

BUCSAI KÖZÖS ÖNKORMÁNYZATI
HIVATAL

ADATVÉDELMI ÉS ADATBIZTONSÁGI
SZABÁLYZATA

2017.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 24. § (3) bekezdésében kapott felhatalmazás alapján a Bucsai Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) működésére vonatkozóan az alábbi **Adatvédelmi és Adatbiztonsági Szabályzatot** adom ki.

A szabályzat hatálya a Bucsai Közös Önkormányzati Hivatalnál nyilvántartott adatok védelmére terjed ki.

1. ÉRTELMEZŐ RENDELKEZÉSEK

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

b) adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől, és eszköztől, valamint az alkalmazás helyétől;

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

d) adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - ideértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi;

e) adat: adathordozón rögzített információ;

f) személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

g) közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől;

h) adatforrás: az a szerv vagy személy, amelyet (vagy akit) jogszabály az adat szolgáltatására elsődlegesen kötelezett, illetve amelynél (vagy akinél) az adatfelhasználás, illetőleg a további feldolgozás céljára átadásra kerülő adatok eredetileg keletkeztek, továbbá aki azt önmaga közvetlenül szolgáltatta;

- i) adatigénylő:** az érintett kivételével az a szerv vagy személy, akinek a részére az adatkezelő jogszabály kötelezése vagy kérelem teljesítése alapján adatokat szolgáltat, továbbít vagy átad;
- j) adat zárolása:** az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;
- k) érintett:** az a természetes személy, akinek személyes adata az adatkezelés tárgyát képezi,
- l) adattovábbítás:** ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik, ez alatt értve az adat kiadására irányuló adatszolgáltatást, vagy adatátadás iránti kérelem teljesítését is;
- m) adatvédelmi megbízott:** az a személy, akit az adatkezelést végző szerv vezetője az adatvédelmi feladatok ellátására kijelöl;
- n) harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;
- o) hírközlő eszköz:** távbeszélő, rádió és telefax készülék;
- p) hibás adat:** helytelen, pontatlan vagy időszerűtlen adat. Az időszerűtlen adat nem hibás, ha törvény vagy az érintett felhatalmazása alapján azért kezelik, mert korábbi állapotot tükröz;
- q) személyesadat-nyilvántartó rendszer (nyilvántartó rendszer):** személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- r) közvetlen lekérdezés:** a kezelt adatokba számítástechnikai eszköz alkalmazásával előre meghatározatlan időpontban és alkalommal történő betekintés, illetve az így megismerhetővé vált információk kinyomtatása, vagy más módon való rögzítése;
- s) személyes adatállomány:** személyes adatok rendszerezett, állandó vagy változtatott összessége, mely a tartalmazott adatfajták szerint rendezhető, válogatható, kiértékelhető;
- t) technikai adatállomány:** a jogszerűen kezelt adatokból adatbiztonsági vagy technikai célból létrehozott - legfeljebb az adatok jogszabályban előírt törlési határidejéig kezelt - ideiglenes adatállomány, melyet nem továbbítanak, tartalmát nem hozzák nyilvánosságra;
- u) hivatásbeli titok:** különösen az orvosi, ügyvédi, közjegyzői, lelkészi-egyházi személyi hivatásbeli titok;
- v) törvény által védett titok:** az államtitok, a szolgálati titok, továbbá az üzleti, a bank-, a biztosítási, az értékpapír-, a pénztártitok, valamint a magántitok.

2. ADATKEZELŐ NEVE, SZÉKHELYE

Adatkezelő neve: Bucsai Közös Önkormányzati Hivatal

Székhelye: 5527 Bucsá, Kossuth tér 6.

Jegyző: Pap-Szabó Katalin

Belső adatvédelmi felelős: jegyző

3. ADATKEZELŐRE ÉS ADATKEZELÉSRE VONATKOZÓ SZABÁLYOK

- 3.1. Az adatvédelmi szabályok betartásáért az adatkezelő a felelős. Az adatkezelő szerv dolgozója az adatvédelmi és adatbiztonsági szabályok betartásáért személyes felelősséggel tartozik.
- 3.2. Amennyiben az adatkezelő az adatkezelést adatfeldolgozóval végezteti, az adatbiztonsági szabályok betartásáért - a tevékenység végzésére vonatkozó szerződésben foglaltak szerint - az adatfeldolgozó szerv vezetőjét terheli felelősség.
- 3.3. Az adatkezelő személyes adatokat az Infotv. 4. §-ban meghatározott felhatalmazás alapján kezelhet.
- 3.4. A technikai adatállomány külön felhatalmazás nélkül kezelhető.

