Adatvédelmi nyilvántartás 16
10. Az adatok tárolása 17
11. Az adatok felhasználása 17
12. Az adatok feldolgozása 18
13. Adattovábbítás harmadik ország felé, hatósági adatszolgáltatás 21
14. A személyes adatok törlése, helyesbítése, adatkezelés korlátozása 24
15. Az érintett tájékoztatáshoz, hozzáféréshez való joga 25
16. Adathordozáshoz, visszavonáshoz való jog, automatizált döntéshozatal 26
17. Tiltakozás a személyes adatok kezelése ellen 27
18. Adatvédelmi hatásvizsgálat 27
19. Adatvédelmi incidens 32
20. Adatkezelési folyamatok megváltozása, új adatkezelés bevezetése 33
III. Adatbiztonság 34
21. A NEKA által kezelt adatok biztonsága 34
22. Automatizált adatfeldolgozás 36
23. Manuális kezelésű adatok 38
24. Munkavállalói adatbiztonsági kötelezettségek 38
25. Titoktartási kötelezettség 39
IV. A jogellenes adatkezelés következményei 40
26. Záró rendelkezések 42

I. BEVEZETŐ RENDELKEZÉSEK

1. AZ ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT CÉLJA, HATÁLYA

1.1. Az Adatvédelmi és Adatbiztonsági Szabályzat célja, hogy meghatározza Magyar Kézilabda Utánpótlásért Alapítványnál (NEKA, Adatkezelő) mint Adatkezelőnél zajló adatkezelések törvényes kereteit, biztosítsa az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesítését, elősegítse az adatbiztonság követelményeinek való megfelelést, továbbá megakadályozza a jogosulatlan adatkezelést. Az Adatvédelmi és Adatbiztonsági Szabályzat kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat, különös tekintettel a munkavállalók szerepére az adatbiztonságban.

1.2. Jelen Szabályzat hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány egyes szervezeti egységei közötti, az Adatkezelő által igénybe vett adatfeldolgozók felé irányuló adatáramlásra, valamint az Adatkezelő és más adatkezelőkkel való személyes adatokat érintő kommunikációra.

1.3. Jelen Szabályzat hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány által fenntartott NEKA Kollégium (további Adatkezelő) adatkezeléseire, a kollégium egyes szervezeti egységei közötti, az általa által igénybe vett adatfeldolgozók felé irányuló adatáramlásra, valamint a kollégium és más adatkezelőkkel való személyes adatokat érintő kommunikációra.

1.4. Jelen Szabályzat hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány és az általa fenntartott NEKA Kollégium közös adatkezeléseire.

1.5. Jelen Szabályzat hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány. székhelyén folyó valamennyi adatkezelésre, adattovábbításra, információátadásra, az ezen adatkezelés, információátadás tárgyát képező adat, jelen Szabályzatban meghatározottak szerinti, üzleti titokkénti kezelésével és védelmével kapcsolatos tevékenységekre.

1.6. A Szabályzat személyi hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány valamennyi szervezeti egységére, minden alkalmazottjára, valamint a vele szerződéses vagy egyéb kapcsolatban álló, személyes adatkezelést végző személyekre.

1.7. A Szabályzat tárgyi hatálya kiterjed a Magyar Kézilabda Utánpótlásért Alapítvány szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

2. JOGSZABÁLYI HIVATKOZÁS, KAPCSOLAT AZ ADATKEZELŐ BELSŐ SZABÁLYZATAIVAL

2.1. Jelen Adatvédelmi és Adatbiztonsági Szabályzat jogszabályi alapját a következő törvények jelentik:

- Magyarország Alaptörvénye;
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR);
- 2004. évi I. törvény – a sportról (Sporttörvény);
- 2011. évi CXC. törvény – a nemzeti köznevelésről (Köznev. tv.);
- 2012. évi I. törvény – a munka törvénykönyvéről (Mt.);
- 2013. évi V. törvény – a Polgári Törvénykönyvről (Ptk.).

2.2. Jelen Adatvédelmi és Adatbiztonsági Szabályzat az Adatkezelő külön kihirdetett további belső szabályzatához kapcsolódik, azokkal együttesen értelmezendő.

2.3. Jelen Adatvédelmi és Adatbiztonsági Szabályzat az Adatkezelő és a NEKA Kollégium közötti alábbi szerződéshez kapcsolódik, azzal együttesen értelmezendő.

- Együtt működési megállapodás a NEKA és a NEKA Kollégium által a kollégiumi diákok tekintetében megvalósított közös adatkezelésről.

3. ÉRTELMEZŐ RENDELKEZÉSEK

3.1. *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 azonosítható;

3.2. *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;

3.3. *az adatkezelés korlátozása:* a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

3.4. *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;

3.5. *álnevesítés:* a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

3.6. *nyilvántartási rendszer:* a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

3.7. *adatkezelő:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

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

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

3.10. *harmadik fél:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, 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 felhatalmazást kaptak;

3.11. *az érintett hozzájárulása:* az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

3.12. *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;

3.13. *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 említett természetes személyből vett biológiai minta elemzéséből ered;

3.14. *biometrikus adat:* egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

3.15. *egészségügyi adat:* egy természetes személy testi vagy pszichikai 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. AZ ADATKEZELŐK ADATAI

4.1. Az Adatkezelő adatai:

Név: Magyar Kézilabda Utánpótlásért Alapítvány

Székhely: 8630 Balatonboglár, Kodály Zoltán u. 12-13.

Alapítvány nyilvántartási szám: 01-01-0007974

Eljáró bíróság megnevezése: Fővárosi Törvényszék

Adószám: 18171075-2-14

Adatvédelmi tisztviselő: XX

Telefonszám: 06.85.888.852

E-mail: info@neka.hu

4.2. A kollégiumi adatkezelések tekintetében további Adatkezelő adatai:

Név: NEKA Kollégium

Székhely: 8630 Balatonboglár, Kodály Zoltán u. 12-13.

OM azonosító: 203219

Adószám: 15835406-2-14

Adatvédelmi tisztviselő: XX

Telefonszám: 06.85.888.856

E-mail: kollegium@neka.hu

II. ADATVÉDELEM

5. ADATKEZELŐRE ÉS ADATKEZELÉSRE VONATKOZÓ SZABÁLYOK, ALAPELVEK

5.1. Jogszerűség, tisztességes eljárás és átláthatóság

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

5.2. Célhoz kötöttség

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. A közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés az adatkezelés eredti céljával összeegyeztethetőnek tekintendő.

5.3. Adattakarékosság

A kezelt személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsak kell lenniük, és a szükségesre kell korlátozódniuk.

5.4. Pontosság

A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

5.5. Korlátozott tárolhatóság

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok 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 kerül majd sor.

5.6. Integritás és bizalmas jelleg

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

5.7. Elszámoltathatóság

Az Adatkezelő felelős az adatkezelés minden elvének való megfelelésért. Adatkezelő képes a megfelelés előírások szerinti igazolására. Az adatvédelmi szabályok betartásáért az Adatkezelő a felelős. Az Adatkezelő szervezet dolgozója az adatvédelmi és adatbiztonsági szabályok betartásáért személyes felelősséggel tartozik.

6. AZ ADATKEZELÉSEK JOGALAPJAI

6.1. Az Adatkezelő személyes adatokat csak a GDPR. 6. cikkében meghatározott felhatalmazás alapján kezel, nevezetesen:

a) ha az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez, vagy

b) ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges, vagy

c) ha az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, vagy

d) ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges, vagy

e) ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy

f) ha az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

6.2. Ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek igazolnia kell, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulást a más ügyektől egyértelműen megkülönböztethető módon kell beszerezni.

6.3. Az érintett az adatkezeléshez való hozzájárulását kizárólag részletes és egyértelmű tájékoztatás birtokában adhatja meg, melyről az Adatkezelő feladata gondoskodni.

6.4. Adatkezelő által kezelt egészségügyi adatok tekintetében az adatkezelés jogalapja a GDPR 9. cikk (2) bekezdésének a) pontja, azaz az érintett, illetve 16. életév betöltése előtt törvényes képviselőjének kifejezett hozzájárulása.

6.5. A GDPR 13. cikk (2) bekezdésének e) pontja szerint az adat felvételekor tájékoztatást kell adni arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul. Adatkezelő a fenti tájékoztatást Adatkezelési tájékoztatójának a munkavállalók szokásos tájékoztatására szolgáló felületeken, a központi fájlszerveren, létesítményeiben, honlapján és rendezvényein történő nyilvánosságra hozatalával, valamint egyes esetekben nyomtatott változatban történő átadásával valósítja meg.

Kötelező adatkezelés esetén a tájékoztatás megtörténhet az adatkezelésre vonatkozó információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

7. A GDPR 9. CIKK SZERINTI SZEMÉLYES ADATOK KÜLÖNLEGES KATEGÓRIÁINAK KEZELÉSE

7.1. Adatkezelő sportszervezetként a sporttevékenységgel összefüggésben egészségügyi adatokat kezel sportolói egészségének és a sport tisztaságának védelme, a tiltott teljesítményfokozás visszaszorítása érdekében. Az egészségügyi adatok tekintetében adatkezelésének jogalapja a GDPR 9. cikk (2) bekezdésének a) pontja, azaz az érintett, illetve 16. életév betöltése előtt törvényes képviselőjének kifejezett hozzájárulása.

