Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ adatkezelési-, adatvédelmi és titoktartási szabályzata

PREAMBULUM

Jelen Szabályzat a természetes személyek személyes adatainak a Társaság által történő kezelésének (adatkezelési tevékenységének) szabályait tartalmazza az Európai Parlament és a Tanács (EU) 2016. április 27-i 2016/679 számú Rendeletének - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról -, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben foglaltaknak való megfelelés céljából.

Az adatvédelemmel kapcsolatban **az alábbi jogszabályok** alkalmazandóak:

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (általános adatvédelmi rendelet; ismertebb nevén GDPR)

A rendelet szövegét itt olvashatja:
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)

Az Infotv. szövegét itt olvashatja:

- https://net.jogtar.hu/jogszabaly?docid=A1100112.TV

A Szabályzat megállapítása és módosítása és a helyben szokásos módon való közzététele az intézményvezető hatáskörébe tartozik.

Székesfehérvár, 2019. szeptember 05.

KRÍZISKEZELŐ KÖZPONT * SZÉKESFEHÉRVÁR *

Zsabka Attila vezető
Székesfehérvár Megyei Jogú Város
Önkormányzata Kríziskezelő Központ

Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ adatkezelési, adatvédelmi és titoktartási szabályzata

I. Adatkezelő adatai

Név: **Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ (továbbiakban: Kríziskezelő Központ)**
Statisztikai törzsszám: 15364957-8790-322-07
Költségvetési törzsszám:364955
Székhely: 8000 Székesfehérvár, Sörház tér 3.
Levélcíme: 8000 Székesfehérvár, Sörház tér 3.
E-mail címe: krizis@fehervarkrizis.hu
Telefonszám: +36 22-503-433
Képviseli: Zsabka Attila intézményvezető
Honlap: www.fehervarkrizis.hu

II. A Szabályzat célja

A Szabályzat célja, hogy a Kríziskezelő Központ a rá vonatkozó -mindenkor hatályos- jogszabályokkal, EU az Európai Parlament és Tanács 2016/679. számú Általános Adatvédelmi Rendeletével (továbbiakban: Rendelet) összhangban, azok előírásai szerint végezze a természetes személyekre vonatkozó adatkezelését, adatfeldolgozását, vezesse nyilvántartásait, végezze statisztikai adatgyűjtési, információszolgáltatási tevékenységét; kezelje a birtokában levő személyes adatokat. A Kríziskezelő Központ tevékenysége során teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó valamennyi jogszabályi előírásnak.

III. Általános rendelkezések

1. Az adatkezelési, adatvédelmi és titoktartási szabályzat (a továbbiakban: Szabályzat) előírásai Kríziskezelő Központ egészére, minden szervezeti egységére, az adminisztratív és technikai ügyintéző szervezetének minden munkatársára, valamint az ott tevékenykedő, alapító okirat szerinti alaptevékenységében is közreműködő közalkalmazottakra is kötelezők. Fokozott felelősséggel tartozik a Kríziskezelő Központ eljáró ügyintéző szervezete, illetve az eljáró felelős személy.

2. A Kríziskezelő Központ jogi személyként, önállóan működő költségvetési szerv. Pénzügyi, gazdálkodási és számviteli feladatait Székesfehérvár Megyei Jogú Város Önkormányzata Humán Szolgáltató Intézet (8000 Székesfehérvár, Ady E. utca 8.) látja el. Irányító és fenntartó szerve: Székesfehérvár, MJV Önkormányzat Közgyűlése (8000 Székesfehérvár, Városház tér 1.), amely, mint fenntartó látja el az intézmény irányítását, jóváhagyja és ellenőrzi a költségvetést és annak végrehajtását. Székesfehérvár MJV Önkormányzat Közgyűlése nyilvános pályázati eljárás útján határozott időre szóló megbízás útján nevezi ki az intézményvezetőt.

a.) A költségvetési szerv működésének rendjét, a vezetők közötti feladatmegosztást, valamint a belső és külső jogviszonyokra vonatkozó rendelkezéseket az Kríziskezelő Központ Szervezeti és Működési Szabályzata határozza meg.

b.) A Kríziskezelő Központ alaptevékenysége: közfeladat ellátása; nevezetesen: szociális alapszolgáltatás és szakosított ellátás, valamint gyermekjóléti alapellátás biztosítása. A főtevékenység államháztartási szakágazati besorolása: 879060 „Egyéb bentlakásos ellátás".

- illetékességi területe: Székesfehérvár Megyei Jogú Város közigazgatási területe

- Az alaptevékenységek felsorolása és a feladatok leírása az alábbi:

  - Népkonyha és szociális konyha ellátás keretében napi egyszeri meleg étel biztosítása.
  - Hajléktalanok számára éjjeli menedék, nappali melegedő, utcai szociális munka és átmeneti szállás biztosítása.
  - Volt állami gondozott fiatalok részére átmeneti szállás biztosítása.
  - Családok átmeneti otthonának működtetése.
  - Speciális szolgáltatások keretében hajléktalanok részére egészségügyi és mentálhigiénés ellátás, pszichiátriai tanácsadás és egészségnevelési tevékenység.
  - Hajléktalanok számára innovatív szolgáltatásokat nyújtó nappali szolgáltató centrum.
  - Utógondozás a kiléptető lakásokban élők számára.
  - Szakmai képzések (felnőttképzés keretében) tréningek szervezése szociális ágazatban dolgozók, önkéntesek és ellátottak részére.
  - Nappali melegedő éjszakai nyitva tartással, éjjeli menedékhelynek minősülő időszakos férőhely működtetése.

- A Kríziskezelő Központ alaptevékenységének kormányzati funkció szerinti megjelölése:

kormányzati funkciószám	funkció megnevezése
013350	Az önkormányzati vagyonnal való gazdálkodással kapcsolatos feladatok
104012	Gyermekek átmeneti ellátása
106010	Lakóingatlan szociális célú bérbeadása, üzemeltetése
107013	Hajléktalanok átmeneti ellátása
107015	Hajléktalanok nappali ellátása
107016	Utcai szociális munka
107051	Szociális étkeztetés

- A Kríziskezelő Központ által működtetett www.fehervarkrizis.hu honlapon megtalálható a felhasználók részére az Adatvédelmi tájékoztató, mely kiterjed a böngészők használatával járó „sütik" esetében alkalmazandó eljárásra is. A leggyakrabban használt internetes böngészők (Chrome, Firefox, stb.) többsége alapbeállításként elfogadja és engedélyezi a sütik letöltését és használatát, azonban lehetőség van arra, hogy a felhasználó a böngésző beállításainak módosításával ezeket visszautasítsa vagy letiltsa, illetve a már a számítógépen lévő eltárolt sütiket is tudja törölni. A sütik használatáról az egyes böngészők „súgó" menüpontja nyújt bővebb tájékoztatást.
  A hozzájárulást igénylő sütikről – amennyiben az adatkezelés már az oldal felkeresésével megkezdődik – a Kríziskezelő Központ az első látogatás megkezdésekor tájékoztatja a felhasználókat és kéri is valamennyi felhasználó hozzájárulását.

Kríziskezelő Központ nem alkalmaz és nem is engedélyez olyan sütiket, amelyek segítségével harmadik személyek a felhasználó hozzájárulása nélkül adatot gyűjthetnek. A sütik elfogadása nem kötelező, Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ azonban nem vállal azért felelősséget, ha sütik engedélyezése hiányában a weblap esetleg nem az elvárt módon működik.

IV. Jogszabályi alap (a felsorolt jogszabályok mindenkor hatályos állapota):

- 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; Magyarország Alaptörvénye;
- 1990. évi LXV. törvény a helyi önkormányzatokról
- 2013. évi V. törvény – a Polgári Törvénykönyvről (Ptk.);
- 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Info tv.);
- 2003. évi XXIV. törvény – a közpénzek felhasználásával, a köztulajdon használatának nyilvánosságával, átláthatóbbá tételével és ellenőrzésének bővítésével összefüggő egyes törvények módosításáról;
- az egészségügyi adatokról és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény;
- a gyámhatóságok, területi gyermekvédelmi szakszolgálatok, a gyermekjóléti szolgálatok és a személyes gondoskodást nyújtó szervek és személyek által kezelt személyes adatokról szóló 235/1997. évi (XII.17.) Korm. rendelet;
- a szociális, gyermekjóléti és gyermekvédelmi szolgáltatók, intézmények és hálózatok hatósági nyilvántartásáról és ellenőrzéséről szóló 369/2013. (X.24.) Korm. rendelet;
- a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény;
- a szociális igazgatásról és a szociális ellátásokról szóló 1993. évi III. törvény;
- 2012. évi I. törvény – a munka törvénykönyvéről (Mt.);
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról (Kjt)
- A gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény
- 2005. évi XC. törvény – az elektronikus információszabadságról;
- Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ alapító okirata; és Szervezeti és Működési Szabályzata
- Az állami vagyonról szóló 2007. évi CVI. törvény;
- Az államháztartásról szóló 2011. évi CXCV. törvény;
- 1/2000. (I. 7.) SzCsM rendelet a személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről;
- 15/1998. (IV. 30.) NM rendelet a személyes gondoskodást nyújtó gyermekjóléti, gyermekvédelmi intézmények, valamint személyek szakmai feladatairól és működésük feltételeiről;
- 8/2000 (VIII.4,(SzCsM rendelet a személyes gondoskodást végző személyek adatainak nyilvántartásáról
- egyéb jogszabályok, kormányrendeletek, melyek az egyes tevékenységekhez kapcsolódnak (a folyamatok adatkezelésének leírásánál felsorolásra kerülnek).

V. A Szabályzat hatálya:

- A Kríziskezelő Központ Adatvédelmi és Adatbiztonsági Szabályzata (a továbbiakban: Szabályzat) előírásai a Kríziskezelő Központ egészére, minden szervezeti egységére, az

ügyintéző szervezetének minden munkatársára kötelező, valamint a vele szerződéses vagy egyéb kapcsolatban álló személyes adatkezelést vagy adatfeldolgozást végző személyekre kötelező. Fokozott felelősséggel a Kríziskezelő Központ eljáró ügyintéző szervezete, illetve az eljáró felelős személy.

- Az Intézmény szervezeti egységei az alábbiak:
  - Családok Átmeneti Otthona; (8000 Székesfehérvár, Palotai u. 51/A.);
  - Éjjeli menedékhely; (8000 Székesfehérvár, Sörház tér 3.);
  - Átmeneti Szálló (8000 Székesfehérvár, Sörház tér 3.);
  - Átmeneti Szálló (8000 Székesfehérvár, Kikindai út 8.);
  - Átmeneti Szálló (8000 Székesfehérvár, Széchenyi út 60.);
  - Nappali melegedő; (8000 Székesfehérvár, Sörház tér 3.);
  - Nappali melegedő, Nappali szolgáltató Centrum (8000 Székesfehérvár, Sörház tér 7.);
  - Szociális konyha, népkonyha; (8000 Székesfehérvár, Sörház tér 3.);
  - 1. sz. Utcai szociális szolgálat; (8000 Székesfehérvár, Sörház tér 3.);
  - 2. sz. Utcai szociális szolgálat. (8000 Székesfehérvár, Sörház tér 7.);
- A Szabályzat személyi hatálya kiterjed továbbá az Adatkezelő által igénybe vett adatfeldolgozók felé irányuló adatáramlásra.
- A Szabályzat tárgyi hatálya kiterjed az Adatkezelő szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére.

VI. A Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ által közalkalmazotti jogviszonyban foglalkoztatottak személyes adatainak kezelése

- A Kríziskezelő Központ alkalmazásában álló személyek személyi iratainak és adatainak kezelését, a Rendelet, az Infó tv., illetve a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény szerint kell ellátni.
- Személyi irat minden – bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett – adathordozó, amely a közalkalmazotti jogviszony létesítésekor, fennállása alatt, megszűnésekor, valamint azt követően keletkezik, és a természetes személy alkalmazott személyével összefüggésben adatot, megállapítást tartalmaz.
- A foglalkoztatottakról csak a közalkalmazotti jogviszonyukkal összefüggő adat tárolható. Az érintettől csak olyan nyilatkozat, vagy adatlap kitöltése kérhető, amely személyiségi jogait nem sérti.
- A közalkalmazotti jogviszonnyal összefüggésben Kríziskezelő Központ alkalmazásában álló személyekről nyilvántartásokat vezet, így különösen, de nem teljes körűen a jogszabály által előírt személyi anyagok, egészségbiztosítási ellátások nyilvántartása, magán-nyugdíjpénztári nyilvántartás, fizetési jegyzékek, járulék-nyilvántartások, számfejtési anyagok, bérfeladások, bérátutalások, statisztikai jelentések, személyi jövedelemadó nyilvántartások, OEP elszámolások, adó- és járulékbevallások, kiküldetési rendelvények nyilvántartása, hivatali célra saját gépkocsi használat nyilvántartása.
- A személyi iratokat és a személyi adatokat védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A a Kríziskezelő Központ alkalmazásában álló személyekre vonatkozó személyi iratokat, egyéb papír alapú nyilvántartásokat a hivatalos helyiségben, zárható szekrényben kell tárolni, megakadályozandó, hogy illetéktelenek hozzáférjenek. Az elektronikusan tárolt adatok esetén az adatvédelemről a Informatikai Biztonsági Szabályzat előírásai szerint kell gondoskodni. A Kríziskezelő Központ az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy

megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. Továbbá olyan technikai, szervezési és szervezeti intézkedésekkel gondoskodik az adatok biztonságáról, ami az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő védelmi szintet nyújt.

- A személyi iratokat az illetékes ügyintéző a feladatvégzéshez szükséges mértékben kezelheti. Az iratokba az intézmény fenntartójának bérszámfejtéssel foglalkozó munkatársai (adatfeldolgozási megállapodás alapján), illetve a foglalkoztatói jogkör gyakorlójának ügyintéző szervezetében tevékenykedő illetékes munkatársaknak is joga van betekinteni.
- A közalkalmazotti jogviszonnyal kapcsolatos személyi irat, dokumentum kizárólag személyesen, vagy meghatalmazott útján vehető át, illetve tértivevényes ajánlott küldeményként az érintett lakcímére postázható.
- A Kríziskezelő Központ alkalmazásában álló személyekre kiírt álláspályázatokra beküldött jelentkezésekhez mellékelni kell a pályázóknak a személyes adatok kezeléséhez a pályázati anyaggal együtt megadott személyes hozzájárulását.
    a) A pályázat elbírálása után az eredménytelen pályázók személyes adatait tartalmazó adathordozókat a pályázónak – kérésére – 90 napon belül igazolható módon vissza kell küldeni, vagy a pályázónak a személyes adatai további pályázatok során történő felhasználására vonatkozó hozzájárulása hiányában meg kell semmisíteni. A megsemmisítésről (törlésről) jegyzőkönyvet kell felvenni.
    b) Kivételt képez ez alól: a pályázati finanszírozással, vagy állami támogatásból betöltött munkakörök esetében benyújtott álláspályázat. Ez esetben a Kríziskezelő Központnak igazolnia kell, milyen módon töltötte be az állásokat, ezért a beadott pályázatokra, a meghirdetésekre is szükség van nyilvántartási célból, hogy az illetékes minisztériumi szaktárca, illetve a Magyar Államkincstár illetékes szerve, illetve az Állami Számvevőszék az ellenőrzési eljárásban ezen adatokról meggyőződhessen. (Ilyen esetekben a Kríziskezelő Központ tájékoztatja a pályázót arról, hogy a pályázati anyaga általa megőrzésre kerül és annak végleges rendelkezésre bocsátását – visszaszármaztatás nélkül - tudomásul kell vennie.)
- A Kríziskezelő Központhoz bármilyen formában álláskeresési céllal (hirdetésre, pályázatra) a pályázó (érintett) által eljuttatott önéletrajzokban lévő személyes adatok kezeléséhez az érintett hozzájárulását vélelmezni kell. Amennyiben a pályázó kifejezetten nem járul hozzá a további adatkezeléshez, alkalmazás hiányában a személyes adatokat törölni kell és a törlésről jegyzőkönyvet kell felvenni. Felhívás nélkül megküldött önéletrajzokat a Kríziskezelő Központ nem őriz meg, azokat jegyzőkönyv felvétele mellett megsemmisíti.

VII. Az adatkezelési és adatvédelmi feladatok ellátásának szervezeti rendje

A Kríziskezelő Központ adminisztratív ügyintéző szervezetének állományából, az intézményvezető megbízásából kerül kijelölésre az adatkezelési és adatvédelmi feladatok ellátásáért felelős személy, aki tevékenységéért közvetlenül a Központ intézményvezetőjének felelős.

A Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ ügyintéző szervezetéből erre jogosult adatkezelési és adatvédelmi felelős:

a) végzi a partneri, intézménybe bármelyik jogcímen szolgáltatást igénybe vevők, valamint a foglalkoztatotti nyilvántartások működtetésével kapcsolatos feladatokat,
b) ellátja az adatbázisok kezeléséből és védelméből eredő feladatokat,
c) köteles az adatminőség (pontosság, naprakész állapot) folyamatos fejlesztésére,
d) ellátja a jogszabályokban és az egyéb szabályzatokban meghatározott feladatokat.

Nem tárgya az adatvédelmi nyilvántartásnak az az adatkezelés, amely kizárólag statisztikai célt szolgáló olyan adatokat tartalmaz, amelyek - a statisztikai törvényben foglaltak szerint - az adatok és az érintettek közötti kapcsolat megállapítását véglegesen kizárják.

Krízískezelő Központ, mint adatkezelő gondoskodik az adatok biztonságáról; megteszi azokat a technikai adatvédelmi és szervezeti intézkedéseket és kialakítja azokat a belső eljárási szabályokat (hozzáférési jogosultsági rendszer stb.), amelyek a biztonságos adatkezelés helyi sajátosságok szerinti feltételeinek biztosítására alkalmasak.

VIII. Adat és titokvédelem, titoktartási kötelezettség

A Krízískezelő Központ partneri nyilvántartása, az általa közfoglalkoztatásban alkalmazottak, a rehabilitációs foglalkozásokon, vagy szociális ellátásokban részesülő személyek, emellett az intézménybe járó, szakmáz biztosító képzéseken résztvevők, illetve rendezvényekre jelentkezők személyes adatai tekintetében sajátos, a titokvédelmi szabályokra figyelemmel kezelt elemei a kulturális és szociális kapcsolatok alakulása, továbbá az érintettek érdekütközései kapcsán szerzett – kulturális, szociális és etikai jellegű - értesülések, amelyekre kiterjed a titoktartási kötelezettség.

A Krízískezelő Központ nyilvántartásában szereplő adatok kizárólag a partneri nyilvántartáshoz, valamint a szociális ellátásban részesülő, valamint a közfoglalkoztatott személyek és felnőttoktatásban részesülő nagykorú személyek és diákok, valamint a szüleik, nevelőik és a családi kapcsolataik szükségszerű megismeréséhez kapcsolódó feladatok teljesítéseként használhatók fel, oly módon, hogy az adat célhoz kötött felhasználása ellenőrizhető legyen. A partneri és a működés körben vezetett nyilvántartással kapcsolatos szervezési feladatok teljesítése során az üzleti titkok védelmére és a személyes adatok védelmére vonatkozó jogszabályoknak megfelelően kell eljárni.

A Fejér Megyei Művelődési Központ ügyintéző szervezetének munkavállalói és a pedagógusok - a titoktartási nyilatkozatuk szerinti körben és feltételek mellett - kötelesek az ügykörükben tudomásukra jutott üzleti titkokat és személyes jellegű szociális és más érzékeny információkat titokként megőrizni.

IX. Értelmező rendelkezések: GDPR szerint

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;

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. **„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;

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

5. **„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;

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

7. **„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 2016.5.4. L 119/33 Az Európai Unió Hivatalos Lapja HU 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;

8. **„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;

9. **„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;

10. **„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;

11. **„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;

12. **„személyes adatok határokon átnyúló adatkezelése":**

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

X. A Kríziskezelő Központ által végzett adatkezelések fajtái

— a) a közalkalmazottak, ill. a szerződéses kapcsolatban együttműködő megbízottak/egyéb partnerek személyes adatait, az intézmény szolgáltatásait igénybe vevő személyek, illetve közfoglalkoztatottak, valamint a szakmát adó képzéseken résztvevők, és a rehabilitációs, és szociális céllal vagy szakkörökön, kulturális műhelyek szolgáltatásaiban részesülők, valamint gyermek- és fiatalkorúak esetén szüleik, nevelőik személyes adatait;
— b) ügyfelek, partnerek, együttműködő oktatási intézmények és közintézmények képviseletében eljáró természetes személyek személyes adatait,
— c) a Családok Átmeneti Otthona; Éjjeli menedékhely; (8000 Székesfehérvár, Sörház tér 3.); Átmeneti Szálló (8000 Székesfehérvár, Sörház tér 3.); Átmeneti Szálló (8000 Székesfehérvár, Kikindai út 8.); Átmeneti Szálló (8000 Székesfehérvár, Széchenyi út 60.); Nappali melegedő, (8000 Székesfehérvár, Sörház tér 3.) Nappali Melegedő, Nappali szolgáltató Centrum (8000 Székesfehérvár, Sörház tér 7.); Szociális konyha, népkonyha; (8000 Székesfehérvár Sörház tér 3.); 1. sz Utcai szociális szolgálat; (8000 Székesfehérvár, Sörház tér 3.) 2. sz. Utcai szociális szolgálat (8000 Székesfehérvár Sörház tér 7.) feladat ellátási helyein, illetve az egyes szervezeti egységek adminisztratív ügyintézési helyén, nevezetesen: a szervezeti egységek épületeinek közvetlen külső környezetében a bejárat megfigyelése céljából a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény rendelkezései alapján elektronikus megfigyelő rendszert működtet, melynek alkalmazása adatkezelésnek minősül.

