Gávavencsellői Közös Önkormányzati Hivatal

4472 Gávavencsellő Petőfi utca 1.

4475 Paszab Fő út 9.

Információ Védelmi szabályzat

Érvényes: 2020. május 1-től

Adatok osztályozása

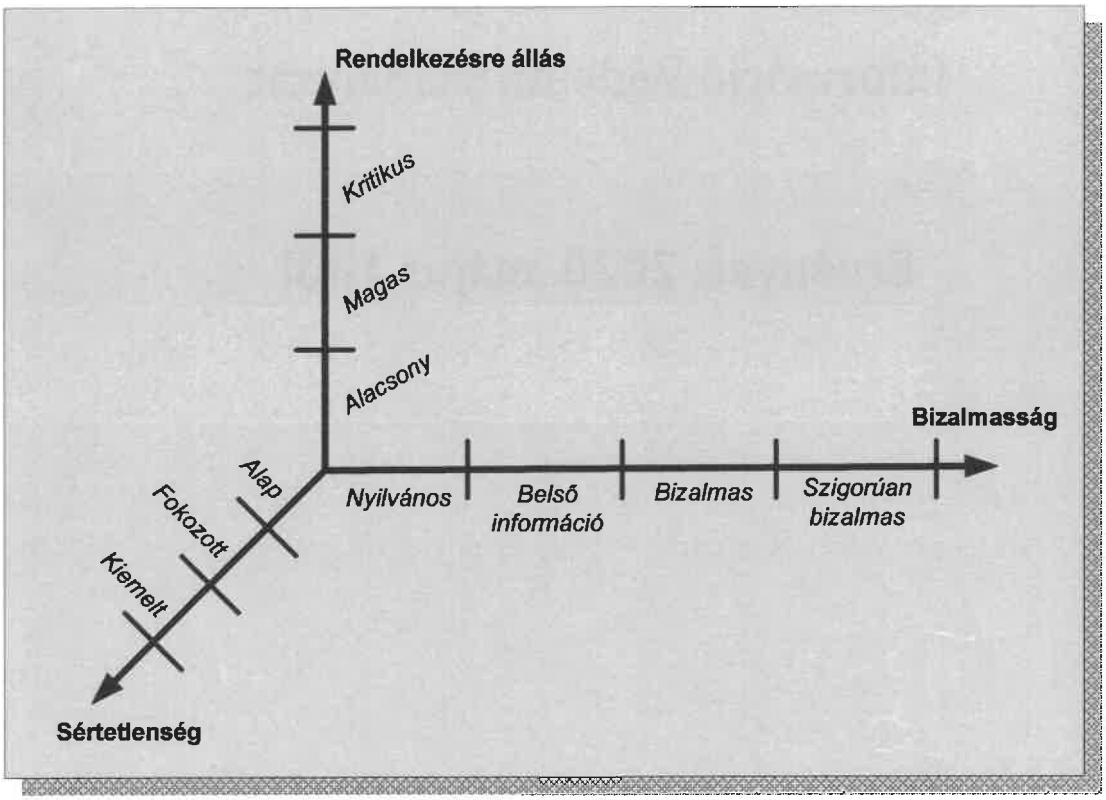
1. A szabályzat célja

A szabályzat egy olyan adatosztályozó rendszer létrehozása, amely a Hivatal által kezelt adatok fontosságuknak, értéküknek megfelelően osztályozza, és ezzel megfelelő védelmi, kezelési intézkedéseket foganatosít megóvásuk érdekében. A Hivatal szervezetén belül található rendszerezendő és osztályozandó adatok köre kiterjed minden adatra, amely a Hivatal számítógépes rendszerében kerül tárolásra vagy feldolgozásra.

2. A hivatal informatikai eszközein kezelt és tárolt adatok besorolási rendszere

- **Bizalmasság:** az információt csak az legyen képes elolvasni, aki arra jogosult
- **Sértetlenség:** az információt csak az módosíthassa vagy törölhesse, aki arra jogosult, továbbá az adat hiteles forrása bizonyítható legyen
- **Rendelkezésre állás:** az arra jogosult felhasználó a szükséges információhoz a megfelelő helyen és időben hozzáférhessen

Adatok besorolása információbiztonsági szempontok alapján



3. Az információ bizalmasságának besorolási kategóriái

- **Nyilvános:** Minden olyan személyes és közérdekű adat, amelynek nyilvánosságra kerülése az érintett személyek, illetve szervezetek számára erkölcsi, anyagi és jogi következményekkel nem jár.