7.2. Adatkezelő a GDPR 9. cikke szerinti egészségügyi adatokat az alábbi adatkezelési során kezel:

a) Adatkezelő a sport tisztaságának védelme, a tiltott teljesítményfokozás visszaszorítása érdekében kezel egészségügyi adatokat. E körbe tartoznak a gyermekorvosi, sportorvosi, illetve Adatkezelő egyéb szakorvosi szerződött partnerei által megvalósított adatkezelések.

b) Sportegészségügyi informatikai rendszerek, melyeket Adatkezelő a sportolók egészségének védelme, teljesítményének, terhelhetőségének folyamatos mérése, elemzése és azok alapján személyre szabott edzésterv, fejlesztési program kialakítása céljából alkalmaz az alábbiak:

- AlterG,
- Cosmed,
- FDM-T,
- Humac,
- HUR,
- HUR iBalance,
- HUR Labs,
- OptoJump,
- Vast.Rehab,
- Witty.

Adatkezelő csak olyan sportegészségügyi informatikai rendszereket alkalmazhat, mely az elérni kívánt célt is figyelembe véve indokolt, arányos és szükséges adatkezelést valósít meg figyelembe véve a kezelt adatok körét és az adatkezelés időtartamát is:

i. indokolt az adatkezelés, ha az általa elérni kívánt cél, előny az Adatkezelő vagy az érintett részére ténylegesen elérhető, az adatkezelés eredményeképpen realizálódik (a sportegészségügyi informatikai rendszerben kezelt adatok, az azokból levont következtetések, készített elemzések, az azok alapján tett javaslatok az Adatkezelő, vagy az érintett hasznára válnak);

ii. arányos az adatkezelés, ha az elérni kívánt adatkezelési cél a kezelt személyes adatok bármelyikének hiányában nem érhető el, és az nem jelent súlyosabb beavatkozást az érintettek privát szférájába, mint az Adatkezelő által elérhető (anyagi, erkölcsi) előny (ha a sportegészségügyi informatikai rendszer nem kezel a cél eléréséhez szükséges adatnál többet és az adatok felhasználása kizárólag az adatkezelési cél elérésére korlátozódik);

iii. szükséges az adatkezelés, ha az elérni kívánt adatkezelési cél más módon, a személyes adatok kezelése nélkül nem érhető el és a kezelt adatok valóban alkalmasak a cél elérésére (ha a sportegészségügyi informatikai rendszerben kezelt személyes adatok nélkül nem érhető el az adatkezelés célja, a méréseket, elemzéseket azok hiányában nem lehet elvégezni).

c) Sportági kiválasztó, mely adatkezelést Adatkezelő a tehetséges gyermekek kiválasztása érdekében alkalmazza.

d) Adatkezelő dietetikai tanácsadás érdekében kezel sportolói egészségügyi adatokat.

e) Adatkezelő a NEKA Kollégium további adatkezelővel közös adatkezelésként kezeli a kollégiumi diákok egészségügyi adatait.

8. SZERVEZETEN BELÜLI FELADATOK ÉS FELELŐSSÉGEK

8.1. Adatvédelmi tisztviselő

Az Adatkezelő erre jogosult vezetője a jelen Adatvédelmi és Adatbiztonsági Szabályzat érvényesítése érdekében a GDPR 37. cikke alapján kijelöli az adatvédelmi tisztviselőt.

Az adatvédelmi tisztviselő

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

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

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

d) együttműködik a Nemzeti Adatvédelmi és Információszabadság Hatósággal;

e) az adatkezeléssel összefüggő ügyekben kapcsolatot tart Nemzeti Adatvédelmi és Információszabadság Hatósággal, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

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

Az Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével

kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

Adatkezelő biztosítja számára azokat az forrásokat, amelyek a feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az Adatkezelő az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.

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

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

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

8.2. Az egyes szervezeti egységek vezetői

a) felelősek az irányításuk alá tartozó szervezeti egység adatkezeléseinek jogszabályoknak és jelen Szabályzatnak, vagy a kapcsolódó szabályzatoknak való megfelelőségéért;

b) felelősek azért, hogy az általuk vezetett szervezeti egység adatkezelései során a jelen Szabályzat III. részében foglalt adatbiztonsági előírások maradéktalanul teljesüljenek;

c) ellenőrzik az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseink betartását;

d) az adatvédelmi tisztviselő segítségét kérik, amennyiben a személyes adatok, üzleti titkok, közérdekű adatok kezelésével összefüggésben kérdésük merül fel;

e) együttműködnek az adatvédelmi tisztviselővel az adatvédelemmel kapcsolatos szabályok érvényesülése érdekében;

f) biztosítják, hogy beosztottaik az adatvédelmi tisztviselő által szervezett, illetve tartott adatvédelemmel kapcsolatos képzéseken részt vehessenek.

Amennyiben valamely szervezeti egység új, személyes adatokat is tartalmazó nyilvántartás vezetését határozza el, vagy a meglévőt kívánja módosítani, illetve törölni, úgy a szervezeti egység vezetője az adatvédelmi jogszabályoknak való megfelelőséget

vizsgáló konzultáció, és az adatvédelmi nyilvántartásba való bejelentés céljából értesíti az adatvédelmi tisztviselőt.

8.3. A Sporttudományos és Szakmai Főigazgató, Sportigazgató felelős a sportegészségügyi informatikai rendszerekkel megvalósított adatkezelések jogszerűségéért. E körben:

a) felelős azért, hogy a sportegészségügyi informatikai rendszerekkel megvalósított adatkezelések Adatkezelő mindenkori adatkezelési tájékoztatójában és jelen szabályzatban foglaltaknak, valamint a hatályos jogszabályoknak megfelelően valósuljanak meg;

b) tájékozódik az alkalmazni kívánt sportegészségügyi informatikai rendszer jogi hátteréről, GDPR megfelelőségéről;

c) sportszakmai érvekkel támasztja alá az alkalmazni kívánt sportegészségügyi informatikai rendszer szükségességét;

d) biztosítja, hogy a sportegészségügyi informatikai rendszerekben kizárólag az elérni kívánt adatkezelési célhoz feltétlenül szükséges személyes adatokat, az adatkezelés céljának megfelelő ideig kezelje Adatkezelő;

e) ellenőrzi, hogy csak olyan sportolók adatai kerüljenek a sportegészségügyi informatikai rendszerekben kezelésre, akik a GDPR 9. cikk (2) bekezdése szerinti hozzájárulásukat megadták;

f) biztosítja, hogy a sportegészségügyi informatikai rendszerhez Adatkezelő kizárólag azon jogosultsággal rendelkező munkavállalói férjenek hozzá, akiknek ez munkaviszonyból származó kötelezettségük teljesítéséhez szükséges;

g) gondoskodik az adatkezelési tájékoztatók sportegészségügyi informatikai rendszereket érintő részeinek pontosságáról, naprakészségéről;

h) gondoskodik arról, hogy a már nem alkalmazott rendszerekből a sportolói és munkavállalói személyes adatok törlésre kerüljenek.

8.4. A Kollégium igazgató felelős az Adatkezelő és a NEKA Kollégium közös adatkezelésében megvalósuló kollégiumi adatkezelések jogszerűségéért. E körben:

a) felelős azért, hogy a NEKA Kollégium adatkezelései Adatkezelő mindenkori adatkezelési tájékoztatójában és jelen szabályzatban foglaltaknak, valamint a hatályos jogszabályoknak megfelelően valósuljanak meg;

b) gondoskodik a NEKA Kollégiumba beiratkozó sportolók megfelelő adatvédelmi tájékoztatásáról;

c) gondoskodik az adatkezelési tájékoztatók NEKA Kollégiumi adatkezeléseket érintő részeinek pontosságáról, naprakészségéről;

d) biztosítja, hogy a NEKA Kollégium adatkezelési során kizárólag az elérni kívánt adatkezelési célhoz feltétlenül szükséges személyes adatokat, az adatkezelés céljának megfelelő ideig kezeljék az Adatkezelők;

e) biztosítja, hogy a NEKA Kollégium adatkezelései során kezelt személyes adatokhoz Adatkezelők kizárólag azon jogosultsággal rendelkező munkavállalói férjenek hozzá, akiknek ez munkaviszonyból származó kötelezettségük teljesítéséhez szükséges;

f) a NEKA Kollégium adatkezeléseit érintő, hozzá érkező észrevételeket, panaszokat továbbítja Adatkezelő kijelölt munkavállalója felé.

8.5. A Létesítményigazgató a felelősségi körébe tartozó adatkezelések (így különösen a Sportcsarnok és lakófalu elektronikus megfigyelő- és rögzítőrendszere, beléptetőrendszer, vagyonvédelmi nyilvántartások, létesítményüzemeltetés során igénybe vett külsős vállalkozásokat érintő adatkezelések) jogszerűségért felel.

a) felelős azért, hogy a felelősségi körébe tartozó adatkezelések Adatkezelő mindenkori adatkezelési tájékoztatójában és jelen szabályzatban foglaltaknak, valamint a hatályos jogszabályoknak megfelelően valósuljanak meg;

b) ellenőrzi az elektronikus megfigyelő- és rögzítőrendszer kamerái által megfigyelt területet, a kamerák látószögét;

c) gondoskodik a létesítményekben az elektronikus megfigyelő- és rögzítőrendszert érintő tájékoztatások, táblák kihelyezéséről, és folyamatosan ellenőrzi azok állapotát, épségét, olvashatóságát és naprakészségét;

d) gondoskodik Adatkezelő létesítményüzemeltetésében részt vevő, Adatkezelő területére belépő külsős vállalkozások és munkavállalóik megfelelő, előzetes adatvédelmi tájékoztatásáról;

e) gondoskodik az adatkezelési tájékoztatók felelősségi körébe tartozó adatkezeléseket érintő részeinek pontosságáról, naprakészségéről;

f) biztosítja, hogy a vagyonvédelmi célú és létesítményüzemeltetés során kezelt személyes adatokhoz Adatkezelő kizárólag azon jogosultsággal rendelkező munkavállalói férjenek hozzá, akiknek ez munkaviszonyból származó kötelezettségük teljesítéséhez szükséges.

