Ügyiratszám: I./1160-1/2018.

Készült: 3 példányban

Hajdúsámson Város Önkormányzata Jegyzőjének
2/2018. számú

UTASÍTÁSA

a Hajdúsámsoni Polgármesteri Hivatal
Adatvédelmi
és
Informatikai Biztonsági
Szabályzatáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés j) pontjában, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 24. § (3) bekezdésében és 35. § (3) bekezdésében, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 30. § (1) bekezdésében szereplő felhatalmazás alapján, Hajdúsámson Város Önkormányzata Képviselő-testületének Hajdúsámson Város Önkormányzata Szervezeti és Működési Szabályzatáról szóló 1/2016. (I. 29.) önkormányzati rendelete, valamint Hajdúsámson Város Önkormányzata Képviselő-testülete 132/2016. (IV. 28.) öh. sz. határozatával jóváhagyott Hajdúsámson Város Polgármesteri Hivatala Szervezeti és Működési Szabályzata rendelkezéseire figyelemmel a Hajdúsámsoni Polgármesteri Hivatal Adatvédelmi és Informatikai Biztonsági Szabályzata a következők szerint kerül meghatározásra.

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

A Szabályzat hatálya

1. § (1) A Szabályzat személyi hatálya a Hajdúsámson Város Polgármesteri Hivatallal (a továbbiakban: Hivatal) közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, ügykezelőkre, valamint a munkaviszony keretében foglalkoztatott alkalmazottakra, munkavállalókra, a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyekre terjed ki, különös tekintettel azokra, akik személyes adatot, közérdekű adatot, vagy közérdekből nyilvános adatot tartalmazó adatkezelést és adatfeldolgozást, továbbá informatikai rendszerhasználatot és rendszerüzemeltetést végeznek.

(2) A Szabályzat tárgyi hatálya kiterjed:
- a Hivatal tulajdonában lévő, vagy bérelt valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára is,
- a rendszer- és felhasználói programokra,
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- az adatok felhasználására, tárolására, kezelésére vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására, kezelésére,
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció),
- valamint az ASP szakrendszerben végzett valamennyi munkafolyamatra.

(3) A Szabályzat előírásait alkalmazni kell a Hivatal szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások, továbbá dokumentumok esetében.

(4) Az iratokat és az adatokat, továbbá az iratkezelés során használt valamennyi eszközt védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, valamint a megsemmisülés és sérülés ellen.

(5) Iratokat, adatokat a munkaköri feladat ellátásán kívül a munkahelyről kivinni, a munkahelyen kívül feldolgozni, tárolni csak a jegyző engedélyével lehet, azzal a feltétellel, hogy az irat, adat tartalmát illetéktelen személy nem ismerheti meg.

(6) Az iratok tárolása, kezelése során fokozottan ügyelni kell arra, hogy illetéktelen személyek ne ismerhessék meg azok tartalmát. A munkavégzés céljára szolgáló irodákat távozáskor kulcsra kell zárni. Az irodahelyiségek nyitva tartása miatti illetéktelen hozzáférés esetén az érintett fegyelmi felelősséggel tartozik.

(7) A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős.

(8) Jelen Szabályzat rendelkezéseit a Hivatal hatályos Egyedi Iratkezelési Szabályzatával és Közzétételi Szabályzatával összhangban szükséges alkalmazni.

2. § (1) A Szabályzat rendelkezéseit

- a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény,
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtására kiadott 146/1993. (X.26.) Korm. rendelet,
- az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény,
- a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény,
- az államháztartásról szóló 2011. évi CXCV. törvény,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet,
- az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet,
- az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI. 13.) Korm. rendelet,
- az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet,
- az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII. 28.) BM rendelet,
- az elektronikus formában tárolt iratok közlevéltári átvételének eljárásrendjéről és műszaki követelményeiről szóló 34/2016. (XI. 30.) EMMI rendelet,
- a közlevéltárak és a nyilvános magánlevéltárak tevékenységével összefüggő szakmai követelményekről szóló 27/2015. (V. 27.) EMMI rendelet előírásaival összhangban kell alkalmazni.

A Szabályzat rendelkezéseit a minősített iratokra és azok kezelési rendje vonatkozásában

- a minősített adat védelméről szóló 2009. évi CLV. törvényben,
- a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendeletben, továbbá
- a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendeletben foglalt eltérésekkel kell alkalmazni.

(2) A Szabályzat rendelkezéseit az elektronikus ügyintézés esetén az elektronikus ügyintézés részletszabályairól szóló kormányrendeletben foglalt eltérésekkel kell alkalmazni.

A Szabályzat célja

3. § (1) A szabályozás célja, hogy a személyes adatok védelméhez, és a közérdekű adatok megismeréséhez fűződő – Alaptörvényben meghatározott – jogok teljeskörű biztosítása, valamint a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, továbbá a létfontosságú információs rendszerek és rendszerelemek biztonsága érdekében meghatározza a hivatali adatkezelés, adatfeldolgozás, adattovábbítás általános kereteit. Továbbá megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

(2) A Szabályzat célja továbbá, hogy az informatika alkalmazása során biztosítsa a Hivatalban az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett informatikai eszközök, az ASP rendszer rendeltetésszerű használatát,

- a számítógépes és ASP rendszerek zavartalan üzemeltetését,
- az üzembiztonságot szolgáló karbantartást és fenntartást,

- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését,
- az adatállományok tartalmi és formai épségének megőrzését,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit.

