



**Füzesgyarmat Város Önkormányzat
Polgármesteri Hivatalának**

ADATVÉDELMI SZABÁLYZATA

a polgárok személyi adatainak és lakcímének nyilvántartásáról

Hatályba lépés dátuma: 2007. november 1.

Aláírás:

Tartalomjegyzék

1. A Szabályzat célja
2. Alapfogalmak
3. A Szabályzat hatálya
4. A Szabályzathoz kapcsolódó szabályozások
5. A védelmet igénylő adatok, eszközök köre
 - 5.1. A védelem tárgya
 - 5.2. A védelem eszközei
6. Adatszolgáltatás a nyilvántartásból
7. Adatszolgáltatást korlátozó, megtiltó nyilatkozat
8. Nyilvántartások
9. A kiemelt védelem felelősei és tevékenységi körei
10. A Szabályzat alkalmazásának módja
 - 10.1. A Szabályzat karbantartása
 - 10.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság
11. Védelmi eszközök és módszerek
 - 11.1. Általános rendelkezések
 - 11.1.1. Tűzvédelem
 - 11.1.2. Vagyonvédelem, fizikai biztonság
 - 11.1.3. Adathordozók védelme, tárolása, hordozása és karbantartása
 - 11.1.4. Adatvédelem
 - 11.1.5. Vírusvédelem
 - 11.1.6. Szoftver védelem
 - 11.1.7. Hardver védelem
 - 11.2. A Hivatal további védelmi előírásai
12. Hatályba léptetés

Mellékletek:

1. számú: Adatszolgáltatási nyilvántartás
2. számú: Nyilatkozat az adatszolgáltatási korlátozásról
3. számú: Jogosultsági nyilvántartás, az on-line rendszer használatára jogosultakról
4. Technikai háttérnyilvántartás
5. Nyilvántartás azokról a köztisztviselőkről, akik az eljárás során jogosultak az egyes okmány-nyilvántartások adataihoz hozzáférni

I. fejezet

PREAMBULUM

A Polgármesteri Hivatalban (a továbbiakban: Hivatal) a polgárok személyi adatainak és lakcímének nyilvántartásával kapcsolatos adatvédelmi Szabályzatát (a továbbiakban: Szabályzat), a következők szerint határozom meg:

A Szabályzat az alábbi jogszabályokon alapul:

- a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény;
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény;
- az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény.

1. A Szabályzat célja

A Szabályzat célja, hogy meghatározza a polgárok személyi és lakcím adatait tartalmazó nyilvántartás működésének adatvédelmi szabályait.

A Szabályzat biztosítja a természetes személy (a továbbiakban: polgár) személyes adataival való önrendelkezési jogának, valamint az egyéb alkotmányos jogok érvényesítéséhez és a közigazgatás hatékonyságának biztosításához szükséges személyazonosító és lakcímadatok használatához fűződő közérdek összhangját.

A Szabályzat további célja, hogy biztosítsa a Hivatalban az alábbiakat:

- a papír alapú nyilvántartások esetén is megfelelően gondoskodik a kezelő a fizikai megsemmisülés elleni védelméről, és arról, hogy e nyilvántartásokhoz csak a feladatok ellátására felhatalmazott személyek a feladatuk ellátásához szükséges mértékben férhessenek hozzá,
- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,
- a védelem működését a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

Jelen Szabályzat a Hivatal adatvédelmének általános érvényű előírását tartalmazza, meghatározza a polgárok személyi adatainak és lakcímének nyilvántartásával kapcsolatosan az adatvédelem és adatbiztonság feltételrendszerét.

2. Alapfogalmak

3. A Szabályzat alkalmazásában:

1. *személyes adat*: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) 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;

2. *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;

3. *bűnügyi személyes adat*: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

4. *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;

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

6. *hozzájárulás*: az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

7. *tiltakozás*: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

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

9. *adatkezelés*: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a 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 személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérimpró, DNS-minta, íriszkép) rögzítése is;

10. *adattovábbítás*: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik;

11. *nyilvánosságra hozatal*: ha az adatot bárki számára hozzáférhetővé teszik;
12. *adattörlés*: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
13. *adatzárolás*: az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;
14. *adatmegsemmisítés*: az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;
15. *adatfeldolgozás*: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;
16. *adatfeldolgozó*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi;
17. *személyesadat-nyilvántartó rendszer (nyilvántartó rendszer)*: személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;
18. *adatállomány*: az egy nyilvántartó rendszerben kezelt adatok összessége;
19. *harmadik személy*: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;
20. *EGT-állam*: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Közösség és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
21. *harmadik ország*: minden olyan állam, amely nem EGT-állam.

