KLEBELSBERG
KÖZPONT

Iktatószám: KK/08/714/2018.
verziószám: v1.

A Klebelsberg Központ 5/2018. (VIII. 21.) szabályzata

A Klebelsberg Központ Archiválási szabályzata

Készítette:
Budapest, 2018. augusztus 21.

.....
dr. Ács Szilvia
főosztályvezető

Jóváhagyom:
Budapest, 2018. augusztus 21.

.....
Marsi Márta
kijelölt gazdasági vezető

Kiadmányozom:
Budapest, 2018. augusztus 21.

.....
Hajnal Gabriella
elnök

Tartalomjegyzék

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.), az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet, valamint az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet (a továbbiakban: Korm. rendelet) előírásainak figyelembevételével, a Klebelsberg Központ (a továbbiakban: Központ, vagy Adatkezelő) Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás (a továbbiakban: SZMSZ) 1. mellékletének 5. § (1) bekezdés b) pontjában biztosított jogkörömben eljárva a Központ informatikai rendszereinek és információvagyonának mentésére, archiválására vonatkozó feladatokat, kötelezettségeket az alábbiak szerint szabályozom[1].

I. Fejezet

Általános rendelkezések

1. A szabályzat célja

1. § (1) A szabályzat célja, hogy meghatározza a Központ E-ügyintézési tv. 25. § (4a) bekezdése szerinti, az ügyek intézésével kapcsolatos elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentésével és adattrezor szolgáltatást nyújtó őrző szervhez továbbításával, és a kapcsolódó folyamatokkal kapcsolatos részletszabályokat.

(2) Az adattrezor-archiválási kötelezettség célja az Adatkezelőnek az e-ügyintézési kötelezettség teljesítésével összefüggő adatai sérüléséből eredő működési zavara esetén a működési képesség helyreállítása és az adatvesztés minimalizálása.

2. A szabályzat során alkalmazandó jogszabályok köre

2. § A szabályzat alkalmazása során figyelemmel kell lenni különösen az alábbi jogszabályok rendelkezéseire:

a) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény,

b) az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet,

c) az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet,

d) a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.

3. Értelmező rendelkezések

3. § E szabályzat értelmében:

1. *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.

2. *adatfeldolgozó:* az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki, vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

---

[1] *A szabályzat az Elektronikus Ügyintézési Felügyelet által kibocsátott archiválás szabályzat minta figyelembe vételével készült. A szabályzat 2018. augusztus 21. napján lépett hatályba.*

3. *adatgazda*: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

4. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.

5. *adatkezelő:* az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

6. *archiválás*: a nem, vagy nagyon ritkán használt, de megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik, elkülönített tárolóra.

7. *archiválási eljárás:* az archiválási stratégiát végrehajtó informatikai folyamat.

8. *archiválási szolgáltatás*: az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás.

9. *archiválási politika:* az archiválandó tartalomra vonatkozó szakmai elvárások, valamint az archivált adatok eléréséhez kapcsolódó szakmai követelmények meghatározása.

10. *archiválási stratégia:* az archiválás alapvető szabályainak meghatározása, amely magában foglalja az archiválás tárgyát, módját, az archiválás személyi és tárgyi feltételeinek meghatározását, archiválási hardver, szoftver egység és szabálya azonosítását, az archiválás időpontját, ütemezését, megőrzési idejét.

11. *automatikus információátadás:* információátadás az információ átadását biztosító együttműködő szerv részéről emberi beavatkozást nem igénylő módon.

12. *automatikus információátadási felület:* az információ átadását biztosító együttműködő szerv által létrehozott és üzemeltetett, automatikus információátadást lehetővé tevő műszaki megoldás.

13. *BCP (business continuity planning):* működés folytonossági terv.

14. *bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

15. *DRP (data recovery planning):* adat helyreállítási terv.

16. *elektronikus információs rendszer (EIR):* az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. Egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

17. *elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

18. *folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

19. *inkrementális mentés:* nem kerül elmentésre minden kiválasztott elem, csak azok, amelyek a korábbi mentés óta változtak. Két alapvető típusa:

    a) a kumulatív mentés során mindig az utolsó teljes mentés óta megváltozott adategységek kerülnek elmentésre.

    b) a differenciális mentés során csak az utolsó inkrementális mentés óta megváltozott adategységek kerülnek elmentésre.

20. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

21. *kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

22. *központi mentés*: alapértelmezésben a mentések a rendszerbe állított központi mentőeszköz igénybevételével történnek.

