MAGYAR KÖZLÖNY 145. szám

A MAGYAR KÖZTÁRSASÁG HIVATALOS LAPJA
2009. október 14., szerda

Tartalomjegyzék

Tartalomjegyzék

III. Kormányrendeletek

A Kormány 222/2009. (X. 14.) Korm. rendelete az elektronikus közszolgáltatás működtetéséről

A Kormány az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény 31. § (1) bekezdés a) és b) pontjában, a (2) bekezdés a) és f) pontjában, a (3) bekezdésében, valamint az egyes jogszabályok és jogszabályi rendelkezések hatályon kívül helyezéséről szóló 2007. évi LXXXII. törvény 6. § (2) bekezdésében foglalt felhatalmazás alapján az Alkotmány 35. § (1) bekezdés b) pontjában meghatározott feladatkörében eljárva a következőket rendeli el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. § (1) E rendelet hatálya kiterjed

a) az elektronikus közszolgáltatást nyújtó, valamint az elektronikus közszolgáltatáshoz szakmai és informatikai támogatást biztosító természetes és jogi személyekre, valamint jogi személyiség nélküli szervezetekre,

b) a központi elektronikus szolgáltató rendszer (a továbbiakban: központi rendszer) útján nyújtott szolgáltatásokra,

c) az elektronikus közszolgáltatásokat igénybe vevő szervezetekre és személyekre (a továbbiakban: felhasználó).

(2) E rendelet szabályait a központi rendszeren keresztül vagy annak szolgáltatásai igénybevételével nyújtott elektronikus közszolgáltatások vonatkozásában kell alkalmazni.

Értelmező rendelkezések

2. § E rendelet alkalmazásában:

a) *2D pontkód:* az elektronikus űrlapon rögzített tartalom nyomtatott formában történő, megfelelő vonalkód olvasóval elektronikus információvá alakítható, tömörített ábrázolása. A kinyomtatott és postán, papír alapon beküldött vagy személyesen benyújtott elektronikusan kitöltött űrlapok feldolgozásánál használatos megoldás;

b) *fix IP cím:* egy hálózati eszköz (pl. számítógép, szerver) elektronikus címzésének az a módja, amikor az eszközhöz az internet címzés szabályainak megfelelő állandó címet rendelünk. Állandó közvetlen internet kapcsolattal rendelkező eszközöknél általános megoldás;

c) *informatikai közháló:* a magyarországi közintézmények, oktatási intézmények, könyvtárak, önkormányzatok és más közösségi hozzáférési helyek számára széles sávú internetelérést biztosító és kapcsolódó egyéb szolgáltatások igénybevételét lehetővé tevő virtuális hálózati szolgáltató, a végponton elhelyezett hálózati eszközök üzemeltetésének biztosításával;

d) *illesztő felület:* két vagy több informatikai rendszer, alrendszer olyan közös felülete, ahol képesek egymásnak adatokat egymás által értelmezhető formában átadni-átvenni;

e) *KR boríték:* a központi rendszerben továbbított üzenetek címzésének és védelmének eszköze, amely biztosítja a tartalom megismerhetetlenségét és lehetővé teszi a címzéshez, eljuttatáshoz szükséges adatok kezelését, feldolgozását;

f) *második szintű domain:* a h) pont szerinti URL szerkezetben az első szint a pontokkal elválasztott utolsó elem, ettől balra található a második szint, jelen esetben a gov.hu tartomány, amelyben a Miniszterelnöki Hivatal regisztrál címeket (azaz a harmadik szinten);

g) *metaadat:* az adatok leírását, tulajdonságaik rögzítését szolgáló adat, információ;

h) *működtető:* e rendeletben kijelölt, az elektronikus közszolgáltatás megvalósítását a központi elektronikus szolgáltató rendszeren lehetővé tevő, a közszolgáltatásokat összehangoló közigazgatási szerv;

i) *szervezet:* valamennyi jogi személyiséggel rendelkező és jogi személyiséggel nem rendelkező jogképes szervezet, valamint az egyéni vállalkozás;

j) *URL:* webcím (Uniform Resource Locator [egységes erőforrás-azonosító] rövidítése), az Interneten megtalálható bizonyos erőforrások (például szövegek, képek) szabványosított címe. A formátumot részletesen az IETF RFC 1738

szabványa írja le. Egyetlen címben összefoglalja a dokumentum megtalálásához szükséges négy alapvető információt:

ja) a protokollt, amit a célgéppel való kommunikációhoz használunk;

jb) a szóban forgó gép vagy tartomány nevét;

jc) a hálózati port számát, amin az igényelt szolgáltatás elérhető a célgépen;

jd) a fájlhoz vezető elérési utat a célgépen belül;

k) *üzemeltető:* e rendeletben kijelölt, a központi rendszer elemeinek létrehozását, fejlesztését és üzemeltetését a működtető irányításával – szükség esetén más szervezetek bevonásával – közszolgáltatási szerződés keretében ellátó, a rendszer, mint egész működőképességét biztosító szervezet.

II. FEJEZET
A KÖZPONTI RENDSZER SZOLGÁLTATÓI

A központi rendszer működtetője, adatkezelője és üzemeltetője

3. § Az elektronikus közszolgáltatásokat biztosító központi elektronikus szolgáltató rendszert a Miniszterelnöki Hivatal működteti (a továbbiakban: működtető) a Pénzügyminisztérium, mint az elektronikus fizetési szolgáltatást biztosító alrendszer működtetője közreműködésével.

4. § (1) A központi rendszerben

a) az elektronikus közszolgáltatásról szóló törvény (a továbbiakban: Ekszt.) 16. § (4) bekezdése alapján az ügyfélkapu létesítése céljából kezelt adatok,

b) az Ekszt. 25. § (2) bekezdése alapján a hivatali kapu létesítéséhez szükséges, a hivatali kapu használatára feljogosított személyek adatainak kezelésére felhatalmazott képviselők adatainak,

c) az elektronikus tárhelyek, valamint

d) a szervezeti postafiókok

adatkezelője a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (a továbbiakban rövidítve: KEK KH).

(2) Az (1) bekezdés szerinti adatkezelés tekintetében az adatkezelő adatfeldolgozókat vehet igénybe. Az adatfeldolgozók bevonására a közigazgatási informatikáért felelős miniszter (a továbbiakban: miniszter) jóváhagyásával megkötött adatfeldolgozási szerződéssel kerülhet sor.

(3) Az adatkezelő az (1) bekezdés c) és d) pontjaiban szereplő adatok esetében csak a címzéshez kapcsolódó információt ismeri, kivéve, ha a felhasználó nem gondoskodott a rendelkezésre bocsátott eszközökkel annak titkosításáról, illetve nem tette lehetővé azok titkosítását a részére üzenetet küldők számára.

5. § (1) A központi rendszer – mint rendszer – üzemeltetését a Kopint-Datorg Infokommunikációs Zrt. (a továbbiakban: üzemeltető) a működtetővel kötött közszolgáltatási szerződés keretében látja el.

(2) Az üzemeltető a központi rendszer elemeinek létrehozását, fejlesztését és üzemeltetését a működtető irányításával látja el, a miniszter előzetes hozzájárulásával, a feladat jellegének megfelelően költségvetési szervek, illetve megfelelő beszerzési eljárásban kiválasztott vállalkozók közreműködését igénybe veheti.

(3) A 4. § szerinti adatkezelő az üzemeltetővel a központi rendszer üzemeltetése érdekében adatfeldolgozási megállapodást köt.

(4) Az üzemeltető köteles a központi rendszerhez kapcsolódó beszerzési eljárásaiba a működtető képviselőit bevonni. Az Európai Unió közbeszerzési értékhatárát meghaladó, a központi rendszerhez kapcsolódó beszerzései a miniszter jóváhagyásával válnak hatályossá (feltételhez kötött közbeszerzések).

(5) Az üzemeltető és az adatkezelő a központi rendszer bármely, a működés folyamatosságát veszélyeztető állapota vagy üzemzavara esetén köteles a működtető erre kijelölt képviselőit haladéktalanul értesíteni, és szükség esetén bevonásukkal megtenni a helyzet elhárításához szükséges lépéseket.

(6) Az üzemeltető havi rendszerességgel, utólag, a kormányzati portálon közzéteszi a központi rendszer igénybevételi adatait, valamint költségelszámolását, illetve a rendszer működtetéséből származó bevételeket.

A csatlakozott szolgáltatók

6. § (1) Az Ekszt. szerinti közigazgatási hatóságok – törvény vagy kormányrendelet eltérő rendelkezése hiányában – kötelesek csatlakozni a központi rendszerhez, és az egymás közötti elektronikus kapcsolattartást a központi rendszeren keresztül bonyolítani.

(2) A közigazgatási hatóság az elektronikus kapcsolattartás során – törvény eltérő rendelkezése hiányában – kizárólag a központi rendszer azonosítási szolgáltatását veheti igénybe. A közigazgatási hatóság az azonosítási szolgáltatás igénybevételéhez az informatikai rendszereit – az üzemeltetővel előre egyeztetett – illesztő felülettel látja el.

(3) A közigazgatási hatóság feladata az Ekszt. 7. § (1) és (3) bekezdése és a 9. § (1) bekezdése, valamint a 24. § (1) bekezdése szerinti kötelezettsége teljesítéséhez a központi rendszer és az informatikai rendszerei közötti e rendelet 18–19. §-aiban meghatározott követelményeknek megfelelő illesztő felület biztosítása.

(4) A közigazgatási hatóság a központi rendszerhez történő csatlakozást a központi rendszer működtetőjénél egyoldalú nyilatkozattal kezdeményezi. A központi rendszer működtetője a kezdeményezést köteles befogadni, arról az üzemeltetőt értesíteni, és 15 munkanapon belül megvizsgálni, hogy a közigazgatási hatóság és az általa nyújtani kívánt elektronikus közszolgáltatás a (2) és (3) bekezdésben foglaltaknak, valamint az Ekszt. 19. § (1) és (4), továbbá az elektronikus közszolgáltatás biztonságáról szóló kormányrendeletben foglalt biztonsági feltételeknek megfelel-e. A vizsgálat befejezését követően a működtető haladéktalanul értesíti a közigazgatási hatóságot és az üzemeltetőt a csatlakozás tervezett ütemezéséről, illetve a külön jogszabályban foglalt biztonsági feltételek hiánya esetében a csatlakozás megtagadásáról és a megtagadás okairól.

(5) A központi rendszer az Ekszt. 6. § (1) bekezdése alapján csatlakozók számára az Ekszt. 11. § (1) bekezdése szerinti alapszolgáltatásokon túl díjmentesen biztosítja:

a) a közigazgatási hatóságok csatlakozását, valamint

b) a közigazgatási hatóságok díjmentes, vagy jogszabállyal megállapított illeték vagy igazgatási szolgáltatási díj megfizetéséhez kötött közszolgáltatásainak hozzáférhetővé tételét.

(6) A központi rendszer a kiegészítő és emelt szintű szolgáltatásait a csatlakozott szervezetek számára – az Ekszt. 11. § (2) bekezdése alapján – a 10. § szerinti eljárásban, külön jogszabályban meghatározott díj ellenében nyújtja.

7. § (1) A közüzemi és egyetemes szolgáltatók– különösen a csatorna-, gáz-, távhő-, víz-, elektromos, köztisztasági, postai, temetkezési és tömegközlekedési szolgáltatók – (a továbbiakban együtt: közüzemi szolgáltatók) az Ekszt. 6. § (3), 7. § (2) és (3), valamint 19. § (4) bekezdése szerinti kötelezettségek teljesítése érdekében csatlakoznak a központi rendszerhez. Az érintett informatikai rendszerek az elektronikus közszolgáltatás biztonságáról szóló kormányrendeletben foglalt biztonsági feltételeknek és az e rendelet 18–19. §-aiban meghatározott követelményeknek megfelelő illesztése a központi rendszerhez – az üzemeltetővel előzetesen egyeztetetten – a közüzemi szolgáltató feladata.

(2) Az (1) bekezdés szerinti közüzemi szolgáltatók az 6. § szerinti hatóságokkal a kapcsolatot a központi rendszeren keresztül tartják. Az (1) és e bekezdés szerinti elektronikus kapcsolattartás során a személy- és szervezetazonosítási szolgáltatást a központi rendszer biztosítja.

(3) A közüzemi szolgáltatók a (2) bekezdésben nyújtott azonosítási szolgáltatás mellett ügyfeleiktől az ügyfeleik által velük kötött szolgáltatási szerződésre vonatkozó azonosító megadását is igényelhetik az elektronikus kapcsolattartáshoz.

(4) A közüzemi szolgáltatók csatlakozására a 6. § (4) bekezdésében meghatározott követelmények érvényesek azzal, hogy amennyiben az (1) és (2) bekezdésben meghatározott tevékenységeken túlmenő szolgáltatásokkal kívánnak csatlakozni, akkor ezen szolgáltatások tekintetében – az Ekszt. 6. § (7) bekezdésében foglaltak alapján – a kapcsolattartás a 11. §-ban foglaltak szerint díjköteles.

(5) A közüzemi szolgáltatók a várható ügyfélforgalommal arányosan – melynek megállapítására évenként, az előző év a központi rendszer naplózása nyomán megállapított forgalma alapján kerül sor – hozzájárulnak a központi rendszer fenntartásához. A hozzájárulást időarányosan, havonta kell megfizetni.

8. § (1) A bíróság, az ügyészség, a nyomozó hatóság az általuk folytatott eljárásokban egymással, a többi hatósággal, a védővel és a jogi képviselővel a központi rendszeren keresztül tartják az eljárási szabályok szerint írásbeliséget (dokumentummozgást) szükségessé tevő kapcsolatot. Az azonosítást a központi rendszer biztosítja.

(2) Az (1) bekezdésben említett szervezetek közérdekű és közérdekből nyilvános adataikat a kormányzati portálon is közzéteszik.

9. § (1) A 6–8. §-okban nem említett költségvetési szervek a 6. § (5) bekezdés b) pontja szerinti közszolgáltatások nyújtása és a 6–8. §-okban említett szervezetekkel való kapcsolattartás érdekében a 6. § (4) bekezdésben meghatározott eljárásrendben díjmentesen jogosultak a központi rendszerhez csatlakozni.

(2) Az (1) bekezdésben említett szervezetek az ott fel nem sorolt szolgáltatások nyújtásához a működtetővel kötött megállapodás alapján vehetik igénybe a központi rendszert. A megállapodás részeként az igényelt szolgáltatás erőforrás-igényével arányosan járulnak hozzá a központi rendszer fenntartásához. A költségek elszámolása havonta utólag, teljesítményarányosan történik.

10. § (1) A 6–9. §-okban nem említett nonprofit szervezetek a működtetővel kötött megállapodás alapján nyújthatnak szolgáltatásokat a központi rendszeren keresztül.

(2) A működtető a 6. § (4) bekezdésében rögzített feltételeknek megfelelő (1) bekezdés szerinti igénylőket – az üzemeltető egyidejű értesítése mellett – 30 munkanapon belül tájékoztatja a csatlakozás és szolgáltatásnyújtás rájuk érvényes feltételeiről.

(3) A megállapodásban rögzíteni kell a szervezet csatlakoztatásának díját és teljesítményigénnyel arányos költségviselésének feltételeit.

(4) A működtető közhasznú és kiemelkedően közhasznú szervezetek által nyújtott közérdekű, díjtalan szolgáltatások esetében jogosult eltekinteni a csatlakozási díjtól és a költségviseléstől.

11. § (1) Az 5–10. § hatálya alá nem tartozó szervezet az Ekszt. 6. § (7) bekezdése alapján, a működtető egyetértésével, az üzemeltetővel kötött visszterhes szerződés alapján csatlakozhat a központi rendszerhez, nyújthat szolgáltatásokat azon keresztül, illetve veheti igénybe annak szolgáltatásait. A csatlakozás kezdeményezését az üzemeltetőhöz kell benyújtani. Az üzemeltető a kezdeményezést – a kezdeményezés megérkezésétől számított 15 munkanapon belül –, a csatlakozás műszaki lehetőségeire és költségeire vonatkozóan kidolgozott javaslatával együtt továbbítja a működtetőnek.

(2) A működtető a csatlakozás támogatásáról az üzemeltető javaslatának kézhezvételét követő 15 munkanapon belül dönt. Elutasítás esetén döntését indokolnia kell. Amennyiben az elutasítás oka kapacitáshiány, meg kell jelölnie azt az időpontot, amikor az igényt ismételten meg fogja vizsgálni.

(3) Az üzemeltetőt a működtető egyetértése esetén is csak a 6–10. és 12. § alapján csatlakozó szervezetekkel szemben terheli szerződéskötési kötelezettség. A szerződéskötési kötelezettség csak az Ekszt. szerinti alapszolgáltatások biztosítására vonatkozik.

(4) A szerződés alapján csatlakozott szervezeteket a központi rendszer szolgáltatásainak igénybevételéért az üzemeltető felé terheli díjfizetési kötelezettség.

(5) Az üzemeltető maximum 5%-os haszonkulcsot érvényesíthet e szerződésekben és a tevékenység eredményét köteles a rendszer üzemeltetésére és fejlesztésére fordítani.

12. § (1) A működtető jogosult – a központi rendszer által és a központi rendszeren keresztül biztosított szolgáltatások elérhetőségének biztosítása érdekében – a központi rendszer erőforrásait az ügysegédi tevékenységre vállalkozók, a felhasználóknak informatikai, ügyintézési támogatást biztosító természetes és jogi személyek, jogi személyiség nélküli szervezetek számára, térítés ellenében rendelkezésére bocsátani.

(2) A vállalkozás jelleggel végzett ügysegédi tevékenység szakmai, biztonsági és informatikai feltételeit, az ellenőrzés szabályait külön jogszabály tartalmazza.

(3) A vállalkozás jelleggel ügysegédi tevékenységet végző által a központi rendszer üzemeltetőjének – a vele kötött szerződés alapján – fizetendő térítés egységes díjtételeit az üzemeltető a kormányzati portálon közzéteszi.

(4) A (2) bekezdésben szereplő feltételek nem teljesítése esetén a szolgáltatásra vonatkozó szerződés azonnali hatállyal felmondható.

A szervezetek és szolgáltatások csatlakoztatásának eljárásrendje

13. § (1) A 6–12. §-okban meghatározott szervezetek – az elektronikus közszolgáltatások nyújtásában való részvételre vonatkozó – csatlakozási igényüket a (3) és (4) bekezdésben meghatározott módon, csatlakozási űrlapon (a továbbiakban: űrlap) nyújthatják be a működtetőhöz.

(2) Az űrlap adattartalma:
   a) A szervezet neve
   b) A szervezet rövid neve
   c) A szervezet nyilvántartási vagy regisztrációs azonosító száma (költségvetési szervek esetében kincstári azonosító, PIR szám)
   d) A szervezet által használt fix IP cím
   e) A szervezet hivatali kapu kezelésére felhatalmazott képviselőjének neve és elektronikus levélcíme, valamint telefonszámai munkaidőben és azon kívül
   f) A szervezet – a bejegyzésére, nyilvántartására jogszabályban feljogosított szerv által vezetett nyilvántartás szerinti – képviselőjének aláírása

(3) A (2) bekezdés szerinti adatokat a (2) bekezdés f) pontja szerinti nyilvántartás adattartalmával megegyezően kell megadni. A (2) bekezdés f) pontja szerinti aláírás mellőzhető, amennyiben a csatlakozási űrlapot a (2) bekezdés f) pontja szerinti képviselő saját ügyfélkapuján keresztül továbbítja a működtető számára.

(4) Az űrlap a kormányzati portálról és a működtető honlapjáról tölthető le. A kitöltött űrlapot a csatlakozó szervezet (2) bekezdés f) pontja szerinti nyilvántartás szerint képviseletre jogosult vezetője a saját ügyfélkapujáról – a (3) bekezdésnek megfelelően, aláírás nélkül – elektronikusan küldheti meg. Amennyiben a (2) bekezdés f) pontja szerinti képviselőnek nincs ügyfélkapuja, az űrlapot postai úton kell megküldeni, a szervezet (2) bekezdés f) pontja szerinti képviselőjének aláírásával, valamint azt – a szervezet hivatali kapujának kezelésére felhatalmazott képviselő ügyfélkapuján keresztül – aláírás nélkül – is továbbítani szükséges.

(5) A megküldött űrlapban szereplő adatok módosítása az űrlap – a szervezet számára megnyitott hivatali kapun keresztüli, a szervezet hivatali kapujának kezelésére felhatalmazott képviselő általi – ismételt megküldésével lehetséges. Az adatok módosítása a hivatali kapu nyilvántartásában 1 üzemórán belül megtörténik.

(6) Amennyiben a szervezet hivatali kapujának kezelésére felhatalmazott képviselő adatai változnak, arra a (4) bekezdésben foglaltak alkalmazásával kerülhet sor.

(7) A csatlakozó szervezetek a csatlakozást követően lehetőséget kapnak az ügyfélkapuval, hivatali kapuval – annak a különböző szervezettípusok számára kialakított megjelenési formáival – rendelkező felhasználóktól érkező, a központi rendszerben rendszeresített elektronikus űrlapok fogadására, azok a szervezet nevében történő megválaszolására, valamint a hivatali kapuval, ügyfélkapuval rendelkező jogalanyokkal történő dokumentált, hiteles üzenetváltásra.

14. § (1) A csatlakozott szervezet a csatlakozást követően vagy azzal egyidejűleg igényelheti az általános nyomtatványtervezőnek a szervezet számára biztosított példányát, melynek segítségével megtervezheti a saját elektronikus és hagyományos beküldésre is alkalmas űrlapjait.

(2) Az általános nyomtatványtervező igényléséhez a 13. § (2) bekezdésében meghatározott adatokon kívül az ott előírt űrlapon a következő kiegészítő adatokat kell megadni:
   a) A szervezet nyomtatványainak és frissítéseinek elérését biztosító URL
   b) A szervezet nyomtatvány-erőforrásainak frissítését biztosító URL
   c) A szervezet ügyfélszolgálatának e-mail címe, telefon- és telefaxszáma, egyéb elérhetősége, az ügyfélszolgálat rendelkezésre állási ideje
   d) Igényli-e 2D pontkód nyomtatását
   e) A KR borítékon kezelendő speciális adatok, jellemzők

(3) A működtető a megszemélyesített nyomtatványtervezőt 10 munkanapon belül – az üzemeltető és az elektronikus űrlapok kezeléséért felelős KEK KH egyidejű értesítése mellett – elektronikus úton bocsátja rendelkezésre.

(4) A nyomtatványtervező rendelkezésre bocsátásával egyidejűleg a fix IP címmel csatlakozott szervezetek számára 2 felhasználói jelszóval az üzemeltető hozzáférést biztosít a központi rendszer tesztrendszeréhez, ahol lehetősége nyílik még jóvá nem hagyott nyomtatványok kipróbálására, ellenőrzésére.

(5) A működtető folyamatosan gondoskodik a nyomtatványtervező aktualizálásáról, továbbfejlesztéséről és az új verzió kibocsátásáról, illetve a szükséges teendőkről, ismeretekről, segédanyagokról a központi rendszeren keresztül tájékoztatja a szervezet – a csatlakozási űrlapon megjelölt – kapcsolattartóját. A nyomtatványok kialakítása során a KIB 27. számú ajánlásában foglaltakat kell figyelembe venni.

(6) A technikai vagy biztonsági okból szükséges verzióváltásra a működtető határidőt tűzhet ki. Az verzióváltás szükségességéről a (3) bekezdésben megjelölt, az elektronikus űrlapok kezeléséért felelős szerv értesíti az elektronikus

űrlapokat előállító szervezeteket, akik elkészítik az új verziókat és azokat minőségellenőrzésre megküldik az értesítést küldő szervezet részére.

(7) A verzióváltásra megjelölt határidő lejártát követően a lecserélt, elavult űrlapokat az űrlap előállítója és a (3) bekezdésben megjelölt, az elektronikus űrlapok kezeléséért felelős szerv egyaránt archívumba helyezi. Az archivált űrlapokat a központi rendszer a továbbiakban nem fogadja, azok csak a korábban elküldött adatszolgáltatások értelmezéséhez, megjelenítéséhez használhatók fel.

15. § (1) Az űrlapot készítő szervezet – az APEH kivételével – a bevezetésre tervezett elektronikus űrlapot minőségellenőrzés céljából az erre szolgáló, a kormányzati portálról letölthető elektronikus űrlap mellékleteként a 14. § (3) bekezdésében megjelölt, az elektronikus űrlapok kezeléséért felelős szervnek elektronikusan megküldi.