- **Belső információ:** Minden olyan adat, amely a Hivatalon belül minden alkalmazottnak és szerződéses munkatársnak korlátozás nélkül rendelkezésére áll, ugyanakkor szervezeten kívül nem kerül kihirdetésre.
- **Bizalmas:** Olyan nem minősített adat, amelynek nyilvánosságra kerülése az érintett személyek vagy szervezetek számára hátrányos erkölcsi, jogi és anyagi következményeket von maga után.
- Szigorúan bizalmas: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott adatok, különös tekintettel a személyes és azon belül a különleges adatokra.

4. Az információ sértetlenségi igényének besorolási kategóriái

- Alap: Mindazon adatok, amelyek véletlen vagy rosszindulatú módosítása, illetve törlése a Hivatal működési folyamatait lényegesen nem befolyásolhatja, a Hivatal és bármely érintett személy vagy szervezet számára erkölcsi és jogi következményekkel nem jár.
- Fokozott: Mindazon adatok, amelyek véletlen vagy rosszindulatú módosítása, illetve törlése a Hivatal jó hírét veszélyeztetheti, vagy működési folyamatait lényegesen befolyásolhatja, ugyanakkor a Hivatal jogszabályokban előírt kötelezettségeinek határidőben és kellő minőségben történő teljesítését közvetlenül nem érintheti.
- Kiemelt: Mindazon adatok, amelyek véletlen vagy rosszindulatú módosítása, illetve törlése a Hivatal működési folyamatait és jogszabályokban előírt határidőben és kellő minőségben történő teljesítését közvetlenül, lényeges mértékben befolyásolhatja, vagy a Hivatal számára jogi és/vagy anyagi következményekkel járhat.

5. Az adatok besorolásának eljárásrendje

Minden adatot, amely a Hivatal számítógépes rendszerében kerül tárolásra vagy feldolgozásra, be kell vonni a besorolási eljárásba.

A besorolási eljárás végeredménye a Besorolási ív (1. melléklet), amelynek célja egyrészt, hogy olyan adatcsoportokat határozzon meg, amelyekhez a Hivatal informatikai rendszerében kezelt összes adat egyértelműen hozzárendelhető; másrészt meghatározza ezen adatcsoportok biztonsági besorolását. A Besorolási ív az IVSZ mellékletét képezi, a következő tartalommal:

- Az adatcsoport megnevezése

- Az adatcsoporthoz tartozó alkalmazás megnevezése
- Az adatcsoport bizalmassági besorolása
- Az adatcsoport sértetlenségi besorolása
- Az adatcsoport rendelkezésre állási besorolása
- Az adatgazda meghatározása

A Besorolási Ív tartalmát a jegyző hagyja jóvá és adja ki.

6. Az adatgazdák szerepe és felelőssége

A Hivatal informatikai rendszerének minden felhasználója köteles az általa tárolt, kezelt vagy létrehozott adatot annak besorolása szerint, az IVSZ-ben meghatározott módon kezelni és tárolni. Az egyes adatokra és adatbázisokra vonatkozó előírások betartatásáért az Besorolási ívben meghatározott adatgazda a felelős.

A Hivatal informatikai rendszerében tárolt és kezelt adatok adatgazdája alapesetben az a felhasználó, aki azt a rendszerben rögzítette, illetve létrehozta. Az alapesettől kivételt képező adatcsoportok adatgazdáit a Besorolási ív határozza meg.

Amennyiben a rögzítendő vagy létrehozandó elektronikus adat egyik adatcsoportba sem sorolható be egyértelműen, akkor az alapértelmezett adatgazda köteles az adat besorolási eljárását kérni az jegyzőtől. A kérelmet írásban, az IVSZ mellékletét képező Adatbesorolási kérelem (2. melléklet) formanyomtatványon kell benyújtani a javasolt besorolások megjelölésével és indoklásával. A kérelem benyújtását követően a jegyző döntéséig a kezdeményező saját felelősségi és hatáskörén belül érvényesíti és érvényesítteti a javasolt besorolás szerinti adatkezelési és tárolási eljárásrendeket.

A Besorolási ív karbantartása

A Besorolási ív tartalmát az biztonsági felelős az IVSZ rendszeres évi felülvizsgálata során áttekinti, és szükség esetén – az érintett adatok tekintetében – az újra besorolási eljárást a jegyzőnél kezdeményezi. Az újra besorolási eljárásba a jegyző az érintett adatgazdákat bevonhatja.

