

Tiszaföldvár Város Jegyzője

3/2009. számú Utasítás

Tiszaföldvár Város Önkormányzata Képviselőtestületének Hivatala (Polgármesteri Hivatal) Adatvédelmi és Adatbiztonsági Szabályzatáról

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 31/A. § (3) bekezdésére tekintettel kiadom az alábbi

u t a s í t á s t.

- 1./ Az Adatvédelmi és Adatbiztonsági Szabályzatot /továbbiakban: Szabályzat/ ezen utasítás mellékleteként bocsátom ki.
- 2./ Az utasítás hatálya kiterjed a Tiszaföldvár Város Polgármesteri Hivatalban (továbbiakban: Hivatal) folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz. Az utasítás hatálya vonatkozik továbbá a Hivatal adatkezelésben és adatfeldolgozásban részt vevő munkavállalóira, valamint a polgármesterre.
- 3./ Az utasítás célja annak biztosítása, hogy a személyes adatokat megfelelő védelemben részesüljenek, valamint a közérdekű adatokat mindenki megismerhesse.
- 4./ Ez az utasítás 2009. július 3. napján lép hatályba. A Szabályzat rendelkezéseit a hatályba lépés napjától - a folyamatban lévő ügyekre is kiterjedően - kell alkalmazni.
- 5./ Az utasítást valamennyi munkavállalóval egyszerű kézbesítéssel közölni kell. A Szabályzatot közölni kell továbbá Tiszaföldvár Város Polgármesterével.

Tiszaföldvár, 2009. július 2.

**/: Hajós Attiláné Dr. Szlama Katalin :/
címzetes főjegyző**

TISZAFÖLDVÁR VÁROS POLGÁRMESTERI HIVATAL

5430 TISZAFÖLDVÁR, BAJCSY ZS. ÚT 2.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

2009.

I. BEVEZETŐ RENDELKEZÉSEK

1. A szabályozás célja

A szabályozás célja, hogy – amennyiben jogszabály kivételt nem tesz – személyes adatával mindenki szabadon rendelkezessen, a közérdekű adatokat pedig mindenki megismerhesse. A nyilvántartott személyes adatok védelme érdekében olyan technikai, szervezési intézkedések, ellenőrzési rendszerek kerüljenek kialakításra, melyek biztosítják az adatvédelmi követelmények teljesítését. A szabályozás további célja, hogy biztosítsa a személyes, a közérdekű és a közérdekből nyilvános adatok biztonságos védelmét, az informatikai feldolgozás és tárolás feltételeit.

2. Kapcsolódó jogszabályok

- a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Atv.),
- a statisztikáról szóló módosított 1993. évi XLVI. törvény,
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (továbbiakban: Nytv.),
- a közpénzek felhasználásával, a köztulajdon használatának nyilvánosságával, átláthatóbbá tételével és ellenőrzésének bővítésével összefüggő egyes törvények módosításáról szóló 2003. évi XXIV. törvény,
- az elektronikus információszabadságról szóló 2005. évi XC. Törvény
- a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.)
- az államháztartás működési rendjéről szóló 217/1998.(XII.30.) Korm. rendelet.
- a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII. 25.) Korm. rendelet
- a közzétételi listákon szereplő adatok közzétételéhez szükséges közzétételi mintákról szóló 18/2005. (XII. 27.) IHM rendelet

3. 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 tenyérynymat, 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) különleges adat:

a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra,

b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat;

h) 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;

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

j) 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;

k) adatigénylő: az érintett kivételével az a szerv vagy személy, akinek a részére az adatkezelő jogszabály kötelezése vagy kérelem teljesítése alapján adatokat szolgáltat, továbbit vagy átad;

l) adat zárolása: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;

m) érintett: az a természetes személy, akinek személyes adata az adatkezelés tárgyát képezi,

n) adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik, ez alatt értve az adat kiadására irányuló adatszolgáltatást, vagy adatátadás iránti kérelem teljesítését is;

o) 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;

ö) 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) nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

- s) adattörlés:* az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
- sz) adatmegsemmisítés:* az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;
- t) adatállomány:* az egy nyilvántartó rendszerben kezelt adatok összessége;
- ty) 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;
- u) személyes adatállomány:* személyes adatok rendszerezett, állandó vagy változtatott összessége, mely a tartalmazott adatfajták szerint rendezhető, válogatható, kiértékelhető;
- v) 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;
- z) hivásbéli titok:* különösen az orvosi, ügyvédi, közjegyzői, lelkészi-egyházi személyi hivásbéli titok;
- zs) törvény által védett titok:* az államtitok, a szolgálati titok, továbbá az üzleti, a bank-, a biztosítási, az értékpapír-, a pénztártitok, valamint a magántitok.

4. Adatkezelő neve, székhelye

Adatkezelő neve: Tiszaföldvár Város Polgármesteri Hivatal (továbbiakban: Hivatal)
Székhelye: 5430 Tiszaföldvár, Bajcsy Zs. út 2.

II. AZ ADATVÉDELEM SZERVEZETE

5. Az adatvédelem szervezete

- 5.1 A Hivatalban kezelt személyes adatok védelméről és a Hivatal tevékenységére vonatkozó közérdekű és közérdekből nyilvános adatok nyilvánosságáról szóló jogszabályi előírások betartásáról a jegyző, az aljegyző, a szervezeti egységek vezetői, valamint a hivatal minden munkatársa köteles gondoskodni.
- 5.2 A Hivatal informatikai hálózatának üzemeltetéséről (ideértve a hardver eszközök karbantartásával, a szoftver hibák elhárításával, az informatikai hálózat külső behatolás elleni védelmével, a hálózati meghibásodás elhárításával kapcsolatos teendőket) a Hivatal rendszergazdája gondoskodik.

6. A jegyző adatvédelmi feladatai

- meghozza az adatkezeléssel összefüggő döntéseket, valamint biztosítja az érintettek jogait,
- ellenőrzi az Atv. és az adatkezelésre vonatkozó más jogszabályok, valamint a Szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását,
- kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelő vagy az adatfeldolgozót,
- jogosult az előírásokat megsértőkkel szemben felelősségre vonási eljárást kezdeményezni,

- ellenőrzi a számítógépes programokat, valamint az archivált adatokat tartalmazó számítástechnikai adathordozók nyilvántartását és tárolását,
- koordinálja az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítását, módosításait,
- kezeli az adatvédelmi szabályzatot, gondoskodik annak naprakészen tartásáról, illetve a módosítások átvezetéséről,
- ismerteti a Hivatal dolgozóival az adatvédelmi követelményeket, szükség esetén oktatást szervez,
- ellenőrzi az adatvédelmi szabályzatban foglalt rendelkezések betartását.

7. Az aljegyző feladatai

Az aljegyző a jegyző távolléte esetén helyettesítési jogkörben ellátja a jegyző feladatkörébe tartozó valamennyi feladatot, valamint azok közül azokat, amelyekkel a jegyző megbízza.

8. A szervezeti egységek vezetői az adatvédelmi rendelkezések betartása érdekében

- biztosítják, hogy a Hivatal általuk irányított munkatársai betartsák az Atv. és a Szabályzat rendelkezéseit,
- a jegyző rendelkezésére bocsátják azokat a Hivatal tevékenységét érintő és munkakörükkel kapcsolatos közérdekű adatokat, amelyeket az Atv. 19. § (2) bekezdése szerint közzé kell tenni,
- A jegyző egyetértésével intézkednek a szerv tevékenységével kapcsolatos közérdekű adatok közzétételéről.

9. A Hivatal munkatársai az adatvédelmi szabályok betartása során

- gondoskodnak az általuk felvett és kezelt adatok jellegének beazonosításáról, tartalmának helyes rögzítéséről és azok védelméről,
- napközben esetleges hiba észlelésekor értesítik a jegyzőt és a rendszergazdát,
- lemezmozgások, CD/DVD adathordozón, pendrive-on tárolt adatok mozgatása során minden alkalommal elvégzik a vírusellenőrzést.