XI. Az adatkezelés jogalapja:

A Kríziskezelő Központ, mint adatkezelő adatkezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) **az érintett hozzájárulását** adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
A hozzájárulásnak mindig önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Kríziskezelő Központ, mint adatkezelő a hozzájárulást valamennyi adatkezelési célhoz egyenként szerzi be, egyúttal felhívja az érintett figyelmét azon jogára, hogy a hozzájárulást bármikor egyszerű módon visszavonhatja.

b) 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;
Kríziskezelő Központ a foglalkoztatási jogviszony (közalkalmazotti jogviszony) alapjául szolgáló kinevezési okirat létrejöttét megelőzően, illetőleg a létrejött jogviszony kapcsán is – az adattakarékosság elve mellett – kezel személyes adatot, azonban minden esetben írásos hozzájáruló nyilatkozat alapján és a társadalombiztosítási – nyilvántartási és bejelentési kötelezettség teljesítéséhez szükséges mértékben.

c) az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség teljesítéséhez** szükséges;
Kríziskezelő Központ a bérszámfejtés, illetőleg az adó- és járulék fizetés, közfoglalkoztatással együtt járó bevallási kötelezettségek teljesítése, valamint a Magyar Államkincstár által az intézmény szolgáltatásait igénybe vevők után (esetlegesen) járó normatíva folyósítása, illetve ezen adatszolgáltatási kötelezettsége érdekében kezel személyes adatokat, ezen kötelezettségek teljesítéséhez szükséges mértékben.

d) az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges;
Kríziskezelő Központ a szociálisan nehéz helyzetbe került, szenvedélybetegségben szenvedő, munkavégzésre képtelen, vagy a munkahelyét elveszített és a társadalomba beilleszkedési zavarokkal küzdő, valamit az önmaga gondozására egyéb okból képtelen személyek emberközpontú segítése és szociális és mentális egészségügyi ellátásainak rendelkezésre állása kapcsán az ellátásban részesülők létfontosságú érdekeinek védelmében kezeli a személyes adatokat.

e) az adatkezelés **közérdekű** vagy az adatkezelőre ruházott **közhatalmi jogosítvány gyakorlásának keretében** végzett feladat végrehajtásához szükséges;
Kríziskezelő Központ közérdekű adatkezelést végez a jogszabály, vagy Székesfehérvár Megyei Jogú Város Önkormányzat rendeletei által ráruházott közhatalmi jogosítvány gyakorlása keretében végzett feladatok végrehajtásához szükséges mértékben. Ilyenek például a szociális ellátásokhoz kapcsolódó adatkezelések, valamint az önkormányzat szociális és egészségügyi, valamint a közfoglalkoztatási feladatainak helyi szintű ellátásához kapcsolódó adatkezelések.

f) 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.
Kríziskezelő Központ az egyes szervezeti egységeinek hivatalos helyiségeiben a bejáratnál, ill. az információ szolgálaton, az ügyféltérben található elektronikus megfigyelő rendszer működtetését Családok Átmeneti Otthona; Éjjeli menedékhely; (8000 Székesfehérvár, Sörház tér 3.); Átmeneti Szálló (8000 Székesfehérvár, Sörház tér 3.); Átmeneti Szálló (8000 Székesfehérvár, Kikindai út 8.); Átmeneti Szálló (8000 Székesfehérvár, Széchenyi út 60.); Nappali melegedő, (8000 Székesfehérvár, Sörház tér 3.) Nappali Melegedő, Nappali szolgáltató Centrum (8000 Székesfehérvár, Sörház tér 7.); Szociális konyha, népkonyha; (8000 Székesfehérvár Sörház tér 3.); 1. sz Utcai szociális szolgálat; (8000 Székesfehérvár, Sörház tér 3.) 2. sz. Utcai szociális szolgálat (8000 Székesfehérvár Sörház tér 7.) feladat ellátási helyein, illetve az egyes szervezeti egységek adminisztratív ügyintézési helyén ezen a jogalapon végzi, hiszen itt a személyes adatkezelésének alapjául szolgáló érdek a személy- és vagyonvédelem, valamint az

emberi méltósághoz fűződő alkotmányos alapjog és a különösen védendő egészségügyi diszkréció.

XII. Érintettek jogainak tiszteletben tartása, illetve biztosítása

Kríziskezelő Központ, mint adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy biztosítsa az érintett jogait. Adatkezelő az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtja,. A tájékoztatást oly módon kell megadni, amilyen módon azt az Érintett kérte.

1. Tájékoztatáshoz való jog

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az adatkezelőnek és képviselőjének neve, elérhetősége;
b) a személyes adatok kezelésének célja;
c) a személyes adatok kezelésének jogalapja (amennyiben ez az adatkezelő vagy harmadik fél jogos érdeke, azt konkrétan megjelölni);
d) személyes adat címzettje;
e) harmadik országba történő adattovábbítással kapcsolatos információk, garanciák;
f) a személyes adatok tárolásának időtartama;
g) az érintett azon jogáról, hogy kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az adathordozhatósághoz való jogáról;
h) hozzájáruláson alapuló adatkezelés esetén arról, hogy a hozzájárulás bármely időpontban visszavonható (a visszavonás nem érinti a visszavonás előtt a hozzájárulás alapján végzett adatkezelés jogszerűségét);
i) a felügyeleti hatósághoz fordulás joga;
j) az érintett köteles-e a személyes adatokat megadni, az adatszolgáltatás elmaradásának következményei.

A tájékoztatás mellőzhető, ha az érintett már rendelkezik az információkkal.

Amennyiben az adatkezelő a személyes adatokat nem az érintettől szerezte meg, a fentieken felül tájékoztatja az érintettet az átvett személyes adatokról, valamint az adatok forrásáról.

Ebben az esetben a tájékoztatás időpontja: az adat megszerzésétől számított
- max. 30 nap,
- kapcsolattartási célú adatkezelésénél az első kapcsolatfelvétel,
- ha más címzettel is közlik az adatokat, legkésőbb az első közlés.

A tájékoztatás mellőzhető az alábbi esetekben:
- ha az érintett már rendelkezik az információkkal,
- a szóban információk rendelkezésre bocsátása lehetetlen, vagy aránytalanul nagy erőfeszítéssel jár,
- jogszabály által elrendelt adatkezelés esetén,

- jogszabályban előírt titoktartási kötelezettség alapján.

2. *Az érintett hozzáférési joga*

Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- személyes adatok másolata,
- adatkezelés célja,
- adatok kategóriái,
- adatátvételnél a forrásra vonatkozó információk,
- címzettek,
- harmadik országba történő adattovábbítással kapcsolatos információk, garanciák,
- tárolás időtartama,
- az érintett jogai,
- a felügyeleti hatósághoz fordulás joga.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat elektronikusan kell rendelkezésére bocsátani, kivéve, ha az érintett másként kéri.

3. *A helyesbítéshez való jog*

Az érintett jogosult arra, hogy kérésére az adatkezelő a rá vonatkozó pontatlan adatokat indokolatlan késedelem nélkül helyesbítse, kiegészítse.
Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ a valóságnak meg nem felelő adatot a tudomásszerzését követő 15 nap alatt helyesbíteni köteles. A helyesbítésről - kérelemre - értesíteni kell az érintetteket.

4. *A törléshez való jog*

- Az érintett bármikor jogosult a rögzített adatainak törlését kérni az adatkezelőtől, akinek indokolatlan késedelem nélkül meg kell tennie a szükséges lépéseket ennek érdekében.
- A törlés nem vonatkozik azokra az adatokra, amelyeket az adatkezelő jogszabály alapján kezel.

5. *Az elfeledtetéshez való jog*

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 az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését..

A törléshez való jog és az elfeledtetéshez való jog szabályai nem alkalmazandók, amennyiben az adatkezelés szükséges:

- a véleménynyilvánítás szabadságához,
- jogi kötelezettség teljesítéséhez,

- közhatalmi jogosítvány gyakorlásához,
- közérdekű archiválás, tudományos és történelmi kutatási célból,
- jogi igények érvényesítéséhez.

6. *Az adatkezelés korlátozásához való jog*

Az adatkezelő az érintett kérelmére korlátozza az adatkezelést, ha:

- az érintett vitatja a személyes adatok pontosságát (arra az időtartamra, amely lehetővé teszik, hogy az adatkezelő ellenőrizze az adatok pontosságát),
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését és ehelyett kéri az adatkezelés korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények érvényesítéséhez,
- az érintett tiltakozott az adatkezelés ellen (az adatkezelő korlátozza az adatkezelést, amíg vizsgálódik, hogy jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben).

Ha az adatkezelés korlátozás alá esik, az ilyen 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 fontos közérdekből lehet kezelni.
Az adatkezelő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Az adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, törlésről vagy korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

7. *Az adathordozhatósághoz való jog*

Az érintett jogosult arra, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátott, ha az adatkezelés hozzájáruláson, vagy szerződésen alapul.

Az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

8. *A tiltakozáshoz való jog*

Az érintett tiltakozhat a személyes adatai kezelése ellen a következő jogalapok esetén:

- közérdekű adatkezelés, illetve az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés,
- adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelés.

Az érintett tiltakozhat továbbá a személyes adatai kezelése ellen a közvetlen üzletszerzési cél esetén.

Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények érvényesítéséhez kapcsolódnak.

A tiltakozáshoz való jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

XIII. Jogorvoslat

Az érintett a jogainak megsértése esetén

- élhet az érintetti jogaival az adatkezelő felé az alábbi elérhetőségek valamelyikén:
  Név: Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ
  Székhely: 8000 Székesfehérvár, Sörház tér 3.
  Levélcíme: 8000 Székesfehérvár, Sörház tér 3.
  E-mail címe: krizis@fehervarkrizis.hu
  Telefonszám: +36 22-503-433
  Honlap: www.fehervarkrizis.hu

- bírósághoz fordulhat (Székesfehérvári Törvényszék, 8000 Székesfehérvár, Dózsa György út 1., 8000 Székesfehérvár, Zichy liget 10., www.birosag.hu/torvenyszekek/szekesfehervari-torvenyszek),

- valamint vizsgálatot kezdeményezhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál :
  (Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/C
  Levelezési cím: 1530 Budapest, Postafiók: 5.
  Telefon: +36 -1-391-1400
  Fax: +36-1-391-1410
  E-mail: ügyfelszolgalat@naih.hu

XIV. A Kríziskezelő Központ által az adatkezelés körében az alábbi szabályoknak felel meg képfelvétel készítése, felhasználása (nyilvánosságra hozatala) esetén

A Polgári Törvénykönyvről szóló 2013. évi V. Törvény 2:43. § külön kiemeli a képmáshoz való jog védelmét: a személyiségi jogok megsértését jelenti különösen a képmáshoz és a hangfelvételhez való jog megsértése. Kríziskezelő Központ az adatkezelése során elkerüli mindazon jogsértő magatartásokat, illetve tartózkodik mindazon jogellenes mulasztástól, amelyeket a Ptk. a képmáshoz és a hangfelvételhez való jog megsértése esetén szankcionál, vagyis amelyekhez joghátrány fűződik.

A hatályos jogszabályok alapján egy személy arca, képmása személyes adatnak, a fényképfelvétel készítése és felhasználása pedig adatkezelésnek minősül, amihez – külön törvényi felhatalmazás hiányában – az érintett hozzájárulása szükséges. Alapvetően olyan

esetben van szükség hozzájárulásra, ha a képen szereplő személy felismerhető, különösen, ha a felvétel az illető egyéni ábrázolására alkalmas.
Nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és az elkészített felvétel felhasználásához tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén, továbbá rendezvényekről, táj- és utcarészletekről készült felvételek készítéséhez és felhasználásához, amikor tehát az ábrázolás módja nem egyéni, hanem a felvétel összhatásában örökíti meg a nyilvánosság előtt lezajlott eseményeket. Ide tartoznak különösen az olyan eseményeken készült felvételek, ahol megszokott a felvételek készítése, például rendezvényeken, tréningeken. A külön hozzájárulás nélkül készíthető fényképfelvételek hozzájárulás nélkül csak olyan körben használhatóak fel, amelyet az elkészítés körülményei indokolnak, például az esemény megörökítése, tájékoztatás céljából.

16. életévét be nem töltött kiskorúakról készített képek közzététele a szülők hozzájárulásával minősülnek jogszerűnek.

Felhasználás (nyilvánosságra hozatal) a Kríziskezelő Központ esetében:
a) a képfelvételnek a Fehérvári Médiacentrum által (Fehérvár TV, Vörösmarty Rádió, kapcsolódó online felületeken, valamint a Fehérvári Médiacentrum kiadásában és ingyenes terjesztésében megjelenő időszaki kiadvány: „Fehérvári Program" magazinban való megjelenése.
b) Elektronikus felületen a nyilvánosságra hozatal esetleges helye: www.fehervarkrizis.hu

Mindezen felhasználás és nyilvánosságra hozatal csak abban a körben értendő, ha a Kríziskezelő Központ egyes alkalomszerű jótékony és szociális céllal gyűjtést, ételosztás, ünnepséget, vagy a társadalomba újra beilleszkedést segítő képzést, ételosztást, téli időszakban melegedési eseményeket szervez, illetve informatív céllal az intézmény szervezeti egységeinek elérhetősége, nyitvatartási rendje, vagy a rendjének megváltozása az információs cél.

XV. Kiskorúakra vonatkozó külön szabályok

A gyermekek személyes adatainak kezeléséhez szükséges a gyermek, illetve szülő vagy törvényes képviselőjének felhatalmazása:

- 16 év alatti gyermek esetében a szülő vagy a törvényes képviselő,
- 16 év felett pedig már kizárólag a gyermek jogosult a hozzájárulás megadására.

Különélő vagy elvált szülők esetében csak az a szülő adhat érvényes adatkezelési nyilatkozatot, aki a szülői felügyeleti jogok gyakorlására jogosult – az adatkezelőnek azonban nem feladata, hogy ezt a kérdést mélységében vizsgálja, el kell fogadnia az erről szóló szülői tájékoztatást azzal, hogy vita esetén az ellentmondást az erre jogosult hatóságnak (gyámhatóság, bíróság) kell megoldania.
Az általános felhatalmazás (hozzájáruló nyilatkozat) azonban nem azt jelenti, hogy az egyes fotózásokról előzetesen ne kellene tájékoztatást adni és amennyiben valamelyik fénykép feltétele kifejezetten zavarja az érintett gyermeket vagy szülőt, törlési (vagy szöveg esetén helyesbítési) kérelmének haladéktalanul eleget kell tenni.

XVI. Adatbiztonsági előírások

A személyes adatokat tartalmazó dokumentumok kezelése során az adatkezelő a (Kríziskezelő

Központ) címére érkező postai, illetve ügyfélfogadási időben személyesen leadott küldemények érkeztetési és kézbesítési utasítását kell alkalmazni minden olyan kérdésben, amelyre jelen szabályzat nem tartalmaz előírást.

Kríziskezelő Központ ügyfél levelezései

Amennyiben a Kríziskezelő Központ szolgáltatásainak igénybevétele során az ellátottaknak, a hozzátartozóiknak, illetve egyéb partnereinek, illetve ügyfeleinek kérdése, információ igénye van a szolgáltatás kapcsán az ügyfélszolgálattal telefonon és e-mailen kapcsolatba léphet. Adatkezelő a beérkezett leveleket, a küldő nevével és e-mail címével, valamint más, önként megadott személyes adatával együtt, az ügy elintézésétől számított legfeljebb öt év elteltével törli.

Egyéb adatkezelések

Az itt fel nem sorolt adatkezelésekről az adat felvételekor ad a Kríziskezelő Központ tájékoztatást.

A személyes adatok tárolásának módja, az adatkezelés biztonsága

Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ által működtetett www.fehervarkrizis.hu címen elérhető honlap számítástechnikai rendszerei és más adatmegőrzési helyei az adatkezelő székhelyén, találhatók meg.

Kríziskezelő Központ a személyes adatok kezeléséhez a szolgáltatásai nyújtása során alkalmazott informatikai eszközöket úgy választja meg és üzemelteti, hogy a kezelt adat:

a) az arra feljogosítottak számára hozzáférhető (rendelkezésre állás);
b) hitelessége és hitelesítése biztosított (adatkezelés hitelessége);
c) változatlansága igazolható (adatintegritás);
d) a jogosulatlan hozzáférés ellen védett (adat bizalmassága) legyen.

XVII. Szervezeten belüli feladatok

Az adatkezelő gondoskodik az adatok biztonságáról; megteszi azokat a technikai adatvédelmi és szervezeti intézkedéseket és kialakítja azokat a belső eljárási szabályokat (hozzáférési jogosultsági rendszer stb.), amelyek a biztonságos adatkezelés helyi sajátosságok szerinti feltételeinek biztosítására alkalmasak.

Kríziskezelő Központ – fenntartója közbenjárásával - olyan műszaki, szervezési és szervezeti intézkedésekkel gondoskodik az adatkezelés biztonságának védelméről, amely az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő védelmi szintet nyújt.

Kríziskezelő Központ az adatkezelés során megőrzi
a) a titkosságot: megvédi az információt, hogy csak az férhessen hozzá, aki erre jogosult;
b) a sértetlenséget: megvédi az információnak és a feldolgozás módszerének a pontosságát és teljességét;

c) a rendelkezésre állást: gondoskodik arról, hogy amikor a jogosult használónak szüksége van rá, valóban hozzá tudjon férni a kívánt információhoz, és rendelkezésre álljanak az ezzel kapcsolatos eszközök.

Kríziskezelő Központ és partnereinek informatikai rendszere és hálózata egyaránt védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá a számítógépvírusok, a számítógépes betörések és a szolgálatmegtagadásra vezető támadások ellen. Kríziskezelő Központ a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.

Kríziskezelő Központ – fenntartóján keresztül - rendelkezik olyan szabályzattal, amely a használt szoftverek és rendszerek etikus felhasználását szolgálja. A napi munkavégzés során folyamatosan újabb technológiák és szoftverek kerülnek alkalmazásra. Kríziskezelő Központ az informatikai biztonsági szabályzata biztosítja az informatikai rendszerek használata során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát.

Az adatkezelő belső képzést szervez közalkamazottai részére az adatvédelemről, valamint erősíti a munkavállalók adatvédelmi tudatosságát.

XVIII. Adatvédelmi incidens kezelése

Kríziskezelő Központ alkalmazásában álló közalkalmazott, aki az adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést észlel, azt köteles az adatkezelő képviseletében eljáró személlyel haladéktalanul közölni.

Az adatkezelő képviseletében eljáró személy a bejelentést megvizsgálja, a foglalkoztatottól (bejelentőtől) további adatszolgáltatást kérhet, amelyet a közalkalmazott haladéktalanul köteles teljesíteni.

A vizsgálat alapján az adatkezelő képviseletében eljáró személy megteszi a szükséges lépéseket az adatvédelmi incidens elhárítása érdekében, amennyiben ez lehetséges. A kockázatokat figyelembe véve adatkezelő gondoskodik a további szükséges intézkedések meghozataláról, melyről tájékoztatja az adatok kezelését vagy feldolgozását végző szakterületet.
Az adatvédelmi incidensről az adatkezelő nyilvántartást vezet.

Az adatkezelő azonnal, de legkésőbb 72 órán belül bejelenti a hatóság részére, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintettet nem kell tájékoztatni az adatvédelmi incidensről a következő esetekben:

— az adatkezelő megfelelő védelmi intézkedéseket hajtott végre, amelyek az adatok megismerésére nem jogosult személyek számára megismerhetetlenné, vagy értelmezhetetlenné teszik az adatokat;

— az adatkezelő az adatvédelmi incidenst követően olyan intézkedéseket tesz, amelyek biztosítják, hogy a kockázat a továbbiakban valószínűsíthetően ne valósuljon meg;
— a tájékoztatás aránytalan erőfeszítést tenne szükségessé, ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni.
—

XIX. Hatályba lépés

Jelen módosított szabályzat a kihirdetés napjától – 2019. szeptember 05. napjától - hatályos.

Jelen szabályzat kihirdetéséről saját hatáskörben intézkedik a Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ intézményvezetője (igazgatója) a fenntartó intézményi szervezetrendszer Közgyűlésének egyidejű tájékoztatása mellett.

Székesfehérvár, 2019. szeptember 05.

KRÍZISKEZELŐ KÖZPONT

Zsabka Attila
intézményvezető
Székesfehérvár Megyei Jogú Város Önkormányzata
Kríziskezelő Központ

KRÍZISKEZELŐ KÖZPONT

ADATVÉDELMI TÁJÉKOZTATÓ
- hatályos 2018. május 25-től -

1. Bevezetés

1.1. Az alábbiakban szeretnénk tájékoztatni Önt az **Kríziskezelő Központ** általi adatkezeléssel kapcsolatos tudnivalókról.

1.2. Jelen adatvédelmi tájékoztató lényeges tájékoztatást tartalmaz az Ön személyes adatainak kezelésére vonatkozóan. **Személyes adatai megadásával Ön elfogadja a jelen adatvédelmi tájékoztatóban foglalt feltételeket.** Kérjük, hogy az adatvédelmi tájékoztatót rendszeresen olvassa el, hiszen annak változásai automatikusan alkalmazandóak az Ön által megadott személyes adatok kezelésére, abban az esetben is, ha a személyes adatai megadásakor még egy korábbi adatvédelmi tájékoztató volt hatályban. Az adatvédelmi tájékoztató módosítását honlapunkon közzétesszük, illetve egyéb módon is értesítjük Önt, attól függően, hogy mely forrásból áll rendelkezésünkre az Ön adata. Kérjük, hogy külön figyelemmel olvassa el a jelen adatvédelmi tájékoztató félkövérrel kiemelt rendelkezéseit, mert azok lényeges rendelkezéseket tartalmazhatnak az Ön személyes adatai kezelésére vonatkozóan.

1.3. **Honlap: www.fehervarkrizis.hu (továbbiakban: „Honlap")**

Amennyiben az adatkezelés honlapunkon valósul meg, úgy a Honlap használatával Ön elfogadja a jelen adatvédelmi tájékoztatóban foglalt feltételeket, függetlenül attól, hogy regisztrál-e a Honlapon. Ha az adatvédelmi tájékoztatóban foglaltakat nem fogadja el, kérjük, ne használja a Honlapot.

1.4. **Jelen adatvédelmi tájékoztató kizárólag a természetes személy Érintettek személyes adataira vonatkozik**, tekintettel arra, hogy jogi személyek, illetve jogi személyeknek nem minősülő egyéb szervezetek adatai nem minősülnek személyes adatoknak.

1.5. Az adatvédelemmel kapcsolatban **az alábbi jogszabályok** alkalmazandóak:

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (általános adatvédelmi rendelet; ismertebb nevén GDPR)
  A rendelet szövegét itt olvashatja: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) Az Infotv. szövegét itt olvashatja:

https://net.jogtar.hu/jogszabaly?docid=A1100112.TV

2. Az adatkezelő személye

Név:	**SZÉKESFEHÉRVÁR MEGYEI JOGÚ VÁROS ÖNKORMÁNYZATAT KRÍZISKEZELŐ KÖZPONT**
E-mail:	krizis@fehervarkrizis.hu
Telefon:	06 22 501793
Székhely:	8000 Székesfehérvár Sörház tér 3
Törzskönyvi szám:	364955
Adószám:	15364957-1-07

3. Alapvető információk

3.1. A Kríziskezelő Központ (a továbbiakban: Kríziskezelő Központ) általi adatkezelés jogalapja a szerződésen törvényes kötelezettségen, jogos érdeken, vagy az Érintett önkéntes hozzájárulásán alapulhat. **Az Érintett a hozzájáruláson alapuló adatkezelés esetén jogosult a hozzájárulását bármikor visszavonni, amely azonban nem érinti a visszavonás előtti adatkezelés jogszerűségét.** A hozzájárulás tényének igazolására vonatkozó adatokat a Kríziskezelő Központ mindaddig megőrzi, amíg azt a hozzájárulás bizonyíthatósága vagy a Kríziskezelő Központ más jogos érdeke szükségessé teszi.

3.2. Az Érintett **felelős** az általa megadott személyes adatok valóságáért és pontosságáért. A Kríziskezelő Központ a közölt személyes adatok valódiságát nem ellenőrzi. **Az Kríziskezelő Központ nem felelős** az Érintett által megadott téves vagy valótlan adatok kezeléséért, sem az Érintett által közölt téves vagy valótlan adatközlés folytán akár az Érintettet, akár harmadik személyt érő károkért.

3.3. **A hozzájárulás megadása**

a) **Honlap esetén** a Honlap használatával, a Honlapon történő regisztrációval vagy a személyes adatok egyéb módon történő megadásával,

b) **minden más esetben** az Érintett általi egyéb igazolható módon (papíralapon – írásban, elektronikus levélben, faxon, kép- és/vagy hangfelvétellel stb.) történik.

3.4. **A 16. életévét betöltött kiskorú** adatkezeléshez történő hozzájárulását tartalmazó jognyilatkozatának érvényességéhez (azaz a regisztrációhoz, vagy személyes adatai más módon történő megadásához) törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges. Az ilyen Érintett az adatfelvétel módjától függően megadhatja az adatkezeléshez történő hozzájárulását.

3.5. Az Érintett hozzájárulását megadottnak kell tekinteni az Érintett közszereplése során általa közölt vagy nyilvánosságra hozatalra általa átadott személyes adatok tekintetében.