A Besorolási ívben felsorolt egyes adatok újbóli besorolását a Hivatal bármely dolgozója, illetve a rendszerben tárolt adatok bármely adatgazdája kezdeményezheti. Az újra besorolás kezdeményezését írásban, részletes indoklással kell benyújtani a jegyzőnek. A kezdeményezés benyújtását követően a jegyző döntéséig a kezdeményező saját felelősségi és hatáskörén körén belül érvényesítheti vagy érvényesíttetheti a javasolt besorolás szerinti adatkezelési és tárolási eljárásrendeket, amennyiben azok nem enyhébbek az érvényben levő előírásoknál.

A Besorolási ív módosításait minden esetben a jegyző hagyja jóvá és adja ki és a módosításról az érintett adatgazdákat soron kívül értesíti.

7. A besorolási kategóriák leképezése

Az átláthatóság és könnyebb kezelhetőég érdekében a bizalmasság és sértetlenség szempontjai szerint felállított besorolási kategóriákat az alábbi szabályok alkalmazásával kell csoportosítani:

- Védelmet nem igénylő adatnak minősül minden olyan adat, melynek besorolása alap és nyilvános. (1. szint)
- Kiemelten védendő adatnak minősül minden olyan adat, melynek besorolása kiemelt vagy szigorúan bizalmas. (3. szint)
- Minden más esetben, az adatot a védendő adatok csoportjába kell besorolni. (2. szint)

Az alábbi ábra mutatja a rendelkezésre állási és bizalmassági/sértetlenségi szinteknek megfelelően osztályozott és csoportosított adatok lehetséges elhelyezkedését. Az első számjegy a rendelkezésre állás szerinti szintet, a második számjegy a bizalmasság vagy sértetlenség szerinti szintet jelenti.

Kritikus	31	32	33
Magas	21	22	23
Alacsony	11	12	13
Rendelkezésre állási szint / Bizalmasság/sértetlenség	Védelmet nem igénylő adat	Védendő adat	Kiemelten védendő adat

Az adatok informatikai biztonsági szempontból történő rendelkezésre állási és bizalmassági vagy sértetlenségi szintekbe sorolása során számításba kell venni, hogy az adat érzékenysége és kritikusága gyakran megszűnik egy bizonyos idő után (például a Hivatali jelentések publikálása vagy amikor az információ védelmet nem igénylő adattá válik), illetve a túlzott osztályozások szükségtelen többletköltségeket okozhatnak.

Ha védendő, vagy kiemelten védendő információk eltűnnek, illetéktelen kezekbe vagy nyilvánosságra kerülnek, vagy ennek gyanúja felmerül, az észlelő felhasználó köteles ezt az informatikusnak és a jegyzőnek jelezni.

8. Adatcsoportok jelölése és kezelése

- **A rendelkezésre állás szintek alapján**

Jelölés

- Alacsony rendelkezésre állású
- Magas rendelkezésre állású
- Kritikus rendelkezésre állású

Tárolás

- Alacsony besorolási kategóriába tartozó adatcsoportokat nem kell redundáns módon tárolni.
- Magas rendelkezésre állási szinten működő rendszerek esetén az adatokat fokozott biztonságú, hibatűrő tárolási móddal (pl.: RAID5) vagy tükrözéssel és napi mentéssel kell védeni. A mentet adatoknak területileg elkülönítetten kell elhelyezkednie az éles rendszerektől.
- Kritikus rendelkezésre állás esetén az adatcsoporthoz tartozó informatikai rendszert, vagy legfontosabb részeit megfelelő másolattal (RAID5, tükrözés, virtualizáció, stb.) kell biztosítani, ami nem csak az adatok másolatát, hanem az egyes rendszerelemek másolatát is (pl. virtuális gép másolat) jelenti. A másolt rendszernek, a másolat adatokkal együtt területileg elkülönítetten kell elhelyezkednie az éles rendszerektől. A mentéseket legalább napi sűrűséggel kell elvégezni, és lehetőleg két példányban tárolni.

Adatátvitel

- Alacsony rendelkezésre állási szinten lévő adatok továbbításánál nem kell biztonsági előírásokat alkalmazni.
- Magas rendelkezésre állási szinten lévő adatok továbbítása előtt meg kell győződni arról, hogy a továbbítandó adatból létezik–e legalább egy példány a forrás helyen.
- Kritikus adat továbbítása csak úgy lehetséges, ha az adat legalább két példányban elérhető, és ezek közül az egyik a forráshelyen, a másik pedig, a forrás és cél állomástól különböző, harmadik helyen

Eltávolítás

- Alacsony rendelkezésre állási szinten lévő adatok eltávolítása az adatgazda engedélyével lehetséges.
- Magas és kritikus rendelkezésre állási szinten lévő adatok eltávolítása a jegyző és az adatgazda engedélyével lehetséges.
- A Bizalmatlansági vagy sértetlenségi szintek alapján

Az itt felsorolt adattípusokat a megfelelő biztonsági osztályba sorolva a fenti utasításokkal összhangban lévő fizikai és logikai védelemmel kell ellátni az informatikai rendszerekben.