23. *központi mentési eszköz:* a szervezet adatbázisainak, alkalmazásainak, operációs rendszereinek és ezek környezetei mentési igényeinek végrehajtására rendszerbe állított nagyteljesítményű, megfelelő biztonsági megoldással és menedzsment felülettel rendelkező berendezés.

24. *kritikus szolgáltatás:* informatikai szolgáltatás, amely a szervezet működése szempontjából létfontosságú.

25. *offline mentés:* a mentés a szolgáltatások leállításával történik, a szolgáltatások a mentés ideje alatt nem érhetőek el.

26. *online mentés:* a mentés online módon, az informatikai szolgáltatás leállítása nélkül történik. A mentés ideje alatt az adott szolgáltatás elérhető, azonban lehetnek olyan funkciók, amelyek a mentés ideje alatt nem vagy csak korlátozott mértékben vehetők igénybe.

27. *őrzésért felelős szerv:* a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság (a továbbiakban: NISZ Zrt.).

28. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

29. *sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

30. *tartós adathordozó*: olyan eszköz, amely a címzett számára lehetővé teszi a neki címzett adatoknak az adat céljának megfelelő ideig történő tartós tárolását és a tárolt adatok változatlan formában és tartalommal történő megjelenítését. Ilyen eszköz különösen az USB kulcs, a CD-ROM, a DVD, a memória kártya, a számítógép merevlemeze.

31. *teljes (full) mentés:* minden kiválasztott elem mentésre kerül.

32. *teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

33. *visszaállítás:* meghibásodás vagy sérülés miatt leállt informatikai szolgáltatás helyreállítása, amely megkívánhatja a rendszerek és adatbázisok mentéseinek visszatöltését. Katasztrófa-elhárítás esetén leginkább a gyors, ideiglenes szolgáltatás visszaállítást jelenti, megkülönböztetve a végleges helyreállítástól.

4. A Központ által ellátandó tevékenységek köre

4. § (1) Az adattrezor-archiválási kötelezettség a Központot, mint e-ügyintézést biztosító szervet terheli az általa saját szoftverkörnyezetben kezelt adatok tekintetében.

(2) A Központ felelős azért, hogy az archivált adatokból az eredeti környezet teljes vagy részleges megsemmisülése esetén helyreállítható legyen az eredeti működés a megfelelő hardvereszközök üzembe helyezését követően.

(3) Az Adatkezelőnek az elektronikus ügyintézés biztosításához szükséges elektronikus információs rendszereit a Korm. rendelet szerint archiválási osztályba kell besorolnia, archiválásukat az ott meghatározott gyakorisággal kell elvégeznie. A Központ archiválási osztályba sorolás összesítő táblázatát ld. az *1. számú mellékletben*, az archiválási kategória meghatározását a *2. számú mellékletben*.

(4) Első alkalommal valamennyi elektronikus információs rendszer vagy nyilvántartás esetében a teljes adatállományt archiválni kell. A változások archiválása ehhez az állományhoz képest történik úgy, hogy a legutolsó állomány legfeljebb két állományból helyreállítható legyen. A teljes adatállomány archiválása esetén az archiválandó adatmennyiség őrzésért felelős szerv részére történő átadása az Adatkezelő által biztosított fizikai adathordozó használatával történik. Az Adatkezelő és az őrzésért felelős szerv megállapodhat abban, hogy a technikai és biztonsági feltételek fennállása esetén a teljes adatállomány átadása hálózati kapcsolat útján történjen.

(5) Az adattrezor-archiválást titkosító kulcs alkalmazásával az Adatkezelőnek úgy kell elvégeznie, hogy abból az adatkezelőnél működtetett elektronikus információs rendszerek külön-külön is visszaállíthatóak legyenek. Az Adatkezelőnek jól beazonosítható módon meg kell jelölnie, hogy az átadott adatállomány mely adatkezelő elektronikus információs rendszere archiválását tartalmazza. Az adattrezor-archiválásnak tartalmaznia kell a visszaállításhoz szükséges dokumentációt.

(6) Az őrzésért felelős szervnek átadásra kerülő adatállománynak a technika archiváláskori állása szerint rosszindulatú szoftverkódtól való mentessége az Adatkezelő szerv felelőssége.

5. A szabályzat alkalmazása

5. § Jelen szabályzat rendelkezéseit az elektronikus ügyintézés részét képező vagy ahhoz szervesen kapcsolódó minden informatikai rendszer esetében jelen szabályzatban részletezett módon teljes körűen alkalmazni kell.