3.6. A Kríziskezelő Központ a rendelkezésére bocsátott személyes adatokat – eltérő jogszabályi rendelkezés hiányában – csak a jelen tájékoztatóban ismertetett célok érdekében, a cél

megvalósulásához szükséges mértékben és ideig kezeli.

3.7. A Kríziskezelő Központ adatfeldolgozóként profilalkotást végez.

4. AZ EGYES ADATKEZELÉSEK

a) HONLAP MŰKÖDTETÉSE ÉS HASZNÁLATA, REGISZTRÁCIÓ, REGISZTRÁCIÓN KERESZTÜL IGÉNYBE VEHETŐ SZOLTÁLTATÁSOK

Érintettek	AKríziskezelő Központ Honlapját látogató, illetve ott regisztráló személyek, egyes tartalmakhoz hozzászóló személyek (komment)
Adatkezelés célja	A Honlapon elérhető szolgáltatások működtetése, regisztráció létrehozása, felhasználó azonosítása, hozzászólások moderálása
Kezelt adatok köre	Név*, e-mail cím*, jelszó*, egyéb személyes adat, amelyeket az Érintett a Honlap használata során – a Honlap jellegétől függően – megad (hozzászólás stb.)
Adatkezelés jogalapja	Hozzájárulás
Adatfeldolgozó	Tárhelyszolgáltató: ..... Kft
Az adatkezelés időtartama	A regisztráció vagy az Érintett által megadott tartalom Érintett általi törléséig, illetve hozzájárulás visszavonásáig. Amennyiben az
Egyéb	A *-gal megjelölt adatok megadása szükségesek a regisztrációhoz. Amennyiben nem adja meg az adatokat, nem tud regisztrálni. A Honlapon való böngészés közben gyűjtött adatokkal összefüggésben ld. a süti tájékoztatónkat

b) HÍRLEVÉLKÜLDÉS

Érintettek	A honlap hírlevelére feliratkozó személyek
Adatkezelés célja	A Honlapon megjelenő tematikus összefoglaló tájékoztató e-mail küldése
Kezelt adatok köre	Név*, e-mail cím*,
Adatkezelés jogalapja	Hozzájárulás
Adatfeldolgozó	Tárhelyszolgáltató:
Az adatkezelés időtartama	hozzájárulás visszavonásáig
Egyéb	A *-gal megjelölt adatok megadása szükséges a szolgáltatás igénybevételéhez. Amennyiben nem adja meg ezen adatokat, Az Kríziskezelő Központ nem tud hírleveleket küldeni.

c) A KRÍZISKEZELŐ KÖZPONT SZOLGÁLTATÁSAIVAL KAPCSOLATOS TÁJÉKOZTATÁS

Érintettek	A Kríziskezelő Központ szolgáltatásait igénybe vevő személyek
Adatkezelés célja	A Kríziskezelő Központ által nyújtott szolgáltatásokkal, a szerződés teljesítésével összefüggő kapcsolattartás
Kezelt adatok köre	név, cím, telefonszám, e-mail cím (szükség szerint)
Adatkezelés jogalapja	szerződés teljesítése
Adatfeldolgozó	
Az adatkezelés időtartama	A szolgáltatás igénybevételének idejéig
Egyéb	Ez az adatkezelés magában foglalja a szolgáltatás nyújtásával kapcsolatos elengedhetetlen információkat tartalmazó e-mailes, , vagy írásbeli tájékoztatás adását. A Kríziskezelő Központ által (ún.

	rendszerüzenetek és tájékoztatók), így ezen tájékoztatásokról nem lehet leiratkozni, illetve ezeket nem lehet visszautasítani.

d) EGYÉB KOMMUNIKÁCIÓ, PANASZKEZELÉS

Érintettek	A Kríziskezelő Központ-nél kapcsolatot felvevő, vagy panaszt tevő személy
Adatkezelés célja	Érintett általi kapcsolatfelvétel esetén a kapcsolatfelvétel céljától függő adatkezelési cél (pl. bejövő e-mailek megválaszolása, panasz érdemi elintézése és tájékoztatás a megtett lépésekről stb.)
Kezelt adatok köre	Név, e-mail cím, telefonszám, lakcím (attól függően, hogy az Érintett mely adatokat közli, vagy milyen csatornán keresztül zajlik a kommunikáció)
Adatkezelés jogalapja	Jogos érdek
Adatfeldolgozó	****
Az adatkezelés időtartama	A kommunikáció, illetve panasz jellegétől függően, de minden esetben legalább a panasz elintézését követő 3 évig.
Egyéb	Jogos érdek megnevezése: ügyfelekkel történő kommunikációban foglaltak utólagos bizonyíthatósága, panaszügyintézés, minőségbiztosítás.

e) IGÉNYÉRVÉNYESÍTÉS, JOGVITÁK, HATÓSÁGI ELJÁRÁSOK

Érintettek	Azon személyek, akikkel szemben a Kríziskezelő Központ igényt érvényesít (pl. a Kríziskezelő Központ. felszólító levelet küld ki vagy jogi eljárást indít követelés megfizetése iránt), vagy akik a Kríziskezelő Központ-vel szemben igényt érvényesítenek Hatósági eljárással érintett ügy kapcsán kezelt személyes adatok Érintettjei
Adatkezelés célja	A Kríziskezelő Központ követeléseinek érvényesítése, behajtása, a Kríziskezelő Központ-vel szembeni igényérvényesítés esetén A Kríziskezelő Központ álláspontjának bizonyítása, hatósági megkeresések, felhívások teljesítése
Kezelt adatok köre	Név, lakcím, telefonszám, követeléssel kapcsolatos egyéb információk
Adatkezelés jogalapja	Jogos érdek Jogi kötelezettség teljesítése
Adatfeldolgozó	****
Az adatkezelés időtartama	Az igényérvényesítés vagy eljárás jogerős lezárultát követő 8 év
Címzett	Szükség szerint jogi képviselő Hatóság
Egyéb	Jogos érdek megnevezése: követelésbehajtás, igényérvényesítés, jogvédelem

f) ÜZLETI PARTNEREK KAPCSOLATTARTÓI

Érintettek	Üzleti partnerek kapcsolattartói
Adatkezelés célja	A szerződéses kapcsolatok során történő gördülékeny, akadálymentes kommunikáció biztosítása a kapcsolattartók révén, ehhez szükséges, hogy a kapcsolattartók adatait Az Kríziskezelő Központ ismerje

Kezelt adatok köre	Név, e-mail cím, telefonszám, a kapcsolódó cégnév és esetlegesen beosztás
Adatkezelés jogalapja	Jogos érdek
Adatfeldolgozó	****
Az adatkezelés időtartama	Az alapul szolgáló szerződés hatálya, illetve amennyiben a személyes adat a szerződésben vagy az azzal összefüggésben kiállított számlán szerepel, akkor a számviteli bizonylatokra vonatkozó szabályok értelmében ezen okiratokat a Kríziskezelő Központ 8 évig tárolja
Egyéb	Jogos érdek megnevezése: Harmadik személyekkel kötött szerződések teljesítése során szükséges kommunikáció biztosítása

5. Adatfeldolgozás

5.1. Adatfeldolgozónak minősül az a természetes vagy jogi személy vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel. Az adatfeldolgozás az adatokkal kapcsolatos döntési jogosultságot nem jelent: az adatfeldolgozó az adatkezelő adatkezelési döntéseit hajtja végre.

5.2. A Kríziskezelő Központ az egyes adatkezelésekkel összefüggő részletes tájékoztatás kapcsán ismertette az adatfeldolgozók személyét és feladataikat (ld. fenti 4. pont). Tekintettel arra, hogy jelen tájékoztatás nem alkalmas valamennyi adatfeldolgozó megnevezésére, ezért összefoglaló ismertetjük a Kríziskezelő Központ által igénybe vett adatfeldolgozók által nyújtott szolgáltatásokat:

a) tárhelyüzemeltetés
b) informatikai támogató jellegű szolgáltatás
c) hírlevélküldő és tömeges e-mail küldő szolgáltatás
d) fényképkészítés
e) Székesfehérvár Megyei Jogú Város Humán Szolgáltató Intézet (bérszámfejtés, munkaügy)

5.3. Egyedi esetekben a Kríziskezelő Központ igénybe vehet más adatfeldolgozó(ka)t is, amely(ek) személyéről az adott részvételi feltételekben ad tájékoztatást.

5.4. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Kríziskezelő Központ rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat Az Kríziskezelő Központ rendelkezései szerint köteles tárolni és megőrizni.

6. Adattovábbítás

6.1. Az egyes adatkezelések ismertetésénél a Kríziskezelő Központ felsorolta az adattovábbítások címzettjeit, illetve azok kategóriáit.

6.2. A Kríziskezelő Központ továbbá jogos érdeke alapján (pl. adminisztratív célokból egységes, nyilvántartások létrehozása) továbbíthatja a személyes adatokat a fenntartójához: Székesfehérvár Megyei Jogú Város Önkormányzata és szervei.

6.3. Az Érintett személyes adatainak továbbítása lehetséges olyan harmadik felek részére, akik jogszabály Ilyen esetben az Kríziskezelő Központ által az Érintettre vonatkozóan tárolt személyes adatok is átadásra kerülhetnek, a tranzakció által indokolt mértékben. **Az ilyen adattovábbításhoz az Érintett előzetes hozzájárulására nincs szükség,** A Kríziskezelő Központ azonban arról az Érintettet előzetesen tájékoztatja azzal, hogy **ha az Érintett az**

adattovábbítás ellen tiltakozik, adatainak továbbítására nem kerül sor.

6.4. Az Érintett automatizált adatkezelés esetén a hozzájárulása vagy a szerződés teljesítése alapján – a Kríziskezelő Központ számára általa megadottan – kezelt adataira vonatkozóan kérheti, hogy a Kríziskezelő Központ, ha ez technikailag megoldható, tagolt, széles körben használt, géppel olvasható formátumban A Kríziskezelő Központ-én kívüli adatkezelőnek továbbítsa; a címzett adatkezelőnek az adattovábbítás teljesítéséhez szükséges adatait az Érintett közli. AKríziskezelő Központ az ilyen adattovábbítási kérés teljesíthetőségének akadályáról az Érintettet észszerű időn belül értesíti.

6.5. A Kríziskezelő Központ jogosult és kötelesek minden olyan rendelkezésére álló és általa szabályszerűen tárolt személyes adatot az illetékes hatóságoknak továbbítani, amely továbbítására jogszabály vagy jogerős hatósági kötelezés kötelezi. Ilyen adattovábbítás, valamint az ebből származó következmények miatt a Kríziskezelő Központ nem tehető felelőssé.

7. Adattovábbítás harmadik országba

7.1. Harmadik országban (értsd nem EGT tagállamban) székhellyel rendelkező adatkezelő részére a Kríziskezelő Központ nem továbbít személyes adatot.

7.2. Adott esetben az Kríziskezelő Központ harmadik országban székhellyel rendelkező adatfeldolgozót vehet igénybe. Az Kríziskezelő Központ például bizonyos esetekben tömeges hírlevélküldés céljából igénybe veszi a MailChimp szolgáltatóját, a The Rocket Science Group, LLC-t (675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308). A Mailchimp 2016-ban elfogadott ún. Privacy Shield hatálya alatt működik, amely lehetővé teszi a jogszerű adattovábbítást az Európai Unió és az Amerikai Egyesült Államok adatkezelői és adatfeldolgozói között.

8. Adatbiztonság

8.1. A Kríziskezelő Központ az adatok biztonságáról a vonatkozó előírásoknak megfelelően gondoskodik.

8.2. AzKríziskezelő Központ az adatbiztonságra vonatkozó intézkedések körében megteszi különösen azokat a technikai és szervezési intézkedéseket, és kialakítja azon eljárási szabályokat, amelyek biztosítják, hogy a kezelt adatok védettek legyenek a jogosulatlan hozzáféréssel, megváltoztatással, továbbítással, nyilvánosságra hozatallal, törléssel, megsemmisítéssel, véletlen megsemmisüléssel, vagy sérüléssel szemben, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

8.3. A Kríziskezelő Központ az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintetbe veszi a technika mindenkori fejlettségét. Több lehetséges adatkezelési megoldás közül A Kríziskezelő Központ azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Kríziskezelő Központ-nek. A Kríziskezelő Központ ezen követelményeket az adatfeldolgozók irányában is érvényesíti.

8.4. AKríziskezelő Központ kötelezi magát arra, hogy minden olyan harmadik felet, akik részére az adatokat esetlegesen továbbítja vagy átadja, felhívja a fenti vállalások betartására. A Kríziskezelő Központ általi jogszerű adattovábbítás esetén ugyanakkor a Kríziskezelő Központ nem vállal felelősséget a címzett által okozott károkért.

8.5. A Kríziskezelő Központ valamennyi munkatársa, munkaviszonya vagy más jogviszonya alapján köteles az adatkezelésre, valamint adatbiztonságra vonatkozó fenti elvek

betartására.

9. **Érintett jogai a személyes adatainak kezelésével kapcsolatban**

9.1. Az Érintett bármikor, a jelen tájékoztatóban megjelölt elérhetőségeken **tájékoztatást kérhet** az őt érintő adatkezelésről, kérelmezheti a rá vonatkozó adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen. Az Érintettet megilleti továbbá az adathordozhatóság joga.

9.2. AKríziskezelő Központ indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül **tájékoztatja** az Érintettet az alábbiak szerinti **kérelem nyomán hozott intézkedésekről**. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról a Kríziskezelő Központ - a késedelem okainak megjelölésével - a kérelem kézhezvételétől számított egy hónapon belül tájékoztatás ad. Ha a kérelem elektronikus úton érkezett, a tájékoztatás lehetőség szerint szintén elektronikus úton történik, kivéve, ha az Érintett azt másként kéri. Ha úgy ítéljük meg, hogy nem kell intézkedéseket tennünk az Érintett kérelme nyomán, úgy késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatni fogjuk az Érintettet az intézkedés elmaradásának okairól, valamint arról, hogy panasztételi lehetőséggel élhet az adatvédelmi hatóságnál, továbbá élhet bírósági jogorvoslati jogával is.

9.3. A kérelmek teljesítése ingyenes, ha azonban a kérelem egyértelműen megalapozatlan vagy - különösen ismétlődő jellege miatt - túlzó, a Kríziskezelő Központ, figyelemmel a kérelem folytán felmerülő adminisztratív költségekre, észszerű díjat számíthat fel, vagy megtagadhatja a kérelem teljesítését.

9.4. Ha a kérelmet benyújtó Érintett kilétével kapcsolatban megalapozott kétség merül föl, további, a személyazonosságának megerősítéséhez szükséges információk nyújtása kérhető.

9.5. Az Érintett kérelmére aKríziskezelő Központ tájékoztatást ad arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, az Érintett jogosult arra, hogy AKríziskezelő Központ által kezelt rá vonatkozó személyes adatokhoz, illetve az adatkezelés céljára, az érintett adatok kategóriáira, azon címzettekre vagy címzettek kategóriáira, akikkel a személyes adatokat közölték vagy közölni fogják, az adatkezelés tervezett időtartamára vagy az időtartam meghatározásának szempontjaira, valamint az adatok forrására vonatkozó információkhoz hozzáférést kapjon.

9.6. Kérelemre a Kríziskezelő Központ az adatkezelés tárgyát képező személyes adatok másolatát az Érintett rendelkezésére bocsátja. Az Érintett által kért további másolatokért az adminisztratív költségeken alapuló, észszerű mértékű díj számítható fel. Ha az Érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha azt az Érintett másként kéri.

9.7. Az Érintett **kérheti a pontatlan adatok helyesbítését**, és joga van arra is, hogy kérje a hiányos adatai kiegészítését.

9.8. Az Érintett **kérheti, hogy a Kríziskezelő Központ a személyes adatokat törölje**, ha

a) azokra már nincs szükség abból a célból, amelyre figyelemmel az adatkezelés történt;

b) ha az Érintett a hozzájárulását visszavonja, és az adatkezelésnek nincs más

jogalapja;

c) annak a 9.13. pont szerinti feltételei fennállnak;
d) az adatkezelés jogellenes;
e) azokat a Kríziskezelő Központ-re- vonatkozó jogi kötelezettség teljesítéséhez törölni kell,
f) az Érintett 16. életévét be nem töltött kiskorú.

9.9. A Kríziskezelő Központ **fenti kérelemre az adatokat törli, kivéve, ha** a további adatkezelés

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása,
b) az azt előíró, a Kríziskezelő Központ-re vonatkozó jogi kötelezettség teljesítése,
c) jogi igények előterjesztése, érvényesítése, illetve védelme

céljából szükséges.

9.10. Az Érintett kérésére **a Kríziskezelő Központ korlátozza az adatkezelést**, ha

a) az Érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi az adatok pontosságának ellenőrzését,
b) bár az adatkezelés jogellenes, de az Érintett ellenzi a törlést, és ehelyett a korlátozást kéri,
c) a Kríziskezelő Központ-nek már nincs szüksége az adatok kezelésére, de az Érintett azt jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez igényli,
d) az Érintett a 9.13. pont szerint tiltakozott az adatkezelés ellen, amely esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben.

9.11. Ha az adatkezelés az előzőek szerint korlátozás alá esik, az ilyen személyes adatok – a tárolás kivételével – csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből kezelhető. A korlátozás feloldásáról az Kríziskezelő Központ az azt kérő Érintettet előzetesen tájékoztatja.

9.12. A helyesbítésről, a törlésről vagy korlátozásról a Kríziskezelő Központ az Érintettet, továbbá mindazokat értesíti, akiknek korábban az adatot továbbította. Az értesítést a Kríziskezelő Központ mellőzi, ha ez lehetetlen, vagy nagy erőfeszítést igényel. Ha a Kríziskezelő Központ 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 az Érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

9.13. Az Érintett **tiltakozhat** személyes adatának kezelése ellen,

a) ha az jogos érdek alapján történik; ebben az esetben az adatkezelés nem folytatható, kivéve, ha az Érintett érdekeivel, jogaival és szabadságaival szemben elsőbbséget élvező kényszerítő erejű jogos okok, vagy olyan okok indokolják, amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak,
b) ha az közvetlen üzletszerzés érdekében történik vagy ahhoz kapcsolódik; ilyen

esetben e célból az adatkezelés a továbbiakban nem folytatható.

A 9.2-9.4. pontok a tiltakozás esetére is irányadók.

9.14. **Az adathordozhatóság joga** alapján az Érintett egyrészt kérheti, hogy a Kríziskezelő Központtól, ha ez technikailag megoldható, tagolt, széles körben használt, géppel olvasható formátumban a kezelt személyes adatait megkapja és azt bármely adatkezelőnek ő maga továbbítsa, másrészt kérheti a 6.4. pont szerinti adattovábbítást a Kríziskezelő Központtól.

9.15. Ha a Kríziskezelő Központ az Érintett fentiek szerinti kérelmét nem teljesíti, legkésőbb a kérelem beérkezésétől számított 30 napon belül tájékoztatja annak okáról.

9.16. Amennyiben az Érintett meglátása szerint a személyes adataival kapcsolatos jogai sérültek, úgy kérjük, hogy panaszát jelezze a Kríziskezelő Központ felé a lent megadott elérhetőségek egyikén.

9.17. A Kríziskezelő Központ értesítésétől függetlenül a hatósághoz is fordulhat. Ha így dönt, azt az alábbi elérhetőségeken tehet bejelentést a hatóságnál:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Postafiók: 5.
Telefon: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

9.18. Ha jogellenes adatkezelést tapasztal, polgári pert is kezdeményezhet. A per elbírálása a törvényszék hatáskörébe tartozik. A per az Ön lakóhelye szerinti törvényszék előtt is megindítható (az alábbi hivatkozáson találja törvényszékek felsorolását és elérhetőségét: http://birosag.hu/torvenyszekek).

10. **Az adatvédelmi tájékoztató változásai** a Honlapon kerülnek közzétételre. Mindig az aktuálisan hatályos adatvédelmi tájékoztató alkalmazandó a személyes adatok kezelésére, abban az esetben is, ha az Érintett regisztrációjakor, vagy személyes adatai egyéb módon történő megadásakor még egy korábbi adatvédelmi tájékoztató volt hatályban.

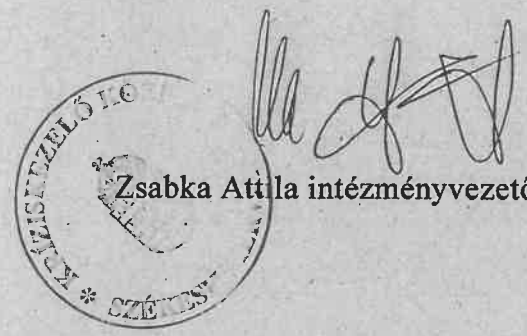
11. **Kapcsolat**

11.1. Amennyiben kérdése, észrevétele vagy kérése van jelen adatvédelmi tájékoztatóval kapcsolatban, panaszt tenne, vagy a 10. pontban rögzített jogait szeretné gyakorolni, kérjük, vegye fel velünk a kapcsolatot a következő elérhetőségeken:

Név:	**Kríziskezelő Központ**
E-mail:	krizis@fehervarkrizis.hu
Telefon:	06 22 501793
Székhely:	8000 Székesfehérvár Sörház tér 3
Cégjegyzékszám:	364955
Adószám:	15364957-1-07

12. Hatály

Jelen adatvédelmi tájékoztató 2018. május 25-étől alkalmazandó és visszavonásig érvényes.



Zsabka Attila intézményvezető

KAMERA SZABÁLYZAT AZ

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE ALAPJÁN

Tájékoztatás a Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ adminisztratív ügyintézésének helyén (8000 Székesfehérvár, Sörház tér 3.) valamint a Központ egyes szervezeti egységeiben a bejáratnál üzemeltetett térfigyelőrendszerhez (kamerához) fűződő adatkezelésről

1. **A kezelt adatok köre**

A Krízis kezelő Központ, mint adatkezelő adminisztratív ügyintézési helyén és az egyes szervezeti egységeken *Családok Átmeneti Otthona; Éjjeli menedékhely; Átmeneti Szálló (8000 Székesfehérvár, Sörház tér 3.); Átmeneti Szálló (8000 Székesfehérvár, Kikindai út 8.); Átmeneti Szálló (8000 Székesfehérvár, Széchenyi út 60.); Nappali melegedő, Nappali szolgáltató Centrum (8000 Székesfehérvár, Sörház tér 7.); Szociális konyha, népkonyha; 1. sz Utcai szociális szolgálat; 2. sz. Utcai szociális szolgálat feladat ellátási helyein a bejáratnál elhelyezett kameraállásokkal* a mozgás megfigyelésére elektronikus térfigyelőrendszert (továbbiakban: kamerákat) alkalmaz, mely használat során személyes adatok (képfelvétel) kezelése történik.

Kezelt személyes adatok:

- képfelvételek

A kamerarendszert az Adatkezelő működteti, a felvételek tárolása az Adatkezelőnél történik.

2. **Érintettek**

Valamennyi, az adatkezelő székhelyére belépő személy (közalkalmazottak, intézményi ellátásban részesülők, szerződéses partnerek; harmadik személyek)

3. **Az adatkezelés célja**

A megfigyelésnek és a képfelvételek rögzítésének a célja az adatkezelő adminisztratív ügyintézésének épületében a recepció, ügyféltér bejáratában tartózkodó személyek életének, testi épségének, valamint az adatkezelő székhelyének területén tartózkodó személyek, továbbá az adatkezelő, illetve az adatkezelő székhelyén és szervezeti egységeinek ügyintézési helyein lévők tulajdonában, vagy használatában álló vagyontárgyak, valamint az üzleti titkok és személyes adatok (a székhelyen található számítógépeken található adatok, papír alapú dokumentumokon

található üzleti titkok és érzékeny egészségügyi és szociális adatok) védelme.