Jelölés

- Védelmet nem igénylő adatok: Nincs adatbiztonságra vonatkozó követelmény.
- Védendő adatok:
    - Olyan speciális egyedi programok (alkalmazások) esetén, melyek védendő adatokat kezelnek, a „védendő" megjelölést az adatok feldolgozója/szemlélője számára egyértelműen felismerhetővé kell tenni.
    - A fizikai adathordozókat „védendő" megjegyzéssel kell jelölni.
- Kiemelten védendő:
    - Olyan speciális, egyedi alkalmazások, vagy programok esetén, melyek szigorúan bizalmas adatokat kezelnek, a „SZIGORÚAN BIZALMAS" megjelölést az adatok feldolgozója/szemlélője számára egyértelműen felismerhetővé kell tenni.
    - A fizikai adathordozókat „KIEMELTEN VÉDENDŐ" megjegyzéssel kell jelölni.

Tárolás

- Védelmet nem igénylő adatok: Nincs semminemű adatbiztonságra vonatkozó követelmény.
- Védendő adatok:
    - Védendő adatokat olyan szerveren kell elhelyezni, ahol érvényesíthetőek a bizalmasság/sértetlenség előírásai.
    - Ha a mentés mobil adathordozón szükséges, úgy egy biztos, kódolt mentést kell végrehajtani.
- Kiemelten védendő: Az adatokat csak egy behatárolt és engedélyezett felhasználói kör részére hozzáférhetővé tenni.

Adatátvitel

Ezen szabályok az adatok – az adatokat fizikailag tároló adathordozók útján történő – szétosztására, vagy elektronikai úton történő adatátvitelére alkalmazandók.

- Védelmet nem igénylő adatok: Nincs semmiféle biztonsági megkötés az adatok szállítására vonatkozóan.
- Védendő adatok:
    - A Hivatal belső hálózatán történő adattovábbítás esetén biztonságos SSL kódolás ajánlott
    - Az Interneten keresztüli adatátvitel esetén biztonságos SSL kódolás szükséges.
- Kiemelten védendő: Adatok elektronikus átvitele során biztonságos SSL kódolás szükséges.

Adatmegosztás

- Védelmet nem igénylő adatok minden munkatárs számára korlátozás nélkül elérhetők.
- Védendő adatok:
    - Megosztás csak az adatgazdák hozzájárulásával lehetséges.
    - Külső cégek, partnerek részére történő átadást az adatgazda és az átvevő aláírásával hitelesített titoktartási nyilatkozat kíséretében lehet megtenni.
- Kiemelten védendő:
    - A megosztás csak egy név szerint meghatározott személyi körben engedélyezett.
    - Elektronikus formátumban lévő dokumentumokat el kell látni a szerzőre utaló információval.

Eltávolítás

- Védelmet nem igénylő adatok esetében a kérdéses adat bejegyzésének törlése szükséges.
- Védendő/ kiemelten védendő adatok:
    - Az adathordozót (pl. lemezeket) fizikailag törölni kell új adatokkal történő felülírás révén.
    - A hibás mágnes/optikai adathordozókat meg kell semmisíteni, és nem szabad a gyártónál visszacserélni.

Az adathordozók selejtezéséről és a tartalmazott adatok megsemmisítéséről az fejezete rendelkezik.

Naplózás

- Védelmet nem igénylő adatok esetében naplózás nem szükséges.
- Védendő adatok: Naplózást csak a legutolsó adatmódosításra vonatkozóan kell a rendszernek elvégeznie.
- Kiemelten védendő adatok: A kiemelten védendő adatokat tartalmazó informatikai rendszerek esetén, a naplózó rendszert úgy kell kialakítani, hogy lehetőség legyen teljes tranzakció- és történeti naplózásra (history) valamint az alkalmazásgazdai tevékenység naplózására.

Jelen szabályzat 2020. május 1. napján lép hatályba.

Gávavencsellő, 2020. április. 27.

Bakos Tóth Ildikó
jegyző

Az információ védelmi szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás