BVSC-Zugló Közhasznú Egyesület

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZATA

Hatályos: 2026.05.05.
Verzió szám:2

Tartalom

A BVSC-Zugló Közhasznú Egyesület (a továbbiakban: 'BVSC'/'Egyesület') a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács (EU) 2016/679 rendeletet (a továbbiakban: általános adatvédelmi rendelet vagy GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján, a jogszerűség biztosítása céljából, az adatkezeléssel kapcsolatos belső folyamatait, eljárásait - így különösen az adatkezelés rendjét, a személyes adatok kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásban résztvevők feladatait és együttműködésük kereteit - az alábbi Adatvédelmi és Adatkezelési Szabályzatban (a továbbiakban: 'Szabályzat') határozza meg:

I.Fejezet
Általános Rendelkezések

A Szabályzat célja, hatálya, alkalmazása
1§.

(1) Jelen Szabályzat az adatkezelő adatvédelmi jogi megfelelésének elősegítésére szolgál, mely egységes szabályokat állapít meg az adatkezelő által folytatott valamennyi adatkezelésre vonatkozóan, továbbá előírásokat határoz meg annak érdekében, hogy az Adatkezelő által folytatott adatkezelési műveletek jogszerűségét biztosítsa.

(2) Jelen Szabályzat célja tehát, hogy

- biztosítsa a BVSC tevékenysége, működése során a személyes adatok védelméhez fűződő jogok érvényesülését, továbbá, hogy a BVSC által kezelt személyes-, illetve különleges személyes adatok (a továbbiakban együttesen: 'Személyes Adatok') jogosulatlan felhasználásának megakadályozása érdekében meghatározza a Személyes Adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat; továbbá
- hogy meghatározza a BVSC egyes feladati során vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint azokat a szervezési és technikai intézkedéseket, amelyek kialakításával a BVSC gondoskodik a Személyes Adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat a BVSC által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket is tartalmazza. Ezeket az előírásokat minden egyes adatkezelési folyamat/tevékenység során, annak teljes tartalma alatt figyelembe kell venni; valamint
- hozzájáruljon az adatkezelő szervezetén belül az adatvédelmi tudatosság növeléséhez, illetve az emberi mulasztásból eredő adatvédelmi kockázatok és jogsértések bekövetkezésének minimalizálásához.

(3) A Szabályzatban foglaltak értelemzése, alkalmazása és végrehajtása során minden esetben irányadó a vonatkozó, mindenkor hatályos szabályozási környezet, illetve a mindenkor hatályos jogszabályok tartalma a Személyes Adatokkal kapcsolatos valamennyi tevékenységre vonatkozóan is irányadó.

(4) Az adatkezelő megjelölése:

Neve: BVSC-Zugló Közhasznú Egyesület (rövidített név: BVSC-Zugló)
Székhely: 1142 Budapest, Szőnyi út 2.
Telephelyek: 1143 Budapest, Tatai út 79-85; 1143 Budapest, Tatai út 3.
Adószám: 19806990-2-42
Nyilvántartva: Fővárosi Törvényszék által: 0100/Pk.61267/1990 ügyszám alatt 149. határozattal, korábbi nyilvántartási formátumban: 1196/1990;
Nyilvántartási szám:01-02-0001196
Telefon: +36 30/273 1426
Honlap: https://www.bvsc.hu
Adatkezelő Képviselője: Szentpáli Gábor ügyvezető elnök

Adatkezelő e-mail címe: info@bvsc.hu
Az Adatkezelő adatvédelmi tisztviselőjének megjelölése: Dr. Peterdi Dominika (e-mail:adatvedelem@bvsc.hu; tel: +36 30/627 2438)

(5) Amennyiben egy adatról nem dönthető el annak személyes adat jellege, vagy különleges személyes adat jellege, úgy az azzal kapcsolatos belső döntésig azt úgy kell tekinteni, mintha ezen minősége/jellege fennállna. Az adat személyes adatként, avagy különleges személyes adatként való minősítéséről a BVSC képviselője dönt.

(6) A Személyes Adatok kezelése során a jogszabályok, valamint a jelen Szabályzat maradéktalan betartása mellett úgy kell eljárni, hogy a tevékenység
   a) Személyes Adatok kezelését csak az adott cél elérésre nézve feltétlenül indokolt mértékben és ideig eredményezze;
   b) a Személyes Adatok biztonságát, az érintett természetes személyek jogait és szabadságát ne veszélyeztesse.

(7) Jelen Szabályzat
   a) személyi hatálya kiterjed tehát i)a BVSC mindazon – *munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban, vagy a BVSC-vel fennálló egyéb jogviszonyban (a továbbiakban együttesen: munkaviszony) álló* - munkatársra, aki Személyes Adatot kezel (értve ez alatt a tárolást, megismerést, hozzáférést is) és/vagy Személyes Adatokkal bármilyen más kapcsolatba kerülnek (a továbbiakban együttesen: munkatársak); ii) továbbá azon természetes személyekre (érintett), akik személyes adatait a Jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, érintik, továbbá iii) azon érintettekre, akik jogait vagy jogos érdekeit a BVSC adatkezelése érinti;
   b) tárgyi hatálya kiterjed i) a Személyes Adatok BVSC általi kezelésére, függetlenül attól, hogy az adatkezelés papíralapon vagy elektronikusan történik; továbbá ii) minden, a BVSC működése során keletkezett vagy alkalmazott Személyes Adatokat tartalmazó dokumentumra, függetlenül az adattároló típustától és adattárolás módjától. Tehát a Szabályzat tárgyi hatálya kiterjed a BVSC-nél megvalósuló minden folyamatra, melynek során a GDPR 4. cikk 1 pontjában meghatározott személyes adat kezelése történik.

(8) Jelen Szabályzatot nem kell alkalmazni azokra az adatkezelési műveletkere, amelyek nem a Személyes Adatokra vonatkoznak.

(9) Jelen Szabályzat megismerése és betartása az adatkezelő minden munkatársa számára kötelező. A BVSC képviselője (ügyvezető elnök) köteles arról gondoskodni, hogy a BVSC munkatársai a jelen Szabályzatban, valamint a BVSC mindenkor hatályos Általános Adatkezelési Tájékoztatójában, illetve a munkatársakat-, valamint a sportolókat, sportszakembereket érintő adatkezelési tájékoztatókban (Adatkezelési Tájékoztató a BVSC Kollégái részére és Adatkezelési Tájékoztató Sportolók és Sportszakemberek részére) foglaltakat (a továbbiakban együttesen: Dokumentumok) megismerhessék.

(10) Jelen Szabályzat az adatkezelő belső dokumentumának minősül.

Értelmező rendelkezések és az adatkezelés feltételei

2.§

(1) E Szabályzat alkalmazásában használt fogalmak – a Szabályzatban meghatározott kivételekkel – megegyeznek a mindenkor hatályos, vonatkozó jogszabályi rendelkezésekben meghatározott fogalommeghatározásokkal, így különösen az alábbiakkal:

- ***Érintett:*** azonosított vagy azonosítható természetes személy;
- ***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.

- ***Különleges adat:*** a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
- ***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.
- ***Közérdekű adat***: a BVSC kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
- ***Közérdekből nyilvános adat***: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
- ***Adatkezelés***: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
- ***Adatkezelő***: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.
- **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatfeldolgozó végzi.
- ***Adatfeldolgozó***: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
- ***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.
- ***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.
- ***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.
- ***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.

- ***Profilalkotás***: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
- ***Álnevesítés***: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni
- ***Nyilvántartási rendszer***: a személyes adatok bármely módon tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

(2) Személyes Adatokat csak és kizárólag a törvényes cél eléréséhez szükséges esetekben és mértékben lehet kezelni a vonatkozó jogszabályok és jelen Szabályzat előírási alapján, az adatvédelmi alapelvek figyelembevételével.

(3) A BVSC-t, mint adatkezelőt terhelő kötelezettségek teljesítéséről az ügyvezető elnök gondoskodik, melynek keretében a feladata különösen:

a) döntés az adatkezelés szükségességére, céljára és időtartamára vonatkozóan;
b) az adatkezelés rendszeres felülvizsgálata;
c) az érintettek tájékoztatásának előkészítése, illetve az érintettek tájékoztatása;
d) az adatkezelés jogszerűségét alátámasztó körülmények dokumentálása (pl. hozzájárulás);
e) adatvédelmi incidens bekövetkezése esetén az adatvédelmi incidens értékelése az adatvédelmi tisztviselő bevonásával és az annak nyomán a szükséges intézkedések meghatározása.

Adatvédelmi Alapelvek
3.§

(1) A Személyes Adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni *(„jogszerűség, tisztesség eljárás és átláthatóság")*;
b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon *(„célhoz kötöttség")*;
c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk *(„adattakarékosság")*;
d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek *(„pontosság")*;
e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé *(„korlátozott tárolhatóság")*;
f) 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 *(„integritás és bizalmas jelleg")*;

(2) A BVSC, mint adatkezelő felelős az a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására *(„elszámoltathatóság")*.