Ennek keretében cél a jogsértések észlelése, az elkövető tettenérése, e jogsértő cselekmények megelőzése továbbá; hogy - szükség esetén - ezekkel összefüggésben bizonyítékként kerüljenek bírósági vagy más hatósági eljárás keretében felhasználásra.

4. Az adatkezelés jogalapja

Az adatkezelő az adatkezelést jogos érdek alapján végzi.

Az adatkezelő az érdekmérlegelést elvégezte, és az alábbiakat állapította meg:

- az érintett jogai: személyiségi jogainak védelme (képmás)
- jogos érdek: az adatkezelés céljánál részletezett személy- és vagyonvédelem
- szükségesség és arányosság, célhoz kötöttség, adattakarékosság figyelembevételével a kamerák az alábbi helyeken kerülnek kihelyezésre:
    - bejárat
- az érintettek tájékoztatása jelen szabályzat bejáratnál/recepciónál és /vagy portaszolgálatnál történő kihelyezésével.

5. A kamerák elhelyezkedése és az általuk megfigyelt területek

Valamennyi kamera elhelyezkedése: bejárat és ügyféltér

megfigyelt terület: bejárat és ügyféltér

A kamera nem irányul közterületre, jelenlétét külön tájékoztató tábla jelzi.

6. Az adatkezelés helye és időtartama

A képfelvételeket az Adatkezelő székhelyén levő központi felvevőegységen 3 munkanapig tároljuk. A 3. munkanapon túl az adatkezelő kizárólag akkor tárolja külön rögzítve az érintett felvételt, ha a tárolásra rendkívüli esemény (pl. bűncselekmény, vagy hatósági megkeresés) miatt szükség van. 30 nap után a felvételt véglegesen és visszavonhatatlanul törli az adatkezelő.

7. **Adatkezelő: Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ**

Adatkezelő személy

Neve/ munkaköre: Zsabka Attila intézményvezető

Elérhetősége: 8000 Székesfehérvár, Sörház tér 7.

8. **Adatbiztonsági intézkedések**

- A képfelvételek megtekintésére és visszanézésére szolgáló monitorok úgy kerülnek elhelyezésre, hogy a képfelvételek sugárzása alatt azokat az adatkezelő személyén kívül más személy ne láthassa.
- A megfigyelést és a tárolt képfelvételek visszanézését kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából figyelhetik. A kamerák által sugárzott képekről a központi felvevőegységen kívül más eszközzel felvételt készíteni nem lehet.
- A tárolt képfelvételekhez történő hozzáférés csak biztonságos módon, és akként történhet (jelszóval), hogy az adatkezelő személye azonosítható legyen. A tárolt képfelvételek visszanézését és a képfelvételekről készített mentést dokumentálni kell. A jogosultság indokának megszűnése esetén a tárolt képfelvételekhez történő hozzáférést haladéktalanul meg kell szüntetni.

9. **Az érintettek jogorvoslati lehetőségei**

- az adatkezelőhöz fordulhat
- a felügyelő hatósághoz fordulhat:
    - Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH, címe: 1125 Budapest, Szilágyi Erzsébet fasor 22/C, e-mail címe: ugyfelszolgalat@naih.hu). Az érintett panaszt nyújthat be a NAIH-hoz amennyiben álláspontja szerint a rá vonatkozó személyes adat kezelés nem felel meg a jogszabályi kötelezettségeknek.

      A NAIH döntése ellen bírósági felülvizsgálat kezdeményezhető.

• bírósághoz fordulhat (Székesfehérvári Törvényszék, 8000 Székesfehérvár, Dózsa György út 1., 8000 Székesfehérvár, Zichy liget 10., www.birosag.hu/torvenyszekek/szekesfehervari-torvenyszek),

Kelt: Székesfehérvár, 2018. május 25.

Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ,

mint adatkezelő

képviseletében: Zsabka Attila intézményvezető

Székesfehérvár Megyei Jogú Város
Krízis

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Székesfehérvár, 2019. október 21.

.....

intézményvezető

Szakmai szempontból egyet értek!

.....

rendszergazda

A munkáltató döntése előtt legalább tizenöt nappal kikérte a Székesfehérvári Hajléktalan ellátásban Dolgozók Alapszervezete véleményét jelen szabályzat tervezetéről, aki azt megfelelőnek találta:

Székesfehérvár, 2019. október 6.

.....

szakszervezeti titkár

12.2. Munkaállomások (USER-ek) 25
12.3. Hozzáférési jogosultságok meghatározása 27
12.4. Munkaerő belépésével kapcsolatos biztonsági eljárások 28
12.5. Munkaerő kilépésével kapcsolatos biztonsági eljárások 28
13. Távmunka 28
14. Mobil eszközök 29
15. Internet hozzáféréssel kapcsolatos intézkedések 29
16. Az elektronikus levelezés szabályai 30
17. Ellenőrzés 32
18. Oktatás, képzés és a biztonsági tudatosság fokozása 32
1. melléklet 33
TITOKTARTÁSI NYILATKOZAT 33
2. melléklet 34
FELHASZNÁLÓI JOGOSULTSÁGKEZELÉS - BELÉPÉS LAP 34
3. melléklet 36
ESZKÖZ ÁTADÁS-ÁTVÉTELI NYOMTATVÁNY 36
4. melléklet 37
MEGSEMMISÍTÉSI JEGYZŐKÖNYV 37
5. melléklet 38
Jegyzőkönyv kockázatok értékeléséhez 38
6. melléklet 39
Jegyzőkönyv informatikai eszköz/szoftver 39
beszerzését megelőző szempontok értékeléséről 39
7. melléklet 40
FELHASZNÁLÓ KILÉPTETŐ LAP 40

A Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ (a továbbiakban: Intézmény) Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) 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 rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján, és a az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (továbbiakban: BM rendelet) szerint az alábbiakban határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető céljai:

- ***az intézmény informatikai rendszer alkalmazása során biztosítsa az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását, törlését és jogosulatlan nyilvánosságra hozatalát.***
- ***az intézményt érintő rossz szándékú felhasználói, illetve kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás elleni hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek elérése;***
- ***az intézmény adatvagyonának megfelelő szintű védelme;***
- ***az intézmény működéséhez elengedhetetlenül szükséges informatikai rendszerek felhasználói működésének üzembiztossága;***
- ***a megfelelően gyors, hatékony és a veszteséget minimalizáló helyreállítási képesség megléte;***
- ***a hazai és nemzetközi biztonsági tanúsítási szabványoknak megfelelő, a nemzetközi jógyakorlatnak megfelelő színvonalú informatikai, hírközlési termékek és szolgáltatások alkalmazása;***
- ***a felhasználók megfelelő színvonalú oktatása, képzése;***
- ***a felhasználók jogainak figyelembevétele.***

Az Informatikai Biztonsági Szabályzat célja továbbá:

- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,

- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen Informatikai Biztonsági Szabályzat az adatbiztonság általános érvényű előírását tartalmazza, meghatározza az adatbiztonság feltételrendszerét.

2. Célok elérése érdekében meghatározott feladatok

Az intézmény az információs rendszerének, teljeskörű, zárt és kockázatarányos védelmére törekszik, a beszerzés költségei, valamint a tudomány és technológia állásának figyelembevételével, amelyet a PDCA modell keretében a tervezés, végrehajtás, ellenőrzés és beavatkozás során érvényesít.

A célok eléréséhez szükséges **feladatok:**
– munkatársak közti kommunikáció, koordináció, vezetői ellenőrzés,
– megfelelő együttműködés kialakítása állami, önkormányzati, civil, gazdasági és a tudományos szervezetekkel,
– az adatvédelmi incidensek kezelésére kialakított eljárásrend a szakterületek bevonásával,
– szabályozásban együttműködés a civil, a gazdasági és a tudományos terület szereplőivel,
– tudatosság, oktatás,
– megfelelő nyilvántartás, dokumentálás
– érintettek jogainak megfelelő védelme,
– az intézmény adatkezelést végző munkavállalóinak motivációja az adatvédelem fokozására.
– kidolgozni és a szabályzatokban, jogosultság kiosztási lapokon és a munkaköri leírásokban rögzíteni az informatikai rendszerhez történő hozzáférések jogosultsági rendszerét, ahol a felhasználók azonosításának egyedinek, jellemzőnek, ellenőrizhetőnek és hitelesítésre alkalmasnak kell lennie;
— az informatikai rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására;

az informatikai rendszernek képesnek kell lennie a felhasználók által végzett műveletek regisztrálására,
- a rendszerben a biztonsági naplóknak lehetővé kell tenniük a felhasználók tevékenységének vizsgálatát;
- a biztonsági eseménynapló adatait védeni kell az illetéktelen hozzáféréstől, ezekhez az adatokhoz csak erre felhatalmazott személy férhet hozzá.

3. Az Informatikai Biztonsági Szabályzat hatálya

3.1. Személyi hatálya

Az IBSZ személyi hatálya az intézmény valamennyi fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

3.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

A tárgyi hatály nem terjed ki a közérdekű és közérdekből nyilvános adatok közzétételére, továbbá részben terjed ki az adatvédelmi incidenskezelésre.

4. Az adatkezelés során használt fontosabb fogalmak

érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon, vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai

tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

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

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

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

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

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 adatokon végzik;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

5. Az Intézmény informatikai rendszerének biztonsági osztálya, az Intézmény biztonsági szintje

Az Intézmény informatikai rendszere a BM rendelet alapján** 2. biztonsági osztályba **tartozik, mivel informatikai rendszerében kezelt:

-személyes adat sérülhet;
-az érintett szervezet ügymenete szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat vagy elektronikus információs rendszer sérülhet;
-a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető.

Az intézmény a **2. biztonsági szintbe** tartozik, mivel olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és az intézmény jogszabály alapján kijelölt szolgáltatót vesz igénybe. A biztonsági szint alapján a következő intézkedések alkalmazandók:
-az érintett szervezet az érintett személyi kör részére biztosítja a szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más erre célra szolgáló dokumentumot jelen szabályzat szerint (a továbbiakban együtt: szabályzat);
-az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;
-az informatikai biztonsági szabályzat az egész intézményre vonatkozik;
-az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezető hagyta jóvá.
-a informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;
-az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.
az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;
-az eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;
-az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;
-az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel;
-a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.

6. Az informatikai rendszerre ható kockázatok

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,

- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

Az informatikai rendszerre ható kockázatokat évente értékelni kell az **5. melléklet** szerint. A megfelelő hardver és szoftver beszerzést megelőzően a **6. melléklet** szerint szükséges értékelni a termékeket.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

6.2. A védelem eszközei

Az intézmény adminisztratív, fizikai és logikai védelmi intézkedések alkalmazására kerül sor.

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

7. A védelem felelőse

A védelem felelőse az intézményvezető, aki rendszergazdát bíz meg a megfelelő adatbiztonság biztosítása érdekében, aki egyben az informatikai rendszer biztonságáért felelős személy.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról és ellenőrzéséről az intézményvezetőnek és megbízása alapján a rendszergazdának kell gondoskodnia.

7.1. Intézményvezető

Feladata a vezetése alatt álló szervezeti egységre kiterjedően:

a) A helyi adatforgalom és a munkaidőn túli géphasználat ellenőrzése.
b) A hozzáférési jogosultságok megadásának és visszavonásának kezdeményezése írásos formában.
c) A szervezeti egység által gyűjtött és kezelt adatok biztonsági osztályba sorolása.
d) Az intézmény informatikai rendszereinek üzemeltetésének, működésének irányítása és ellenőrzése, figyelembe véve a biztonsági szempontokat is.
e) A rendellenes használattal kapcsolatos ügyeket jelenti a rendszergazdának.

Felelőssége:

A vezetése alatt álló szervezeti egységre kiterjedően az informatikai biztonsági követelmények betartatása.

7.2. A rendszergazda megbízatása

A rendszergazdát az intézményvezető bízza meg eseti jelleggel, aki tevékenységére vonatkozóan az 1. számú melléklet szerinti titoktartási nyilatkozatot tesz, melyet átad az intézményvezető részére.

Munkáját az intézményvezető irányításával végzi.

1. Feladata:
   a) Az intézménynél működő Linux, Windows (valamennyi verziója) munkaállomások biztonsági adminisztrálása.
   b) A meghatározott jogosultságok szerinti felhasználói hozzáférések biztosítása, illetéktelen hozzáférések gátlása.
   c) A felhasználói igénybejelentések alapján a munkaállomásokról mentések, archiválások elvégzése.
   d) Adatsérülés esetén a mentésekből az adatok visszaállítása.
   e) A fellépett technikai problémák során a hibák kezelése, szükség esetén szakértők bevonása.
   f) Hardverberendezések hibáinak javítása.
   g) A felhasználók részére támogatás nyújtása a szoftverek és hardverek használatában.
   h) A tűzfal és a hálózat adminisztrálása, üzemeltetése.
   i) A tűzfal konfigurációs beállításaira vonatkozó dokumentumok naprakészen tartása.
   j) A hálózati konfigurációk biztonságának ellenőrzése.
   k) A konfiguráció-módosítások megtervezése és dokumentálása.
   l) Riportok készítése az intézmény vezetője számára.
   m) A hálózaton mérhető forgalmi terhelés nyomon követése, indokolatlanul nagy hálózati forgalom esetén a túlterhelés okainak kivizsgálása.
   n) A felhasználók által bejelentett hálózati meghibásodások okainak felderítése és elhárítása.
   o) A rendszergazdának a hálózat minden eleme fölött teljes és hathatós irányítási, kezelési, módosítási lehetőséggel kell rendelkeznie.

p) A hálózati rendszer üzemeltetését központosított formában kell megvalósítani.
q) A szabályoknak megfelelően eljárni.
r) A szerverek internet, levelezés, és egyéb rendszerek (a továbbiakban: IT eszközök és rendszerek) biztonsági adminisztrálása.
s) Adatbázisokkal kapcsolatos rendszeradminisztrációs (adminisztrátori, rendszergazdai) tevékenységek ellátása.

t) A meghatározott jogosultságok szerinti hozzáférések biztosítása, illetéktelen hozzáférések gátlása.
u) A meghatározott, szükséges mentések, archiválások elvégzése.
v) Sérülés esetén a mentésekből az adatbázis visszaállítása.
w) A konzisztencia és a koherencia biztosítása.
x) A fellépett technikai problémák során a hibák kezelése, szükség esetén szakértők bevonása.
y) Hardverberendezések hibáinak bejelentése és a hibaelhárítás nyomon követése.
z) Az intézmény szervezeti egységei munkájának ellenőrzése az adatbiztonság és a minősített adatok elektronikus kezelésének vonatkozásában. Az esetleges szabálytalanságok, biztonsági események kivizsgálása, jelentése.
aa) Az intézmény informatikai biztonságra vonatkozó intézkedéseinek véleményezése.
bb) Felkérésre véleményezi az intézmény vezetésének utasítás-tervezeteit, azok biztonsági kihatásainak vonatkozásában.
cc) Részt vesz a külső és belső hálózatvédelemmel összefüggő szakmai munkában.
dd) A hozzá érkezett bejelentések alapján kivizsgálja az adatfeldolgozás és kezelés biztonságát sértő eseményeket, az esetleges rossz szándékú hozzáférési kísérleteket, illetéktelen adatfelhasználást. Az eseménnyel kapcsolatban értékeli a rendszer eseménynaplóit. Javaslatot tesz a további intézkedésekre.
ee) Nyilvántartja és őrzi az adattároló eszközök titkosító kulcsait.
ff) Ellenőrzi, hogy az informatikai rendszerben kialakított, aktuálisan beállított jogosultságok megegyeznek-e a jóváhagyott jogosultságokkal.
gg) Ellenőrzi a leselejtezésre kerülő eszközök adathordozóinak törlését.
hh) Az alkalmazói szoftverek használatában a felhasználók támogatása.

2. Felelőssége:
a) A telepített új eszközök beállításainak az informatikai biztonsági követelményekkel történő összehangolása.
b) Biztonsági javítócsomagok telepítése az IT eszközökön és rendszereken.
c) Szoftverfrissítések telepítése az IT eszközökön és rendszereken.
d) Informatikai rendszer szintű felhasználók regisztrálása, kezelése.
e) Az intézmény által támogatott szoftver és hardver elemek karbantartása esetén az IBSz-ben megfogalmazott irányelvek betartása.
f) A biztonsági beállítások helyességének és sértetlenségének biztosítása.
g) Az adatbázis-kezelő szoftverek működésének fenntartása.
h) Az egyes modulok új verzióinak bevezetése.
i) Az adatbázis-felhasználók regisztrálása.
j) Az adatbázisok tárolóhelyével való gazdálkodás figyelemmel kísérése.
k) Az adatbázisok hatékony működtetése.

l) Az észlelt és jelentett az informatikai biztonságot érintő események kivizsgálása, és az elkövetett szabályszegésről az ellenőrzött személy munkahelyi vezetője értesítése.
m) A licenc-gazdálkodás figyelemmel kísérése.

3. Hatásköre:
a) Biztonsági adminisztrálás, javítócsomagok telepítése.
b) Rendszerszintű jogosultságok és hozzáférések kezelése.
c) Az adatbázis-kezelő szoftverek műveletei, biztonsági adminisztrációja.
d) Hardverhibák elhárítása.

7.3. Felhasználó

Felhasználónak minősül minden olyan intézménynél dolgozó személy, aki az intézménynél alkalmazott informatikai rendszerek kezelésére jogosultságot kapott.

Feladata:
a) A felhasználó a munkaállomásán jogosult a támogatott és az engedélyezett irodai alkalmazások használatára.
b) A munkájához szükséges adatfeldolgozó és adatbázis-lekérdező szoftverek alkalmazására.

Felelőssége:
a) Az általa használt, a munkájához szükséges szoftverek megismerése és megfelelő alkalmazása.
b) A jelen szabályzatban megfogalmazott szabályok megismerése és betartása.
c) A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

Hatásköre:
A használatra átvett, jogosultsági körébe tartozó informatikai eszközök és szoftverek alkalmazása, az esetleg észlelt hibák jelzése a rendszergazdának.

8. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok (működésre, statisztikára vonatkozó adatok),
- személyes adatok, különleges személyes adatok
- pályázati anyaghoz kapcsolódó adatok, dokumentumok

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

A naplófájlok áttekintéséért, értékeléséért a rendszergazda a felelős.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatbiztonsági nyilatkozatot kell aláíratni. (**2. sz. melléklet**)

Az adatkezelési nyilatkozat naprakészen tartásáért az intézményvezető felelős.

9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

9.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - földrengés,
  - árvíz,
  - tűz,
  - villámcsapás, stb.
- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).
- Közüzemi szolgáltatásban bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a jelszó gyakori megváltoztatásának az elmulasztása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az informatikai eszközök környezete, azok védelme

10.1. A szerverszoba minimális védelme

A szerverszobát amennyiben ott jogosult nem tartózkodik folyamatosan zárva kell tartani. A szerverszoba kulcsát elzárva tárolja az intézményvezető, a szerverszobába való belépést dokumentálni szükséges. A szerverszobában egyedül csak az intézményvezető, illetve a rendszergazda jogosult tartózkodni.

A szerverszobát a következő fizikai védelmi intézkedésekkel szükséges védeni:

a) Behatolás védelem: Ablakok

Elektromos vagy fizikai (pl. rács) védelemi eszközöket kell alkalmazni az ablakon keresztül történő bejutás megakadályozására a földszinti helyiségek esetében.

b) Behatolás védelem: Ajtók
Az ajtóknak kulccsal zárhatónak kell lenniük.
A kulcsot az intézményvezetőnél kell elhelyezni.

c) Hálózati eszközök védelme
A hálózati eszközöket zárt rack szekrényben, lehetőleg a padozatról el nem érhető magasságban kell elhelyezni.

d) Elektromos- és villámvédelem
Biztosítani kell minden kritikus rendszerelem szünetmentes elektromos ellátását és túlfeszültség védelmét.
A szerverek áramellátását külön szünetmentes áramforrással kell biztosítani.
A szerverszobát közművezeték (víz, szennyvíz) nem keresztezheti.

e) Tűzvédelem
A szerverszobában tilos tűzveszélyes, éghető, gyúlékony anyagokat tárolni.
Tűzjelző berendezés alkalmazása indokolt.

f) Klíma
A szerverszoba megfelelő hőmérsékleten tartása érdekében biztosítani kell szünetmentesített klímaberendezést.

10.2. Folyamatos áramellátás biztosítása

A szerverek és aktív hálózati eszközök (router, switch) folyamatos áramellátását biztosítani kell legalább 15 percig, a szükséges mentések elvégzésére. Erre a célra ennek megfelelő UPS-eket (szünetmentes tápegységeket) kell alkalmazni az intézmény rendszerében, melynek biztosítása Informatikai vezető feladata.

Az alkalmazandó UPS-ek telepítése és tervezése során biztosítani kell, hogy minden eszközről egyértelműen el lehessen dönteni, hogy van-e hozzá biztonsági tápellátás (UPS) illetve ezek biztonságosan, megfelelő védelemben részesítik-e az adott eszközt.

A rendszergazdának az UPS-ek megfelelő működésről módszeres tesztelés biztosításával gondoskodniuk kell.

10.3. A kábelhálózat kialakítása és karbantartása

A rendszergazda köteles módszeresen ellenőrizni a kábelhálózatot funkcionalitás és integritás szempontjából.

Az informatikai biztonság sérülése esetén a rendszergazda köteles az észlelt eseményt az intézményvezetőnek jelenteni.

Az intézmény számítógépes hálózatának menedzselése során a rendszergazdának az eljárások következetes alkalmazásával folyamatosan biztosítani kell a hálózat

a) működőképességét,

b) egyéb, meghatározott rendszerekkel való együttműködését.

Az intézmény informatikai hálózati infrastruktúrájának fejlesztése, bővítése, kiépítése során az abban résztvevőknek úgy kell eljárniuk, hogy a fejlesztés továbbra is biztosítsa az intézmény informatikai rendszerének

a) fizikai védelmét,

b) megfelelő teljesítményét,

c) megbízhatóságát,

d) megfelelő képességét a jogosulatlan hozzáférések megtagadására.

10.4. Informatikai biztonsági események jelentése

Az intézmény informatikai infrastruktúra bármilyen eszközében bekövetkezett biztonsági eseményt annak felfedezése után lehető legrövidebb időn belül írásban (e-mail) jelenteni kell a rendszergazdának:

-A felismert vagy felismerni vélt informatikai biztonságot veszélyeztető eseményt.

-A felismert vagy felismerni vélt védelmi gyengeség, biztonsági rés, sérülékenységet.

-A tapasztalt informatikai biztonsági szempontból nem megfelelő felhasználói magatartást.

-Bármilyen bizalmas információ kiszivárgást.

A rendszergazdának, a káresemény bekövetkezése és annak észlelése után az informatikai biztonságot érintő javítások, helyreállítások érdekében a lehető legrövidebb időn belül intézkednie kell:

-A felhasználó jelentése(i), tájékoztató(i) alapján a folyamatban lévő biztonsági esemény megszüntetése érdekében eljárni.

-Biztosítani, hogy az intézkedések arányosak legyenek a kockázat mértékével.

-Indokolt esetben a rendelkezésre állás ideiglenes felfüggesztésének kérése az intézmény vezetőjétől az intézmény adatvagyonának megőrzése érdekében.