10. A Hivatal rendszergazdája

- ellátja a Hivatal informatikai hálózatának szakmai felügyeletét. Feladata a rendszerek működése során keletkezett esetleges hibák kijavítása.
- felelős a számítástechnikai rendszer üzembiztonságáért, szervezi a hardver eszközök rendszeres karbantartását,
- folyamatosan figyelemmel kíséri a veszélyforrások körében bekövetkezett változásokat, szükség esetén intézkedést kezdeményez,
- szükség esetén gondoskodik a rendszer újraindításáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- folyamatosan ellenőrzi a védelmi eszközök működését,
- a vírusinformációk naprakészen tartása érdekében folyamatosan kapcsolatot tart a vírusvédelemmel foglalkozó szervezetekkel, javaslatot tesz a velük való együttműködésre,
- a vírusfertőzés gyanúja eseték gondoskodik a feltételezett fertőzött rendszer izolálásáról, a fertőzés okának felderítéséről, a vírusmentes generálásról,

- gondoskodik arról, hogy minden számítógépen és a hálózatokon automatikus vírusellenőrzés működjön,
- gondoskodik az eredeti programot és a biztonsági másolatot tartalmazó adathordozó biztonságos őrzéséről,
- ellenőrzi a vásárolt szoftverek helyes működését, a használat jogszerűségét,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működését és annak biztonságát, ellenőrzi a rendszer saját adminisztrációját, javaslatot tesz a rendszer bővítésére, fejlesztésére,
- az egyedi alkalmazást használó szervezeti egység vezetőjével egyeztetett időpontban az adatbázisról biztonsági másolatot készít (szerverre, winchesterre vagy CD-re). Az archivált adatokat nyilvántartásba veszi és gondoskodik biztonságos őrzésükről. A fenti feladatok ellátása a szervezeti egységek kijelölt munkatársainak feladata,
- a Hivatal adatszerverén létrehozott „Átadás” nevű mappa adatok átadására szolgál. Az itt található adatok évente két alkalommal – előzetesen közölt időpontban – törlésre kerülnek,
- Az adatszerver további helyein lévő adatok archiválásáról a Hivatal munkatársai gondoskodnak, az archiválás technikai lebonyolításában a rendszergazda/informatikus segítséget nyújt,
- a közös könyvtárakba mentett adatokat évente megvizsgálja és a fölöslegessé vált adatokat törli. Az adatokat igény szerint frissíti.

III. ADATVÉDELEM, ADATBIZTONSÁG

11. Adatkezelőre és adatkezelésre vonatkozó általános szabályok

11.1 Az adatvédelmi szabályok betartásáért az adatkezelő a felelős. Az adatkezelő szerv dolgozója az adatvédelmi és adatbiztonsági szabályok betartásáért személyes felelősséggel tartozik.

11.2 Amennyiben az adatkezelő az adatkezelést adatfeldolgozóval végezteti, az adatbiztonsági szabályok betartásáért - a tevékenység végzésére vonatkozó szerződésben foglaltak szerint - az adatfeldolgozó szerv vezetőjét terheli felelősség.

11.3 Az adatkezelő személyes adatokat az Atv. 3. §-ban meghatározott felhatalmazás alapján kezelhet.

11.4 A technikai adatállomány külön felhatalmazás nélkül kezelhető.

12. Adatvédelem a hatósági eljárás és szolgáltatás során

12.1 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.

12.2 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.

- 12.3 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.
- 12.4 Nem tekinthet 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.
- 12.5 Az ügyfél az adatok konkrét megjelölésével kérheti az ellenérdekű ügyfél iratbetekintési jogának kizárását személyes adatainak, valamint üzleti és más méltányolható magánérdekének védelmében. A jogi személy és a jogi személyiséggel nem rendelkező szervezet ügyfél az iratbetekintési 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.
- 12.6 Az iratbetekintési 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.
- 12.7 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.
- 12.8 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.
- 12.9 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.

12.10 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.

12.11 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.

12.12 Az adat védelmére vonatkozó szabályok megtartása nem vezethet a jogorvoslathoz való jog korlátozásához.

12.13 A hatóság – hatáskörének keretei között – jogosult a feladatai ellátásához szükséges, jogszabályban meghatározott védett adat, továbbá törvényben meghatározott esetben személyes adat megismerésére és kezelésére.

12.14 Hivatalból indított vagy folytatott eljárásban korlátozó rendelkezés hiányában az ügyfél nem akadályozhatja a hatóságot a tényállás tisztázásához szükséges más iratok átvizsgálásában.

12.15 A hatóság az eljárás során a birtokába került védett adatot, 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.

13. Informatikai adatbiztonság

13.1 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.

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

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

13.2 A Hivatalnál az információ-rendszer védelmének fenntartásának és működtetésének felelőse: Baczúr István szervezési, személyzeti és munkaügyi osztályvezető.

13.3 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.

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

13.5 A Hivatalban a rendszer megtervezéséért és fejlesztéséért felelős rendszerirányító: Baczúr István szervezési, személyzeti és munkaügyi osztályvezető.

