Csabacsűdi Közös Önkormányzati Hivatal

Adatvédelmi és Informatikai Biztonsági Szabályzat

|  |
| --- |
|  |

**I. Bevezetés**

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény (a továbbiakban: Isztv.) részletesen szabályozza a személyes adatok védelmével, és a közérdekű adatok nyilvánosságával kapcsolatos legfontosabb teendőket, illetőleg az alapvető jogok érvényesülését

Magyarország Alaptörvényének VI. cikk 82) bekezdése értelmében „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez”. Ezen alapvető jogok védelme és tiszteletben tartása az állam és az önkormányzatok elsőrendű kötelessége.

Csabacsűdi Közös Önkormányzati Hivatalának Adatvédelmi és Informatikai Biztonsági Szabályzatát az Isztv., a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv. (a továbbiakban: Nytv.), és az annak végrehajtására kiadott 146/1993. (X.26.) Korm. rendeletben, illetve a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. Törvényben foglaltak alapján, továbbá a Nytv. 30. § (1) bekezdésben kapott felhatalmazás alapján, az államháztartásról szóló 2011. évi CXCV. Törvény ( a továbbiakban Áht.), a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. Törvény ( a továbbiakban Ötv.) alapján a Polgármesteri Hivatal ( a továbbiakban: Hivatal) adatvédelemmel összefüggő feladatait és eljárási rendjét az alábbiak szerint szabályozom.

**II. Általános szabályok**

## A szabályzat célja

A szabályzat célja, hogy biztosítsa Csabacsűdi Közös Önkormányzati Hivatal és intézményei, alkalmazottai által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A cél egyrészt biztosítani az alapvető jogok érvényesülését a Hivatalban folyó munkavégzés során, másrészt biztosítani az előírt feladatok ellátása keretében az adatvédelem szabályainak, valamint a lakosság tájékoztatására vonatkozó előírások betartását, továbbá eleget tenni az Isztv. 24. § (3) bekezdése szerinti kötelezettségnek, mely szerint az állami és önkormányzati adatkezelőknek, e törvény végrehajtása érdekében, adatvédelmi és adatbiztonsági szabályzatot kell készíteniük, amely a polgárokat megillető és a jogszabályok által rögzített jogok érvényesülését biztosítja és meghatározza a Hivatal belső szervezeti egységei ezzel kapcsolatos kötelezettségeit.

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 számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
* a számítógépes 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, illetve minimális mértékre csökkentését,
* 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

## A szabályzat hatálya

E szabályzat személyi hatálya a Hivatallal közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, valamint a munkaviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, közszolgálati munkavállalókra terjed ki.

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

## A közszolgálati nyilvántartásra vonatkozó szabályok

### 3.1. Általános szabályok

Személyi iratként kell kezelni minden olyan adathordozót, amely a közszolgálati jogviszony:

* létesítésekor
* fennállása alatt
* megszűnésekor
* illetve azt követően keletkező
* és a köztisztviselő személyével összefüggő adatot, megállapítást tartalmaz.
* Eszerint személyi iratok:
* a személyi anyag iratai,
* a közszolgálati jogviszonnyal összefüggő egyéb iratok,
* a köztisztviselőnek a közszolgálati jogviszonyával összefüggő más jogviszonyaival kapcsolatos iratok,
* a köztisztviselő saját kérelmére kiállított vagy önként átadott adatokat tartalmazó iratok.
* Személyi anyag közé az alábbi iratok tartoznak a köztisztviselő közszolgálati jogviszonyával kapcsolatos iratok közül:
* a köztisztviselő 5 évnél nem régebbi fényképe,
* adatnyilvántartó lap,
* önéletrajz,
* erkölcsi bizonyítvány,
* esküokmány,
* kinevezés, annak módosítása,
* címadományozás,
* besorolásról rendelkező irat,
* vezetői megbízás és annak visszavonása,
* visszatartásról rendelkező irat,
* áthelyezésről rendelkező irat,
* minősítés,
* a közszolgálati jogviszonyt megszüntető irat,
* a hatályban lévő fegyelmi büntetést kiszabó határozat,
* a közszolgálati igazolás másolata.

A személyi anyagokat adott személyre vonatkozóan együttesen kell tárolni.

A személyi iratokat a központi iktatás keretében iktatni kell.

Az így beiktatott személyi iratokat tartalmuknak megfelelően csoportosítva, keletkezésük sorrendjében, az e célra személyenként kialakított gyűjtőben kell őrizni. Az így elhelyezett iratokról tartalomjegyzéket kell készíteni, amely tartalmazza az iktatószámot és az ügyirat keletkezésének időpontját. A tartalomjegyzékre azonnal rá kell vezetni a változásokat.

A személyi anyagra csak olyan adat és megállapítás vezethető, amelynek alapja:

* + közokirat vagy a köztisztviselő írásbeli nyilatkozata,
  + a munkáltatói jogkör gyakorlójának írásbeli rendelkezése,
  + bíróság vagy más hatóság döntése,
  + jogszabályi rendelkezés.

A közszolgálati jogviszony megszűnése után a köztisztviselő személyi iratait -kivéve a vagyonnyilatkozat tételével összefüggő személyi iratokat – a központi irattárban kell elhelyezni.