10.5. Informatikai biztonsági események kivizsgálása

A rendszergazdának a tudomására jutott biztonsági események kivizsgálását késedelem nélkül meg kell kezdeni.

-ki kell jelölnie a vizsgálatban résztvevő személyeket.

A kivizsgálás kapcsán vizsgálni kell:

a) a biztonsági esemény bekövetkezésének okát,

b) az esetleges személyi felelősséget és

c) az okozott kár mértékét.

Az összegyűjtött bizonyítékokról feljegyzést kell készíteni, amelyben pontosan felsorolásra kerülnek az összegyűjtött bizonyítékok és azok biztonsági eseménnyel kapcsolatos tartalmi pontjai.

Az elkészült feljegyzéseket fel kell használni hasonló biztonsági események megelőzésére a biztonsági dokumentációs rendszer felülvizsgálatakor.

A biztonsági esemény észlelésekor azonnal meg kell tenni a szükséges válaszlépéseket. A körülmények figyelembevételével a vizsgálatba be kell vonni egyéb szakértőket pl.: adatvédelmi tisztviselőt, az incidensben érintett szervezeti egységek vezetőit stb.

10.6. Informatikai biztonsági események nyilvántartása

A rendszergazda feladata gondoskodni olyan Informatikai Biztonsági Nyilvántartás létrehozásáról és karbantartásáról, amely tartalmazza a korábbi biztonsági események kapcsán végrehajtott válaszintézkedéseket és a biztonsági események feljegyzéseit.

A nyilvántartásnak minimálisan a következő információkat kell tartalmaznia:

a) a biztonsági esemény pontos leírását,

b) a problémamegoldás során alkalmazott eljárások leírását,

c) biztonsági esemény idejét, végrehajtóját és engedélyezőjét.

A nyilvántartás felhasználható a következő esetekben:

a) bekövetkezett biztonsági esemény következményeinek enyhítésére, illetve

b) az intézményt fenyegető további biztonsági események, védelmi gyengeségek, sérülékenységek bekövetkezéseinek gyakoriságának csökkentésére és

c) kockázatok elviselhető szinten tartására.

10.7. A biztonsági eseményekkel kapcsolatos egyéb eljárások

A rendszergazdának gondoskodnia kell a felügyelete alatt álló informatikai rendszerek:

a) szükség szerinti monitorozásáról,

b) a váratlan események rögzítéséről, kivizsgálásáról,

c) rendszeres, periodikus felülvizsgálatáról (vezetői átvilágításáról).

A rendszergazdának a rendszerhibák okán fellépett biztonsági eseményeket elemeznie kell, amelynek eredményéről az intézményvezetőt tájékoztatja.

Az intézményvezető feladata az adatosztályozási besorolásnak megfelelő alap, fokozott besorolású adatok, információk kezelését végző felhasználók figyelmét felhívni, hogy a meghatározott adatok tekintetében az IBSz-ben meghatározott szabályoknak megfelelően járjanak el.

Az informatikai biztonsági eseményekkel kapcsolatos hivatalos információt, tájékoztatást csak az intézményvezetője adhat.

11. Védelmi eszközök és módszerek

11.1. Vírus védelem

Az intézmény informatikai rendszerének biztonságos, vírusmentes üzemeltetéséről a rendszergazda gondoskodik, amelynek során figyelembe kell venni különös tekintettel az alábbiakat:

Az informatikai rendszerben kétszintű vírusvédelmet kell kialakítani, mely:

a) a klienseken,

b) a szervereken fejti ki hatását.

A levelező szerveren is vírusvédelmi rendszert kell üzemeltetni.

11.2. Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt –vírusfertőzésre utaló – jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő.

  Nagyon erős vírusjegy.
- Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy. Ha az operációs rendszer újraindítása után is fennáll, erős vírusjegynek tekinthető.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

11.3. Teendők vírusfertőzés esetén

Tájékoztatni kell a vírusvédelemért felelős személyt – rendszergazdát- a fertőzésről vagy annak gyanújáról.

A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).

A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.

A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál. Ezek után a rendszer újraindítható a szokott módon.

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Ne nyissunk meg ismeretlen forrásból származó levelet!
- A gyanús e-mail-eket olvasatlanul töröljük!
- Soha ne adjuk meg jelszavunkat e-mail-es kérésre!
- Minden olyan esetben, amikor gyanús a levél, vagy annak küldője ismeretlen, a levél megnyitása előtt kérjük informatikus segítségét!

- Ne telepítsünk és ne futtassunk semmilyen szoftvert rendszergazda közreműködése nélkül!
- Ne indítsunk ismeretlen alkalmazást az internetről vagy böngészőből!
- Számítógépünk biztonsági beállításait ne bíráljuk felül, ne állítsuk át!

11.4. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftvert ellenőrző funkciókkal kell ellátni, biztosítani kell a rögzített tételek visszakeresésének és javításának lehetőségét,
- hozzáférési lehetőség:
  = a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá)
- adatrögzítés folyamatához kapcsolódó dokumentációk:
  = megőrzési utasítások,
  = gépkezelési leírások.

11.5. Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.

Az informatikai eszközök üzemeltetéséért a rendszergazda a felelős.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (floppy, CD, DVD, pendrive) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,

- adathordozót más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.
- a mobil adathordozók kizárólag titkosított adathordozók lehetnek, melyről nyilvántartást kell vezetni.

11.5.1. Adathordozók tárolása

Adathordozót az intézményből ki-, illetve oda bevinni csak az intézményvezető írásbeli engedélye alapján lehet. A mobil adathordozó (laptop, pendrive, telefon) intézményből ki-, illetve bevitelétére csak az arra engedéllyel rendelkezők jogosultak.

Az adattárolók biztonsági tárolása kapcsán a rendszergazdának (a mentést, archiválást és egyéb adattárolási eljárásokat végrehajtó munkatársaknak) gondoskodniuk kell arról, hogy a mentéseket csoportosítva, adatbiztonsági osztályok szerint elkülönítve tárolják.

A rendszergazda feladata, hogy ellenőrizze, hogy az adattárolás során betartásra kerültek-e az adatok, információk biztonsági osztályba sorolási modelljében leírtak.

11.5.2. Az adathordozók nyilvántartása

Az adathordozókról név szerinti nyilvántartást kell vezetni, az átadásukat a 3. melléklet szerint kell dokumentálni.

11.5.3. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá az államháztartás szervezete Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

11.5.4. Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Az intézmény tulajdonában levő eszközök selejtezésekor a selejtezések végrehajtásáért a rendszergazda felel.

A selejtezést a következő előírások betartása mellett szabad végezni:

-A selejtezés végrehajtására kijelölt, feljogosított személynek a vonatkozó szakmai, működési ismeretek birtokában kell lennie.

-A selejtezésről jegyzőkönyvet kell készíteni, amit az intézményvezetőnek meg kell küldeni.

-Olyan eszközöket, rendszereket nem lehet leselejtezni, amelyek hiánya információ-vesztéssel jár, vagy fennáll annak a veszélye, hogy a selejtezés során bizalmas adat kerülhet ki a szervezetből.

-Adathordozót csak annak teljes megsemmisítése, vagy fizikailag olvashatatlanná tétele után lehet selejtezni.

-Selejtezéssel tilos a folyamatos üzemeltetést veszélyeztetni.

Selejtezést csak abban az esetben szabad végezni, ha a selejtezni kívánt eszköz hiánya nem veszélyezteti az informatikai biztonságot. Amennyiben a selejtezés elkerülhetetlen, azt megelőzően gondoskodni kell az eszköz funkcionális pótlásáról.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott) mágneslemezt, CD-t, DVD-t, pendrive-ot.
- véglegesen elhasználódott anyagot *(pl. leporelló).*

A selejtezés során az alkalmatlan adattárolókat fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezésről (3 példányban) 4. melléklet szerinti jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

- ***a selejtezendő adathordozók tulajdonosának megnevezését,***
- ***a selejtezés időpontját,***
- ***milyen adathordozók, és azok mely adatai kerülnek selejtezésre,***
- ***a selejtezést végzők aláírását.***

A selejtezési jegyzőkönyvek nem selejtezhetőek.

***Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.* (Az üzemi másolás nem minősül másolásnak.)**

Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

11.5.5. Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

11.5.6. Mentések, file-ok védelme

A biztonsági mentéseket meghatározott időszakonként el kell végezni.

A munkák során létrehozott dokumentumok mentése az azt létrehozó munkatársak feladata, mely a szerverre történik.

Az alkalmazottak, gyermekek nyilvántartásával kapcsolatos adatok mentését az adatfeldolgozás folyamatában a programban az ügyintéző végzi el.

A levelezések mentését a felhasználó végzi el.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak.

A másolt lemezek csak az intézményvezető engedélyével adhatók ki.

A mentésekkel és archiválásokkal szembeni követelmények

Az intézmény elektronikus dokumentumainak mentésére és archiválására használt adathordozókat biztonságos helyen kell tárolni.

Az adattárolásra szolgáló adathordozók meg kell, hogy feleljenek az adatok, információk biztonsági osztályba sorolási modellben meghatározott időn belüli működőképesség követelményének.

Adatállományok visszaállítása

Az adat-visszaállítási eljárásoknak az a céljuk, hogy az informatikai biztonság elveinek érvényesítése érdekében a rendszer, illetve a rendszerben tárolt adatok egy korábbi állapotát állítsák vissza.

A rendszergazda feladata ellenőrizni, hogy a visszaállítási eljárások során is csak az arra jogosult személyek férhessenek hozzá a visszaállítandó adatokhoz.

A rendszer helyreállítása és újraindítása

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az intézmény által üzemeltetett rendszerek előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának kritériumai.

A mentéseket a rendszerek terhelésének csökkentése érdekében az éjszakai órákban ütemezve, háttérfolyamat alkalmazásával automatikusan kell végezni az épületben biztonságosan elhelyezett, erre a célra kialakított adattárolóra.

Rendkívüli archiválás kezdeményezése

Az archiválást az intézményvezetőjének jóváhagyásával bárki kezdeményezheti.

Az archiválási eljárást a rendszergazda végzi.

11.6. Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Minden felhasználónak jelszóval kell védenie az informatikai eszközét. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

A jelszavak megválasztásakor a jelszavak minőségét a felhasználóknak kell biztosítaniuk, a rendszerben beállított kritériumoknak megfelelően.

A jelszóválasztással kapcsolatosan a rendszergazda, illetőleg a jelszót kezelő alkalmazások tervezőinek, fejlesztőinek a feladata, hogy számítógépes eljárások alkalmazásával a felhasználókat jelen szabályzat előírásainak megfelelő jelszóválasztásra kényszerítsék.

A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

- *Az alkalmazáshoz szükséges jelszavaknak legalább 8 karakterből kell állni.*
- *A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.*
- *Vegyes karakterek használata kötelező, melyek lehetnek nagybetű, kisbetű, szám, egyéb karakter. Minimális követelmény ezek közül legalább három használata a képzett jelszóban.*
- *A felhasználók azonosítása egyedi, jellemző, ellenőrizhető, és hitelesítésre alkalmas legyen.*
- *A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat szükség esetén, illetve 6 havonta meg kell változtatniuk.*
- *Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.*
- *A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.*
- *Tilos az informatikai rendszerben ismert parancsot vagy alkalmazás nevet jelszóként használni.*
- *A jelszó nem lehet azonos a felhasználói azonosítóval.*
- *A felhasználóknak tilos más felhasználók jelszavainak megszerzésére irányuló magatartást mutatniuk.*
- *A jelszó más számára történő felfedése vagy ennek valószínűsíthetősége esetén a felhasználó köteles azt haladéktalanul megváltoztatni.*
- *A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.*
- *A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.*

Minden új jelszó kialakításánál törekedni kell arra, hogy szerkezetében ne hasonlítson az előző, lecserélendő jelszóra.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A szoftver licenc lejártával, vagy engedély nélküli szoftverek használatával a szoftverfrissítést, terméktámogatást visszautasíthatja a szolgáltató cég, valamint a szoftverek licence nélkül, vagy azzal ellentétes módon történő használatával olyan jogsértő helyzet állhat elő, mely az informatikai biztonság szempontjából nem engedhető meg.

A szoftverek beszerzése és használata során a törvényeknek való megfelelés és a folyamatos terméktámogatás céljából szigorúan be kell tartani a végfelhasználói licenc megállapodásokat.

A felhasználók felelősek a saját használatukban levő számítógép vonatkozásában az általuk feltelepített szoftverek jogtisztaságáért.

A rendszergazdának gondoskodnia kell arról, hogy:

a) **Minden használatban lévő szoftver rendelkezzen megfelelő számú, érvényes licenccel.**

b) **Az időben korlátozott licencek lejárata után, ha még szükség van a programra, a licenc megújításáról.**

A rendszergazda feladata, hogy a szoftverekhez szükséges javítócsomagokat telepítsék.

c) A rendszergazda feladata a javítócsomagok telepítését megelőzően az érintett rendszerekről biztonsági mentés készítése.

d) Az éles rendszerekre való telepítés előtt a rendszergazdának lehetőség szerint tesztelést kell végeznie.

11.7. Egyéb vagyonvédelmi előírások

- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős,
- az informatikai eszközök por, hő, pára egyéb környezeti hatásokkal szembeni védelméről a felhasználó gondoskodik.

12. A központi számítógép(ek) és a hálózat munkaállomásainak működésbiztonsága

12.1. Központi gépek (Server)

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

12.2. Munkaállomások (USER-ek)

Az irodákban és egyéb helyiségekben elhelyezett információ-feldolgozó eszközöket az illetéktelen hozzáférések megakadályozása érdekében zárható helyiségben kell tartani. Ha a helyiségben nem tartózkodik senki, az ajtót be kell zárni. A munkaállomásokat a váratlan áramkimaradás esetére szünetmentes tápegységgel kell ellátni.

A felhasználó részére beállított jogosultságokat a **2. melléklet** szerint szükséges dokumentálni.

Az intézménynél használt munkaállomásokat rendeltetésszerűen, munkavégzés céljából, az intézmény érdekeinek szem előtt tartásával, az intézmény által meghatározott módon, a felhasználó felelősségére lehet használni. A munkaállomások minden egyéb célú használata tilos.

A felhasználó felelősséggel tartozik a munkavégzés céljára biztosított munkaállomásért, köteles megőrizni a munkaállomás hardver, szoftver integritását. Hordozható eszközök esetén felelősség vállalását az eszköznyilvántartás bizonylatának aláírásával kell igazolnia.

Az intézménynél lévő munkaállomások hardver-, szoftver integritásának megőrzése céljából a felhasználónak tilos:

a) a számítógépre bármilyen szoftver komponenst installálni,

b) a számítógépet fizikailag megbontani: alkatrészeket cserélni, be-, kiszerelni.

Szerzői jogokat sértő állományok elhelyezése a rendszerekben tiltott tevékenység.

A rendszergazdának a munkaállomás leadásakor ellenőriznie kell, hogy a felhasználó a részére a 3. melléklet szerint átadott hardver-, szoftver specifikációval adja-e vissza a munkaállomást.

A felhasználóknak a mindennapos munkájuk során a munkaállomás használat tekintetében a következő szabályok szerint kell eljárniuk:

a) A számítógépes informatikai szolgáltatások igénybevételéhez kötelesek (a saját felhasználói nevükkel és jelszavaikkal hitelesítve magukat) a munkaköri feladataikban meghatározott tevékenységek elvégzéséhez szükséges domainbe és rendszerekbe belépni.

b) Bejelentkezési jogosultsággal rendelkező felhasználóknak más felhasználó azonosítójával az intézmény hálózatára bejelentkezni akkor és csak akkor szabad, ha erre az intézményvezetőjétől engedélyt kapott. A bejelentkezésről és az ott folytatott munkavégzésről a másik felhasználót tájékoztatni kell.

c) Abban az esetben, amikor a felhasználók munkaállomásaikat felügyelet nélkül hagyják, kötelesek a munkaállomást zárolni úgy, hogy a zárolás csak az arra jogosult által legyen feloldható.

d) A munkaállomás használatát nem szabad senkinek átengedni úgy, hogy eközben a munkaállomás funkcióinak illetéktelen használatával az informatikai biztonság sérülhessen.

e) Abban az esetben, ha a felhasználó az irodai helyiséget (iroda) elhagyja:

- tilos az irodában felügyelet nélkül hagyni nem felhasználónak minősülő (külsős) személyt,
- köteles a helyiséget bezárni, ha a helyiségben más felhasználó nincs,
- abban az esetben, ha más felhasználó is tartózkodik az irodában, akkor az adatok, információk biztonsági osztályba sorolási modellje szerint „fokozott" vagy magasabb osztályba sorolt nyomtatott adatokat, információkat köteles zárható helyen elhelyezni.

f) A felhasználó a munkaállomás használata során csak a munkaállomásra telepített irodai és egyéb adatfeldolgozó alkalmazásokat használhatja. Újabb alkalmazás(oka)t igényelni csak az intézményvezetőjének engedélye alapján lehetséges a rendszergazdától. Az igénylés teljesítése csak az adott alkalmazás jogtisztaságát biztosító licensz igazolás ellenében lehetséges. A rendszergazda az informatikai biztonsági szempontok figyelembevételével jogosult felülbírálni az igény végrehajtását.

g) A felhasználók kötelesek a központi erőforrásokkal feldolgozható anyagokat a központi hálózati erőforrások igénybevételével feldolgozni, és központi helyen (szervereken) tárolni.

h) A munkaállomások merevlemezén lokálisan - az adatok, információk biztonsági osztályba sorolási modellje szerint „fokozott" vagy annál magasabb osztályba sorolt adatot csak a feldolgozás ideje alatt lehet tárolni.

i) A számítógépes munka befejeztével a felhasználóknak a munkaállomásaikat ki kell kapcsolniuk, áramtalanítani szükséges a tűzvédelmi előírásoknak megfelelően.

j) Otthoni munkavégzés és bármilyen más célból nem „minősített" osztályba tartozó adatot elektronikus tárolón, elektronikus levélben vagy egyéb más módon az intézmény informatikai infrastruktúrájából kijuttatni csak a szervezeti egység vezetőjének írásos engedélyével szabad.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:

- Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia 1 perces várakozási idő beállítása mellett.
- Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

Minden olyan felhasználónak, aki munkája kapcsán adatkezeléssel, adatmódosítással foglalkozik, gondoskodnia kell a munkaállomásokon az általa létrehozott, kezelt állományok mentéséről és a mentések biztonságos helyen történő tárolásáról.

A felhasználó felelős a saját munkaállomásán bekövetkezett adatvesztésekért és az adatok sérüléséből keletkezett károkért.

A felhasználó felelős azért, hogy:

a) a mentésből visszaállíthatók legyenek az adatok,

b) a mentéseket központilag kijelölt tárhelyekre, vagy az erre a célra biztosított eszközre kell készíteni.

12.3. Hozzáférési jogosultságok meghatározása

Az intézményvezető feladata a rendszergazda részére megadni azon hozzáférési jogosultságokat, amelyekkel a meghatározott feladat elvégezhető.

A hozzáférési jogosultságok körét úgy kell kialakítani, hogy:

-Minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés.

-Az egyes területek kapcsán meghatározott jogosultsági körök összhangban legyenek az adatok, információk biztonsági besorolásával.

-Legyen lehetőség a jogosultságok számonkérésére, ellenőrzésére, visszavonására.

-Hozzáférést írásos kérelem alapján engedélyezhet az intézményvezetője.

-A meghatározott jogosultsági beállításokat a rendszergazdának kell megtennie és karbantartania.

A bizalmasság szempontjából legalább „fokozott" biztonsági osztályba sorolt rendszerek esetén biztosítani kell, hogy:

- a hozzáférés megvalósítására tervezett környezeten kívüli hozzáférés ne valósulhasson meg,
- a feladatok a rendszerben a lehető legalacsonyabb jogosultságok mellett legyenek elvégezhetők,
- az operációs rendszerhez való rendszerszintű hozzáférést csak a rendszergazdák

számára szabad engedélyezni.

A hozzáférési jogosultságokról az Intézményvezető által erre megbízott munkavállaló naprakész nyilvántartást vezet.

12.4. Munkaerő belépésével kapcsolatos biztonsági eljárások

Új felhasználó az intézményvezető által írásban meghatározott feladat- és munkakörhöz szükséges jogosultságokat kaphat.

A felhasználó számára az intézményvezető a rendszergazdának címzett írásos kérelemben 2. melléklet szerint igényelhet felhasználói fiókot és informatikai eszközöket, hozzáférést a dolgozó munkájához szükséges rendszerekhez.

Az új belépő köteles megismerni és elfogadni az IBSz rá vonatkozó szabályait, utasításait. Erről a felhasználói fiók létrehozásakor Az Intézményvezető által erre megbízott munkavállaló értesíti.

12.5. Munkaerő kilépésével kapcsolatos biztonsági eljárások

A kilépő felhasználóról az intézményvezető írásban értesíti a rendszergazdát.

A rendszergazdának el kell végeznie a következő eljárásokat:

a) Az erőforrás hozzáférési jogosultságok azonnali felfüggesztését, korlátozását, törlését, visszavonását, a felesleges állományok áthelyezését, törlését, valamint az elektronikus levelek átirányítását, törlését, a használatba adott informatikai eszközök azonnali dokumentált elszállítását.

b) Az áthelyezett, más munkakörbe került felhasználók, munkavállalók erőforrás hozzáférési jogosultságainak felülvizsgálatát.

A kilépés dokumentálására a **7. mellékletet** szükséges alkalmazni.

13. Távmunka

A távmunka végzését a felhasználóknak az intézmény vezetője engedélyezheti.

A távmunka végzés technikai feltételeinek meghatározásakor a következő szempontokat kell figyelembe venni:

a) Távmunkával kapcsolatosan nyilvános hálózatokon kommunikációt csak biztonságos technikai megoldás igénybevételével (pl. VPN) szabad használni.

b) Távmunka csak abban az esetben végezhető, ha a távmunka végzés műszaki feltételei lehetővé teszik az adatok és információk adatminősítésnek megfelelő kezelését és védelmét.

c) A távmunkát végző felhasználó köteles a munkavégzés során minden előírást és szabályt betartani, valamint felelős azért, hogy az intézmény informatikai rendszerének biztonságát, és az intézmény ehhez fűződő érdekeit ne veszélyeztesse.

14. Mobil eszközök

1. A mobil eszközök felhasználói felelősek az általuk használt eszközök biztonságos használatáért:
   a) „alap" besorolási osztályba sorolt adatok kiszivárgása, elvesztése, megsérülése miatt bekövetkezett károk terén,
   b) jogosulatlan szoftverhasználatból eredő jogi következményekre vonatkozóan,
   c) vírusok és más rosszindulatú szoftverek okozta károk esetén,
   d) lopás és az ebből származó károk terén,
   e) a felügyelet nélkül hagyott eszköz sérülékenységei terén.
2. A munkatársak által hálózatra csatlakoztatni kívánt mobil eszközöket csak rendszergazda konfigurálhat a csatlakozás érdekében.
3. Mobil munkaállomásokon tilos *„fokozott"* vagy annál magasabb biztonsági osztályban lévő adatot tárolni.

15. Internet hozzáféréssel kapcsolatos intézkedések

Az internet eléréseket biztosító informatikai eszközökre a munkaállomásokra vonatkozó szabályok érvényesek, így minden esetben működtetni kell a vírusvédelmet.

A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.

A rendszergazda jogosult az Internet használatának korlátozására, a használati jogosultság visszavonására.