(2) A 14. § (3) bekezdése szerinti, az elektronikus űrlapok kezeléséért felelős szerv 15 munkanapon belül elvégzi a tervezett nyomtatványok minőségellenőrzését, és javaslatot tesz az esetleg szükséges módosításokra, kiegészítésekre.

(3) A 14. § (3) bekezdése szerinti, az elektronikus űrlapok kezeléséért felelős szerv az általa megfelelőnek minősített elektronikus űrlapokat a kormányzati portál elektronikus űrlapok közzétételére szolgáló aloldalán haladéktalanul közzéteszi, és az elkészült elektronikus űrlapot az előkészítő szervezetnek megküldi.

(4) Az APEH az (1) bekezdés szerinti minőségellenőrzést önállóan végzi, és az elkészült űrlapot megküldi a 14. § (3) bekezdése szerinti, az elektronikus űrlapok kezeléséért felelős szervnek. A közzétételt a kormányzati portálon 1 munkanapon belül kell biztosítani.

(5) A központi rendszer csak a 14–15. §-okban meghatározott eljárásrend alapján közzétett űrlapok forgalmazását biztosítja az ügyfélkapuk és a hivatali kapuk között.

(6) Biztonsági kockázat vagy más az űrlapot tervező szervezettől független ok miatt bekövetkező rendkívül verzióváltás vagy űrlap soron kívüli bevezetésének szükségessége esetén a 14. § (3) bekezdése szerinti, az elektronikus űrlapok kezeléséért felelős szerv a miniszter utasítására haladéktalanul elvégzi az e rendelkezés szerinti feladatait.

16. § (1) Amennyiben egy csatlakozott szervezet vagy azok társulása olyan alkalmazást, szolgáltatást kíván megvalósítani, amely használja a központi rendszer valamely szolgáltatását, erre az üzemeltetővel előzetesen egyeztetett, a működtetővel kötött együttműködési megállapodás alapján kerülhet sor. A működtető a csatlakozáshoz, az egyes szolgáltatások igénybevételéhez szükséges dokumentumokat, segédleteket a www.ekk.gov.hu honlapon bocsátja rendelkezésre.

(2) Az (1) bekezdés szerinti megállapodásnak tartalmazni kell:

a) az együttesen megvalósítandó szolgáltatást, annak jogalapját,

b) az adatok kezelésére vonatkozó felhatalmazás megjelölését,

c) a központi rendszer és a csatlakozott rendszer által e szolgáltatás megvalósításához biztosított szolgáltatásokat,

d) a szolgáltatások kialakításához, együttműködési képességéhez (interoperabilitásához) szükséges információkat, előírásokat,

e) az adatok kezelésére vonatkozó felhatalmazás alapján átadandó és átveendő adatokat,

f) a szolgáltatás támogatásával, a tájékoztatással, az ügyfélszolgálat feltételrendszerével kapcsolatos rendelkezéseket, valamint

g) az üzemzavar esetén követendő eljárásrendet.

(3) A megállapodásban rendelkezni kell továbbá a vállalt rendelkezésre állási szintről és az esetlegesen elégtelen kapacitás esetén követendő eljárásokról.

(4) A megállapodást újabb szolgáltatás igénybevétele esetén ki kell egészíteni az arra vonatkozó követelményekkel. Nem kell a megállapodás műszaki tartalmát módosítani, ha azonos szolgáltatás igénybevétele, illetve nyújtása bővül. Ebben az esetben, amennyiben az új szolgáltatás e rendelet 6–12. §-ai alapján díjköteles, csak a költségviselésről szükséges kiegészítő megállapodás.

(5) A működtető és megbízottja jogosult a megállapodásban foglaltak az üzemeltetőnél és a csatlakozott szervezetnél történő helyszíni ellenőrzésére.

(6) A megállapodás megkötését és a külön jogszabályban rögzített biztonsági, adatbiztonsági követelmények igazolását követően az alkalmazást először a központi rendszer tesztrendszeréhez kell csatlakoztatni, majd az elvégzett sikeres együttműködési, kommunikációs teszteket követően kell a szolgáltatást a központi rendszerben hozzáférhetővé tenni. A tesztelést dokumentálni kell.

(7) A működtető jogosult a (2) bekezdés szerinti megállapodásban rögzített korlátozási feltételek bekövetkezésekor, valamint a rendszer biztonsága és működőképessége veszélyeztetésének észlelése esetén a veszélyeztető vagy túlterhelő szolgáltatásokat korlátozni, felfüggeszteni.

(8) Veszélyhelyzet esetén az üzemeltető – a működtető és az érintett egyidejű tájékoztatása mellett – jogosult a (7) bekezdésben rögzített azonnali intézkedésekre.

Együttműködés az ügyfélvonallal

17. § (1) Minden az Ekszt. hatálya alá tartozó szervezet – a nemzetbiztonsági szolgálatok kivételével – együttműködésre kötelezett az ügyfélvonallal.

(2) A központi államigazgatási szervek kötelesek az ügyfélvonal rendelkezésére bocsátani:

a) az általuk és az általuk irányított szervek által intézett ügyekre vonatozó ügymenet modelleket, és

b) az egyes ügytípusokhoz kapcsolódó, állampolgári tájékoztatást szolgáló információkat.

(3) A központi, területi és helyi önkormányzati közigazgatási hatóságok az egyedi ügyben történő felvilágosítás biztosíthatósága érdekében – törvény eltérő rendelkezése hiányában – kötelesek az ügyfélvonal rendelkezésére bocsátani az egyes ügytípusok intézéséért felelős vezető nevét, hivatali elérhetőségét.

(4) Az egyéb elektronikus közszolgáltatást nyújtó szervezetek kötelesek az ügyfélvonal rendelkezésére bocsátani az ügyfélszolgálataik elérhetőségét, az ügyfélszolgálatoknál tájékoztatásra használt információkat, segédanyagokat.

(5) Az együttműködés tartalmi elemeit az ügyfélvonal (2) bekezdés szerinti alaptevékenysége, valamint az érintett közigazgatási szerv feladat-, hatáskörére, illetve a közszolgáltató szerv tevékenységi, ellátási körére figyelemmel az elektronikus közszolgáltatást nyújtó szervezet és az ügyfélvonal üzemeltetője között megkötött – a 16. § szerinti megállapodás részét képező – együttműködési megállapodás rögzíti.

(6) Az ügyfélvonal üzemeltetőjét és az adatszolgáltatásra kötelezett elektronikus közszolgáltatást nyújtó szervezetet az elektronikus közszolgáltatás igénybevételéről szóló rendelet szerinti alaptevékenységek vonatkozásában kölcsönös megállapodáskötési és az ügyfélvonal üzemeltetőjét feladatellátási kötelezettség terheli.

(7) Az ügyfélvonal üzemeltetője az ügyfélvonal alaptevékenységéhez nem tartozó ügyfélkapcsolati szolgáltatások igénye esetén a szolgáltatásra megbízást adó szervezettel költségtérítésben állapodhat meg.

III. FEJEZET
A SZOLGÁLTATÁSNYÚJTÁS MŰSZAKI KÖVETELMÉNYEI

18. § (1) Az elektronikus közszolgáltatásban részt vevő informatikai rendszerek tervezése és megvalósítása során biztosítani kell a következő követelmények teljesítését:

a) képesnek kell lenniük az egymás közötti együttműködésre, az alrendszerek közötti kommunikáció, azonosítás, adatcsere, adatelérés, alkalmazás-integráció és azok biztonsága terén,

b) adatjelentéstani (szemantikai) szempontból egységes alapra kell épülniük, ami lehetővé teszi az átadott adatok, metaadatok közvetlen feldolgozását, az egységes fogalmi modellezést, tranzakció- és eseménykezelést,

c) ügyféloldalon a megkövetelt informatikai eszközök lehetséges minimumára kell építeni úgy, hogy azok minden, széles körben elterjedt operációs rendszerből funkcióvesztés nélkül elérhetők legyenek,

d) képesnek kell lenniük – megfelelő illesztéssel – az Európai Unió hasonló rendszerei számára történő adatszolgáltatásra, illetve az onnan átvett adatok értelmezésére.

(2) Az (1) bekezdésben megfogalmazott követelményeknek való megfeleléshez elégséges szabványokat, ajánlásokat és más műszaki előírásokat a miniszter az egységes közigazgatási informatikai követelmény- és tudástár részeként elektronikusan közzéteszi a www.ekk.gov.hu honlapon, illetve gondoskodik annak karbantartásáról, frissítéséről.

(3) Az (1) bekezdésben meghatározott technikai információk kialakításában a Közigazgatási Informatikai Bizottság részt vesz. A Közigazgatási Informatikai Bizottság tagjai jogosultak javaslatot tenni a követelmény- és tudástár bővítésére, egyes elemeinek cseréjére, módosítására.

(4) Költségvetési és EU forrásokból csak olyan elektronikus közszolgáltatás létrehozása, fejlesztése valósítható meg, amely biztosítani képes az együttműködést a központi rendszerrel. Együttműködésre a követelménytárban szereplő előírásokat kielégítő vagy az együttműködési képességet egyéb módon igazoló rendszer képes. Az együttműködési képesség igazolása, illetve annak a működtető általi elfogadása a fejlesztés indításának feltétele.

(5) A lehetséges fejlesztési irányok gyakorlati kipróbálása érdekében a miniszter engedélyével a követelmény- és tudástárban rögzített megoldásoktól el lehet térni. A miniszter engedélyét indoklással ellátott javaslatban kell kérni, melyben ki kell térni az eltérő fejlesztési irány elvárt előnyeire és a követelmény- és tudástár többi elemeivel való összhang megteremtésének költségeire. A javaslatról a miniszter – szükség esetén független szakértők és szakmai szervezetek, illetve a Nemzeti Hírközlési és Informatikai Tanács véleményének kikérésével – dönt.

19. § (1) Az elektronikus közszolgáltatások nyújtása, illetve igénybevétele során az elektronikus űrlapokhoz csatolt elektronikus dokumentum akkor kezelhető, ha a dokumentum olyan formátumban készült, amelyre a 18. § (1) bekezdésében foglalt követelmények teljesülnek és szerepel a 18. § (2) bekezdése szerint közzétett, a követelmények teljesítésére alkalmas megoldások között.

(2) A dokumentum csak akkor tekinthető a követelményeket kielégítőnek, ha a tartalmához való hozzáférést nem akadályozza olyan műszaki intézkedés (így különösen rejtjelezés, nyomtatás tiltása, korlátozása, a hozzáférés időbeli, funkciók vagy felhasználók szerinti korlátozása digitális jogvédelem útján vagy bármely egyéb hasonló módon), amelyet a beküldő a szolgáltatás nyújtójával előzetesen nem egyeztetett, vagy jogszabály annak használatát nem írja elő.

(3) Az űrlapot fogadó szervezet a 18. § (2) bekezdés szerint közzétett megoldásokon túlmenően is alkalmazhat dokumentumformátumokat a küldemények mellékleteiben – különösen nemzetközi együttműködés alapján fennálló kötelezettségek miatt –, ha az adott formátum meghatározását előzetesen a miniszter egyetértésével jogszabályban rögzítette, valamint honlapján és a kormányzati portálon az űrlapra vonatkozó tájékoztató részeként közzétette.

(4) A szolgáltatást nyújtó szervezet a (3) bekezdésben meghatározott közzététel érdekében a miniszterhez benyújtja:

a) az alkalmazni kívánt formátum meghatározását, amely magában foglalja a szabványt vagy a formátumra vonatkozó nyilvános dokumentumot, továbbá szükség szerint a formátummal kapcsolatos egyes korlátozásokat vagy más jellemzőket, és az elfogadni kívánt adatszerkezet vagy más műszaki tartalom tételes, az alkalmazáshoz és az egyetértés gyakorlásához szükséges részletezettségű leírását;

b) annak a közigazgatási hatósági eljárásnak a megnevezését, amelyben a javasolt formátumot elfogadni tervezi, valamint azt a jellemzőt, amely miatt a formátumot a követelménytárban szereplőknél célszerűbbnek ítéli a feladat ellátására.

(5) A miniszter a formátum egyedi alkalmazási lehetőségéről 22 munkanap alatt dönt. Az engedélyezést akkor tagadhatja meg, ha egyenértékű vagy jobb megoldás szerepel a követelmény- és tudástárban, és a konverzió külön költség nélkül és egyenértékűen biztosított.

(6) Az elektronikus közszolgáltatást nyújtó szervezet a 18. § (2) bekezdés szerint közzétett lehetőségekhez képest szűkítheti a kezelt formátumokat, ha az az adott feladatra nem értelmezhető, és erről a honlapján és a kormányzati portálon megfelelő tájékoztatást tett közzé. A tájékoztatás az alkalmazható formátumok felsorolásával is történhet.

(7) A támogatott, kezelt formátum megváltozása esetén a fogadó szervezet legalább az új formátum közzétételétől számított 60 napig köteles a már nem támogatott formátumot is fogadni, kivéve, ha a formátum alkalmazása biztonsági kockázatot jelent. Ez utóbbi esetben 60 napig szankciómentes hiánypótlási lehetőséget kell biztosítani.

(8) Az elektronikus közszolgáltatást nyújtó szervezet egyes felhasználóival egyedileg is megállapodhat a közzétett formátumtól eltérő formátumok használatában, de ez a megoldás nem érinti a szervezet irattárazási, dokumentálási – illetve amennyiben van – levéltárba adási kötelezettségének egységességét.

20. § Az elektronikus ügyintézés használatának könnyítése céljából az elektronikus közszolgáltatást ellátó alrendszerek kialakítása során törekedni kell az egységes arculat és ügyfélbarát felhasználói felület használatára, és biztosítani kell az akadálymentességet. Az ennek megvalósítását lehetővé tevő dokumentumokat a működtető a www.ekk.gov.hu honlapon közzéteszi.

IV. FEJEZET
AZ ELEKTRONIKUS KÖZSZOLGÁLTATÁST NYÚJTÓK SZÁMÁRA BIZTOSÍTOTT SZOLGÁLTATÁSOK

Hálózati alap- és emelt szintű szolgáltatások

21. § (1) A központi rendszer részét képező elektronikus kormányzati gerinchálózat (a továbbiakban: EKG), illetőleg az informatikai közháló (a továbbiakban: IKH) alapszolgáltatásként biztosítja a hálózatokhoz csatlakozottak számára az

internet-hozzáférést, illetve az elektronikus közszolgáltatást az EKG-n keresztül nyújtók számára a szolgáltatásuk EKG-n keresztüli nyújtásának lehetőségét, elérhetőségét.

(2) A Miniszterelnöki Hivatal
   a) felügyeli a gov.hu második szintű domaint, amelyben minden kormányzati, közigazgatási szerv külön díjazás nélkül domain-név használati lehetőséget kaphat;
   b) működteti az e szolgáltatáshoz szükséges névfeloldó (DNS) szervereket;
   c) az EKG és IKH felhasználói számára biztosítja virtuális magánhálózatok kialakításának lehetőségét és működtetését;
   d) az EKG-n és IKH-n elektronikus levéltovábbítási szolgáltatást biztosít;
   e) az EKG és IKH felhasználóinak a biztonságos működés támogatására folyamatos helpdesk szolgáltatás biztosít interneten és telefonon.

(3) Az e szakaszban leírt szolgáltatások külön díjazás nélkül vehetők igénybe.

22. § (1) A központi rendszer az Ekszt. 11. § (2) bekezdése alapján kiegészítő infrastrukturális szolgáltatásokat is nyújthat, ennek minősül különösen:
   a) az időbélyeg szolgáltatás;
   b) az emelt szintű integrált adatszolgáltatás;
   c) az internet-telefon (VoIP) alapú hangszolgáltatás;
   d) az informatikai biztonsági és védelmi szolgáltatások;
   e) a videokonferencia szolgáltatás;
   f) az elektronikus adatcsere szolgáltatás (EDI);
   g) üzemeltetési szolgáltatás az intézmények tulajdonában lévő, a központi rendszerhez csatlakozó eszközök vonatkozásában;
   h) központilag felügyelt tűzfal-szolgáltatás;
   i) adatközpont szolgáltatások.

(2) Felhasználói igény esetén az üzemeltető az (1) bekezdéstől eltérő, további kiegészítő szolgáltatást is nyújthat, ennek feltételeiről és az igénybevételért fizetendő díjról az üzemeltető és a szolgáltatás igénybe vevője külön megállapodást köt.

(3) Az EKG, illetve az IKH használója a hálózati kapcsolatot biztosító és a kiegészítő szolgáltatásokat is kizárólag a működtető által lebonyolított nemzetbiztonsági beszerzés eredményeként létrejött keretmegállapodásban szereplő szolgáltatóktól, egyoldalú nyilatkozattal rendelheti meg.

(4) A szolgáltatások – az alapvető biztonság, nemzetbiztonsági érdekeket érintő beszerzések szabályairól szóló kormányrendelet alapján létrejött keretmegállapodás szerinti – kiinduló díjait – melyeknél a csatlakozott szervezet a szolgáltatóval folytatott írásbeli konzultáció alapján kedvezőbb feltételekben is megállapodhat – a működtető a www.ekk.gov.hu, az EKG, illetve IKH a szolgáltatást igénybe vevő felhasználói számára hozzáférhető aloldalán teszi közzé.

(5) A központi rendszer igénybe vett kiegészítő szolgáltatásainak díjait, továbbá a megyei EKG csatlakozási ponttól a szervezetig terjedő hálózati szolgáltatás díját a felhasználó tervezi és viseli.

Az elektronikus kormányzati gerinchálózat

23. § (1) Az EKG hálózatgazdája a zártcélú hálózatokról szóló kormányrendelet alapján, az ott rögzített jogokkal és kötelezettségekkel a közigazgatási informatikáért felelős miniszter. A miniszter a hálózat működtetésével kapcsolatos feladatát a közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala közreműködésével látja el.

(2) Az EKG biztosítja a közigazgatási és rendvédelmi szervek egységes hálózati infrastruktúrájának alapját. Ezen szervek – jogszabályban meghatározott kivételekkel – más zárt célú hálózatot nem tarthatnak fenn, az EKG-tól eltérő hordozón – a nyilvános vezetékes és mobil távközlési szolgáltatóktól igénybe vett beszédcélú telefonszolgáltatáson kívül – nem létesíthetnek távközlési, informatikai összeköttetéseket.

(3) A Központi Szolgáltatási Főigazgatóság az EKG-t mint infrastruktúrát használva működteti a kormányzati hálózatot.

(4) Az EU intézményeivel kapcsolatot tartó közigazgatási szervek számára a TESTA kapcsolat az EKG-n keresztül biztosított.

(5) Az EKG Budapesten kívüli hálózati csomópontjai a Magyar Államkincstár megyei szolgáltató egységeinek épületeiben üzemelnek.

(6) Nem részei az EKG-nak a következő – részben közigazgatási feladatot is ellátó – zártcélú hálózatok:
a) a nemzetbiztonsági szolgálatok speciális műveleti hálózatai;
b) a Honvédelmi Minisztérium által működtetett katonai műveleti hálózatok;
c) az Egységes Digitális Rádiótávközlő Rendszer;
d) a Külügyminisztérium által Magyarországon és külképviseleti viszonylatban működtetett diplomáciai információs rendszerek;
e) a Magyar Köztársaság nemzetközi kötelezettségeiből adódóan működtetett nemzetközi zártcélú hálózatok.

(7) A (6) bekezdés c) pontjában meghatározott zártcélú hálózat és az EKG együttműködését összekapcsolással kell biztosítani.

(8) Az EKG-val összefüggő használati követelményeket, az e rendelet mellékletében foglalt EKG használati szabályzat tartalmazza.

(9) Rendkívüli esemény esetén, annak észlelését követően az érintettek kötelesek haladéktalanul tájékoztatni erről a hálózatgazdát, és haladéktalanul kötelesek megkezdeni hiba, veszélyhelyzet felszámolását. Amennyiben az EKG üzembiztonsága ezt megköveteli, úgy a rendellenesség megszüntetéséig a hálózatgazda a hálózat működőképességének fenntartása érdekében a hálózati zavart okozó hálózati kapcsolatát megszakítja.

24. § (1) A központi államigazgatási szervek, a kormányhivatalok – törvény eltérő rendelkezése hiányában – területi szerveikkel együtt kötelesek csatlakozni az EKG-hoz.

(2) Rendvédelmi szervek – jogszabály eltérő rendelkezése hiányában – kötelesek csatlakozni az EKG-hoz.

(3) Más költségvetési szervek, köztestületek, valamint a helyi önkormányzatok önként csatlakozhatnak az EKG-hoz.

(4) Vállalkozás csak a következő esetekben csatlakozhat az EKG-hoz, és annak szolgáltatásait csak a következő célokból használhatja:
a) jogszabályban közfeladat ellátására kötelezett vállalkozás – a közfeladatával összefüggésben nyújtott elektronikus közszolgáltatással kapcsolatban,
b) a központi rendszer egyes elemeit üzemeltető vagy a központi rendszerhez csatlakozásra kötelezett szervezet által nyújtott elektronikus közszolgáltatást üzemeltető vállalkozás – ezen üzemeltetési feladatainak ellátásával kapcsolatban.

(5) Az (1)–(4) bekezdésben foglaltakon túl, az EKG-hoz más jogi személy és jogi személyiséggel nem rendelkező szervezet, illetve természetes személy nem csatlakozhat.

25. § (1) Az EKG-hoz csatlakozni kívánó vagy arra kötelezett szervezet az EKG csatlakozást a hálózatgazdához címzett és a központi rendszert működtetőjének megküldött EKG csatlakozási bejelentésben igényli.

(2) Az EKG felhasználói hozzáférési pontja az EKG és a felhasználó rendszere között kapcsolatot biztosító hálózati elem (felhordó hálózat) felhasználói végpontján létesül. Amennyiben a felhasználónál – műszaki, gazdasági okok miatt – hozzáférési pont nem létesíthető, úgy az EKG hálózatgazdája és a felhasználó megállapodhat arról, hogy a felhasználó a csatlakozást e célra külső szolgáltató által létesített összeköttetés igénybevételével is megvalósíthatja.

(3) A felhasználó által igénybe vett sávszélességről, a szolgáltatás körülményeiről az EKG hálózatgazdája – az üzemeltető szakmai előkészítésével, támogatásával – a felhasználóval állapodik meg.

(4) Az EKG-hoz csatlakozott elektronikus közszolgáltatást nyújtó szervezet – a (2) bekezdés szerinti kivétellel – szolgáltatásait kizárólag az EKG útján teheti elérhetővé.

(5) A szervezetet az EKG-hoz történő csatlakozása – az EKG és a központi rendszer számára nyújtott szolgáltatásain túlmenően – nem jogosítja fel arra, hogy a központi rendszer útján elektronikus közszolgáltatást nyújtson. Az elektronikus közszolgáltatás nyújtásának további feltétele e rendelet 16. § szerinti megállapodás megkötése.

Az informatikai közháló

26. § (1) Az IKH működtetését a Miniszterelnöki Hivatal a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala közreműködésével biztosítja. A rendszer felügyeletét, szolgáltatásait az EKG-val összehangoltan valósítja meg. A szolgáltatást közbeszerzés alapján kiválasztott szolgáltatók biztosítják.

(2) A közhálóra csatlakozott szervezetek alapszintű szolgáltatásra külön díj megfizetése nélkül jogosultak, emelt szintű szolgáltatások igénybevétele esetén a közbeszerzési eljárás eredményeként kialakult díjtételeket meg kell fizetniük.

(3) Az IKH alapszintű szolgáltatása: szélessávú internet és levelezési szolgáltatás a legjobb gyakorlat szerint, minőségi garanciák nélkül.

V. FEJEZET
MÓDOSULÓ RENDELKEZÉSEK

27. § (1) A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről szóló 276/2006. (XII. 23.) Korm. rendelet (a továbbiakban: R.) 16/C. § (5) bekezdése c) pontja helyébe a következő rendelkezés lép:

[A KEK KH]

„c) a központi elektronikus szolgáltató rendszer által kezelt adatok tekintetében adatkezelőként jár el, továbbá a központi rendszer működtetőjével és üzemeltetőjével együttműködve ellátja az ügyfélkapuhoz és hivatali kapuhoz történő csatlakozások koordinációs és adminisztratív feladatait."

(2) Az R. 16/C. § (6) bekezdése helyébe a következő rendelkezés lép:

„(6) A KEK KH ellátja – az APEH kivételével – központi államigazgatási szervek és helyi, területi szerveik hatósági eljárásaiban rendszeresített, elektronikusan kitölthető nyomtatványok ellenőrzési, minőségbiztosítási, valamint a központi rendszerben történő megjelenítési feladatait. Szakmai támogatást nyújt a közigazgatási szerveknek az űrlapok tervezése során."