6. A szabályzat személyi hatálya

6. § A Szabályzat hatálya kiterjed a Központra, mint adatkezelőre, a Központ belső információs rendszereit üzemeltető szervezeti egységeire, ezen szervezeti egységek érintett munkatársaira, üzemeltetésben érintett külső szakértőkre.

7. A szabályzat tárgyi hatálya

7. § A szabályzat tárgyi hatálya az elektronikus ügyintézés részét képező vagy ahhoz szervesen kapcsolódó minden, a Központ által üzemeltetett informatikai rendszerre (hardver, operációs rendszer, alkalmazás szerver, alkalmazás, adatbázis szerver, adatbázis, web szerver, file szerver, dokumentumkezelő) terjed ki:

a) Hivatali Kapu szerverei,

b) Köznevelési Regisztrációs és Tanulmányi Alaprendszer Klebelsberg Képzési Ösztöndíj Program modulja.

8. A szabályzat időbeli hatálya

8. § A szabályzat visszavonásig hatályos.

9. Kapcsolódó szabályzatok, eljárások, rendelkezések

9. § Jelen szabályzat alkalmazása során figyelemmel kell lenni különösen a Központ alábbi szabályzatainak rendelkezéseire:

a) a Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata,

b) a Központ informatikai rendszereinek felhasználásáról szóló szabályzata,

c) a Központ információátadási szabályzata,

d) a Központ közérdekű adatok közzétételéről és megismerésére irányuló kérelmek intézéséről szóló szabályzata.

II. FEJEZET

KÜLÖNÖS RENDELKEZÉSEK

10. Az archiválási folyamat résztvevői

10. § (1) A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Központ ügyintézési ciklusával.

(2) A Központ Informatikai Főosztálya személyi állományának feladata a rendszeres és időszakos biztonsági mentések elvégzése. Azon információs rendszereknél, ahol a Központ adatfeldolgozót vesz igénybe, a mentés az adatfeldolgozó közreműködésével történik. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve az egyéb munkaállomások hálózati munkáját ne akadályozza.

(3) A Központ informatikai rendszereire nézve a biztonsági másolatok készítésének, a mentések elvégzésének és tárolásának részletes rendjét a Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata tartalmazza.

11. Kockázatelemzés

11. § A Központ meghatározza az ügymenet folytonosság biztosításához szükséges, szabályokat, követelményeket, amelynek érdekében:

a) el kell készíteni a fontos informatikai szolgáltatások helyreállítási terveit,

b) a fontos informatikai szolgáltatások meghatározásához kockázatelemzést kell végezni,

c) az azonosított szolgáltatásoknál meg kell vizsgálni a kulcsfontosságú elemeket, így:

ca) meg kell határozni a még tolerálható helyreállítási időket,

cb) el kell készíteni a helyreállítási terveket és azokat a gyakorlatban is tesztelni kell.

d) főszabályként a következőt kell alkalmazni a kockázatok megosztásánál:

da) a szoftverkörnyezet infrastrukturális hibája esetén – ideértve a hálózatot, hálózati tárolót,,internetkapcsolatot, virtualizációt – az elsődleges felelős a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet szerinti központi szolgáltató (a továbbiakban: Szolgáltató), aki felé a Központnak hibabejelentése kötelezettsége áll csak fent,

db) az alkalmazáskörnyezet meghibásodása esetén – ideértve a külső támadást, szoftver termék hibát, emberi mulasztást – az elsődleges felelősség a Központot terheli. Az alábbi BCP és DRP kockázatkezelések a fentiek figyelembevételével értendőek.

12. § Lehetséges kockázatok:

a) Internet kapcsolat (WAN World Area Network) kiesése

Működésfolytonosság (BCP):

aa) hatása az ügymenetre: kritikus (valamennyi felhőalapú rendszer elérhetetlenné válik)

ab) valószínűsége: magas rendelkezésre állás miatt évente legfeljebb 1 alkalom

ac) helyreállítási idő: legfeljebb 8 óra

ad) kockázatkezelés:

ada) az esetet a Szolgáltatónak be kell jelenteni,

adb) a szerződésben törekedni kell arra, hogy az SLA (Service Level Agreement) alapú legyen, azaz a szolgáltatás minőségétől függ a szolgáltatási díj és 99,95%-os rendelkezésre állást biztosítson.