1. Az Internet használatra vonatkozó szabályok:
   a) Minden felhasználó saját felelősségére használja az Internetet, mint szolgáltatást, betartva az ide vonatkozó szerzői jogi, büntetőjogi és polgári jogi előírásokat.
   b) Tilos szoftverek letöltése rendszergazda közreműködése nélkül.
   c) Tilos a fájlcserélők használata és nagyméretű (50 MB feletti méret) file-ok magáncélra történő letöltése.
   d) Tilos a felhasználóknak a Web-böngészők biztonsági beállításait (cookie-k, a JavaScriptek, JVM-ek, ActiveX környezetek, plug-in-ek, jelszó megjegyzés tiltás használatát) megváltoztatni.
   e) Az Internetről letöltött fájlokat csak vírusellenőrzés után szabad megnyitni.
   f) Tilos a felhasználóknak jogosulatlan, az intézmény érdekeivel ellentétes cselekményt végrehajtani az Internet használata közben.
   g) Az Internet használata és az azáltal megvalósított bármely cselekmény kizárólag az ide vonatkozó törvények és egyéb szabályok keretei között megengedett.

16. Az elektronikus levelezés szabályai

A munkaköri leírásban meghatározott alkalmazottnak lehetősége van internetes postafiókot igényelni, azt kizárólag munkaügyi célokra használhatják.

Az intézmény hálózatán átmenő leveleken központilag vírusellenőrzés történik, a forgalom monitorozására sor kerül.

A levelező rendszer és az abban forgalmazott üzenetek rendelkezésre állásának biztosítása a rendszergazda feladata. A saját adatforgalmi munkaállomására letöltött levelek kezelése, archiválása a felhasználók felelőssége. A felhasználó kérheti a rendszergazda segítségét az archiválás elvégzésében.

Az elektronikus levelezés alapelvei:

- A hatályos magyar jogszabályokba ütköző magatartás tiltott.
- Az intézmény levelezési tartományába tartozó címről az intézmény rendszerének felhasználásával a levelező rendszert a felhasználók csak a hivatalos feladataik elvégzéséhez használhatják.
- A felhasználók által a személyes és egyéb védendő adatok intézményen kívülre történő továbbításához az intézményvezetőjének írásos engedélye szükséges, és az adatot csak titkosított formában szabad elküldeni.
- A rendszergazda a felhasználók levelezési postafiókjainak méretét (mailbox) technikai eszközökkel korlátozza, a megengedett maximális méret a mail szerveren 1 GB. Ettől eltérni csak indokolt esetben, a rendszergazda engedélyével lehet. A felhasználók kötelessége a saját postafiókjuk méretének figyelése és a levelezést kezelő program (Outlook) erre vonatkozó helyes beállítása.
- Az elektronikus levelek a felhasználó munkahelyi e-mail címéről más e-mail címére történő automatikus továbbítása (forward) csak a rendszergazda engedélyezével lehetséges. Ilyen esetben a webmail szolgáltatás használata preferált.
- Az intézmény által hivatalosan támogatott levelező rendszeren kívül más, elektronikus levelezést (freemail, hotmail, stb.) hivatalos, az intézményt érintő ügyekre használni az intézmény munkaállomásain tilos. A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek tartalma nem sérthet meg szerzői és szomszédos jogokat.
- A levelek nem ronthatják az intézmény hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése, illetve tovább küldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.

- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről az intézmény levelező rendszerét e-mail szeméttel (spam) terhelhetik meg.

Ismeretlen feladótól érkezet, különös témájú, csatolt fájlt tartalmazó levelekkel legyünk nagyon óvatosak, a jelek vírusfertőzésre utalhatnak, töröljük a levelet.

A rendszergazda által eszközölt rendszerbeállításokat (pl. proxy szerver, IP cím, subnet mask, átjáró) megváltoztatni tilos.

A rendszergazda feladatai az elektronikus levelezés, internet és intranet használattal kapcsolatban:

a) Az intézmény központi e-mail szerverének üzemeltetése, a folyamatos működés ellenőrzése.

b) Az e-mail szerver naplóbejegyzéseinek vizsgálata, az esetleges szabálytalan e-mail használat (túl nagy csatolmányok, helytelen címzés) kiszűrése.

c) Időszakos mentések készítése a központi szerveren tárolt e-mail postafiókokról jelen szabályzat előírásai szerint.

d) A felhasználók bejelentése alapján az e-mail rendszer működésében tapasztalható egyéb hibák elhárítása.

A rendszer üzemeltetése során az informatikai biztonsággal kapcsolatban a következő teendőket kell a rendszergazdának teljesítenie:

a) Biztosítania kell, hogy a rendszerszintű hozzáférés jogosultsága ne eredményezhessen automatikus levél-felhasználói jogosultságokat. Amennyiben a rendszer működése a szerver szintű levelezés lehetőségét megköveteli, abban az esetben gondoskodnia kell arról, hogy ez csak az adott rendszerre terjedhessen ki.

b) Biztosítania kell a használt levelező rendszerek gyártó és egyéb biztonsági fórumok által javasolt biztonsági javításainak alkalmazását. Ezeknek a javításoknak az alkalmazásakor az IBSz-ben megfogalmazott előírások figyelembevételével kell eljárni.

c) Biztosítania kell, hogy a rendszerüzemeltetés során a levelező rendszer üzemelésével kapcsolatban olyan naplófájlok készüljenek és tárolódjanak, melyek segítségével a biztonsági események, felhasználói tevékenységek utólagosan is nyomon követhetők.

d) A levelező rendszer üzemelésével kapcsolatban vírusszűrő és spamszűrő rendszert kell működtetnie.

e) Biztosítania kell, hogy az operációs rendszerben a levelező rendszer állományainak jogosultsági beállításai az operációs rendszer felhasználóinak engedélyezett jogosultságaival összhangban legyenek.

f) A levelező rendszerek és biztonsági karbantartásai során a szabályzatban megfogalmazott előírások figyelembevételével kell eljárni.

17. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve a megismétlődés megakadályozása.

A folyamatba épített előzetes, utólagos és vezetői ellenőrzés során jelen szabályzat rendelkezéseinek betartását az intézményvezetője folyamatosan ellenőrzi.

Jelen szabályzat megsértése esetén fegyelmi vizsgálatot szükséges kezdeményezni, amennyiben büntetőjogi szabályba ütköző cselekmény gyanúja felmerül, az intézmény büntetőfeljelentést tesz.

Jelen szabályzatban meghatározott rendelkezések ismételt megszegése szándékos elkövetésnek minősül.

18. Oktatás, képzés és a biztonsági tudatosság fokozása

1. Az informatikai biztonság tudatosítása érdekében az adatvédelmi tisztviselőnek, rendszergazdának legalább évente oktatásokat, képzéseket kell biztosítani a következő témakörökben:

a) általános informatikai biztonsági oktatás (jelszómenedzsment, e-mail, Web etikus használata, IBSz oktatása stb.), minden új és minden hasonló oktatáson eddig részt nem vett felhasználó részére,
b) vírusvédelemmel és a vírusvédelmi rendszerekkel kapcsolatos oktatás minden új, és eddig oktatáson részt nem vett felhasználó részére,
c) új, bevezetésre kerülő rendszerekkel kapcsolatos biztonsági oktatás minden, a rendszer bevezetésében érintett felhasználó részére,
d) egyéni, a felhasználó beosztásának, munkakörének megfelelő további informatikai biztonsági oktatás,
e) minősített adatok kezelésével kapcsolatos oktatás minden, abban érintett felhasználó részére,
f) a legfrissebb fenyegetésekkel, veszélyforrásokkal, a védelmet szolgáló biztonsági eszközökkel, technikákkal kapcsolatban.

1. melléklet

TITOKTARTÁSI NYILATKOZAT

Adatfeldolgozó ... (neve) (székhely: ....., cégjegyzékszám, adószám, képviselő)

Munkavállaló (beosztása): .....

Tudomásom van arról, hogy a **Székesfehérvár Megyei Jogú Város Önkormányzata Kríziskezelő Központ** (8000 Székesfehérvár Sörház tér 3.) részére végzett rendszergazdai tevékenység tekintetében 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 rendelete (2016. április 27.), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény mindenkor hatályos szabályai szerint adatfeldolgozónak minősülök. Tudomásom van arról is, hogy az adatfeldolgozónak biztosítania kell, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállaljanak, továbbá ismerve a „személyes adat" fogalmát, miszerint személyes adatnak minősül az azonosított vagy azonosítható természetes személyre 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 tényező alapján azonosítható - **a következő titoktartási nyilatkozatot teszem:**

Kötelezettséget vállalok arra, hogy a munkám során tudomásomra jutott személyes adatokat kizárólag a munkaköri feladataim teljesítése céljából kezelem és továbbítom, más célra nem használom, azokat illetéktelen személlyel nem közlöm és nem adom át, a személyes adatokhoz jogosulatlan hozzáférést nem engedek, a személyes adatokat nyilvánosságra nem hozom. Nyilvánosságra hozatalnak minősül a jogosulatlan harmadik személlyel történő közlés is.
Az adatfeldolgozói szerződés keretében a munkám során tudomásomra jutott minden információt, adatot vagy tényt bizalmasan kezelek.
Tudomásom van arról, hogy titoktartási kötelezettség a munkaviszony megszűnésére tekintet nélkül, határidő nélkül terhel.
Tudomásul veszem, hogy a titoktartási kötelezettség megsértése a munkaviszonyból eredő kötelezettség lényeges megsértésének minősül, amelyre a munkáltató munkajogi jogkövetkezményeket alkalmazhat.
Tudomással bírok arról, hogy aki a foglalkozásánál vagy közmegbízatásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, bűncselekményt követ el, továbbá arról, is, hogy aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból, vagy jelentős érdeksérelmet okozva jogosulatlanul, vagy a céltól eltérően személyes adatot kezel, vagy az adatok biztonságát szolgáló intézkedést elmulasztja bűncselekményt követ el.

Kelt, Székesfehérvár, 20 ..... év ..... hó ..... nap

.....

a munkavállaló aláírása

2. melléklet

FELHASZNÁLÓI JOGOSULTSÁGKEZELÉS - BELÉPÉS LAP

Belépő felhasználó neve, rendfokozata:	
Beosztása:	
Szervezeti egység:	
Iroda száma:	
Irodai telefonszám:	

A felhasználó számítógépének hálózati azonosítójának aktiválása:

Számítógép-azonosító (Tartomány \ számítógépnév)	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

A felhasználó operációs rendszer szintű azonosítójának aktiválása:

Felhasználó-azonosító (Tartomány \ felhasználó)	Ideiglenes jelszó	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

A felhasználó alkalmazás szintű azonosítójának aktiválása:

Felhasználó-azonosító	Ideiglenes jelszó	Alkalmazás adatai	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Alkalmazások/Szolgáltatások			
	Igen/Nem		*Igen/Nem*
Notebook*		Webszerver	
Vezetékes telefon		e-mail*	
Mobiltelefon*		VPN*	
Mappahozzáférés:*		Nyilvántartási rendszer:	
Kamerarendszer*		egyéb: megnevezés	

Hozzáférési engedélyek lejártának dátuma:

.....

Egyéb észrevételei a beléptetési folyamattal kapcsolatban:

.....
.....
.....
.....

A felhasználó tudomásul veszi, hogy:

- *a rábízott adatokért és jogosultságokért személyes felelősséggel tartozik;*
- *a felhasználói-azonosítóját és jelszavát nem szolgáltatja ki más személyeknek;*
- *ideiglenes jelszavát az első belépés alkalmával megváltoztatja;*
- *a saját számítógépén és a hozzákapcsolódó rendszerekben létrehozott és kezelt állományok – beleértve az elektronikus levelezést is –, az intézmény tulajdonát képezik, ezért a belső szabályozóiban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.*
- *az Informatikai Biztonsági Szabályzatot meg kell ismernie és munkaviszonyának megkezdésétől számított 30 munkanapon belül eredményes vizsgát kell letennie.*
- *A fentieken túl a felhasználói regisztráció alkalmával közölt személyes adatok kezelését mint kötelező, illetve a munkáltató adatkezelői érdekének érvényesítése körében végzett adatkezeléseket tudomásul veszi. Az adatkezelés körülményeiről az adatvédelmi tisztviselő a belépéskor tájékoztatást nyújtott.*

Dátum: .....

.....

Felhasználó

Dátum: .....

.....

Rendszergazda

3. melléklet

ESZKÖZ ÁTADÁS-ÁTVÉTELI NYOMTATVÁNY

Felhasználó név:

IP cím:

MAC cím:

Tárolási hely:

Eszköz-szoftver			
Megnevezés	***Típus***	***Gyári szám***	***Eszköz azonosító***
Monitor			
Számítógép*			
Processzor			
RAM			
HDD/SSD			
OP rendszer			
Office			
Egyéb			

Megjegyzés:

Kelt, Székesfehérvár, 20…., év …….. hónap ….. nap

Át(vissza) adó:		Át (vissza) vevő:	
NÉV	Aláírás	NÉV	Aláírás

4. melléklet

MEGSEMMISÍTÉSI JEGYZŐKÖNYV

Kelt:

Jelen vannak:

Vezetői döntés kelte a megsemmisítésről:

Eszköz-szoftver			
Megnevezés	***Típus***	***Gyári szám***	***Eszköz azonosító***
Monitor			
Számítógép			
Processzor			
HDD/SSD			
Egyéb			

Megjegyzés:

Kelt, Székesfehérvár, 20...., év ..... hónap ..... nap

Jegyzőkönyvvezető:		Jelen lévő:	
NÉV	Aláírás	NÉV	Aláírás

5. melléklet

Jegyzőkönyv kockázatok értékeléséhez

JEGYZŐKÖNYV

Adatbiztonsági kockázatok éves felülvizsgálata, értékelése:

További kockázati tényező megnevezése vált indokolttá (kockázatokat azonosító táblázat kiegészítése):
.....(kockázat neve)

Az elmúlt év biztonsági eseményei miatt a következő adatkezelések kockázatainak átértékelése vált szükségessé:
..... (adatkezelések)

Az elmúlt évi informatikai biztonsági fejlesztések miatt a következő adatkezelések kockázatának átértékelése vált szükségessé:
..... (adatkezelések)

Az elmúlt év egyéb szervezeti, személyi, objektumvédelmi intézkedései miatt a következő adatkezelések kockázatának átértékelése vált szükségessé:
.....

További adatkezelés azonosítása, értékelése:
..... (adatkezelés)

További javaslat, észrevétel:
.....

Dátum: .....

Készítette:

.....
NÉV
aláírás

Jóváhagyó vezető:

.....
NÉV
aláírás

6. melléklet

Jegyzőkönyv informatikai eszköz/szoftver beszerzését megelőző szempontok értékeléséről

JEGYZŐKÖNYV

Informatikai eszköz/szoftver beszerzését megelőző szempontok értékelése (termékenként külön):

Igen/Nem Előzetes kockázatértékelés alapján a várható kockázatoknak való megfelelés?

Igen/Nem Érintetti jogok biztosítása (hozzáférés, helyesbítés, adathordozhatóság, korlátozás, magánhasználat, ellenőrizhetőség, érintett előzetes tájékoztatása, törlés)

Igen/Nem Adatbiztonsági követelmények az IBSZ szerint teljesülnek? (eltérő jogosultsági szintek/ hozzáférések/ naplózás/ adatok álnevesített tárolása/ titkosítás/ anonimizálás/ hozzáférés/ CIA elvek)?

Igen/Nem Indokolatlan személyes adatkezelésre sor kerül-e?

Igen/Nem Gyártó/forgalmazó ország/cég GDPR-nak való megfelelősége, ennek igazolása?

Igen/Nem Hatásvizsgálati igazolást a gyártó/forgalmazó rendelkezésre bocsátotta-e?

Igen/Nem Tudomány technikai állásának megfelelő biztonsági intézkedések?

Igen/Nem Előnyösebb ár?

Igen/Nem A cél a beszerzés hiányában nem valósítható meg (pl. versenytárs terméke)?

Igen/Nem Alkalmazott informatikai rendszerhez való kapcsolódása?

Egyéb követelmények:.....

Dátum: .....

Készítette:

.....

NÉV

aláírás

Jóváhagyó vezető:

.....

NÉV

aláírás

7. melléklet

FELHASZNÁLÓ KILÉPTETŐ LAP

□ **végleges**
□ **ideiglenes** (GYES, GYED, rendelkezési állományba helyezés, tartós egészségügyi távollét esetén)

Kilépő felhasználó neve, rendfokozata:	
Beosztása:	
Szervezeti egység neve:	
Közvetlen vezető, felettes:	
Irodai telefonszám:	
Céges mobil telefonszám:	

Könyvtárak/dokumentációk adatainak mentése (amennyiben szükséges):

Munkaállomás azonosító	**Mentés időpontja**	**Mentést végző személy olvasható aláírása**

A központi szerveren lévő felhasználói könyvtár archiválása (amennyiben szükséges):

Felhasználói könyvtár	**Mentés időpontja**	**Mentést végző személy olvasható aláírása**

A felhasználó által használt hardver eszközök átvétele:

Eszköz megnevezése	**Leltári száma**	**Gyári száma**	**Megjegyzés**

Egyéb észrevételei a kiléptetési folyamattal kapcsolatban:

.....
.....
.....

A felhasználó operációs rendszer szintű azonosítójának letiltása:

Felhasználó-azonosító (Tartomány\felhasználó)	Letiltás időpontja	Letiltást végző személy olvasható aláírása

A felhasználó alkalmazás szintű azonosítójának letiltása:

Felhasználó-azonosító	Alkalmazás adatai	Letiltás időpontja	Letiltást végző személy olvasható aláírása

Egyéb észrevételei a kiléptetési folyamattal kapcsolatban:

.....

.....

.....

A kilépő felhasználó kötelezettséget vállal, hogy:

- A foglalkoztatási jogviszony megszűnése után az intézményt érintő, a munkavégzése során tudomására jutott személyes adatokat, üzleti titkokat, információkat, adatokat harmadik személlyel nem közli, nem hozza nyilvánosságra, valamint a munkavégzés során birtokába jutott dokumentumot harmadik személy részére nem adja át, azt nem reprodukálja, kivéve, ha a közléshez az intézmény, illetve az adat tulajdonosa előzetesen, írásban hozzájárult.

A kilépő felhasználó tudomásul veszi, hogy:

- A felhasználó munkahelyi elektronikus postafiókja 30 napon belül letiltásra kerül.
- GYES, GYED, tartós egészségügyi távollét esetén az érintett felhasználó jogosultságai az informatikai és a távközlési rendszerekben felfüggesztésre kerülnek, valamint az általa használt mobiltelefon előfizetés teljes díja kiszámlázásra kerül.

Dátum: .....

.....	.....	.....
Intézményvezető	Felhasználó	Rendszergazda

Az e-mail használata, távmunka, külső elérés, ellenőrzés szabályai

Jelen Szabályzat a természetes személyek személyes adatainak a Társaság által történő kezelésének (adatkezelési tevékenységének) szabályait tartalmazza az Európai Parlament és a Tanács (EU) 2016. április 27-i 2016/679 számú Rendeletének - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról -, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben foglaltaknak való megfelelés céljából.

A Szabályzat megállapítása és módosítása és a helyben szokásos módon való közzététele az Intézményvezető hatáskörébe tartozik.

1.) E-mail címek kiosztása és használatának módja és korlátai

Minden munkatárs (a továbbiakban: Felhasználó), aki rendelkezik „céges" email fiókkal, köteles betartani az alábbi rendelkezéseket.

A Kríziskezelő Központ (a továbbiakban: szervezet) által biztosított email-cím használatának kizárólagos célja a munkavégzés: a Felhasználó nem jogosult magáncélra használni sem az e-mail címét, sem magát a levelező rendszert. A szervezetnél kiosztott minden email cím a munkavégzést és a szervezet ügyeinek, illetve a szervezettel kapcsolatba lévők (kliensek) ügyeinek intézését szolgálja, függetlenül attól, hogy egy-egy Felhasználó személyéhez kötött az elnevezés.

A Felhasználó közvetlen felettesének jóváhagyása nélkül nem jogosult a céges levelezését kívülre átirányítani. A Felhasználó nem jogosult a szervezet belső informatikai rendszerén kívüli helyszínen/helyszínről publikus eszközről vagy publikus csatornán elérni vagy megpróbálni elérni a leveleit, sem egyéb belső informatikai szolgáltatást, ezt kizárólag a szervezet igényei szerint megfelelően védett eszközről védett csatornán teheti meg (saját mobilról és otthoni számítógépről, amennyiben azok a belső eszközökkel azonos védelmi rendszerrel rendelkeznek és nincs más Felhasználójuk).

(...mert ezzel idegen környezetben a rendszerhez való hozzáférést lehetővé tevő azonosítókat ad meg, amelyeket az ismeretlen gépen lévő egészen egyszerű programok is el tudnak lopni, így a Felhasználó bizalmas adatok hozzáférhetővé tételét kockáztatja.)

A megfelelő védettségű eszköz és csatorna fogalmát az Intézményvezető (a továbbiakban: szervezet vezetője) állapítja meg, az informatika információi alapján.

(...mert a közvetlen külső mail-elérés megkerüli a cég saját szűrőit, amely a cég saját szándékainak megfelelően van beállítva. A szervezet működésére potenciálisan veszélyes, kártékony levelek ilyen alternatív útvonalon való beérkezését kívánja kizárni e szabály).

A szervezet vezetője jogosult az e-mail címmel és az ottani -nem személyes - adatokkal minden egyéb műveletre is. Például, de nem kizárólag: átirányítani, megszüntetni, automatikus válaszüzenetet applikálni, biztonsági mentést készíteni a levelekről, azokat tárolni, letörölni, publikálni, kizárólag megosztani más Felhasználókkal. *(...a mailek munkavégzés során létrejött információkat tartalmaznak, és ha valaki munkáját másnak kell folytatnia, szüksége van az ügy előtörténetére.)*

A Felhasználó köteles az email fiókhoz tartozó jelszavát úgy tárolni, hogy ahhoz illetéktelen harmadik személy ne férjen hozzá. Az e-mail fiókokról – az ellenőrzés során talált tiltott magán levelek törlését követően a szervezet vezetője biztonsági másolatot készíthet a munkavégzés folyamatosságának biztosítása végett, amit 1 évig jogosult megőrizni, a határidő leteltét követően a fiók tartalmát véglegesen törli.

2.) E-mail forgalom az egyes részlegek között, illetve külső címzettekhez

- az egyes részlegek közötti e-mail forgalom a fenti szabályok szerint bonyolítandó

- hivatalos (személyre szóló) e-mail címről külső szervhez, fenntartóhoz az e-mail forgalom kizárólag az intézményvezető írásos engedélye útján lehetséges

3.) Ellenőrzés

A szervezet vezetője ellenőrizheti a jelen utasítás betartását. Az ellenőrzés célja a szervezettel kapcsolatban lévő kliensek személyes adatai védelme betartásának, illetve jelen utasítás szabályai szerinti munkavégzés ellenőrzése. Az e-mail folyamba a szervezet vezetője betekinthet, még akkor is, ha e címen valamelyik, a postafiókhoz hozzáférő Felhasználó a tiltás ellenére magánjellegű levelezést is folytatott.