II. FEJEZET
ÉRTELMEZŐ RENDELKEZÉSEK

4. § A Szabályzat alkalmazásában, az Infotv. rendelkezéseivel összhangban:
1. Adat: a természetes vagy mesterséges objektumok, folyamatok, állapotok jellemzői illetőleg azok részleteinek érzékelhető formában történő megjelenítése. Adat tágabb értelemben jelenthet szöveget, számot, rajzot, térképi részleteket vagy bármely más információt a megjelenési módjára vagy formájára való tekintet nélkül.
2. Adatállomány: az egy nyilvántartásban kezelt adatok összessége.
3. Adatkezelés: az alkalmazott eljárástól függetlenül, adatokon végzett bármely művelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése, stb.
4. Adatkezelő: az a szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.
5. Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.
6. Adatközlő: az a belső szervezeti egység, amely az adatfelelős által szolgáltatott adatokat a jogszabályokban meghatározott módon közzéteszi.
7. Adatszolgáltatás a polgárok személyes adataiból: a nyilvántartásban szereplő polgárok adatainak a törvényben meghatározott tartalmú és terjedelmű közlése. Ezen belül:
8. egyedi adatszolgáltatás: egy polgár adatainak közlése;
9. csoportos adatszolgáltatás: az adatigénylő által vagy jogszabályban meghatározott szempontok szerint képzett csoportba tartozó polgárok adatainak rendszeres vagy eseti közlése.
10. Adattovábbítás: az adat meghatározott személy számára történő hozzáférhetővé tétele.
11. Adatvédelem: az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés, stb. megakadályozása; a személyes adatok esetében kiegészül az adott személy személyes adatainak jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.
12. Adattörlés: az adatok felismerhetetlenné tétele olya módon, hogy a helyreállításuk többé nem lehetséges.
13. Információ: jelentéssel bíró adat, megjelenési módjára vagy formájára való tekintet nélkül.
14. Kötelezően közzéteendő közérdekű adat: az Isztv 26. § (2) – (3) bekezdésében meghatározott körbe tartozó adat.
15. Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, melynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
16. Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
17. Különleges adat: a faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, továbbá az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
18. Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

19. Polgár természetes személyazonosító adatai: családi és utóneve(i), nők esetében leánykori családi és utóneve(i) (a továbbiakban együtt: név); neme; születési helye és ideje; anyja leánykori családi és utóneve(i) (a továbbiakban : anyja neve).
20. Polgár lakcím adata: bejelentett lakóhelyének, illetve tartózkodási helyének címe (a továbbiakban együtt lakcím).
21. Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;
22. Elektronikus tájékoztató szolgáltatás (tájékoztatás): az elektronikus közigazgatási szolgáltatás körén kívüli ügyintézésről elektronikus úton hozzáférhetővé tett általános jellegű információs szolgáltatás.
23. Interaktív szolgáltatás: az egyszerű tájékoztatáson túlmenően olyan szolgáltatás (például letölthető űrlapok, kereső rendszerek, tematikus tájékoztatók), amely csak a használó aktivitását igényli, a szolgáltatást nyújtó szerv által előkészített dokumentumok kitöltéséhez, felhasználásához.
24. alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja;
25. felhasználó: az a személy (vagy szervezet), aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;
26. felhasználói jog: az a jogosultság az informatikai eszközökön, hálózaton, amely a felhasználó számára szükséges és elégséges munkájának elvégzéséhez;
27. gépterem (iroda): az a helyiség, amelyben a Hivatal dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz;
28. hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;
29. hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó része;
30. informatika: a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működéséhez;
31. informatikai biztonság: olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni;
32. munkaállomás: egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál;
33. rack szekrény: üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket üzemeltetnek;
34. rendszerprogram (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.
35. szerver: olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza;
36. szerverszoba: az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a kijelölt illetékes személyek juthatnak be;
37. vírus: olyan programrész, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet.

III. FEJEZET
ADATVÉDELMI SZABÁLYOK

Az adatkezelésben részt vevő szervezeti egységek és személyek

5. § (1) A Hivatal belső szervezeti egységei szakmai feladataik ellátása során kizárólag az adott feladat, a tevékenység megítélése, az adott döntés előkészítése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges – és a személyes adatok körébe tartozó – adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását, irattárazását láthatják el.

(2) Hajdúsámson Város Önkormányzata Képviselő-testülete és bizottságai kötelesek biztosítani a Hivatal tevékenységének átláthatóbbá tételét szolgáló, valamint a jogszabályok által közérdekűnek – nyilvánosnak – minősített adatok kezelését, majd ezek közzétételét.

6. § Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért és szolgáltatásáért.

7. § § (1) A jogszabály által védett adatok kezelésével kapcsolatos szabályok betartásáról a Hivatal teljes személyi állománya köteles gondoskodni. Az adatvédelmet illetően a szükséges döntések meghozataláért a jegyző felelős, aki a feladat- és hatásköröket a szervezeti egységek vezetői útján gyakorolja.
(2) Az adatvédelemre, a közérdekű adatok nyilvánosságára és az elektronikus információszabadságra vonatkozó jogszabályok által előírt feladatokat a jegyző koordinálja, valamint kijelöli a belső adatvédelmi felelőst.
(3) A Hivatal tevékenységére vonatkozó adatvédelmi előírások betartatásáról, a következő személyek gondoskodnak:
a) a belső adatvédelmi felelős (1. függelék),
b) a belső információ technikai (IT) rendszerek adatvédelmével, biztonságos üzemeltetésével, összefüggésben a Hivatal informatikai rendszerüzemeltetője,
c) a közszolgálati adatok kezelése, közszolgálati ellenőrzések tekintetében a Hivatal humánpolitikai feladatkörben eljáró ügyintézője,
d) a közérdekű adatok nyilvánosságának biztosítása tekintetében valamennyi szervezeti egység vezetője.

A belső adatvédelmi felelős

8. § A belső adatvédelmi felelős:
a) feladatkörével összefüggésben utasítást csak a jegyzőtől kaphat, illetve fogadhat el,
b) ellenőrzési jogköre a Hivatal valamennyi szervezeti egységére kiterjed,
c) koordinálja az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítását, módosításait,
d) az állami és szolgálati titkok megtartásával korlátozás nélkül jogosult a szervezeti egységek adatkezelésébe, az azzal kapcsolatos ügyiratokba, illetve a közérdekű adatot tartalmazó iratokba betekinteni,
e) figyelemmel kíséri a vagyonnyilatkozatok munkahelyi kezelésének adatvédelmi szempontból történő maradéktalan végrehajtását,
f) jogosult az előírások ellen vétőkkel szemben a jegyző útján büntető-, szabálysértési, fegyelmi eljárást, vagy egyéb felelősségre vonást kezdeményezni,
g) vezeti a belső adatvédelmi nyilvántartást,
h) tevékenységével összefüggésben az adatvédelem helyzetéről évente beszámolót készít,
i) elkészíti és szükség esetén módosítja az adatvédelmi szabályzatot,
j) gondoskodik az adatvédelmi ismeretek oktatásáról,
k) részt vesz a belső adatvédelmi felelősök konferenciáján.

Az adatvédelem tárgya

9. § Az adatvédelem folyamatában a védelem tárgya:
a) a Hivatal működése során keletkezett személyes és közérdekű adatok teljes köre, keletkezésüktől a megsemmisítésükig,
b) az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, illetőleg közérdekű adatokat tartalmaznak. Az adathordozók lehetnek papír alapúak, mágneses vagy optikai adathordozók, egyéb informatikai hardverek, amelyek adattárolásra alkalmasak,
c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

Az adatkezelés alapkövetelményei

10. § Az önkormányzati feladatok ellátása során az adott feladat szerinti ügymenet részeként biztosítani kell az adatkezelés szabályainak a maradéktalan betartását, a természetes személyek adatainak védelmét a jogellenes felhasználástól.

11. § Az adatkezelés során biztosítani kell:
a) az adott egyén szempontjából fontos adatok helyes, pontos kezelését. A hibás adat előfordulása esetén annak észlelésekor hivatalból, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;

b) az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába;
c) a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását;
d) a különböző célú adatok, adatállományok (adatbázisok) folyamatos vezetését, aktualizálást és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára. A személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;
e) a különböző adatok, adatállományok (adatbázisok) valódiságát, pontosságát, részletességét, hitelességét;
f) a különböző adatok, adatállományok (adatbázisok) jellegétől függően azok bizalmas, illetőleg az adott területre vonatkozó jogszabályok szerinti kezelését. A pályázatok, ajánlatok elbírálásáig azok tartalmának zárt – nem nyilvános – kezeléslét;
g) a Hivatal gondozásában készült információs rendszerek, adatbázisok folyamatos működését, és szükség szerinti folyamatos hozzáférés lehetőségét, a folyamatos aktualizálást, a közérdekű adatok folyamatos a jogszabályoknak megfelelő szolgáltatását, az érdeklődők véletlenszerű internetes rendelkezésre állásának a garantálását;
h) az adatrendszer (akár számítógépes, akár manuális) fizikai biztonságát. Az adatok és az adathordozó eszközök összességében jelentős értéket képviselnek. Megsemmisülésük esetén újra előállításuk többletmunkát és költséget igényel.

Az adatvédelem eszközei

12. § Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani mindazon igazgatási, iratkezelési, szervezési, személyi, műszaki, technikai, informatikai és egyéb intézkedéseket, melyek elengedhetetlenek az egyes adatok, adatállományok (adatbázisok) zavartalan működéséhez, és védelmet nyújtanak ahhoz, hogy

a) illetéktelenek ne jussanak a különböző személyes adatokhoz (személyes adatokat tartalmazó adatbázisokhoz), dokumentumokhoz,
b) a különböző adatok (adatbázisok) dokumentumok megsérülésére, meghibásodására ne kerüljön sor,
c) az adatkezelés során ismeretek hiánya, hozzá nem értés miatt, emberi mulasztásból károsodásra, adatok, dokumentumok megsemmisülésére ne kerüljön sor.

Személyi feltételek biztosítása

13. § A személyes adatok kezelésével kapcsolatos teendőket csak a Hivatal illetékes belső szervezeti egységének e feladattal megbízott ügyintézői látnak el. A folyamatos ügyintézés érdekében a megfelelő helyettesítésről gondoskodni kell. A közérdekű adatok folyamatos szolgáltatása érdekében a feladatkör szerint illetékes belső szervezeti egység vezetője felelős a szakterületet jól ismerő és az elektronikus adatkezelésben, tájékoztatásban jártas személy(ek) kijelöléséért.

14. § A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Hivatal adatvédelmi felelősének kell gondoskodnia.

15. § A Hivatal megbízott informatikusa végzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét, és a műszaki ellátást, biztonsági másolatot készít, segíti, ellenőrzi a Hivatal dolgozóinak számítástechnikai munkáját.

Az adatvédelem technikai módjai, és megvalósításai
Tűzvédelem

16. § A tűzveszélyességi osztályba sorolás szerint a szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, mely mérsékelt tűzveszélyes üzemet jelent.

Fizikai védelem

17. § A teljes körű fizikai védelem megvalósítása érdekében:

- a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;

- a szerverszoba kulcsát az adatvédelmi felelős és/vagy az informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel;
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- a szerverszobába történő illetéktelen behatolás tényét a jegyzőnek azonnal jelenteni kell;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Adathordozók védelme, tárolása, hordozása és karbantartása

18. § (1) Az adathordozók mindennemű külső és belső behatástól való megóvása érdekében:
- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- az adathordozók nyilvántartásában 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;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével 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.

(2) Selejtezendő:
a) a fizikailag sérült, javíthatatlan;
b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
c) ha a kapacitás a névleges érték 75%-ánál kevesebb;
d) véglegesen elhasználódott adathordozót.

(3) Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

(4) A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

Adatok károsodása, megsemmisülése elleni védelem

19. § Az adathordozókon tárolt adatok károsodásának és megsemmisülésének elkerülése érdekében:
- az adatbevitel hibátlan műszaki állapotú berendezésen történhet;
- csak hibátlan adathordozóra lehet adatállományt rögzíteni;
- adatrögzítő szoftver védelme érdekében a programokat, adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni;
- az adatok bevitele során alapvető követelmény, hogy 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 biztonsági másolatot kell időnként készíteni.

Adatok illetéktelen személy(ek)hez kerülése elleni védelem

20. § Az adatok illetéktelen személy(ek)hez kerülésének megakadályozása érdekében:
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (alapelvi szintű követelmény, hogy a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá);
- a biztonsági másolatok csak az illetékes vezető engedélyével adhatók ki;
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell;
- adatokat átadni nem azonos szervezeti egységben, vagy biztonsági szinten levő személynek csak a szervezeti egység vezetőjének engedélyével lehet,
- adatokat adathordozón, vagy hálózaton keresztül kijuttatni csak a jegyző engedélyével lehet.

Vírusvédelem

21. § A munkaállomásokon aktív védelemmel ellátott vírusirtó szoftvernek kell működnie. A vírusvédelmi programok adatbázisát naprakészen kell tartani.

22. § Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az 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 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. Amennyiben külső adathordozóról/hálózatból szükséges adatokat a Hivatal informatikai rendszerébe juttatni, az adathordozót csatlakozáskor, vagy a külső hálózatból érkező adatokat vírusirtóval át kell vizsgálni.

Szoftvervédelem

23. § (1) Az informatikusnak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

(2) 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

24. § (1) A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
a) Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
b) A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

(2) 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.