II. fejezet

A SZEMÉLYES ADATOK VÉDELME

Adatkezelés

3. A Szabályzat hatálya

Az Szabályzat **személyi hatálya** a Hivatal valamennyi köztisztviselőjére, illetve a számítástechnikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

Tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,

- az adatok felhasználására, tárolására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására,
- a Hivatal tulajdonában lévő valamennyi papír alapú, számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációra is,
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció),
- a rendszer- és felhasználói programokra.

4. Kapcsolódó szabályozások

A Szabályzatot a Hivatal Szervezeti és Működési Szabályzatával és mellékleteivel összhangban kell alkalmazni.

5. Védelmet igénylő adatok, eszközök köre

5.1. A védelem tárgya:

- a település közigazgatási területén lakcímmel rendelkező polgár adatainak, illetve adatváltozásainak, valamint a polgár adataiban a település közigazgatási területén bekövetkezett változásnak a nyilvántartáson történő átvezetése;
- a polgár személyi azonosítóval történő ellátásával, annak módosításával, illetőleg visszavonásával kapcsolatos feladatok;
- a lakcímbejelentés tudomásul vételével összefüggő első fokú hatósági feladatok;
- a törvényben meghatározott feltételek fennállása esetén adatszolgáltatást teljesítése a nyilvántartásból;
- közokirat kiadása a nyilvántartott adatokról;
- a személyes adatok védelme;
- a nyilvántartásba felvett adatok továbbítása a központi nyilvántartás részére, illetve a helyi szinten kezelt nyilvántartásban az adatok változásának átvezetése.

5.2. A védelem eszközei

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

6. Adatszolgáltatás a nyilvántartásból

6.1. A Hivatal a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben meghatározott feltételekkel és korlátok között - a polgár, illetve jogi személy és jogi személyiséggel nem rendelkező szervezet kérelmére, a felhasználás céljának és jogalapjának igazolása esetén - adatot szolgáltat.

A nyilvántartásból adatok az alábbi csoportosítás szerint szolgáltatathatók:

- a) név és lakcím adatok (felvilágosítás a lakcímről);
- b) név- és lakcímadatok, anyja neve, állampolgárság, születési hely, születési idő, családi állapot, a házasságkötés helye, a nem, a nyilvántartásból való kikerülés oka, helye és ideje;
- c) a b) pontban felsorolt adatok és a személyazonosító jel;
- d) a nyilvántartásba felvett adatok teljes köre.

6.2. A név és lakcím adatok szolgáltatását bármely polgár, illetve jogi személy és jogi személyiséggel nem rendelkező szervezet a felhasználás céljának és jogalapjának igazolása mellett jogosult kérni:

- a) jogának vagy jogos érdekének érvényesítése érdekében,
- b) tudományos kutatás céljából,
- c) közvélemény-kutatás és piackutatás megkezdéséhez szükséges minta, valamint
- d) közvetlen üzletszerzés (direkt marketing) célját szolgáló lista összeállításához.

6.3. A kérelem teljesítését meg kell tagadni, ha

- a) az adatok kiadását a polgár letiltotta, kivéve, ha az adat kiszolgáltatására eseti engedélyt adott;
- b) a kérelmező az adat felhasználásának célját, illetőleg jogalapját nem vagy nem megfelelően igazolta;
- c) a megjelölt cél a kérelmező jogát, illetve jogos érdekét nem érinti, vagy az adattal érintett polgár személyiségi jogát sérti;
- d) az újszülött adatainak nyilvántartásba vételét követően kilencven nap még nem telt el.

6.4. A Hivatal az 1. számú melléklet szerinti adattartalommal adatszolgáltatási nyilvántartást vezet.

6.5. A polgár az adatszolgáltatási nyilvántartásból jogosult megismerni, hogy mely adatszolgáltatások alanya volt.

Az adatszolgáltatási nyilvántartást öt évig meg kell őrizni.

6.6. Az adatszolgáltatási nyilvántartásból a polgár tájékoztatást kérhet a Hivaltól, hogy mely adatszolgáltatások alanya volt.

6.7. Az adatszolgáltatási nyilvántartásból az adatvédelmi biztosnak, az adatvédelmi felelősnek, valamint a bíróságnak és a nemzetbiztonsági szolgálatoknak feladataik ellátása érdekében - a rájuk vonatkozó törvényekben meghatározott célok és feltételek teljesülése esetén -, valamint a nyomozó hatóságoknak bűnüldözési tevékenységük ellátásához, továbbá az állampolgársági ügyekben eljáró szervnek a kérelmező adatainak azonosításához szolgáltatatható adat.

6.8. A polgár kérelmére saját adatairól a nyilvántartásból kivonatot vagy másolatot, illetve szóbeli tájékoztatást kell adni.

7. Adatszolgáltatást korlátozó, megtiltó nyilatkozat

7.1. A polgár adatai szolgáltatását korlátozó vagy tiltó nyilatkozatát, illetőleg annak visszavonását személyesen vagy meghatalmazott képviselője útján, továbbá ajánlott levélben teheti meg Hivatalnál a 2. számú mellékletben foglalt tartalommal.

7.2. Ha a polgár a korlátozó nyilatkozatát megtette vagy visszavonta, az adatváltozást a nyilvántartáson haladéktalanul, de legkésőbb öt munkanapon belül átvezeti.

8. Nyilvántartások

8.1. A Hivatal a következő nyilvántartásokat vezeti:

- a) adatszolgáltatási nyilvántartást, az általa teljesített adatszolgáltatásokról (lásd: 6.4. pont);
- b) jogosultsági nyilvántartást, az on-line rendszer használatára jogosultakról (lásd 3.számú melléklet);
- c) üzemeltetési naplót;
- d) technikai háttérnyilvántartást (lásd 4. számú melléklet).

8.2. A jegyző az 5. számú melléklet szerinti nyilvántartást vezeti azokról a köztisztviselőkről, akik az eljárás során jogosultak az egyes okmány-nyilvántartások adataihoz hozzáférni.

Az érintett köztisztviselő nevét, és az 5. számú melléklet szerinti nyilvántartási adatokat legkésőbb a jogosultság kezdő időpontját megelőző munkanapon közölni kell a személyiadat- és lakcímnnyilvántartás központi hivatalával.

A nyilvántartás adatait a hozzáférési jogosultság megszűnésétől számított 5 évig kell megőrizni.

9. A kiemelt védelem felelősei és tevékenységi köreik

9.1. Az adatbiztonság szabályozásának biztosítania kell:

- a) az adatkezelésre használt számítástechnikai és manuális eszközökhöz történő illetéktelen fizikai hozzáférés megakadályozását,
- b) az adathordozók tartalma illetéktelen megismerésének, lemásolásának, megváltoztatásának vagy az adathordozó eltávolításának a megelőzését,
- c) annak megakadályozását, hogy az adatkezelésre használt számítástechnikai és manuális eszköztárba illetéktelen bevitelt hajtsanak végre vagy a tár tartalmát illetéktelenül megismerjék, töröljék vagy bármilyen módon megváltoztassák,
- d) annak megakadályozását, hogy adatkezelésre használt távadat-átviteli vonalon az adatokhoz illetéktelenül hozzáférjenek,
- e) a hozzáférési jogosultság betartását,
- f) azoknak az azonosítását, akiknek az adatkezelésből adatokat továbbítanak,
- g) annak azonosítását, hogy a számítástechnikai, valamint manuálisan vezetett eszköztárba milyen adatokat, mikor és ki rögzített, illetve intézkedett a rögzítésről,
- h) annak megakadályozását, hogy az adatok továbbítása alkalmával az adatokat illetéktelenül megismerjék, lemásolják, töröljék vagy bármilyen módon megváltoztassák.

9.2. A fizikai biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- az adathordozó eszközök elhelyezésére szolgáló helyiségeket úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen;
- azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését a hivatalos feladataikkal összhangban megállapított felhatalmazás alapján kell szabályozni, ellenőrizni;
- számítástechnikai eszközzel olvasható és manuális adathordozók tárolását, felhasználását és a hozzáférést ellenőrizni kell;
- az adathordozókról, azok mozgásáról, tartalmáról és felhasználásukról nyilvántartást kell vezetni;
- meg kell határozni azoknak a személyeknek a körét, akik az adathordozó eszközöket üzemeltethetik;
- a számítástechnikai eszközök hozzáférési kulcsát (azonosító kártya, jelszó) szolgálati titokként kell kezelni;
- gondoskodni kell arról, hogy a számítástechnikai eszközök biztonsági megoldásainak dokumentációjához csak az arra felhatalmazott személyek férjenek hozzá.

9.3. Az üzemeltetési biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- össze kell állítani és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott személyek névsorát, feladataikat körül kell határolni;
- meg kell határozni az adatokhoz való hozzáférés szintjének szabályait;
- külső személy – pl. karbantartás, javítás, fejlesztés céljából – a számítástechnikai eszközökhöz lehetőleg úgy férjen hozzá, hogy a kezelt adatokat ne ismerje meg;
- a számítástechnikai rendszert – ideértve a programokat is – dokumentálni kell. A rendszer vagy annak bármely eleme csak az arra illetékes személy felhatalmazásával változtatható meg, amelyet ellenőrizni kell;
- a hozzáférés jelszavait időközönként, de az üzemeltető személyének megváltozásakor azzal egyidejűleg meg kell változtatni. Jelszót ismételtelen nem lehet kiadni;
- a számítástechnikai rendszer üzemeltetéséről – hagyományos vagy automatikus módon – nyilvántartást kell vezetni, amelyet az arra illetékes személynek folyamatosan ellenőriznie kell;
- a rendszerbe kerülő adatokat tartalmazó (hagyományos vagy számítástechnikai eszközzel olvasható) dokumentumokat úgy kell kezelni, hogy elvesztésük, elcserélésük vagy meghibásodásuk elkerülhető, kiküszöbölhető legyen;
- olyan tervet kell kidolgozni, amely a számítástechnikai eszközök előre nem látható üzemzavarának hatását ellensúlyozni képes intézkedéseket tartalmaz.

9.4. A technikai biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- az adatok és programok véletlen vagy szándékos megrongálását számítástechnikai módszerekkel is meg kell akadályozni;
- az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell;
- a hozzáférést jelszavakkal kell ellenőrizni;
- az adatok és az adatállományok változását naplózni kell;
- az adatbevitel során a bevitt adatok helyességét ellenőrizni kell;
- on-line adatmozgás kezdeményezésének jogosultságát ellenőrizni kell;
- programfejlesztés vagy próba céljára valódi adatok felhasználását – ha a próbát külső szerv vagy személy végzi – el kell kerülni.

10. A Szabályzat alkalmazásának módja

A Szabályzat megismerését az érintett köztisztviselők részére a jegyző biztosítja, az egyes munkaköri leírásoknak és a Szabályzat előírásainak megfelelően.

10.1. A Szabályzat karbantartása

A Szabályzatot a vonatkozó jogi szabályozásban, informatikában, valamint a Hivatalban bekövetkező változások miatt időközönként aktualizálni kell. Ez feladata.

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

10.2.1. Az adatok kezelésére, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott személyek az adatokhoz csak a feladatuk ellátásához szükséges mértékben, az alábbiak szerint férhetnek hozzá:

- A rendszerben adatkarbantartást csak a felelős vezető által erre felhatalmazott dolgozó végezhet. Az adatszolgáltatást igénybe vevő, illetve a nyilvántartást vezető vagy üzemeltető szerv más dolgozója az adatállományban változtatást nem végezhet. Az általa észlelt adathiba esetén erről a felhatalmazott köztisztviselőt értesíti, aki a kijavítás elvégzéséről intézkedik.
- A rendszerfejlesztők a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban nem használhatják fel más célra, és nem hozzátják mások tudomására.
- Az üzemeltető, illetve az adatszolgáltatást közvetlenül (on-line) igénybe vevő szerv dolgozói csak meghatározott jelszó és azonosító használatával férhetnek hozzá az adatállományhoz, amelyek egyidejűleg meghatározzák az adathozzáférési jogosultság mértékét is.
- A rendszer üzemeltetői csak az adatállományok kezelésére, a nyilvántartás szervei által jelentett változások átvezetésére, a szolgáltatásokkal kapcsolatos technikai feladatok ellátására, a számítógépes rendszer működéséhez szükséges beavatkozások elvégzésére jogosultak. Az üzemeltető az adatállományban szereplő adatokat más, általa kezelt nyilvántartáshoz törvényi felhatalmazás nélkül nem használhatja fel.

10.3. A nyilvántartás más nyilvántartásokkal - ha törvény az adatkezelés céljának és az adatok körének pontos meghatározásával másképp nem rendelkezik - nem kapcsolható össze.

11. Védelmi eszközök és módszerek

11.1. Általános rendelkezések

11.1.1. Tűzvédelem

A kiszolgáló helyiség "D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a Hivatal Tűzvédelmi Szabályzata tartalmazza.

11.1.2. Vagyongvédelem, fizikai biztonság

- a helyiségeket biztonsági zárral kell felszerelni,
- a helyiségekbe való be- és kilépés rendjét szabályozni kell,
- a helyiségek kulcsának felvétele és leadása csak aláírás ellenében a személyazonosság igazolása mellett történhet,
- munkaidőn túl a helyiségekben csak engedéllyel lehet tartózkodni,
- a helyiségekbe történő illetéktelen behatolás tényét a szervezet vezetőjének azonnal jelenteni kell,
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők használhatják,
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

11.1.3. Adathordozók védelme, tárolása, hordozása és karbantartása

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni,
- a nyilvántartásban az azonosító adaton kívül a felírás és megőrzés dátumát, a védettség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni,
- a használni kívánt adathordozót (floppy disk, CD-ROM, stb.) a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni,
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet,
- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót más intézménynek átadni csak engedéllyel lehet,
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg,
- az adathordozókat félévenként ellenőrizni és tisztítani kell,
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:
 - a) a fizikailag sérült, javíthatatlan,
 - b) a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott),
 - c) ha a kapacitás a névleges érték 75%-ánál kevesebb,
 - d) véglegesen elhasználódott adathordozót,

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni, bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törülő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni,

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni, az üzemi másolás nem minősül másolásnak, biztonsági illetve archív adatállomány előállítása másolásnak számít.

Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

11.1.4. Adatvédelemi feladatok:

- az adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- csak tesztelt adathordozóra lehet adatállományt rögzíteni,
- adatrögzítés szoftver védelme: a programokat és az adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni,
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá),
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

11.1.5. Vírusvédelem

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

11.1.6. Szoftver védelem

Az üzemeltetésért felelős köztisztviselőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetőek legyenek az illetékes felhasználók számára.

- Rendszerszoftver védelem:

- a) a rendszerszoftver módosításához az illetékes engedélye szükséges,
- b) a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni,
- c) a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló).

- Programhoz való hozzáférés, programvédelem:

A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

- A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a) a program azonosítója,
- b) a program készítőjének neve,

c) a feldolgozási rendszer megnevezése.

- Programok megőrzése, nyilvántartása:

- a) a programokról naprakész nyilvántartást kell vezetni,
- b) a nyilvántartásból egyértelműen megállapíthatóak legyenek a program azonosítására és kezelésére vonatkozó adatok.

- Programok fizikai védelme:

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni

11.1.7. Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől,
- a számítógép közelében ételt és italt fogyasztani tilos,
- a számítógépteremben és a szerver teremben klímaberendezés használata ajánlott,
- szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerver-teremben kell elhelyezni,
- a számítógép-hálózat csatornáit külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát,
- a fali csatlakozók megbontása szigorúan tilos,
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez,
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni,
- a számítógépek belsejébe nyúlni, és ott bármilyen változtatást okozni tilos, csak az illetékes szakember, illetve a szervizek szakemberei nyúlhatnak bele,
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

11.2. A Hivatal további védelmi előírásai

11.2.1. A rendszerben adatkarbantartást csak a felelős vezető által erre felhatalmazott dolgozó végezhet. Az adatszolgáltatást igénybe vevő, illetve a nyilvántartást vezető vagy üzemeltető szerv más dolgozója az adatállományban változtatást nem végezhet. Az általa észlelt adathiba esetén erről a felhatalmazott köztisztviselőt értesíti, aki a kijavítás elvégzéséről intézkedik.