Az ellenőrzés szabályai a következők:

- az ellenőrzésre a szervezet vezetőjének utasítása alapján, annak jelenlétében, a mindenkori rendszergazda jogosult. A kizárólag munkaidőben történő ellenőrzésen - előzetes írásbeli értesítés alapján – az ellenőrzött munkatárs jelenléte kötelező. Amennyiben objektív akadályok miatt az ellenőrzésem részt venni nem tud, írásbeli jelzésére a szervezet vezetője még egy további ellenőrzési időpontot tűz ki.
- Az ellenőrzés főszabály szerint az észlelésig, illetve annak megállapítására terjed ki, hogy a munkatárs a vezetői utasítást nem tartotta be. A szervezet vezetője ugyanakkor nem jogosult megismerni a magánjellegű e-mailek tartalmát. Az észlelés maga elegendő munkajogi jogkövetkezmény alkalmazásához.
- Az e-mail fiók ellenőrzésénél első lépéseként az e-mail cím és a levél tárgyának az ellenőrzése is elegendő lehet, amennyiben az e-mail cím felépítéséből és az e-mail tárgyából is lehet látni azt, hogy az magáncélú e-mail, és ezért nem szükséges megismerni az e-mail tartalmát.
- A szervezet vezetője nem kötelezhető arra, hogy a Felhasználó személyes és szervezeti leveleit kiválogassa abból a célból, hogy a további munkavégzés céljából történő megosztás során más személyek ne férjenek hozzá a Felhasználó személyes levelezéséhez. Ezért ezeket a magáncélú leveleket az ellenőrzés során - az észlelést követően haladéktalanul - a szervezet vezetője másolat készítése nélkül törli.

Az e-mail fiókot– a Felhasználó alkalmazási jogviszonyának megszűnésekor -, annak tartalmától függetlenül oly módon kell törölni a rendszerből, hogy az ne legyen visszaállítható.

4.) Egyéb szabályok

Amennyiben az ellenőrzés nem végezhető el anélkül, hogy személyes adatot kezelne a szervezet vezetője, úgy az alábbi szabályokat alkalmazzák:

Az adatkezelés célja:

- személy- és vagyonvédelem, üzleti titok védelme, munkavállalói kötelezettségek teljesítésének ellenőrzése

Adatkezelés jogalapja:

- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges [Rendelet 6. cikk 1) bek. f)]

Adatkezelés címzettjei:

- munkatárs szervezeti vezetője, IT szolgáltató, rendszergazda

Adatkezelés időtartama:

- haladéktalanul, de legkésőbb az ellenőrzés befejezését követő munkanap végén törölni kell a személyes adatokat

Jogsértés esetén:

Az érintett munkatársnak jogában áll az adatkezelőtől

- a rá vonatkozó személyes adatokhoz való hozzáférést,
- azok helyesbítését, törlését vagy
- kezelésének korlátozását kérni és
- tiltakozhat az ilyen személyes adatok kezelése ellen, valamint
- élhet az adathordozhatósághoz való jogával.

Az érintett munkatárs jogosult továbbá az adatkezeléssel kapcsolatos panaszával a

Nemzeti Adatvédelmi és Információszabadság Hatósághoz

(1125 Budapest, Szilágyi Erzsébet fasor 22/c.; www.naih.hu, Telefon: +36 (1) 391-1400, Telefax: +36 (1) 391-1410, E-mail: ugyfelszolgalat@naih.hu) fordulni vagy a Polgári perrendtartásról szóló törvény szerint hatáskörrel és illetékességgel rendelkező Bíróság előtt érvényesíteni személyes adatok kezelésével kapcsolatos jogait.

Jelen módosított szabályzat a kihirdetését követően lép hatályba.

Székesfehérvár, 2020. január 20.

Zsabka Attila

intézményvezető

Jelen szabályzatot megismertem és a magamra nézve kötelezőnek ismerem el.

Székesfehérvár, 2020. .....

Név: .....

Aláírás: .....

SÜTI tájékoztató

Ez a weboldal sütiket (cookie) használ: a tartalmak személyre szabásához, közösségi funkciók biztosításához, valamint weboldalforgalom elemzéséhez. A weboldalon való böngészés folytatásával Ön hozzájárul a sütik használatához.

A sütik olyan kis szöveges fájlok, amelyeket egy weboldal felhasználhat arra, hogy még hatékonyabbá tegye a felhasználói élményt. A jogszabályok szerint a sütiket abban az esetben tárolhatjuk az Ön eszközén, ha erre feltétlenül szükség van a weboldalunk működése érdekében. Minden egyéb típusú süti használatához az Ön engedélyére van szükségünk. Jelen weboldal különféle sütiket használ.

A weboldalunkon megjelenő némelyik sütit harmadik fél szolgáltatóink helyezik.

Ön bármikor módosíthatja vagy visszavonhatja weboldalunkon a Sütinyilatkozathoz való hozzájárulását.

1.) Elengedhetetlen/szükséges sütik

Az elengedhetetlen sütik segítenek használhatóvá tenni a weboldalunkat azáltal, hogy engedélyeznek olyan alapvető funkciókat, mint az oldalon való navigáció és a weboldal biztonságos területeihez való hozzáférés. A weboldal ezen sütik nélkül nem tud megfelelően működni.

Mentés:

Ezzel a beállítással az alábbiakat engedélyezi: biztonságos bejelentkezés, bejelentkezési adatok megjegyzése, feladatok, tranzakciók folyamatának megjegyzése

2.) Funkcionális/ Statisztikai sütik

Az adatok névtelen formában való gyűjtésén és jelentésén keresztül a statisztikai/analitikai sütik segítenek a weboldal tulajdonosának abban, hogy megértse, hogyan lépnek interakcióba a látogatók a weboldallal.

Mentés:

Ezzel a beállítással az alábbiakat engedélyezi: biztonságos bejelentkezés, bejelentkezési adatok megjegyzése, feladatok, tranzakciók folyamatának megjegyzése, statisztikai célú webanalitikai mérések

3.) Kényelmi sütik

Lehetőséget biztosítanak arra, hogy az oldal használatát elemezve személyre szóló tartalmakat és hirdetéseket jelenítsünk meg, vagy küldjünk Önnek, illetve az elemzéseket felhasználva továbbfejlesszük szolgáltatásainkat.

Mentés

Ezzel a beállítással az alábbiakat engedélyezi: biztonságos bejelentkezés, bejelentkezési adatok megjegyzése, feladatok, tranzakciók folyamatának megjegyzése, statisztikai célú webanalitikai mérések, hirdetések megjelenítése az oldalon

ADATVÉDELMI INCIDENS NYILVÁNTARTÁS AZ

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE ALAPJÁN

Sorszám: .....

HATÁLYOS: SZÉKESFEHÉRVÁR, 2018. MÁJUS 25.

Az adatkezelő /képviselője/ megnevezése és elérhetőségek:	Név: Zsabka Attila intézményvezető Tel:06-22/ 330-604, Mobil: 00-36/70-669-9221
Az adatvédelmi tisztviselő van-e, elérhetőségei: **van/nincs**	Név: dr. Szilágyi Zsuzsanna Tel:+36 30 350 7541 E-mail: drszilagyiugyved@t-email.hu
Adatkezelési cél:	az adatvédelmi biztonság sérülésének megszüntetése, a bejelentési kötelezettség teljesítése
Az adatkezelés jogalapja:	GDPR 33. cikk
Adatvédelmi incidens jellege, személyes adat kategóriák és száma:	pl. adatok véletlen megsemmisítése, jogosulatlan közlése,... pl. név, cím, telefonszám, e-mail cím, TAJ szám, adóazonosító vagy érzékeny adat pl. egészségügyi, v közfoglalkoztatási adat adókedvezményhez
Érintettek kategóriái és száma:	
Valószínűsíthető következmények:	
Technikai és szervezési intézkedések:	
Bejelentés felügyeleti hatóságnak: **Időpontja:**	

Kelt: Székesfehérvár, 2019....../.....hó.....nap

Székesfehérvár MJV Önkormányzat Kríziskezelő Központ, mint adatkezelő
képv.: Zsabka Attila intézményvezető

Székesfehérvár MJV Kríziskezelő Központ - KOCKÁZATELEMZÉS - 2018. május - Felkészülés a GDPR rendelet alkalmazására

Terület (folyamat)	Adatvagyontárgy (amin személyes adat van)	Elhelyezés, tárolás	Felelős	Veszélyforrás (mi történhet?)	Káresemény (mit okozhat?)	Jelenlegi védelem (most hogyan védekezem a káresemény bekövetkezése ellen?)	Adatkör (bizalmas, belső használatra)	Bekövetkezés valószínűsége (kicsi, közepes, nagy)	Kockázat (kicsi, közepes, nagy)
Beszerzés	Megbízási szerződések (magánszemély)	digitálisan és papír alapon	Folyamatgazda és a gazdasági iroda munkatársai	Bizalmas személyi adatok nyilvánosságra kerülnek	Személyi jogok megsértése	Titkorsított tárhelyen való elhelyezés, zárható szekrényben tartás	Bizalmas	Kicsi	Nagy
Emberi Erőforrások	közalkalmazotti kinevezési okiratok, szgk törzskönyv, biztosítás, forgalmi engedély, bizonyítványmásolatok, személyi adatlap, személyes okmányok másolatai, jelenléti ívek, kérelmek, orvosi igazolások, táppénz, tb papír, hatósági végzések, nyilatkozatok, álláspályázatok, önéletrajzok, Munkavállalói kedvezményekhez kapcsolódó iratok, eü állapot igazolások, meghatalmazások, megbízólevelek, bérpapírok, számfejltési lapok	digitálisan és papír alapon	Folyamatgazda és a gazdasági iroda munkatársai, intézményvezető	Bizalmas személyi adatok nyilvánosságra kerülnek	Személyi jogok megsértése	Titkorsított tárhelyen való elhelyezés, zárható szekrényben tartás	Bizalmas	Kicsi	Nagy
Gazdálkodás	Közalkalmazotti kinevezési okiratok, megbízási szerződések (magánszemély), bizonyítványmásolatok (megbízásos munkavégzésnél), ellátásban részesülők személyes adatai; Vevő magánszemélyek adatai (pl. rendezvények részvételi díjának számlázása)	digitálisan és papír alapon	Folyamatgazda és a gazdasági iroda munkatársai, ügyvezető	Bizalmas személyi adatok nyilvánosságra kerülnek	Személyi jogok megsértése	Titkorsított tárhelyen való elhelyezés, zárható szekrényben tartás	Bizalmas	Kicsi	Nagy
Informatika	IT rendszer			Áramszünet	Szolgáltatás kimaradás	Szünetmentes tápegység		közepes	kicsi
	Minden IT rendszer			Vírus, kémprogram	Adatvesztés, Gazdasági kár	Rendszerek naprakészen tartása, Információ adás		kicsi	közepes
	Szerverek			Szerver hiba	Szolgáltatás kimaradás, Adatvesztés	Szerverek redundanciája		kicsi	nagy
	Mobil eszközök			Mobil eszköz elvesztése, eltulajdonítása	Adatszivárgás	Mobil eszköz menedzsment szoftver bevezetése folyamatban		közepes	közepes
	Alkalmazások			Adatszivárgás	Gazdasági kár	Felhasználó kezelés, Jogosultsági rendszer		közepes	nagy
	Alkalmazások			Adatvesztés	Gazdasági kár	Szerverek redundanciája, Biztonsági mentés, Szünetmentes rendszer		kicsi	nagy
	Minden IT rendszer			Nem naprakész rendszerek	Szolgáltatás kimaradás, Vírustámadás, Hackertámadás	Rendszerfrissítések		kicsi	közepes
	Alkalmazások			Jelszómegosztás	Jogosulatlan hozzáférés, Adatszivárgás	Képzés, Különálló jelszavak használata		közepes	közepes
	Minden Alkalmazás			Jelszócserék gyakorisága, jelszó reset funkció hiánya	Jogosulatlan hozzáférés, Hackertámadás	Jelszóhossz és bonyolultság meghatározása		közepes	közepoes
	Web alapú rendszerek			Titkosított kapcsolat hiánya (https)	Adatok kikerülése, Hackertámadás	Saját rendszerek esetén fokozatos áttérés, külső rendszerek esetén javaslat az áttérésre		kicsi	közepes
	Alkalmazások			Alkalmazások esetén elkülönített felhasználókezelés hiánya vagy csak egy hozzáférés	Jogosulatlan hozzáférés	Saját rendszerek esetén fokozatos áttérés, külső rendszerek esetén javaslat az áttérésre		közepes	kicsi
	Minden IT rendszer			Biztonságtudatosági képzés hiánya	Adathalászat, Vírustámadás, Jelszó kikerülés	Információ adás értekezleten, Emailben		közepes	közepes
	Minden érintett adat			Adattárolás saját eszközön	Adatok kikerülése	Jogosultsági rendszer		közepes	közepes
	Szerverek, Hálózat			Szerver szoba nincs zárva	Szolgáltatás kimaradás, Fizikai károkozás, Lopás	Információ szolgálat, Biztonsági mentés		közepes	nagy
	Alkalmazások			Fejlesztési hiba, kikerülnek hozzáférések	Adatszivárgás	Fejlesztési módszerek, Kommunikáció		közepes	közepes
	IT rendszer			Fizikai hozzáférés a hálózathoz fali csatlakozón keresztül	Jogosulatlan hozzáférés	Használaton kívüli aljzatok kikötése		kicsi	közepes

Pályázatok gondozása	E-mail	digitálisan	Folyamatgazda	Bizalmas személyi adatok és a gazdálkodási nem nyilvános adatok nyilvánosságra kerülnek	Személyi jogok megsértése; üzleti hátrány; adatlopás	Jelszóval védett PC, telefon		Kicsi	Kicis
Székesfehérvár MJV Önkormányzat Kríziskezelő Központ partnereivel való kapcsolattartás	együttműködési megállapotás nyilvántartás (excel tábla és beszkennelt, aláírt megállapodások), partneri adatbázik, telefonregiszter	digitálisan és papír alapon	folyamatgazda	Bizalmas személyi adatok nyilvánosságra kerülnek	Személyi jogok megsértése	Titkorsított tárhelyen való elhelyezés, zárható szekrényben tartás	Bizalmas	Kicsi	Nagy
Rendezvényszervezés	online jelentkezések, e-mailek, fotók, jelenléti ív	digitálisan	Folyamatgazda	Bizalmas személyi adatok nyilvánosságra kerülnek	Személyi jogok megsértése	hozzáférés jelszóval biztosított	Bizalmas	Kicsi	közepes
	Székesfehérvár, 2018. május 25.	Zsabka Attila intézményvezető							

Székesfehérvár MJV Önkormányzat Kríziskezelő Központ - ADATVAGYON LELTÁR - 2018. május - a GDPR rendelet alkalmazására

Adatkezelő neve, elérhetősége (Székesfehérvár MJV Kríziskezelő Központ 8000 Székesfehérvár, Sörház tér 3.)	**Személyes adat kategóriája** (milyen személyes adatot tárolunk; egy vagy több adat, amivel adott személy beazonosítható; személy neve, lakcím, telefonszám, email cím, személyi azonosító szám, TAJ szám stb.)	**Adatvagyon típusa** (az a dokumentum, ami az adatot tartalmazza pl. jelentkezési lapok, szerződés, kinevezési okiratok, adatlap, kérelem, teljesítés-igazolás, tárolt email stb.)	**Érintettek** (akire az adat vonatkozik pl.közalkalmazottak, ügyfelek)	**Címzettek** (akinek/ahova az adatot továbbítjuk pl. Székesfehérvár MJV Önkormányzata, ügyben más eljárók)	**Adatkezelés célja** (amilyen céllal az adatot rögzítjük, tároljuk, továbbítjuk stb. pl. törvényi kötelezettség, kapcsolatfelvétel stb.)	**Adat elérhetősége** (ahol az adatot tároljuk) **(elektronikus úton)** pl. mappaszerkezet, adatbázisok, honlap stb.	**Adat elérhetősége** (ahol az adatot tároljuk) **(papír alapon)** pl. irattár, zárható szekrény stb.	**Adatfeldolgozók** (aki az általunk kezelt adattal a írásbeli megbízásunkból valamilyen tevékenységet végez és nem az intézmény Alkalmazásában álló személy; munkatárs pl. szerződött partnerek, ügyvéd stb.)	**Adattárolás időtartama** (pl. számlák, szerződéseknél 8+1 év, tövényi előírás, ill. szerződésben foglaltak szerint vagy korlátozott tárolhatóság elve szerint ameddig szükség van rá, különös tekintettel a törlésre előirányzott határidőkre)	**Adatkezelési tevékenység kategóriái** (adaton végzett bármely művelet: gyűjtés, felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás, felhasználás, lekérdezés, továbbítás, nyilvánosságra hozatal, törlés…)	**Tárolt adat típusa** (személyes adat, különleges adat, közérdekű adat, közérdekből nyilvános adat)	**Jogalap** (hozzájárulás, jogi kötelezettség, szerződés teljesítése, közérdekű adatkezelés vagy közhatalmi jogostívány gyakorlásának keretében végzett feladat ellátása érdekében végzett adatkezelés, adatkezelő vagy harmadik fél jogos érdekének érvényesítése)
BESZERZÉS A SZFV MJV Önkormányzat Kríziskezelő Központ gazdasági szervezetének (Szfv MJV Önkormányzat Humán Szolgáltató Intézet pénzügyi és számviteli munkatárs, gazdasági vezető	Társas vállalkozások és egyéni vállalkozók, magánszemélyek adatai (vezető neve, telefonszám, e-mail cím, cím, adóazonosító, bankszámlaszám)	vállalkozási vagy megbízási szerződés	ügyfelek	könyvelő program, pályázati elszámolási oldalak, NGM, Emberi Erőforrások Minisztériuma, NAV, OEP, Székesfehérvár MJV Önkrmányzata	a gazdasági folyamatok lekövetése	Könyvelő szoftverben tárolt partnertörzs Beszerzés minősített beszállítói lista Szerződésnyilvántartás, ügyfélnyilvántartó rendszer	Gazdasági iratok, irattár Irattár	jogász, könyvvizsgálók,fenntartó gazdasági és pénzügyi ellenjegyzői,	10 év	felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás (esetlegesen), felhasználás, továbbítás	közérdekű adat	
EMBERI ERŐFORRÁS GAZDÁLKODÁS Székesfehérvár MJV Önkormányzat Kríziskezelő Központ - pénzügyi és személyügyi munkatársak (külső)- Székesfehérvár MJV Önkormányzat Humán Szolgáltató Intézet (8000 Székesfehérvár, Ady E. utca 8.)	Foglalkoztatottak (név, lakcím, TAJ, besorolási adatok, adóazonosító jel, szül.h.,idő, anyja neve, bankszámlaszám, bizonyítványszám, végzettséget igazoló okmányok, személyes iratok másolatai, nyugdíjas törzsszám, Eü-i bizalmas adatok)	kinevezési okiratok,, jelenléti ív, gk. törzslap, biztosítás, forgalmi engedély, személyi adatlap, oktatási jegyzőkönyvek, kérelmek, táppénzes papírok, orvosi igazolások, eü. -i állapotot igazoló iratok, hatósági végzések, számfejtési lapok, nyilatkozatok, álláspályázatok, önéletrajzok, foglalkoztatotti kedvezményekhez kapcsolódó iratok (születési és halotti akvi.kivonat, házzassági akvi.kivonat)meghatalmazások, megbízó levelek	munkavállalók és közvetlen hozzátartozók	könyvelő program pályázati elszámolási oldalak (NGM), mberi Erőforrások Minisztériuma, Állami Számvevőszék, NAV OEP	a gazdasági folyamatok lekövetése	Könyvelő program partnertörzs Szerződésnyilvántartás koözalkalmazotti jogviszonyokra vonatkozó elektronikus nyilvántartás, papír alapú dokumentumok	Gazdasági iratok, irattár Irattár (lemezszekrény)	jogász könyvvizsgálók Ellenőrző Bizottsági tagok NAV OEP NGM EMMI ÁSZ ISO minősítési auditor vevők szállítók	nem selejtezhető iratok	felvétel, rögzítés, rendszerezés, tárolás, megválotztatás (esetlegesen), felhasználás, továbbítás	személyes adat	Számviteli törvény Adótörvények TB Jogszabály Belső szabályzatok EU Irányelvek Közbeszerzési törvény Pályázati/támogatási szerződések előírásai
GAZDÁLKODÁS gazdasági vezető	Társas vállalkozások és egyéni vállalkozók, magánszemélyek adatai (vezető neve, telefonszám, e-mail cím, cím, adóazonosító, bankszámlaszám)	vállalkozási vagy megbízási szerződés	ügyfelek	könyvelő program pályázati elszámolási oldalak (NGM), Emberi Erőforrások Minisztériuma NAV, OEP	a gazdasági folyamatok lekövetése	Könyvelői program partnertörzs Szerződésnyilvántartás,	Gazdasági Iroda Irattár	jogász, könyvvizsgálók, Ellenőrző Bizottság,	10 év	felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás (esetlegesen), felhasználás, továbbítás	közérdekű adat	Számviteli törvény Adótörvények TB Jogszabály Belső szabályzatok Közbeszerzési törvény Pályázati/támogatási szerződések előírásai
Székesfehérvár MJV Önkormányzat Kríziskezelő Központ - partneri kapcsolatok	PARTNER név, vállalkozás neve, lakcím, telefonszám, e-mail, aláírás	partneri adatbázis (excel tábla), együttműködési megállapodások, telefonregiszter	PARTNEREK	Kríziskezelő Központ partnerek	partneri igények együttműködésre, közös programok, rendezvények szervezésére, kölcsönös együttműködésből származó előnyök, szövetségi kapcsolatrendszer fejlődése,	Elektronikus nyilvántartás és telefonregiszter	-	-	folyamatos			

Adatkezelő neve, elérhetősége (Székesfehérvár MJV Kríziskezelő Központ 8000 Székesfehérvár, Sörház tér 3.)	**Személyes adat kategóriája** (milyen személyes adatot tárolunk; egy vagy több adat, amivel adott személy beazonosítható; személy neve, lakcím, telefonszám, email cím, személyi azonosító szám, TAJ szám stb.)	**Adatvagyon típusa** (az a dokumentum, ami az adatot tartalmazza pl. jelentkezési lapok, szerződés, kinevezési okiratok, adatlap, kérelem, teljesítés-igazolás, tárolt email stb.)	**Érintettek** (akire az adat vonatkozik pl.közalkalmazottak, ügyfelek)	**Címzettek** (akinek/ahova az adatot továbbítjuk pl. Székesfehérvár MJV Önkormányzata, ügyben más eljárók)	**Adatkezelés célja** (amilyen céllal az adatot rögzítjük, tároljuk, továbbítjuk stb. pl. törvényi kötelezettség, kapcsolatfelvétel stb.)	**Adat elérhetősége** (ahol az adatot tároljuk) **(elektronikus úton)** pl. mappaszerkezet, adatbázisok, honlap stb.	**Adat elérhetősége** (ahol az adatot tároljuk) **(papír alapon)** pl. irattár, zárható szekrény stb.	**Adatfeldolgozók** (aki az általunk kezelt adattal a írásbeli megbízásunkból valamilyen tevékenységet végez és nem az intézmény Alkalmazásában álló személy; munkatárs pl. szerződött partnerek, ügyvéd stb.)	**Adattárolás időtartama** (pl. számlák, szerződéseknél 8+1 év, törvényi előírás, ill. szerződésben foglaltak szerint vagy korlátozott tárolhatóság elve szerint ameddig szükség van rá, különös tekintettel a törlésre előirányzott határidőkre)	**Adatkezelési tevékenység kategóriái** (adaton végzett bármely művelet: gyűjtés, felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás, felhasználás, lekérdezés, továbbítás, nyilvánosságra hozatal, törlés…)	**Tárolt adat típusa** (személyes adat, különleges adat, közérdekű adat, közérdekből nyilvános adat)	**Jogalap** (hozzájárulás, jogi kötelezettség, szerződés teljesítése, közérdekű adatkezelés vagy közhatalmi jogostívány gyakorlásának keretében végzett feladat ellátása érdekében végzett adatkezelés, adatkezelő vagy harmadik fél jogos érdekének érvényesítése)
Rendezvényszervezés folyamatgazdái	vállalkozás neve, személy neve, címe, e-mail, telefon,fotók	online jelentkezések, e-mailek, fotók, jelenléti ív,	rendezvényekre jelentkezők, rendezvények résztvevői,	pályázati projektelszámolás esetén Székesfehérvár MJV Önkormányzatnak továbbítás, egyéb esetekben nem releváns	kapcsolatfelvétel, kapcsolattartás, dokumentáció	www.fehervarkrizis.hu: online jelentkezések fényképek	Irattár: Rendezvényszervezés, polc, irattár	Rendezvényszervezés folyamatgazdái	általában 10 év	gyűjtés, rögzítés, rendszerezés, tárolás, megváltoztatás, felhasználás, lekérdezés,	személyes adat, közérdekből nyilvános adat	szerződés/megállapodás teljesítése,
Informatika	Név, Teszt adatai, értékelése	Teszt fájlok, értékelés	felvételizők		felvételi eljárás	informatika folyamat mappa		HR tanácsadó esetenként				
Testületek, tisztségviselők	Székesfehérvár MJV Önkormányzat Kríziskezelő Központ tisztségviselők adatai (intézményvezető, helyettes, munkatársak) név, vállalkozás neve, beosztás, telefon, fax, mobilszám, e-mail, születési hely, idő	névsor, meghívók testületi ülésre, önkormányzat közgyűlésre, jelenléti ív testületi ülésről, jegyzőkönyv, határozat, tisztségelfogadó nyilatkozatok	Kríziskezelő Központ tisztségviselők	Székesfehérvár MJV Önkormányzat közgyűlése, képviselők/bizottsági tagok; csak név, honlap látogatói	törvényi kötelezettség(a helyi önkormányzatokról szóló törvény)	www.fehervarkrizis.hu honlap	irattár, iroda	-	törvényi kötelezettség	felvétel, rögzítés, rendszerezés, tárolás, megválotztatás (esetlegesen), felhasználás, továbbítás	személyes adat	közhatalmi jogostívány gyakorlásának keretében végzett feladat ellátása érdekében végzett adatkezelés
Székesfehérvár, 2018. május 25.												