ae) helyreállítás (DRP):

aea) fővonal hiba esetén: hibabehatárolás, a hiba jelentése a Szolgáltatónak, az érintettek tájékoztatása, az esetnek a Szolgáltatónál történő haladéktalan bejelentése, az incidens és az elhárítás dokumentálása,

aeb) router/modem hiba esetén: hibabehatárolás, a hiba jelentése a Szolgáltatónak, az érintettek tájékoztatása, funkcionális csereeszköz haladéktalan igénylése a Szolgáltatótól, tesztelés, próbaüzem, éles üzem,

b) Belső hálózat (LAN Local Area Network) elemeinek meghibásodása

Működésfolytonosság (BCP):

ba) hatása az ügymenetre: kritikus (minden szerveren tárolt dokumentum és onnan futó szolgáltatás, illetve minden felhő alapú szakalkalmazás elérhetetlenné válhat a belső hálózatból),

bb) valószínűsége évente legfeljebb egyszer,

bc) helyreállítási idő: 4 óra,

bd) kockázatkezelés: jó minőségű hálózati eszközök és legalább CAT5 minőségű kábelezés alkalmazása, a bizonytalan elemek cseréje, rendszeres karbantartással, teszteléssel jelentősen csökkenthető a meghibásodás valószínűsége; meghibásodás esetén a hibás eszközök azonnali cseréje, amelyek a Szolgáltató feladatát képezik

be) helyreállítás (DRP):

bea) aktív elem meghibásodása esetén: hibabehatárolás, a hiba jelentése a Szolgáltatónak, az érintettek tájékoztatása, funkcionális csereeszköz beállítása és konfigurálása, tesztelés, próbaüzem, éles üzem, dokumentálás,

beb) passzív elem (kábel, rack, stb.) meghibásodása esetén: hibabehatárolás, a hiba jelentése a Szolgáltatónak, az érintettek tájékoztatása, a passzív szakasz, vagy alkatrész cseréje, tesztelés, próbaüzem, éles üzem, dokumentálás,

c) Hálózati tároló (SAN) meghibásodása

Működésfolytonosság (BCP):

ca) hatása az ügymenetre: lényeges (minden szerveren tárolt dokumentum és onnan futó szolgáltatás elérhetetlenné válhat)

cb) valószínűsége: háromévente egyszer,

cc) helyreállítási idő: legfeljebb 24 óra,

cd) kockázatkezelés:

cda) az esetet Szolgáltatónál be kell jelenteni,

cdb) a szerződésben törekedni kell arra, hogy az SLA (Service Level Agreement) alapú legyen, azaz a szolgáltatás minőségétől függ a szolgáltatási díj és 99,95%-os rendelkezésre állást biztosítson.

ce) helyreállítás (DRP):

cea) fővonal hiba esetén: hibabehatárolás, a hiba jelentése, az érintettek tájékoztatása, az esetet a Szolgáltatónál történő haladéktalan bejelentése, az incidens és az elhárítás dokumentálása,

ceb) router/modem hiba esetén: hibabehatárolás, a hiba jelentése, az érintettek tájékoztatása, funkcionális csereeszköz haladéktalan igénylése a Szolgáltatótól, tesztelés, próbaüzem, éles üzem.

12. Az archiválás folyamata

13. § (1) A mentési, archiválási rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét.

(2) A mentéseknek ki kell terjednie a működési folyamatok és tevékenységek támogatásában és kiszolgálásában részt vevő informatikai eszközökre, illetve azok elhelyezésére szolgáló kiszolgáló rendszerekre/infrastruktúrákra.

(3) Törekedni kell arra, hogy a mentések tárolása fizikailag biztonságos legyen, védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz, mágnesesség, stb.).

(4) A központi szervereken tárolt elektronikus információvagyont a biztonsági káresemények ellen szintén mentéssel kell védeni. A mentéseket minden mentési rendet érintő (fizikai, logikai, vagy adminisztratív) változáskor, de legalább évente egyszer ellenőrizni kell aszerint, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzéseket dokumentált módon kell végrehajtani. A mentéseket a szerverektől elkülönítve, legalább külön helyiségben kell tárolni, védve mind a különböző fizikai káreseményektől (tűz, csőtörés-vízbetörés, stb.), mind az illetéktelen hozzáféréstől (lopás, illegális másolás).

(5) A szervezet információs rendszerei – a jelen szabályzat mellékletei szerint – 3-as és 5-ös kategóriákba kerültek besorolásba. A 3-as kategóriába sorolt rendszerekről első alkalommal, valamint fél évente teljes adatállomány archiválás történik, továbbá archiválás történik havonta a változásokról. Az 5-ös kategóriába sorolt rendszerekről első alkalommal, valamint legalább évente teljes adatállomány archiválás történik.

14. § (1) Az archiválási folyamat főbb szakaszai:

a) az érintett adatállomány kijelölése és mentése az adatmennyiségtől függő típusú tartós adathordozóra, illetve ennek ellenőrzése,

b) a mentett adatokat tartalmazó adathordozó titkosítása,

c) a titkosított adathordozó átadása az őrzésért felelős NISZ Zrt. felé, egyúttal az adathordozó NISZ Zrt. általi átvétele.

(2) Az (1) bekezdés szerinti feladatokat a Központ részéről a jelen szabályzat 10. § (2) bekezdése szerinti felelősök látják el, szükség esetén a Központ további, a feladat ellátásával érintett munkatársai útján.

13. A tárolt és mentésre kerülő adatok köre

15. § A Központban tárolt és mentésre kerülő adatok:

Az Elektronikus Információs Rendszer neve	EIR rövid kódja	EIR állapota
Hivatali Kapu szerverei	HKP	Aktív
Köznevelési Regisztrációs és Tanulmányi Alaprendszer Klebelsberg Képzési Ösztöndíj Program	KRÉTA KKÖP	Aktív

14. Hatósági ellenőrzés

16. § (1) A jelen szabályzatban meghatározott információs rendszerek archiválása az osztályba sorolást követően az előírt gyakorisággal történnek.

(2) Az archiválások gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Szervezet ügyintézési ciklusával.

15. Tesztelés

17. § (1) A biztonsági mentéseket hibajelzés-mentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szúrópróbaszerűen tesztelni kell, illetve automatikus ellenőrzéseket kell végrehajtani. Ennek betartásáért a biztonsági mentés elvégzésével a Központ Informatikai Főosztályának személyi állománya, illetve – amennyiben a Központ adatfeldolgozót vesz igénybe – a Központ által megbízott adatfeldolgozó tartozik felelősséggel. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

(2) A tesztelések elvégzésének menetét, eredményét dokumentálni kell.

III. Fejezet

Záró és hatályba léptető rendelkezések

18. § (1) A szabályzat kiadmányozását követő napon lép hatályba.

(2) Jelen szabályzatot évente, vagy jelentősebb infrastrukturális változás, illetve jogszabályváltozás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell.

(3) Jelen szabályzatot Elektronikus Ügyintézési Felügyelet részére meg kell küldeni.

MELLÉKLETEK

1. számú melléklet

Archiválási osztály összesítő tábla

(Külön MS Excelben)

Archiválási osztályba sorolás összesítő táblázat

Adatkezelő szervezet megnevezése: Klebelsberg Központ

Sorsz.	Az Elektronikus Információs Rendszer neve	EIR rövid kódja	EIR állapota	Adatgazda neve	Adatgazda elérhetősége (e-mail, telefon)	Adatfeldolgozó szervezet megnevezése	Mentési osztályba sorolás dátuma	EÜF kapcsolattartó megnevezése	EÜF kapcsolattartó elérhetősége (e-mail, telefon)
1	Hivatali Kapu szerverei	HKP	Aktív	Hajnal Gabriella elnök	gabriella.hajnal@kk.gov.hu	-	2018.08.21	Dr. Stefán Péter főosztályvezető	peter.stefan@kk.gov.hu; +36 1 795 1742
2	Köznevelési Regisztrációs és Tanulmányi Alaprendszer Klebelsberg Képzési Ösztöndíj Program	KRÉTA KKÖP	Aktív	Hajnal Gabriella elnök	gabriella.hajnal@kk.gov.hu	-	2018.08.21	Turóczi Péter projektreferens	peter.turoci@kk.gov.hu; +36 1 795 2067; +36 70 396 2393

Az adatkezelő szervezet vezetője

PH

Klebelsberg Központ

Adatgazda

2. számú melléklet

Archiválási osztály elemzési tábla

(Külön MS Excelben)

Az EIR-hez tartozó alapadatok

(A pirossal jelölt cellák kitöltése kötelező!)