8.6. A Lurkó csoportvezető felelős a Lurkó program során megvalósított adatkezelések jogszerűségéért. E körben:

a) felelős azért, hogy a Lurkó program adatkezelései Adatkezelő mindenkori adatkezelési tájékoztatójában és jelen szabályzatban foglaltaknak, valamint a hatályos jogszabályoknak megfelelően valósuljanak meg;

b) biztosítja, hogy a Lurkó program adatkezelései során kizárólag az elérni kívánt adatkezelési célhoz feltétlenül szükséges személyes adatokat, az adatkezelés céljának megfelelő ideig kezelje Adatkezelő;

c) gondoskodik a Lurkó programban részt vevő diákok és pedagógusok megfelelő, előzetes adatvédelmi tájékoztatásáról;

d) gondoskodik az adatkezelési tájékoztató Lurkó programmal megvalósított adatkezeléseket érintő részeinek pontosságáról, naprakészségéről;

e) biztosítja, hogy a Lurkó program során kezelt személyes adatokhoz Adatkezelő kizárólag azon jogosultsággal rendelkező munkavállalói férjenek hozzá, akiknek ez munkaviszonyból származó kötelezettségük teljesítéséhez szükséges.

8.7. A Kommunikációs igazgató felelős Adatkezelő honlapján, közösségi oldalain, marketing tevékenysége során megvalósított adatkezelések jogszerűségéért. E körben:

a) felelős azért, hogy a felelősségi körébe tartozó adatkezelések Adatkezelő mindenkori adatkezelési tájékoztatójában és jelen szabályzatban foglaltaknak, valamint a hatályos jogszabályoknak megfelelően valósuljanak meg;

b) biztosítja, hogy a felelősségi körébe tartozó adatkezelések során kizárólag az elérni kívánt adatkezelési célhoz feltétlenül szükséges személyes adatokat, az adatkezelés céljának megfelelő ideig kezelje Adatkezelő;

c) gondoskodik arról, hogy Adatkezelő honlapján, közösségi oldalain Adatkezelő hatályos adatkezelési tájékoztatója kerüljön elhelyezésre;

d) felelős azért, hogy Adatkezelő csak olyan érintetteket keressen meg direkt marketing üzenetekkel, akik ehhez a Grt. 6. § szerinti hozzájárulását Adatkezelő részére megadta;

e) felelős Adatkezelő direkt marketing célú adatbázisában kezelt személyes adatok jogszerű gyűjtéséért, az adatbázis naprakészségért, pontosságáért, valamint a direkt marketing üzenetek jogszerű kiküldéséért;

f) gondoskodik Adatkezelő Kommunikációs igazgató felelősségi körébe tartozó rendezvényein a résztvevők megfelelő, előzetes adatvédelmi tájékoztatásáról a rendezvényeken készülő fényképek, filmfelvételek tekintetében;

g) gondoskodik az adatkezelési tájékoztató felelősségi körébe tartozó adatkezeléseket érintő részeinek pontosságáról, naprakészségéről;

h) biztosítja, hogy a felelősségébe tartozó adatkezelések során kezelt személyes adatokhoz Adatkezelő kizárólag azon jogosultsággal rendelkező munkavállalói férjenek hozzá, akiknek ez munkaviszonyból származó kötelezettségük teljesítéséhez szükséges;

i) gondoskodik Adatkezelő fényképeinek, filmfelvételeinek jelen szabályzat adatbiztonsági előírásainak megfelelő tárolásáról.

8.8. Az adatkezelést végző személy

A Magyar Kézilabda Utánpótlásért Alapítvány szervezetén belül adatkezelést végző személy a tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért.

Az adatkezelést végző személy tevékenysége során:

a) kezeli és megőrzi a feladata ellátása során birtokába került adatokat;

b) ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására;

c) gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá;

d) betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;

e) haladéktalanul jelzi vezetője felé, amennyiben az adatvédelmi ügyben a felettes vagy az adatvédelmi tisztviselő segítségére szorul;

f) részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

Aki üzleti titok, illetve személyes adat birtokába jut, köteles a titkot időbeli korlátozás nélkül megtartani.

Az üzleti titkot, személyes adatot nem lehet visszaélésszerűen felhasználni, így különösen tilos a Magyar Kézilabda Utánpótlásért Alapítvány feladatkörén kívül a munkavállaló saját vagy más személyes, illetve üzleti céljainak, közvetlen vagy közvetett előnyök elérésére, valamint az Adatkezelő vagy ügyfeleinek megkárosítására használni.

9. ADATVÉDELMI NYILVÁNTARTÁS

9.1. Adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről írásbeli – ideértve az elektronikus formátumot is – nyilvántartást vezet a következő információkkal:

a) az Adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;

b) az adatkezelés céljai;

c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

e) 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 megfelelő garanciák leírása;

f) a különböző adatkategóriák törlésére előirányzott határidők;

g) az adatkezelés biztonságát szolgáló technikai és szervezési intézkedések általános leírása.

9.2. Az adatkezelő megkeresés alapján a Nemzeti Adatvédelmi és Információszabadság Hatóság részére rendelkezésére bocsátja a nyilvántartást.

9.3. Az adatvédelmi nyilvántartás a Magyar Kézilabda Utánpótlásért Alapítvány egyes személyes adatkezeléseinek központi nyilvántartása. A nyilvántartásban haladéktalanul rögzíteni kell az egyes szervezeti egységek által bevezetett meglévő és új adatkezeléseket,

és a korábbi adatkezelések változásait, míg a megszűnt adatkezeléseket törölni kell a nyilvántartásból

A belső adatvédelmi nyilvántartás részét képezik az egyes adatkezeléseket részletesen ismertető Adatkezelési Tájékoztatók is.

10. AZ ADATOK TÁROLÁSA

10.1. A kezelt adatokat úgy kell tárolni, hogy azokhoz illetéktelenek – ideértve azon munkavállalókat is, akik nem jogosultak ezen adatok megismerésére, kezelésére – ne férhessenek hozzá. Papír alapú adathordozók esetében a fizikai tárolás, irattárazás rendjének kialakításával, zárható szekrények és a munkavégzés idején zárva tartott, külön beléptetési jogosultsággal elérhető területen található irodákkal, elektronikus formában kezelt adatok esetén a központi fájszerveren jogosultságkezelő rendszer alkalmazásával.

10.2. Az adatok informatikai módszerrel történő tárolási módját úgy kell megválasztani, hogy azok törlése – az esetleg eltérő törlési határidőre is tekintettel – az adattörlési határidő lejártakor, illetve ha az egyéb okból szükséges, elvégezhető legyen. A törlésnek visszaállíthatatlannak és ellenőrizhetőnek kell lennie.

10.3. A papír alapú adathordozókat iratmegsemmisítő segítségével, vagy külső, iratmegsemmisítésre szakosodott vállalkozó igénybevételével kell a személyes adatoktól megfosztani. Elektronikus adathordozók (merevlemezek, optikai adathordozók, mágneses adathordozók, nyomtatók, multifunkciós gépek háttértárai, flash (NAND) adathordozók, SIM kártyák, mobileszközök, telefonok, PDA-k, Tablet-ek, laptopok, stb.) esetében az elektronikus adathordozók selejtezésére vonatkozó szabályok szerint kell gondoskodni a fizikai megsemmisítésről, illetve szükség szerint előzetesen az adatoknak a biztonságos és visszaállíthatatlan törléséről. Az adathordozók megsemmisítését ellenőrizni, dokumentálni kell, valamint a dokumentációt visszakereshető módon kell megőrizni, illetve selejtezni.

11. AZ ADATOK FELHASZNÁLÁSA

11.1. A Magyar Kézilabda Utánpótlásért Alapítvány által kezelt adatok kizárólag a GDPR, a Sporttörvény, a Köznev. tv. és más jogszabályok rendelkezéseinek megfelelően, illetve az aktuális Adatkezelési Tájékoztatókban meghatározott célokra használhatók fel.

11.2. Számítástechnikai, távközlési eszközök és programok helyességének ellenőrzésére, felhasználók betanítására, illetve oktatási célra valós személyi adatokat felhasználni nem lehet. Informatikai (funkcionális, integrációs) tesztkörnyezetekben gondoskodni kell arról, hogy az éles rendszerben kezelt személyes adatok és a tesztkörnyezetben használt és anonimizált adatok közötti kapcsolat technikai úton ne legyen visszaállítható.

11.3. A Magyar Kézilabda Utánpótlásért Alapítvány által kezelt személyes adatok nyilvánosságra hozatala tilos, kivéve, ha azt törvény rendeli el.

11.4. Az előző pontban foglalt tilalom nem érinti az Adatkezelőről szóló statisztikai adatokat, melyek korlátozás nélkül nyilvánosságra hozhatók.

12. AZ ADATOK FELDOLGOZÁSA

12.1. A személyes adatokon technikai műveletet az Adatkezelő alvállalkozója adatfeldolgozóként az érintett hozzájárulása nélkül is végrehajthat, amennyiben tevékenysége során önálló érdemi döntést nem hoz.