4. ADATVÉDELEM A HATÓSÁGI ELJÁRÁS ÉS SZOLGÁLTATÁS SORÁN

- 4.1. A hatóság köteles gondoskodni az eljárás során megismert, törvény által védett titok (védett adat) és a hivatás gyakorlásához kötött titok (hivatásbeli titok) megőrzéséről és a személyes adatok védelméről.
- 4.2. A hatósági eljárás tartama alatt – különösen az iratokba való betekintés engedélyezésénél, a tárgyalás során, a döntés szerkesztésénél és a döntések hirdetményi úton való közlésénél – a hatóság gondoskodik arról, hogy a védett adat és a hivatásbeli titok ne kerüljön nyilvánosságra, ne juthasson illetéktelen személy tudomására, és a személyes adatok védelme biztosított legyen.
- 4.3. Az adat védelmére vonatkozó szabályok megtartása nem vezethet a jogorvoslathoz való jog korlátozásához.
- 4.4. A hatóság – hatáskörének keretei között – jogosult a feladatai ellátásához szükséges, jogszabályban meghatározott védett adat, továbbá törvényben meghatározott esetben személyes adat megismerésére és kezelésére. E jogát törvény korlátozhatja.
- 4.5. Hivatalból indított vagy folytatott eljárásban korlátozó rendelkezés hiányában az ügyfél nem akadályozhatja a hatóságot az üzleti könyvek és a tényállás tisztázásához szükséges más iratok átvizsgálásában.
- 4.6. A hatóság az eljárás során a birtokába került védett adatot, hivatásbeli titkot, továbbá személyes adatot – az ugyanazon ügyben folyó, a Ket-ben meghatározott eljárások kivételével – csak akkor továbbíthat más szervhez, ha ezt törvény megengedi, vagy ha az érintett ehhez hozzájárult.

5. ADATBIZTONSÁG

- 5.1. Az adatkezelések során - az adatkezelés jellegétől függően - az információ-rendszerek következő védelmi módszereit kell alkalmazni:

a) Ügyviteli védelem: az információ-rendszer felelőseinek (rendszerirányító, rendszergazda, üzemeltető) és az adatkezeléssel kapcsolatos tevékenységnek szervezési és adminisztratív módon történő nyomon követése, a felelősség körülhatárolása. Kiterjed az

információ-rendszerre és annak szolgáltatásaira, valamint az adathordozók kezelésére, beleértve a hozzáférési jogosultság és a betekintés dokumentálását is. Ahol annak technikai feltételei adottak, a hozzáférési jogosultság ellenőrzésére és dokumentálására digitális aláírás vagy ujjlenyomat felismerő eszköz is alkalmazható.

5.2. A Hivatalnál az információ-rendszer felelőse: informatikus

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

b) *Algoritmikus védelem*: matematikai algoritmusok alapján működő védelem, amely egyedi számítógépen és hálózaton is lehetővé teszi a használó azonosítását, a jogosultság ellenőrzését. Magában foglalhat szoftver módon történő rejtjelezést is. Algoritmikus védelmet minden olyan információs rendszernek biztosítani kell, amely azonosítható természetes személyre vonatkozó adatot dolgoz fel és hálózat is csak algoritmikus védelem alatt üzemeltethető.

5.3. Az információ-rendszereket biztonsági szempontból a következő fokozatok valamelyikébe sorolja be a Hivatal:

a) *Alap biztonsági fokozatba*: azokat a rendszereket, amelyek egyedi azonosításra alkalmas személyes adatokat nem dolgoznak fel és a feldolgozott adatok egyéb okból sem minősülnek államtitkoknak vagy szolgálati titoknak, továbbá azokat a személyes adatokat feldolgozó rendszereket, amelyekben a személyes adatok feldolgozását kifejezetten a nyilvánosság számára szánták, vagy a szolgáltatott adatokból a természetes személyt nem lehet egyedi módon azonosítani;

b) *Minősített biztonsági fokozatba*: azokat a rendszereket, amelyeknél a feldolgozott adatok minősítése szolgálati titok, és azokat a rendszereket, amelyek azonosítható személyes adatot kezelnek;

c) *Kiemelt biztonsági fokozatba*: az államtitkot feldolgozó rendszereket.

5.4. Az információ-rendszer minősítését a rendszer üzembe állításáig kell a minősítésre jogosultnak meghatározni.

5.5. A Hivatal képviselőjében a rendszer informatikai működőképességéért és a jogosultságok érvényesítéséért felelős rendszergazda:

- a) kialakítja a rendszer védelmi és biztonsági előírásait;
- b) meghatározza a jogszabályoknak megfelelő igények és hozzáférési jogosultságok szerinti hozzáférési előírásokat;
- c) tervezi és ellenőrzi az adatszolgáltatások nyilvántartását;
- d) ellenőrzi a rendszer biztonságos működését, és szükség szerint intézkedik a feltárt hiányosságok megszüntetésére, rendszerkatasztrófa esetén átveszi a rendszer közvetlen irányítását.

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

- a) Az adathordozó eszközök elhelyezésére szolgáló helyiségeket (épületeket, épületrészeket) úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen.
- b) Azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését - a minősítéstől függően - korlátozni és ellenőrizni kell. A belépésre adott felhatalmazásnak összhangban kell lennie az adott személy hivatalos feladataival, illetőleg az ott kezelt adatokhoz történő hozzáférési jogosultságával.
- c) A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell. Különös figyelmet kell fordítani arra, hogy a biztonságos területről kivitt eszközök maradványadatokat ne tartalmazzanak.
- d) Az adathordozókról és mozgásukról, azok tartalmáról és felhasználásáról nyilvántartást kell vezetni.
- e) Meg kell határozni azoknak a személyeknek a körét, akik az adathordozó eszközöket üzemeltethetik.
- f) A számítástechnikai eszközök, különösen hálózatba kapcsolt - eszközök hozzáférési kulcsát (azonosító kártya, jelszó) szolgálati titokra vonatkozó szabályok szerint kell kezelni. Az internet kapcsolatot lehetőség szerint külön eszközökkel kell biztosítani.
- g) A számítástechnikai eszközök biztonsági megoldásának, valamint az adatokat feldolgozó rendszerek rendszerterveiből a biztonságra vonatkozó megoldások dokumentációjához csak az arra felhatalmazott személyek férhetnek hozzá.
- h) Ha az adatok tárolásának technikai körülményei, az épület elhelyezkedése, vagy egyéb fontos ok, illetőleg a kezelt adatok minősítése szükségessé teszi, célszerű gondoskodni a számítástechnikai eszközök másodlagos kibocsátásának árnyékolásáról.

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

- a) A számítástechnikai eszközöket üzemeltető személyek feladatait egyértelműen meg kell határozni. Egyéb, a feladatoktól eltérő tevékenységet csak külön, erre irányuló egyedi vezetői felhatalmazás alapján lehet végezni.
- b) Össze kell állítani, és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott személyek névsorát.
- c) Meg kell határozni az adatokhoz való hozzáférés szintjét és személyekre lebontott egyedi szabályait.
- d) Külső személy - pl. karbantartás, javítás, fejlesztés céljából - a számítástechnikai eszközökhöz lehetőleg úgy férjen hozzá, hogy a kezelt adatok megismerése elkerülhető legyen.
- e) Azoknak a személyeknek, akik a számítástechnikai eszközök biztonságáért felelősek - az egymás között kialakított készenléti rendszerben - állandóan elérhetőnek kell lenniük. Az illetéktelen hozzáférési kísérlet észlelésekor haladéktalanul értesíteni kell a készenlétkben levő személyt.
- f) A számítástechnikai rendszer üzemeltetéséről - hagyományos vagy automatikus módon - nyilvántartást kell vezetni. A nyilvántartást, - ideértve a rendszer üzeneteit is, - az

illetéktelen hozzáférés vagy hozzáférési kísérlet azonosítása céljából, az arra illetékes személynek folyamatosan ellenőriznie kell.

- g)* A rendszerbe kerülő adatokat tartalmazó hagyományos vagy számítástechnikai eszközökkel olvasható dokumentumokat úgy kell kezelni, hogy elvesztésük, elcserelésük vagy meghibásodásuk kiküszöbölhető legyen.
- h)* A hozzáférés jelszavait időközönként, az üzemeltető személyének megváltozása esetén haladéktalanul, de legkésőbb 24 órán belül meg kell változtatni. Jelszót ismételtelen nem lehet kiadni.
- i)* A számítástechnikai eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható.

5.8. A technikai biztonság érdekében szükséges intézkedések:

- a)* Az adatok és programok véletlen vagy szándékos megrongálását számítástechnikai módszerekkel is meg kell akadályozni.
- b)* Az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell.
- c)* Az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, ennek érdekében az adatállományokról rendszeresen biztonsági másolatot kell készíteni és azt az eredeti adatállománytól lehetőleg földrajzilag is eltérő helyen, biztonságosan kell tárolni. A biztonsági másolathoz kizárólag az eredeti állomány részleges vagy teljes megsemmisülése, illetőleg katasztrófa esetén lehet hozzáférni.
- d)* Az adatokhoz és a számítástechnikai eszközökhöz való hozzáférést jelszavakkal kell ellenőrizni.
- e)* Az adatok és az adatállományok változását naplózni kell.
- f)* Az adatkezelő programok jogtisztaságát és előírászerű működését ellenőrizni kell, ideértve biztonsági vizsgálatot is.
- g)* Programfejlesztés vagy próba céljára valódi adatok felhasználását, különösen ha a próbát külső szerv vagy személy végzi, el kell kerülni (valós személyes adatok felhasználása az utasítás alapján nem megengedett).
- h)* Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell.
- i)* Közvetlen adathozzáférés kezdeményezésének jogosultságát ellenőrizni kell.
- j)* Az adatbiztonsági programokat úgy kell megszerkeszteni, hogy az adatokhoz, vagy az adatkezelő programokhoz való illetéktelen hozzáférés kísérletét is jelezzék, illetőleg többszöri ilyen kísérlet esetén a hozzáférést megakadályozzák.

6. AZ ADATOK TÁROLÁSA

- 6.1. Az adatok tárolási módját úgy kell megválasztani, hogy - az esetleg eltérő törlési határidőre is tekintettel - törlésük az adattörlési határidő lejártakor, illetve ha az más okból szükséges, elvégezhető, és a törlés ténye ellenőrizhető legyen.

7. AZ ADATOK FELHASZNÁLÁSA

- 7.1. Az adatok a jogszabályban meghatározott célra használhatók fel.