(3) Programok megőrzése, nyilvántartása:
a) a programokról naprakész nyilvántartást kell vezetni;
b) a nyilvántartásból egyértelműen megállapíthatónak kell lennie a program azonosítására és kezelésére vonatkozó adatoknak.

(4) Programok fizikai védelme érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni.

Hardver védelem

25. § A hardver védelme érdekében:
- a számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a szerverszobában klímaberendezés használata ajánlott;
- szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerverszobában kell elhelyezni;
- a számítógép-hálózat csatornáit lehetőség szerint 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, alapvető követelmény, hogy a sűrűn használt utat szabadon kell hagyni;

- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (hivatali informatikus), illetve a szervizek szakemberei nyúlhatnak bele;

IV. FEJEZET
KÖZÉRDEŰ ADATOK MEGISMERÉSÉNEK SZABÁLYAI

Közérdekű adatok, információk, valamint dokumentumok meghatározása

26. § Az Infotv. 26 §-a, valamint egyéb jogszabályok alapján közérdekű, nyilvános adat különösen az Önkormányzat költségvetésével és annak végrehajtásával, vagyonával és annak kezelésével, a közpénzek felhasználásával, szervei feladatkörével, működésével, tevékenységével, átláthatóságával, ellenőrizhetőségével kapcsolatos információk.

27. § (1) A kötelezően közzéteendő közérdekű információk az Infotv. előírásaira tekintettel:
a) az Önkormányzat feladat- és hatáskörével, működésével, kapcsolatos információk – dokumentumok- keretében: az Önkormányzat Szervezeti és Működési Szabályzata, éves költségvetése, éves költségvetési beszámolója, a képviselő-testület nyilvános ülésein hozott rendeletei, határozatai;
b) a Hivatal működésével, szervezetével kapcsolatos információk, dokumentumok;
c) továbbá mindaz, amit jogszabály közérdekűvé nyilvánít.

(2) Nem tehetők hozzáférhetővé azok az adatok,
a) melyeket törvény alapján az arra jogosult szerv állami, vagy szolgálati titokká nyilvánított,
b) melyek a nemzetközi szerződésből eredő kötelezettség alapján minősített adatok,
c) melyek esetében a közérdekű adatok nyilvánosságához való jogot- az adatfajták meghatározásával – törvény más nevesített okból, illetőleg bírósági vagy közigazgatási hatósági eljárásra való tekintettel a nyilvánosságra hozatalt korlátozza,
d) melyek esetében
- az adatfajtára vonatkozó külön törvény a nyilvánossá tételt kizárja vagy korlátozza,
- a Ptk. előírásai alapján üzleti titok szabályait kell alkalmazni.

28. § A keletkezésüktől számított 10 éven belül nem hozhatók nyilvánosságra a feladat- és hatáskörbe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített és a döntés külső befolyástól mentes előkészítését, megalapozását szolgáló adatok, dokumentumok. Ezen adatok megismerését a jegyző hatáskörébe tartozó ügyek esetén a jegyző engedélyezi. Jogszabály egyes adatok megismerhetőségének korlátozására a fent meghatározottnál rövidebb időtartamot állapíthat meg. A döntés megalapozását szolgáló adat megismerésére irányuló igény tíz éves időtartamon belül – a döntés meghozatalát követően akkor utasítható el, ha az adat megismerése a hivatal törvényes működésének rendjét vagy feladat – és hatáskörének illetéktelen külső befolyástól mentes ellátást, így különösen az adatot, keletkeztető álláspontját a döntések előkészítése során történő szabad kifejtését veszélyeztetné.

29. § Azon ügyek, illetőleg dokumentumok esetén, amelyekben mind a személyes, illetőleg az üzleti titkot jelentő, mind a közérdekű adatok előfordulnak, biztosítani kell az adatok pontosítását és a személyes, az üzleti titkot képező adatok elhatárolását. Amennyiben a közérdekű dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz úgy a kiadott másolaton felismerhetetlenné, kell tenni ezen adatokat.

A közérdekű adatok előkészítése

30. § A közérdekű adatok feldolgozása, előállítása a jogszabály által meghatározott formában és határidőre történő elhelyezése az illetékes belső szervezeti egység feladata.

31. § Az interneten csak hiteles, a jogszabályi előírásoknak megfelelő tartalmú és formájú információk helyezhetők el. Az adatok hitelességéért, megbízhatóságáért, a jogszabályban meghatározott formában történő előállításáért, a szükséges aktualizálásáért az illetékes belső szervezeti egység vezetője személyileg felelős. A belső szervezeti egység vezetője felelős azért, hogy a megjelenő jogszabályok által közérdekűvé nyilvánított adatok előírás szerinti publikálását biztosítsa.

Az igény vizsgálata, intézése
Nyilvántartás az elutasított kérelmekről

32. § (1) A beérkezett igényeket haladéktalanul meg kell vizsgálni abból a szempontból, hogy
a) az adatközlés teljesítéséhez szükséges adatokat tartalmazza-e,

b) a megismerni kívánt adatok köre pontosan meghatározható-e,
c) az adatok ténylegesen a Hivatal kezelésében vannak-e.

(2) Amennyiben az igény nem tartalmazza az igény teljesítéséhez, valamint a döntéshez szükséges adatokat – ideértve azt az esetet is, ha az ügyfél a megismerni kívánt adatot nem tudja pontosan megjelölni – az ügyintéző haladéktalanul felveszi a kapcsolatot az ügyféllel és segítséget nyújt a megismerni kívánt adatok körének pontos meghatározása érdekében.

(3) A közérdekű adatok megismerésére irányuló kérelmek elutasításáról nyilvántartást kell vezetni. A nyilvántartás tartalmazza:
a) a közérdekű adatok megismerésére irányuló kérelem benyújtásának időpontját,
b) a megismerni kívánt közérdekű adatok körét, az elérés módját,
c) az elutasítás a megtagadás, dátumát, indokát nem elérhető nem nyilvános minősítését.

(3) A Hivatal évente, az adatvédelmi biztos közleményében meghatározott időpontra értesíti az adatvédelmi biztost az elutasított igényekről, valamint az elutasítások indokairól.

Jogorvoslati eljárás szabályai

33. § (1) Ha a Hivatal az igénylő közérdekű adatra vonatkozó igényét nem teljesíti, az igénylő az Infotv. 31. §-ban foglalt eljárási rendnek megfelelően bírósághoz fordulhat. A megtagadás jogszerűségét és megalapozottságát a Hivatal köteles bizonyítani.

(2) A fenti rendelkezések nem alkalmazhatók a közhitelű nyilvántartásból történő – külön törvényben szabályozott – adatszolgáltatásra.

V. FEJEZET
A SZEMÉLYES ADATOK KEZELÉSÉVEL KAPCSOLATOS SZABÁLYOK

Személyes adatok kezelésének jogszerűsége

34. § (1) A Hivatal belső szervezeti egységeinek feladatkörük ellátása céljából részben jogszabály alapján elrendelt nyilvántartások, részben saját készítésű dokumentumok, adatbázisok létesítése, aktualizálása, az adott ellátási formát igénybevevők, közfeladatra jelentkezők azonosítása, közbeszerzésre, vállalkozási feladatra pályázók, illetve e pályázatok stb. nyilvántartásba vétele, irányítási jogkör gyakorlása, döntés előkészítése érdekében személyes adatkezelésre az Isztv. és az adott feladatra vonatkozó külön törvény előírásai alapján kerül(het) sor.

(2) Ennek megfelelően:
a) az érintett hozzájárulása alapján, a hozzájárulás beszerzésével, valamint a hozzájárulás megadásáról szóló dokumentumnak az érintett részéről történő átadásával (aláírásával), és az iratokhoz csatolásával;
b) a kérelem alapján induló eljárás esetén az alapeljárás keretében benyújtott kérelem figyelembevételével az érintett (a kérelmező) az eljárás szerint szükséges adatai kezeléséhez való hozzájárulásának a vélelmezésével kerülhet sor; mely tényre az érintett figyelmét fel kell hívni. Ennek megtörténtét az iraton rögzíteni kell.
c) A közszereplés során az érintett által már nyilvánosságra hozott (a nyilvánosságra hozatal dokumentálható helyének, idejének, módjának az iraton történő feltüntetésével), illetőleg kifejezetten a nyilvánosságra hozatal céljából átadott adatok esetében a hozzájárulást megadottnak kell tekinteni;
d) Ha jogszabály a következő adatkezelést az adatkezelés céljának és feltételeinek, a kezelendő adatok körének és megismerhetőségének, az adatkezelés időtartamának, valamint az adatkezelő személyének a meghatározásával elrendelte;
e) A különleges adatok esetében az érintett előzetes írásbeli nyilatkozata alapján, annak csatolásával, valamint az Infotv. 3. § 3. a) pontban foglalt adatok esetében nemzetközi egyezményen alapul vagy az Alaptörvényben biztosított alapvető jog érvényesítése érdekében törvény elrendeli;
f) Az érintettel írásban kötött szerződés alapján, ha az abban foglaltak teljesítése érdekében a hozzájárulást megtagadta.
A szerződésnek tartalmaznia kell:
- a kezelendő adatok meghatározását,

- az adatkezelés időtartamát,
- a felhasználás célját, (például közérdekű adatok keretében történő nyilvánosságra hozatal tényét, és 5 éves nyilvános kezelést),
- az érintett azon nyilatkozatát, hogy a szerződés aláírásával hozzájárul adatainak a szerződésben foglaltaknak megfelelő kezeléséhez, nyilvánosságra hozatalához, amennyiben az adatok továbbításra kerülnek, illetőleg adatfeldolgozó igénybevételre kerül sor, ahhoz is hozzájárulását adja.

Személyes adatok kezelésének célhoz kötöttsége

35. § Az Adatkezelő a személyes adatokat – azok keletkezésétől a megsemmisítésükig – kizárólag az eredeti rendeltetési célra használhatja. Az eredeti rendeltetéstől eltérő célú felhasználásra csak akkor kerülhet sor, ha a törvény azt lehetővé teszi, vagy az érintett ahhoz írásban hozzájárult.

36. § A közérdekű feladatok, illetőleg a jogszabályon alapuló kötelezettségek teljesítése során felmerült személyes adatok csak a jogszabályi előírásoknak megfelelő célra és ideig használhatóak fel. Az Adatkezelő felelős azért, hogy a tudomásra jutott személyes adatokat, illetőleg ilyen adatokat tartalmazó dokumentumokat kizárólag a jogszabály előírásainak megfelelően használja fel, és azokat harmadik személyek részére nem teheti hozzáférhetővé.

37. § A képviselő-testület, valamint bizottságai részére készülő előterjesztések, tájékoztatók és azok mellékletei személyes adatokat csak a jogszabály szerinti kötelezettség teljesítése érdekében és csak a jogszabály szerinti terjedelemben tartalmazhatnak.

38. § Az irányítási jogkör gyakorlása, a döntés előkészítés keretében az Infotv. 26. § (1)-(3) bekezdésében, továbbá az egyéb jogszabályokban meghatározott adatkört meghaladó, a személyes, az üzleti titok fogalomkörébe tartozó adatokat vagy ilyen adatokat tartalmazó dokumentumokat keletkezésüktől, illetőleg a Hivatal belső szervezeti egységeihez érkezéstől számítottan elkülönítetten „nem nyilvános" adat vagy dokumentumként kell kezelni, és azokat csak az adott ügyben hozandó döntés során lehet felhasználni.

39. § A kezelés során folyamatosan dokumentálni kell egyrészt a betekintésre feljogosítottak nevét, besorolását, másrészt, hogy az adott iratokat, dokumentumokat, ki, mikor és milyen célból tekintette meg.

40. § Ezen dokumentumok nem sokszorosíthatók az ezzel kapcsolatosan a képviselő-testület vagy az illetékes bizottságok részére készülő előterjesztéshez nem csatolhatók. Az előterjesztésben a megjelölt helyen tekinthetik meg a betekintésre jogosultak (a dokumentumok megtekinthetők az előterjesztés előkészítésért felelős belsőszervezeti egység meghatározott helyiségében, a betekintésre megjelölt időpont, vagy időtartam meghatározásával).

41. § Az ezzel kapcsolatos előterjesztések az Mötv. szerint zárt ülés keretében tárgyalhatók és a zárt ülésen résztvevők tekinthetik meg a dokumentumokat.

42. § Ezen adatokat, illetőleg dokumentumokat az Infotv. 4. § (2) bekezdése alapján csak a cél megvalósításához szükséges mértékben és ideig lehet kezelni.