Zsabka Attila
intézményvezető
Székesfehérvár MJV
Önkormányzat
Kríziskezelő Központ

Adatfeldolgozói kiegészítés megbízási szerződéshez/.....szerződéshez

amely a(z)

.....
székhely:
Cégjegyzékszám:
Adószám:

Képviseli:

mint megbízott (a továbbiakban: Megbízott/Adatfeldolgozó)

és a

.....
Székhely: .....
Cégjegyzékszám: .....
Adószám: .....

Képviseli: .....

mint megbízó (a továbbiakban: Megbízó/Adatkezelő)

között 201..... napján létrejött megbízási szerződés („Alapszerződés") elválaszthatatlan mellékletét képezi, tekintettel arra, hogy az Alapszerződés olyan feladatok elvégzésére is kiterjed a Megbízott részére az Alapszerződés alapján átadásra kerülő adatok kapcsán, amely adatok vonatkozásában a Megbízott Adatfeldolgozónak minősül.

1. Figyelemmel arra, hogy az Alapszerződés kapcsán természetes személyek adatainak kezelése történik, a Felek az alábbiak szerint rögzítik a személyes adatok kezelésének elveit, figyelembe véve az Európai Parlament és a Tanács (EU) 2016/679 sz. általános adatvédelmi rendeletének (a továbbiakban: **„Rendelet"**) vonatkozó rendelkezéseit is.

2. Felek rögzítik, hogy az Alapszerződés alapján átadott adatok tekintetében a Megbízó az Adatkezelő, míg a Megbízott az Adatfeldolgozó.

3. **Az adatkezelés jellege:** az Adatfeldolgozó az Érintettek személyes adatait az Alapszerződésben vállalt feladatai teljesítésének érdekében kezeli.

4. **Az adatkezelés időtartama:** az Alapszerződésben vállalt feladatok ellátásához igazodik.

5. **Az adatkezelés célja:**

6. **Az Alapszerződés alapján átadásra kerülő személyes adatok: .....**

7. **Az érintettek kategóriái**: természetes személy hirdetési ügyfelek.

8. **A Felek kötelezettségei és jogai:**

A Felek együttesen biztosítják, hogy a személyes adatok kezelése a vonatkozó jogszabályokkal összhangban történik.

8.1. Az Adatkezelő kijelenti és szavatol azért, hogy

a) a személyes adatok kezelése, azoknak az Adatfeldolgozó részére történő továbbítása megfelel az alkalmazandó tagállami és uniós adatvédelmi jog vonatkozó hatályos rendelkezéseinek;
b) elegendő garanciával rendelkezik a technikai és szervezési biztonsági intézkedések érvényesítéséhez;
c) az adatbiztonsági intézkedések alkalmasak adatvédelmi incidens (a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, adatok jogosulatlan közlése vagy az azokhoz történő jogosulatlan hozzáférés) elleni védelemre;
d) gondoskodik az adatbiztonsági intézkedések tiszteletben tartásáról.

Az Adatkezelő jogosult:

a) a jelen szerződés megkötését követően csatlakozni valamely jóváhagyott magatartási kódexhez vagy jóváhagyott tanúsítási mechanizmushoz;
b) szükség esetén adatvédelmi hatásvizsgálatot kezdeményezni, illetve azt lefolytatni;
c) konzultációt kezdeményezni a felügyeleti hatósággal, ha az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár.

8.2. Az Adatfeldolgozó kötelezi magát arra és szavatol azért, hogy

a) **kizárólag az Adatkezelő megbízásából, annak írásbeli utasításai alapján és kizárólag a jelen szerződésben meghatározott célra, a szerződésben foglaltakkal összhangban** kezeli a részére átadott személyes adatokat. Saját céljára adatfeldolgozást nem végezhet és adatkezelést érintő érdemi döntést nem hozhat, kivéve, ha az adatkezelést az Adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben erről a jogi előírásról az Adatfeldolgozó az Adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az Adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja. Amennyiben az Adatkezelő bármely oknál fogva nem képes megfelelni ezeknek a követelményeknek, ezen tényről haladéktalanul tájékoztatja az Adatkezelőt. Az Adatkezelő ebben az esetben jogosult felfüggeszteni az adattovábbítást és/vagy jogosult a szerződést felmondani.

b) **nincs tudomása arról, hogy a rá vonatkozó jogszabályok akadályoznák az Adatkezelőtől kapott utasítások és a jelen szerződésben foglalt kötelezettségek teljesítését.** Amennyiben a hatályos jogszabályok módosításának előkészítése során birtokába került információk alapján fennáll a lehetősége, hogy a módosított

jogszabály és a jelen szerződésben vállalt kötelezettségek együttesen jelentősen hátrányos helyzetbe hoznák, köteles erről az Adatkezelőt haladéktalanul értesíteni. Ebben az esetben az Adatkezelő jogosult felfüggeszteni az adattovábbítást és/vagy a szerződést felmondani.

c) csak olyan munkavállalókat bíz meg a jelen szerződésben felvázolt adatfeldolgozással, akik titoktartási kötelezettség alatt állnak és a munkavégzés megkezdése előtt megismerték a munkájukra vonatkozó adatvédelmi rendelkezéseket. Az Adatfeldolgozó szavatol azért, hogy a részére átadott személyes adatok kezelésére feljogosított, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek **titoktartási kötelezettséget** vállalnak és **kizárólag az Adatkezelő utasításának megfelelően** kezelik az átadott személyes adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket,

d) a továbbított személyes adatok kezelése előtt 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 végrehajtotta a - GDPR 32. cikkében előírt - szükséges **technikai és szervezési adatbiztonsági intézkedéseket** annak érdekében, hogy a kockázattal arányos adatbiztonságot biztosítsa, így:
   - a személyes adatok álnevesítését és titkosítását,
   - a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,
   - fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani,
   - az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást (GDPR 32. cikk),
   - hogy az irányítása alatt eljáró, 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;

e) **azonnal értesíti az Adatkezelőt** a következőkről:

   - bűnüldözési szervek felhívása a személyes adatok közlésére;
   - bármilyen véletlen vagy jogosulatlan hozzáférés és az érintettet fenyegető kár;
   - közvetlenül az érintettek részéről történő érdeklődés, anélkül hogy erre válaszolna, kivéve, ha erre felhatalmazást kapott;
   - az Adatkezelőt haladéktalanul értesíteni kell a felügyeleti hatóság által végzett minden vizsgálatról és intézkedésről, amennyiben azok a jelen szerződéshez kapcsolódnak. Ugyanígy kell eljárni, amennyiben az Adatfeldolgozó vizsgálat alatt áll, illetve érintett valamely illetékes hatóság által – a jelen Szerződés keretében folytatott, személyes adatok feldolgozásával kapcsolatos –

polgárjogi, büntetőjogi, közigazgatási szabály vagy rendelet megszegésével kapcsolatban folytatott vizsgálatban.

f) **azonnal és szakszerűen reagál az Adatkezelőtől érkező,** az adatfeldolgozás tárgyát képező személyes adatok feldolgozására vonatkozó **valamennyi kérdésre** és aláveti magát a felügyeleti hatóság adatfeldolgozásra vonatkozó utasításainak;

g) az Adatkezelő kérésére **megtekinteni, illetve megvizsgálni engedi az adatfeldolgozási tevékenységével összefüggő berendezéseket** a jelen szerződés tárgyát képező Adatfeldolgozói tevékenységek ellenőrzése céljából, amelyet az Adatkezelő végez;

h) **nyilvántartást vezet a nála és - további Adatfeldolgozó igénybevétele esetén - a további Adatfeldolgozónál felmerülő esetleges adatvédelmi incidensekről,** mely tartalmazza az incidens időpontját, az adatvédelmi incidenssel érintettek körét és számát, az érintett személyes adatok körét, az incidens körülményeit és annak hatásait, az elhárítására tett intézkedések leírását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat, a nyilvántartásba történt bejegyzésekről haladéktalanul értesíti az Adatkezelőt;

i) **segíti az Adatkezelőt az őt terhelő jogszabályi kötelezettségek teljesítésében,** így különösen:
   - az adatbiztonsági intézkedések megtételében,
   - megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolásában;
   - az Adatkezelő rendelkezésére bocsát minden olyan információt, amely jogszabályban meghatározott, illetve a jelen szerződésben vállalt 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;
   - haladéktalanul felhívja az Adatkezelő figyelmét, amennyiben megítélése szerint annak utasítása ellentétben áll az adatvédelmi uniós vagy tagállami előírásokkal;
   - segíti az Adatkezelőt az adatvédelmi hatásvizsgálat és az adatvédelmi incidens tekintetében felmerülő kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az Adatfeldolgozó rendelkezésére álló információkat;

j) **nyilvántartást vezet** az általa az Adatkezelő nevében végzett **adatkezelési tevékenységekről;**

k) hogy amennyiben az Adatkezelő jelen szerződés megkötését követően csatlakozik valamely **jóváhagyott magatartási kódexekhez vagy jóváhagyott tanúsítási mechanizmushoz,** akkor az azokban előírt intézkedéseket magára nézve **kötelezőnek ismeri el;**

l) hogy amennyiben nemzeti-, vagy EU-s jogi aktus, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság, mint felügyeleti hatóság az Felek közötti szerződések kapcsán **további kötelező tartalmi elemet** határoz meg, akkor azt magára nézve kötelező érvényűnek ismeri el.

m) A GDPR-ban megfogalmazott feltételek szerint szükség esetén az Adatfeldolgozó adatvédelmi tisztviselőt nevez ki (ennek hiányában kapcsolattartó személyt), akinek elérhetőségéről tájékoztatja az Adatkezelőt.

9. További adatfeldolgozás

9.1 Az Alapszerződés alapján jelen adatfeldolgozási szerződés szerint kezelt személyes adatok, illetve a feldolgozásukból származó eredmények harmadik személyek – ideértve az Adatfeldolgozó konszernjéhez tartozó vállalkozásokat is - részére történő továbbítása alapvetően tilos.

9.2 Az Adatfeldolgozó kizárólag az Adatkezelő előzetes írásbeli hozzájárulásával vehet igénybe további Adatfeldolgozót, alvállalkozót az Alapszerződésben és a jelen Szerződésben vállalt tevékenységre. Alvállalkozónak minősül minden természetes és jogi személy, aki vagy amely nem az Adatfeldolgozó, vagy annak munkavállalója.

Adatfeldolgozó ezért kötelezi magát arra, hogy aláírást megelőzően haladéktalanul megküldi az Adatkezelőnek a fenti írásbeli hozzájárulása alapján megkötendő, további feldolgozásra vonatkozó megállapodások tervezetét.

9.3. Adatfeldolgozó kötelezettséget vállal arra, hogy az általa jogszerűen igénybe vett további Adatfeldolgozóval megkötendő írásbeli megállapodásban a jelen szerződésben foglaltakkal azonos adatvédelmi kötelezettségeket telepít a további Adatfeldolgozóra, ideértve az Adatkezelőt megillető ellenőrzési jogosultságokat is. Függetlenül a jelen szerződésből eredő adatvédelmi kötelezettségek további Adatfeldolgozóra történő telepítésétől az Adatkezelővel szemben kizárólag a Adatfeldolgozó felel az Alapszerződésben vállalt szolgáltatás teljesítéséért valamint a törvényi és szerződéses kötelezettségek teljesítéséért. Az Adatfeldolgozó és a további adatfeldolgozó közötti írásbeli megállapodásnak tartalmaznia kell az Adatfeldolgozó helytállási kötelezettségéről szóló rendelkezést is.

10. Felelősség

10.1. Amennyiben az Adatkezelő, mint Adatkezelő a hatályos nemzeti és uniós jog alapján az érintettnek jogellenes adatkezeléssel vagy az adatbiztonsági követelmények megszegésével kárt okoz, köteles azt megtéríteni. Amennyiben az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonsági követelmények megszegésével az érintett személyiségi jogait megszegi, az érintett sérelemdíjat követelhet tőle.

10.2. Abban az esetben, ha az érintett – az Adatfeldolgozó meghatározott kötelezettségei valamelyikének megszegéséből eredően - azért nem tudja az előző pontban foglalt kártérítési és/ vagy sérelemdíj iránti igényt érvényesíteni az Adatkezelővel, mint Adatkezelővel szemben, mert az ténylegesen eltűnt, jogilag megszűnt vagy fizetésképtelenné vált, az Adatfeldolgozó hozzájárul ahhoz, hogy az érintett kártérítési és/vagy sérelemdíj iránti igényét vele szemben ugyanúgy érvényesíthesse, mintha ő lett volna az Adatkezelő.

10.3. Felek megállapodnak abban, hogy amennyiben bármelyik Fél a jelen szerződés rendelkezéseit, a vonatkozó szerződéses vagy jogszabályi adatkezelési, adatfeldolgozási, adatbiztonsági követelményeket megszegi, és a másik felet ezzel összefüggésben elmarasztalják, úgy a szerződésszegő vagy jogszabályi kötelezettségeket elmulasztó fél köteles a másik fél ebből eredő kárát, költségeit, kiadásait és veszteségeit stb. teljeskörűen megtéríteni.

10.4. A kártalanítás, kártérítés előfeltétele, hogy

- az eljárás alá vont fél haladéktalanul értesítse a másikat a jogvitáról; és
- a bevont félnek lehetősége legyen együttműködni az eljárás alá vont féllel a jogvitában a védekezés, illetve az egyezségkötés során.

10.5. Adatfeldolgozó abban az esetben tartozik felelősséggel az adatkezelése által okozott károkért, ha nem tartotta be a Rendeletben meghatározott, kifejezetten az Adatfeldolgozókat terhelő kötelezettségeket, vagy az Adatkezelő utasításait és/vagy a jelen szerződésben foglaltakat figyelmen kívül hagyta vagy azokkal ellentétesen járt el. Mentesül a felelősség alól, ha bizonyítja, hogy a szerződésszegést ellenőrzési körén kívül eső, a szerződéskötés időpontjában előre nem látható körülmény okozta, és nem volt elvárható, hogy a körülményt elkerülje vagy a kárt elhárítsa.

11. A személyes adatok törlése, helyesbítése, a személyes adatok feldolgozásának megszüntetése után fennálló kötelezettség

11.1. Adatfeldolgozó saját hatáskörében az Adatkezelő nevében kezelt adatokat nem helyesbítheti, nem törölheti, illetőleg nem korlátozhatja azok kezelését. Ez kizárólag Adatkezelő utasítása alapján megengedett. Amennyiben az Érintett közvetlenül az Adatfeldolgozót keresi meg a helyesbítés, a törlés vagy az adatkezelés korlátozása ügyében, a Adatfeldolgozó az érintett kérését köteles haladéktalanul továbbítani az Adatkezelő felé.

11.2. Adatfeldolgozó köteles az Adatkezelő utasításának megfelelően - indokolatlan késedelem nélkül biztosítani a törlési eljárásrendet, „az elfeledtetéshez való jogot", a helyesbítést, az adatok hordozhatóságát és az azokhoz való hozzáférést.

11.3. Szerződő felek megállapodnak abban, hogy az adatfeldolgozás megszüntetését követően a Adatfeldolgozó az Adatkezelő írásban közölt döntése alapján visszaszolgáltatja részére a számára megküldött személyes adatokat vagy az Alapszerződés megszűnésétől számított 30 napon belül véglegesen és helyreállíthatatlanul megsemmisíti az összes személyes adatot, és ennek megtörténtét igazolja Adatkezelő felé.

11.4. Adatfeldolgozó szavatolja, hogy a továbbított személyes adatokat a továbbiakban ténylegesen nem dolgozza fel.

12. Kapcsolattartás

12.1. Felek a jelen Szerződés teljesítése során egymással kölcsönösen együttműködnek, ezen együttműködés keretében kötelesek a szerződés teljesítését befolyásoló minden lényeges körülményről egymást haladéktalanul, de legkésőbb 3 munkanapon belül tájékoztatni.

12.2. A jelen Szerződésben foglaltakkal összefüggő kérdésekben kapcsolattartásra jogosult személyek:

	Adatkezelő részéről	**Adatfeldolgozó részéről**
Név		
Cím		
E-mail		

12.3. Felek rögzítik, hogy a kapcsolattartóként megjelölt személy(ek) vagy azok adataiban bekövetkezett változásról haladéktalanul tájékoztatják egymást. A kapcsolattartók adataiban bekövetkezett változás nem minősül szerződésmódosításnak.

13. Záró rendelkezések

13.1. Jelen szerződés aláírásával szerződő Felek kijelentik és elismerik, hogy a szerződésben foglaltakkal egyetértenek és azt magukra nézve kötelezőnek ismerik el.

13.2. A jelen szerződésre a magyar jog szabályai, különösen a Polgári Törvénykönyvről szóló 2013. évi V. törvény, valamint a Rendelet az irányadók.

13.3. A Felek megállapodnak abban, hogy megkísérlik a jelen szerződésből eredő vitás kérdéseket egymás között, tárgyalásos úton rendezni.

13.4. A Felek kötelezettséget vállalnak arra, hogy minden olyan körülményről tájékoztatják egymást, amely a szerződés teljesítését, illetve a másik Fél jogos érdekét érinti. A bejelentési kötelezettség elmulasztásából eredő károkért a mulasztó Fél felelősséggel tartozik.

13.5. Jelen szerződés bármely pontjának vagy rendelkezésének érvénytelensége nem jelenti a teljes szerződés érvénytelenségét, kivéve, ha az érvénytelennek minősülő rendelkezés vagy rész nélkül a felek a szerződést nem kötötték volna meg, vagy e rendelkezés, illetve rész hiányában a szerződés értelmetlenné vagy értelmezhetetlenné válna.

13.6. Jelen szerződés az aláírásának napján lép hatályba, és az az Alapszerződés hatályára szól, annak bármely okból történő megszűnése jelen szerződés bontó feltételét képezi azzal, hogy a jelen szerződés 11. pontjában foglalt rendelkezések az Alapszerződés megszűnését követően is változatlanul hatályban maradnak.

13.7. Jelen szerződés módosítása kizárólag írásban, a felek közös megegyezésével érvényes.

13.8. Jelen szerződést aláírók kijelentik, hogy a jelen szerződés aláírásához szükséges felhatalmazással rendelkeznek.

Jelen szerződést felek - elolvasást és értelmezést követően -, mint akaratukkal mindenben megegyezőt, jóváhagyólag, cégszerűen írják alá.

....., 2019. ..... hó .... napján

Képv.: .....

....., 2019. ..... hó ... napján

Képv.: .....

ÉRINTETT (TERMÉSZETES SZEMÉLY) HOZZÁJÁRULÁSA

EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE ALAPJÁN

Alulírott: _____

Címe: .....

..... *(anyja neve)*
az Európai Parlement és a Tanács (EU) 2016/679 rendelete (GDPR) alapján önkéntes, konkrét, tájékoztatáson alapuló, külső befolyástól mentes egyértelmű hozzájárulásomat adom a személyes adataim kezeléséhez a következő adatkezelő számára: **Székesfehérvár MJV Önkormányzat Kríziskezelő Központ** *(8000 Székesfehérvár, Sörház tér 3., adószáma:* 15364957-1-07*)*

Az érintett adatok tárolásának időtartama: jogviszony fennállása alatt/ *visszavonásig*

Hozzájárulás tárgyában érintett adatok: a Szociális Törvény 1993. évi III. törvény a szociális igazgatásról és szociális ellátásokról 20. § (2) alapján.

Az adatkezelő neve: Kríziskezelő Központ
elérhetősége: .....

Az adatkezelés célja: éjjeli menedékhely/átmeneti szálló
itt kell megjelölni azokat az okokat amiért a hozzájárulást kéri, pontos tájékoztatás szükséges , pl. *adatbázisban való szereplés, közfoglalkoztatásban adatszolgáltatás.*

Tájékoztatjuk Önt, hogy nem történik ***adattovábbítás harmadik országba vagy nemzetközi szervezet részére.***

(amennyiben igen, akkor jelölendő, hogy konkrétan hová)

Tájékoztatjuk, hogy Önnek, mint természetes személynek az adatkezelés során az Európai Parlement és a Tanács (EU) 2016/679 rendeletének értelmében Önt az alábbi jogok illettik meg:

- kérheti egy vagy több adatának korlátozását
- kérheti, hogy az automatizált döntés hatálya ne terjedjen ki Önre
- kérheti adatainak átadását vagy továbbítását
- tájékoztatást kérhet a kezelt adatokról, jogalapról, célról és a kezelés időtartamáról
- kérheti egy vagy több adatának módosítását
- kérheti adataihoz való hozzáférését
- tiltakozhat egy vagy több adata kezelése ellen
- kérheti, hogy töröljük egy vagy több adatát
- panaszt jogosult benyújtani a következő elérhetőségek valamelyikén:

  Nemzeti Adatvédelmi és Információszabadság Hatóság

  Székhely: 1125 Budapest Szilágyi Erzsébet fasor 22/c

  Postacím:1530 Budapest, Pf.: 5.

  Telefonszám: +36 (1) 391-1400

  Központi elektronikus levélcím: ugyfelszolgalat@naih.hu

Amennyiben bármilyen kérése vagy kérdése van az adatkezeléssel kapcsolatban, kérelmét postai úton a 8000 Székesfehérvár, Sörház tér 3. címre vagy elektronikusan a krizis@fehervarkrizis.hu címre küldheti. Válaszainkat késedelem nélkül, de legfeljebb 30 napon belül küldjük az Ön által meghatározott címre.

Székesfehérvár, 20..... .....

.....

érintett természetes személy aláírása