Az így irattározott anyagokat a „megszűnt” csoportban kell tárolni, hogy az elkülönítés biztosított legyen.

A személyi anyagot a közszolgálati jogviszony megszűnésétől számított ötven évig meg kell őrizni. Tárolásról és levéltárba helyezésről a szerv egyéb (ügyiratkezelési) szabályzata és melléklete rendelkezik.

A személyi iratok tárolási módja megegyezik a közszolgálati nyilvántartás tárolási módjával.

A közérdekű adatokon túl a köztisztviselő nyilvántartott adatairól tájékoztatás nem adható; személyi anyagát a Kttv.180.§-ában foglalt kivételes esetben lehet kiadni.

A személyi anyagokba való betekintésre jogosultak köre megegyezik a közszolgálati nyilvántartásba betekintésre jogosultak körével.

A személyi anyagok közül a pályázatokra vonatkozó speciális szabályok:

A pályázatok kezelési módja:

* A pályázatokat iktatni kell.
* A benyújtott pályázatokról a munkáltatói jogkör gyakorlója dönt.
* Kinevezni csak azt a köztisztviselőt lehet, aki a pályázati eljárásban részt vett és a pályázati feltételeknek megfelelt.

A benyújtott pályázat tartalma a pályázat elbírálásában résztvevőkön, valamint a közszolgálati alapnyilvántartásba betekinteni jogosultakon kívül csak a pályázó beleegyezésével közölhető harmadik személlyel.

A pályázatok esetében a pályázat eredményéről a pályázókat haladéktalanul, de legkésőbb 8 napon belül írásban kell tájékoztatni.

Az eredménytelenül pályázóknak az értesítéssel együtt meg kell küldeni a teljes pályázati anyagukat is.

Az előadói ívre fel kell vezetni a visszaküldés tényét.

Vissza kell adni a közszolgálati jogviszony létrehozását kezdeményező iratokat akkor is, ha a személy nem pályázott, hanem más szerv küldte meg a személyi anyagot, de a közszolgálati jogviszony nem jött létre.

### 3.2. A közszolgálati alapnyilvántartás adatlapjai vezetésének adatvédelmi szabályai

#### 3.2.1. A közszolgálati alapnyilvántartásra vonatkozóan az alábbi szabályokat kell érvényesíteni

a) A Hivatal a foglalkoztatott köztisztviselőkről a 2011.évi CXCIX. törvény 2. mellékletében meghatározott adatkörre kiterjedően nyilvántartást vezet. A mellékletben nem szereplő adatokról adatgyűjtés nem végezhető, ilyen adat nyilvántartása és kezelés tilos.

b) A közszolgálati alapnyilvántartás adatai közül a közigazgatási szerv megnevezése, a köztisztviselő neve, állampolgársága, jogviszony kezdete, továbbá a besorolására, besorolásának időpontjára, munkakörének megnevezésére és a betöltés időtartamára, a vezetői kinevezésének és megszűnésének időpontjára, címadományozásra, illetményre vonatkozó adat közérdekű, ezeket az adatokat a köztisztviselő előzetes engedélye nélkül nyilvánosságra lehet hozni.

c) A közszolgálati alapnyilvántartásban szereplő alapadatokról és változásairól, továbbá a létszám alakulásáról a kormány által megállapított rendben a hivatal folyamatosan adatszolgáltatást végez a központi közszolgálati nyilvántartás részére a Kttv.178.§-ában foglaltak szerint.

d) A Hivatal közszolgálati alapnyilvántartási rendszere törvényi felhatalmazás hiányában más alrendszerrel nem kapcsolható össze.

e) Az alapnyilvántartásról statisztikai célra csak személyazonosításra alkalmatlan módon szolgáltatható adat.

Az alapnyilvántartás adatlapja vezetésének adatvédelmi szabályai különbözőek lehetnek attól függően, hogy a nyilvántartás vezetése milyen módon történik:

* + hagyományosan, kézzel, papír alapon, vagy
  + számítógépes program segítségével.

A nyilvántartási módokra vonatkozó konkrét szabályokat a szabályzat külön része tartalmazza.

#### 3.2.2. A betekintési jog gyakorlásának szabályai az alábbiak szerint kerülnek meghatározásra:

a) A személyzeti szerv köteles biztosítani, hogy a köztisztviselő a róla nyilvántartott adatokba és iratokba korlátozás nélkül betekinthessen, azokról másolatot vagy kivonatot kaphasson.

b) A köztisztviselő jogosult a róla nyilvántartott helytelen adat helyesbítését, a jogellenesen nyilvántartott adat törlését kérni, a jogellenesen kért adata közlését megtagadni. Az adatkezelő köteles a helytelen adatot haladéktalanul helyesbíteni, illetve törölni.

c) A közszolgálati nyilvántartás első alkalommal történő kitöltésekor az érintett köztisztviselőnek aláírásával kell igazolnia, hogy a felvett adatok helyesek és a valóságnak megfelelnek.