43. § A pályázatok, ajánlatok keretében benyújtott dokumentumokat azok tartalma szerint kell megítélni, és a vonatkozó jogszabályok előírásai szerint kell kezelni.

44. § Amennyiben az ajánlatok bontása során megállapításra kerül, hogy az ajánlattevő az üzleti titok körébe tartozó adatokat, dokumentumokat közöl, csatol be azokat a bontást követően elkülönítetten az 32. §-ban foglaltak szerint kell kezelni.

45. § Az érintett írásbeli hozzájárulása alapján olyan adatok kezelésére is sor kerülhet, amelyet jogszabály nem ír elő. Az így kezelt adatok csak arra a célra használhatóak, amelyekre az érintett hozzájárulását megadta.

A személyes adatok kezelésének biztonsága

46. § (1) Az adatkezelés teljes folyamatában az Adatkezelő köteles biztosítani, hogy a személyes adatokhoz mind a manuális, mind az automatizált feldolgozás (nyilvántartás), mind az elektronikus

ügyintézés során csak az Infotv. és a külön törvény szerinti felhatalmazással rendelkezők férhessenek hozzá. Az automatizált feldolgozás során olyan intézkedések szükségese, melyek:

a) megakadályozzák, hogy illetéktelen személyek a számítógépes adatállományhoz hozzáférjenek,
b) megakadályozzák a tárolóeszközök jogosulatlan olvasását, másolását, módosítását, eltávolítását, megváltoztatását,
c) megakadályozzák, hogy illetéktelen személyek az adatfeldolgozó rendszert adatátviteli eszközök útján elérjék, károsítsák,
d) biztosítják, hogy a jogosult felhasználók csak a hozzáférési joguk szerinti személyes adatok köréhez férjenek hozzá,
e) rögzítik, hogy az adatfeldolgozó rendszert ki, mikor milyen célból érte el továbbá ki és milyen adatrögzítést, módosítást, másolást, stb. hajtott végre,
f) biztosítsák annak az ellenőrzését, hogy mikor, mely személyes adat került kezelésre és azt ki végezte.

(2) A konkrét egyedi ügyekben az eljáró belső szervezeti egység vezetője felelős azért, hogy az eljárás minden mozzanata és az abban közreműködő személyek megállapíthatóak legyenek, az eljárás során keletkezett iratok illetéktelen személyek birtokába ne kerülhessenek.

Az érintettek jogai

47. § (1) Az érintett jogosult tájékoztatást kérni személyes adatai kezeléséről: sor került-e személyes adatai kezelésére, nyilvántartására, ha igen tájékoztatást kérhet, az adatkezelés céljáról, jogalapjáról, időtartamáról, kik és milyen célból kapták meg az adatait.

(2) Az érintett kérelmére lehetővé kell tenni, hogy személyes adatait tartalmazó nyilvántartásba, az adott feladat ellátására vonatkozó külön törvény szabályai szerint betekinthessen.

(3) Az érintett elírás, tévedés esetén kérheti azok helyesbítését. Amennyiben a pontosítást jogszabályi feltételei biztosítottak úgy az Adatfelelős a jogszabályi előírásoknak megfelelően a szükséges intézkedést megteszi, ellenkező esetben tájékoztatja az érintettet a helyesbítés jogszabály szerinti lehetőségekről.

(4) Az érintett személyes adatai kezelésével kapcsolatos kérelmét szóban vagy írásban terjesztheti elő. A szóban előterjesztett kérelemről jegyzőkönyvet kell felvenni. Az előterjesztett kérelemre 30 napon belül kell választ adni.

(5) A betekintésnél biztosítani kell, hogy a betekintő csak a rá vonatkozó, és a külön törvény előírásai szerint általa megismerhető adatokat tekintse, illetőleg ismerje meg. A betekintésről szükség szerint jegyzőkönyvet kell felvenni, vagy azt az iraton rögzíteni kell, úgy hogy az tartalmazza:

a) a betekintés időpontját és célját
b) a jelenlévők nevét és minőségét
c) a betekintés során tett megállapítást vagy észrevételt
d) a jelenlévők aláírását.

(6) Az érintett tiltakozhat személyes adatai kezelése ellen, ha

a) a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el;
b) a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;
c) a tiltakozás jogának gyakorlását egyébként jogszabály lehetővé teszi.

(7) Az érintett tiltakozásában foglaltakat haladéktalanul ki kell vizsgálni, és a vizsgálat eredményéről az érintettet legkésőbb 15 napon belül írásban tájékoztatni.

(8) A személyes adatok törlésére kerül sor. Ha azok nyilvántartása törvényellenes, vagy az adatok a valóságnak nem felelnek meg és nem korrigálhatóak, az adatkezelés megszűnt, illetőleg a tárolásra a jogszabály által megállapított határidő lejárt, vagy a törlést arra jogosult szerv elrendelte.

Az adatkezelés, az adattovábbítás összekapcsolása

48. § A Hivatal belső szervezeti egységei által kezelt személyes adatokat tartalmazó rendszerek összekapcsolására, továbbítására csak akkor kerülhet sor,

a) ha azt törvény megengedi, vagy
b) az érintett ahhoz előzetesen hozzájárult

és az adatkezelés jogszabályi feltételei minden esetben teljesülnek.

A személyes adatokkal kapcsolatos nyilvántartások

49. § (1) A nyilvántartás során – egyedi ügyben az iraton vagy az előadói íven – rögzíteni kell, hogy:

a) ki, vagy mely szervezet kérte a személyes adatok kiadását, illetőleg a betekintés lehetőségét,
b) milyen célból,
c) a teljesítésre milyen jogcímen került sor.
   - törvény alapján
   - az érintett írásbeli hozzájárulásával vagy az Infotv. 6. § (7) bekezdése alapján a közszereplése során általa már közölt vagy nyilvánosságra hozatal céljából átadott adatokról van szó,
   - az Infotv. 6. § (6) bekezdése alapján az – érintett kérelmére – indult eljárásban a hozzájárulás vélelmezésével,
d) mikor történt az adatszolgáltatás, a betekintés.

(2) Az érintett kérheti, hogy a rá vonatkozó adatokat, illetőleg a személyes adatait megismerőkről információt kapjon.