11.2.2. A rendszerfejlesztők a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban nem használhatják fel más célra, és nem hozhatják mások tudomására.

A védelem felelőse a Jegyző.

Számítástechnikai védelmi előírások:

- a számítógépeket csak indítójelszóval lehessen elindítani,
- induláskor minden esetben vírus-ellenőrző programot kell elindítani,
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell,
- a bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel, vagy külső programmal is,
- a módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni,
- a teljes anyagról heti mentéseket kell készíteni, ezeket a havi mentésekig kell megőrizni,

- a teljes anyagról havi mentéseket kell készíteni, ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény),
- a felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

12. Hatályba léptetés

Ezen Szabályzat 2007. év november hó 01. nappal lép hatályba.

Kelt: Füzesgyarmat, 2007- év október hó 15. nap

.....
Jegyző

Adatszolgáltatási nyilvántartás

Az adatkezelő nyilvántartási azonosítója	Adatszolgáltatás ideje	Az adatszolgáltatás		Az adatszolgáltatást igénylő polgár, jogi személy vagy jogi személyiséggel nem rendelkező szervezet, illetve megbízottja vagy képviselője neve	Megjegyzés
		Célja	Jogalapja		

Nyilatkozat az adatszolgáltatási korlátozásról

ÉRKEZETT:
IKT. SZÁM:
TOVÁBBÍTVÁ:
CÍMZETT:

ÉN

- CSALÁDI NEVE:
- UTÓNEVE(I):
- ANYJA SZÜLETÉSI CSALÁDI NEVE:
- SZÜLETÉSI UTÓNEVE(I):
- A SZEMÉLYAZONOSÍTÓ IGAZOLVÁNYBAN SZEREPLŐ
 - = lakóhelye (állandó lakcím):
 - = tartózkodási helye (ideiglenes lakcím):
- SZEMÉLYI AZONOSÍTÓJA (VOLT SZEMÉLYI SZÁM):
.....

a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 2. §-ának (1) bekezdése alapján a rólam nyilvántartott adatok kiadását megtiltom.

TUDOMÁSUL VESZEM, HOGY A JEGYZŐ VAGY A KÖZIGAZGATÁSI ÉS ELEKTRONIKUS KÖZSZOLGÁLTATÁSOK KÖZPONTI HIVATALÁNAK MEGKERESÉSÉRE - ESETI ENGEDÉLYEM ALAPJÁN - AZ ADATSZOLGÁLTATÁSI TILALMAT FELOLDHATOM.

A NYILATKOZAT NEM ÉRINTI A TÖRVÉNYBEN KÖTELEZŐEN ELŐÍRT ADATSZOLGÁLTATÁSOK TELJESÍTÉSÉT (PL. ADÓIGAZGATÁS, HONVÉDELMI NYILVÁNTARTÁS, INGATLAN-NYILVÁNTARTÁS), TOVÁBBÁ A TÖRVÉNY 20. §-A ALAPJÁN ENGEDÉLYEZETT ADATSZOLGÁLTATÁSOKAT.

KELT:

.....
ALÁÍRÁS / ELEKTRONIKUS ALÁÍRÁS

**Jogosultsági nyilvántartás, az on-line rendszer használatára
jogosultakról**

A bevezetés időpontja	A rendszer használatára felhatalmazott személyek		A jogosultság tartalma (esetleges korlátozása)
	neve	aláírása	

Technikai háttérnyilvántartást

Az alkalmazott számítógép egyedi jelölése	A használatra feljogosított szerv/köztisztviselő	Alkalmazott szoftver megnevezése

Nyilvántartás azokról a köztisztviselőkről, akik az eljárás során jogosultak az egyes okmány-nyilvántartások adataihoz hozzáférni

Az érintett köztisztviselő		Okmány-nyilvántartás megnevezése	Hozzáférési jogosultság tartalma	Hozzáférési jogosultság				
Neve	Személyi azonosítója			Kezdő időp.	Idő-tartama	Módosítása	Visszavonásának	
							Oka	Ideje