VI. FEJEZET
ZÁRÓ RENDELKEZÉSEK

28. § (1) A rendelet – a (2)–(3) bekezdésben meghatározott kivétellel – a kihirdetését követő 8. napon lép hatályba.

(2) Az 5. § (1) bekezdése 2010. január 1-jén lép hatályba.

(3) A 8. § 2012. január 1-jén lép hatályba.

(4) A 27. § 2009. november 1-jén hatályát veszti.

(5) A 30. § 2011. január 2-án hatályát veszti.

(6) A 31–32. § 2012. január 2-án hatályát veszti.

29. § Hatályát veszti az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól szóló 12/2005. (X. 27.) IHM rendelet.

Átmeneti rendelkezések

30. § (1) A közüzemi szolgáltatók a 7. § (1) bekezdésben meghatározott adataik és szolgáltatásaik hozzáférhetővé tétele, illetve a közigazgatási hatóságokkal való elektronikus kapcsolattartás érdekében az Ekszt. 33. § (2) bekezdésében meghatározott időpontig (2010. január 1.) kötelesek a központi rendszerhez csatlakozni.

(2) Az első naptári évben a 7. § (1) bekezdésben meghatározott szolgáltatások nyújtásához biztosított központi rendszer szolgáltatás díjmentes.

31. § A bíróságok a hivatalos iratok elektronikus kézbesítéséről szóló törvény 14–15. §-ában meghatározott feladataik megvalósítása érdekében 2010. január 1-jéig a 6. § (4) bekezdésében meghatározott módon csatlakoznak a központi rendszerhez.

32. § A jelenleg elektronikus közszolgáltatást nyújtó rendszereknek az e rendelet 18–20. §-aiban foglalt együttműködési feltételeknek 2011. december 31-ig kell megfelelniük az elektronikus közszolgáltatás biztonságáról szóló kormányrendelet szerinti auditálással együtt.

33. § A mezőgazdasági és vidékfejlesztési támogatási szerv a mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény hatálya alá tartozó intézkedésekkel összefüggő eljárásokban 2012. január 1-jéig terjedő időszakban az ügyfélkapu azonosításával, részben a központi rendszeren keresztül nyújtja az elektronikus közszolgáltatást.

Bajnai Gordon s. k.,
miniszterelnök

Melléklet a 222/2009. (X. 14.) Korm. rendelethez

Az elektronikus kormányzati gerinchálózat használati szabályzata

1. Elektronikus kormányzati gerinchálózat (a továbbiakban: EKG)

1.1. A kormányzati hálózat szerepe

A kormányzati és közigazgatási adatbázisok, informatikai rendszerek összekapcsolása, valamint a különböző szolgáltatások elérhetőségének biztosítása a kormányzati hálózat feladata. Ez az infrastrukturális elem – a központi elektronikus szolgáltatási rendszer egyik fő összetevőjeként – távolról is elérhetővé teszi a különféle átfogó alkalmazásokat, számítógépes külső és belső adatszolgáltatásokat, kommunikációs elemeket, amelyek ennek révén egységes egészként funkcionálnak. Ezzel válik lehetővé a kormányzati rendszerek elektronizálása és új, hatékony szolgáltatási rendszerek bevezetése, vagyis az e-kormányzat kialakítása.

1.2. Az EKG célja, rendeltetése

– Nagy sebességű, nagy üzembiztonságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú IP hálózati infrastruktúra biztosítása;
– Az infrastruktúrára épülő szolgáltatások és egyes, eddig elszigetelt (pl. ágazati) hálózatok elérhetővé tétele a jogosult felhasználók számára;
– A kormányzati szervek közötti kommunikáció, az adatátvitel költségeinek csökkentése, minőségi szintjének emelése;
– Kormányzati szintű, több felhasználó által használt alkalmazások hatékony működtetése;
– Olyan infrastrukturális háttér biztosítása, amely alkalmas az elektronikus ügyvitel, elektronikus ügyintézés feltételeinek biztosítására, az elektronikus közigazgatás koncepciójának, vagyis az állampolgár és a kormányzat újszerű kapcsolatának kiszolgálására.

1.3. Az EKG legfőbb feladatai

a) Biztosítson megfelelő informatikai infrastruktúrát a civil szféra számára az állami intézmények által nyújtott szolgáltatások eléréséhez (Front-Office feladatok).
b) Biztosítson megfelelő informatikai infrastruktúrát a kormányzati intézmények számára a kormányzati feladatok ellátásához (Back-Office feladatok).
c) Biztosítsa a megfelelő védettségű kétirányú kormányzati kapcsolatokat a brüsszeli EU adminisztráció informatikai rendszereihez.

Az országos kormányzati hálózat nagysebességű kapcsolatot valósít meg mind a budapesti intézmények, mind a gerinchálózat elérési pontjain keresztül az ország területén működő, elsődlegesen közigazgatási, és a közigazgatás működését támogató intézmények között.

1.3.1. Az EKG által biztosított szolgáltatások főbb tulajdonságai

Az intézményi hálózatok logikai elkülöníthetősége biztosítható. A hálózatot számos intézmény használja, ezért garanciális és biztonsági szempontok miatt arra van szükség, hogy a jelenlegi, fizikailag is különálló rendszerekhez hasonló rugalmasság és logikai elkülönültség megvalósítható legyen. Ez a követelmény kielégíthető az ún. távközlési virtuális magánhálózatok (MPLS VPN-ek) kialakításával.

Az egyes intézményi hálózatok között szabályozott kommunikáció működik az érintett intézmények igényei szerint, így megvalósul az intézményi hálózatok közötti szabályozott kapcsolat a hálózat fizikai topológiájának megváltoztatása nélkül. Léteznek olyan központi erőforrások, amelyekhez egyidejűleg több intézménynek is hozzá kell férnie, ezt a célt szolgálják az ún. extranetek is.

A hálózat rendelkezésre állása azonos vagy jobb, mint a különálló megoldásokkal elérhető rendelkezésre állási szint.

A hálózat a gerincszakaszokon biztosítja az infrastruktúrát nagy sávszélesség-igényű, multimédiás alkalmazások számára is (pl. videokonferencia stb.), a csatlakozó intézménynek magának kell a kapcsolat sávszélességéről a csomópontig terjedő szakaszra vonatkozóan gondoskodnia az EKG hálózatgazdájával egyeztetetten.

1.3.2. Alap infrastruktúra és az üzemeltetés jellemzői

Biztonsági vagy technikai indokok alapján az összeköttetésekben az optikai alapú technológia, ezen belül szolgáltatótól bérelt ún. „sötét szál" alkalmazása dominál Budapesten. A hálózat felügyeletét a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala látja el a közigazgatási informatikáért felelős miniszter munkaszervezeteként.

A gerinchálózat szolgáltatásai országosan a megyei gerinchálózat elérési pontoknál (Point of Presence, PoP) állnak rendelkezésre. A PoP-ok feladata a fizikai infrastruktúra, az üzemeltetési környezet (helyiség, szünetmentes tápellátás stb.) biztosítása. Az üzemeltetés részét képező rendszerfelügyeletet és menedzsmentet a központi üzemeltetést felügyelő szervezet végzi, távolról. A PoP-ok a Magyar Államkincstár kijelölt megyei telephelyein üzemelnek.

Az üzemeltetés feladatát a 100%-os állami tulajdonú Kopint-Datorg Infokommunikációs Zrt. látja el. Ez a megoldás – más, vásárolt szolgáltatásokkal kiegészítve – képes biztosítani a szükséges szaktudást, ugyanakkor kezelhetővé csökkenti a biztonsági kockázatot. Ez az üzemeltetési modell megfelelően rugalmas számos központi felügyeletet igénylő kormányzati informatikai feladat ellátására is (pl. kormányzati portál, ügyfélkapu stb.).

1.4. A kormányzati gerinchálózat néhány gazdasági kérdése

A gerinchálózat a párhuzamos hálózatok üzemeltetési költségeinél (távközlési díjainál) lényegesen alacsonyabb pénzügyi ráfordítással (30–50%-os megtakarítással) és/vagy lényegesen nagyobb sebességgel (sávszélességgel), jobb minőségben és nagyobb üzembiztonsággal szolgáltatja az infrastruktúrát és a szolgáltatásokat az intézmények számára. A magasabb üzembiztonsági követelmény ugyanakkor a megyei elosztóponttól az intézményi hálózat csatlakozási pontjáig terjedő szakaszt esetenként költségesebbé teheti. A rendszer egészének alkalmazása azonban egyértelműen költségcsökkentő.

A kialakított IP alapú hangátviteli lehetőség és kapcsolóközpont további jelentős megtakarításokat tesz elérhetővé azáltal, hogy az EKG-t hangátvitelre is használó intézmények intézményen belüli és a rendszerhez csatlakozott társintézményekbe irányuló telefonforgalma díjmentes, de más – Magyarország területén belül maradó – telefonforgalmuk is csak a helyi hívásoknak megfelelő díjszabás alá esik. A megtakarítások annak arányában növekednek, minél több intézmény kapcsolódik az EKG IP alapú hangátviteli hálózatához.

2. A szabályzat célja

A szabályzat a felhasználók, a hálózatgazda, az üzemeltető által alkotott rendszer érdekeinek összehangolását szolgálja; a biztonsági szempontok elsődlegessége mellett, e közösség által kialakított működési rendet rögzíti. A szabályzat módosítását, korszerűsítését a közösség bármely tagja meghatározott eljárási rend szerint javasolhatja.

A szabályzat célja, hogy meghatározza és szabályozza az együttműködő felek – hálózatgazda, üzemeltetők, felhasználók, külső szolgáltatók – kapcsolatát a szolgáltatás működtetésének teljes időtartamára, az együttműködés kezdetétől annak lezárásáig.

A szabályozás további célja, hogy a kapcsolatok, interakciók alapjául szolgáló folyamatokat, felelősségi köröket, szerepeket egyértelművé tegye, szükség esetén egységesítse.

Nem ennek a szabályzatnak a tárgya az adatbiztonság és adatvédelem, az EKG eszköz- és vagyonmentésének szabályozása. Szükséges – jelen dokumentum keretein kívül – a biztonsági szabályzat, az EKG informatikai katasztrófaelhárítási terv (Disaster Recovery Plan, DRP) kidolgozása.

Az előző bekezdésben említett szabályozásokhoz, valamint e szabályzat 1. számú függelékben szereplő dokumentumokhoz igazodva a felhasználó szervezeteknek katasztrófaelhárítási tervüket, illetve intézményi működésük folytonossági tervét (Business Continuity Plan, BCP) célszerű aktualizálni, és ezek kialakítása esetén tekintettel kell lenni az EKG normálistól eltérő működési eseteire.

2.1. A szabályzat hatálya

A szabályzat tárgyi hatálya kiterjed minden egyes, az EKG használathoz kapcsolódó, elkülönült szervezetekhez rendelt szerepkör együttműködési folyamataira, a kezdeményező eseménytől a célállapot bekövetkezéséig.

Az egyes érintett szervezetek belső kapcsolódó folyamatait a szervezeteknek saját maguknak kell szabályozni, érvényesítve a szabályzat előírásait.

A szabályzat alanyi hatálya: közvetlenül a felhasználó szervezetekre, illetve a hálózatgazdára terjed ki, közvetve minden további, szabályzatban említett szerepkört ellátó szervezetre, melyet a velük kötött szerződésekkel kell biztosítani (pl. a szabályzat megfelelő pontjaira hivatkozva).

3. Az EKG-n elérhető szolgáltatások

A felhasználók által az EKG-n elérhető szolgáltatások a következő alapvető csoportokba sorolhatók:

Alapszolgáltatások

– EKG kapcsolódási pont – hozzáférés –, IP sávszélesség garantált biztosítása, MPLS VPN létrehozása,
– 24 órás helpdesk (felhasználói támogatás),
– Internetkapcsolat, az intézmény által meghatározott védelmi politikának megfelelően,

– Névfeloldás (Domain Name Service – DNS),
– Levéltovábbítás az internet és az intézmények felé/felől.

Az alapszolgáltatásként definiált szolgáltatások az EKG-hoz kapcsolódó felhasználók számára a kapcsolódás után automatikusan elérhetővé válnak, azonban bizonyos, a felhasználó szervezettől függő különbségek előfordulhatnak.

Egyéb szolgáltatások

– Kapcsolat biztosítása az EU informatikai szolgáltatásaihoz a TESTA hálózaton keresztül,

Az egyéb szolgáltatásokat az intézmények konkrét feladataik végrehajtásához veszik igénybe.

Emelt szintű szolgáltatások

Az emelt szintű szolgáltatások körébe tartozik minden olyan szolgáltatás, amelyet az intézmények szerződéses keretek között, az EKG infrastruktúrájára, alapszolgáltatásaira támaszkodva vesznek igénybe (pl. hangintegráció, videokonferencia stb.).

3.1. Kapcsolódási pont, illetve VPN-létesítés

Az EKG szolgáltatások lényegi és alapvető szolgáltatása olyan kapcsolódási pont biztosítása, amelyen keresztül lehetővé válik az egyes intézményi rendszerek EKG infrastruktúrához való hozzáférése és zárt kommunikációja egymással, valamint az internet irányába.

A kapcsolódás fizikailag (csatornázott E3, STM1, MetroEthernet és ADSL) távközlési szabvány által meghatározott módon történik, de indokolt esetben lehetőség van az ettől való eltérésre is (pl. „sötét üvegszál" használatával).

Az adat-, hang- és egyéb forgalom IP protokoll használatával zajlik.

Az EKG belső kommunikációja MPLS VPN (Multiprotocol Label Switching; Virtual Private Network) technológiával történik, amely az EKG csatlakozási felületétől kezdve meghatározza az útválasztást, és biztosítja a felhasználói virtuális magánhálózatok (intranetek) bizalmasságát, elkülönültségét. E technológia garantálja a felhasználó számára biztosított IP sávszélességet, a hozzáférések kontrollját és a biztonsági irányelvek érvényesülését. Ennek segítségével zárt virtuális intraneteket lehet létrehozni, amelyeket általánosságban a hálózatgazda működtet, de a felhasználó (illetve egy kijelölt feladatgazda) adminisztrálhat (jogosultságkezelés).

A kapcsolódás fő paraméterei: a sávszélesség (általában 0,25–100 Mbps/intézmény), a közös VPN-ben részt vevők száma, jogosultságai, valamint a kapcsolódási pont(ok) helye. Az EKG működtetője által az adott paraméterek szerint konfigurált VPN a felhasználói körön kívül eső felhasználók számára közvetlenül nem elérhető, biztonságos kapcsolatot valósít meg. A VPN-ek bizalmasságát az önálló biztonsági irányelvek (az egyes határ-útválasztókon beállított MPLS VPN szabályrendszerek) jellemzik.

A kapcsolódás vidéki és egyes fővárosi felhasználók esetén ráhordó (nem az EKG üzemeltetője által működtetett – jellemzően távközlési szolgáltató által üzemeltetett) hálózat közbeiktatását igényli. A ráhordó hálózat feladata az intézmény és az EKG kapcsolódási pont közötti kapcsolat biztosítása.

3.2. Helpdesk

Az EKG-n keresztüli adatforgalmazás során hibák fordulhatnak elő a felügyelt hálózati aktív és passzív eszközökben. Az EKG felügyeleti rendszere folyamatosan ellenőrzi a hálózati rendelkezésre állást, ezért egy esetleges hibát nagy valószínűséggel a felhasználók észlelése előtt képes felfedni.

A hálózatfelügyelet egy ún. egyablakos helpdesk szolgáltatást biztosít a felhasználók számára szükséges kommunikációs lehetőségként, amelyen keresztül a hálózati működéssel, az egyes igénybe vett szolgáltatások paramétereivel kapcsolatos információkat, problémákat lehet jelezni az üzemeltető felé.

3.3. TESTA hálózatok elérése

A TESTA (Trans-European Services for Telematics between Administrations) hálózat az Európai Unió adminisztrációja és a nemzeti kormányzatok elektronikus, extraneten történő a fogadási pontig titkosított információcseréjét teszi lehetővé. A szolgáltatás igénybevételéhez a felhasználó intézménynek kiépített kapcsolattal kell rendelkeznie az EKG-hoz, mivel a TESTA kapcsolat csak az EKG-n keresztül hozható létre.

A TESTA hálózathoz való kapcsolódáshoz az Európai Unió IDA-TESTA szervezete biztonsági szempontból rendszeresen auditálja az EKG-t. A TESTA hálózat és az EKG között a TESTA szolgáltató bérelt vonali összeköttetéseket hozott létre, amelynek mindkét végén a vonali adatforgalmat titkosító kódoló eszközt helyeztek el. A kódoló eszközöket a TESTA szolgáltató telepítette az EKG központban.

Az így kiépült csatornát EU adminisztráció menedzseli és finanszírozza az EKG és a TESTA hálózat között. Ezen a kapcsolaton keresztül – más nemzeti hálózatokhoz hasonlóan –, az EKG is részévé válik az ún. európai informatikai rendszernek – az euro-domainnek.

3.4. Internet-hozzáférés

Az EKG-hoz csatlakozott felhasználók – kapcsolódási pontjukon keresztüli – internethez való hozzáférése jellemzően kétféle lehet, a felhasználó csoportjától függően:

– az adott sávszélesség engedte kereteken belül korlátlan hozzáférés (a kötelezettek esetén),

– egyes protokollokra vonatkozóan átmenetileg korlátozott hozzáférés (a nem kötelezettek esetén).

A korlátlan hozzáférés azoknak a felhasználóknak áll rendelkezésre, amelyek kapcsolódását az EKG-hoz jogszabályi kötelezettség írja elő. Mivel számukra nincsen választási lehetőség az EKG-használatot (és így az internetelérést) illetően, teljes forgalmuk az EKG-n keresztül bonyolódik, korlátozás nélkül.

Átmenetileg korlátozott internet-hozzáférés egyes protokollok vonatkozásában: ilyen internet eléréssel rendelkeznek azok a felhasználók, amelyek kapcsolódása az EKG-hoz nem kötelező jellegű. Számukra a tevékenységükhöz szükséges, illetve általános célú (pl. híroldalak stb.) internetforgalom mindenkor korlátlanul engedélyezett, ugyanakkor – átmenetileg – a nagy sávszélesség-igényű tartalmak (pl. real audio, real video, ftp típusú letöltések) forgalma (a terhelés kezelhető szinten tartása érdekében) mindaddig alacsonyabb szinten priorizált. A korlátozást kizárólag a hálózatgazda jogait gyakorló vezető rendelheti el.

3.5. DNS (Domain Name Service)

A DNS az EKG azon szolgáltatása, amely minden csatlakozott felhasználó számára domain-nevet, cím- és névfeloldást biztosít. A domain-név a felhasználó Internet Protokoll (IP) címének felel meg, annak egyfajta lefordított, szöveges megfelelője.

E szolgáltatáshoz kapcsolódóan kapnak a csatlakozó felhasználók saját IP-címet is, de kizárólag arra a hálózati pontra vonatkozólag (lehet ez az EKG csatlakozási pont vagy egy Web-szerver stb.), amelynek „láthatónak" kell lennie a többi felhasználó számára. Az IP címekkel kapcsolatos allokációs és regisztrációs feladatokat az EKG hálózatgazda végzi. Az EKG üzemeltetés kezeli a gov.hu zónát, így ezen aldomain alatt bármilyen közfeladatot ellátó szervezet számára egyszerűen és gyorsan – külön költségek nélkül – kialakítható a szükséges név és zóna.

3.6. Kormányzati levelezőrendszer

A kormányzati levelezőrendszer a kormányzati és központi közigazgatási szervek számára biztosított levelezőszolgáltatás. A szolgáltatáshoz a kormányzati szervek minden egyéni felhasználója hozzáfér, és a rendszer rendeltetése szerint egymással ezen keresztül végzi levelezését.

3.7. Levéltovábbítás

A levéltovábbítás szolgáltatás olyan hálózati alapszolgáltatás, amely azt biztosítja, hogy a felhasználók az EKG-n kívülről érkező levelei transzparens módon, biztosan eljussanak a címzetthez.

3.8. Hosting

A hosting szolgáltatás lényege, hogy az EKG üzemeltetője igény szerint felvállalhatja a csatlakozott intézmény szervereinek üzemeltetését az EKG központjaiban az EKG egységes infrastruktúráján. A központban rendelkezésre álló nagyobb sávszélesség miatt az üzemeltetett szerver elérhetősége, szolgáltatásminősége javul, az intézmény és az EKG-hez közvetlenül vagy közvetve kapcsolódó külvilág (felhasználó) között.

A szolgáltatás olyan, főként ráhordó hálózaton keresztül csatlakozott felhasználók számára előnyös, amelyek esetében a szerver eredeti üzemeltetési helyén rendelkezésre álló sávszélesség lényegesen kisebb, mint amit a központban biztosítani lehet. A szolgáltatás az EKG üzemeltetés fizikai lehetőségei függvényében, megállapodás alapján áll rendelkezésre.

4. Szerepkörök az EKG szolgáltatásban

4.1. Felhasználó

A felhasználókat a következő csoportok alkotják:

4.1.1. Jogszabály által csatlakozásra kötelezettek

A központi államigazgatási szervek, kormányhivatalok csatlakozásra kötelezettek, kivéve a jogszabályban tételesen felsorolt hálózatokat (pl. a Magyar Honvédség hálózata és egyéb katonai hálózatok).

A csatlakozásra kötelezettek hálózatai egy vagy több ponton kapcsolódnak az EKG-hoz és egymással, illetve a külvilággal hálózati kapcsolatuk az EKG-n keresztül valósulhat meg.

A felhasználók csoportja – általában azonos központi államigazgatási szerv felügyelete alá tartozó szervezetek – együttesen is kapcsolódhat az EKG-ra.

4.1.2. Csatlakozásra nem kötelezett, közpénzből, közfeladatot ellátó szervezetek

Az ebbe a csoportba tartozó szervek – lásd egyéb, a 4.1.1. pontban fel nem sorolt állami költségvetési szervek, köztestületek, helyi önkormányzatok – EKG-hoz való csatlakozása nem jogszabályi kötelezettség, azonban – állami szerepük és feladataik miatt – csatlakozásuk célszerű. Ilyen szervezetek például:

– Országgyűlés,
– Köztársasági Elnök Hivatala,
– Országgyűlési Biztosok Hivatala,
– Bíróságok,
– Ügyészségek,
– Helyi önkormányzatok,
– Állami Számvevőszék.

Az EKG koncepciója szerint megfogalmazott cél, hogy ezek a szervezetek saját döntésük alapján csatlakozzanak az EKG-hoz. Ennek eredményeként a közigazgatással összefüggő állami feladatokhoz kapcsolódó adatcsere egységesen az EKG alkalmazásával fog lebonyolódni.

4.1.3. Csatlakozásra nem jogosult szervezetek

Nem lehet az EKG felhasználója vállalkozás és civil szervezet, kivéve azon vállalkozást, mely az EKG-t használó intézmények vagy a központi elektronikus szolgáltató rendszert használó ügyfelek számára nyújt szolgáltatást, illetve azok szolgáltatásainak lebonyolításában vesz részt. Ebben az esetben is csak e szolgáltatások megvalósítását szolgálóan. Az ilyen, kivételként felsorolt szolgáltató nem veheti igénybe az EKG előzőekben megállapítottakon túli egyéb szolgáltatásait.

Az internetfelhasználók és más hálózatokon keresztül kommunikálók egy megfelelően védett csatlakozási ponton keresztül vehetik igénybe az EKG-ból kifele irányuló szolgáltatásokat, illetve ugyanott tarthatnak kapcsolatot az EKG által ellátottakkal.

4.2. Hálózatgazda

Az EKG hálózatgazdája a közigazgatási informatikáért felelős miniszter. A hálózatgazda feladatait, felelősségét az 50/1998. (III. 27.) Korm. rendelet általánosságban szabályozza, alapvető felelősség az EKG üzembiztos működtetése. Az EKG-val kapcsolatos folyamatokból adódó konkrét felelősségeket jelen szabályzat részletezi. A hálózatgazdai feladatok ellátását az infokommunikációért felelős kormánybiztos segíti, munkamegosztásukat a Miniszterelnöki Hivatal Szervezeti és Működési Szabályzatáról szóló miniszterelnöki utasítás rögzíti. A 276/2006. (XII. 23.) Korm. rendelet 14. §-a alapján az EKG működtetésével kapcsolatos feladatokat a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala látja el.

4.3. Üzemeltető

Az EKG üzemeltetői szerepkörét ellátó szervezetnek alapfeladata a hálózat üzemeltetése, folyamatos szolgáltatásainak biztosítása. Ezen belül fő feladatai:

– Helpdesk szolgáltatás nyújtása,
– A rendszerek működésének folyamatos felügyelete, monitorozása, riportolása,
– Az eszközök karbantartása,
– Hibák javítása,
– A rendszerek konfigurálása,
– Mentések és elemzések készítése,
– Az intézmények hálózatinformatikai támogatása,
– ISP tevékenység ellátása az EKG IP publikus IP címeinek biztosítása tekintetében,
– Műszaki nyilvántartások, dokumentációk naprakész vezetése,
– Eszköznyilvántartás,
– Fejlesztési javaslatok készítése.

Az üzemeltető feladatait elsősorban a hálózatgazdával kötött szerződés szabályozza, de az EKG-val kapcsolatos folyamatokból adódó konkrét felelősségét jelen szabályzat dokumentálja.

4.4. Ráhordó hálózati szolgáltató

Az ún. ráhordó hálózati szolgáltató az EKG csatlakozási pont és a csatlakozó intézmény közötti kapcsolatot szolgáltatja, amennyiben az adott intézmény nem rendelkezik közvetlen (fizikailag az adott intézmény telephelyén kiépített) hozzáférési ponttal. A ráhordó hálózati szolgáltatást az EKG-hoz kapcsolódó intézmény – amennyiben létezik ilyen hatályos szerződés – a hálózatgazda által, az Országgyűlés Nemzetbiztonsági Bizottságának engedélye alapján lefolytatott eljárás eredményeként megkötött keretszerződés terhére rendelheti meg. Amennyiben nincs érvényes

keretszerződés, úgy a beszerzést egyenként a Nemzetbiztonsági Bizottságtól kért engedély alapján a 143/2004. (IV. 29.) Korm. rendelet szerinti követelményeknek megfelelő piaci szereplőktől lehet lebonyolítani.

4.5. A területi elosztó telephelyet szolgáltató

Az EKG területi csomópontjainak üzemeltetési feltételét biztosító Magyar Államkincstár feladatköre és felelőssége csupán a végpont eszközeinek elhelyezésére és az alapvető üzemeltetési feltételek (energia, hőmérséklet, őrzésvédelem) szolgáltatására terjed ki, melyet a MeH és a Magyar Államkincstár között megkötött megállapodás szabályoz.

4.6. EU adminisztrációs tartalomszolgáltató

A magyar EKG felhasználóknak az Európai Unióval történő együttműködés során szüksége lehet elektronikus kommunikációra, adatcserére. Az EU adminisztrációs tartalomszolgáltató az a partner intézmény, amely a feladathoz kapcsolódóan a magyar EKG felhasználókkal együttműködik, azoknak adatot küld, illetve tőlük adatot fogad.

4.7. TESTA hálózat

Az Európai Unió a tagországokkal egy európai szintű elektronikus hálózatot alakított ki, amely közöttes hálózatként összeköti az egyes európai nemzeti (kormányzati) hálózatokat. Amennyiben egy nemzeti felhasználó intézménynek feladatához kapcsolódóan adatcserére van szüksége valamelyik, az európai adminisztrációhoz tartozó intézménnyel, az EKG-n keresztül kapcsolódhat e hálózathoz.

Az EuroDomain hálózat adminisztrációját az Európai Unió IDABC nevű kezdeményezése látja el, míg a hálózatok csatlakoztatásának technikai megvalósításáért az IDABC-TESTA (TransEuropean Services for Telematics between Administrations) szervezet a felelős.

4.8. Külső hálózatok szolgáltatói

Külső távközlési hálózatok, illetve egyéb – a felhasználókat tekintve – nyílt hálózatok is csatlakozhatnak az EKG-hoz. A külső (nem kormányzati) hálózatok csatlakozása egy védett ponton valósul meg.

5. A szolgáltatások szabályozása

A szabályzat az elkülönült szervezetekhez rendelt szerepkörök együttműködési folyamatainak – a kezdeményező eseménytől, a célállapot bekövetkezéséig terjedő – megvalósítását írja elő. Az egyes érintett szervezetek belső, kapcsolódó folyamatait a szervezeteknek saját maguknak kell szabályozni, figyelembe véve e szabályzat előírásait. A szabályok alkalmazásának támogatása érdekében a szabályzat tartalmazza azokat a feladatköröket, amelyek szükségesek a folyamatok kezdeményezésére, a folyamatok állapotának követésére.

5.1. Általános szabályok

A szabályozás általános irányelve, hogy a szolgáltatás nyújtásából, illetve igénybevételéből következő jogok és kötelezettségek alapvetően a hálózatgazda szerepkört ellátó intézményt, valamint a felhasználó intézményt, illetve felhasználó intézménycsoport esetén a csoportból nevesített eljáró szervezetet illetik, vagy terhelik. Ezeket a jogokat és kötelezettségeket a felhasználó és hálózatgazda közötti megállapodásnak kell részleteznie, a konkrét helyzetre alkalmaznia (a hatályos szabályzatra hivatkozva).

Az EKG működésének kiemelt szabálya, hogy bármelyik félnek, aki a hálózat „megtámadását" vagy annak sérülésével járó eseményt észlel (ideértve a funkcionalitás bármiféle csökkenését is), azonnal értesítenie kell az üzemeltető helpdesk-jét. Az üzemeltető joga s kötelezettsége a sérülés haladéktalan, bármilyen módon történő elhárítása az üzemképesség megtartásának érdekében. (A lehetséges veszélyforrások részletezésével a biztonsági szabályzat foglalkozik.)

A szabályzat az üzemeltető, illetve a ráhordó hálózatot szolgáltató szervezetre vonatkozó előírásait a hálózatgazda és üzemeltető, illetve a felhasználó és a ráhordó hálózati szolgáltató közötti szerződésnek kell tartalmaznia (a hatályos szabályzatra hivatkozva).

A kapcsolódási és üzemelési folyamatok során keletkező dokumentumok továbbítási módja vonatkozásában a jogkövetkezménnyel járó dokumentumok esetén a felek között hitelesként elfogadott dokumentum az, amelyet faxon vagy hagyományos módon továbbítottak. A felek minden, a szakmai előkészítést szolgáló dokumentumot gyorsítás céljából e-mail útján is eljuttathatnak az érintettekhez, ez azonban az elektronikus iktatás és aláírás bevezetéséig még nem lehet kizárólagos.

Az EKG belső logikája szerinti MPLS VPN technológia ráhordó hálózat esetében is csak az EKG-n belül, a kapcsolódási ponttól érvényes, tehát a köztes szakasz bizalmasságát és egyéb paramétereit az intézménynek kell garantálnia.

Amennyiben egy területen több intézményt azonos ráhordó szolgáltató kapcsol az EKG-hoz, a szolgáltató az EKG felé egy ponton kapcsolódik, azonban az intézmények adatforgalmának elkülönítését a saját hálózatán belül is teljes hosszban is biztosítania kell.

A jogok, kötelezettségek, felelősségek összefoglalását a szabályzat 3. számú függeléke tartalmazza.

A szolgáltatás specifikus szabályozásokkal kapcsolatos szakmai dokumentumok (megvalósíthatósági tanulmány, kivitelezési tervek) tartalmi és formai követelményeit a szabályzat nem definiálja.

5.2. Szolgáltatásspecifikus szabályok

Ez a pont szolgáltatásonként a kezdeményezéstől a megszüntetésig alkalmazandó specifikus szabályokat tartalmazza.

A szolgáltatásspecifikus szabályok alkalmazását – a könnyebb és gyorsabb áttekinthetőség érdekében – a dokumentum végén (2. számú függelék – A szabályozott folyamatok) található folyamatábrák is szemléltetik.

5.2.1. Kapcsolat létesítése

A kapcsolat létesítését kérheti egy intézmény önállóan vagy egy intézményi csoport. Egyedi intézményi igény esetén az EKG-hoz való kapcsolódás folyamata, illetve elsősorban annak tervezése és kivitelezése egyszerűbb, mint a csoportos intézményi csatlakozások megvalósítása. Ennek megfelelően a két esetet a szabályozás elkülönülten tárgyalja.

5.2.1.1. Kapcsolat létesítése egyedi igénylő esetén

Egyedi intézményi igénylő EKG-hoz való csatlakozását a hálózatgazdához címzett, EKG csatlakozás létesítését kérő levelével igényelheti.

Amennyiben a hálózatgazda az igénylést befogadja, a csatlakozás elvi jóváhagyásáról küldött tájékoztató levélben köteles tájékoztatni az igénylőt a jóváhagyott sávszélességről, valamint a csatlakozás egyedi feltételeiről.

Az elvi jóváhagyást követően az igénylő intézmény feladata az EKG csatlakozási pont és a felhasználó közötti kapcsolatot biztosító ráhordó hálózati szolgáltató biztosítása (amennyiben az igénylő saját hálózati végpontja az EKG végponttól eltérő pontban található – lásd 4.4 pont).

A hálózatgazda és az igénylő között kötött együttműködési megállapodás előkészítése és megkötésének kezdeményezése a hálózatgazda feladata, aláírására a technikai paraméterek és finanszírozási feltételek egyeztetését követően kerülhet sor. Az egyeztetésben esetenként az üzemeltetőnek is részt kell vennie a hálózatgazda utasítása szerint, szakértőként.

A ráhordó hálózati kapcsolatot a felhasználó számára biztosító szolgáltató (a továbbiakban: ráhordó hálózati szolgáltató) és a felhasználó közötti kapcsolatot szabályozó szolgáltatási szerződés – az együttműködési megállapodással összhangban – megkötése az igénylő felelőssége.

A ráhordó hálózati szolgáltatóval szemben követelmény, hogy amennyiben az EKG megyei központjához több intézmény kíván kapcsolódni (nem feltétlenül csoportosan), a központ oldalán csak egy kapcsolódási pontot alakítson ki, a forgalom összesítését pedig saját hálózatán belül oldja meg az informatikai függetlenség biztosításával együtt (aggregált kapcsolódás).

A megvalósítás feladatainak egy része (a kapcsolat feltételeinek biztosítása) a felhasználót, illetve a vele együttműködő ráhordó hálózati szolgáltatót terheli – a ráhordó hálózat fizikai hozzákapcsolása az EKG-hoz (azaz a kapcsolódási ponton található EKG hálózati eszközhöz való csatlakoztatás, bekötés, tesztelés) a felhasználó felelőssége.

Amennyiben a csatlakozás megtörtént, a felhasználó köteles értesíteni a hálózatgazdát. Ezt követően a hálózatgazda utasítja az üzemeltetőt az EKG oldali feladatok végrehajtására. Az üzemeltetőnek aktivizálnia kell a kapcsolatot a konfigurálási feladatok elvégzésével, valamint az intézményi IP-címek kiosztásával.

A szabályozott folyamatot a 2. számú függelék 1.1. folyamatábrája szemlélteti.

5.2.1.2. Kapcsolat létesítése csoportos igénylés esetén

Új EKG kapcsolódást igénylő intézménycsoport kapcsolódásának megvalósítását az intézménycsoport felügyeleti vagy szakmai irányítási jogokat gyakorló szervének kell kezdeményeznie.

A kezdeményező szervezet (a továbbiakban: igénylő) a hálózatgazdához címzett levelével igényelheti a kapcsolatok létesítését.

Amennyiben az igénylő nem rendelkezik a csatlakozási igény összeállításához szükséges EKG-specifikus technikai ismeretekkel, tájékoztatást kérő levelet küldhet a hálózatgazdának, megjelölve a témafelelős kapcsolattartót.

A hálózatgazda feladata a tájékoztatás, illetve csatlakozást kérő igényének elvi jóváhagyása. A hálózatgazda erről köteles levélben tájékoztatni az igénylőt. A hálózatgazda felkéri az üzemeltetőt az igénylővel történő egyeztetésre. Az egyeztetés időpontjának – a levélben meghatározott egyeztetési határidővel összhangban történő – kijelölése és az egyeztetésben érintett felhasználó(k) tájékoztatása az üzemeltető feladata.

Az egyeztetést alapvetően az üzemeltető és az igénylő, és esetenként a felhasználó intézménycsoport kijelölt szakmailag kompetens, szakmai kérdésekben döntési jogkörrel felruházott képviselői részvétele mellett kell

lefolytatni a hálózatgazda képviselőjének részvételével, azonban a felhasználók az egyeztetésbe bevonhatják az érintett ráhordó hálózati szolgáltató(k) képviselőit is.

Az egyeztetés célja az EKG csatlakozás kivitelezéséhez szükséges műszaki megvalósítási és ütemtervek kidolgozása, egyeztetése. A kivitelezés tervezése csatlakozó intézménycsoport esetében egy-egy

– részletes műszaki megvalósítási terv,
– közös (felhasználó és üzemeltető oldali feladatokat együttesen és felső szinten tartalmazó) ütemterv, valamint
– csatlakozási pontonként egy-egy felhasználói ütemterv

kidolgozását kell, hogy magába foglalja.

A ráhordó hálózatok műszaki megvalósításával kapcsolatos feladatok ütemezését tartalmazó felhasználói ütemtervek kidolgoztatása az igénylő feladata. (Ebben a tevékenységben együttműködnek vele a ráhordó hálózati összeköttetés biztosítására kiválasztott szolgáltatók is.) A felhasználói ütemtervek üzemeltetővel történő véleményeztetése és elfogadtatása szintén az igénylők feladata.

A részletes EKG-oldali kivitelezési tervek kidolgozásának és egyeztetésének felelőse az üzemeltető, és a kidolgozott terveknek minden esetben meg kell felelniük a hálózatgazda által meghatározott, műszaki, megvalósítási és ütemtervek kidolgozására vonatkozó tartalmi és formai követelményeknek.

Az üzemeltető a kivitelezési terveket köteles véleményezésre megküldeni a hálózatgazdának, aki a meghatározott formai és tartalmi követelményeknek való megfelelés vizsgálatát követően dönt azok elfogadásáról.

A tervek elfogadását követően – az igénylő közreműködése mellett – a hálózatgazda feladata létrehozni az együttműködési megállapodást a felhasználókkal, az egyeztetett követelményeknek és ütemezésnek megfelelő feltételekkel.

A hálózatgazda feladata továbbá a kiviteli tervekkel összhangban a szükséges EKG oldali fogadókészség biztosítása. Ebbe a feladatba a hálózatgazda – a szükséges mértékben – bevonhatja az üzemeltetőt is.

A felhasználók feladata, hogy az együttműködési megállapodás aláírását követően megkössék a ráhordó hálózati szolgáltatókkal a ráhordó hálózati szolgáltatás igénybevételéről szóló – előzetesen, a tervezési folyamat során előkészített – szolgáltatási szerződést.

A létesítés kivitelezése során az alábbiakat kell betartani:

– a felhasználók hozzák létre a műszaki tervnek megfelelő, a hálózatra csatlakoztatható megoldást,
– a felhasználók csatlakoztatják ráhordó hálózatukat az üzemeltető által csatlakozási célból a felhasználók rendelkezésére bocsátott eszközökhöz és tesztelik a kapcsolatot,
– a felhasználók megszüntetik EKG-ra csatlakozó hálózatának azon összeköttetéseit, amelyeknek használatát az EKG biztonsági szabályzata nem tesz lehetővé,
– az üzemeltető végrehajtja a tervezett működésnek megfelelő konfigurálást.

A szabályozott folyamatot a 2. számú függelék 1.2. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó (csoportos esetben igénylő):

Jogok:

– EKG-kapcsolat igénylése, tájékoztatás kérése.

Feladatok, felelősségek:

– Csatlakozás létesítésének kezdeményezése;
– Részvétel kivitelezési egyeztetéseken;
– Az üzemeltetővel folytatott egyeztetések alapján felhasználói ütemtervek kidolgozása;
– Együttműködési megállapodás megkötése;
– Ráhordó hálózati szolgáltatás igénybevételéről szóló szolgáltatási szerződés megkötése.

Hálózatgazda:

Jogok:

– Döntés a csatlakozási igényről (kötelezettek esetében a csatlakozási paraméterekről);
– Az üzemeltető utasítása a csatlakozás előkészítési, megvalósítási feladatainak elvégzésére.

Feladatok, felelősségek:

– Csatlakozási igény jogosultságának vizsgálata;
– A felhasználó tájékoztatása a csatlakozás lehetőségeiről, technikai paraméterekről – tájékoztató levél küldése;
– Az üzemeltető felkérése egyeztetésen való részvételre – amennyiben a technológiai kérdések szükségessé teszik;
– Az üzemeltető utasítása szükség esetén a kivitelezés megtervezését célzó egyeztetésekre;
– Kiviteli tervek véleményezése, jóváhagyása, vagy módosításuk kezdeményezése;

– A kiviteli tervekkel összehangolt együttműködési megállapodás megkötése a felhasználóval.

Üzemeltető:

Jogok:

– Szakmai tanácsadás a felhasználók számára;
– Javaslattétel a hálózatgazdának a szükséges eszközbeszerzésekre.

Kötelességek:

– A felhasználóval, igénylővel való technikai egyeztetés – a hálózatgazda felkérésére;
– Részvétel a kivitelezés részletes tervezésében és a tervezéssel kapcsolatos egyeztetésben – a hálózatgazda felkérésére;
– Felhasználói ütemtervek véleményezése;
– Kiviteli tervek véleményezése és jóváhagyásra felterjesztése a hálózatgazdának;
– Az EKG hatókörébe tartozó konfigurációs feladatok végrehajtása.

Dokumentumok adattartalma:

CSATLAKOZÁST IGÉNYLŐ LEVÉL	
Adat megnevezése	Jelentése
Azonosító adatok	Az igénylő(k) adatai, az igénylés indításának dátuma. Kapcsolati felelős és elérhetősége.
Előzetes információk	Az igénylést megelőzően folytatott tárgyalások, levelezések hivatkozásai.
Műszaki adatok	Az igényelt kapcsolat műszaki jellemzői és az igénylő jelenlegi jellemző, az EKG szempontjából releváns műszaki környezete.

EGYÜTTMŰKÖDÉSI MEGÁLLAPODÁS	
Adat megnevezése	Jelentése
Általános adatok	– Megállapodó partnerek azonosító adatai. – Kapcsolati felelős neve és elérhetősége. – Általános szerződéses adatelemek.
Előzmény	Az előzményként hivatkozott igény és jóváhagyás adatai.
Szolgáltatás jellemzői	– A szolgáltatás műszaki jellemzői (sávszélesség, teljesítmény stb.) és műszaki környezete, feltételei, valamint díjazása. – A szolgáltatás időbelisége (igénybevételének kezdete, várható időtartama stb.). – Támogatás és helpdesk szolgáltatás feltételei. – Karbantartási rendelkezések. – Egyes hálózati kapcsolatok megszüntetésére vonatkozó megállapítások.

FELKÉRÉS AZ ÜZEMELTETŐ FELÉ	
Adat megnevezése	Jelentése
Tárgy	A feladat rövid megfogalmazása, címe.
A feladat leírása	Az elvégzendő feladat – adott csatlakozás kiépítése – műszaki leírása, tervezett ütemezése.
Határidő	A lebonyolítás határideje.

TÁJÉKOZTATÓ LEVÉL	
Adat megnevezése	Jelentése
Előzmény dokumentumok	– Igénylés azonosítói. – Üzemeltetői állásfoglalás azonosítója. – Hivatkozott adatforgalmi kimutatás azonosítója.
Döntés eredménye	– Elutasítás esetén: az elutasítás indoklása. – Igény jóváhagyása esetén: = a jóváhagyott paraméterek, szolgáltatások leírása, = együttműködési megállapodás minta szerint.

MŰSZAKI MEGVALÓSÍTÁSI TERV	
Adat megnevezése	Jelentése
Műszaki megvalósítási terv	Az EKG minőségügyi rendszere szerint.
Megvalósítási ütemterv	Az EKG minőségügyi rendszere szerint.
Felhasználói ütemterv	Az EKG minőségügyi rendszere szerint.

5.2.2. Változási kérelem

Az EKG felhasználóinak – intézményi feladataik, illetve kapcsolódó technikai lehetőségeik, igényeik változásából adódóan – joguk van az EKG-n keresztül elérhető szolgáltatásokat, pl. a sávszélességet illető változtatást igényelni a hálózatgazdától.

A változást a hálózatgazdához eljuttatott változást igénylő levélben kell kezdeményezni. Változási igény esetén a felhasználó dokumentumban (írásban, ideértve az elektronikus dokumentumot is) specifikálja igényeit, illetve az igényelt módosítás paramétereit. A hálózatgazda a változtatási igény teljesítéséről esetleges módosításáról vagy elutasításáról folyamatos egyeztetést végez az igénylővel, amely alapján a hálózatgazda képes megismerni a változtatási igény okát és megítélni annak indokoltságát.

Sávszélesség-módosítási igény esetén – a sávszélesség módosítására vonatkozó igény megalapozása érdekében – minden intézmény jogosult saját intézményi forgalmi adataihoz való hozzáférésre. Az adatok a www.forgalom.ekg.gov.hu honlapon érhetők el, az adatokhoz való hozzáférési jogosultságokat az üzemeltető köteles biztosítani a felhasználók számára. Egy csatlakozó szervezetnél 2 fő számára biztosított a hozzáférés – kizárólag a saját forgalmi adatokhoz.

A változtatási igények kezelése, azok jóváhagyása vagy elutasítása esetén a módosítások megvalósításának kezdeményezése az üzemeltető felé a hálózatgazda feladata.

Amennyiben a felhasználó a számára jelenleg rendelkezésre állónál nagyobb sávszélességet igényel, a hálózatgazda köteles ellenőrizni a műszaki feltételeket, valamint megvizsgálni, hogy az igényelt sávszélesség indokolt-e. A műszaki feltételek teljesülésének vizsgálatához a hálózatgazda kezdeményezheti az üzemeltető bevonását. Az üzemeltető a hálózatgazda utasítására (egyebek mellett) adatforgalmi kimutatást készít, amelyet a hálózatgazda a sávszélesség-bővítés vizsgálatához felhasznál.

Amennyiben a sávszélesség-bővítés iránti igény kielégítését a műszaki adottságok lehetővé teszik és az adatforgalmi adatok (illetve a tervezett újabb alkalmazások) azt alátámasztják, a hálózatgazda jóváhagyja az igénylést.

Sávszélesség-bővítés iránti igény esetén a hálózatgazda döntését a következő szempontok figyelembevételével hozza meg:

– Műszaki feltételek megléte,
– Korábbi időszakra vonatkozó adatforgalmi adatok,
– Kötelező (egy adott államigazgatási szerv által ellátandó) feladat ellátásához van-e szükség a módosításra.

Az EKG-n keresztül elérhető valamelyik kiegészítő szolgáltatás iránti igény esetén a hálózatgazda – amennyiben szükségesnek tartja – utasítja az üzemeltetőt a szolgáltatásigénylés megvalósíthatóságának véleményeztetésére, illetve a technikai paraméterek, erőforrásigény felhasználóval történő egyeztetésére.

Az üzemeltető az egyeztetést követően köteles megküldeni a hálózatgazdának az igénylés műszaki megvalósíthatóságáról szóló véleményét. A hálózatgazda az igény jóváhagyásáról, illetve elutasításáról szóló döntését az üzemeltetői vélemény figyelembevételével, a műszaki megvalósíthatóság alapján hozza meg.

Jóváhagyott (sávszélességre, új szolgáltatásra vonatkozó) igény esetén a hálózatgazda tájékoztatja a felhasználót, és kezdeményezi a felhasználóval korábban kötött megállapodás módosítását, majd egyeztetik és megkötik a módosított szolgáltatásra vonatkozó együttműködési megállapodást.

A módosított megállapodás megkötését követően a hálózatgazda utasítja az üzemeltetőt, hogy hajtsa végre a sávszélesség bővítéséhez, illetve az új szolgáltatás eléréséhez szükséges feladatait.

Amennyiben a tényleges adatforgalom a rendelkezésre álló sávszélesség 75%-át meghaladja, a hálózatgazda köteles sávszélesség-gazdálkodási, illetve szolgáltatásfejlesztési feladatokat kezdeményezni. A sávszélesség-gazdálkodási, illetve szolgáltatásfejlesztési feladatok részletes leírása az 5.2.14. „Sávszélesség-gazdálkodás" és 5.2.10. „Szolgáltatások fejlesztése" pontokban található.

A műszaki megvalósítás tervezésének és végrehajtásának – ennek keretében a felhasználóval folytatott műszaki-technikai egyeztetések, a szolgáltatás változtatásához kapcsolódó EKG infrastruktúra-bővítési és eszközkonfigurálási feladatok lebonyolításának – felelőse az üzemeltető.

A felhasználó köteles képviselőt delegálni a műszaki-technikai egyeztetésekre, és a megvalósítás folyamán együttműködni az üzemeltetővel.

A változási kérelem – elsősorban költségcsökkentési céllal – vonatkozhat szolgáltatások lemondására, illetve a rendelkezésre álló sávszélesség csökkentésére is.

A felhasználó sávszélesség-, illetve szolgáltatásterjedelem csökkentési igényét a hálózatgazdához küldött levelében jelezheti. A hálózatgazda az igény vizsgálatát követően köteles kezdeményezni az együttműködési megállapodás módosítását és a csökkentés kivitelezését.

A szabályozott folyamatot a 2. számú függelék 2. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Szolgáltatások változtatásának igénylése;
– Saját intézményi adatforgalmi adatainak megtekintése;
– Elutasított igény esetén a felülvizsgálat kérése.

Feladatok, felelősségek:

– Szolgáltatások módosítása iránti igény szakszerű specifikálása;
– Részvétel üzemeltetővel folytatott műszaki-technikai egyeztetéseken;
– Együttműködés az üzemeltetővel a megvalósítás tervezésében és végrehajtásában;
– Szükség esetén a ráhordó hálózati szolgáltatásváltozáshoz illeszkedő módosíttatása.

Hálózatgazda:

Jogok:

– A felhasználók adatforgalmi adatainak vizsgálata;
– A változtatási igény elbírálása;
– Az üzemeltető utasítása a szükséges feladatok végrehajtására;
– Módosított együttműködési megállapodás megkötése.

Feladatok, felelősségek:

– Változási kérelem fogadása, a döntéshez szükséges információk gyűjtése, vizsgálata, az igény szakszerű elbírálása;
– A felhasználó tájékoztatása a döntésről;
– Üzemeltetői egyeztetések időben történő kezdeményezése;
– Módosított együttműködési megállapodás megkötése a felhasználóval;
– A kérelem elbírálását követően a szükséges sávszélesség-gazdálkodási, illetve szolgáltatásfejlesztési feladatok kezdeményezése.

Üzemeltető:

Jogok:

– A hálózatgazda által kiadott feladatok ellátása közben felmerülő fejlesztési javaslatok megfogalmazása a hálózatgazda számára.

Feladatok, felelősségek:

– A hálózatgazda által kiadott feladatok ellátása közben felmerülő, az EKG biztonságos működését veszélyeztető tényezők jelentése a hálózatgazdának;
– Adatforgalmi kimutatás összeállítása a hálózatgazda és a felhasználó részére;
– Kiegészítő szolgáltatások műszaki megvalósíthatóságának véleményezése a hálózatgazda utasítására;
– A hálózatgazda utasítására egyeztetés a felhasználóval műszaki-technikai kérdésekben;
– A megvalósítás keretében a felhasználóval folytatott műszaki-technikai egyeztetések és módosított együttműködési megállapodás alapján a szolgáltatás változtatásához kapcsolódó eszközkonfigurálási feladatok lebonyolítása.

Dokumentumok adattartalma:

VÁLTOZÁSI IGÉNY	
Adat megnevezése	Jelentése
Azonosító adatok	Szervezet általános azonosító adatai; kapcsolattartó azonosítását, elérhetőségét biztosító adatok.
Dátum információk	Az igénylés indításának dátuma.
Igény leírása	Az igény adatai.

VÁLTOZÁSI IGÉNY	
Adat megnevezése	Jelentése
A jellemző műszaki adatok	Infrastruktúra- és eszközkonfigurációs specifikáció, az új sávszélesség becsült adatforgalmi jellemzői.
Indoklás	Az igény indoka, különös tekintettel a változást generáló körülményekre.
Határidő	A módosítás kezdetének kért határideje.

ADATFORGALMI KIMUTATÁS	
Adat megnevezése	Jelentése
Azonosító	A kimutatás egyedi azonosítója.
Dátum információk	A kimutatás kiadásának dátuma és a vizsgált időszak.
Felhasználók azonosítója	Egyedi azonosító, név, cím.
Jellemző műszaki adatok	Átlagos forgalom, csúcsterhelések eloszlása (kiemelkedő forgalmú napok, ezeken belül időszakok és időtartamok, meghatározó forgalmi volumenű kapcsolatok).

ÜZEMELTETŐI SZAKVÉLEMÉNY	
Adat megnevezése	Jelentése
Üzemeltetői műszaki információk	– Az igénylő és EKG működési környezetének jelenlegi jellemzői. – A szolgáltatási szint jelenlegi jellemzői és változásai, minősítése.
Javaslatok	– A műszaki környezetre vonatkozó változtatási kérések, javaslatok: Műszaki megvalósíthatóság leírása (kiemelten: erőforrás-szükséglet, ütemezés, a megvalósítás miatti várható EKG-fejlesztés szükséglet, tartalék feltöltési szükséglet várható-e). – A szolgáltatás várható jellemzői. – Döntési változatok és azok hatása.

TÁJÉKOZTATÓ LEVÉL	
Adat megnevezése	Jelentése
Előzmény dokumentumok	– Igénylés azonosítói. – Üzemeltetői állásfoglalás azonosítója. – Hivatkozott adatforgalmi kimutatás azonosítója.
Döntés eredménye	– Elutasítás esetén: az elutasítás indoklása. – Igény jóváhagyása esetén: = a jóváhagyott paraméterek, szolgáltatások, = műszaki megvalósíthatóság módjának meghatározása, = a módosítás megvalósítására vonatkozó határidő, = együttműködési megállapodás módosítás tervezet.

5.2.3. Hibabejelentés, hibaelhárítás

Az EKG-n keresztül elérhető szolgáltatások működésében, elérhetőségében keletkezett hibát észlelheti a felhasználó, az üzemeltető és a hálózatgazda is.

Amennyiben a hibát a felhasználó észleli, azt az üzemeltető által működtetett központi helpdesk-nek jelentheti be (az EKG honlapon – www.ekg.gov.hu – közzétett helpdesk elérhetőségnek megfelelően). A bejelentés történhet telefonon és e-mailben is, de azt minden esetben meg kell erősíteni egy, a hiba leírását tartalmazó bejelentő fax-szal is. Van lehetőség a hibajelzés beküldésére hivatali kapun keresztül elektronikus űrlapon is, akkor nincs szükség külön megerősítésre, ha olyan személy küldi be, akit előzetesen a helpdesk-nél a szervezet jogosultként bejelentett.

A helpdesk a bejelentést hibajegyen dokumentálja – amit a bejelentés megérkezésétől számított 15 percen belül meg kell nyitni –, majd haladéktalanul átadja az üzemeltető illetékes szervezeti egységének (a továbbiakban: üzemeltető), amely megkezdi a hiba okának feltárását és a hiba elhárítását.

Amennyiben a tapasztalt hiba a TESTA kapcsolathoz köthető, a helpdesk a hiba feltárását követően az európai szolgáltató megfelelő szakembereihez továbbítja a hibát.

Az üzemeltető a saját tevékenysége során észlelt, vagy a felhasználók által jelzett hibákról, a hiba okáról, a várható elhárítási folyamatról a hiba regisztrálását követően köteles tájékoztatni a hálózatgazdát.

Az üzemeltető hibaelhárítási tevékenységéről köteles havi összefoglaló jelentésében is tájékoztatni a hálózatgazdát az elhárított és megoldásra váró hibákról, problémákról.

Az üzemeltető által az EKG közvetett szolgáltatói (ráhordó hálózati szolgáltatók, TESTA hálózatgazda stb.) által felügyelt rendszerkomponensekben, illetve hálózati hibák észlelése esetén, vagy ha a felhasználók, illetve a hálózatgazda ezekről az eszközökről jelent hibát, akkor azt köteles tovább jelenteni az érintett szolgáltatónak a hibajegy megküldésével.

Az üzemeltető több felhasználói csoportot, illetve az EKG jelentős részét vagy egészét érintő hiba esetén köteles haladéktalanul tájékoztatni a hálózatgazdát, valamint köteles intézkedni a felhasználók tájékoztatása érdekében és a hibák elhárítására.

A hálózatgazda kritikus erőforrásokat érintő probléma esetén kezdeményezheti az üzemeltető felé a normál működéstől való eltérés kezelését, a biztonsági szabályzatban meghatározott módon.

Nem kritikus, de a munkavégzést hosszú távon várhatóan hátráltató (pl. koncepcionális) hiba esetén a hálózatgazdának haladéktalanul kezdeményeznie kell a probléma megoldására irányuló EKG fejlesztést (az EKG fejlesztésére vonatkozó előírások szerint).

Az üzemeltető az üzemeltetői szerződésben meghatározott időn belül köteles megkezdeni a hiba megszüntetését. A hiba okáról, a hiba elhárításának várható határidejéről, a hibajavítás folyamatáról, illetve a felhasználó szükséges közreműködéséről a kapcsolatfelvételt követően a hibajegy egyedi azonosítójának (sorszám) megküldésével együtt az üzemeltető köteles tájékoztatni a hibabejelentőt.

Amennyiben a hiba elhárítása nem igényel speciális szakértelmet – tehát a felhasználó által is elhárítható – az üzemeltető egyezteti a hibakezelés módját a felhasználó képviselőjével, aki saját hatáskörben köteles gondoskodni annak elhárításáról.

Ha a hiba elhárítása meghaladja a felhasználók ismereteit, az üzemeltető köteles a helyszínen vagy távoli eszközmenedzsment segítségével helyreállítani a normál működést.

Amennyiben a hibaelhárítás valamely tartalék eszköz felhasználását igényli – és a hibaelhárítási tevékenység eredményeképpen a tartalék eszközkészlet az eszközgazdálkodási irányelvek szerinti ún. kritikus szint alá csökken –, az üzemeltető köteles kezdeményezni a tartalék eszközkészlet feltöltésére irányuló közbeszerzési folyamat hálózatgazda általi megindítását.

A tartalék eszközszállítók kiválasztásának és az eszközök beszerzésének felelőse a hálózatgazda.

Az eszközök átvétele, elhelyezése és tárolása a hálózatgazda kezdeményezése alapján az üzemeltető feladata. Az üzemeltető a hibajavítás, üzemeltetési, karbantartási feladatok ellátása során az eszközökkel szabadon rendelkezik, illetve azok felhasználásáról pontos nyilvántartást vezet.

A szabályozott folyamatot a 2. számú függelék 3. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– EKG-val kapcsolatos hiba elhárításának igénylése;
– Tájékozódás a hibaelhárítás menetéről, a hibaelhárítás határidejéről.

Feladatok, felelősségek:

– Az EKG működésével kapcsolatos észlelt probléma bejelentése, a probléma leírása;
– Saját eszközök hibáinak elhárítása;
– Az EKG eszközök csatlakozási hibáinak elhárítása az üzemeltető irányításával;
– Visszajelzés az üzemeltetőnek az elhárított hibáról.

Hálózatgazda:

Jogok:

– Tájékozódás a hibákról, azok elhárításáról, a megoldásra váró hibákról, esetenként és havi összesítő jelentés alapján;
– Kritikus erőforrásokat érintő hiba esetén a normál működéstől való eltérés kezelése;
– Koncepcionális hiba esetén a várható probléma megelőzésére vonatkozó EKG fejlesztés kezdeményezése;
– A tartalék eszközfelhasználás, az erről készített nyilvántartás ellenőrzése.

Feladatok, felelősségek:

– A hibaelhárítási tevékenység folyamatos figyelemmel kísérése (monitoring), a vonatkozó jelentések vizsgálata;
– A tartalék eszközkészlet feltöltésére irányuló közbeszerzési eljárás megindítása – az üzemeltető kezdeményezésére.

Üzemeltető:

Jogok:

– EKG fejlesztésére irányuló javaslatok megtétele.

Feladatok, felelősségek:

– Hibabejelentések fogadásáért és a hibaelhárítás kezdeményezéséért felelős helpdesk felállítása és működtetése;
– Felhasználótól, hálózatgazdától érkezett hibabejelentések fogadása, dokumentálása, illetve a saját maga által észlelt hibák dokumentálása;
– Hibajegyek kiállítása, hibajegykezelő rendszer üzemeltetése;
– Hálózatgazda tájékoztatása a hibákról, eseti és havi összesítő jelentés készítése és eljuttatása a hálózatgazdához;
– Az EKG közvetett érintettjei (ráhordó hálózati szolgáltatók, EuroDomain hálózatgazda stb.) által felügyelt rendszerek, hálózatok működésében bekövetkezett, üzemeltető által észlelt hiba esetén hibajegy kiállítása, hibajelentés küldése az érintett szolgáltató felé;
– Hiba elhárításának megkezdése az üzemeltetői szerződésben meghatározott időn belül;
– Hibabejelentő tájékoztatása a hiba elhárításának várható határidejéről, a hibajavítás folyamatáról, illetve a felhasználó, esetleg a hálózatgazda szükséges közreműködéséről;
– Felhasználó által elhárítható hiba esetén egyeztetés a felhasználóval a hiba elhárításáról, szakmai irányítás;
– Hibaelhárítás, problémamegoldás folyamatának követése, hibajegy vezetése, lezárása;
– Tartalék eszközkészlet feltöltésének kezdeményezése a hálózatgazda felé;
– Részvétel beérkező tartalék eszközök szállítótól történő átvételében;
– Nyilvántartás vezetése a tartalék eszközök felhasználásáról;
– Felhasználók és hálózatgazda tájékoztatása a hiba elhárításáról.

Dokumentumok adattartalma:

HIBABEJELENTÉS	
Adat megnevezése	Jelentése
Azonosító adatok	A bejelentő azonosító adatai, a bejelentés dátuma.
Leírás	A hiba műszaki leírása, esetleg a jelenséget alátámasztó dokumentumok, az előfordulás gyakorisága.
A hiba minősítése	A hiba súlyosságának, kritikusságának besorolása a hiba adatforgalomra gyakorolt hatása alapján.

HIBAJEGY	
Adat megnevezése	Jelentése
Azonosító adatok	A bejelentő azonosító adatai, elérhetősége, a bejelentés dátuma.
Leírás	A hiba műszaki leírása, esetleg a jelenséget alátámasztó dokumentumok, előfordulás gyakorisága.
A hiba minősítése	A hiba súlyosságának, kritikusságának besorolása, adatforgalomra gyakorolt hatás alapján.
Hibakövetés	– A hiba elhárítására vonatkozóan javasolt műszaki megoldás leírása. – A végrehajtás kijelölt felelőse. – A megvalósítás ütemezése: kezdés – befejezés dátuma. – A megvalósítás módja, hibatörténet. – A megvalósítást követően értesítendők listája. – Értesítés kiküldésének dátuma.

HAVI HIBABEJELENTÉS ÖSSZEFOGLALÓ	
Adat megnevezése	Jelentése
Dátum	A jelentésben érintett időszak meghatározása (dátum -tól -ig).
Összefoglaló	A jelentett hibák, hibatípus, felhasználók szerint csoportosítva.
Statisztika	– Összes jelentett hiba, ebből a jelentés időpontjáig elhárított és folyamatban lévő hibák (azaz a nyitott hibajegyek) száma. – A hibabejelentés és a javítás-visszajelentés között átlagosan eltelt idő hibatípusonként. – Átlagos szolgáltatás kiesési idő (hiba miatt). – Szolgáltatási szint alakulása.

5.2.4. Sávszélesség-ellenőrzés, felülvizsgálat

Az EKG használatának alapvető szabálya, hogy minden felhasználó intézmény akkora (de alapvetően nem nagyobb) sávszélességgel rendelkezzen, amekkora feladatainak végrehajtásához szükséges. Ennek biztosítása, az EKG sávszélesség-gazdálkodási feladatainak ellátása a hálózatgazda felelőssége.

A mindenkor megfelelő sávszélesség biztosítása érdekében az üzemeltetőnek – szerepéből adódóan – rendszeresen elemeznie kell a hálózatfelügyeleti rendszer adatforgalmi mérőszámait. Az üzemeltető a forgalom napi szintű elemzésével képes kimutatni, hogy egy felhasználó intézmény hogyan használja ki a rendelkezésre álló sávszélességet. Az üzemeltetőnek a napi szintű adatokból havi összesítést kell készítenie (minden hónap 5. munkanapjáig), amelynek alapján javaslatot fogalmaz meg a hálózatgazda felé arról, hogy vélhetően szükséges-e nagyobb sávszélesség valamely felhasználó tevékenységéhez, vagy kisebb sávszélesség is elegendő lenne.

A hálózatgazda az üzemeltető javaslata alapján – amennyiben a módosítást sávszélesség-gazdálkodás szempontjából indokoltnak tartja – technikai egyeztetést kezdeményez minden egyes érintett a felhasználóval, majd az egyeztetési információk birtokában dönt a szolgáltatási paraméterek változtatásáról.

A felhasználóval történő egyeztetést és döntést követően a hálózatgazda és a felhasználó együtt módosítja a közöttük korábban létrejött együttműködési megállapodást.

A hálózatgazda utasítja az üzemeltetőt a szolgáltatás fizikai paramétereinek módosításáról, aki az együttműködési megállapodásnak megfelelően végrehajtja a hálózati beállítások módosítását, a megállapodásban foglalt határidőre.

Amennyiben a felhasználó valamely ráhordó hálózaton keresztül kapcsolódik az EKG-hoz, a felhasználónak az adott ráhordó hálózati szolgáltatóval is egyeztetnie kell arról, hogy szükséges-e a ráhordó szolgáltatás módosítása. Ezt követően az érintett felek az egyeztetésnek megfelelően módosítják a kettejük között létező ráhordó szolgáltatási szerződést.

A folyamatot a 2. számú függelék 4. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Hálózatgazda:

Felelősségek:

– A rendelkezésre álló EKG sávszélesség gazdaságos és hatékony elosztásának biztosítása, figyelembe véve az EKG mindenkori üzembiztonságát;
– Sávszélességet érintő döntések meghozatala üzemeltetői javaslat alapján és az összfelhasználói érdekeket figyelembe véve, valamint a meghozott döntések érvényesítése az egyes felhasználóknál;
– A felhasználói szolgáltatások és az azokhoz tartozó együttműködési megállapodások összhangjának folyamatos biztosítása;
– Üzemeltető tájékoztatása a módosított együttműködési megállapodásról a szolgáltatásban történt változás esetén.

Üzemeltető:

Felelősségek:

– Az EKG adatforgalmának mérése, havi jelentés és – szükség esetén – sávszélesség módosítási javaslat készítése, megküldése a hálózatgazda részére, minden hónap 5-éig;
– Hálózati beállítások módosítása a szolgáltatásmódosítás esetén, az együttműködési megállapodásnak megfelelően.

Felhasználó:

Felelősségek:

– Együttműködés a hálózatgazdával a szolgáltatások módosítása tekintetében;
– A ráhordó hálózati szolgáltatás (ha létezik) szinkronizálása, annak megvalósíttatása.

Dokumentumok adattartalma:

HAVI ÜZEMELTETŐI JELENTÉS A FELHASZNÁLÓK FORGALMÁRÓL	
Adat megnevezése	Jelentése
Dátum	A jelentésben érintett időszak (dátum -tól -ig).
Statisztika	– Átlagos, minimális, maximális (csúcsterhelés) adatforgalmi adatok és azok időbeli eloszlása – felhasználónként. – Az adatforgalom – sávszélesség kihasználtsági mutatói, viszonyítva az EKG maximális teljesítményéhez.

ÜZEMELTETŐI JAVASLAT	
Adat megnevezése	Jelentése
Üzemeltetői műszaki információk	– Az EKG működési környezet aktuális jellemzői. – A szolgáltatási szint aktuális jellemzői és várható változások. – A szolgáltatás szintjének értékelése, minősítése.
Javaslatok	– A sávszélesség módosításra vonatkozó műszaki változtatási javaslatok. – A sávszélesség módosításra (növelésre-csökkentésre) javasolt felhasználók köre és a javasolt módosítás mértéke. – A szolgáltatás optimális jövőbeni jellemzői.

EGYÜTTMŰKÖDÉSI MEGÁLLAPODÁS-MÓDOSÍTÁS	
Adat megnevezése	Jelentése
Általános adatok	– Megállapodó partnerek azonosító adatai. – Kapcsolati felelős és elérhetősége. – Általános szerződéses adatelemek módosulása (ha van ilyen).
Előzmény	Az előzményként hivatkozott üzemeltetői javaslat információtartalma és annak elfogadása (az ezt igazoló hivatkozások).
Módosult szolgáltatás jellemzői	– A módosult szolgáltatás műszaki jellemzői (sávszélesség, teljesítmény stb.), környezete és feltételei. – A szolgáltatás időbeli kiterjedése (dátum -tól -ig, ha értelmezhető).

5.2.5. Kapcsolódás megszüntetése

Amennyiben egy adott felhasználó EKG kapcsolata a megváltozó jogszabályi keretekkel ellentmondásba kerül, illetve egy adott – kapcsolódásra nem kötelezett intézmény – funkcionális vagy nem funkcionális igényeit az EKG hálózat nem képes kielégíteni, a felhasználó kérheti a kapcsolat megszüntetését. Az EKG kapcsolat megszüntetésének igényét a felhasználónak – megszüntetési kérelemben – kell jelezni a hálózatgazda felé.

A hálózatgazda a levél kézhezvételét követően egyeztetést kezdeményez a felhasználóval a megszüntetés feltételeiről, lebonyolításáról. Az egyeztetés során a felhasználó és a hálózatgazda tisztázzák a megállapodás megszüntetésének jogi, pénzügyi részleteit.

Szükség esetén a technikai részletek tisztázása érdekében a hálózatgazda utasítja az üzemeltetőt a felhasználóval való egyeztetésre. Az üzemeltető felelőssége hogy a felhasználóval együttműködve kidolgozza a megszüntetés műszaki lebonyolításának és az átállás műszaki megvalósításának ütemezését.

Ebben az esetben a felhasználó és az üzemeltető az egyeztetett határidőkkel összhangban köteles – párhuzamosan futó felkészülési projektek keretében – végrehajtani a kapcsolat megszüntetésére, illetve az átállásra való felkészülés szükséges lépéseit.

A felhasználó kötelessége a felkészülés részeként

– az alternatív hálózati szolgáltató kiválasztása,
– az alternatív hálózati szolgáltatások beszerzése,
– az átállás, az EKG tulajdonban lévő hálózati eszközök, erőforrások kiváltásának részletes tervezése, valamint
– az érintett, hatáskörébe tartozó intézményeknek az átállásra való felkészítése.

Az üzemeltetőnek kell – a felhasználó tevékenységével párhuzamosan – a megszüntetéssel kapcsolatos belső feladatokat elvégezni, így

– az EKG érintettek belső tájékoztatását,
– a megszüntetést követő, a megszüntetéssel járó karbantartási feladatok szervezését,
– a megszüntetést követő változtatásokra való felkészülést megtervezni.

A megszüntetés technikai lebonyolítása az üzemeltető felelőssége, de amennyiben szükséges, a felhasználó köteles együttműködni vele a megszüntetés során, különös tekintettel arra, hogy az átálláskor is érvényesüljenek az EKG biztonsági szabályzat átállásra érvényes szabályai.

Az átállás szerződéses és műszaki feltételeinek megteremtéséről a felhasználó köteles gondoskodni – az alternatív hálózati szolgáltatókkal együttműködésben.

A megszüntetés lebonyolításának utolsó feladataként a hálózatgazda és a felhasználó közös akarattal megszünteti az együttműködési megállapodást.

A felhasználó vagy felhasználói csoport által használt és a kapcsolat megszüntetése miatt felszabaduló sávszélesség további felhasználásáról – annak tartalékolásáról vagy kiosztásáról – a hálózatgazda dönt, sávszélesség-gazdálkodási feladatai keretében.

A szabályozott folyamatot a 2. számú függelék 5. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– EKG kapcsolat megszüntetésének kezdeményezése.

Feladatok, felelősségek:

– Részvétel a megszüntetés feltételeiről, lebonyolításáról, a megállapodás megszüntetésének jogi részleteiről a hálózatgazdával folytatott egyeztetés(ek)en;
– Részvétel a megszüntetés műszaki lebonyolításának ütemezéséről, és az átállás műszaki megvalósításáról és ütemezéséről az üzemeltetővel folytatott egyeztető megbeszélés(ek)en;
– A felkészülés részeként az alternatív hálózati szolgáltató kiválasztása; az alternatív hálózati szolgáltatások beszerzése; az átállás és az EKG tulajdonában lévő hálózati eszközök, erőforrások kiváltásának részletes tervezése; az érintett intézmények átállásra való felkészítése;
– Szükség szerint együttműködés az üzemeltetővel a megszüntetés technikai lebonyolításában;
– Részvétel az EKG együttműködési megállapodás megszüntetésében.

Hálózatgazda:

Jogok:

– Egyeztetések kezdeményezése.

Feladatok, felelősségek:

– Megszüntetési kérelem fogadása, a felhasználóval történő egyeztetés kezdeményezése a megszüntetés feltételeiről, lebonyolításáról, valamint a megállapodás megszüntetésének jogi részleteiről;
– Szükség esetén az üzemeltető utasítása a felhasználóval folytatandó technikai egyeztetések lebonyolítására;
– Az együttműködési megállapodás megszüntetése;
– Sávszélesség-gazdálkodási feladatok keretében döntés a felszabaduló sávszélesség kezeléséről.

Üzemeltető:

Jogok:

– Javaslat adása a felszabaduló sávszélesség kezelésére.

Feladatok, felelősségek:

– Utasítás szerinti egyeztetés a felhasználóval a megszüntetés technikai részleteiről, a megszüntetés és az átállás ütemezésével és lebonyolításával kapcsolatban;
– A megszüntetéssel kapcsolatos felkészülési feladatok keretében az EKG érintettek belső tájékoztatása;
– Szükség esetén a megszüntetést követő változtatásokra való felkészülés tervezése;
– A megszüntetés technikai lebonyolítása a felhasználóval együttműködésben.

Dokumentumok adattartalma:

MEGSZÜNTETÉSI KÉRELEM	
Adat megnevezése	Jelentése
A felhasználó adatai	A felhasználó egyértelmű azonosító adatai, kapcsolattartó felelős és annak elérhetősége.
Dátum adatok	A megszüntetés bejelentésének dátuma, a szolgáltatás megszüntetésének javasolt kezdeti dátuma.
Műszaki leírás	– Előzetes intézkedések, tárgyalások összefoglalása. – A megszüntetés indoklása. – A megszüntetés műszaki megvalósításának leírása. – Az alternatív szolgáltató megjelölése. – Az átálláshoz szükséges üzemeltetői és hálózatgazda közreműködés definiálása.

5.2.6. Adatcsere-kapcsolat létrehozása az EU adminisztrációval

Az EU adatcsere kapcsolati szolgáltatás azokra a felhasználókra vonatkozik, amelyek tevékenységéhez szükség van egyes EU társszervezetek adatbázisaihoz, tartalomszolgáltatásaihoz való hozzáférésre.

A megvalósítás a felhasználók és az EU adminisztrációs tartalomszolgáltatók közötti igénylési-jóváhagyási folyamattal indul. Bármelyik fél kezdeményezheti a kapcsolat kialakítását, mégpedig adatcsere igényük megfogalmazásával és Igénylő levél elküldésével.

A kapcsolat felvétele után az EKG felhasználó és az érintett EU adminisztrációs intézmény között az igényt egyeztetni kell.

Az együttműködés részleteinek egyeztetése után a felek együttműködési megállapodást írnak alá.

Az adatcsere-kapcsolatról való tájékoztatás érdekében az együttműködési megállapodást az EU adminisztrációs partner megküldi az EuroDomain szolgáltatónak és a hálózatgazdának.

Az együttműködési megállapodásban foglaltaknak megfelelően – a hálózatgazda utasítása alapján – az üzemeltető (EKG-oldalon) és az EuroDomain szolgáltató (EU-oldalon) elvégzik a szükséges hálózati beállításokat.

A felhasználó és az EU adminisztrációs partner között ezután használható az EKG-n keresztül megvalósuló összeköttetés.

A folyamatot a 2. számú függelék 6. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Az EU adatcsere-kapcsolat kialakításának kezdeményezése.

Felelősségek:

– Kapcsolatfelvétel az EU adminisztrációs adatkapcsolat vonatkozásában az EU adminisztrációs partnerrel;
– Együttműködési megállapodás kialakítása az EU adminisztrációs partnerrel;
– Az EU adminisztrációs partner felelősségi körébe tartozó feladatok teljesülésének követése, és szükség szerint közreműködés azok végrehajtásában.

EU adminisztrációs partner:

Felelősségek:

– Az érintett EU szolgáltatók értesítése a magyar felhasználó intézmény és az EU adminisztrációs partner közötti együttműködésről – az együttműködési megállapodás megküldésével.

EuroDomain szolgáltató:

Felelősségek:

– Az EuroDomain oldali hálózati paraméterek beállítása, az EKG felhasználó és az EU adminisztrációs partnerintézmény között létrejött együttműködési megállapodás alapján.

Üzemeltető:

Felelősségek:

– Az EKG oldali hálózati paraméterek beállítása – az EKG felhasználó és az EU adminisztrációs partnerintézmény között létrejött együttműködési megállapodás alapján.

Dokumentumok adattartalma:

EU ADATCSERE-KAPCSOLATOT IGÉNYLŐ LEVÉL	
Adat megnevezése	Jelentése
Azonosító adatok	Az igénylő(k) adatai, az igény bejelentésének dátuma. Kapcsolati felelős és elérhetősége
Előzetes információk	Az igénylést megelőzően folytatott tárgyalások, levelezések hivatkozásai, az adatcsere indokoltságát alátámasztó dokumentumok hivatkozásai.
Résztvevők	A tervezett adatcsere-kapcsolatban részt vevő intézmények azonosító adatai.
Műszaki információk	Az adatforgalom tárgya (milyen jellegű adatokra irányul), becsült nagysága, sávszélesség-igénye.

EGYÜTTMŰKÖDÉSI MEGÁLLAPODÁS	
Adat megnevezése	Jelentése
Általános adatok	– Általános szerződéses adatelemek. – Megállapodó partnerek azonosító adatai. – Kapcsolati felelős és elérhetősége.
Előzmény	Az előzmény igény és jóváhagyás adatai.
Szolgáltatás jellemzői	– A szolgáltatás műszaki jellemzői (Az adatcsere tárgya, indokoltsága) és műszaki környezete, feltételei. – A szolgáltatás igénybevételének időbeli kiterjedése. – Támogatás és helpdesk feltételek. – Tartalomfrissítéssel kapcsolatos rendelkezések. – A tartalomszolgáltatás megszüntetésével kapcsolatos megállapítások és megállapodások.

5.2.7. Hosting szolgáltatás igénybevétele

A hosting szolgáltatás igénylését a felhasználó intézmény levélben kezdeményezi a hálózatgazda felé, az üzemeltetendő szerverkapacitás, illetve az arra telepítendő alkalmazás paramétereinek megadásával.

Az igény fogadása után a hálózatgazda felelőssége a felhasználóval folytatott technikai egyeztetés kezdeményezése, amelybe bevonhatja az üzemeltetőt is. Az üzemeltető feladata – szükség esetén – az egyeztetések során a szolgáltatásokhoz kapcsolódó technikai specifikáció elkészítése.

A szolgáltatás megvalósíthatóságáról, az együttműködés létrejöttéről (az alkalmazás telepítéséről és üzemeltetéséről) az egyeztetések alapján a hálózatgazda dönt. Jóváhagyó döntés esetén a hálózatgazda és a felhasználó megköti a hosting szolgáltatás igénybevételére vonatkozó együttműködési megállapodást.

Az együttműködési megállapodás aláírását követően a hálózatgazda utasítja az üzemeltetőt a hosting szolgáltatásban érintett szerverek üzembe helyezésére az EKG valamely területi központjában.

A folyamatot a 2. számú függelék 7. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Hosting szolgáltatás igénybevételének kezdeményezése.

Feladatok, felelősségek:

– Igény megfogalmazása, benyújtása a hálózatgazda felé;
– Hosting szolgáltatás igénybevételével kapcsolatos technikai egyeztetésen való részvétel;
– Az üzemeltetendő alkalmazás telepítése, felhasználó oldalról történő távmenedzselési megoldása;
– Együttműködési megállapodás megkötése a hálózatgazdával.

Hálózatgazda:

Jogok:

– Döntés az igénylésről.

Feladatok, felelősségek:

– Technikai egyeztetés kezdeményezése, lebonyolítása;
– Döntés a szolgáltatás megvalósításáról;
– Együttműködési megállapodás előkészítése és megkötése.

Üzemeltető:

Feladatok, felelősségek:

– A hálózatgazda utasítása szerint részvétel technikai egyeztetésen;
– Hosting szolgáltatás igénybevételével kapcsolatos technikai specifikáció kidolgozása.

Dokumentumok adattartalma:

HOSTING SZOLGÁLTATÁST IGÉNYLŐ LEVÉL	
Adat megnevezése	Jelentése
Azonosító adatok	A felhasználó adatai, az igény benyújtásának dátuma Kapcsolati felelős és elérhetősége.
Előzetes információk	Az igénylést megelőzően folytatott tárgyalások, levelezések hivatkozásai.
Műszaki adatok	– Szerver- és alkalmazás-paraméterek. – Üzemeltetési feltételek, feladatok. – Technikai specifikáció: követelmény specifikáció az elvárt műszaki teljesítményre vonatkozóan.

EGYÜTTMŰKÖDÉSI MEGÁLLAPODÁS	
Adat megnevezése	Jelentése
Általános adatok	– Általános szerződéses adatelemek. – Megállapodó partnerek azonosító adatai. – Kapcsolati felelős és elérhetősége.
Előzmény	Az előzmény igény és jóváhagyott műszaki specifikáció adatai.
Szolgáltatás jellemzői	– A hosting szolgáltatás műszaki jellemzői (szerver és alkalmazás), környezete és feltételei. – A szolgáltatás időbeli kiterjedése (dátum -tól -ig). – Támogatást és helpdesk szolgáltatást érintő feltételek. – Karbantartási rendelkezések. – Megszüntetéssel kapcsolatos megállapítások és megállapodások.

5.2.8. Szabályozások, szabályzatmódosítások bevezetése

Az EKG működését érintő szabályozások – ilyen többek között a használati szabályzat és az EKG biztonsági szabályzat –, valamint szabályzatmódosítások kidolgozása és bevezetése elsősorban a hálózatgazda feladata.

A szabályozások módosításának, új szabályzatok kidolgozásának igényét jellemzően az EKG működésében, szolgáltatásaiban bekövetkezett jelentős változások, illetve jogszabályi változások okozhatják.

A szabályzatok, módosítások az EKG érintettjeinek szükséges mértékű bevonásával készülhetnek, ezért a szabályzatok kidolgozásáért felelős hálózatgazda a szabályzat kidolgozásába, de elsősorban annak véleményezésébe vonja mind az üzemeltetőt, mind a kapcsolódásra kötelezett központi felhasználók szükséges kompetenciával rendelkező képviselőit.

A szabályzatok kidolgozását, módosítását elsősorban a hálózatgazda kezdeményezi, de a hálózatgazda mellett a felhasználóknál vagy az üzemeltetőnél is jelentkezhet olyan szabályzatmódosítási igény, amelynek megvalósítása emeli az EKG szolgáltatásainak színvonalát, vagy megkönnyíti a felek együttműködését. Az utóbbi esetben a felhasználó vagy az üzemeltető megküldi javaslatát a hálózatgazda részére.

A hálózatgazda – a javaslatok alapján – koncepciót dolgoz ki a szabályozás módosításáról, majd azt véleményezésre megküldi az üzemeltetőnek, valamint a központi felhasználók szükséges kompetenciával rendelkező képviselőinek.

Az üzemeltető és a felhasználók képviselői a kért határidőre véleményezik a koncepciót.

A hálózatgazda utasíthatja az üzemeltetőt, hogy működjön közre a szabályozás egyes részterületeinek kidolgozásában a hálózatgazda koncepciója alapján.

A koncepcióra épülő szabályzattervezetet a hálózatgazda egyezteti az érintettek képviselőivel, és az egyeztetés eredménye alapján véglegesíti a szabályzatot.

A véglegesített szabályzat kiadása (kivéve, amikor jogszabályi kihirdetés szükséges) és bevezetése a hálózatgazda feladata. A hálózatgazda a változások kezelésére – szükség esetén – külön tervet készít és hajt végre.

A hálózatgazdának az EKG közvetlen szereplői mellett tájékoztatnia kell az érintett külső szolgáltatókat is az őket közvetlenül érintő változásokról.

A szabályozott folyamatot a 2. számú függelék 8. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– A meglévő szabályozás módosításának vagy új, még nem szabályozott terület szabályozásának kezdeményezése, javaslat formájában.

Felelősségek:

– A hálózatgazda szabályzati vagy szabályzatmódosítási koncepciójának véleményezése;
– Az új vagy módosított szabályzattervezet véleményezése;
– A végleges szabályzat bevezetése.

Hálózatgazda:

Jogok:

– A meglévő szabályozás módosításának kidolgoztatása vagy új, még nem szabályozott terület szabályozása.

Felelősségek:

– A szabályzatmódosítás koncepciójának kidolgozása és annak véleményeztetése az üzemeltetővel és a központi felhasználókkal;
– A szabályzat véglegesítése és (amennyiben nem jogszabályban rögzített) kiadása – az érintettek véleményének figyelembevételével. Jogszabályi szabályozás igénye esetén a közigazgatási előterjesztések általános szabályai érvényesülnek a szakmai előkészítés után.

Üzemeltető:

Jogok:

– A meglévő szabályozás módosításának vagy új, még nem szabályozott terület szabályozásának kezdeményezése.

Felelősségek:

– A hálózatgazda szabályzat vagy szabályzatmódosítási koncepciójának véleményezése;
– Az új vagy módosított szabályzattervezet véleményezése, közreműködés a szabályzat kidolgozásában;
– A végleges szabályzat bevezetése.

Dokumentumok adattartalma:

SZABÁLYZATMÓDOSÍTÁSI JAVASLAT	
Adat megnevezése	Jelentése
Kezdeményező	A szabályzatmódosítást kezdeményező azonosító adatai.
Módosítandó szabályzat javaslat	A módosítás tárgya: – A módosításra javasolt megnevezése. – A javasolt módosítás részletes kifejtése. – A módosítás indoklása.

ÚJ SZABÁLYZAT KONCEPCIÓ	
Adat megnevezése	Jelentése
Megnevezés	A folyamat megnevezése.
Módosító	A hálózatgazda azonosító adatai.
Koncepció	A szabályzat célja: – A folyamat részletes leírása – egységes szerkezetben és összefüggéseiben, a javasolt módosítást követően. – A módosítás várható hatása az EKG működésére.

FELKÉRŐ LEVÉL VÉLEMÉNYEZÉSRE	
Adat megnevezése	Jelentése
Tárgy	A véleményezés tárgya, a szabályzat(ok), folyamat(ok) neve, meghatározása.
Határidő	A véleményezés határideje.
Információk, mellékletek	– A módosított folyamat koncepciója, mint melléklet. – A módosítással kapcsolatos egyéb, járulékos, tisztázó információk.

5.2.9. Szolgáltatások fejlesztése

Az EKG-n keresztül elérhető szolgáltatások EKG-t érintő fejlesztéséért a hálózatgazda felel.

A fejlesztési feladatok származhatnak jogszabályi változásokból, illetve eredhetnek a felhasználóktól, üzemeltetőtől vagy a hálózatgazdától – jellemzően ilyenek a hibalehetőségek kiszűrésére, a szűk keresztmetszetek megszüntetésére irányuló kezdeményezések.

A felhasználók és az üzemeltető a hálózatgazda számára küldi meg fejlesztési javaslatait. A hálózatgazda a beérkezett javaslatok, illetve a jogszabályi változások ismeretében dönt a fejlesztés szükségességéről, és döntésének függvényében megfogalmazza a fejlesztési feladatot.

A fejlesztési feladat megvalósítója – a fejlesztés biztonsági jelentőségétől függően – a hálózatgazda felelős döntése alapján lehet közbeszerzés útján vagy az Országgyűlés illetékes bizottsága közbeszerzést kizáró előzetes döntése alapján a 143/2004. (IV. 29.) Korm. rendelet szabályai szerint kiválasztott vállalkozó. Az üzemeltető a fejlesztések előrehaladásáról folyamatosan, havi jelentések formájában számol be a hálózatgazdának. A rendszer biztonságát befolyásoló fejlesztések esetében minden alkalommal vizsgálat tárgyát kell képezze a beszerzés minősítése.

Komplex fejlesztések esetén a fejlesztési feladat megfogalmazását követően megvalósíthatósági tanulmány készül az üzemeltető, külső szakértők bevonásával. A megfelelő fejlesztési irány kiválasztásáról, a megvalósítás módjáról szóló döntést a hálózatgazda hozza meg.

A döntést követően a kivitelező vállalkozót (szállítót) közbeszerzési, illetve nemzetbiztonsági beszerzési eljárás során választja ki a hálózatgazda. A közbeszerzési eljárásban – szükség esetén a hálózatgazda utasítására – az üzemeltető is részt vesz szakértőként a technikai részletek egyeztetésében.

A hálózatgazda és a vállalkozó (szállító) az egyeztetést követően szerződést köt a fejlesztési feladatok kivitelezésére.

A fejlesztési feladat megvalósítására irányuló projekt során a kivitelezéssel kapcsolatos változáskezelés, a megvalósítással kapcsolatos döntések meghozatala és a projekt minőségbiztosítása a hálózatgazda, a kivitelezés az üzemeltetés igényeivel való összehangolása az üzemeltető feladata.

A fejlesztés eredményének szakmai átvétele, a szakmai szempontok érvényesítése az átadás-átvételi folyamat során az üzemeltető feladata. Az üzemeltető a műszaki átvételről Átvételi jegyzőkönyvet köteles kiállítani, és azt a hálózatgazdának megküldeni.

Az Átvételi jegyzőkönyv alapján a hálózatgazda dönt a teljesítés mértékéről, és arról teljesítésigazolást állít ki.

A teljesítésigazolásnak és a szerződésnek megfelelően a vállalkozó által kiállított és benyújtott számlát a hálózatgazda ellenjegyzi, és azt pénzügyi teljesítés céljából továbbítja az illetékes szervezeti egység felé.

A szabályozott folyamatot a 2. számú függelék 9. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Az EKG szolgáltatásfejlesztési javaslat benyújtása.

Hálózatgazda

Feladatok, felelősségek:

– EKG infrastruktúrához és szolgáltatásokhoz kapcsolódó, jogszabályokból adódó fejlesztésének kezdeményezése;
– A fejlesztési irányok kijelölése, fejlesztési feladatok megfogalmazása;
– Közbeszerzéses megvalósítás esetén megvalósíthatósági tanulmány elkészíttetése, szükség esetén KIB általi véleményeztetése, a vállalkozó kiválasztása és a megvalósítás koordinálása;
– Teljesítés igazolása, Vállalkozói (szállítói) számla ellenjegyzése.

Üzemeltető:

Jogok:

– Az EKG szolgáltatásai továbbfejlesztésének, módosításának kezdeményezése, fejlesztési javaslat formájában.

Feladatok, felelősségek:

– A kivitelezés szakmai követése és műszaki átvétele.

Dokumentumok adattartalma:

FEJLESZTÉSI JAVASLAT	
Adat megnevezése	Jelentése
Azonosító, dátum	A javaslat azonosító adatai.
A javaslattevő adatai	A kezdeményező szervezet általános azonosító adatai; kapcsolattartó azonosítói, elérhetőségére vonatkozó adatok.
Előzmény adatok	Hibabejelentés vagy egyéb levélváltás azonosítója, tárgya.

FEJLESZTÉSI JAVASLAT	
Adat megnevezése	Jelentése
Fejlesztési javaslat	A fejlesztési javaslat műszaki tartalma, paraméterei, a megvalósítás javasolt módja.
Indoklás	A fejlesztési javaslat indoklása, különös tekintettel a kiváltó okokra, várható hasznára.
Határidő	A fejlesztés javasolt megvalósítási határideje.

MEGVALÓSÍTHATÓSÁGI TANULMÁNY	
Adat megnevezése	Jelentése
Azonosítók	A megvalósíthatósági tanulmány egyértelmű azonosító adatai: cím, rendelés szám, dátum stb.
A készítő adatai	A tanulmány készítőjének általános azonosító adatai; kapcsolattartó azonosítására, elérhetőségére vonatkozó adatok.
Előzmény adatok	Megrendelés, ajánlat vagy egyéb levélváltás azonosítója, tárgya.
Műszaki leírás	– A megrendelt fejlesztés műszaki megvalósításának leírása. – A megvalósítás lebonyolításának módja, ütemezése. – A fejlesztés által biztosított, megváltozott műszaki paraméterek. – Egyéb, a minőségügyi rendszer által megkövetelt szakmai tartalom.
Üzleti adatok	– A megvalósítás tervezett pénzügyi ráfordításai és ütemezése.

HAVI JELENTÉS A FEJLESZTÉSEKRŐL	
Adat megnevezése	Jelentése
Dátum információk	A kimutatás kiadásának és vizsgált időszakának dátuma.
Fejlesztések adatai	– A fejlesztések jellemző adatai. – Futamidő, státusz. – Időszakra tervezett feladatok. – Időszakban lezárt, megvalósult feladatok. – Esetlegesen meghiúsult feladatok. – Eltérések, megvalósítási kockázatok.
Statisztika adatok	A fejlesztések és az általuk megvalósított műszaki mutatóváltozások.

SZERZŐDÉS KÜLSŐ SZÁLLÍTÓVAL	
Adat megnevezése	Jelentése
Általános szerződés kellékek	Dátum, szerződő partnerek adatai.
Műszaki specifikáció	– Hivatkozott műszaki megvalósítási terv. – A fejlesztések jellemzői, szállítandó termék, szolgáltatás. – A kivitelezés ütemezése, határidők. – A kivitelezés módja, körülményei.
Üzleti megállapodás	A megvalósítás pénzügyi ráfordításai, fizetési ütemezés és feltételek.

ÁTVÉTELI JEGYZŐKÖNYV	
Adat megnevezése	Jelentése
Hivatkozási adatok	Szerződés, átadó-átvevő azonosítói, az átadás-átvétel tárgya.
Műszaki megfelelőség értékelése	– Hivatkozott szerződés szerint a specifikációnak való tételes megfelelőség. – A specifikációtól való eltérés jelzése és az eltérés mértéke (nem készült el, javítható eltérés, a megoldás elfogadhatatlan). – A kivitelezés határidő igazolása, eltérés jelzése. – Az átvétel minősítése: elfogadás, elutasítás és indoklása. – A követő feladat jelzése (teljesítésigazolás, javítás stb.).

TELJESÍTÉSI IGAZOLÁS	
Adat megnevezése	Jelentése
Hivatkozási adatok	Szerződés, az átadás-átvételi jegyzőkönyv azonosítója, tárgya.
Pénzügyi adatok	A szerződésben meghatározott fizetési feltételek, valamint az átadás-átvétel műszaki tartalmával összhangban: – a teljesítés dátuma; – a teljesítés mértéke, aránya.

5.2.10. EKG-n keresztül megvalósuló internet kapcsolódás sávszélességének bővítése

Az EKG-n keresztül nyújtott internet-hozzáférés alapja az, hogy az EKG külső hálózatokkal és internet kapcsolati központokkal van összeköttetésben.

Megnövekedett internet-sávszélesség igény esetén a hálózatgazda a szolgáltatás feltételeinek módosítását kezdeményezi az internet kapcsolódási pont szolgáltatójánál, a módosítási igény meghatározásával.

A hálózatgazda és az internet kapcsolódási pont szolgáltatója ezt követően egyeztet a feltételek módosításáról. Amennyiben az egyeztetés eredményesen zárul, és a felek sikeresen megállapodnak a jövőbeli együttműködés (pénzügyi, szolgáltatási és technikai) feltételeiben, módosítják a kettejük között érvényben lévő szerződést.

Sikertelen egyeztetés esetén, ha az eddigi internet kapcsolódási pont szolgáltatóval nem lehetséges a szolgáltatás feltételeinek módosítása, a hálózatgazda kezdeményezi új internet szolgáltató igénybevételét.

A hálózatgazda internet szolgáltatási igény megküldésével felveszi a kapcsolatot a szóba jöhető – esetleg több – új szolgáltatóval, és egyeztetéseket, tárgyalásokat kezdeményez. A hálózatgazda ez irányú utasítása esetén, az egyeztetéseken részt vesz az üzemeltető is.

Amennyiben az egyeztetéseken megállapodás születik a pénzügyi, technikai és szolgáltatási paramétereket illetően, a hálózatgazda szerződést köt az új szolgáltatóval.

A szolgáltatási szerződés megkötését követően a hálózatgazda utasítja az üzemeltetőt az új internet kapcsolódási pont megvalósítására, az új szolgáltatóval kötött szerződésben foglaltak teljesülése érdekében.

A folyamatot a 2. számú függelék 10. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Hálózatgazda:

Jogok:

– Új EKG internet-kapcsolat igénybevételének kezdeményezése, megnövekedett sávszélesség-igény esetén.

Felelősségek:

– Kapcsolatfelvétel kezdeményezése nagyobb sávszélesség-szükséglet esetén a meglévő, illetve új internet kapcsolati pontot nyújtó szolgáltatóval;
– Szerződéskötés, illetve módosítás az internet kapcsolati pontot nyújtó szolgáltatóval.

Üzemeltető:

Felelősségek:

– Rendelkezésre állás technikai egyeztetés céljából, a hálózatgazda felkérésére.

Dokumentumok adattartalma:

INTERNET KAPCSOLAT LÉTESÍTÉSÉNEK VAGY MÓDOSÍTÁSÁNAK IGÉNYLÉSE	
Adat megnevezése	Jelentése
Azonosító	Az igény azonosító adatai.
Dátum információk	Az igény benyújtásának dátuma.
A jellemző műszaki adatok	Igényelt sávszélesség, módosítás műszaki feltételei, specifikációja.
Indoklás	A módosítási igény műszaki indokai.
Határidő	A módosítás kezdetének kért határideje.

SZERZŐDÉS – INTERNETSZOLGÁLTATÓVAL	
Adat megnevezése	Jelentése
Általános szerződés kellékek	Dátum, szerződő partnerek adatai.
Műszaki specifikáció	– Hivatkozott műszaki dokumentumok. – Az internetcsatlakozás jellemzői. – A szolgáltatás kezdete.
Üzleti megállapodás	A szolgáltatás pénzügyi feltételei, a megállapodás elemei.

5.2.11. Karbantartás

A hálózati eszközök tervszerű és rendkívüli esetekben végzett karbantartása az üzemeltető feladata.

A rendszeres vagy tervszerű karbantartás időpontjait az üzemeltető a hálózatgazdával közösen jelöli ki. Ezekről az időpontokról, illetve a karbantartás felhasználókat érintő vonzataikról az üzemeltető az EKG honlapon tájékoztatást ad, illetve értesíti a felhasználókat.

Az üzemeltetői szerződésben meghatározott eseteken túl tervezett, illetve rendkívüli karbantartási feladatokról az üzemeltető előzetesen, írásban köteles tájékoztatni a hálózatgazdát, kérve annak jóváhagyását.

A hálózatgazda a körülményeket mérlegelve (rendkívüli karbantartás szükségessége esetén haladéktalanul) dönt a karbantartás megkezdéséről, és döntéséről – a karbantartás megkezdése előtt legalább 3 nappal – tájékoztatja az üzemeltetőt és a felhasználókat.

Amennyiben a karbantartások ideje alatt a szolgáltatási színvonal várhatóan csökken, a csökkenés várható mértékéről és eloszlásáról (időben, földrajzilag, fizikai paraméterekre vonatkozóan) az üzemeltető levélben, elektronikus levélben, a központi rendszerben küldött elektronikus üzenetben, a karbantartás megkezdése előtt tájékoztatja a várhatóan érintett felhasználókat.

Amennyiben a karbantartási feladatok végrehajtásához szükséges eszközök nem állnak rendelkezésre, az üzemeltető a hálózatgazda felé beszerzési eljárás lefolytatását kezdeményezi.

A beszerzés megfelelő határidőre történő lebonyolítása – és ennek keretében a szükséges eszközök szállítójának kiválasztása, az eszközök beszerzése és a beszerzés finanszírozása – a hálózatgazda felelőssége. A hálózatgazda szükség esetén kezdeményezheti az üzemeltető bevonását az eszközök és szállítójuk kiválasztásába.

Az eszközök átvétele, elhelyezése és tárolása az üzemeltető feladata. Az üzemeltető a karbantartási feladatok ellátása során az eszközökkel szabadon rendelkezik, illetve azok felhasználásáról pontos nyilvántartást vezet.

A karbantartás megvalósításáért, a karbantartási feladatok – üzemeltetői tevékenység naplóban történő – dokumentálásáért az üzemeltető felel.

Amennyiben a karbantartás során, illetve azt követően a tartalék eszközök szintje a kritikus szint alá süllyed, az üzemeltető köteles jelezni azt a hálózatgazda felé, aki az eszközkészlet szükség szerinti feltöltésére vonatkozóan beszerzési eljárást kezdeményez.

A szabályozott folyamatot a 2. számú függelék 11. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Időben történő tájékozódás a karbantartás okozta várható szolgáltatási szintcsökkenésről.

Feladatok, felelősségek:

– Karbantartásra vonatkozó tájékoztatás fogadása, felkészülés a karbantartási időszakra.

Hálózatgazda:

Jogok:

– Üzemeltetői szerződés megkötése, módosítása;
– Karbantartás elhalasztása.

Feladatok, felelősségek:

– Üzemeltetői szerződés megkötése, módosítása;
– Döntés a tervszerű vagy rendkívüli karbantartás időpontjairól;
– A karbantartáshoz, üzemeltetéshez szükséges eszközök beszerzése, szakmai részvétel a beszerzési eljárásban, a beszerzett eszközök átadása az üzemeltetőnek.

Üzemeltető:

Jogok:

– Üzemeltetői szerződés karbantartásra vonatkozó módosításának kezdeményezése.

Feladatok, felelősségek:

– A tervezett karbantartási időpontok kialakítása;
– A hálózatgazda és a felhasználók tájékoztatása az üzemeltetői szerződésben meghatározott időszakon kívül eső tervezett és rendkívüli karbantartási feladatokról;
– Részvétel a beszerzési eljárásban, az eszközök és szállítók kiválasztásában – igény szerint;
– Beszerzett eszközök átvétele, elhelyezése és tárolása;
– Karbantartási feladatok végrehajtása, dokumentálása;
– A tartalék eszközszint kritikus érték alá való csökkenése esetén beszerzési eljárás kezdeményezése a hálózatgazda felé.

Dokumentumok adattartalma:

TÁJÉKOZTATÓ LEVÉL	
Adat megnevezése	Jelentése
Dátum	A karbantartás idő intervalluma.
Leírás	– A karbantartás oka. – A karbantartás műszaki hatása a szolgáltatásra (esetleges teljesítmény csökkenés mértéke). – Igényelt felhasználói közreműködés.

NYILVÁNTARTÁS TARTALÉK ESZKÖZÖK FELHASZNÁLÁSÁRÓL	
Adat megnevezése	Jelentése
Leltári azonosítók	A felhasznált eszköz leltári nyilvántartás szerinti azonosító adatai. A lecserélt eszköz leltári száma, megnevezése.
Dátum adatok	Az üzembe állítás dátuma, csere és leselejtezés dátuma.
Magyarázat	Felhasználás oka.

ÜZEMELTETŐI TEVÉKENYSÉG NAPLÓ	
Adat megnevezése	Jelentése
Megnevezés, leírás	Feladat műszaki tartalmának leírása.
Dátum adatok	A feladat végrehajtásának időtartama.
Közreműködők	Felelős és végrehajtó megnevezése.
Ráfordítás	– Humánráfordítás volumene, díja (szerződés alapján). – Eszközráfordítás (eszközfelhasználás alapján). – Időráfordítás (órában).

5.2.12. Üzemeltetés havi értékelése

Az üzemeltetői hatáskörben végzett tevékenységek dokumentálásának, elismerésének, értékelésének, valamint az üzemeltető teljesítés elszámolásának az üzemeltetői tevékenységekről készített különböző jelentések képezik az alapját. Ennek megfelelően az üzemeltető köteles tevékenysége során rendszeresen vezetni a tevékenység naplót, havi rendszerességgel pedig elkészíteni a következő jelentéseket:

– Havi jelentés (az üzemeltetői tevékenység napló alapján);
– Havi jelentés az elhárított és elhárítandó hibákról, problémákról;
– Összefoglaló az EKG fejlesztések pillanatnyi állapotáról;
– Havi üzemeltetői jelentés a felhasználók forgalmáról.

Az üzemeltető a fenti kimutatásokat, jelentéseket havonta köteles megküldeni a hálózatgazdának. Igény esetén köteles a tevékenységi naplót is megküldeni.

A hálózatgazda felelőssége a megkapott dokumentumok vizsgálata, valamint azok jóváhagyása vagy elutasítása.

A hálózatgazdának joga van a dokumentumokkal kapcsolatban tartalmi vagy formai kifogással élni: ezzel összhangban a jelentéseket elutasíthatja, illetve módosításukat, kiegészítésüket kezdeményezheti az üzemeltető felé.

Amennyiben a hálózatgazda kifogást nem emel, azok jóváhagyásával egyidejűleg elismeri az üzemeltetői havi jelentésben regisztrált feladatok teljesítését, és kiállítja az üzemeltetői teljesítésigazolást.

A hálózatgazda a jelentések elfogadását követően – amennyiben a jelentések tartalmából adódóan szükségesnek látja – szolgáltatásfejlesztési, illetve sávszélesség-ellenőrzési, felülvizsgálati feladatok végrehajtását kezdeményezheti.

Az üzemeltető a teljesítésigazolás – és az üzemeltetői szerződésben meghatározott ellentételezés – alapján számlát állít ki.

A szabályozott folyamatot a 2. számú függelék 12. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Hálózatgazda:

Jogok:

– Üzemeltetői szerződés módosításának kezdeményezése;
– Az üzemeltetői jelentések elutasítása, módosításuk, kiegészítésük kezdeményezése;
– Üzemeltetői teljesítés igazolása;
– Üzemeltetői számla ellenjegyzése.

Feladatok, felelősségek:
– Az üzemeltetői jelentések vizsgálata, döntés elfogadásukról;
– Teljesítési igazolás kiállítása.
Üzemeltető:
Jogok:
– Számla benyújtása az elfogadott jelentések alapján.
Feladatok, felelősségek:
– Üzemeltetői jelentések összeállítása és megküldése a hálózatgazdának;
– Üzemeltetői számla kiállítása és benyújtása.
Dokumentumok adattartalma:

HAVI JELENTÉS	
Adat megnevezése	Jelentése
Dátum	A tevékenységek dátum intervalluma (hónap, nap).
Tevékenységek jellemzői	(Kivonat a tevékenységi naplóból) – A tevékenység indító, előzmény dokumentuma. – Az elvégzett tevékenység leírása. – A felelős megnevezése. – A ráfordítások: eszköz, emberóra. – A tevékenység eredménye, státusza. – Tevékenység statisztika.

ÖSSZEFOGLALÓ AZ EKG FEJLESZTÉSEK PILLANATNYI ÁLLAPOTÁRÓL	
Adat megnevezése	Jelentése
Dátum adatok	Az összefoglaló készítésének időpontja, mely időponttól kezdve történik a változás kimutatása.
Bázis időszak műszaki jellemzői	Az előző jelentési időszak műszaki jellemzői, a rendszer kiépítettsége.
Változások	– Az üzemeltető által az EKG-n elvégzett tervszerű fejlesztések, beruházások jellemzői és státuszuk. – A rákapcsolások mennyiségi változásai. – Megszüntetések száma. – Folyamatban lévő műszaki tervek adatai. – Teljesítmény, adatforgalmi mutatók és változásuk. – Tartalék kapacitások. – A hálózatgazda által esetileg, előzetesen megkért információ.

5.2.13. Sávszélesség-gazdálkodás

A még rendelkezésre álló sávszélesség használatára vonatkozó igények kielégítésének alapja a sávszélesség-gazdálkodás.

A sávszélesség-gazdálkodási tevékenység és az ezzel kapcsolatos döntések meghozatala a hálózatgazda feladata.

Felhasználói sávszélesség-csökkentési igény esetén a hálózatgazda köteles dönteni a felszabaduló sávszélességről – a sávszélesség tartalékolásáról, illetve valamely sorban álló (jogos, de még nem teljesített) sávszélesség növelési igény teljesítéséről.

Amennyiben egy felhasználó(csoport) sávszélesség növelési igénnyel jelentkezik, a hálózatgazda az igény jóváhagyásával kapcsolatos döntés meghozásakor – szükség esetén az üzemeltető közreműködésével – megvizsgálja, hogy az igényelt sávszélesség-bővítéshez szükséges EKG-sávszélesség rendelkezésre áll-e.

Ha a szükséges sávszélesség nem áll rendelkezésre – és az adott igényt a körülmények mérlegelése alapján haladéktalanul teljesíteni kell – a hálózatgazda a felhasználók közül kiválasztja az(oka)t, amely(ek) sávszélességének csökkentése nem okozhat zavart az adott felhasználó(k) működésében. Ily módon esetenként a hálózatgazda szükségszerűségből kezdeményezi egy-egy felhasználó sávszélességének csökkentését és erről az érintett felhasználót tájékoztatja.

A sávszélesség csökkentése az adatforgalmi adatok vizsgálata alapján történik meg. Az adatforgalmi vizsgálathoz szükséges adatokat tartalmazó kimutatás előállítása a hálózatgazda utasítására az üzemeltető feladata.

A sávszélesség-csökkentésben érintett felhasználók – adatforgalmi vizsgálat alapján történő – kiválasztása és velük egyeztetés kezdeményezése a hálózatgazda felelőssége.

A sávszélesség csökkentése esetén a hálózatgazda és a felhasználó módosított együttműködési megállapodást ír alá.
A sávszélesség-gazdálkodási problémák megelőzése érdekében a hálózatgazda folyamatosan követi a kapacitások alakulását, és adott kritikus szint elérése esetén kezdeményezi a sávszélesség-kapacitás növelését célzó fejlesztést.
A szabályozott folyamatot a 2. számú függelék 13. folyamatábrája szemlélteti.

Az egyes szerepkörökhöz tartozó jogok és felelősségek

Felhasználó:

Jogok:

– Sávszélesség-módosítás igénylése;
– Sávszélesség-csökkentésre kijelölt felhasználóként új adatforgalmi vizsgálat kezdeményezése a KIB-nél.

Feladatok, felelősségek:

– Sávszélesség-módosítási igény bejelentése;
– Sávszélesség-csökkentésre kijelölt felhasználóként részvétel hálózatgazdával folytatott egyeztetésen;
– Módosított együttműködési megállapodás megkötése.

Hálózatgazda:

Jogok:

– Döntés a sávszélesség-módosítási igényről;
– Döntés felszabaduló sávszélesség sorsáról;
– Felhasználó(k) kiválasztása, melyek sávszélesség-csökkentését kezdeményezi az adatforgalmi vizsgálatok alapján;
– A sávszélesség-kapacitás bővítését biztosító szolgáltatásfejlesztési feladatok kezdeményezése.

Feladatok, felelősségek:

– Üzemeltető felkérése adatforgalmi kimutatás elkészítésére (lásd 6.2.2. Változási kérelem);
– Felhasználó sávszélesség-csökkentésének kezdeményezése, ha a kapacitások szükségessé teszik és az adatforgalmi adatok indokolják;
– Egyeztetés a sávszélesség-csökkentésre kijelölt felhasználókkal a csökkentés működésre gyakorolt hatásáról;
– Együttműködési megállapodás módosítása;
– Üzemeltető utasítása a sávszélesség-csökkentésének megvalósítására.

Üzemeltető:

Feladatok, felelősségek:

– Adatforgalmi kimutatás (lásd 6.2.2. Változási kérelem) elkészítése;
– A sávszélesség-gazdálkodási feladatok technikai megvalósítása – sávszélesség csökkentése vagy növelése.

Dokumentumok adattartalma:

ÖSSZEFOGLALÓ AZ EKG FEJLESZTÉSEK PILLANATNYI ÁLLAPOTÁRÓL	
Adat megnevezése	Jelentése
Azonosító	Az igény azonosító adatai.
Dátum információk	Az igény benyújtásának dátuma.
Változtatást kérő(k) adatai	Érintett szervezet általános azonosító adatai; kapcsolattartó azonosítását, elérhetőségét tartalmazó adatok.
A jellemző műszaki adatok	Infrastruktúra- és eszközkonfiguráció meghatározása, a módosult sávszélesség adatforgalmi jellemzői.
Indoklás	Az igény indoka, különös tekintettel a változás szükségességét előidéző körülményekre.
Határidő	A módosítás kezdetének javasolt határideje.

6. Záró rendelkezések

6.1. Közzététel

A hálózatgazda a szabályzatot, annak módosításait az EKG honlapján közzéteszi (www.ekg.gov.hu vagy www.ekk.gov.hu), és az EKG üzemeltetésére kötött szerződésben, illetve a felhasználókkal kötött megállapodásokban a honlapon elérhető, mindenkor hatályos szabályzatot a felek számára kötelezően betartandó előírásként rögzíti.

1. számú függelék

Az EKG működését meghatározó dokumentumok

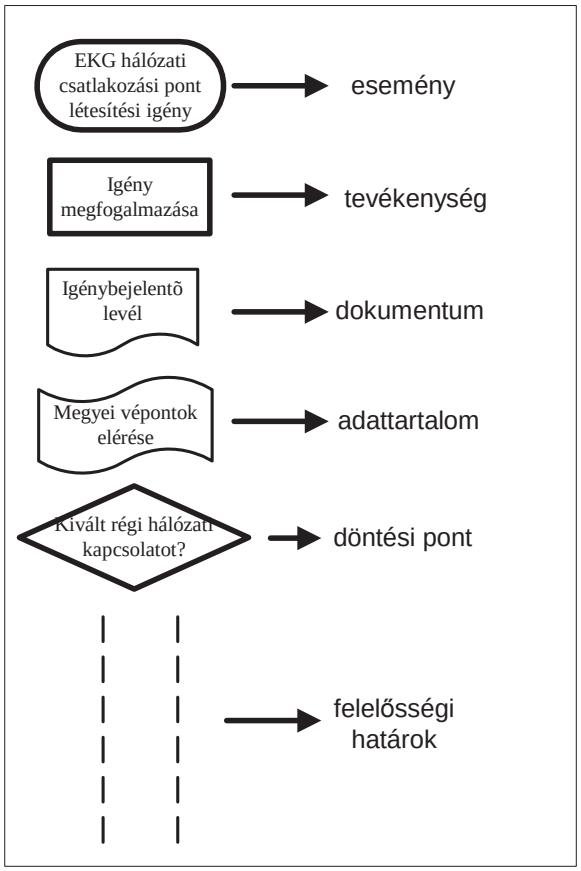
A dokumentumok elérhetők a www.ekg.gov.hu vagy www.ekk.gov.hu honlapon, az elfogadott dokumentumok honlapon történő megjelenéséért az EKG üzemeltetője felel.

Dokumentum megnevezése		Karbantartásáért felel
1.	Az EKG használati szabályzata	Hálózatgazda
2.	EKG biztonsági szabályzata	Hálózatgazda
3.	Szolgáltatások rendelkezésre állása (üzemidő)	Üzemeltető
4.	Helpdesk elérése	Üzemeltető
5.	Az EKG szolgáltatásban együttműködő felek felelősei (hálózatgazda, üzemeltető, felhasználók)	Üzemeltető
6.	Együttműködési megállapodás (EKG szolgáltatás tárgyában a hálózatgazda és a felhasználó között kötött szerződés) mintája	Hálózatgazda

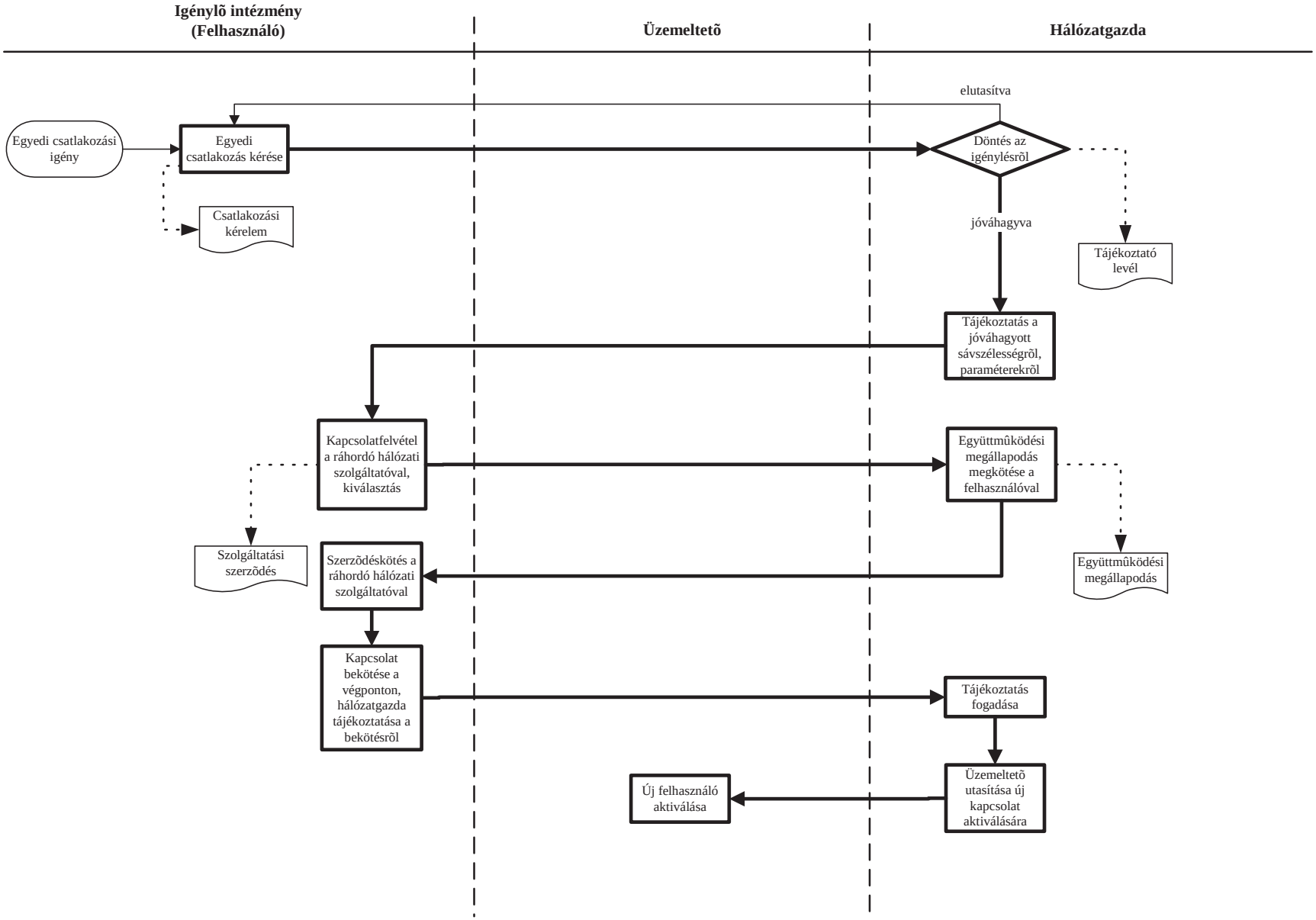
2. számú függelék

A szabályozott folyamatok

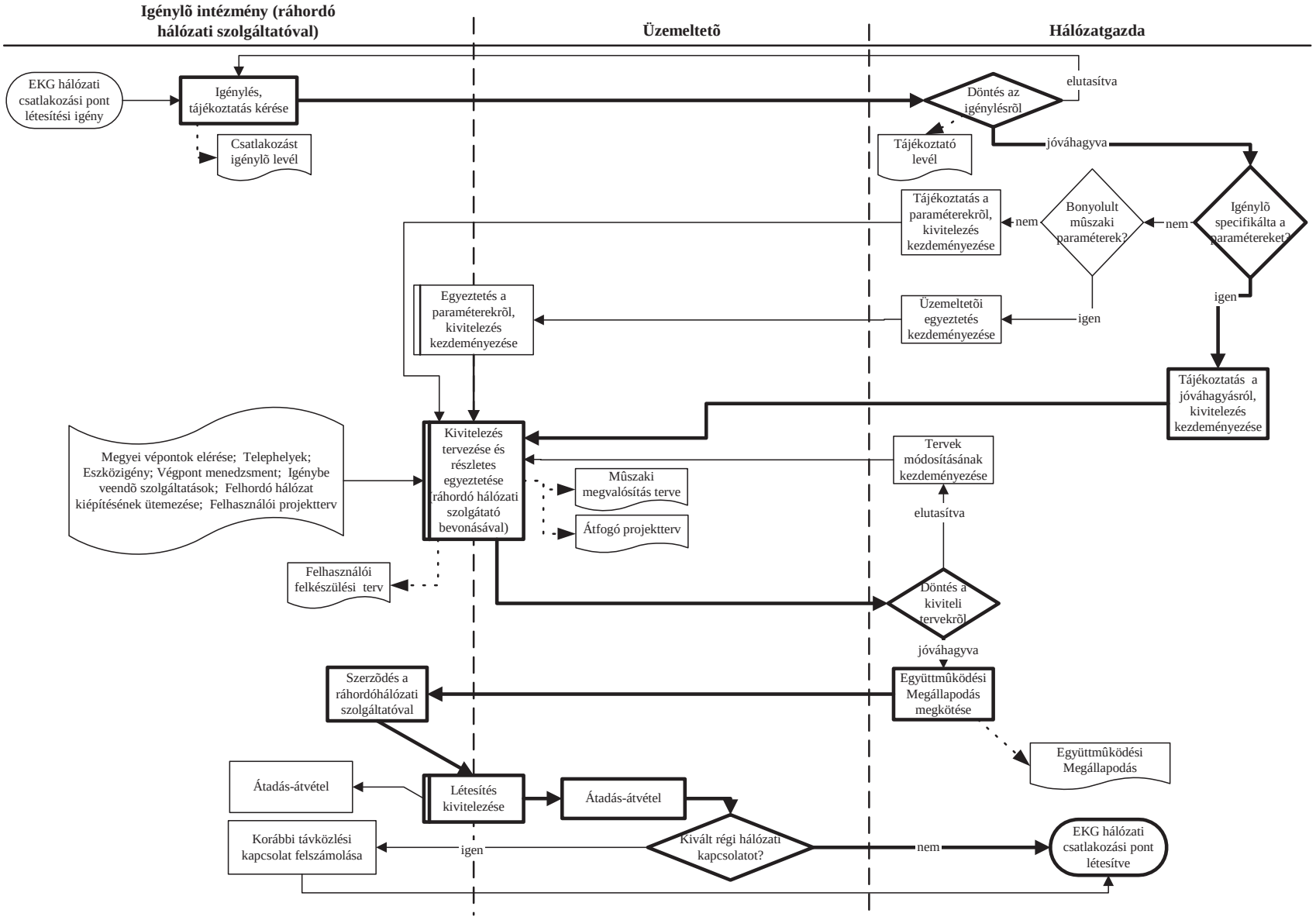
A függelék az 5. fejezet szabályozásaihoz kapcsolódó folyamatábrákat tartalmazza.