- 7.2. Az adatkezelő szerv vezetője szervezési intézkedésekkel, ellenőrzési rendszer kiépítésével, szükség szerint az adatfelhasználás nyilvántartásával és műszaki, informatikai megoldások alkalmazásával biztosítja az adatok felhasználásának nyomon követhetőségét.
- 7.3. Az adatkezelő szerv nyilvántartásának, közvetlen lekérdezést lehetővé tevő számítástechnikai rendszerének (a továbbiakban közvetlen hozzáférést biztosító rendszer) vagy hírközlési eszközzel működő tájékoztató szolgálatának a szerv saját dolgozói által való igénybe vételét, az adattovábbítások nyilvántartásának adattartalmát és megőrzési idejét figyelembe véve dokumentálni kell.
- 7.4. Számítástechnikai, távközlési eszközök és programok helyességének ellenőrzésére, felhasználók betanítására, illetve oktatási célra valós személyi adatokat felhasználni nem lehet.

8. BELFÖLDI JOGSEGÉLY

- 8.1. Jogsegélyt akkor lehet kérni, ha a megkereső hatóság
 - illetékességi területén kívül kell valamely eljárási cselekményt elvégezni, illetve azt az ügyfél jogos érdeke vagy a költségtakarékosság indokoltá teszi;
 - feladatának ellátásához olyan adat vagy ténybeli ismeret szükséges, amely a megkeresett hatóság nyilvántartásából, illetve irataiból szerezhető meg;
 - feladatának ellátásához olyan irat vagy más bizonyíték szükséges, amely a megkeresett hatóságnál van, vagy onnan szerezhető meg.
- 8.2. A megkeresésben meg kell jelölni az adat, irat, vagy más bizonyíték felhasználásának célját, valamint azt, hogy a személyes adat beszerzésére törvény alapján vagy az ügyfél kérelmére és írásbeli hozzájárulásával kerül sor.
- 8.3. A megkeresett hatóság csak akkor tagadhatja meg a megkeresésben foglaltak teljesítését, ha az jogszabályba ütközik. Amennyiben a jogsegély nyújtására más szerv jogosult, a megkeresett hatóság a megkeresést haladéktalanul, de legkésőbb a megkeresés megérkezésétől számított öt napon belül e hatósághoz továbbítja, és erről egyidejűleg tájékoztatja a megkereső hatóságot.
- 8.4. Ha jogszabály ennél rövidebb határidőt nem állapít meg, a jogsegély iránti kérelmet 8 napon belül kell teljesíteni.

9. NEMZETKÖZI JOGSEGÉLY

- 9.1. Ha a Magyar Köztársaságnak valamely állammal közigazgatási jogsegélyegyezménye van, vagy annak hiányában az államok között viszonzossági gyakorlat áll fenn, vagy többoldalú nemzetközi szerződés ezt lehetővé teszi, továbbá az együttműködési megállapodás alapján az eljáró hatóság a belföldi jogsegélynél meghatározott jogsegély érdekében külföldi hatósághoz fordulhat, illetve - ha ez nem ütközik magyar jogszabályba - köteles teljesíteni a külföldről érkező jogsegélykérelmet.
- 9.2. A viszonzosság fennállása tekintetében a Külügyminisztérium állásfoglalása az irányadó, amelyet az érintett minisztériummal egyetértésben alakít ki.
- 9.3. Ha jogszabály vagy nemzetközi szerződés másként nem rendelkezik, a nemzetközi jogsegélyügyben érintett magyar és külföldi (nemzetközi) hatóság közvetlenül érintkezik egymással. Ha a magyar hatóság előtt nem ismert, hogy a jogsegélykérelem teljesítése az érintett külföldi állam melyik hatóságának hatáskörébe tartozik, a kérelmet felügyeleti

szervén keresztül a Külügyminisztériumhoz juttatja el. A Külügyminisztérium a külföldi állam külügyekben illetékes minisztériuma útján továbbítja a jogsegélykérelmet a külföldi hatósághoz.

- 9.4. Ha a külföldről érkező jogsegélykérelem teljesítésére nem a megkeresett hatóság jogosult, a megkeresést haladéktalanul, de legkésőbb az érkezéstől számított öt napon belül átteszi a hatáskörrel rendelkező illetékes hatósághoz, és erről a megkereső felet egyidejűleg tájékoztatja.
- 9.5. Unió jogi aktusa, nemzetközi szerződés és törvény felhatalmazást adhat az ügyben eljárni jogosult magyar és külföldi hatóság közötti együttműködési megállapodás létrehozására hatósági feladataik ellátásának kölcsönös előmozdítása érdekében.
- 9.6. Nemzetközi jogsegély keretében személyes adat továbbítására az Unió jogi aktusa, nemzetközi szerződés, illetve törvényi felhatalmazás vagy az érintett írásos hozzájárulása alapján kerülhet sor.
- 9.7. A hatóság - ha az Unió jogi aktusa vagy nemzetközi szerződés eltérően nem rendelkezik - megtagadja a külföldi megkeresés teljesítését, ha az sértené
 - a Magyar Köztársaság nemzetbiztonsági érdekeit vagy a közbiztonságot,
 - az ügyben érintett személy alapvető jogát,
 - a védett adat megőrzéséhez fűződő érdekeket, és annak továbbítását jogszabály nem teszi lehetővé, vagy a továbbításához a jogszabályban előírt feltételek nem állnak fenn.
- 9.8. A külföldi megkeresés teljesítésének megtagadásáról és annak okáról a megkereső felet haladéktalanul tájékoztatni kell.
- 9.9. A nemzetbiztonság vagy a közbiztonság veszélyeztetésének elbírálásához a hatóság szükség esetén az illetékes minisztérium, országos hatáskörű szerv állásfoglalását kéri.