d) A köztisztviselő jogosult megismerni, hogy a közszolgálati nyilvántartásban szereplő adatait kinek, milyen célból és milyen terjedelemben továbbították. Ennek biztosítása érdekében a személyi anyagot „Betekintési lap” kimutatással kell ellátni, amelyen dokumentálni kell a személyi anyagba történő betekintés tényét, jogosultjának személyét, jogszabályi alapját és időpontját.

e) A Hivatalnál vezetett alapnyilvántartásba – az eljárásban indokolt mértékig – jogosult betekinteni, illetőleg a központi közszolgálati nyilvántartáson túlmenően abból adatokat átvenni:

* saját adataira vonatkozóan a köztisztviselő,
* a köztisztviselő felettese,
* a minősítést végző személy,
* a törvényességi ellenőrzést végző,
* a fegyelmi eljárást lefolytató testület vagy személy,
* a munkaügyi per kapcsán az eljáró bíróság,
* feladatkörében eljárva a nemzetbiztonsági szolgálatok, valamint a közszolgálati jogviszonnyal összefüggésben indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,
* ügyészi törvényességi feladatkörében eljárva az ügyész,
* a személyes adatok kezelésével összefüggésben a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke,
* a személyzeti, munkaügyi és illetmény-számfejtési feladatokat ellátó szerv e feladattal megbízott munkatársa feladatkörén belül, a Kttv. 2. számú mellékletének I/A., I/B., II., IV., V., VII., VIII. és X. pontokban foglalt adatkörből a köztisztviselő illetményének számfejtése, illetve annak ellenőrzése céljából,
* a közszolgálati statisztikai adatgyűjtéssel összefüggésben a közigazgatási minőségpolitikáért és személyzetpolitikáért felelős miniszter és a Békés Megyei Kormányhivatal kormánytisztviselője feladatkörében.

1. **Általános adatvédelmi és adatbiztonsági szabályzat**

Az információs önrendelkezési jogról és az információszabályságról szóló 2011.évi CXII. tv.(továbbiakban: Isztv.), a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv. és az annak végrehajtására kiadott 146/1993. (X. 26.) Korm. rendeletben, illetve a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvényben foglaltak alapján, az 1992. évi LXVI. tv. 30. § (1) bekezdésében kapott felhatalmazás, valamint az államháztartásról szóló 2011.évi CXCV. törvény, Magyarország helyi önkormányzatairól szóló 2011.évi CLXXXIX. törvény alapján a Hivatal adatvédelemmel összefüggő feladatait és eljárási rendjét a következők szerint szabályozom.

## ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

### A szabályzat célja, hatálya

A szabályzat célja, hogy a rendelkezéseinek figyelembevételével meghatározza a Hivatalban az alapvető jogok érvényesülését a munkavégzés során, és biztosítsa az előírt feladatok ellátása keretében az adatvédelem szabályainak, valamint a lakosság tájékoztatására vonatkozó előírások betartását, továbbá eleget tegyen az Isztv. 24.§ (3) bekezdése szerinti kötelezettségnek.

A szabályzat **személyi hatálya** kiterjed a Csabacsűdi Közös Önkormányzati Hivatalával közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, valamint a munkajogviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra közszolgálati munkavállalókra. Kiterjed továbbá azokra a személyekre, akik az önkormányzattól kapott megbízásuk alapján az Adatvédelmi és Informatikai Biztonsági Szabályzat előírt rendelkezéseivel kapcsolatba kerülnek.

A szabályzat **tárgyi hatálya** kiterjed a Kondorosi Közös Önkormányzati Hivatal belső szervezeti egységei által vezetett nyilvántartásokra, adatbázisokra és valamennyi egyedileg kezelt adatra, elektronikus szolgáltatásokra illetőleg dokumentumokra.

A Hivatalban a nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

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

Az irat 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.

### 1.2. Az adatkezelés során használt fontosabb fogalmak

**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.

**Adatbázis:** számítógépes adatállomány, amelyet megfelelő fejlesztő szoftverrel hoztak létre, előre meghatározott struktúrában és a benne tárolt információk adatbázis kezelő szoftverrel kezelhetők, illetőleg érhetők el.

**Adatkezelő**: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

**Adatkezelés**: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése stb.

**Adatmegsemmisítés:** az adatok, az adathordozók fizikai megsemmisítése, felismerhetetlenné tétele olyan módon, hogy helyreállításuk nem lehetséges.

**Adatközlő**: az a belső szervezeti egység, amely az adatfelelős által szolgáltatott adatokat a jogszabályokban meghatározott módon közzéteszi.

**Adatszolgáltatás a polgárok személyes adataiból**: a nyilvántartásban szereplő polgárok adatainak a törvényben meghatározott tartalmú és terjedelmű közlése. Ezen belül:

* egyedi adatszolgáltatás: egy polgár adatinak közlése,
* csoportos adatszolgáltatás: az adatigénylő által vagy jogszabályban meghatározott szempontok szerint képzett csoportba tartozó polgárok adatainak rendszeres vagy eseti közlése

**Adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele

**Adatvédelem:** az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés, stb. megakadályozása, a személyes adatok esetében kiegészül az adott személy személyes adatai jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.

**Adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges

**Információ**: jelentéssel bíró adat megjelenési módjára vagy formájára való tekintet nélkül

**Kötelezően közzéteendő közérdekű adat:** az Isztv. 26. § (2) – (3) bekezdésében meghatározott körbe tartozó adat

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

**Közérdekű adat**: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és a 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.

**Különleges adat:** a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, továbbá az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat

**Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele

**Polgár természetes személyazonosító adatai:** családi és utóneve(i), nők esetében leánykori családi és utóneve(i) (továbbiakban együtt: név), neme, születési helye és ideje, anyja leánykori családi és utóneve(i) (a továbbiakban: anyja neve)

**Polgár lakcímadata:** bejelentett lakóhelyének, illetve tartózkodási helyének címe (a továbbiakban együtt: lakcím)

**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

**Elektronikus tájékoztató szolgáltatás (tájékoztatás):** az elektronikus közigazgatási szolgáltatás körén kívüli ügyintézésről elektronikus úton hozzáférhetővé tett általános jellegű információs szolgáltatás

**Interaktív szolgáltatás:** az egyszerű tájékoztatáson túlmenően olyan szolgáltatás (például: letölthető űrlapok, kereső rendszerek, tematikus tájékoztatók), amelyek csak a használó aktivitását igényli, a szolgáltatást nyújtó szerv által előkészített dokumentumok kitöltéséhez, felhasználásához.

**felhasználó:** az a személy (vagy szervezet), aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;

**felhasználói jog:** az a jogosultság a hálózaton, amely a felhasználó számára szükséges és elégséges munkájának elvégzéséhez;

**gépterem (iroda):** az a helyiség, amelyben a Hivatal dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz;

**hálózat:** két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;

**hardver:** az informatikai rendszer eszközeit, fizikai elemeit alkotó része;

**informatika:** a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működéséhez;

**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;

**munkaállomás:** egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál;

**rack szekrény:** üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket üzemeltetnek;

**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.

**szerver:** olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza;

**szerverszoba:** az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a kijelölt köztisztviselők, megbízott személyek regisztrálás után juthatnak be;

**vírus:** önállóan nem működő programrész, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet más, az informatikai rendszerben lévő rendszer- illetve felhasználói programra, sokszorozva önmagát és egy beépített feltételhez kötötten (pl. konkrét időpont) pusztítást indít el.

### 1.3. 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, irattározását stb. láthatják el.
* A Képviselő-testület, a bizottságai, valamint a Hivatal tevékenységének átláthatóbbá tételét szolgáló, illetőleg a jogszabályok által közérdekűnek – nyilvánosnak – minősített adatok kezelését, majd ezek közzétételét kötelesek biztosítani.

Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért, védelméért és szolgáltatásáért.

E szabályzatot a Polgármesteri Hivatal

* Szervezeti és Működési Szabályzatával, és
* Informatikai Katasztrófa Tervével összhangban kell alkalmazni.

### 1.4. Az adatvédelem tárgya

Az adatvédelem folyamatában a védelem tárgya:

* a Hivatal működése során keletkezett személyes és közérdekű adatok teljes köre, keletkezésüktől a megsemmisülésükig,
* az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, illetőleg közérdekű adatokat tartalmaznak. Az adathordozók lehetnek papír alapú iratok, kimutatások, listák, térképek, műszaki dokumentációk, mágneses adathordozók, informatikai rendszerek,
* az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

#### 1.4.1 Az adatkezelés alapkövetelményei

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.

Az adatkezelés során biztosítani kell:

* az adott egyén szempontjából fontos adatok helyes, pontos kezelését. A hibás adat előfordulása estén annak észlelésekor hivatalból, valamint az érintet kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell,
* az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába,
* a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását,
* a különböző célú adatok adatállományok (adatbázisok) folyamatos vezetését, aktualizálását 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,
* 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 – kezelését,
* 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 internet kapcsolódására az elektronikus adatok folyamatos rendelkezésre állásának a garantálását
* az adatrendszer (akár számítógépes, akár manuális) fizikai biztonságát, mert az adatok és az adathordozó eszközök összességében jelentős értéket képviselnek, megsemmisülésük esetén újra előállításuk jelentős többletmunkát és költséget igényel

#### 1.4.2. Az adatvédelem eszközei

Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani kell 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

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

#### 1.4.3. .Személyi feltételek biztosítása

A személyes adatok kezelésével kapcsolatos teendőket csak a Hivatal illetékes belső szervezeti egység e feladattal megbízott ügyintézői láthatnak 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.

#### 1.4.5. Fizikai, technikai védelem

**Tűzvédelem**

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.

**Vagyonvédelem, fizikai biztonság**

* a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
* a szerverszobába való be- és kilépés rendjét szabályozni kell;
* a szerverszoba kulcsát az adatvédelmi felelős és a megbízott rendszergazda 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**

* 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. Selejtezendő:

1. a fizikailag sérült, javíthatatlan;
2. gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
3. ha a kapacitás a névleges érték 75%-ánál kevesebb;
4. véglegesen elhasználódott adathordozót.

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.

A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

**Adatvédelemi feladatok:**

* az adatbevitel hibátlan műszaki állapotú berendezésen történhet;
* csak hibátlan adathordozóra lehet adatállományt rögzíteni;
* adatrögzítő szoftver védelme: a programokat, 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.