(3) További, a GDPR-ban nem nevesített elvek, melyek mentén és figyelembevételével adatkezelési tevékenységet végez az Egyesület:

a) Adatbiztonság elve: A BVSC, mint adatkezelő köteles az adatkezelési műveleteket úgy megszervezni és végrehajtani, hogy az adatkezelésre vonatkozó jogszabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Köteles gondoskodni az általa kezelt Személyes Adatok biztonságáról, köteles továbbá megtenni azokat a technikai- és szervezési intézkedéseket, illetve kialakítani azon eljárási szabályokat, amelyek az adatvédelmi jogszabályok és a jelen Szabályzat érvényre juttatásához szükségesek.

b) Átláthatóság elve: A nyilvánosságnak vagy az érintettnek nyújtott tájékoztatásnak átláthatónak, könnyen értelmezhetőnek és hozzáférhetőnek kell lennie, valamint azt világosan és közérthető nyelven kell megfogalmaznia. Jelen rendelkezés a Személyes Adatok kezelésével összefüggő tájékoztatásra is vonatkozik. Ez az elv vonatkozik különösen

- az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatásra, valamint az azt célzó további tájékoztatásra, hogy mindenkor biztosított legyen az érintett Személyes Adatainak tisztességes és átlátható kezelése, továbbá
- azon tájékoztatásra, mely szerint az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról. A természetes személyt a Személyes Adatok kezelésével összefüggő szabályokról, garanciákról, jogokról tájékoztatni kell, valamint arról is, hogy hogyan gyakorolhatja az adatkezelés kapcsán őt megillető jogokat.

c) Tisztességes és átlátható adatkezelés elve: Ezen elv megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljáról. Az adatkezelő olyan további információkat is az érintett rendelkezésére bocsát, amelyek a tisztességes és átlátható adatkezelések biztosításához szükségesek, figyelembe véve a Személyes Adatok kezelésének konkrét körülményeit és kontextusát.

d) Dokumentálás elve: A BVSC által kezelt, Személyes Adatokat is tartalmazó adathordozókkal kapcsolatosan végrehajtott minden tevékenységet dokumentálni kell annak érdekében, hogy a Személyes Adatok útja és azok fellelhetőségének helye pontosan megállapítható legyen.

e) A felelősség elve: A Személyes Adatok kezelésében részt vevő/közreműködő munkatársak kötelesek ezen adatok védelmére vonatkozó előírásokat és jelen Szabályzat rendelkezéseit megismerni és betartani.

II.Fejezet
Adatvédelmi Rendelkezések

A BVSC adatvédelmi keretrendszere

Ügyvezető elnök
4.§

(1) A BVSC ügyvezető elnöke

a) felelős a BVSC adatkezelésének jogszerűségéért;

b) felelős a BVSC által kezelt Személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;

c) gondoskodik a NAIH-tól érkező megkeresések és ajánlások kezeléséről;

d) kinevezi vagy megbízza az adatvédelmi tisztviselőt, biztosítja számára feladatai ellátásnak feltételeit;

e) felügyeli az adatvédelmi feladatok ellátásának szervezeti kereteit;

f) jóváhagyja és kiadja az Adatvédelmi és Adatkezelési Szabályzatot.

(2) Amennyiben az ügyvezető elnök tudomást szerez súlyos vagy ismétlődő adatvédelmi jogszabálysértésről, kezdeményezi a szükséges vizsgálat/eljárás megindítását.

Adatvédelmi tisztviselő

5.§

(1) A BVSC a személyes adatok kezelésére vonatkozó jogi előírások teljesítéséhez és az érintettek jogai érvényesítésének elősegítése érdekében adatvédelmi tisztviselőt alkalmaz, aki adatvédelmi feladati ellátásával kapcsolatban nem utasítható és ebben a minőségében közvetlenül az ügyvezető elnök felügyelete alá tartozik és az ügyvezető elnöknek tartozik beszámolási kötelezettséggel is.

(2) Az Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátása során utasítást nem kap, feladatai ellátásával összefüggésben hátrányos jogkövetkezmény nem éri, továbbá biztosítja a feladatai ellátásához szükséges erőforrásokat és hozzáféréseket, valamint azt, hogy az adatvédelmi tisztviselő a személyes adatok kezelésével kapcsolatos kérdésekben kellő időben bevonásra kerüljön.

(3) Az adatvédelmi tisztviselő többek között:

a) fogadja az érintettek adatkezelőhöz beérkező adatvédelemmel összefüggő panaszait és kezdeményezi a panasz orvoslásához szükséges intézkedések megtételét;

b) kapcsolatot tart és együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatásában a felügyeleti hatósággal, a Nemzeti Adatvédelmi és Információszabadság Hatósággal ('NAIH');

c) adatvédelmi incidens esetén közreműködik az incidens kivizsgálásában és értékelésében;

d) segíti az ügyvezető elnököt és a munkatársakat az adatvédelmi kérdésekben, figyelemmel a GDPR vonatkozó előírásra;

e) eljár a BVSC-hez érkező, a BVSC Személyes adatokat érintő adatkezelésével összefüggő megkeresések tekintetében;

f) közreműködik az adatkezeléssel kapcsolatos egyéb, jogszabályokban meghatározott dokumentumok előkészítésében;

g) közreműködik a közérdekű adatigénylések teljesítésével kapcsolatos feladatokban.

(4) Az adatvédelmi tisztviselő jogosult valamennyi szervezet egységnél betekinteni az adatkezelésekbe, valamint a hozzájuk kapcsolódó dokumentumokba (pl. jegyzőkönyvekbe, nyilvántartásokba); a szervezeti egységek vezetőitől és munkatársaitól szóban és írásban is felvilágosítást kérhet. Az adatvédelmi tisztviselő részére hozzáférést kell biztosítani mindazon információkhoz és adatokhoz, amelyek feladati ellátáshoz szükségesek.

(5) Az adatvédelmi tisztviselőt feladati teljesítésével kapcsolatban titoktartási kötelezettség, illetve az adatok bizalmas kezelésére vonatkozó kötelezettség terheli. Az adatvédelmi tisztviselő az adatkezelővel fennálló jogviszonyának fennállása alatt és annak megszűnését követően is titokként megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott Személyes Adatokat.

(6) Az Adatkezelő az adatvédelmi tisztviselő elérhetőségét közzéteszi valamennyi adatkezelési tájékoztatójában, valamint az adatvédelmi tisztviselőt a NAIH részére bejelenti.

Az adatkezelésben résztvevők

6.§

(1) Az egyes szervezeti egységek/szakosztályok vezetői

a) felelősek azért, hogy az irányításuk vagy vezetésük alatt álló szervezeti egységeknél/szakosztályoknál az adatkezelés a jelen Szabályzatban meghatározottak szerint történjen,

b) gondoskodnak a külső hatóságoktól, szervektől, személyektől érkező, az adott szervezeti egység/szakosztály feladatkörébe tartozó személyes adatokat érintő adatkezelésekkel kapcsolatos megkeresések teljesítéséről; amennyiben indokolt és szükséges, egyeztetnek az adatvédelmi tisztviselővel;

c) felelősek azért, hogy a vezetésük alatt álló szervezeti egység/szakosztály által végzett adatkezelések során az adatbiztonsági előírások maradéktalanul teljesüljenek;

d) kötelesek tájékoztatást adni az adatvédelmi tisztviselő által valamely konkrét ügyhöz vagy adatkezeléshez kapcsolódóan szóban vagy írásban tett felvilágosítás kérésére;
e) az adatvédelmi incidenseket, egyéb adatvédelmi jogsértéseket vagy ezek gyanúját haladéktalanul jelzik az adatvédelmi tisztviselőnek;
f) amennyiben a területükhöz tartozó adatkezelési tevékenységek bővülnek, a meglévő folyamatok változnak, haladéktalanul tájékoztatják az adatvédelmi tisztviselőt

(2) Az Adatkezelő adatvédelmi rendszerének alapját azon munkatársak napi szintű munkája képezi, akik ennek során a Személyes adatokhoz hozzáférnek, azokkal dolgoznak. Az érintett munkatársak gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be az Adatkezelő által kezelt Személyes adatokba, és azokon egyéb jogosulatlan műveleteket se legyen módjuk végrehajtani.

(3) Az Adatkezelő valamennyi munkatársa köteles a Személyes adatok kezelése során az alábbi szabályokat megtartani:
a) a munkavégzés során csak az ahhoz elengedhetetlenül szükséges Személyes adatok kezelhetők, továbbíthatók, az adott feladatot ellátó szervezeti egység/szakosztály vezetőjének felelőssége a munkafolyamatok ennek megfelelő kialakítása;
b) informatikai jogosultságok engedélyezésekor figyelemmel kell lenni arra, hogy a Személyes adatokhoz csak az a személy és csak annyi ideig férhessen hozzá, akinek a munkavégzéséhez az adat, adatkör elengedhetetlenül szükséges;
c) Személyes adatokat tartalmazó papír alapú dokumentum csak zárt borítékban, vagy dokumentum-továbbításra alkalmas, zárt eszközben továbbítható;
d) e-mail útján személyes adatot – *különösen nagy mennyiségű, különleges vagy kiskorúakra vonatkozó adatot* – csak megfelelő technikai védelem (pl. titkosítás, jelszóvédelem) alkalmazása mellett lehet továbbítani. Amennyiben ilyen védelem nem biztosítható, az adat továbbítása kizárólag biztonságos belső tárhely használatával történhet
e) a szervezeti egységek/szakosztályok által használt közös meghajtókon személyes adatot tartalmazó dokumentum csak akkor tárolható, ha biztosított, hogy azt csak az arra jogosultak tekinthetik meg; a közös meghajtók esetében a meghajtóért felelős szervezeti egység/szakosztály vezetője a felelős a jelen pontban írt kötelezettség tekintetében;
f) az adatkezelési szabályok megsértéséért a munkatársak kötelesek – *annak észlelését követően* – haladéktalanul jelezni az adatvédelmi tisztviselő részére.

