Dunaharaszti
Polgármesteri Hivatal

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

Készítette:

dr. Kulcsár Zoltán sk.
adatvédelmi szakértő

Jóváhagyta:

Pethő Zoltán
jegyző

DUNAHARASZTI POLGÁRMESTERI HIVATAL * JEGYZŐ *

Ellenőrizte:

Baldauf Mirtill
belső adatvédelmi felelős

2008. május 5.

Dunaharaszti Polgármesteri Hivatal Jegyzője

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

Adatvédelmi és Adatbiztonsági Szabályzatot

adom 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: Dunaharaszti Város Polgármesteri Hivatala
Székhelye: 2330 Dunaharaszti, Fő út 152.
Jegyző: Pethő Zoltán
Belső adatvédelmi felelős: Baldauf Mirtill

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 Avtv. 3. §-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. Dunaharaszti Polgármesteri Hivatalnál az információ-rendszer felelőse: ... ...

b) 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.

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 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 Polgármesteri 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 Polgármesteri Hivatal képviseletében a rendszer megtervezéséért és fejlesztéséért felelős rendszerirányító: .....

5.6. 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;

5.7. A Polgármesteri Hivatal képviseletében 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;

5.8. 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.

5.9. 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 készenlétben 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.

5.10. 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.