**Szoftvervédelem**

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

Rendszerszoftver védelem:

1. a rendszerszoftver módosításához az illetékes engedélye szükséges;
2. a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
3. a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló).

Programhoz való hozzáférés, programvédelem:

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

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

1. a program azonosítója;
2. a program készítőjének neve;
3. a feldolgozási rendszer megnevezése.

Programok megőrzése, nyilvántartása:

1. a programokról naprakész nyilvántartást kell vezetni;
2. a nyilvántartásból egyértelműen megállapíthatónak kell lennie 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.

**Hardver védelem**

* 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, alapelv: 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;
* havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

Biztosítani kell a Hivatalban kezelt manuális, papíralapú és elektronikus adatállományok biztonságos működési feltételeit. A Hivatal minden olyan helyisége esetében ahol adatkezeléssel, adatszolgáltatással kapcsolatos feladat ellátására számítógépes feldolgozására kerül sor, meg kell akadályozni az illetéktelen személyek bejutását.

A személyes, a jó hírnév körébe tartozó adatokat, az üzleti titkot tartalmazó iratokat, nyilvántartásokat, dokumentumokat a munkaidő végeztével zárható szekrényben kell elhelyezni és az adatkezelést végző személyek felelősek azért, hogy a személyes adatokat tartalmazó iratok, nyilvántartások, a munkaidő végeztével elzárásra kerüljenek.

Számítógépes adatbázisok esetében az illetéktelen hozzáférés megakadályozása érdekében a számítógépet kezelő munkatársak felelősek azért, hogy a munkaidő végeztével a számítógép kikapcsolásra kerüljön.

### 1.5. Informatikai Védelem

### 1.5.1 Adatok és programok védelme

Mind a személyes, mind a közérdekű adatokat tartalmazó számítógépes információs rendszerek (adatbázisok) esetében biztosítani kell

* a rendszer folyamatos, zavartalan működését,
* az adatállomány(ok) illetékesek által történő folyamatos elérését, illetőleg az illetéktelenek kizárását, a hozzáférési jogosultságok biztosítását, az elektronikus közigazgatási szolgáltatás igénybevételének biztosításához szükséges technikai feltételeket, az informatikai rendszerben bekövetkező események, műveletek, rögzítésre kerülő adatok naplózását és biztonságos tárolását (archiválását),
* a rendszer hardver és szoftver védelmét

A szervezet számítógépes adat-feldolgozási folyamatába kerülő információkat és programokat fokozott biztonsági szabályok szerint kell kezelni.

A szervezetnél működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.

Tilos vírusellenőrzés nélkül CD-t, vagy DVD-t, vagy más adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni!

Vásárolt, vagy átvett CD vagy DVD lemezen tárolt program esetén minden esetben biztonsági másolatot kell készíteni, majd az eredeti lemezt írásvédetté kell tenni.

A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni.

**Feldolgozásra kerülő adatok előkészítése**

a) Számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek.

b) Az ellenőrzésért az adatfelelősség elve szerint adatlapos rögzítés esetén az adatlapot kiállító, adatlap nélküli rögzítés esetén feldolgozást végző kijelölt köztisztviselő felelős. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

**Feldolgozás folyamata**

a) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni.

b) Az adatfeldolgozás során a számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülésére az informatikai felelőst haladéktalanul értesíteni kell.

**Mentés**

a) A számítógépeken tárolt információk biztonságos megőrzése céljából az adatokat szükséges rendszerességgel legalább két egyező példányban menteni kell.

b) Naponta szükséges menteni az iktatási adatállományokat a hálózati rendszerbe.

c) Hetente mentést kell végezni a hálózati működést biztosító központi gépen történt adatváltozásokról.

d) Egyedi gépek vagy programok esetén a mentés gyakoriságát az adott adatfeldolgozási tevékenységet felügyelő illetékes vezető határozza meg.

e) Az egyedi gépekről a mentést az egyedi gép használója, a szervezet központi szervergépéről a mentést a kijelölt számítástechnikai munkatárs végzi el.

**Másolás**

A számítógépes programok a szerzői jog szerint védelmet élveznek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

**Törlés**

Mágneses adathordozókon tárolt adatok és programok törlését csak a tevékenységet felügyelő illetékes vezető írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattározási és selejtezési szabályok betartására.

**Archiválás**

Az informatikai eszközein tárolt adatok archiválását az adatok biztonságos kezelése érdekében a szervezetnél hetente egyszer kell elvégezni. Az archív adatok tárolásánál figyelembe kell venni a biztonsági előírásokat (zárható, tűzbiztos tárolóeszköz, távol a szervertől), és biztosítani kell a tárolási körülményeket (hőmérséklet, páratartalom).

**Visszatöltés**

Az adathordozókon tárolt adatok visszatöltését, visszaállítását a szervezetnél a jegyző engedélyezheti. Ez alól kivételt képeznek az egyedi felhasználók, akik a mentésekből saját munkakönyvtáruk adatait engedély nélkül is visszatöltetik.

Hálózati alkalmazások esetében az adatvesztés elkerülésére és az adatbiztonság fokozására személyre lebontott hozzáférési jogosultságot kell meghatározni.