Személyes adatok kezelésének különös szabályai

50. § Az érintettel kötendő és a kötelezően közzéteendő közérdekű adatok körébe tartozó szerződések esetén a szerződésben rögzíteni kell, hogy az érintett tudomásul veszi és hozzájárul személyes adatai (neve, a szerződés megnevezése, típusa, tárgya, értéke, időtartama, és esetleges módosulásuk) közérdekű adatként történő nyilvánossá tételéhez, és 5 éven keresztül történő nyilvános kezeléséhez. Amennyiben az érintett nem járul hozzá úgy a szerződés megkötésére, nem kerülhet sor.

51. § Pályázat kiírásakor, az érintettekkel közölni kell, hogy pályázatuk, ajánlatuk érvényességi feltétele, az a) pont szerinti adatok nyilvánosságra hozatalához történő hozzájárulásuk. Ennek korlátozására irányuló nyilatkozat érvénytelen.

52. § Amennyiben az érintett személyes adatának kiadását harmadik személy (természetes vagy jogi személy) az adatszolgáltatás jogcímének megjelölésével kéri, és az nem tartozik az a) vagy a b) pont hatálya alá, és azt törvény nem zárja ki úgy az adatszolgáltatás teljesítése előtt az érintettet tájékoztatni kell törvényes jogairól és az adatszolgáltatás teljesítésére nyilatkozata alapján kerülhet sor.

53. § A polgárok személyi adatainak és lakcímének nyilvántartásából történő adatszolgáltatás engedélyezése során a kérelem benyújtására és teljesíthetőségének elbírálására az Nytv. valamit a végrehajtására kiadott 146/1993. (X. 26.) Korm. rendelet rendelkezéseit kell alkalmazni. Az adatszolgáltatásért fizetendő igazgatási szolgáltatási díjra a polgárok személyi adatainak és lakcímének nyilvántartásából teljesített adatszolgáltatásért, a kapcsolatfelvétel céljából való megkeresésért, valamint értesítésért fizetendő igazgatási szolgáltatási díjról szóló 16/2007. (III. 13.) IRM-MeHVM együttes rendelet előírásait kell alkalmazni.

VI. FEJEZET
INFORMATIKAI BIZTONSÁGI SZABÁLYOK

Informatikai jogosultsági szintek

54. § A Szabályzat alkalmazásában az alábbi informatikai jogosultsági szinteket különböztetjük meg:

a) Felhasználó – alap szint,
b) Szoftver adminisztrátor – adott szoftver jogosultságait, beállításait kezeli,
c) Vezető – a területéhez tartozó jogokat, beállításokat módosíthatja,

d) Rendszergazda – minden informatikai rendszer minden jogosultságát, beállítását módosíthatja.

Általános védelmi, biztonsági szabályok

55. § (1) A szerverszobában az informatikuson kívül más csak az informatikus, vagy a jegyző jelenlétében vagy engedélyével tartózkodhat.

(2) Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát az adatvédelmi felelős és/vagy az informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben.

(3) Az irodákban, szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért az informatikus a felelős.

(4) A szerverszobában tüzet okozó tevékenységet folytatni szigorúan TILOS!

(5) A szerverszoba takarítását csak az informatikus felügyelete mellett, legalább hetente egyszer, a kijelölt személyek végezhetik.

(6) A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak az informatikus és a szervizek szakemberei végezhetnek.

(7) A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.

(8) Adathordozókat csak az informatikus engedélyével lehet be- és kivinni a szerverszobából.

(9) Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.

(10) A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet.

(11) Munkaállomások védelme:
a) a számítógépeket csak indítójelszóval lehet elindítani, az indítójelszavat időnként meg kell változtatni, a jelszavak nem adhatók ki illetéktelen személynek;
b) induláskor minden esetben vírus-ellenőrző programot kell elindítani;
c) a teljes anyagról időnként mentéseket kell készíteni;
d) a teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni és ezt a 2. számú mellékletben meghatározott módon kell megőrizni. Ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény).
e) felhasználó szoftvert csak az illetékes vezető engedélyével és a rendszergazda ellenőrzése mellett telepíthet.

(12) Az internet használat szabályai:
a) tilos a szervezettel kapcsolatos információkat nyilvános internetes oldalakon engedély nélkül megosztani, vagy ilyen oldalakon a Hivatal nevében nyilatkozni,
b) tilos illegális programokat, adatokat, iratokat, szerzői jogokat sértő fájlokat megosztani,
c) kerülni kell a személyes információkat, email címeket bekérő oldalakat.

(13) Az elektronikus levelezés szabályai:
a) a levelek nem tartalmazhatnak hatályos magyar jogszabályba ütköző anyagokat,
b) a levelek nem sérthetik mások becsületét, emberi jogait; faji, nemzetiségi hovatartozását; politikai, vallási világnézetét,
c) a levelek tartalma nem sérthet szerzői jogokat,
d) a levelezés nem veszélyeztetheti a hálózati infrastruktúra működését,

e) tilos:
- kéretlen leveleket (SPAM) küldeni,
- a levelek fejlécének megváltoztatása, hamis levelek küldése,
- levelezési címet olyan listára feltenni, amelyről a hivatali levelező rendszert levélszeméttel terhelhetik meg,
- hivatali dokumentumokat, adatokat engedély nélkül nem hivatali címre továbbítani,
- más személyazonosságát ellopni: más email címével, nevével visszaélni, az ő nevében levelet küldeni,

f) munkához kapcsolódó hivatalos levelezésre csak a hivatali e-mail címek használhatók,
g) minden dolgozó, aki rendelkezik az elektronikus levelező rendszerhez hozzáféréssel köteles rendszeresen használni azt, a levelező rendszerbe minden munkanapon be kell jelentkezni és naponta többször ellenőrizni kell, hogy érkezett-e új levél.

(14) Információs rendszerek jogosultságainak kiadása, visszavétele:
a) az alkalmazottnak a munkahelyre történő belépéskor a munkájához szükséges jogosultságokat mihamarabb meg kell kapnia, ez tartalmazza a számítógép, levelező rendszer, és a munkaterületéhez igazodó szoftverek, rendszerek őt megillető jogosultságait, jogosultsági szintjétől függően
b) munkahelyről történő kilépéskor a jogosultságok azonnal megszűnnek, illetve, ha a munka jellege megköveteli, ideiglenesen más veszi át azokat az aktuális munkafolyamat lezárulásáig vezetői engedéllyel.

Az informatikai beszerzések szabályai

56. § A beszerzéseket a közbeszerzésekről szóló 2015. évi CXLIII. törvény és Hajdúsámson Város Polgármesteri Hivatala Beszerzési Szabályzata figyelembevételével kell lebonyolítani.

Teendők káresemény bekövetkezésekor

57. § (1) Ha az informatikai eszközökben kár keletkezik, a Hivatali rendszergazdát azonnal értesíteni kell a kár mielőbbi elhárítása érdekében.

(2) Ha a kár fizikai jellegű vagy adatvesztést okozhat, az eszközt ki kell kapcsolni, áramtalanítani kell.

(3) Ha a kár szoftveres jellegű, a rendszergazda utasításától függően vagy ki kell kapcsolni az érintett rendszert, vagy a káresemény bekövetkezésekor fennálló állapotot kell megőrizni a kivizsgálásig, elhárításig.

(4) Az elhárítás során elsődleges a munkafolyamatok folytonosságának biztosítása.

A Hivatal biztonsági osztályba sorolása

58. § (1) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 7. § (3) bekezdése alapján a biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

(2) Az Ibtv. 8. § (1) bekezdése alapján a biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

VII. FEJEZET
ZÁRÓ RENDELKEZÉSEK

59. § Jelen Szabályzat 2018. év január 1. napján lép hatályba.

60. § Jelen Szabályzat hatályba lépésével egyidejűleg a 2014. szeptember 15. napján kiadott Adatvédelmi és Informatikai Biztonsági Szabályzat hatályát veszti.

Hajdúsámson, 2018. január 1.

Hajdúsámson Város Jegyzője

Dr. Danku József
jegyző

Megismerési Nyilatkozat az Adatvédelmi és Informatikai Biztonsági Szabályzatban foglaltak megismeréséről és tudomásul vételéről

Név	Aláírás

1. melléklet

A 2014. évben megtörtént az informatikai rendszer biztonsági osztályba sorolása.

A Polgármesteri Hivatal informatikai rendszere törvényi szabályozás szerint 2-es biztonsági szinten van.

A hiányosságok javítását 90 napon belül cselekvési tervben kell rögzíteni.

Az értékelés dokumentálásra kell kerüljön.

Kárérték-táblázatok

Bizalmasság kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adat bizalmasságának sérülése esetén a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Társadalmi-politikai hatás	Jogi következmény
2. / csekély kár	1.000.000 Ft-ig	Kínos helyzet a szervezeten belül	Belső szabályozóval védett adat vagy néhány személyes adat bizalmassága sérül

Sértetlenség kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adat pontatlansága esetén a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Közvetett anyagi kár	Társadalmi-politikai hatás
2. / csekély kár	1.000.000 Ft-ig	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül

Rendelkezésre állás kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Közvetett anyagi kár	Társadalmi-politikai hatás	Szolgáltatási időszak (nap x óra)	Szolgáltatási szint (heti maximum kiesési idő)
2. / csekély kár	1.000.000 Ft-ig	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül	5x8	96,5% hetente 1,5 óra

Belső adatvédelmi felelős kijelölése

A szabályzat alapján az adatvédelmi felelősi feladatok ellátásával megbízott köztisztviselő:

- neve:

- beosztása:

Hajdúsámson, 2018. 01. 10.

.....
jegyző

Záradék: az adatvédelmi feladatok ellátásra való kijelölést tudomásul veszem, a Szabályzatot és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Hajdúsámson, 2018. 01. 10.

.....
aláírás

Hajdúsámsoni Polgármesteri Hivatal
kiemelt rendszer- és felhasználói programjai,
illetve azok mentési rendje

1. Kiemelt felhasználói programok szervezeti egységek szerint, a programoknál az adattárolás módjának megjelölésével:

Adó csoport:

- ÖNKADÓ – helyi (arhivált)
- ASP-ADÓ – távoli

Iktató:

- ASP-IRAT – távoli
- DMS One Iktató rendszer – helyi (arhivált)

Pénzügy:

- ASP-GAZDÁLKODÁS – távoli
- Polisz – távoli (arhivált)
- tatigazd – helyi (nem módosul)
- kis és nagy értékű tárgyi eszköz nyilvántartó – helyi (arhivált)

Szociális és Gyámügyi Iroda:

- Közszolgálati szoftverház szociális programcsomag – helyi
- PTR – távoli

Jogi és Szervezési Iroda:

- KIR – távoli (arhivált)
- KIRA – távoli
- ASP-IVK – távoli
- ASP-TELEPÜLÉS – távoli
- HONLAP - távoli

Anyakönyvvezető:

- Vizuál Regiszter népesség nyilvántartó – helyi
- ASZA – távoli
- EAK – távoli
- VÜR – távoli

Biztonsági mentés a helyi adat tárolású (helyi adatbázisú) programoknál valósul meg, a távoli adatbázisokat a távoli elérésű programok szolgáltatói végzik.

2. Rendszerprogramok:

Windows Server 2008 R2, pfSense

3. A mentési rend

A szerverszobában elhelyezett Windows server külön merevlemezére történik a mentés az alábbi eljárás szerint:

napi mentések: minden nap 1:00 és 12:00;

4. Az adatok mentése, az adathordozók biztonsága

4.1. A napi adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott fájlokat naponta, a munka befejezésével az adatmentés helyének kijelölt külső adathordozóra kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba (vagy feltöltheti az erre a célra létrehozott FTP tárhelyre).

(2) A külső, biztonságos másolatokat tartalmazó adathordozót csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni (FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg kell szakítani).

(3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább frissebb adatmentés az állományokról.

5. Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.
(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az adatvédelmi felelős további utasításági nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó adattárolóhoz.
(3) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.
(4) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) haladéktalanul értesíti a Hivatal rendszergazdáját.
(5) A rendszergazda kiérkezéséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését (senki nem nyúlhat hozzá, még az adatvédelmi felelős sem).

6. Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

Nyilatkozat a hozzáférési jogosultság létrehozásához

Az elektronikus információs rendszerhez való hozzáférés érdekében a törvény írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

Megismertem a biztonsági szabályokat és megkaptam a jogosultságokat a következő rendszerekhez:

-
.....
.....

-
.....
.....

-
.....
.....

-
.....
.....

Tudomásul veszem, hogy a munka során szerzett információkkal kapcsolatban titoktartás kötelez.

Kelt :.....

.....
aláírás