12.2. A Magyar Kézilabda Utánpótlásért Alapítvány harmadik személy kezelésében lévő személyes adatokon – amennyiben e tevékenysége során érdemi döntési jogkörrel nem rendelkezik – adatfeldolgozóként az érintett hozzájárulása nélkül is végezhet technikai műveleteket.

12.3. A GDPR 28. cikk (1) bekezdése szerint az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

12.4. Az adatfeldolgozók átvilágítása során vizsgálandó szempontok

a) Milyen szerződéses felelősségvállalást tud tenni?

b) Milyen garanciát vállalnak a szerződés teljesítéséért, az esetleges károkért való helytállásért? (pl. kötbér, felelősségbiztosítás, tulajdonosi kezességvállalás)

c) Milyen szakértőkkel rendelkeznek? (a részt vevők végzettségére, tapasztalatára, a részt vevők és a cég referenciájára vonatkozó információk)

d) Az adatfeldolgozásban részt vevők, munkavállalók milyen titoktartási kötelezettséget vállaltak? (munkaszerződés vagy külön titoktartási minta)

e) Megbízhatóságra vonatkozó információk begyűjtése (pl. korábbi tapasztalatok, vagy referenciák tapasztalatai, reputáció)

f) Milyen pénzügyi erőforrások állnak rendelkezésre? (a szervezet gazdasági elemzése)

g) Milyen fizikai erőforrással, adatbiztonsági eszközökkel és intézkedésekkel dolgoznak? (IT, adatbiztonsági átvilágítás)

h) Hogyan biztosítja az egyéb rendszereitől, adatbázisaitól való elkülönítést?

i) Milyen naplózási vagy egyéb eljárásokkal válik az adatkezelő felé elszámoltathatóvá a gyakorlata?

j) Tartozik-e valamilyen magatartási kódexhez vagy tanúsítási mechanizmushoz?

k) Milyen módon és garanciákkal tudja a szerződés megszűnése esetén vállalni az adatok visszaadását és törlését?

l) Mutassa be biztonsági incidens kezelési gyakorlatát!

12.5. Az adatfeldolgozó átvilágítását követő eljárás:

a) Az adatfeldolgozó alvállalkozójának átvilágítása a fenti szempontok alapján általában nem lehetséges, de az al-adatfeldolgozók neve, feladata, feladatvégzésük intenzitása, és az értük való helytállás rendezettsége fontos.

b) Külföldi (EU-n kívüli) adatfeldolgozás kizárása/kezelése.

c) Adatfeldolgozói szerződés megkötése (Amennyiben szükséges, SLA-k meghatározása: mérendő indikátorok és elvárt értékek, mérések módja és gyakorisága, jogkövetkezmények).

d) Az adatfeldolgozónál adatvédelmi tisztviselő vagy felelős személy kijelölése.

e) Az adatfeldolgozó köteles vezetni a GDPR 30. cikk (2) bek. szerinti adatfeldolgozói nyilvántartást, és az adatkezelő részére ehhez hozzáférést biztosítani.

f) Az adatfeldolgozókkal való kommunikációs csatorna (incidensek, al-adatfeldolgozó változás, utasítások adása, teljesítés igazolása és dokumentálása) biztosítása, ellenőrzése, ideértve a szoros határidőket is.

g) Transzparencia biztosítása, az adatkezelési tájékoztató naprakészen tartása.

h) Mindezek folyamatos ellenőrzése.

12.6. Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a GDPR előírásait vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

12.7. Az adatfeldolgozói szerződést vagy más jogi aktust írásba kell foglalni, ideértve az elektronikus formátumot is. A szerződésnek a következő elemeket kell tartalmaznia:

a) az adatkezelő és az adatfeldolgozó megnevezését;

b) az adatfeldolgozási tevékenység megnevezését;

c) az adatfeldolgozási tevékenység tárgyát;

d) az adatfeldolgozási tevékenység időtartamát, jellegét és célját;

e) a személyes adatok típusát;

f) az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait;

g) automatizált adatfeldolgozás esetén az alkalmazott módszert és lényegét;

h) az adatkezelő szavatolását az adatbázis, az átadott személyes adatok jogszerű kezeléséért;

i) az adatfeldolgozó nyilatkozatát, hogy kizárólag az adatkezelő utasítása alapján végzi az adatok feldolgozását;

j) az adatfeldolgozónak a saját, és a szerződésben foglaltaktól eltérő célú adatfelhasználásának tilalmát;

k) azt az előírást, hogy az adatfeldolgozó tevékenysége ellátása során más adatfeldolgozót az adatkezelő rendelkezése szerint vehet igénybe;

l) az adatfeldolgozó kötelezettségvállalását az adatbiztonsági szabályok megtartására;

m) az adatok sorsára vonatkozó rendelkezést a szerződés megszűnésének eseteire;

n) az adatvédelmi incidenssel kapcsolatos rendelkezéseket;

o) mindezekért való anyagi felelősségvállalást.

12.8. Az adatfeldolgozó részére csak olyan személyes adatok adhatók át, amelyek szerepelnek

a) az adatfeldolgozói szerződésben,

b) vagy a konkrét adatkezelésre vonatkozó tájékoztatásban.

12.9. Az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a szükséges adatbiztonsági intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó előírásokat;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az Adatkezelőt a kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatfeldolgozói szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha jogszabály a személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a fentiekben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az Adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

12.10. Az adatfeldolgozó az Adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

12.11. Ha az adatfeldolgozó további adatfeldolgozó szolgáltatásait is igénybe veszi, a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az Adatkezelő és az adatfeldolgozó között létrejött, a szerződésben szerepelnek:

a) A további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek.

b) Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az Adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

12.12. Az adatfeldolgozói feladat teljesítését követően, illetve a szerződés megszűnésekor az adatfeldolgozó a birtokában lévő személyes adatokat vissza kell, hogy szolgáltassa az Adatkezelőnek. Az átadott adatok adatfeldolgozó számítástechnikai rendszerében található másolatait pedig visszavonhatatlan módon töröltetni kell, melynek megtörténtéről az adatfeldolgozónak nyilatkoznia kell.

13. ADATTOVÁBBÍTÁS HARMADIK ORSZÁG FELÉ, HATÓSÁGI ADATSZOLGÁLTATÁS

13.1. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikke szerinti – a harmadik országba irányuló adattovábbításokra vonatkozó – megfelelő garanciákról.

13.2. Megfelelő garanciát jelent:

a) közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;

b) a GDPR 47. cikke szerinti kötelező erejű vállalati szabályok;

c) a Bizottság által a GDPR 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötések;

d) a Nemzeti Adatvédelmi és Információszabadság Hatóság által elfogadott és a Bizottság által a GDPR 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően jóváhagyott általános adatvédelmi kikötések;

e) a GDPR 40. cikke szerinti, jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat; vagy

f) a rendelet 42. cikke szerinti, jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

13.3. A harmadik országba történő adattovábbítás megfelelő garanciák esetén is csak azzal a feltétellel történhet, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

13.4. A Köznev. tv. 41. § (5) bekezdése alapján a köznevelési feladatokat ellátó intézmény által a Köznev. tv. 41. § (2)-(3) bekezdése szerint kezelt adatok továbbíthatók a fenntartónak, a kifizetőhelynek, a bíróságnak, rendőrségnek, ügyészségnek, a köznevelléssel összefüggő

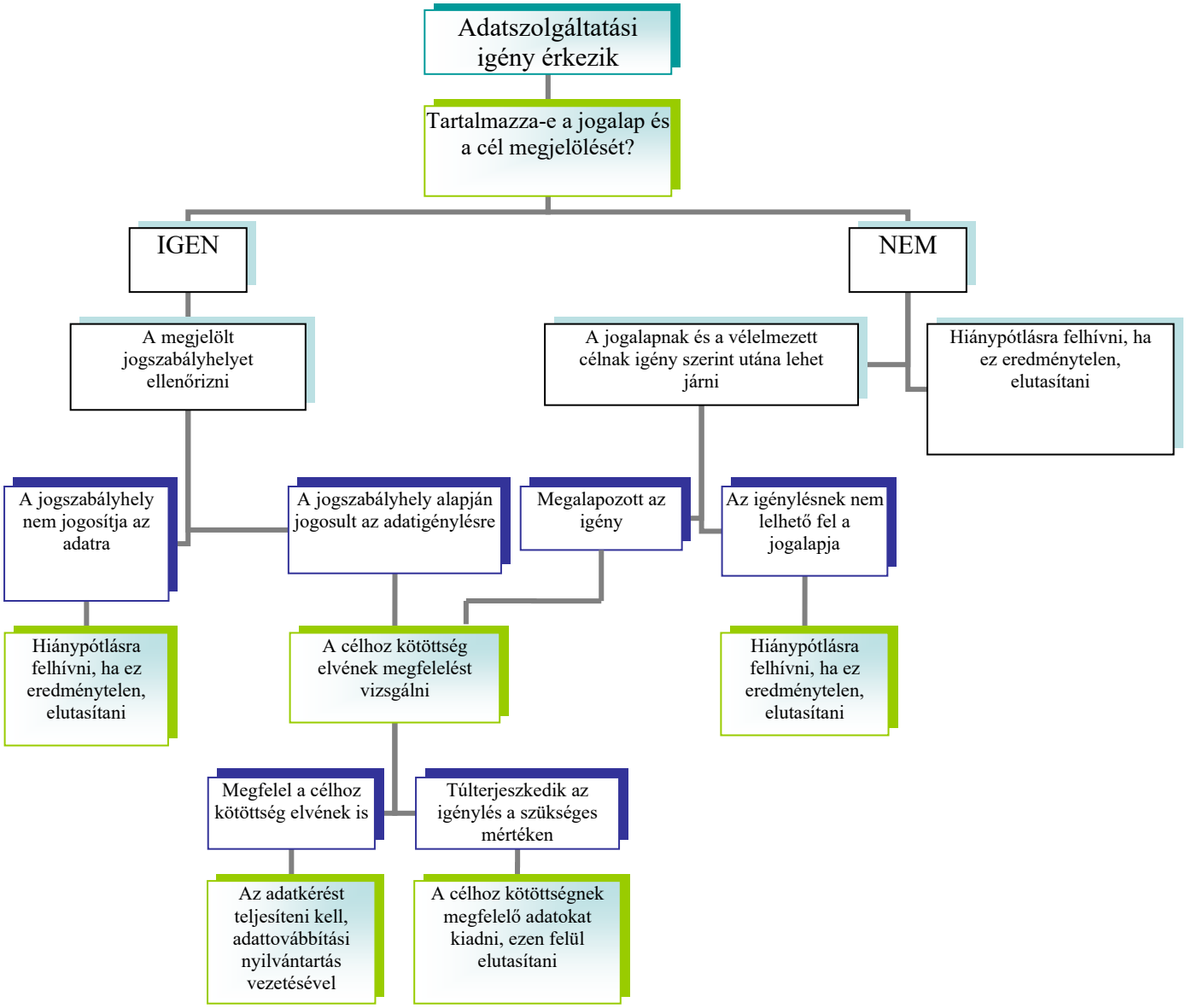
igazgatási tevékenységet végző közigazgatási szervnek, a munkavégzésre vonatkozó rendelkezések ellenőrzésére jogosultaknak, a nemzetbiztonsági szolgálatnak.

13.5. Adatkezelő az államháztartás felé a működési költségeivel kapcsolatosan kezelt személyes adatokat elszámolási célból továbbítja a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogos érdeke alapján, mely a támogatások igénybevételéhez kapcsolódó elszámolási kötelezettségének teljesítéséhez fűződik, tekintettel a 107/2011. (VI. 30.) Korm. rendelet 2. Mellékletére. Adatkezelő jogos érdek jogalap alkalmazását alátámasztó érdekmérlegelési tesztet elvégezte.

13.6. Adatkezelő az általa megbízott biztosítási alkusz felé személyes adatot az érintettet ért káresemény bekövetkezését követően továbbít a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogos érdeke alapján, mely a biztosító Adatkezelő helyetti, károsultakkal szembeni helytállásához fűződik, Adatkezelő jogos érdek jogalap alkalmazását alátámasztó érdekmérlegelési tesztet elvégezte.

13.7. Nem lehet üzleti titokra hivatkozással visszatartani az információt a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, külön törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettség esetén.

13.8. Amennyiben valamely adatkezelőtől adatszolgáltatási kérelem érkezik, az adatszolgáltatás teljesítésére jogosult személy a következő eljárást köteles alkalmazni:



14. A SZEMÉLYES ADATOK TÖRLÉSE, HELYESBÍTÉSE, ADATKEZELÉS KORLÁTOZÁSA

14.1. Az adatokat törölni – manuális nyilvántartás esetén megsemmisíteni – kell, ha

a) az adatkezelésre a tájékoztatóban, illetve jogszabályban előírt határidő eltelt – a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az adatkezelés jogszerűtlensége megállapítást nyert;

c) az érintett az adatkezelés alapját képező hozzájárulását visszavonta és az adatkezelésnek nincs más jogalapja, kivéve, ha törvény az adatok további kezelését lehetővé teszi;

d) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett tiltakozik a közvetlen üzletszerzés érdekében történő adatkezelés ellen;

e) az adat hiányos vagy téves, és ez az állapot jogszerűen nem orvosolható – feltéve hogy törvény a törlést nem zárja ki;

f) az adatkezelés célja megszűnt;

g) az adatvédelmi hatóság, vagy bíróság jogerős határozattal elrendelte.

h) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

i) a személyes adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatásokkal kapcsolatosan került sor.

14.2. Az adatok törlése nem kezdeményezhető, ha az adatkezelés szükséges: a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából; a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából; a népegészség-ügy területét érintő, vagy archiválási, tudományos és történelmi kutatási célból vagy statisztikai célból, közérdek alapján; vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

14.3. Az érintett kérheti az Adatkezelő által kezelt, rá vonatkozó pontatlan személyes adatok helyesbítését, és a hiányos adatok kiegészítését.

14.4. Az érintett bejelentése vagy az Adatkezelő által észlelt hibás adat esetén – a rendelkezésre álló dokumentumok vagy közhiteles nyilvántartás alapján, illetve az érintettel történt egyeztetést követően – az Adatkezelő a hibás adatot helyesbíti.

14.5. Ha a hibás adat nem helyesbíthető, akkor törölni kell. Amennyiben a törlés vagy a helyesbítés az adatok tárolási módja miatt nem lehetséges, akkor az adatot megfelelő helyesbítő vagy figyelemfelhívó feljegyzés hozzáfűzésével véglegesen zárolni kell.

14.6. Az Adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, a személyes adatok pontosságának ellenőrzését;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

14.7. Ha az adatkezelés korlátozás alá esik, a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

14.8. Adatkezelő. az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

15. AZ ÉRINTETT TÁJÉKOZTATÁSHOZ, HOZZÁFÉRÉSHEZ VALÓ JOGA

15.1. Adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintettek részére a személyes adatok kezelésére vonatkozó, a GDPR 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa.

15.2. A tájékozódáshoz való jog írásban a Bevezetésben, illetve a 4. pontban megjelölt elérhetőségeken keresztül gyakorolható.

15.3. Az érintett részére kérésére – személyazonosságának hitelt érdemlő igazolása és beazonosítását követően – szóban is adható tájékoztatás.

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

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli

címzetteket, illetve a nemzetközi szervezeteket; a személyes adatok tárolásának tervezett időtartama;

d) a helyesbítés, törlés vagy adatkezelés korlátozásának és a tiltakozás joga;

e) a felügyeleti hatósághoz címzett panasz benyújtásának joga;

f) az adatforrásokra vonatkozó információ;

g) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár;

h) személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozó megfelelő garanciákról.

15.5. Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Az érintett kérelmére az információkat Adatkezelő elektronikus formában szolgáltatja.

15.6. A tájékoztatást az Adatkezelő a következő esetekben tagadhatja meg:

a) az érintett nem a saját adataira vonatkozóan kér tájékoztatást;

b) a tájékoztatást kérő személy nem tudja hitelt érdemlő módon igazolni, hogy ő lenne az adatkezeléssel érintett személy;

c) amennyiben törvény a tájékoztatást kizárja;

d) ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa rendelkezése alapján az Adatkezelő az adatokat egy másik adatkezelőtől akként veszi át, hogy az adatokat átadó adatkezelő jelezte az érintett tájékoztatási jogának korlátozását.

A felvilágosítás megtagadása esetén tájékoztatni kell az érintettet a bírósághoz és az adatvédelmi hatósághoz fordulás jogáról. Ezen felül a folyó évet követő január 31-éig tájékoztatni kell a Nemzeti Adatvédelmi és Információszabadság Hatóságot az elutasított kérelmekről.

16. ADATHORDOZÁSHOZ, VISSZAVONÁSHOZ VALÓ JOG, AUTOMATIZÁLT DÖNTÉSHOZATAL

16.1. Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, és ezeket az adatokat egy másik adatkezelőnek továbbítsa.

16.2. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

16.3. Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

16.4. Nem alkalmazható a fenti jogosultság, ha az adatkezelés

a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;

b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy

c) az érintett kifejezett hozzájárulásán alapul.

17. TILTAKOZÁS A SZEMÉLYES ADATOK KEZELÉSE ELLEN

17.1. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés, vagy az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

17.2. Tiltakozás esetén az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha azt olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

17.3. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

17.4. A személyes adatok közvetlen üzletszerzés érdekében történő kezelése elleni tiltakozás esetén az adatokat e célból az Adatkezelő nem kezeli.

17.5. Tiltakozását szóban, írásban és elektronikus úton is kifejezheti.

18. ADATVÉDELMI HATÁSVIZSGÁLAT

18.1. Amikor valószínűsíthető, hogy az adatkezelési műveletek magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, az e kockázat forrását, jellegét, egyediségét és súlyosságát felmérő adatvédelmi hatásvizsgálat elvégzéséért az Adatkezelő felel. A hatásvizsgálat megállapításait figyelembe kell venni annak meghatározásakor,

hogy mely intézkedések a megfelelőek annak bizonyítására, hogy a személyes adatok kezelése megfelel a rendeletnek. A hatásvizsgálat az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve készül el. A hatásvizsgálat tartalmazza a kockázat mérséklését, a személyes adatok védelmét, valamint a rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat. A hatásvizsgálatot az adatkezelés megkezdése előtt kell elvégezni. Az adatvédelmi hatásvizsgálatot adatkezelésenként, adatkezelési műveletenként kell elvégezni, azzal, hogy olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

18.2. A hatásvizsgálat kiterjed az adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára, az érintett jogait és szabadságait érintő kockázatok vizsgálatára, és a kockázatok kezelését célzó intézkedések bemutatására, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciára, biztonsági intézkedésekre és mechanizmusokra.

18.3. A hatásvizsgálat elvégzése során az alábbi alapelveket kell szem előtt tartani:

a) az adatkezelésnek meghatározott, egyértelmű és törvényes célja kell, hogy legyen,

b) a kezelt adatok megfelelőek, relevánsak és csak az adatkezelés céljának eléréséhez szükséges körben kerülnek kezelésre,

c) az érintettek megkapták az egyértelmű és teljes körű tájékoztatást az adatkezelés körülményeiről,

d) a kezelt személyes adatok korlátozott ideig kerülnek megőrzésre,

e) az érintettek jogainak érvényesítése (felszólalási jog, hozzáférés, javítás és törlés stb).

18.4. A hatásvizsgálat lépései:

a) Az adatkezelés általános leírása (az adatkezelő, az feldolgozó és az adatkezelés céljának leírása, az adatkezelő és a feldolgozó azonosítása).

b) Az adatkezelés részletes leírása (az adatkezelés meghatározása leírása részletesen, az érintett személyes adatok, a címzettek, a megőrzési időszakok, az eljárások leírása a személyes adatok teljes ciklusa során (összegyűjtéstől a törlésig).

c) Jogi szempontú ellenőrzés

1. cél: meghatározott, egyértelmű és törvényes célból történik az adatkezelés,

2. adatminimalizálás: korlátozza a kezelt személyes adatok mennyiségét a feltétlenül szükségesre,

3. minőség: a kezelt személyes adatoknak pontosnak kell lenniük,

4. megőrzési időtartam: az adatkezelési cél eléréséhez szükséges időtartamig, ennek hiányában más jogi kötelezettség által előírt időszakban történjen az adatkezelés,

5. információ: az érintettek tájékoztatáshoz való jogának érvényesülése,

6. hozzájárulás: az adatalanyok hozzájárulásának megléte, vagy más jogalap alapján igazolja a személyes adatok kezelését,

7. kifogás joga: tiszteletben kell tartani az adatalanyok felszólalási jogát,

8. hozzáférési jog: az adatalany azon joga, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és az adatkezelést érintő információkhoz hozzáférést kapjon,

9. helyesbítés, törlés joga: az adatalanyok azon joga, hogy kérésére az adatkezelő javítsa, helyesbítse, és törölje az adatait,

10. adattovábbítás: a kötelezettségeknek való megfeleléssel történik-e a személyes adatok továbbítása az Európai Unió területén kívülre,

11. előzetes ellenőrzés meghatározása és teljesítése az adatkezelés előtt.

d) Kockázat-kezelés ellenőrzése

1. szervezeti kontrollok: szervezeti szintű kockázatkezelés, projekt menedzsment, incidens menedzsment, felügyelet stb,

2. logikai biztonsági ellenőrzések: anonimizálás, titkosítás, biztonsági mentések, adatparticionálás, logikai hozzáférés-vezérlés stb,

3. fizikai biztonsági ellenőrzések: fizikai hozzáférés-ellenőrzés, biztonsági hardver, nem humán kockázatok stb.

e) Veszélyforrás minden olyan esemény, mely a személyes adatokhoz való jogtalan hozzáférést, a személyes adatok nem kívánt változtatását és törlését idézi elő.

1. meg kell határozni a lehetséges hatásokat az adatalanyok tekintetében,
2. fenyegetések azonosítása,
3. a kockázati szint meghatározása.

18.5. A magas kockázatuk miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének meghatározása során a következő szempontokat kell mérlegelni:

a) értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is,

b) joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal, megjegyzendő, hogy az egyénekre nézve csekély vagy semmilyen hatással nem járó adatkezelés nem felel meg ennek a konkrét szempontnak,

c) módszeres megfigyelés, az érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése, azaz az elektronikus megfigyelőrendszer; a WP243. iránymutatás szerint módszeres a megfigyelés, ha

1. módszer szerint zajlik;
2. előre meghatározott, szervezett vagy tervszerű;
3. általános adatgyűjtési terv részeként megy végbe;
4. stratégia részeként történik.

d) különleges adatok vagy fokozottan személyes jellegű adatok kezelése,

e) nagy számban kezelt adatok, a 29-es munkacsoport WP248. számú iránymutatása szerint a nagy számban történő adatkezelés meghatározásakor az alábbiakat kell figyelembe venni:

1. az érintettek száma konkrét számadatként vagy a lakosság arányában;
2. a kezelt adatok mennyisége vagy adatfajták köre;
3. az adatkezelési tevékenység időtartama vagy állandó jellege;
4. az adatkezelési tevékenység földrajzi kiterjedése.

f) az adatkészletek egymással való megfeleltetése vagy összevonása, ideértve több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon,

g) kiszolgáltatott helyzetben lévő érintettekkel (gyermekek, munkavállalók, mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb., valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki) kapcsolatos adatok,

h) új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása,

i) amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek.

18.6. A munkacsoport álláspontja szerint bizonyos esetekben az adatkezelő tekintheti úgy, hogy a mindössze egy szempontnak megfelelő adatkezelés esetében is szükség van adatvédelmi hatásvizsgálatra.

18.7. Megjegyezzük, hogy a felügyeleti hatóságoknak össze kell állítaniuk, nyilvánosságra kell hozniuk, és az Európai Adatvédelmi Testületnek továbbítaniuk kell az olyan adatkezelési műveletek jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni (a 35. cikk (4) bekezdése).

18.8. A következő esetekben nincs szükség adatvédelmi hatásvizsgálatra:

a) ha az adatkezelés valószínűsíthetően nem jár „magas kockázattal […] a természetes személyek jogaira és szabadságaira nézve” (a 35. cikk (1) bekezdése);

b) ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat. Ilyen esetekben felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei (a 35. cikk (1) bekezdése);

c) ha az adatkezelési műveleteket felügyeleti hatóság meghatározott, azóta változatlan feltételek mellett 2018. május előtt ellenőrizte;

d) ha a 6. cikk (1) bekezdésének c) vagy e) pontja szerinti adatkezelési művelet jogalappal rendelkezik az uniós vagy tagállami jogban, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat (a 35. cikk (10) bekezdése), kivéve, ha a tagállam előírta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni;

e) ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) nem kötelező jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni (a 35. cikk (5) bekezdése). Ez a jegyzék olyan adatkezelési tevékenységeket tartalmazhat, amelyek megfelelnek a hatóság által – különösen iránymutatások, egyedi határozatok vagy engedélyek, megfelelési szabályok stb. útján – megállapított feltételeknek.

18.9. A fenti lépéseket felülvizsgálva kell az Adatkezelőnek meghatároznia a nem megfelelő eljárások, gyakorlatok javításának lehetőségeit. Ha a vizsgálatok eredménye szerint a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában az adatkezelés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és az adatkezelő véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell. Valószínűsíthetően ilyen magas kockázattal járnak a személyes adatok kezelésének bizonyos típusai és az adatkezelés bizonyos mértéke és gyakorisága, amelyek emellett kárt is okozhatnak, illetve hátrányosan érinthetik a természetes személy jogait és szabadságait.

18.10. A felügyeleti hatóság a konzultáció iránti megkeresésre meghatározott határidőn belül választ ad. Ha azonban a felügyeleti hatóság az említett határidőn belül nem reagál, nem érinti a felügyeleti hatóságnak az e rendeletben megállapított feladataival és hatásköreivel összhangban álló beavatkozási jogkörét, az adatkezelési műveletek megtiltására vonatkozó hatáskörét is beleértve. E konzultációs eljárás során a szóban forgó adatkezelés tekintetében végzett adatvédelmi hatásvizsgálat eredményét, és különösen a természetes személyek jogait és szabadságait veszélyeztető kockázat mérséklésére szolgáló intézkedések tervezetét be lehet nyújtani a felügyeleti hatóságnak [a GDPR preambulumának (94) bekezdése].

18.11. Adatkezelő az alábbi adatkezelései hatásvizsgálatát végezte el:

f) Sportegészségügyi informatikai rendszerek:

- AlterG,
- Cosmed,
- FDM-T,
- Humac,

- HUR,
- HUR iBalance,
- HUR Labs,
- OptoJump,
- Vast.Rehab,
- Witty;

g) Elektronikus megfigyelő- és rögzítőrendszerek:

- elektronikus megfigyelő- és rögzítőrendszer a lakófaluban
- elektronikus megfigyelő- és rögzítőrendszer a sportcsarnokban,
- elektronikus megfigyelő- és rögzítőrendszer a sportcsarnokban sportesemény idején;

h) Kollégiumi tanulók fejlesztési tervével megvalósított adatkezelés.

19. ADATVÉDELMI INCIDENS

19.1. Az adatvédelmi incidenst az Adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

19.2. A bejelentésben legalább:

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.

19.3. Adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartást a felügyeleti hatóság ellenőrizheti.

20. ADATKEZELÉSI FOLYAMATOK MEGVÁLTOZÁSA, ÚJ ADATKEZELÉS BEVEZETÉSE

20.1. Adatkezelő az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően köteles a kijelölt adatvédelmi tisztviselőhöz fordulni a változtatás, illetve az új adatkezelés jogszerűségének, megfelelőségének, célszerűségének és hatékonyságának vizsgálata tárgyában. Az adatvédelmi tisztviselő véleményezési jogkörrel vesz részt a folyamatban.

20.2. Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően szükséges azok jelen Szabályzatnak való megfelelőségét vizsgálni és azok csak abban az esetben vezethetők át a gyakorlatba, ha nem ütköznek jelen Szabályzat előírásaiba.

20.3. Az adatkezelési folyamatok megváltoztatása esetén vizsgálni kell, hogy az eredeti adatkezelés keretein belüli-e a változás, vagy egy más, új adatkezelés jön létre általa.

20.4. Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően az alábbiakat kell megvizsgálni:

a) az adatkezelés célját,

b) az adatkezelés jogalapját,

c) az érintettek körét,

d) az érintettekre vonatkozó adatok leírását,

e) az adatok forrását,

f) az adatok kezelésének időtartamát,

g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,

h) az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, a tevékenység tárgyát, időtartamát, az adatfeldolgozási feladat jellegét, célját, az érintettek kategóriáit, a feldolgozással érintett adatok típusát,

i) az alkalmazott adatfeldolgozási technológia jellegét,

j) adatvédelmi tisztviselő alkalmazása esetén annak nevét és elérhetőségi adatait.

20.5. Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően meg kell határozni az azzal érintett munkavállalók körét és el kell végezni a szükséges dokumentummódosításokat.

20.6. Az adatkezelési folyamatok megváltoztatását vagy új adatkezelés bevezetését megelőzően az igénybe venni kívánt adatfeldolgozókkal adatfeldolgozói szerződést kell kötnie az Adatkezelőnek.

III. ADATBIZTONSÁG

21.A NEKA ÁLTAL KEZELT ADATOK BIZTONSÁGA

21.1. A jelen Szabályzatban nem szabályozott adatbiztonsági kérdések tekintetében az Adatkezelő egyéb szabályzatai az irányadók.

21.2. Az Adatvédelmi és Adatbiztonsági Szabályzat alapvető rendeltetése a személyes adatok és az üzleti titkok megismerhetőségének korlátozására vonatkozó szabályok kialakítása, illetve ezen adatok illetéktelen személyek általi megismerhetőségének megakadályozása.

21.3. A fenti cél elérése érdekében az adatkezelések során - az adatkezelés jellegétől függően - az információ-rendszerek következő védelmi módszereit kell alkalmazni:

a) Ügyviteli védelem: az adatkezelő rendszerek felelőseinek és az adatkezeléssel kapcsolatos tevékenységnek szervezési és adminisztratív módon történő nyomon követése, a felelősség körülhatárolása. Kiterjed az informatikai és más adatkezelő rendszerekre és azok szolgáltatásaira, valamint az adathordozók kezelésére, beleértve a hozzáférési jogosultság és a betekintés dokumentálását is.

b) Fizikai védelem: olyan eszközök alkalmazása, amelyekkel azok a helyiségek védhetők, ahol számítástechnikai erőforrásokat használnak, vagy az adatmegőrzés szempontjából fontosak. Az információs rendszer minősítésétől függő védelemben kell részesíteni az adathordozókat is.

c) Algoritmikus védelem: matematikai algoritmusok alapján működő védelem, amely az egyedi számítógépen és a hálózaton is lehetővé teszi a használó azonosítását, a jogosultság ellenőrzését.

21.4. Az Adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.

21.5. Mind az Adatkezelő, mind az általa igénybe vett adatfeldolgozó köteles gondoskodni az adatok biztonságáról, és megtenni azokat a technikai és szervezési intézkedéseket, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az Adatkezelőnek és adatfeldolgozójának a fenti szabályok érvényesülését kell szem előtt tartaniuk az eljárási szabályok kialakítása során is.

21.6. Az adatokat megfelelő intézkedésekkel védeni kell különösen 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.

21.7. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében biztosítani kell, hogy e külön nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

21.8. A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a GDPR követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. A rendelet adatbiztonsági előírásainak való megfelelés igazolása érdekében, olyan belső szabályokat kell alkalmazni, valamint olyan intézkedéseket kell végrehajtani, amelyek teljesítik az adatvédelem – különösen a beépített és az alapértelmezett adatvédelem – elveit.

21.9. Az Adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Ilyen intézkedés lehet

a) a személyes adatok álnevesítése és titkosítása;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége;

c) fizikai vagy műszaki incidens esetén a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állás kellő időben történő visszaállítása;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése.

21.10. Az Adatkezelőnek a biztonság megfelelő szintjének meghatározásakor figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

21.11. Mind az Adatkezelőnek, mind az adatfeldolgozónak intézkedéseket kell hozniuk annak biztosítására, hogy a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

21.12. Adatkezelő által az elektronikus formában történő dokumentumtárolásra kialakított központi fájlszervere kizárólag jogosultsággal rendelkező munkavállalói számára érhető el. A felhasználói jogosultságok differenciáltak munkakörtől függően. Adatkezelő központi fájlszerveren a felhasználói tevékenységeket naplózza az aktuális kapcsolat létrejötte, felhasználónév, IP cím, megőrzési idő adatokkal.

21.13. Papír alapú adathordozók esetében a fizikai tárolás, irattárazás a munkavégzés idején zárva tartott, külön beléptetési jogosultsággal elérhető területen található irodákban található zárható szekrényekben történik.

22. AUTOMATIZÁLT ADATFELDOLGOZÁS

22.1. A személyes adatok automatizált feldolgozása során biztosítani kell:

a) a jogosulatlan adatbevitel megakadályozását;

b) a rendszerek jogosulatlan személyek általi használatának megakadályozását;

c) annak ellenőrizhetőségét és megállapíthatóságát 8 évre visszamenőleg,

i. hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;

ii. hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;

d) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát;

e) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

22.2. Az Adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, amennyiben ez nem jelent aránytalan nehézséget az Adatkezelőnek.

22.3. A fizikai biztonság megteremtéséhez az alábbi intézkedéseket szükséges megtenni:

a) Az adathordozó eszközök elhelyezésére szolgáló helyiségeket (épületeket, épületrészeket) úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen.

b) Azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését - a minősítéstől függően - korlátozni és ellenőrizni kell. A belépésre adott felhatalmazásnak összhangban kell lennie az adott személy hivatalos feladataival, illetőleg az ott kezelt adatokhoz történő hozzáférési jogosultságával.

c) A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell. Különös figyelmet kell fordítani arra, hogy a biztonságos területről kivitt eszközök maradványadatokat ne tartalmazzanak.

d) Az adathordozókról és mozgásukról, azok tartalmáról és felhasználásáról nyilvántartást kell vezetni.

e) A kezelt adatokat a Magyar Kézilabda Utánpótlásért Alapítvány szempontjából vett értékükkel és érzékenységükkel kifejezve kell differenciálni, osztályokba sorolni. Minden egyes osztályba sorolási eljáráshoz információkezelési eljárást is meg kell határozni annak érdekében, hogy azok a következő információfeldolgozási tevékenységfajtákat lefedjék:

- a másolást;
- a tárolást;

- a továbbítást postai úton, faxon és elektronikus levelezéssel;
- a beszélt szavakkal való átvitelt, beleértve a mobiltelefont, a hangüzenet szolgáltatást, valamint az üzenetrögzítést;
- a megsemmisítést.

f) Annak érdekében, hogy lecsökkenjen a jogosulatlan hozzáférés, az információvesztés és információrongálás kockázata, mind a rendes munkaidőben, mind azon kívül, bevezetésre kerül az „üres asztal" szabály a papíralapú anyagokra és a hordozható adattárolókra, valamint a „tiszta képernyő" szabály az információ-feldolgozó eszközökre. E szabályok részletesen:

- a papíranyagokat és a számítógépek adathordozóit megfelelő, zárható szekrényben vagy más, hasonlóan biztonságos bútorban kell tárolni, amikor éppen nincsenek használatban, különösen a munkaidőn kívüli időszakokban;
- személyi számítógépeket, munkaállomásokat, nyomtatókat és fénymásolókat nem szabad „bejelentkeztetni", amikor felügyelet nélkül maradnak, és használaton kívül kulcsreteszekkel, jelszavakkal vagy más óvintézkedésekkel legyenek védve;
- a bejövő és kimenő levelező eszközöket, a felügyeletlen faxgépeket védeni kell;
- a személyes adat és az üzleti titok kategóriájába sorolt információt kinyomtatás vagy sokszorosítás után azonnal el kell távolítani a nyomtatóról és a fénymásolóból.

22.4. Az üzemeltetési biztonság kialakítására az alábbi intézkedéseket szükséges megtenni:

a) Az adatkezelő eszközöket üzemeltető személyek feladatait egyértelműen meg kell határozni. Egyéb, a feladatoktól eltérő tevékenységet csak külön, erre irányuló egyedi vezetői felhatalmazás alapján lehet végezni.

b) Az adatkezelő eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható.

c) Az adatkezelést végző eszközök felhasználói kötelesek

- az aktív keresési folyamatok lezárására, ha a munka befejeződött, hacsak alkalmas reteszelő mechanizmussal nem tehetők biztonságossá, például jelszóval védett képernyővédővel;
- az adathordozó eszközöket a jogosulatlan használattal szemben biztonságossá tenni úgy, hogy kulcsra zárják, vagy ezzel egyenértékű védőintézkedést tesznek, például jelszavas hozzáférést használnak.

22.5. A technikai biztonság érdekében szükséges intézkedések:

a) Az adatok és programok véletlen vagy szándékos megrongálását meg kell akadályozni.

b) Az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell.

c) Az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, ennek érdekében az adatállományokról rendszeresen biztonsági másolatot kell készíteni, és azt az eredeti adatállománytól lehetőleg földrajzilag is eltérő helyen, biztonságosan kell tárolni.

d) Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell.

e) Közvetlen adathozzáférés kezdeményezésének jogosultságát ellenőrizni kell.

f) Pontosan meg kell határozni (munkakörönként, ill. személyenként) az egyes adatokhoz való hozzáférést.

23. MANUÁLIS KEZELÉSŰ ADATOK

23.1. A manuális kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) Az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni. Az iratok tárolására szolgáló helyiségek területe beléptetőrendszerrel védett Adatkezelő vagyonvédelmi berendezésekkel védett területén belül.

b) A folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá.

c) A manuális kezelésű iratok archiválását rendszeres időközönként el kell végezni, és a meghatározott adatkezelési határidő elteltével haladéktalanul át kell adni megsemmisítésre.

24. MUNKAVÁLLALÓI ADATBIZTONSÁGI KÖTELEZETTSÉGEK

24.1. Aki a személyes adat és az üzleti titkot képező adat megismerésére jogosult:

a) köteles a személyes adatok és üzleti titok védelmére vonatkozó rendelkezéseket, valamint a jelen Szabályzatban meghatározott előírásokat megismerni, valamint ezen előírásokat alkalmazni;

b) a tudomására jutott személyes adatot és üzleti titkot az érvényességi időn belül illetéktelen személynek át nem adhatja, illetve nem hozhatja illetéktelen tudomására vagy nyilvánosságra (titoktartási kötelezettség);

c) köteles a hozzáférési jog megszűnésekor – ideértve a munkaviszony megszűnésének eseteit is – az üzleti titokká minősített adatot és személyes adatot tartalmazó minden nála lévő adathordozót a Magyar Kézilabda Utánpótlásért Alapítványnak, mint az adattal rendelkező jogosultnak, illetve Adatkezelőnek haladéktalanul átadni.

24.2. Személyhez fűződő jogokat sért [Ptk. 2:46. §], aki üzleti titok birtokába jut, és azt jogosulatlanul nyilvánosságra hozza vagy azzal egyéb módon visszaél.

24.3. Üzleti titok tisztességtelen módon való megszerzésének minősül az is, ha az üzleti titkot a jogosult hozzájárulása nélkül, a vele - a titok megszerzése idején vagy azt megelőzően – bizalmi viszonyban (így különösen a munkaviszony és a munkavégzésre irányuló egyéb jogviszony) vagy üzleti kapcsolatban álló személy közreműködésével szerezték meg [1996. évi LVII. tv. a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról].

24.4. A Magyar Kézilabda Utánpótlásért Alapítvány valamennyi munkavállalója munkavégzése során köteles saját szakterületén jelen Szabályzat rendelkezéseinek, előírásainak érvényt szerezni.

25. TITOKTARTÁSI KÖTELEZETTSÉG

25.1. A Magyar Kézilabda Utánpótlásért Alapítvány munkavégzésre irányuló jogviszonyban lévő személyek kötelesek jelen Adatvédelmi és Adatbiztonsági Szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, illetve tudomásukra jutott személyes adatokat és üzleti titkokat időbeli korlátozás nélkül megőrizni. A munkavállalók kizárólag a munkaköri leírásban meghatározott feladatkörükön belül ismerhetik meg az ilyen adatokat.
E titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, külön törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.

25.2. Az adatbiztonság személyi feltételeinek kialakítása tekintetében a szervezeti rendszer minden tagját, aki feladatai ellátása során személyes adatot vagy üzleti titkot kezel, megfelelő felkészítésben, oktatásban kell részesíteni.

25.3. Minden személyes adatot, üzleti titkot tartalmazó rendszerhez való hozzáférésre feljogosított munkavállaló köteles teljes bizonyító erejű magánokiratba foglalt titoktartási kötelezettség vállalást tenni. A kötelezettség vállalásban nyilatkozni kell arról, hogy a munkavállaló jelen Adatvédelmi és Adatbiztonsági Szabályzat rendelkezéseit megismerte, azokat magára nézve kötelezőként elismeri, a szükséges titokvédelmi ismereteket elsajátította, valamint a személyes adatok védelméhez fűződő jog és az üzleti titok megsértésének mind büntetőjogi, mind polgári jogi következményeivel tisztában van.

IV. A JOGELLENES ADATKEZELÉS KÖVETKEZMÉNYEI

25.4. A GDPR 58. cikk (2) bekezdése szerint az Adatkezelő és az adatfeldolgozó tekintetében a felügyeleti hatóság korrekciós hatáskörében eljárva figyelmeztethet, hogy egyes tervezett adatkezelési tevékenységek valószínűsíthetően sértik a rendelet rendelkezéseit, elmarasztalhat, ha adatkezelési tevékenység megsértette a rendelet rendelkezéseit, utasíthatja az Adatkezelőt vagy az adatfeldolgozót, hogy teljesítse az érintettnek a rendelet szerinti jogai gyakorlására vonatkozó kérelmét, utasíthat – módot és határidőt is szabva – az adatkezelési műveleteknek a rendelet rendelkezéseivel történő összhangba hozására. Utasíthatja továbbá az Adatkezelőt, hogy tájékoztassa az érintettet az adatvédelmi incidensről. A felügyeleti hatóság átmenetileg vagy véglegesen korlátozhatja, megtilthatja az adatkezelést, elrendelheti a személyes adatok helyesbítését, vagy törlését, az adatkezelés korlátozását, valamint azon címzettek erről való értesítését, akikkel vagy amelyekkel a személyes adatokat közölték.

25.5. A hatóság visszavonja a tanúsítványt vagy utasítja a tanúsító szervezetet a kiadott tanúsítvány visszavonására, vagy utasítja a tanúsító szervezetet, hogy ne adja ki a tanúsítványt, ha a tanúsítás feltételei nem, vagy már nem teljesülnek.

25.6. A felügyeleti hatóság a GDPR 83. cikknek megfelelően közigazgatási bírságot szab ki az adott eset körülményeitől függően a fentiekben említett intézkedéseken túlmenően vagy azok helyett, és elrendeli a harmadik országbeli címzett vagy nemzetközi szervezet felé irányuló adatáramlás felfüggesztését.

25.7. A GDPR 83. cikk (4) bekezdés a) pontja szerint az adatkezelő és az adatfeldolgozó tekintetében a gyermek hozzájárulására vonatkozó feltételek, az azonosítást nem igénylő adatkezelések feltételeinek, az adatkezelési, adatfeldolgozási feltételek, a hatásvizsgálat kötelezettségének megsértése esetén legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeggel sújtható; melyek közül a magasabb összeget kell kiszabni.

25.8. A GDPR 83. cikk (6) bekezdése szerint a felügyeleti hatóság korrekciós hatáskörében eljárva [58. cikk (2) bekezdés] észlelt jogsértések esetén 20 000 000 EUR összegű közigazgatási bírságot, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeget állapíthat meg bírságként; melyek közül a magasabb összeget kell kiszabni.

25.9. A bíróság eljárása

a Ptk. 2:51. § (1) bekezdése alapján az érintett fél a fentieken felül a következő igényeket is támaszthatja:

a) a jogsértés megtörténtének bírósági megállapítását;

b) a jogsértés abbahagyását és a jogsértő eltiltását a további jogsértéstől;

c) azt, hogy a jogsértő adjon megfelelő elégtételt, és ennek biztosítson saját költségén megfelelő nyilvánosságot;

d) a sérelmes helyzet megszüntetését, a jogsértést megelőző állapot helyreállítását és a jogsértéssel előállított dolog megsemmisítését vagy jogsértő mivoltától való megfosztását;

e) azt, hogy a jogsértő vagy jogutódja a jogsértéssel elért vagyoni előnyt engedje át javára a jogalap nélküli gazdagodás szabályai szerint.

A személyiségi jog megsértésével okozott nem vagyoni sérelem miatt sérelemdíj követelhető a kártérítési felelősség szabályai szerint. A sérelemdíj megállapításához csak a jogsértés tényét kell bizonyítani, egyéb hátrányt nem.

Ptk. 2:52. §

(1) Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemért.

(2) A sérelemdíj fizetésére kötelezés feltételeire – különösen a sérelemdíjra köteles személy meghatározására és a kimentés módjára – a kártérítési felelősség szabályait kell alkalmazni, azzal, hogy a sérelemdíjra való jogosultsághoz a jogsértés tényén kívül további hátrány bekövetkeztének bizonyítása nem szükséges.

(3) A sérelemdíj mértékét a bíróság az eset körülményeire – különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására – tekintettel, egy összegben határozza meg.

A személyiségi jogok megsértése esetén a jogsértőtől kártérítés követelhető.

Ptk. 2:53. §

Aki személyiségi jogainak megsértéséből eredően kárt szenved, a jogellenesen okozott károkért való felelősség szabályai szerint követelheti a jogsértőtől kárának megtérítését.

25.10. A büntetőeljárás az egyéni felelősségre vonást célozza, tehát a szabályokat megsértő munkatárs, illetve a vezető kerül közvetlenül felelősségre vonásra.

Btk. 219. §

(1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja,

vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása

érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra követik el.

(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

25.11. A Munka Törvénykönyve rendelkezései alapján a munkáltató a Szabályzat és az adatkezelésre vonatkozó jogszabályok be nem tartását akár rendkívüli felmondással is szankcionálhatja, illetve a vétkesség függvényében a bekövetkezett teljes kár megfizetésére is igényt tarthat.

26. ZÁRÓ RENDELKEZÉSEK

26.1. Jelen Szabályzat 2020. április 29. napján lép hatályba.

Kelt és kihirdetve: Balatonbogláron, 2020. április 29-én.

Mocsai Tamás

ügyvezető

Magyar Kézilabda Utánpótlásért Alapítvány