### 1.5.2. Számítógépek, eszközök és dokumentációk védelme

A számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt köztisztviselő felelős.

A hálózati működő számítógépeken kizárólag az erre kiképzett szakemberek dolgozhatnak.

Meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti.

Fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad.

Vagyonvédelmi megfontolásból azokat a szobákat, ahol számítógép üzemel, biztonsági felszereléssel kell ellátni. A köztisztviselő köteles a munkaidő végzetével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A szervezettől javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

Elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. Annak sérülését minden esetben jelezni kell. ***A berendezéseket vízzel oltani vagy tisztítani tilos!***

A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a szervezet Tűzvédelmi Szabályzata tartalmazza.

### 1.3.3. Az adathordozók selejtezése

A szervezet által vásárolt és a dolgozó(k) részére kiadott adathordozót abban az esetben kell selejtezni, ha:

* fizikailag megsérült,
* gyári, gyártási hibából következően felhasználásra alkalmatlan,
* a tároló kapacitás a megengedhető érték alá csökken,
* véglegesen elhasználódott.

A felhasználók felelőssége, hogy a használhatatlanná vált adathordozókat (CD vagy DVD, CD, DVD, stb.) a jegyző felé jelezze, aki gondoskodik azok közös helyen történő összegyűjtéséről. A selejtezés előtt biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

A megsemmisítés során a felesleges vagyontárgyak hasznosításának és selejtezésének szabályzatában előírtak szerint kell eljárni, annak tényét megsemmisítési jegyzőkönyvben kell rögzíteni.

### 1.5.4. Vírusvédelmi eljárások

A szervezetnél alkalmazott vírusvédelmi rendszernek meg kell felelnie a következő elvárásnak:

* a vírusvédelmi szoftvernek jó minőségűnek és kellő gyakorisággal aktualizáltnak (frissítettnek) kell lennie, hogy felismerési hatékonysága maximális legyen;
* a vírusvédelmi szoftvernek minden támadási ponton aktívan üzemelnie kell.

A szervezet egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából vírusvédelemi szoftvert alkalmazzunk. A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért a jegyző felelős. Az újonnan vásárolt számítógépekre azok rendszerbe állítása során telepíteni kell a víruskereső programot.

A számítógépes munkaállomásokon a víruskereső programot úgy kell beállítani, hogy naponta egyszer (az első bejelentkezéskor) megtörténjen az automatikus vírusteszt futtatása. A rendszerbe kívülről bekerülő adatokat (CD vagy DVD lemez, USB portról csatlakoztatható eszközök, CD-ROM, Internet stb.) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső program munkaállomásokon történő lefuttatása a felhasználó feladata és felelőssége.

A víruskereső szoftvernek minden lehetséges bejutási pontot (CD vagy DVD lemez, USB portról csatlakoztatható eszközök, CD-ROM, hálózat, e-mail, stb.) ellenőriznie kell, így az elsődleges támadási felületnek minősülő munkaállomásokat, és a másodlagos támadási felületnek minősülő tűzfalakat, alkalmazás és levelező szervereket.

A vírusadatbázisok frissítése a rendszer hatékony működésének szempontjából fontos, mivel az új vírusok megjelenése és elterjedése között rövid idő (esetenként néhány óra) telik el.

Fontos minden informatikai munkavégzést körültekintően végezni, hogy elkerülhető legyen az esetleges egyéb támadás, például: adathalászat, spam aktiválás.

# a közérdekű adatok megismerésének szabályai

### A közérdekű információk, illetőleg dokumentumok meghatározása

Az Isztv.26.§-a, valamint egyéb jogszabályok alapján közérdekű, nyilvános adat különösen Csabacsűdi Közös Önkormányzati Hivatalának (továbbiakban: Önkormányzatok) költségvetésével és annak végrehajtásával, vagyonával és annak kezelésével, a közpénzek felhasználásával, szerveik feladatkörével, működésével, tevékenységével, átláthatóságával, ellenőrizhetőségével kapcsolatos információk.

A kötelezően közzéteendő közérdekű információk:

* 1. 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;
  2. a Hivatal működésével, szervezetével kapcsolatos információk, dokumentumok;
  3. továbbá mindaz, amit jogszabály közérdekűvé nyilvánít.

Nem tehetők hozzáférhetővé azok az adatok,

* + 1. amelyeket törvény alapján az arra jogosult szerv állam – vagy szolgálati titokká nyilvánított,
    2. amelyek a nemzetközi szerződésből eredő kötelezettség alapján minősített adatok,
    3. amelyek 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,
    4. amelyek esetében

az adatfajtára vonatkozó külön törvény a nyilvánossá tételt kizárja vagy korlátozza,

a Ptk.81.§ előírásai alapján üzleti titok szabályait kell alkalmazni.

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.

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

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

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.

### Nyilvántartás az elutasított kérelmekről

A közérdekű adatok megismerésére irányuló kérelmek elutasításáról nyilvántartást kell vezetni.

A nyilvántartás tartalmazza:

1. a közérdekű adatok megismerésére irányuló kérelem benyújtásának

időpontját,

1. a megismerni kívánt közérdekű adatok körét, az elérés módját: pl. Portálon,

intraneten,

1. az elutasítás a megtagadás, dátumát, indokát nem elérhető nem nyilvános

minősítését.

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

# A személyes adatok kezelésével kapcsolatos szabályok

### 1. Személyes adatok kezelésének jogszerűsége

A Hivatal belső szervezetei egységeinek feladatkörük ellátása céljából részben jogszabály alapján elrendelt nyilvántartások, részben saját készítésű dokumentumok felfektetése, 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.

Ennek megfelelően:

1. az érintett hozzájárulása alapján, a hozzájárulás beszerzésével, illetőleg a hozzájárulás megadásáról szóló dokumentumnak az érintett részéről történő átadásával (aláírásával), és az iratokhoz csatolásával;
2. 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.
3. 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;
4. 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;
5. A különleges adatok esetében az érintett előzetes írásbeli nyilatkozata alapján, annak csatolásával, valamint az Isztv. 3. § 3. a. pontban foglalt adatok esetében nemzetközi egyezményen alapul vagy az Alaptörvényben biztosított alapvető jog érvényesítése érdekében törvény elrendeli;
6. Az érintettel írásban kötött szerződés alapján, ha az abban foglaltak teljesítése érdekében a hozzájárulást megtagadta.

A szerződének tartalmaznia kell:

f.a) a kezelendő adatok meghatározását,

f.b) az adatkezelés időtartamát,

f.c) a felhasználás célját, (például közérdekű adatok keretében történő nyilvánosságra hozatal tényét, és 5 éves nyilvános kezelést),

f.d) 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.

### 2. Személyes adatok kezelésének célhoz kötöttsége

Az Adtakezelő 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.

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.

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

Az irányítási jogkör gyakorlása, a döntés előkészítés keretében az Isztv. 26.§ (1) – (3) bekezdésében, illetőleg az egyéb jogszabályokban meghatározott adtakört 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.

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.

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.)

Az ezzel kapcsolatos előterjesztések a Moöt. szerint zárt ülés keretében tárgyalhatók és a zárt ülésen résztvevők tekinthetik meg a dokumentumokat.

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

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

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 5.2.2. pontban foglaltak szerint kell kezelni.

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.

### 3. A személyes adatok kezelésének biztonsága

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 Isztv. És a külön törvény szerinti felhatalmazással rendelkezők férhessenek hozzá. Az automatizált feldolgozás során olyan intézkedések szükségese, amelyek:

1. megakadályozzák, hogy illetéktelen személyek a számítógépes

adatállományhoz hozzáférjenek,

1. megakadályozzák a tárolóeszközök jogosulatlan olvasását, másolását, módosítását, eltávolítását, megváltoztatását, stb;
2. megakadályozzák, hogy illetéktelen személyek az adatfeldolgozó rendszert adatátviteli eszközök útján elérjék, károsítsák,
3. biztosítják, hogy a jogosult felhasználók csak a hozzáférési joguk szerinti személyes adatok köréhez férjenek hozzá,
4. rögzítik, hogy az adatfeldolgozó rendszert ki, mikor milyen célból érte el továbbá ki és milyen adatrögzítést, módosítást, másolást, stb. hajtott végre,
5. biztosítsák annak az ellenőrzését, hogy mikor, mely személyes adat került kezelésre és azt ki végezte.

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 sorén keletkezett iratok illetéktelen személyek birtokába ne kerülhessenek.

### 4. Az érintettek jogai

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.

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

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.

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.

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:

1. a betekintés időpontját és célját
2. a jelenlévők nevét és minőségét
3. a betekintés során tett megállapítást vagy észrevételt
4. a jelenlévők aláírását.

Az érintett tiltakozhat személyes adatai kezelése ellen, ha

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

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

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.

### 5. Az adatkezelés, az adattovábbítás összekapcsolása

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

1. ha azt törvény megengedi, vagy
2. az érintett ahhoz előzetesen hozzájárult

és az adatkezelés jogszabályi feltételei minden esetben teljesülnek.

### 6. A személyes adatokkal kapcsolatos nyilvántartások

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.

c.a) törvény alapján

c.b) az érintett írásbeli hozzájárulásával vagy az Isztv. 6. § (7) bekezdése alapján a közszereplése során általa már közölt vagy nyilvánosságra hozatal céljából átadott adatokról van szó,

c.c) az Isztv. 6. § (6) bekezdése alapján az – érintett kérelmére – indult eljárásban a hozzájárulás vélelmezésével,

d) mikor történt az adatszolgáltatás, a betekintés.

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

### 7. Személyes adatok kezelésének különös szabályai

* 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.
* 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.
* 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.
* 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 16/2007. (III. 13.) IRM-MeHVM együttes rendelet előírásait kell alkalmazni.

# Jogorvoslati eljárás szabályai

Ha a Hivatal közérdekű adatra vonatkozó igényt nem teljesíti, az igénylő az Isztv. 31. §-ban foglalt eljárási rendnek megfelelően – az elutasítás kézhezvételét követő harminc napon belül – bírósághoz fordulhat. A megtagadás jogszerűségét és megalapozottságát a Hivatal köteles bizonyítani.