10.KÖZVETLEN LEKÉRDEZÉS

- 10.1. Amennyiben az adatigénylő a személyes adatokat közvetlen lekérdezéssel kívánja átvenni, akkor az adatkezelő megvizsgálja, hogy adottak-e a feltételek a közvetlen hozzáférést biztosító rendszer biztonságos igénybevételére. A feltételek fennállásáról az adatigénylőtől előzetesen tájékoztatást kér.
- 10.2. A tájékoztatás-kérés mellőzhető, ha az adatigénylő olyan szervezethez tartozik, amelynek vezetője az adatkezelővel kötött előzetes együttműködési megállapodásban vállalta a szükséges biztonsági feltételek biztosítását a rendszerhez adatigénylőként csatlakozni kívánó szervek részéről.
- 10.3. A lekérdezést végző felelős azért, hogy kizárólag a lekérdezési engedélyben meghatározott adatokat hívja le, az adatokat a lekérdezési engedélyben meghatározott célra használja fel, továbbá gondoskodik a lekérdezett adatok biztonságos kezeléséről és arról, hogy részéről lekérdezéseket csak az általa feljogosított személyek végezhesenek.
- 10.4. Az adatigénylő szerv a lekérdezést végzőkről és az egyedi azonosítójukról naprakész nyilvántartást vezet. A nyilvántartás megőrzési ideje megegyezik az adattovábbítási nyilvántartás megőrzési idejével.
- 10.5. Az adatkezelőt haladéktalanul tájékoztatni kell a lekérdezést végző személyében bekövetkezett változásról.

- 10.6. A közvetlen hozzáférést biztosító rendszert úgy kell kialakítani, hogy a lekérdezés során minden adatigénylő csak a jogosultságának megfelelő adatokat érhesse el. A lekérdezést egyedi azonosító és jelszó megadásához kell kötni.
- 10.7. A lekérdezés szabályait nem kell alkalmazni a nyilvános személyes adatok számítástechnikai eszközzel, a nyilvánosság tájékoztatása céljából történő közzététele esetén.

11. TÁJÉKOZTATÁS HÍRKÖZLŐ ESZKÖZÖN

- 11.1. A nyilvántartott személyes adatokról hírközlő eszközön tájékoztatás csak a jogosult nyomozó hatóságok, nemzetbiztonsági szervek, honvédség szervei, valamint az adatkezelővel közös szervezetbe tartozó adatkezelők (társ-szervek) számára, szervezetszerűen működő ügyfélszolgálat vagy ügyeleti szolgálat által adható.
- 11.2. A fentiekől eltérni csak halaszthatatlan esetben, az élet, a testi épség és a vagyonbiztonság megóvása érdekében lehet.
- 11.3. A hívó azonosságáról jelszó alkalmazásával, visszahívással vagy más módon meg kell győződni. Ha a tájékoztatást igénylő azonossága nem állapítható meg, vagy a hívó az adatok megismerésére nem jogosult, akkor a tájékoztatás nem teljesíthető.
- 11.4. A tájékoztatást az adattovábbítások nyilvántartásának szabályai szerint a tájékoztatást adó ügyeletnél, illetve ügyfélszolgálatnál dokumentálni kell.

12. A HATÓSÁGI ELJÁRÁS IRATAIBA VALÓ BETEKINTÉS

- 12.1. Az ügyfél személyesen, illetve a törvényes vagy írásban meghatalmazott képviselője útján betekinthez az eljárás során keletkezett iratba, arról másolatot, kivonatot készíthet, vagy másolatot kérhet. Ez a jog akkor is megilleti, ha korábban nem vett részt az eljárásban.
- 12.2. Nem tekinthez be az ügyfél
 - a határozat (végzés) tervezetébe,
 - a zárt tanácskozásról készült jegyzőkönyvbe,
 - a tanú vagy a bejelentő természetes személyazonosító adatait tartalmazó jegyzőkönyvbe (iratba), ha a hatóság a tanú, illetve a bejelentő természetes személyazonosító adatait zártan kezeli,
 - betekintési vagy megismerési engedély hiányában az államtitkot vagy szolgálati titkot tartalmazó iratba,
 - a törvény által védett egyéb adatot tartalmazó iratba, ha azt az érintett adat védelmét szabályozó törvény kizárja, vagy ha a védett adat megismerésének hiánya nem akadályozza az e törvényben biztosított jogai gyakorlásában.
- 12.3. Az ügyfél az adatok konkrét megjelölésével kérheti az ellenérdekű ügyfél irat betekintési jogának kizárását személyes adatainak, valamint üzleti és más méltányolható magánérdekének védelmében. A jogi személy és a jogi személyiséggel nem rendelkező szervezet ügyfél az irat betekintési jog kizárását csak az üzleti érdekei védelmében kérheti. A hatóság a kérelemnek - a körülmények gondos mérlegelése alapján - akkor ad helyt, ha az adatok megismerésének hiánya az ellenérdekű ügyfelet nem akadályozza az e törvényben foglalt jogai gyakorlásában.

- 12.4. Az irat betekintési jog kizárása vagy korlátozása miatt önálló jogorvoslatnak csak akkor van helye, ha az ügyfél azt az eljárás jogerős lezárását követően kéri, vagy a hatóság azt, aki iratbetekintést kér, nem tekinti ügyfélnek.
- 12.5. A hatóság akkor engedheti meg az ügyfélen kívül az eljárásban részt nem vevő harmadik személynek az iratokba való betekintést, ha igazolja, hogy az irat megismerése joga érvényesítéséhez, illetve jogszabályon vagy hatósági határozaton alapuló kötelezettsége teljesítéséhez szükséges.
- 12.6. A harmadik személy a határozat (végzés) tervezetébe, a zárt tanácskozásról készült jegyzőkönyvbe, a tanú vagy a bejelentő természetes személyazonosító adatait tartalmazó jegyzőkönyvbe (iratba), ha a hatóság a tanú, illetve a bejelentő természetes személyazonosító adatait zártan kezeli, nem tekinthet be, az államtitkot vagy szolgálati titkot, vagy egyéb védett adatot tartalmazó iratot pedig csak az adat megismerésére vonatkozó törvényi feltételek igazolása esetén ismerheti meg.
- 12.7. A szakértő és a hatósági közvetítő az eljárási feladatainak ellátásához szükséges mértékben ismerheti meg az adatokat, a tanú pedig a vallomását tartalmazó jegyzőkönyvbe tekinthet be.
- 12.8. Ha a harmadik személy az iratbetekintés kizárását vagy korlátozását nem veszi tudomásul vagy vitatja, a hatóság arról öt napon belül önálló jogorvoslattal támadható végzésben rendelkezik.
- 12.9. Törvény egyes ügyfajtákban meghatározhatja az iratbetekintésre jogosult harmadik személyek körét.
- 12.10. A hatóság bárki számára hozzáférhetővé teszi azokat a döntéseket, amelyeket
 - állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy ügyfélnek e tevékenységével kapcsolatban hozott;
 - közérdekű keresetindítással meg lehet támadni;
 - az adott tevékenységgel összefüggésben a hatásterületen élő lakosság jelentős részét érintő ügyben hozott;
 - a fogyasztók, illetve a munkavállalók munkavédelmi, munkabiztonsági jogait közvetlenül érintő ügyben hozott;
 - az épített és természeti környezet, illetve a kulturális örökség állapotát jelentősen befolyásoló tevékenységgel kapcsolatos ügyben hozott;
 - korlátozottan rendelkezésre álló természeti erőforrások elosztásáról, illetve felhasználásáról hozott;
 - olyan ügyekben hozott, amelyekben az ügyfél számára kizárólagos vagy különleges jogot biztosított;
 - törvény rendelkezései szerint hozzáférhetővé kell tenni.

13.A SZEMÉLYES ADATOK TÖRLÉSE, HELYESBÍTÉSE

- 13.1. Az adatokat törölni - manuális nyilvántartás esetén megsemmisíteni - szükséges, ha
 - a) az adatkezelésre a jogszabályban előírt határidő eltelt;
 - b) az adatkezelés jogszerűtlensége megállapítást nyert;
 - c) a felhasználási cél teljesülését követően, ha azt az átdó külföldi fél kérte;
 - d) az érintett hozzájárulását írásban visszavonta, kivéve, ha törvény az adatok további kezelését lehetővé teszi;

- e) az adatkezelés célja megszűnt;
 - f) bírósági jogerős határozattal elrendelte.
- 13.2. Az érintett bejelentése vagy az adatkezelő által észlelt hibás adat esetén az adatkezelő a hibás adatot a helyesbítés elvégzéséig jelzéssel látja el.
- 13.3. A pontatlan, időszerűtlen adat csak a jelzéssel együtt és akkor továbbítható, ha az adatszolgáltatás az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti.
- 13.4. Ha a hibás adat nem helyesbíthető, akkor törölni kell. Amennyiben a törlés vagy a helyesbítés az adatok tárolási módja miatt nem lehetséges, akkor az adatot megfelelő, helyesbítő vagy figyelemfelhívó feljegyzés hozzáfűzésével véglegesen zárolni kell.
- 13.5. Ha az adat hibás volta annak továbbítása után derül ki, akkor ennek tényéről, illetve - amennyiben a hibás adatot az adatkezelő kijavította - a helyes adatról mindazokat tájékoztatni kell, akiknek az adatot továbbították. A tájékoztatás mellőzhető, ha ez az adat jellegére, az adatkezelés céljára, az időmúlásra, illetve az adatkezeléssel összefüggő más körülményeire tekintettel az érintett, illetve a korábbi adattovábbítás címzettjének jogos érdekét nem sérti.

14.ADATTOVÁBBÍTÁS

- 14.1. Személyes adatok akkor továbbíthatók harmadik szervnek vagy személynek, ha ahhoz az érintett írásban hozzájárult (szóbeli nyilatkozatát a hatóság írásba foglalta), vagy törvény elrendelte illetve a hozzájárulását a törvény vélelmezi, és ha az adatkezelés feltételei az adatot átvevő szervnél vagy személynél minden egyes adatra nézve teljesülnek.
- 14.2. Nem minősül adattovábbításnak és ezért az eljárási szabályoknak és az ügykezelési szabályzatban foglaltaknak megfelelően kell dokumentálni:
- a) az egy nyilvántartáson (nyilvántartási rendszeren) belül az egymással alá-, fölé- vagy mellérendeltségi kapcsolatban lévő szervek adatfeldolgozási célú adatátadását;
 - b) a megbízási szerződés alapján történő adatfeldolgozás céljára történő adatátadását;
 - c) az érintett saját adatairól történő tájékoztatását;
 - d) az Infotv. 26. § (2) bekezdésében szereplő személyes adatok bárki számára hozzáférhetővé tételét.

15.ADATTOVÁBBÍTÁSI NYILVÁNTARTÁS

- 15.1. Az adatkezelő a kezelt személyes adat továbbításáról nyilvántartást vezet, amely tartalmazza:
- a. az adattovábbítás célját, jogalapját, időpontját;
 - b. az adatigénylő azonosításához szükséges adatokat;
 - c. a továbbított adatfajták megnevezését.
- 15.2. Az adattovábbítási nyilvántartásban fel kell tüntetni az érintett tájékoztatására vonatkozó tiltást, amennyiben azt a nyilvántartás vezetésének módja lehetővé teszi és a tiltás az adattovábbítás előtt az adatkezelő tudomására jutott.
- 15.3. Az adatigénylő részéről eljáró személy személyazonosító adatait is nyilvántartásba kell venni, ha ezt az adatkezelésről rendelkező jogszabály előírja.
- 15.4. Az adattovábbítási nyilvántartás tartalmazza továbbá az adatkezelést elrendelő jogszabály által meghatározott egyéb adatokat.

- 15.5. Az adattovábbítási nyilvántartásba betekinhet, abból adatot igényelhet:
 - a. az adatvédelmi biztos, a bíróság, nyomozó hatóság, a nemzetbiztonsági szerv, törvényben meghatározott feladatai ellátásához,
 - b. az adatkezelő szerv vezetője, vagy az általa meghatalmazott személy.
- 15.6. Az adattovábbítási nyilvántartásba való betekintést, az abból történő adattovábbítást dokumentálni kell.

16.AZ ÉRINTETT JOGAI GYAKORLÁSÁNAK BIZTOSÍTÁSA

Az érintett kérelmezheti az adatkezelőnél

- 16.1 tájékoztatását személyes adatai kezeléséről,
- 16.2 személyes adatainak helyesbítését, valamint
- 16.3 személyes adatainak - a kötelező adatkezelés kivételével - törlését vagy zárolását.

17.A KÖZÉRDEKŰ ADATOK KEZELÉSE

- 17.1. A Hivatal a feladatkörébe tartozó ügyekben - így különösen az állami és önkormányzati költségvetésre és annak végrehajtására, az állami és önkormányzati vagyon kezelésére, a közpénzek felhasználására és az erre kötött szerződésekre, a piaci szereplők, a magánszervezetek és-személyek részére különleges vagy kizárólagos jogok biztosítására vonatkozóan - köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását.
- 17.2. Rendszeresen elektronikusan vagy más módon közzéteszi, továbbá erre irányuló igény esetén hozzáférhetővé teszi a tevékenységükkel kapcsolatos legfontosabb - így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésre, a birtokában lévő adatfajtákra és a működéséről szóló jogszabályokra, valamint a gazdálkodására vonatkozó - adatokat. A tájékoztatás módját, a vonatkozó adatok körét jogszabály is megállapíthatja.
- 17.3. A Hivatalnak lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot bárki megismerhesse, kivéve, ha az adatot törvény alapján az arra jogosult szerv állam- vagy szolgálati titokká nyilvánította, illetve ha az nemzetközi szerződésből eredő kötelezettség alapján minősített adat, továbbá, ha a közérdekű adatok nyilvánosságához való jogot - az adatfajták meghatározásával – törvény honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi vagy devizapolitikai érdekből, külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra, bírósági vagy közigazgatási hatósági eljárásra tekintettel korlátozza.
- 17.4. Ha törvény másként nem rendelkezik, közérdekből nyilvános adat a Hivatal feladat- és hatáskörében eljáró személy feladatkörével összefüggő személyes adata (pl. név, besorolás), továbbá egyéb, közfeladatot ellátó személy e feladatkörével összefüggő személyes adata. Ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni.

- 17.5. Ha törvény másként nem rendelkezik, közérdekből nyilvános adat a jogszabály vagy állami, illetőleg helyi önkormányzati szervvel kötött szerződés alapján kötelezően igénybe veendő vagy más módon ki nem elégíthető szolgáltatást nyújtó szervek vagy személyek kezelésében levő, e tevékenységükre vonatkozó, személyes adatnak nem minősülő adat.
- 17.6. A közérdekű adatok megismerésével és nyilvánosságával összefüggésben az üzleti titok megismerésére a Polgári Törvénykönyvben foglaltak az irányadók.
- 17.7. A közérdekű adatok nyilvánosságát korlátozhatja, továbbá az Európai Unió jogszabálya az Európai Unió jelentős pénzügy- vagy gazdaságpolitikai érdekére tekintettel, beleértve a monetáris, a költségvetési és az adópolitikai érdeket is.
- 17.8. A Hivatal kezelésében lévő, döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ezen adatok megismerését a jegyző engedélyezheti.
- 17.9. A döntés megalapozását szolgáló adat megismerésére irányuló igény - az előző bekezdésben meghatározott időtartamon belül - a döntés meghozatalát követően akkor utasítható el, ha az adat megismerése a Hivatal törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné.
- 17.10. Jogszabály egyes adatok megismerhetőségének korlátozására rövidebb időtartamot állapíthat meg.
- 17.11. A közérdekű adat megismerése iránt bárki - szóban, írásban vagy elektronikus úton - igényt nyújthat be.
- 17.12. A közérdekű adat megismerésére irányuló igénynek a Hivatal az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül tesz eleget.
- 17.13. Az adatokat tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül az igénylő másolatot kaphat. A Hivatal kizárólag a másolat készítéséért - legfeljebb az azzal kapcsolatban felmerült költség mértékéig terjedően - állapíthat meg költségtérítést, amelynek összegét az igénylő kérésére előre közölni kell.
- 17.14. Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni.
- 17.15. Az adatigénylésnek közérthető formában és - amennyiben az aránytalan költséggel nem jár - az igénylő által kívánt technikai eszközzel, illetve módon kell eleget tenni. Az adatigénylést nem lehet elutasítani arra való hivatkozással, hogy annak közérthető formában nem lehet eleget tenni.
- 17.16. Az igény teljesítésének megtagadásáról, annak indokaival együtt, 8 napon belül írásban vagy - amennyiben az igényben elektronikus levelezési címét közölte - elektronikus úton értesíteni kell az igénylőt.
- 17.17. A közérdekű adat megismerése iránti igény teljesítése nem tagadható meg azért, mert a nem magyar anyanyelvű igénylő az igényét anyanyelvén vagy az általa értett más nyelven fogalmazza meg.
- 17.18. A Hivatal évente értesíti az adatvédelmi biztost az elutasított igényekről, valamint az elutasítások indokairól.
- 17.19. A Hivatal a közzétett adatok megismerését személyazonosító adatok közléséhez nem kötheti. Az elektronikusan közzétett közérdekű adatokhoz történő hozzáférés biztosításához személyes adat csak annyiban kezelhető, amennyiben az technikailag elengedhetetlenül szükséges; a személyes adatokat ezt követően haladéktalanul törölni kell.
- 17.20. Igénylés alapján történő adatszolgáltatás esetén az adatigénylő személyazonosító adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges

költségek megfizetését is - elengedhetetlenül szükséges. Az igény teljesítését, illetőleg a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell.

17.21. Törvény ettől eltérően rendelkezhet.

17.22. E fejezet rendelkezései nem alkalmazhatók a közhitelű nyilvántartásból történő - külön törvényben szabályozott - adatszolgáltatásra.

18. TITOKTARTÁSI KÖTELEZETTSÉG

18.1. A Hivatallal közszolgálati, közalkalmazotti, vagy más munkavégzésre irányuló jogviszonyban lévő személyek kötelesek jelen adatvédelmi és adatbiztonsági szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, illetve tudomásukra jutott titkokat megőrizni. Kizárólag a munkaköri leírásban meghatározott feladatkörükön belül ismerhetik meg az ilyen titkokat.

19. ELJÁRÁSI SZABÁLYOK

19.1. A Hivatalhoz érkező, személyes adatokkal kapcsolatos igényeket, jogorvoslati kérelmeket haladéktalanul továbbítani kell a jegyzőnek

19.2. A jegyző a kérést megvizsgálja az abban foglaltakat teljesíti, vagy elutasítja az igényt.

19.3. A jegyző kiadmányozza a dokumentumot.

19.4. A jegyző és közérdekű adattal kapcsolatos igények elutasításáról, annak időpontjáról és okáról nyilvántartást vezet.

19.5. A jegyző minden év nyilvántartását a következő év január 15. napjáig megküldi az Adatvédelmi Biztos irodájának.

Pap-SzabóKatalin
jegyző

ZÁRADÉK:

Jelen Szabályzat 2017. október 01. napján lép hatályba ugyanezen a napon a 2/2008 számú Adatvédelmi szabályzat hatályát veszti