(4) Az adatkezelésben közvetlenül érintett munkatárs
a) feladatkörén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos és követhető dokumentálásáért;
b) amennyiben szükséges, előzetesen egyeztet az adatvédelmi tisztviselővel a személyes adatok kezelését érintő ügyekben, továbbá a NAIH közreműködését igénylő kérdésekben;
c) kezeli és megőrzi a feladata, illetve munkaköre ellátása során birtokába került adatokat, különös tekintettel a személyes adatokra;
d) köteles tájékoztatást adni az adatvédelmi tisztviselő által valamely konkrét ügyhöz vagy adatkezeléshez kapcsolódóan szóban vagy írásban tett felvilágosítás kérésére;
e) ügyel a nyilvántartások biztonságos kezelésére és tárolására;
f) gondoskodik arról, hogy az általa kezelt adatokhoz, nyilvántartásokhoz illetéktelen személy ne férhessen hozzá;
g) az adatkezeléssel kapcsolatosan feltárt visszásságot, az adatvédelmi tisztviselővel egyeztetve, köteles haladéktalanul megszüntetni;
h) betartja az adatkezelésre vonatkozó jogszabályokat, így különösen az Infotv. és a GDPR, valamint az adatvédelemmel és adatbiztonsággal kapcsolatos belső irányítási eszközök rendelkezéseit.

(5) Az adatkezelésben közvetlenül nem érintett munkatárs

a) köteles az adatkezelésre vonatkozó jogszabályokat, így különösen az Infotv. és a GDPR, valamint az adatvédelemmel és adatbiztonsággal kapcsolatos belső irányítási eszközök rendelkezéseit, valamint a jelen Szabályzat előírásait megismerni és maradéktalanul betartani;

b) közvetlen vezetője útján tájékoztatni az adatvédelmi tisztviselőt a feladatkörében felmerült bármely egyéb ágazati adatvédelmi problémáról, esetleges állásfoglalásról vagy más fejleményről.

Az érintettek jogai és érvényesítésük

7.§

(1) Az adatvédelemre vonatkozó jogszabályok alapján az érintett jogosult arra, hogy

- kérelmezze a személyes adataihoz való hozzáférést;
- kérje a személyes adatainak helyesbítését;
- kérje a személyes adatainak törlését;
- kérje a személyes adatok kezelésének korlátozását;
- tiltakozzon személyes adatainak kezelése ellen;
- kérje az adathordozhatóságot;
- visszavonja a hozzájárulását, illetve panaszt nyújtson be az illetékes felügyeleti hatósághoz.

a) *Hozzáférés joga*: Ezen jog alapján Ön 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 adataihoz és a GDPR-ban felsorolt információkhoz (pl. az adatkezelés célja, jogalapja) hozzáférést kapjon.
Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát köteles az Ön rendelkezésére bocsátani. Felhívjuk azonban a figyelmét arra, hogy a kért további másolatokért az Adatkezelő adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, továbbá a másolat igénylésére vonatkozó jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

b) *Helyesbítéshez való jog*: Ezen jog alapján Ön jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse az Önre vonatkozó pontatlan személyes adatokat, illetve, hogy kérje a hiányos személyes adatainak a kiegészítését.

c) *A törléshez való jog:* Ezen jog alapján Ön jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje az Önre vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy Önre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje meghatározott feltételek esetén.

d) *Az elfeledtetéshez való jog:* Az elfeledtetéshez való jog a törléshez való jog online környezetbe történő kiterjesztését jelenti, amely alapján ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy Ön kérelmezte a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.
Az Adatkezelő felhívja azonban a figyelmet arra, hogy a személyes adatok törlésére és „elfeledtetésére" nincs lehetőség, amennyiben a GDPR 17. cikk (3) bekezdésében meghatározott esetek valamelyike fennáll.

e) *Az adatkezelés korlátozásához való jog*: Ön jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

- Ön vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes, és Ön ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de Ön igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

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

f) *A tiltakozáshoz való jog*: A jogos érdeken, illetve a közhatalmi jogosítványon, mint jogalapokon alapuló adatkezelések esetében Ön jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a (...) kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

g) *Tiltakozás közvetlen üzletszerzés estén:* Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, Ön jogosult arra, hogy bármikor tiltakozzon az Önre vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha Ön tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

h) *Az adathordozhatósághoz való jog*: Ezen jog alapján Ön jogosult arra, hogy az Önre vonatkozó, és egy adatkezelő rendelkezésére bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket a személyes adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. Ezt a jogát akkor gyakorolhatja, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon történik.
Jelen pont szerinti jog nem illeti meg az érintettet, amennyiben az hátrányosan érintené mások jogait és szabadságát.

i) *A hozzájárulás visszavonásához való jog*: Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A beleegyezés megadása előtt az érintettet ezen jogáról tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.
Amennyiben az érintett visszavonja a személyes adatainak kezelésére vonatkozóan az Adatkezelőnek adott hozzájárulását, akkor lehet, hogy egyáltalán nem, vagy csak részben tudja az Adatkezelő biztosítani a kért szolgáltatást, illetve fenntartani az érintettel fennálló jogviszonyt. Erről a tényről az Adatkezelő az érintettet tájékoztatja. Amennyiben az érintett ezen tájékoztatás ellenére továbbra is fenntartja hozzájárulásának visszavonására vonatkozó kérelmét, úgy az Adatkezelő törli a hozzájárulás alapján kezelt személyes adatokat, kivéve, ha azok kezelésére valamilyen más jogalap alapján jogosult. A hozzájárulás visszavonása esetén az Adatkezelő a hozzájáruláson alapuló adatkezelést haladéktalanul megszünteti. Amennyiben az Adatkezelő az adott adatkör kezelése tekintetében más jogalappal is rendelkezik, erről az érintettet tájékoztatja, és az adatkezelést kizárólag e más jogalap keretei között folytatja.

Az érintett a fenti jogok gyakorlására vonatkozó kérelmét az Adatkezelő székhelyére vagy elektronikus elérhetőségeire küldheti el. Az Adatkezelő legkésőbb a kérelem beérkezésétől számított 1 hónapon belül nyújt tájékoztatást a kérelem nyomán hozott intézkedésekről, illetve amennyiben nem tesz intézkedéseket, legkésőbb a kérelem beérkezésétől számított 1 hónapon belül nyújt tájékoztatást az intézkedés elmaradásának okairól. Ekkor az Adatkezelő az érintettet tájékoztatja jogorvoslati jogairól is.

Szükség esetén – *figyelembe véve a kérelem összetettségét és a kérelmek számát* – a fenti bekezdésben jelzett határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról azonban az Adatkezelő köteles a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatni az érintettet.

Az érintetti kérelmekre vonatkozó tájékoztatás és intézkedés főszabály szerint díjmentes. Ha azonban a kérelem egyértelműen megalapozatlan vagy – *különösen ismétlődő jellege miatt* – túlzó, az Adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő

intézkedést. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása azonban az Adatkezelőt terheli.

Hatósághoz és bírósághoz való fordulás joga:

a) Az érintett a GDPR 77. § cikke alapján az Adatkezelő adatkezelési eljárásával kapcsolatos panasszal a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat:

Nemzeti Adatvédelmi és Információszabadság Hatóság
1055 Budapest, Falk Miksa utca 9-11.
Levelezési cím: 1363 Budapest, Pf. 9.
Telefon: +36 -1-391-1400; +36 (30) 683-5969;+36 (30) 549-6838
E-mail: ugyfelszolgalat@naih.hu

b)Az érintett a GDPR 79. cikk (1) bekezdése szerint az Adatkezelő adatkezelési eljárásával kapcsolatos jogsértés miatt a lakóhelye vagy tartózkodási helye szerint illetékes törvényszékhez fordulhat. (A törvényszékek elérhetőségéről az alábbi linken lehet tájékozódni: http://birosag.hu/torvenyszekek)

A személyes adatok kezelhetőségére vonatkozó feltételek
8.§

(1) Az Adatkezelő személyes adatot kizárólag a GDPR 6. cikkében meghatározott jogalapok valamelyike – *valamint különleges adatok esetén a GDPR 9 cikk. (2) bekezdésében foglalt kivételszabályok figyelembevétele* – alapján kezeli. Az adatkezelés jogalapját az Adatkezelő minden esetben az adatkezelés megkezdését megelőzően a kezelt adatok természetét, a tervezett adatkezelés jellegét és az érintetti kör sajátosságait is figyelemeb véve határozza meg, az Európai Adatvédelmi Testület (EDPB), valamint a NAIH iránymutatásait

(2) Személyes Adatok kizárólag az alábbi feltételek együttes teljesülése esetén kezelhetők:
   a) az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének valamely pontját teljesíti, így
      aa) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
      ab) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
      ac) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
      ad) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
      ae) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
      af) 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;
   b) az adatkezelés szükségességét az ügyvezető (mint adatkezelésért felelős vezető) jóváhagyta;
   c) az adatkezelésre vonatkozóan, amennyiben szükséges, úgy az adatvédelmi kockázatelemzés, érdekmérlegelési teszt vagy adatvédelmi hatásvizsgálat elkészült, melyet az ügyvezető által kijelölt/megbízott személy köteles az ügyvezető által megjelölt határidőig elvégezni;
   d) az adatkezelés a belső adatvédelmi nyilvántartásban (a továbbiakban: 'adatkezelési tevékenységek nyilvántartása') rögzítésre került, vagy – *az adatkezelés megkezdését követően* – haladéktalanul rögzítésre kerül.

(3) A különleges adatok kezelése esetén az (1) bekezdésben írt feltételek teljesítésén túl szükséges az is, hogy az adatkezelés megfeleljen a GDPR 9. cikk (2) bekezdésének valamely pontjában foglaltaknak is.

(4) Amennyiben az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének a) pontja (érintett hozzájárulása) és az kiskorú érintett személyes adatainak kezelésére irányul, a hozzájárulást a kiskorú törvényes képviselője adhatja meg az Adatkezelőnek.

(5) Ha a személyes adatok kezelése az adatgyűjtés eredeti céljától eltérő célból válik szükségessé, és e célok egymással összeegyeztethetők, az adatkezelési művelet elvégzéséhez nem kell új jogalapot megjelölni. A célok összeegyeztethetőségéről való döntés során figyelembe kell venni,

- a személyes adatok gyűjtésének körülményeit;
- az érintett és az Adatkezelő közötti kapcsolatot (pl. van-e egyenlőtlenség);
- a személyes adatok jellegét (különleges adatok-e);
- hogy a további adatkezelés az érintettre milyen következménnyel járna; és
- megfelelő garanciák állnak-e rendelkezésre (pl. titkosítás, álnevesítés).

Nem kell külön mérlegelni a célok összeegyeztethetőségét, ha a további adatkezeléshez az érintett hozzájárult, vagy ha azt uniós- vagy nemzetközi jog írja elő. Eltérő célból való további adatkezelés megkezdése előtt a célok összeegyeztethetőségéről és a figyelembe vett szempontokról emlékeztetőt kell írni, az érintettet továbbá tájékoztatni kell az eltérő célról.

(6) Minden olyan esetben, amikor az adatkezelés célját és eszközét nem kizárólag az Adatkezelő határozza meg, úgy az adatkezelés további feltétele, hogy a két (vagy több) adatkezelő a GDPR 26. cikke szerinti közös adatkezelői megállapodást is megkösse, amelyekre az Adatkezelő nevében az ügyvezető jogosult.

(7) Amennyiben az Adatkezelő adatfeldolgozóként jár el, vagy az adatkezelés során adatfeldolgozót (aladatfeldolgozót) kíván igénybe venni és az adatfeldolgozói feladatokról nem, vagy nem teljeskörűen rendelkezik jogszabály, az adatfeldolgozói feladatok ellátásáról szerződést kell kötni a GDPR 28. cikk (3) bekezdése szerinti tartalommal.

(8) Az adatkezelés céljaként csak olyan ok vagy körülmény jelölhető meg, amely a jogszabályi elvárásoknak megfelel, az Adatkezelő tevékenységével közvetlenül összefügg, ahhoz szükséges vagy arra nézve célszerű.

(9) A kezelt adatok köre a minimálisan szükséges, ugyanakkor az Adatkezelő tevékenysége biztonságos és felelős ellátásra nézve indokolt mértékben határozandó meg.

(10) Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően továbbra is magas fenyegetettséggel jár az érintettekre nézve, a személyes adatok kezelését megelőzően az ügyvezető köteles konzultációt kezdeményezni a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH).

(11) Az adatkezelési tevékenységek nyilvántartása adatait az adatvédelmi tisztviselő viszi fel az adatbázisba, amely nyilvántartást az ügyvezető szükség szerint, de legalább évente ellenőrzi.

Érdekmérlegelési teszt jogos érdek jogalap alkalmazása esetén

9.§

(1) Amennyiben az adatkezelést az Adatkezelő a GDPR 6. cikk (1) bekezdés f) pontja szerinti jogalapon (jogos érdek) kívánja végezni, úgy érdekmérlegelési tesztet kell készítenie.

(2) Az érdekmérlegelési teszt elsődlegesen az alábbiakat tartalmazza:

- a kezelni kívánt személyes adatok meghatározása;
- az Adatkezelő bemutatása;
- a jogos érdek bemutatása;
- az adatkezelés céljainak meghatározása;
- annak vizsgálata, hogy az adatkezelés feltétlenül szükséges-e az azonosított jogos érdek érvényesítéséhez;
- ha az adatkezelés szükséges a jogos érdek érvényesítéséhez, annak vizsgálata, hogy az érvényesíthető-e más, az érintett magánszféráját nem, vagy a tervezett adatkezelésnél kevésbé érintő folyamattal;

- ha a jogos érdek nem érvényesíthető más, az előző pont szerinti folyamattal, annak vizsgálata, hogy az adatkezelés esetén az érintett érdekei, alapjogai mennyiben korlátozódnak vagy sérülnek;
- a jogos érdek és az érintetti alapjogi korlátozás összevetése;
- alternatív jogalapok vizsgálata;
- az Adatkezelő által az adatkezelés kapcsán alkalmazott garanciális jellegű intézkedések bemutatása;
- az érdekmérlegelési teszt eredménye, végkövetkeztetés (végezhető az adatkezelés jogos érdek jogalapon vagy sem);
- az érdekmérlegelési teszt elvégzésének dátuma.

(3) Olyan adatkezelésekre nézve, amelyek logikailag egymáshoz kapcsolódnak, vagy valamely folyamat különböző, de egymással összefüggő szakaszaiban történnek, az érdekmérlegelés egy dokumentum (egy teszt) keretén belül elvégezhető.

(4) Amennyiben az érdekmérlegelési teszt eredményeként az Adatkezelő megállapítja, hogy az adatkezeléssel érintett jogos érdekkel szemben elsőbbséget élveznek az érintettek érdekei és alapvető jogai, úgy az adott adatkezelés nem alkalmazható.

(5) Az érdekmérlegelési tesztet az adatvédelmi tisztviselő, illetve az ügyvezető által megbízott minden olyan esetben soron kívül felülvizsgálja, amikor a vonatkozó adatkezelésben ezt indokolttá tevő változást tervez az Adatkezelő. Ilyen körülmény hiányában is szükséges az érdekmérlegelési teszteket legalább két évente felülvizsgálni.

(6) Az érdekmérlegelési tesztet az Adatkezelő az érintettek részére nem teszi elérhetővé. Az érdekmérlegelési teszt az Adatkezelő üzleti titkát képező iratnak minősül, ahhoz kizárólag az adatvédelmi tisztviselő és az ügyvezető, illetve az ügyvezető által felhatalmazott/megbízott személyek rendelkeznek hozzáféréssel.

Adatvédelmi Hatásvizsgálat
10.§

(1) Amennyiben az Adatkezelő új adatkezelést kíván bevezetni, úgy a jelen részben foglaltak szerint köteles megvizsgálni, hogy az adatkezelés megkezdése előtt szükséges -e adatvédelmi hatásvizsgálatot lefolytatni.

(2) Az Adatkezelő adatvédelmi hatásvizsgálatot folytat le az alábbi esetekben:
   a) ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságaira nézve;
   b) ha az adatkezelés jelentős mértékű különleges adatra irányul;
   c) a tervezett adatkezelés – *jellemzőit tekintve* – szerepel a NAIH által közzétett hatásvizsgálati listán.

(3) Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatot jelentenek, egyetlen hatásvizsgálat keretei között értékelhetőek.

(4) Az adatvédelmi hatásvizsgálatnak ki kell terjednie elsődlegesen:
   a) a tervezett adatkezelési művelet módszeres leírására és az adatkezelés céljainak ismertetésére;
   b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
   c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
   d) a kockázatok kezelését célzó intézkedések bemutatására, továbbá
   e) esettől függően minden egyéb releváns körülményre.

(5) Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő végzi el, amelynek során szorosan együttműködik az ügyvezető által megbízott/felhatalmazott személlyel.

(6) Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően továbbra is magas kockázattal jár az érintettre nézve, a személyes adatok kezelését megelőzően az ügyvezető konzultációt kezdeményez a NAIH-val. A konzultációba az adatvédelmi tisztviselőt, illetve az ügyvezető által megbízott, felhatalmazott személyt be kell vonni, akik a konzultáció megállapításai szerint végrehajtott intézkedések eredményei alapján a kockázatelemzést, valamint az adatvédelmi hatásvizsgálatot felülvizsgálják.

Adatkezelési tevékenységek nyilvántartása
11.§

(1) Minden személyes adatokkal kapcsolatos adatkezelést nyilvántartásba kell venni (adatkezelői nyilvántartás). Az adatkezelés és az adatfeldolgozás megkezdését, módosítását és megszüntetését az érintett szervezeti egység/szakosztály vezetőjének be kell jelenteni az adatvédelmi tisztviselőnek, aki gondoskodik annak bejegyzéséről, illetve a változások átvezetéséről a nyilvántartásban. A nyilvántartás vezetése elektronikus úton rögzített formában történik és azt – *kérésére* – a NAIH rendelkezésére kell bocsátani.

(2) Az adatkezelői nyilvántartásban szereplő adatkezelések felülvizsgálatát szükség szerint, indokolt esetben, de legalább évente el kell végezni, amely felülvizsgálatot az adatvédelmi tisztviselő koordinál. A felülvizsgálat megtörténtét követően a nyilvántartás naprakész adatait be kell mutatni az ügyvezetőnek.

(3) Az adatkezelési tevékenységek nyilvántartását a GDPR. 30. cikk szerinti tartalommal kell vezetni.

(4) A személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek – *ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket* – körét és az adattovábbítás egyéb adatait külön nyilvántartás (adattovábbítási) tartalmazza. (1. számú melléklet)

(5) Adatfeldolgozó igénybevételével történő adatkezelés esetén az Adatkezelőnek az adatfeldolgozók nyilvántartásában (2. számú mellékelt) kell rögzíteni az adatfeldolgozó vagy adatfeldolgozók nevét és elérhetőségeit, az adatfeldolgozó képviselőjének nevét és elérhetőségeit, az adatfeldolgozási tevékenységeket, illetve amennyiben lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírását.

(6) A jelen részben rögzített nyilvántartások adatainak valódiságát az adatvédelmi tisztviselő az adott adatkezelést, adatfeldolgozást végző szervezeti egység/szakosztály vezetőjének bevonásával szükség szerint, de legalább évente felülvizsgálja, az időközben történt változásokat átvezeti.

(7) Az érintetti joggyakorlással kapcsolatosan az Adatkezelő az érintett szervezeti egység/szakosztály adatszolgáltatásával az adatvédelmi tisztviselő útján érintett -tájékoztatási nyilvántartást vezet. (3. számú mellélet)

(8) Az adatkezeléssel érintett szervezeti egység/szakosztály adatszolgáltatása alapján az adatvédelmi tisztviselő elektronikus nyilvántartást vezet az érintett hozzáférési jogával kapcsolatos intézkedésekről. A nyilvántartás az alábbi információkat tartalmazza:
   a) az adatokhoz való hozzáférés jogát érvényesítő érintett neve;
   b) a megkeresésé beérkezésének időpontja;
   c) a megkeresés tárgya;
   d) az érintett hozzáférési jogának érvényesítését korlátozó vagy megtagadó intézkedés megtételének időpontja;
   e) az érintett hozzáférési jogának érvényesítését korlátozó vagy megtagadó intézkedés jogi és ténybeli indokai

(9) Az érintetti joggyakorlással kapcsolatos nyilvántartásban szereplő adatokat az Adatkezelő az érintetti kérelem lezárását követően 3 (három) évig őrzi meg az elszámoltathatóság biztosítása céljából, ezt követően törli vagy anonimizálja.

Amennyiben az érintetti joggyakorlás hatósági vagy bírósági eljárást eredményez, az adatok az eljárás jogerős lezárásáig megőrizhetők.

Nyilvánosságra hozatal, Adattovábbítás
12.§

(1) Az Adatkezelőnél kezelt személyes adatok nyilvánosságra hozatala – *kivéve, ha törvény rendeli el, vagy ha az érintett hozzá járul* – tilos! Az Adatkezelő kezelésében lévő személyes adatok nyilvánosságra hozatalát törvény – az adatok körének meghatározásával – közérdekből elrendelheti.

(2) Az Adatkezelőről szóló – *személyes adatokon is alapuló* – statisztikai adatok korlátozás nélkül közölhetők.

(3) Amennyiben a személyes adat kezelése az érintett hozzájárulásán alapult, a hozzájárulás visszavonását követően az Adatkezelő a személyes adatokat kizárólag akkor továbbíthatja, ha az adattovábbítás önálló jogalappal rendelkezik (különösen jogi kötelezettség vagy jogos érdek), és erről az érintettet előzetesen vagy legkésőbb az adattovábbítással egyidejűleg tájékoztatja.

(4) Az Adatkezelő csak olyan személyes adatot továbbíthat, amelynek a BVSC- Zugló törvényben meghatározott adatkezelője, vagy amit más adatkezelőtől jogszerűen átvett, amennyiben ezt az érintett nem tiltotta meg.

(5) Adattovábbítási esetén minden esetben meg kell győződni az adatkezelés jogalapjáról, kétség esetén az adatvédelmi tisztviselő szakmai véleményének kikérése mellett. Személyes adatot továbbítani csak abban az esetben lehet, ha az adattovábbítás jogalapja egyértelmű, célja és az adattovábbítás címzettje pontosan meghatározott. Az adattovábbítást minden esetben dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen. (1. sz. melléklet)

(6) Ha az adattovábbításhoz az érintett hozzájárulására van szükség, akkor e hozzájárulás megtörténtét írásban is rögzíteni szükséges. Az érintett a hozzájárulást az adattovábbítás jogalapja, célja és a címzett ismeretében adja meg.

(7) A BVSC-n kívüli szervtől vagy magánszemélytől érkező, személyes adatokat érintő adatközlésre irányuló megkeresés csak törvényben meghatározott esetekben, vagy akkor teljesíthető, ha ehhez az érintett írásban hozzájárulását adta. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére, feltéve, hogy az erre vonatkozó, megfelelő tájékoztatást megkapta.

(8) A vonatkozó jogszabályokban meghatározott személyes és különleges adatok az érintett nyilatkozattételétől függetlenül továbbíthatóak kizárólag jogszabályon alapuló kötelező adattovábbítás esetén, a jogszabályban meghatározott célra, adattartalomra és címzetti körre korlátozva.

(9) Nem teljesíthető olyan adatigénylés, amelynek törvényessége - *az adatigénylés vagy érintetti hozzájárulás hiányos adatartalmára, vagy más körülményre tekintettel* – nem állapítható meg.

(10) Amennyiben az adattovábbítás jogszerűségével kapcsolatban kétség merült fel, az érintett szervezeti egység vezetője – *írásban vagy elektronikus úton* – az adatvédelmi tisztviselőhöz fordulhat, aki 5 (öt) munkanapon belül állásfoglalást ad ki az adattovábbítás jogszerűségéről.

(11) A megkeresett szervezeti egység/szakosztály vezetője az adattovábbítást - *ha jogszabály vagy egyéb az adattovábbítás teljesítésére vonatkozó előírás nem rendelkezik másképp* – az erre irányuló kérelem beérkezését követő 15 (tizenöt) napon belül teljesíti, vagy szükség esetén az adatvédelmi tisztviselő állásfoglalásának figyelembevételével dönt a megkeresés teljesítésének az elutasításról, a törvényben meghatározott kötelező adatszolgáltatásokat kivéve. A döntés ellen az adatkérő az ügyvezetőhöz írásban benyújtott panasszal fordulhat, aki a panasz beérkezésétől számított 15 (tizenöt) napon belül határoz az adatok továbbíthatóságáról.

(12) Az előző bekezdésben foglalt eljárás nem vonatkozik a közérdekű vagy közérdekből nyilvános adatokkal kapcsolatos adattovábbításokra.

(13) Az Adattovábbításról az adott szervezeti egység/szakosztály a jelen Szabályzat szerinti tartalommal köteles nyilvántartást vezetni (1. számú melléklet), amelyhez hozzáférést biztosít az adatvédelmi tisztviselő részére.

Az adattovábbítási nyilvántartás adatait az Adatkezelő az adattovábbítás teljesítését követő naptári év végétől számított 5 (öt) évig őrzi meg az adattovábbítás jogszerűségének és elszámoltatható teljesítésének igazolása céljából, ezt követően törli vagy anonimizálja.

Amennyiben az adattovábbítással összefüggésben hatósági, bírósági vagy egyéb jogvita indul, a nyilvántartás adatai az eljárás jogerős lezárásáig megőrizhetők.

(14) Személyes adatok harmadik országba (azaz az Európai Gazdasági Térség területén kívülre) kizárólag a GDPR 45., 46., valamint 48-49. cikkei alapján továbbíthatók.

(15) Az Adatkezelő a személyes adatok harmadik országba történő továbbítása esetén elsősorban azt vizsgálja meg, hogy az Európai Bizottságnak van-e az adott ország tekintetében elfogadott megfelelősségi határozata. Az Európai Bizottság a megfelelősségi határozatainak a listáját a honlapján közzéteszi (elérhető: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). Amennyiben igen, úgy a személyes adatok továbbítására a megfelelősségi határozat alapján kerül sor.

(16) Abban az esetben, ha az adattovábbítás olyan országba történik, amelynek tekintetében megfelelősségi határozat nincs, úgy az adattovábbításra csak megfelelő garanciák alkalmazása mellett kerülhet sor. Megfelelő garanciának minősül, ha

a) az adattovábbítás az Európia Bizottság által elfogadott általános adatvédelmi kikötéseken alapul és azoknak megfelel;

b) az adattovábbításra az Európai Unióban elfogadott magatartási kódex vagy tanúsítási mechanizmus alapján kerül sor azzal, hogy a harmadik országbeli címzett kötelező erejű és kikényszeríthető kötelezettségvállaló nyilatkozatot tesz arra, hogy az adott magatartási kódexet és/vagy tanúsítási mechanizmust és az abban foglalt garanciákat alkalmazza.

Amennyiben a személyes adatok továbbítása az Európai Bizottság által elfogadott általános adatvédelmi kikötések (SCC) alapján történik, az Adatkezelő az adattovábbítást megelőzően – *az adattovábbítás körülményeire figyelemmel* – kiegészítő technikai, szervezési és/vagy szerződéses intézkedéseket határoz meg és dokumentál annak érdekében, hogy a továbbított személyes adatok védelmi szintje ténylegesen megfeleljen az Európai Unióban biztosított védelemnek.

(17) Amennyiben a harmadik országba történő adattovábbítás a fentiek szerint nem lehetséges, úgy az adattovábbításra kizárólag a GDPR 49. cikke szerinti esetekben kerülhet sor.

Különleges adatok kezelése
13.§

(1) Különleges adatot kizárólag a GDPR 9. cikk (2) bekezdésében foglalt esetekben (így különösen az érintett kifejezett hozzájárulása alapján) valamint a jelen Szabályzatban meghatározott feltételek teljesülése esetén kezelhetők.

(2) Különleges adatokhoz kizárólag szerepkör-alapú, a feladat ellátásához feltétlenül szükséges hozzáférés biztosítható, a legkisebb jogosultság elve szerint. A hozzáférések engedélyezéséről, módosításáról és visszavonásáról az ügyvezető dönt az adatvédelmi tisztviselő bevonásával, és a jogosultságokat dokumentált módon nyilván kell tartani.

(3) Különleges adatok esetében az adatkezeléssel kapcsolatos kockázatok sem az adatvédelmi hatásvizsgálat, sem az adatvédelmi incidensek keretében nem zárhatók ki és nem értéklehetők az azokkal kapcsolatos tevékenységek valószínűsíthetően kockázatmentesnek.

(4) Különleges adatok esetében az azok jellegére és formájára, valamint az adatkezelés kockázataira figyelemmel indokolt technikai és szervezési intézkedések elrendelése nem mellőzhető.

Adatvédelmi incidenssel kapcsolatos eljárás; adatvédelmi incidensek nyilvántartása

14.§

(1) Az 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. A leggyakoribb incidens lehet különösen i) laptop/külső adathordozó elvesztése, ii) személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott, személyes adatot tartalmazó irat), iii) adatok nem biztonságos továbbítása.

(2) Az adatvédelmi incidens megelőzése, kezelése, a vonatkozó jogi előírások betartása, betartatása az ügyvezető feladata. Az incidens megelőzése, a bekövetkezett incidens előzményeinek visszakereséses érdekében az informatikai rendszereken naplózni kell a hozzáféréseket és a hozzáférési kísérleteket.

(3) Aki adatvédelmi incidens megtörténtéről szerez tudomást, azt haladéktalanul, de legkésőbb 12 órán belül köteles jelezni az ügyvezetőnek vagy az adatvédelmi tisztviselőnek.

(4) Adatvédelmi incidens bejelenthető az Adatkezelő központi e-mail címén, telefonszámán vagy, amennyiben lehetőség van rá, közvetlenül az ügyvezetőhöz, adatvédelmi tisztviselőhöz.

(5) Adatvédelmi incidens bejelentése esetén az ügyvezető, a szükséges egyéb személyek bevonásával haladéktalanul gondoskodik a bejelentés kivizsgálásáról, melynek során azonosítani kell az incidenst, illetve el kell dönteni, hogy valódi incidensről, avagy téves riasztásról van szó. Az ügyvezető gondoskodik továbbá az incidenssel kapcsolatos kockázatok értékeléséről, valamint – *szükség szerint*- az incidens NAIH részére való bejelentésével és az érintettek tájékoztatásával kapcsolatos dokumentáció előkészítéséről. Az incidens kivizsgálása során meg kell határozni azokat a technikai és szervezési intézkedéseket, amelyek a további incidensek elkerülését szolgálják. Az incidens kivizsgálásra irányuló eljárás lefolytatásába az adatvédelmi tisztviselőt be kell vonni.

(6) Amennyiben az adatvédelmi incidens az érintettek jogaira és szabadságára nézve valószínűsíthetően kockázatot jelent, azt haladéktalanul, de legkésőbb - *az incidens bekövetkezésétől vagy az arról való tudomásszerzéstől számított* – 72 órán belül a GDPR 33. cikke szerinti tartalommal be kell jelenteni a NAIH-nak. Ha a bejelentés 72 órán belül nem tehető meg, abban meg jel jelölni a késedelem okát. Ha ez a kockázat valószínűsíthetően magas, a NAIH mellett az érintett(ek)et is értesíteni kell a GDPR 34. cikkében foglaltak szerint.

(7) Az adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni és lehetőség szerint el kell különíteni, továbbá gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően meg kell kezdeni a károk helyreállítását és a jogszerű működés visszaállítását.

(8) Az adatvédelmi incidensekről nyilvántartást kell vezetni (4. sz. melléklet), amely - *minimum* - tartalmazza:
   a) az incidens bekövetkezésének időpontját és helyét,
   b) az incidens körülményeit, hatását;
   c) az érintett személyes adatok körét;
   d) az incidenssel érintettek körét és számát;
   e) az incidens következményeinek elhárítására megtett intézkedéseket;
   f) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat

(9) Az adatvédelmi incidenst az adatvédelmi tisztviselő vezeti a nyilvántartásba. Az adatvédelmi incidenst akkor is rögzíteni kell a nyilvántartásban, ha a NAIH-nak való bejelentése, illetve az érintettek tájékoztatása azzal kapcsolatban nem indokolt.

(10) Az incidens értékelésével kapcsolatos dokumentumokat elektronikus formában kell elmenteni, melyekhez az ügyvezető és az adatvédelmi tisztviselő férhet hozzá.

(11) A nyilvántartásban szereplő, adatvédelmi incidensre vonatkozó adatokat 5 évig kell megőrizni.

(12) Ha az adatvédelmi incidens az Adatkezelő esetleges adatfeldolgozói feladatainak ellátása során következett be, akkor azt, a tudomásszerzést követően haladéktalanul jelezni kell az adatkezelőnek.

III.Fejezet
Adatbiztonság

Adatbiztonsági intézkedések, valamint az adatkezelés technikai szabályai
15. §

(1) A BVSC az adatkezelési tevékenységei vonatkozásában a Személyes Adatok biztonsága érdekében megteszi azokat a technikai és szervezési intézkedéseket, valamint kialakítja azokat az eljárási szabályokat, amelyek a vonatkozó jogszabályi rendelkezések érvényre juttatásához szükségesek.

(2) A BVSC az adatokat megfelelő intézkedésekkel védi a véletlen vagy a jogellenes megsemmisítés, elvesztés, megváltoztatás, sérülés, jogosulatlan nyilvánosságra hozatal vagy az azokhoz való jogosulatlan hozzáférés ellen.

(3) Az adatok elvesztése, megsemmisülése, károsodása és az azokhoz való jogosulatlan hozzáférés megelőzése és megakadályozása érdekében szükséges biztonsági intézkedéseket az adatkezelés (adatfeldolgozás) megkezdése előtt az adatkezelés jellemzőihez és a személyes adatok jellegéhez mérten kell meghatározni és azokat – *az adatokat érintő incidens bekövetkezésének hiányában is* – rendszeresen felül kell vizsgálni.

Az adatok és az azokat hordozó eszközök, iratok védelem
16. §

(1) Az Adatkezelő tehát - *a tudomány és a technológia állása és megvalósítási 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, ideértve többek között, adott esetben:

a) személyes adatok álnevesítését, titkosítását;

b) személyes adatok kezelésre használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, sértetlenségét, rendelkezésre állását és ellenálló képességét;

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

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

(2) Az Adatkezelő technikai és szervezeti intézkedések meghozatala vagy azokon való változtatások esetén konzultál az adatvédelmi tisztviselővel és az illetékes IT munkatárs(akk)al. Az Adatkezelő ügyvezetője a konzultációt követően dönt az adott technikai intézkedés bevezetéséről vagy megváltoztatásáról.

(3) Az adatokhoz csak és kizárólag célhoz kötötten, ellenőrzött körülmények között és csak azon személyek férhetnek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.

(4) A folyamatban lévő munkavégzés, feldolgozás alatt álló iratokhoz kizárólag az illetékes kollégák férhetnek hozzá. Személyes Adatokat tartalmazó papír alapú dokumentum kizárólag megfelelő nyilvántartási rend szerint, biztonságosan elzárva tárolható és azok az Adatkezelő székhelyéről kizárólag az ügyvezető engedélyével vihetők ki.

(5) Elektronikus formában tárolt Személyes Adatok, személyes adatokat tartalmazó dokumentumok kizárólag jelszóval védett számítógépeken kezelhetők. Ilyen dokumentumok vagy adatbázisok külső tárhelyre vagy levelezőrendszerre történő továbbítása, illetve más, harmadik személy által potenciálisan hozzáférhető eszközökön való használata, megnyitása kizárólag az ügyvezető engedélyével történhet.

(6) Személyes Adatokat tartalmazó dokumentumokról vagy adatbázisokról készített biztonsági mentések (vagy ilyen dokumentumokat, illetve adatbázisokat is tartalmazó biztonsági mentések) megfelelő titkosítás mellett is kizárólag olyan környezetben tárolhatók, amelyek magas szinten támogatják az

adatkezeléssel kapcsolatos garanciák megtartását, valamint nem jelentenek kockázatot az adatok biztonságára vonatkozóan.

(7) A számítógépekre, laptopokra olyan biztonsági megoldások telepítendők fel, amelyek az informatikai biztonsági igényeket az adatkezelés tárgyával, valamint a kezelés jellegével összefüggésben biztosítják. A konkrét igények az adatvédelmi kockázatelemzés, illetve szükség szerinti hatásvizsgálat eredményei alapján határozandóak meg.

(8) Törekedni kell arra, hogy különleges személyes adatokat tartalmazó elektronikus dokumentumok vagy adatbázisok kizárólag az Adatkezelő saját eszközein kerüljenek tárolásra, illetve kezelésre.

(9) Az adatok eseti alapú törléséhez az ügyvezetőelőzetes jóváhagyását kell beszerezni, ide nem értve azon automatizált adattörléseket, amelyek elektronikus adatbázisokat vagy dokumentumokat érintenek és amelyekkel kapcsolatosan a törlési rendet az ügyvezető már korábban jóváhagyta. A törlési jóváhagyást megelőzően az ügyvezető konzultál az adatvédelmi tisztviselővel.

(10) A személyes adatok törlése során a következők szerint kell eljárni:

a) a személyes adatokat tartalmazó papír alapú dokumentum teljes egészében megsemmisítendő (pl. iratmegsemmisítővel), vagy amennyiben a dokumentum teljes megsemmisítése nem indokolt, úgy a személyes adatok olvashatatlanná tételével biztosítandó a törlés oly módon, hogy a papír alapú dokumentumról készített elektronikus másolat is törlendő, vagy az olvashatatlanná tett változattal váltandó fel;

b) a személyes adatot tartalmazó elektronikus dokumentum teljes egészében törlendő, vagy amennyiben annak teljes törlése nem indokolt, úgy abból a törlendő adatok távolítandók el oly módon, hogy az elektronikus dokumentum személyes adatot tartalmazó változata ne legyen helyreállítható.

(11) Az elektronikus dokumentumokat, adatbázisokat a biztonsági mentésekből is törölni szükséges, vagy olyan biztonsági protokoll alkalmazandó, amely a kérdése file-okat nem állítja vissza és a biztonsági másolatok tartalmához való hozzáférést nem (akár harmadik személyek, mint pl. rendszergazdai feladatokat ellátók irányában sem) teszi lehetővé.

(12) Az adatok törléséért- *amennyiben arra utasítást kapott* – az adatot közvetlenül kezelő munkatárs felelős.

(13) A nem elektronikus kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) tűz-és vagyonvédelem: az irattári kezelésbe vett iratokat jól zárható, száraz, tűz-és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;

b) hozzáférés védelem: a folyamatos, aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá; a személyzeti, valamint bér-és munkaügyi iratokat lemezszekrényben kell őrizni;

c) archiválás: a hivatkozott adatkezelési eljárások irataink archiválását a BVSC-Zugló iratkezelési szabályzatának megfelelően kell elvégezni.

Védelemi módszerek
17. §

(1) Az adatkezelést érintően a BVSC-Zugló a következő védelmi módszereket alkalmazza:

a) *fizikai védelem:* Olyan eszközök alkalmazását jelenti, amelyekkel azok a helyiségek védhetők, ahol számítástechnikai eszközöket használnak, vagy az adatmegőrzés szempontjából fontosok; az adatkezelési rendszer minősítésétől függő védelemben kell részesíteni az adathordozókat is.

b) *jelszavas védelem:* A számítógépek/laptopok használata során a rendszerbe történő belépést jelszó alkalmazásával kötelezően védeni kell; a jelszavakat meghatározott időnként kötelezően meg kell változtatni, mind a munkaállomásokba, mind a hálózati bejelentkezésekre kiterjedően.

c) *algoritmikus védelem:* Matematikai algoritmusok alapján működő védelem, amely egyedi számítógépen és hálózaton is lehetővé teszi a használó azonosítását, a jogosultság ellenőrzését, amely magában foglalhat szoftver módon történő rejtjelezést is; algoritmikus védelmet minden olyan adatkezelési

rendszernek biztosítani kell, amely azonosítható természetes személyre vonatkozó adatot dolgoz fel és hálózat is csak algoritmikus védelem alatt üzemeltethető.

Fizikai védelem
17/1. §

(1) Az informatikai eszközök elhelyezésére szolgáló épületeket, helyiségeket úgy szükséges kialakítani, hogy elegendő biztonságot nyújtsanak az erőszakos behatolás, tűz vagy természeti csapás ellen, különösen,
   a) megfelelő teljesítményű elektromos hálózat kialakításával;
   b) az épület villámhárítóval történő felszerelésével;
   c) vízbetörés elleni védelemmel;
   d) nyílásszárók védelmével (pl., speciális zár, rács, áttörést nehezítő üvegezés)

(2) A számítógépek vagy az adathordozók tárolására szolgáló helyiségeket a legmagasabb tűzveszélyességi osztályba kell besorolni és ennek megfelelően kell a tűzvédelmi előírásokat megállapítani, illetve a helyiségeket tűz-és vagyonvédelmi eszközökkel ellátni.

Jelszavas védelem
17/2. §

(1) Kötelező szempontok a jelszóvédelem alkalmazásnál:
   a) minden felhasználónak egyedi felhasználói névvel és egyedi felhasználói jelszóval kell rendelkeznie;
   b) a jelszavakat meghatározott időszakonként, kötelező jelleggel változtatni kell;
   c) tilos a jelszavak munkatársak közötti átadása.

(2) Az informatikai rendszerekhez tartozó jelszavak megőrzése és helyreállítása ellenőrzött vészhelyzeti ('break-glass') eljárás keretében történik.
A vészhelyzeti hozzáférés kizárólag dokumentált esetben, az ügyvezető engedélyével, naplózott módon alkalmazható. A hozzáférést követően az érintett jelszót haladéktalanul meg kell változtatni, és az eseményt jegyzőkönyvben kell rögzíteni

(3) A BVSC-Zuglótól kilépő kolléga informatikai rendszerekhez való hozzáférési jogosultságát a munkavégzési folyamatok lezárást követően azonnal meg kell szüntetni.

Az informatikai rendszerben tárolt adatok védelméhez kapcsolódó adatbiztonsági intézkedések
17/3. §

(1) A BVSC-Zugló az adatkezelés során a működtetésre érvényes jogosultsággal rendelkező, vírusellenőrző szoftvert működtet.

(2) Az informatikai rendszerben tárolt adatok védelme érdekében a BVSC-Zugló többszintű hozzáférési rendszert és korszerű vírusvédelmi módszereket alkalmaz, valamint a számítógépek/laptopok használata során a rendszerbe történő belépést jelszó alkalmazásával védi.

(3) Számítógépes hálózat esetén különösen a hálózatra történő bejelentkezésnél, a hálózat alapbeállításainak megváltoztatásánál, a felhasználói jogosultságok beállításánál, illetve más hálózatokkal történő kapcsolatteremtésnél jelszóvédelmet kell alkalmazni.

(4) A számítógépes hálózatot az illetéktelen behatolás ellen a kockázatokkal arányos módon, a technológia állására és a megvalósítás költségeire figyelemmel, de a személyes adatok védelmének sérelme nélkül kell védeni.

(5) A fenti bekezdésben foglaltak érvényre juttatása érdekében a munkaállomásokhoz és egyéb informatikai eszközökhöz kizárólag az ügyvezető, illetve a felhasználó munkahelyi vezetője által engedélyezett külső adathordozó csatlakoztatható.

A személyes adatok kezelését végző személyekkel kapcsolatos adatbiztonsági intézkedések
18. §

(1) Az egyes informatikai rendszerekhez a hozzáférési jogosultságot személyre szólóan kell megállapítani. Amennyiben a jogosultság megállapítására alapot adó körülményben változás történik, haladéktalanul intézkedni kell a jogosultság módosításra vagy visszavonására.

(2) A felhasználót az ügyvezető, vagy a munkahelyi vezetője tájékoztatja az adatkezelési hozzáférési jogosultsággal kapcsolatos jogairól, feladatairól és kötelezettségeiről, a vonatkozó szabályok megszegésének következményeiről. A felhasználók feladatait, kötelezettségeit és jogosultságai a munkaköri leírásban/feladat meghatározásban egyértelműen meg kell jeleníteni. A tájékoztatás tényét és tudomásul vételét írásban kell dokumentálni.

IV. Fejezet
Vegyes-és Záró rendelkezések
19. §

(1) Az adatkezeléssel kapcsolatos nyilatkozatokat és utasításokat írásban kell megtenni. Amennyiben az eset összes körülménye sürgős szóbeli közlést indokol, úgy az azzal kapcsolatosan tett nyilatkozatok és utasításoka szóbeli közlésre okot adó körülmény elmúltát követően haladéktalanul írásba foglalandók. A belső működésben az írásbeliség igényének e-mailben történő rögzítése minden esetben megfelelőnek és elégségesnek tekinthető.

(2) Az adatvédelemmel kapcsolatos működés során mindenkor a legteljesebb mértékben törekedni kell rá, hogy a jelen Szabályzatnak, valamint a vonatkozó jogszabályi elvárásoknak való megfelelés igazolható legyen, különösen
   a) az érintettnek az adatkezeléshez történő hozzájárulására;
   b) az érintettek által az egyes adatok törlésére, helyesbítésére, az adatkorlátozás teljesítéséről szóló teljesítés igazolására;
   c) az adatvédelmi incidensekről szóló érintteti értesítésre;

   Ezen fenti esetekben az igazoltathatóságot biztosító írásbeli (vagy annak minősülő) forma sürgős esetekben sem mellőzhető. Az online rendszerekkel kapcsolatos működési háttér úgy alakítandó ki, hogy ezen igények teljesítését biztosítsa, így pl. abban az adatkezeléshez történő, az azonosított érintett által tett hozzájárulás egyértelműen megállapított legyen.

(3) Jelen Szabályzat szükség esetén, de legalább évente az ügyvezető által felülvizsgálandó. A jelen Szabályzat 2026.05.05. napján lép hatályba, ezzel egyidejűleg a BVSC-Zugló korább kiadott, 2019.09.04. napján kelt Adatvédelmi és Adatbiztonsági Szabályzata hatályát veszti.

Budapest, 2026. 05.05.

Szentpáli Gábor
ügyvezető

1142 Budapest, Szőnyi út 2. BVSC – Zugló Adószám: 19808990-2-42

Mellékletek:
1.számú mellékelt: Adattovábbítási Nyilvántartás
2.számú melléklet: Adatfeldolgozók nyilvántartás
3.számú melléklet: Érintett-tájékoztatási nyilvántartás személyes adatokról
4.számú melléklet: Adatvédelmi incidens nyilvántartás

1.számú melléklet

ADATOVÁBBÍTÁSI NYILVÁNTARTÁS .....évre								
Ssz.	Adatigénylő adatai	Adattovábbítás címzettje	Adattovábbítás célja	Adattovábbítás jogalapja	Adattovábbítás időpontja	Érintettek adatai/köre	Továbbított adatok fajtája (köre)	Adatot továbbító adatai

Kitöltési útmutató az Adattovábbítási nyilvántartás vezetéséhez

I. Általános tájékoztató:

1. A nyilvántartást kizárólag elektronikus úton kell vezetni.

2. A nyilvántartásban azokat a személyes adatokat is tartalmazó adattovábbításokat kell rögzíteni, amelyeket külső megkeresés alapján teljesít az Adatkezelő, ideértve a jogszabályban erre felhatalmazott szervek részéről történő megkereséseket is.

3. Személyes adata kizárólag természetes személynek lehet.

4. Ebbe a nyilvántartásba nem kell rögzíteni például:

- **ha az érintett a saját személyes adati vonatkozásában kér tájékoztatást (lsd: Érintett tájékoztatási nyilvántartás – 3. sz. melléklet);**
- **közérdekű, közérdekből nyilvános adat(ok)ról kért tájékoztatást, adattovábbítást.**

5.Törlési határidő: a nyilvántartás adatait az adattovábbítás teljesítését követő naptári év végétől számított 5 évig kell megőrizni.

II. A nyilvántartás egyes oszlopainak kitöltése:

Sorszám: Évente 1-gyel kezdődő, folyamatos sorszámozás. Minden év január 1-jén új nyilvántartást kell kezdeni.

Adatigénylő adatai: Ebben az oszlopban kell feltüntetni az adatszolgáltatást kérő szerv megnevezését, illetve természetes személy esetén a családi és utónevét. Konkrét adatigénylő nélküli, jogszabályon alapuló, bizonyos időszakonként vagy eseményt követően rendszeres vagy automatikus adattovábbítás esetén az az oszlop üres marad.

Adattovábbítás címzettje: Ezen oszlopban azon szerv vagy személy megnevezését kell feltüntetni, amely/aki az adatokat megkapta. Előfordulhat, hogy az adatigénylő és az adattovábbítás címzettje eltér. Ezen oszlopot a jogszabályon alapuló adattovábbítás esetén is ki kell tölteni.

Adattovábbítás célja: Ebben az oszlopban kell feltüntetni, hogy az adatigénylő milyen célra kívánja használni az Adatkezelőtől kért adatokat. Ez jellemzően az adott szerv hatáskörébe tartozó valamilyen eljárás lefolytatás lehet (bírósági eljárás esetében lehet pl. polgári per)

Adattovábbítás jogalapja: Az adattovábbítás jogalapja lehet az érintett hozzájárulása vagy törvényi felhatalmazás. Ezen oszlopban az adattovábbítás törvényi alapjának pontos jogszabályhelyét kell megjelölni.

Az adattovábbítás időpontja: Ebben az oszlopban a továbbítani kért adatok címzett részére történő megküldésének dátumát kell feltüntetni (elektronikus küldés esetén óra, perc megjelöléssel együtt).

Érintettek adatai/köre: Amennyiben az adatigénylés egyetlen személy adataira vonatkozik, úgy itt az adatigénylő családi és utónevét és az azonosításhoz szükséges további egyéb személyazonosító adatát kell feltüntetni (ez lehet lakcím vagy anyja neve). Amennyiben az adatigénylés több személyre vonatkozik, úgy elegendő a csoportképzés szempontjait feltüntetni.

Továbbított adatok fajtája: Ebben az oszlopban azt kell megjelölni, hogy milyen fajtájú, jellegű személyes adatok kerültek továbbításra (pl., név, lakcím...).

Adatatot továbbító adatai: Papír alapú adattovábbítás esetén itt elegendő az adattovábbító irat iktatószámát feltüntetni. Elektronikus adattovábbítás esetén fel kell tüntetni a küldést végző nevét, szervezeti egységét/szakosztályát.

2.számú melléklet

ADATFELDOLGOZÓK NYILVÁNTARTÁS		
1.	adatfeldolgozó megnevezése	
2.	címe	
3.	telefonszáma	
4.	kapcsolattartója (adatvédelmi tisztviselője)	
5.	(adatfeldolgozói) szerződés iktatószáma	
6.	adatfeldolgozási tevékenység	
7.	GDPR 32. cikk (1) bekezdésében rögzített technikai és szervezési intézkedések leírása	

3.számú melléklet

ÉRINTETT-TÁJÉKOZTATÁSI NYILVÁNTARTÁS A SZEMÉLYES ADATOKRÓL .....évre				
Sorszám	Adatigénylő adatai	Tájékoztatási kérelem beérkezésének időpontja	Tájékoztatási kérelem eredménye	Tájékoztatás iktatószáma

Kitöltési útmutató
az Érintett-tájékoztatási nyilvántartás vezetéséhez

I. Általános tájékoztató:

1. A nyilvántartást kizárólag elektronikus úton kell vezetni.

2. Minden év január 1-jén új nyilvántartást kell kezdeni.

3. A nyilvántartás az érintettek olyan adatigényléseinek nyilvántartására szolgál, amikor saját személyes adataik tekintetében kérnek tájékoztatást.

4. Nem ebben a nyilvántartásban kell rögzíteni: amikor a törvényben erre felhatalmazott szervek (pl. rendőrség, bíróság) kérnek személyes adatot is tartalmazó tájékoztatást. Ezeket az adatszolgáltatásokat az Adattovábbítási nyilvántartásban (1. sz. melléklelt) kell rögzíteni.

5.Törlési határidő: A nyilvántartásban rögzített adatokat az Adatkezelő a szükséges ideig, de legfeljebb 3 (három) év időtartamig őrzi meg az érintetti joggyakorlás elszámoltatható teljesítésének igazolása céljából, ezt követően törli vagy anonimizálja.

II. A nyilvántartás egyes oszlopainak kitöltése:

Sorszám: Évente 1-gyel kezdődő, folyamatos sorszámozás. Minden év január 1-jén új nyilvántartást kell kezdeni.

Adatigénylő adatai: Ebben az oszlopban kell feltüntetni az adatigénylő azonosításához szükséges adatokat. Ez a neve mellett lehet bármely más személyazonosító adat, amely rendelkezésre áll, és alkalmas arra, hogy az alapján később az Adatkezelő azonosítani tudja az igénylőt. A név mellett így szerepelhet például lakcím, anyja neve, születési hely és idő, személyi igazolvány szám stb., ami alkalmas az adatigénylő azonosítására. Jellemzően a név mellett további egy személyes adat már alkalmas ezen cél elérésére, így szükségtelen és tilos többet rögzíteni a nyilvántartásban.

Az érintetti kérelmek teljesítése főszabály szerint díjmentes. Amennyiben az érintett kérelme **nyilvánvalóan megalapozatlan vagy túlzó**, különösen ismétlődő jellege miatt, az Adatkezelő – *a GDPR 12. cikk (5) bekezdése alapján* – jogosult **észszerű mértékű díjat** felszámítani, figyelembe véve a teljesítéssel járó adminisztratív költségeket, vagy a kérelem teljesítését megtagadni. A megalapozatlanság vagy túlzó jelleg bizonyítása az Adatkezelőt terheli.

A tájékoztatás kérelem beérkezésének időpontja: Ezen oszlopban kell feltüntetni az iratkezelést végző szervezeti egység által a kérelemre felvitt érkezési időpontot.

A tájékoztatási kérelem eredménye: Ebben az oszlopban kell feltüntetni a kérelem elbírálásának eredményét: „Teljesítve" vagy „Elutasítva". Amennyiben az érintett a kapott tájékoztatással nem ért egyet és módosítja a kérését, az új tájékoztatási folyamatnak minősül.

Tájékoztatás iktatószáma: Az adatigénylőnek küldött válasz iktatószáma.

4.számú melléklet

Adatvédelmi incidens nyilvántartás							
Ssz	Incidens bekövetkezésének időpontja és helye	Incidens megnevezése, tényei	Érintettek köre, száma	Érintett személyes adatok	Incidens hatása	Incidens orvoslására tett intézkedések	Egyéb adatok