Az Elektronikus Információs Rendszer neve:	Hivatali Kapu szerverei
EIR rövid kódja:	HKP
EIR állapota:	Aktív
Adatkezelő szervezet megnevezése:	Klebelsberg Központ
Adatgazda neve:	Hajnal Gabriella elnök
Adatfeldolgozó szervezet megnevezése:	-
Mentési osztályba sorolás dátuma:	2018. 08.16.
EÜF kapcsolattartó megnevezése	Dr. Stefán Péter főosztályvezető
EÜF kapcsolattartó elérhetősége (e-mail, telefon)	peter.stefan@kk.gov.hu, +36 1 795 1742
Egy teljes mentés mérete (Mbyte-ban)	Nem meghatározható, változó.
Az EIR rövid leírása:	A HKP a Központi Elektronikus Szolgáltató Rendszer (központi rendszer, KR) része. A HKP-n keresztül az igénybevevő szervezetek hitelesen tudnak fogadni elektronikus üzeneteket, illetve a hivatalok elektronikus üzenetei a hitelesen azonosított ügyfelekhez (állampolgár, hivatal, gazdálkodó szervezet) eljuttathatók.

Archiválási kategória meghatározása

(nem kitölthető)

Az EIR archiválási osztálya osztálya	**3. kategória**
AZ EIR archiválásának módja	> Első alkalommal, valamint legalább félévente teljes állomány archiválása > Havonta változások archiválása Kisméretű archív állomány (300 MB alatt) esetén, minden esetben teljes állomány archiválása szükséges A hatósági ellenőrzés éves ellenőrzési terv szerint

Amennyiben az adatgazda a meghatározott besorolással nem ért egyet, javasolhatja az EIR alternatív besorolását.

(Amennyiben szükséges, az EIR archiválási osztályának meghatározását követően töltendő ki.)

Az adatgazda az alábbi indoklás szerint, a fent meghatározottaktól eltérő, alternatív	**Az adatgazda által az EIR bizalmasságára javasolt alternatív biztonsági osztály:**

Az adatgazda indoklása a javasolt archiválási osztályokhoz:

(Az alternatív archiválási osztály megadását követően kötelező kitölteni!)

Az archiválási osztály meghatározásáról készített jelen adatközlő lapot kérjük, hogy hitelesítve küldje meg az euf@bm.gov.hu e-mailcímre!

Az adatkezelő szervezet vezetője

Klebelsberg Központ Elnök 20

PH.

Adatgazda

Az EIR-hez tartozó alapadatok

(A pirossal jelölt cellák kitöltése kötelező!)

Az Elektronikus Információs Rendszer neve:	Köznevelési Regisztrációs és Tanulmányi Alaprendszer Klebelsberg Képzési Ösztöndíj Program
EIR rövid kódja:	KRÉTA KKÖP
EIR állapota:	Aktív
Adatkezelő szervezet megnevezése:	Klebelsberg Központ
Adatgazda neve:	Hajnal Gabriella elnök
Adatfeldolgozó szervezet megnevezése:	-
Mentési oztályba sorolás dátuma:	2018. 08.16.
EÜF kapcsolattartó megnevezése	Turóci Péter projektreferens
EÜF kapcsolattartó elérhetősége (e-mail, telefon)	peter.turoci@kk.gov.hu; +36 1 795 2067; +36 70 396 2393
Egy teljes mentés mérete (Mbyte-ban)	Nem meghatározható, változó.
Az EIR rövid leírása:	A KRÉTA KKÖP kezeli a Klebelsberg Ösztöndíj Programra jelentkezett hallgatók személyes adatait és a Klebesberg Ösztöndíj Program folyamatához kapcsolódó egyéb adatokat.

Archiválási kategória meghatározása

(nem kitölthető)

Az EIR archiválási osztálya osztálya	**5. kategória**
AZ EIR archiválásának módja	> Első alkalommal, valamint legalább évente teljes állomány archiválása A hatósági ellenőrzés éves ellenőrzési terv szerint

Amennyiben az adatgazda a meghatározott besorolással nem ért egyet, javasolhatja az EIR alternatív besorolását.

(Amennyiben szükséges, az EIR archiválási osztályának meghatározását követően töltendő ki.)

Az adatgazda az alábbi indoklás szerint, a fent meghatározottaktól eltérő, alternatív	**Az adatgazda által az EIR bizalmasságára javasolt alternatív biztonsági osztály:**

Az adatgazda indoklása a javasolt archiválási osztályokhoz:

(Az alternatív archiválási osztály megadását követően kötelező kitölteni!)

Az archiválási osztály meghatározásáról készített jelen adatközlő lapot kérjük, hogy hitelesítve küldje meg az euf@bm.gov.hu e-mailcímre!

Az adatkezelő szervezet vezetője

PH.

Klebelsberg Központ 02 Elnök

Adatgazda