13.6 Feladatai:

a) figyelemmel kíséri, hogy az irányított információrendszer tekintetében a biztonsági fokozatnak megfelelő védelmi és biztonsági módszerek megtervezésre és alkalmazásra kerüljenek;

b) ellenőrzi a védelmi és biztonsági szabályok gyakorlati érvényesülését, és szükség szerint intézkedik a hiányosságok felszámolására, ezen belül a felelős vezetőnek javaslatot tesz a szervezeti és működési feltételek és követelmények biztosítására, szükség esetén a személyes felelősségre vonásra;

13.7 A Hivatalban a rendszer informatikai működőképességéért és a jogosultságok érvényesítéséért felelős rendszergazda: Szabó Ferenc informatikus

- 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;

13.8 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.

13.9 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, elcserélésük vagy meghibásodásuk kiküszöbölhető legyen.

h) A hozzáférés jelszavait időközönként, az üzemeltető személyének megváltozása esetén haladéktalanul, de legkésőbb 24 órán belül meg kell változtatni. Jelszót ismételten nem lehet kiadni.

i) A számítástechnikai eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható.

13.10 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 előírás szerű 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.

13.11 Bekapcsolt berendezéseket felügyelet nélkül hagyni tilos. A napi munka végeztével a számítógépet(ek) áramtalanítani kell, az adathordozókat, dokumentációkat biztonsági zárral ellátott tűzbiztos szekrényben kell tárolni.

13.12 Amennyiben a számítógépet használó munkatárs hosszabb időre elhagyja a helyét, úgy az általa használt számítógépet kikapcsolja, vagy zárolt állapotba helyezi az illetéktelen hozzáférések elkerülése érdekében. Minden dolgozó csak a saját felhasználónévvel, jelszavával léphet be a hálózatba.

- 13.11 A számítástechnikai eljárás során keletkezett munkapéldányt, vagy egyéb okból feleslegessé vált példányokat meg kell semmisíteni.
- 13.12 A Hivatalban csak jogtisztá számítógépes programot szabad futtatni. Minden programról biztonsági másolatot kell készíteni, majd az eredeti adathordozót írásvédetté kell tenni. Program telepítési joga kizárólag a rendszergazdának, illetve a szállítónak van.
- 13.13 Vírusellenőrzés nélkül floppyt vagy más adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni tilos.
- 13.14 A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni
- 13.15 Az adatállományok módosítása kizárólag a feldolgozásra készült programmal végezhető el.
- 13.16 A számítógép- vagy programhibából adódó adatvesztés esetén az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülése érdekében a rendszergazda segítségét kell kérni.
- 13.17 A számítógépeken tárolt információk biztonságos megőrzése céljából az adatokról biztonsági másolatot kell készíteni.
- 13.18 A munkaállomások saját könyvtáraiba mentett adatok gondozásáért a felhasználók felelősek.
- 13.19 A hozzáférés védettségét az operációs rendszer és a felhasználói programok védelmi rendszere biztosítja.
- A hálózat supervisor jelszavát a rendszergazda határozza meg, az azt tartalmazó iratot zárt, lepecsételt borítékban, a 12. számú irodában elhelyezett tűzbiztos lemezszekrényben tárolják.
 - A munkaállomások felhasználói jelszavait a rendszergazda határozza meg.
 - Ha bármilyen okból (pl. számítógép meghibásodása, leíró távolléte) fel kell törni egy jelszót tartalmazó borítékot, akkor a felhasználónak új jelszót kell biztosítani.
- 13.20 Az adathordozók érzékenyek, így óvni kell a közvetlen hő-, por-, víz-, fényhatásoktól, a fizikai sérüléstől, ezért használat közben óvakodni kell a mágneses réteg megérintésétől, használata után pedig zárható dobozban vagy gyári csomagolásban elektromos erőterektől (monitor, televízió, hangszóró, hűtőszekrény, mikrohullámú sütő), szennyeződésektől távol kell tartani. A vírust tartalmazó, attól nem mentesíthető adathordozót és a hibás floppykat, CD-ket, DVD-ket selejtezésig elkülönítetten kell tárolni.

14. Informatikai hibaelhárítás

- 14.1 Az informatikai hálózat meghibásodása esetén a meghibásodás okának és helyének megjelölésével azonnal értesíteni kell a jegyzőt, valamint a rendszergazdát.
- 14.2 A beavatkozásig az addig el nem mentett állományokat, felhasználásokat – amennyiben arra lehetőség van – el kell menteni. A meghibásodás elhárítását követően fel kell mérni a

meghibásodás eredményeként bekövetkezett adatok és állományok sérülését, az adatvesztést. A teljes informatikai hálózat újraindítását követően – amennyiben adatvesztés történt – az utolsó mentett állományt kell visszatölteni.

14.3 Helyreállítást és újraindítást követően belső szervezeti egységek vezetői határozzák meg – a munkafolyamatokra figyelemmel – a szervezeti egységen belüli az egyes szoftverek, valamint munkaállomások és hozzáférések helyreállításának sorrendjét.

15. Papíralapú, adatot hordozó eszközön nyilvántartott adatok védelme

15.1 Az ügyiratokat a Hivatal Iratkezelési Szabályzatában előírtak szerint kell kezelni és tárolni. Az ügyiratok kezelése tárolása során arra jogosulatlan személy azokba nem tekinthet be. Ezért a kijelölt ügyintéző, s minden – az ügyirattal kapcsolatba kerülő – köztisztviselő felelősséggel tartozik. A tárolási idő alatt bármilyen adatkezelési eseményről írásos feljegyzést kell készíteni. Az irat típusától függően az irattári jel határozza meg a tárolási időt, melynek lejártá után – a nem selejtezhető iratok kivételével – az iratot selejtezni kell, vagy a Levéltárnak kell átadni. Az ügyiratok tárolási idejének lejártá után az adatokat tartalmazó papírokat úgy kell megsemmisíteni, hogy az azon szereplő személyes adatok felismerhetetlenek – töröltnek tekinthetők – legyenek.

15.2 A Hivatalban az érintett kérelmére induló hatósági ügyintézés során az ügyintéző köteles az érintett figyelmét felhívni arra a tényre, hogy a kérelmére indult eljárásban a személyes adatainak kezeléséhez való hozzájárulást a törvény szerint vélelmezni kell.

15.3 A különleges adatok kezeléséhez az ügyfél hozzájárulását nyilatkozattal kell kikérni, kivéve, ha a hozzájárulását illetve a különleges adatát írásbeli beadványban maga az ügyfél közölte.

15.4 Az ügyintézés során csak azokat a személyes, vagy különleges adatokat szabad felvenni, amelyek az ügy szempontjából feltétlenül szükségesek. A felvett adatokat csak az adott ügy intézése érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal nem kapcsolhatók össze.

15.5 Az adatminőség biztosítása céljából személyes adatot csak az ügyfél személyének azonosítására alkalmas és érvényes hatósági igazolványból, különleges adatot az ügyfél írásos hozzájárulása szerint szabad felvenni.

15.6 A papíralapú fogalmazványban és a számítógépen rögzített személyes és különleges (a továbbiakban: személyes) adatokat, amennyiben céljukat betöltötték, további felhasználásuk megakadályozása érdekében felismerhetetlenné kell tenni (papíralapú adathordozó megsemmisítése, számítástechnikai adathordozóból a teljes kiadmánytervezetek, vagy azokból a személyes adatok törlése).

15.7 Személyes adatokat is tartalmazó iratot a Hivatalból kivinni csak ügyintézőnek, csak hatósági eljárás során - helyszíni szemle, környezettanulmány stb. céljából - a szervezeti egység vezetőjének engedélyével lehet. Az ügyintéző ez esetben is köteles gondoskodni arról, hogy tartalmát illetéktelen személy ne ismerhesse meg. Az iratok, illetve az adatok telefonon, faxon, e-mailben csak a Hivatal vonalainak, számítógépeinek igénybevételével továbbíthatók.

- 15.8 Az iratokba való betekintés és másolat készítése során biztosítani kell a személyes adatok védelmét. A sokszorosításra kiadott képviselőtestületi és bizottsági előterjesztések védelmét is biztosítani kell, hogy azok tartalmát jogosulatlan személyek ne ismerhessék meg.
- 15.9 A Hivatal munkatársai soron kívül kötelesek teljesíteni az érintettnek azt a kérelmét, amely a személyes adatai kezelésére vonatkozó tájékoztatásra, vagy az adatainak helyesbítésére, törlésére irányul.
- 15.10 A képviselőtestület és a bizottságok üléseiről készült jegyzőkönyvek közül a zárt ülések jegyzőkönyveit és az azokról készült hangfelvételeket elkülönítetten kell kezelni, amelyért a Szevezési, Személyzeti és Munkaügyi Osztály vezetője a felelős.
- 15.11 Azon helyiségeket, ahol személyes adatokat is tartalmazó ügyiratok kezelése folyik, munkaidőn kívül, továbbá munkaidőben, ha az ügyintéző nem tartózkodik az irodában, zárva kell tartani.
- 15.12 A tűzrendészeti előírásokat be kell tartani. Ennek érdekében gondoskodni kell oltókészülék felszereléséről.

16. Az adatok tárolása

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.

17. Az adatok felhasználása

- 17.1 Az adatok a jogszabályban meghatározott célra használhatók fel.
- 17.2 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.
- 17.3 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 igénybevételét, az adattovábbítások nyilvántartásának adattartalmát és megőrzési idejét figyelembe véve dokumentálni kell.
- 17.4 Számítástechnikai, távközlési eszközök és programok helyességének ellenőrzésére, felhasználók betanítására, illetve oktatási célra valós személyi adatokat felhasználni nem lehet.

18. Közvetlen lekérdezés

- 18.1 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.

- 18.2 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.
- 18.3 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.
- 18.4 Az adatigénylő szerv a lekérdezést végzőkről és az egyedi azonosítójukról naprakész nyilvántartást vezet. A nyilvántartás megőrzési ideje megegyezik az adattovábbítási nyilvántartás megőrzési idejével.
- 18.5 Az adatkezelőt haladéktalanul tájékoztatni kell a lekérdezést végző személyében bekövetkezett változásról.
- 18.6 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.
- 18.7 A lekérdezés szabályait nem kell alkalmazni a nyilvános személyes adatok számítástechnikai eszközzel, a nyilvánosság tájékoztatása céljából történő közzététele esetén.

IV. A SZEMÉLYES ADATOK VÉDELME

19. Személyes adatok célhoz kötöttsége

- 19.1 Személyes adat akkor kezelhető, ha az érintett, akinek személyes adatát kezelik, ehhez hozzájárul vagy a törvény, illetőleg – törvény felhatalmazása alapján, az abban meghatározott körben – az önkormányzat rendelete elrendeli. A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait – ha a törvény kivételt nem tesz – az adatkezeléshez fűződő más érdekek (ide értve a közérdekű adatok nyilvánosságát) nem sérthetik. Az érintett hozzájáruló nyilatkozata nem – illetve csak kifejezett szándéka, beleegyezése esetén – terjed ki arra, hogy személyi adatait más tudomására hozzák.
- 19.2 Személyes adatot kezelni csak meghatározott célból, jogi gyakorlása és kötelezettség teljesítése érdekében lehet, e cél érvényre jutását az adatkezelés minden fázisában biztosítani kell. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, s a cél megvalósulásához szükséges mértékben és ideig.

19.3 Az érintettel az adat felvétele előtt közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályhelyet. Az érintett kérelmére indult eljárásban a szükséges adatoknak kezeléséhez való hozzájárulását vélelmezni kell.

20. Az érintettek jogai

20.1 Az érintett kérheti adatainak helyesbítését, illetve – jogszabály által elrendelt adatkezelés kivételével annak törlését is. A valóságnak nem megfelelő adatot – ellenőrzési eljárás lefolytatása után – az adatkezelő helyesbíteni köteles. Ha az adat helyesbítése nem lehetséges, vagy az adatkezelő az adatot törvényes felhatalmazás, illetve az érintett hozzájárulása nélkül kezeli, akkor az adatot törölni, illetve véglegesen zárolni kell.

20.2 Az érintett és képviselője az eljárás során keletkezett iratokba betekinthez, és azokról másolatot készíthet. Nem lehet betekíteni, illetve másolatot készíteni az alábbi iratokról:

- a.) határozatok tervezetei,
- b.) ellenőrzési feljegyzések
- c.) államtitkot, szolgálati titkot.

20.3 Az érintett tájékoztatást kérhet személyes adatainak kezeléséről, annak céljáról, jogalapjáról, továbbá arról, hogy kik és milyen célból kapták (kapják) meg az adatokat. Az adatkezelő köteles a tájékoztatásra vonatkozó kérelem benyújtásától számított legrövidebb idő alatt (legfeljebb azonban 30 napon belül) írásban, közérthető formában megadni a tájékoztatást.

20.4 A tájékoztatást csak a honvédelem, a nemzetbiztonság, bűnmegelőzés vagy bűnüldözés érdekében, továbbá állami, vagy önkormányzati pénzügyi érdekből, valamint az érintett vagy mások jogainak védelme érdekében tagadható meg. Az adatkezelő köteles az érintettel a felvilágosítás megtagadásának indokát közölni.

21. A személyes adat módosítása, törlése

21.1 Személyes adatok helyesbítése és törlése csak a törvényben meghatározott eljárással végezhető el. A helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adat adatkezelés céljából továbbításra került. Az értesítés mellőzhető, ha ez – az adatkezelés céljára való tekintettel – az érintett jogos érdekét nem sérti. A helyesbítési, törlési kérelmet érdemben meg kell vizsgálni és amennyiben az megalapozott, a helyesbítést, törlést teljesíteni kell, attól függetlenül, hogy az érintett tájékoztatható-e az eljárás eredményéről. Az érintett adatainak helyesbítésére, illetve törlésére irányuló eljárásra az Atv. és a Ket. rendelkezéseit kell alkalmazni. A kijavításról és a törlésről az érintettet és az Atv. 15. § szerinti szerveket az ott meghatározottak szerint, az Atv. 16. §-ára is figyelemmel kell értesíteni.

21.2 A személyes adatot törölni kell, ha:

- kezelése jogellenes,
- az érintett – az Atv. 11. § (1) bekezdésének b) pontjában foglaltak szerint – kéri,
- az adat hiányos vagy téves – és ez az állapot jogszerűen nem korrigálható -, feltéve, hogy a törlést törvény nem zárja ki,

- az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt,
- azt a bíróság vagy az adatvédelmi biztos elrendelte.

22. Adatszolgáltatás külső szervezetnek

A Hivatal más szerv és természetes személy részére adatot csak jogszabályban meghatározott módon szolgáltatathat. A külső szervektől érkező megkeresésekben rögzíteni kell az adatkezelésre való jogosultságot, valamint az adatkezelés célját. 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.

23. Adattovábbítás

23.1 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 (Atv. 5-10. §§) az adatot átvevő szervnél vagy személynél minden egyes adatra nézve teljesülnek.

23.2 Nem minősül adattovábbításnak és ezért az eljárási szabályoknak és az ügykezelési szabályzatban foglaltaknak megfelelően kell dokumentálni:

- az egy nyilvántartáson (nyilvántartási rendszeren) belül az egymással alá-, fölé- vagy mellérendeltségi kapcsolatban lévő szervek adatfeldolgozási célú adatátadást;
- *b)* a megbízási szerződés alapján történő adatfeldolgozás céljára történő adatátadását;
- *c)* az érintett saját adatairól történő tájékoztatását;
- *d)* az Atv. 19. § (2) bekezdésében szereplő személyes adatok bárki számára hozzáférhetővé tételét.

24. Adattovábbítási nyilvántartás

24.1 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.

24.2 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.

24.3 Az adatigénylő részéről eljáró személy személyazonosító adatait is nyilvántartásba kell venni, ha ezt az adatkezelésről rendelkező jogszabály előírja.

24.4 Az adattovábbítási nyilvántartás tartalmazza továbbá az adatkezelést elrendelő jogszabály által meghatározott egyéb adatokat.

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

V. KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA

25. A közérdekű adatok nyilvánossága

- 25.1 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.
- 25.2 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.
- 25.3 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.
- 25.4 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.
- 25.5 A közérdekű adatok megismerésével és nyilvánosságával összefüggésben az üzleti titok megismerésére a Polgári Törvénykönyvben foglaltak az irányadók.
- 25.6 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.

25.7 Jogszabály egyes adatok megismerhetőségének korlátozására rövidebb időtartamot állapíthat meg.

26. A közérdekű adatok közzététele

26.1 A Hivatal feladatkörében eljáró személyek neve és beosztása bárki számára hozzáférhető, nyilvános adat.

26.2 A Hivatalról a hiteles, pontos és gyors tájékoztatást saját kezdeményezéssel, továbbá szükséges felvilágosításokkal, valamint adatoknak a sajtó rendelkezésére bocsátásával kell elősegíteni.

26.3 A tájékoztatás általános formái: sajtótájékoztatók, fórumok tartása, interjúk adása, Internetes megjelenés, tájékoztató kiadványok. Általános tájékoztatási joggal a jegyző rendelkezik.

24. Közérdekű adatok kérelemre történő szolgáltatása

24.1 A közérdekű adat megismerése iránt bárki - szóban, írásban vagy elektronikus úton - igényt nyújthat be.

24.1 A közérdekű adat megismerésére irányuló kérelem teljesíthetőségéről – a kérelem tárgya szerint illetékes szervezeti egység vezetőjének javaslata alapján – a jegyző dönt. 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. Amennyiben a kért adatokat a kérelmező nem tudja pontosan megjelölni, a kérelmezőnek ehhez segítséget kell nyújtani.

24.2 Az igény teljesítésének megtagadásáról és annak indokairól a kérelmezőt a kérelem beérkezésétől számított 8 napon belül írásban vagy – amennyiben az igényben közölte elektronikus levelezési címét – elektronikus úton értesíteni kell. Az elutasított kérelmekről, valamint az elutasítás indokairól az adatvédelmi biztost az jegyző évente tájékoztatja.

24.3 A közérdekű adat megismerésére irányuló kérelemnek – annak teljesíthetősége esetén – a kérelem tárgya szerint illetékes szervezeti egység vezetője a legrövidebb idő alatt, legfeljebb azonban a kérelem beérkezésétől számított 15 napon belül tesz eleget. Az adatokat tartalmazó dokumentumról vagy dokumentumrészről a kérelmező jegyzetet készíthet, valamint – költségterítés ellenében – kérheti a dokumentum, illetve dokumentumrész másolatát vagy – amennyiben az aránytalan költséggel nem jár – az adat elektronikus adathordozó útján történő rendelkezésre bocsátását.

24.4 Amennyiben a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni. Amennyiben a kérelem már közzétett adatra irányul, ennek tényéről és az adat fellelhetőségéről a kérelmezőt tájékoztatni kell.

24.5 Tudományos kutatómunkához, szakdolgozatok, tanulmányok készítéséhez az anyaggyűjtést és közzétételt a jegyző egyedi kérelem alapján engedélyezheti.

- 24.6 A képviselőtestület, illetve annak szervei elé kerülő előterjesztések, megállapodások, szerződések, előkészítés alatt álló iratok és a döntés- előkészítés körében alkotott iratok nem közérdekűek. Ezek tartalmáról nyilatkozni a döntést megelőzően csak az előterjesztők jogosultak. A döntéshozatalt követő 10 éven belül előterjesztett igény teljesítéséről – az Atv. 19/A§ (2)-(3) bekezdésében meghatározott szempontok figyelembevételével – a jegyző dönt.
- 24.7 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.
- 24.8 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.
- 24.9 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.
- 24.10 A Hivatal évente értesíti az adatvédelmi biztost az elutasított igényekről, valamint az elutasítások indokairól.
- 24.11A 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.
- 24.12 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.

VI. ZÁRÓ RENDELKEZÉSEK

25. Titoktartási kötelezettség

A Hivatallal közszolgálati 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.

26. Eljárási szabályok

26.1 A Hivatalhoz érkező, személyes adatokkal kapcsolatos igényeket, jogorvoslati kérelmeket haladéktalanul továbbítani kell az illetékes szervezeti egység vezetőjének.

- 26.2 A szervezeti egység vezetője a kérést kivizsgálja, szükség esetén a jegyzővel konzultál.
- 26.3 A jegyző ellenőrzi a dokumentumot. Amennyiben az intézkedést jogszerűnek ítéli meg kiadmányozza a dokumentumot.
- 26.4 A Hivatalhoz érkező közérdekű adat megismerése iránti kérelmeket a jegyző részére kell továbbítani, aki teljesíti, vagy elutasítja az igényt.
- 26.5 A jegyző a személyes adattal és közérdekű adattal kapcsolatos igények elutasításáról, annak időpontjáról és okáról nyilvántartást vezet.
- 26.6 Az Adatvédelmi és Adatbiztonsági Szabályzat nem tartalmaz rendelkezéseket a közszolgálati adatok védelmére, arról a Közszolgálati Adatvédelmi Szabályzat rendelkezik.

Tiszaföldvár, 2009. július 2.

**/: Hajós Attiláné Dr. Szlama Katalin :/
címzetes főjegyző**