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

# Hatálybalépés

Jelen szabályzat 2013.xxxxxxx . napján lép hatályba.

Örménykút, 2013. xxxxxxx.

Kasikné Csík Zsuzsanna jegyző

# MELLÉKLETEK

## 1. Megismerési nyilatkozat

**Megismerési nyilatkozat**

Csabacsűdi Közös Önkormányzati Hivatal Jegyzőjének Adatvédelmi és Informatikai Biztonsági Szabályzatát megismertem és gondoskodom arról, hogy a szabályzat tartalmát az érintett szervezeti egység dolgozói megismerjék.

|  |  |  |  |
| --- | --- | --- | --- |
| **Név** | **Beosztás** | **Kelt** | **Aláírás** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 2. Kiemelt szoftverek ismertetése és a mentési rend szabályai

A Hivatal kiemelt rendszer- és felhasználói programjairól napi, heti, valamint éves mentés készül.

Kiemelt felhasználói programok:

Rendszerprogramok:

A mentési rend

A szerverszobában elhelyezett Szerver adattároló eszközeire történik a mentés az alábbi eljárás szerint:

Az adatok mentése, az adathordozók biztonsága

A napi adatmentés a következő módon történik

1. Az adatvédelmi felelős által meghatározott fájlokat naponta, a munka befejezésével zip fájlba tömörítve az adatmentés helyének kijelölt külső merevlemezre 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 merevlemezt 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 5 frissebb adatmentés az állományokról.

A heti adatmentés a következő módon történik

1. Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmazok méretének megfelelően vagy a napi mentésnél már szokásos .zip fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.
2. A külső, biztonsági másolatokat tartalmazó merevlemezt csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből és az adatvédelmi felelős által kijelölt helyre el kell zárni.
3. A korábbi, heti, teljes körű adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik 3 frissebb adatmentés az állományokról.

Az éves adatmentés a következő módon történik

A tárgy év utolsó teljes körű biztonsági mentésének megtörténte után, az adatmentés helyének kijelölt külső adattároló eszköz tükör merevlemeze cserélődik egy új merevlemezre. A mentést tartalmazó merevlemez a jegyzői titkárságon páncélszekrényben kerül elhelyezésre.

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 merevlemezhez.
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).

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.

Tartalomjegyzék

[**I. Bevezetés** 1](#_Toc374893265)

[**II. Általános szabályok** 1](#_Toc374893266)

[1. A szabályzat célja 1](#_Toc374893267)

[2. A szabályzat hatálya 2](#_Toc374893268)

[3. A közszolgálati nyilvántartásra vonatkozó szabályok 2](#_Toc374893269)

[3.1. Általános szabályok 2](#_Toc374893270)

[3.2. A közszolgálati alapnyilvántartás adatlapjai vezetésének adatvédelmi szabályai 4](#_Toc374893271)

[**III.** **Általános adatvédelmi és adatbiztonsági szabályzat** 6](#_Toc374893272)

[1. ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK 6](#_Toc374893273)

[1.1. A szabályzat célja, hatálya 6](#_Toc374893274)

[1.2. Az adatkezelés során használt fontosabb fogalmak 7](#_Toc374893275)

[1.3. A Hivatal belső szervezeti egységei 9](#_Toc374893276)

[1.4. Az adatvédelem tárgya 10](#_Toc374893277)

[1.5. Informatikai Védelem 14](#_Toc374893278)

[1.5.1 Adatok és programok védelme 14](#_Toc374893279)

[1.5.2. Számítógépek, eszközök és dokumentációk védelme 16](#_Toc374893280)

[1.3.3. Az adathordozók selejtezése 16](#_Toc374893281)

[1.5.4. Vírusvédelmi eljárások 17](#_Toc374893282)

[IV. a közérdekű adatok megismerésének szabályai 18](#_Toc374893283)

[1. A közérdekű információk, illetőleg dokumentumok meghatározása 18](#_Toc374893284)

[2. A közérdekű adatok előkészítése 19](#_Toc374893285)

[3. Nyilvántartás az elutasított kérelmekről 19](#_Toc374893286)

[V. A személyes adatok kezelésével kapcsolatos szabályok 20](#_Toc374893287)

[1. Személyes adatok kezelésének jogszerűsége 20](#_Toc374893288)

[2. Személyes adatok kezelésének célhoz kötöttsége 21](#_Toc374893289)

[3. A személyes adatok kezelésének biztonsága 22](#_Toc374893290)

[4. Az érintettek jogai 23](#_Toc374893291)

[5. Az adatkezelés, az adattovábbítás összekapcsolása 24](#_Toc374893292)

[6. A személyes adatokkal kapcsolatos nyilvántartások 25](#_Toc374893293)

[7. Személyes adatok kezelésének különös szabályai 25](#_Toc374893294)

[VI. Jogorvoslati eljárás szabályai 26](#_Toc374893295)

[VII. Hatálybalépés 27](#_Toc374893296)

[VIII. MELLÉKLETEK 28](#_Toc374893297)

[1. Megismerési nyilatkozat 28](#_Toc374893298)

[2. Kiemelt szoftverek ismertetése és a mentési rend szabályai 29](#_Toc374893299)