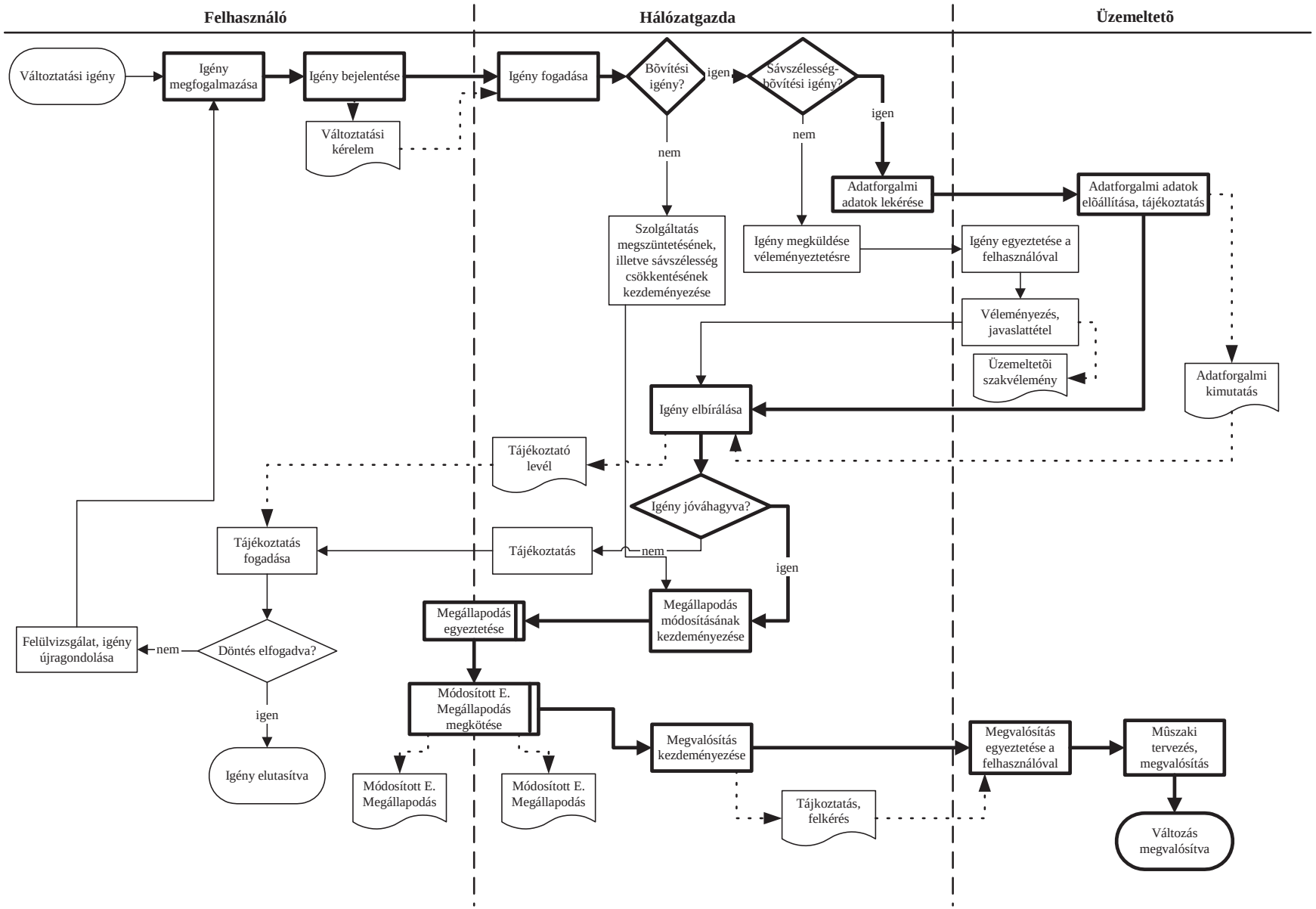
1.1. Kapcsolat létesítése – egyedi igénylő esetén



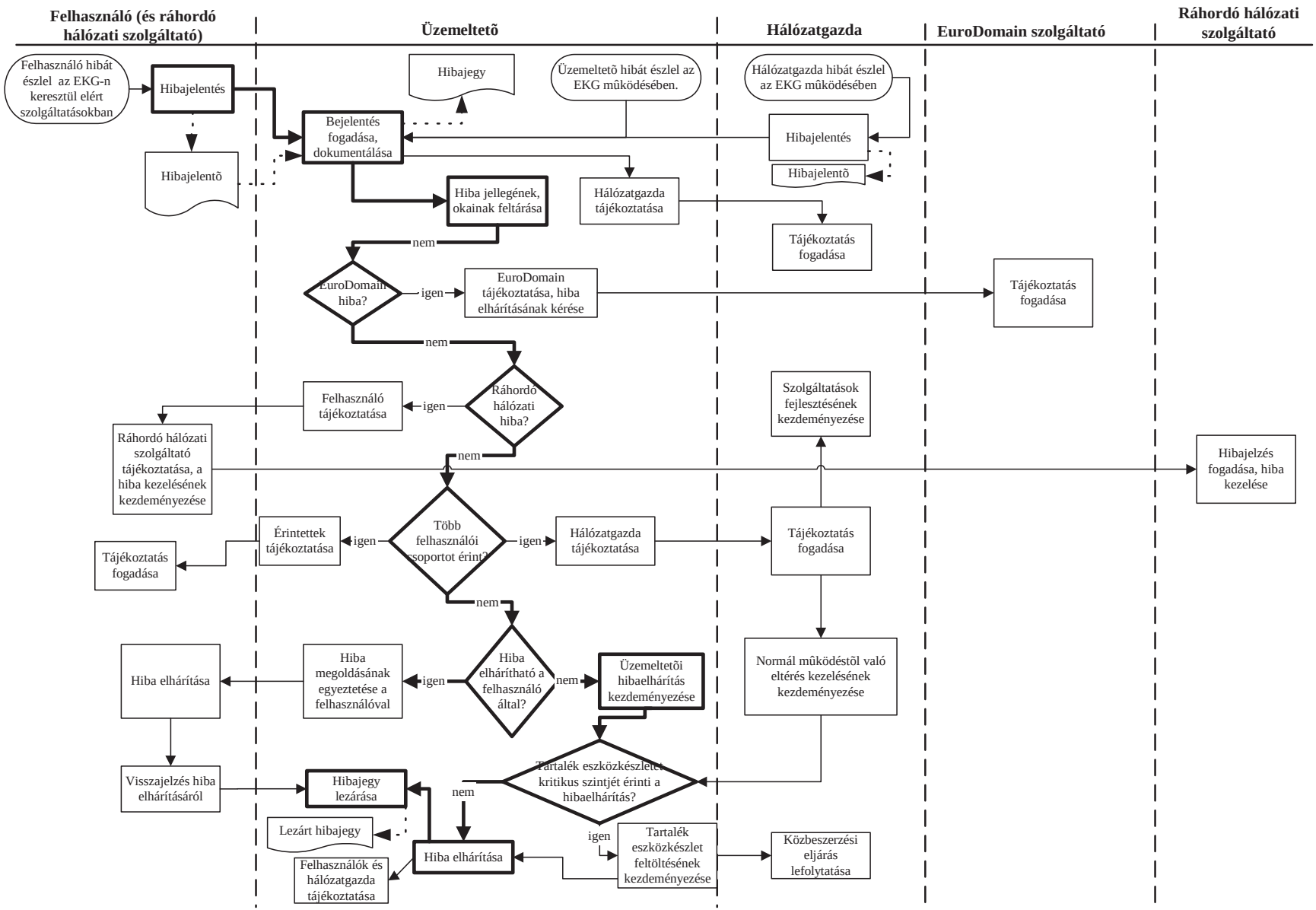
1.2. Kapcsolat létesítése – csoportos igénylés esetén



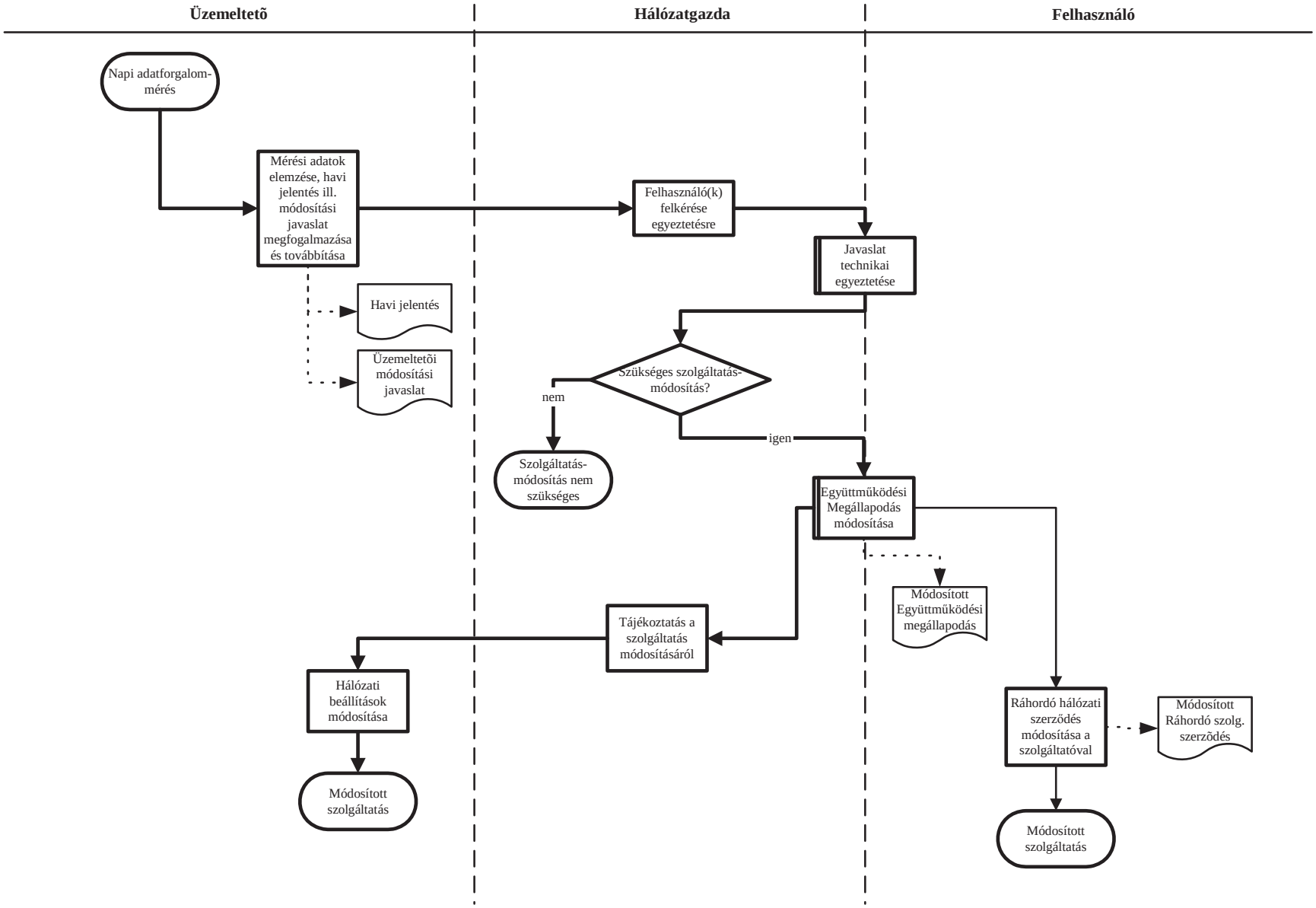
2. Változási kérelem



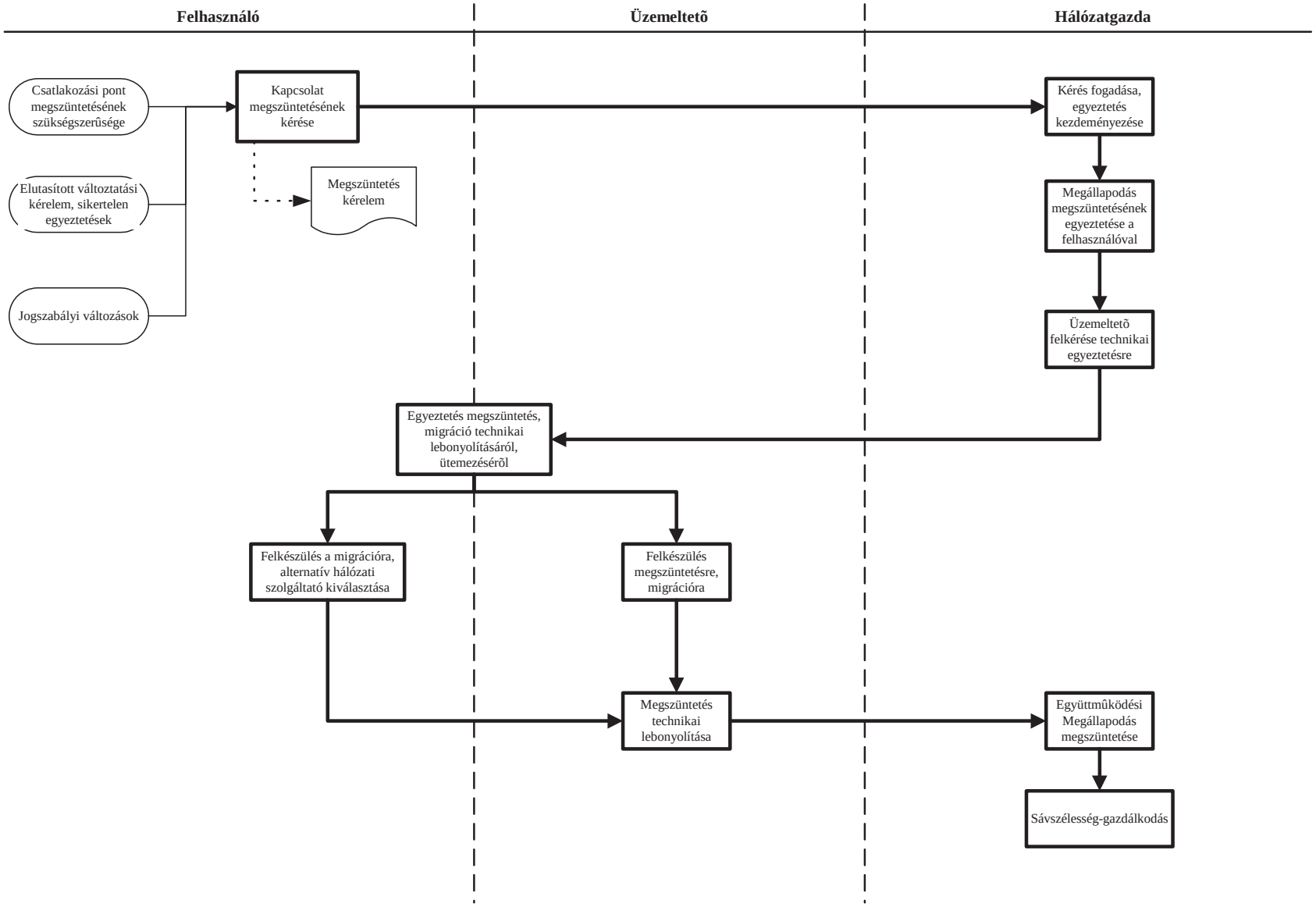
3. Hibajelentés, hibaelhárítás



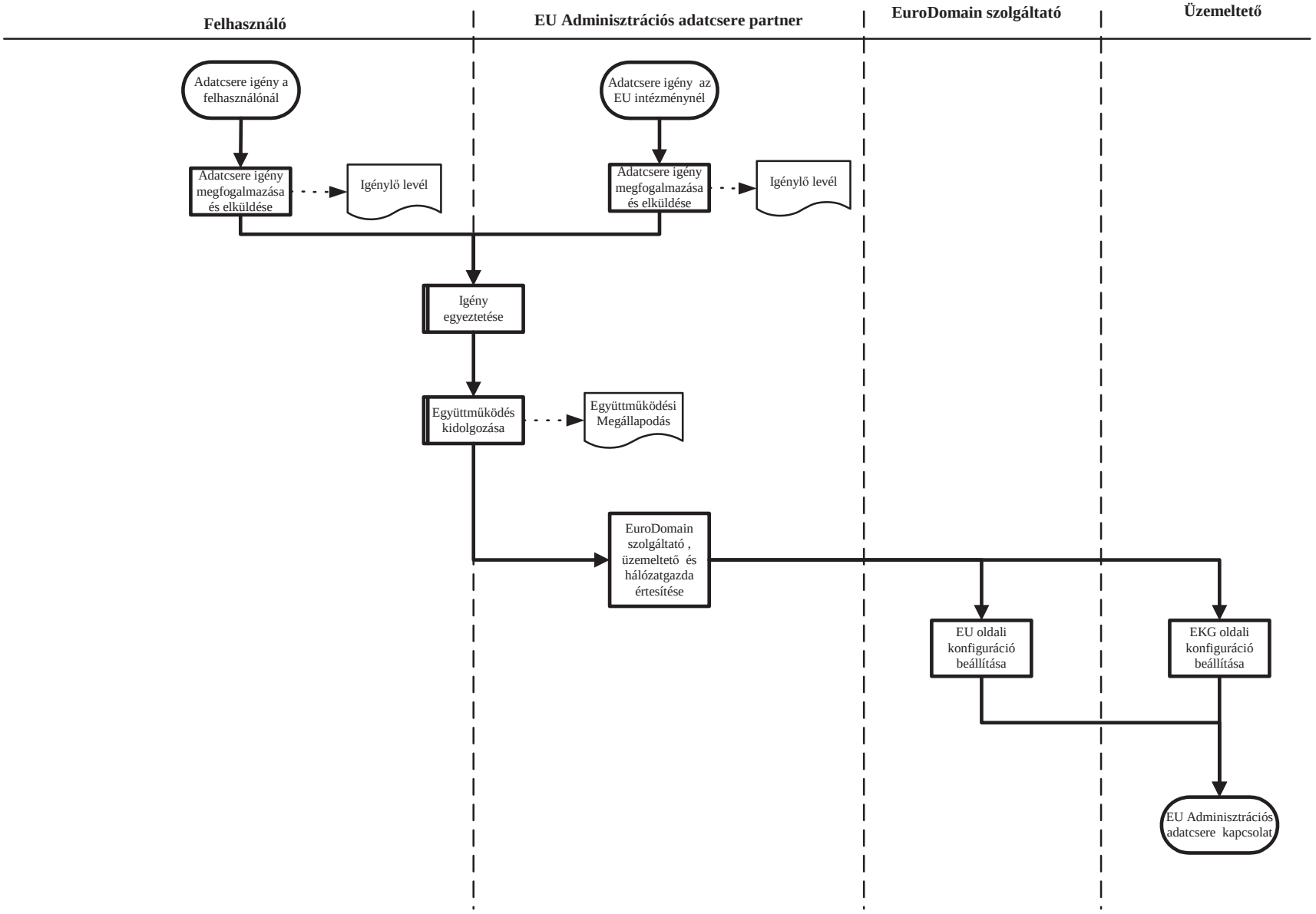
4. Sávszélesség-ellenőrzés, felülvizsgálat



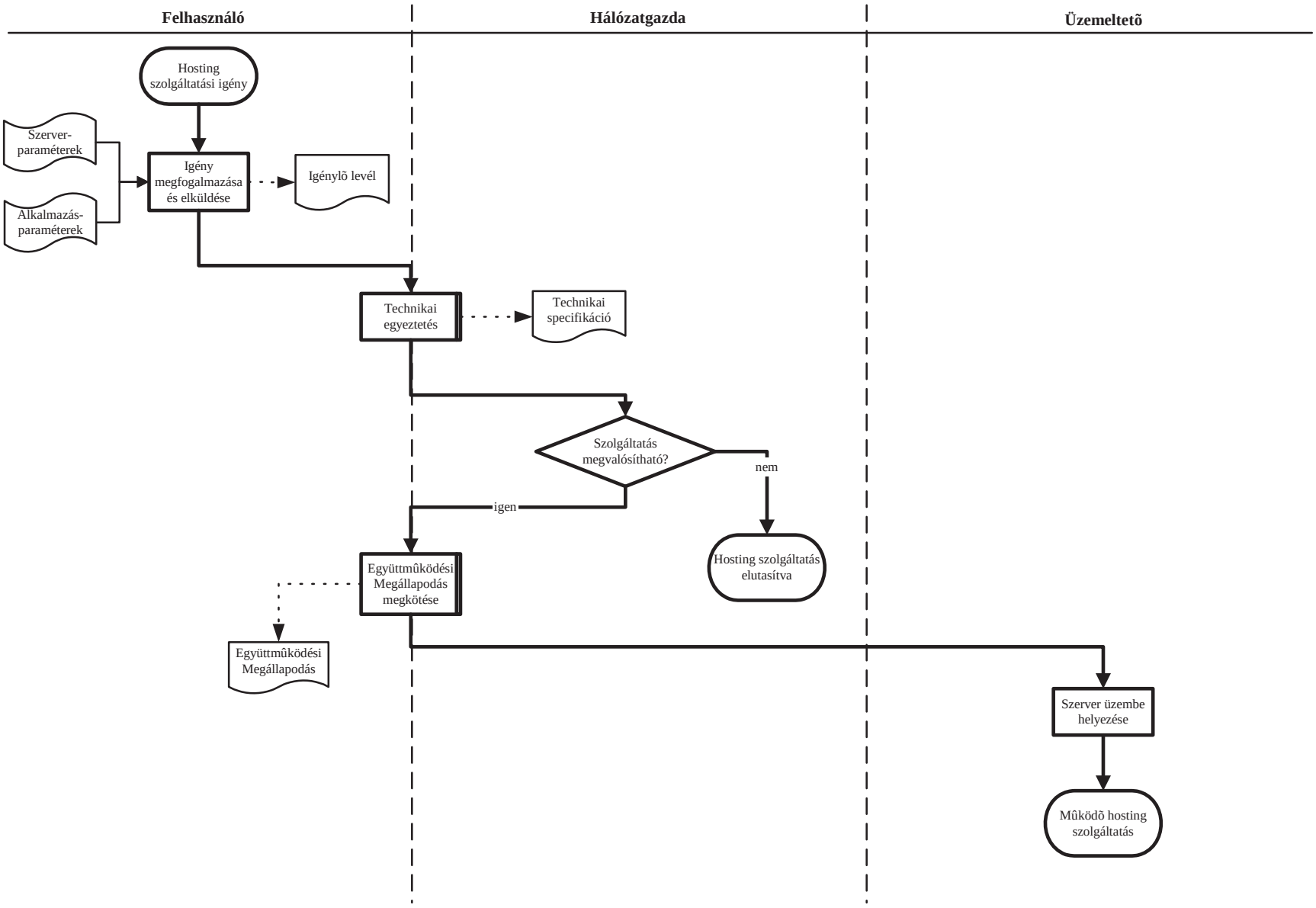
5. Kapcsolódás megszüntetése



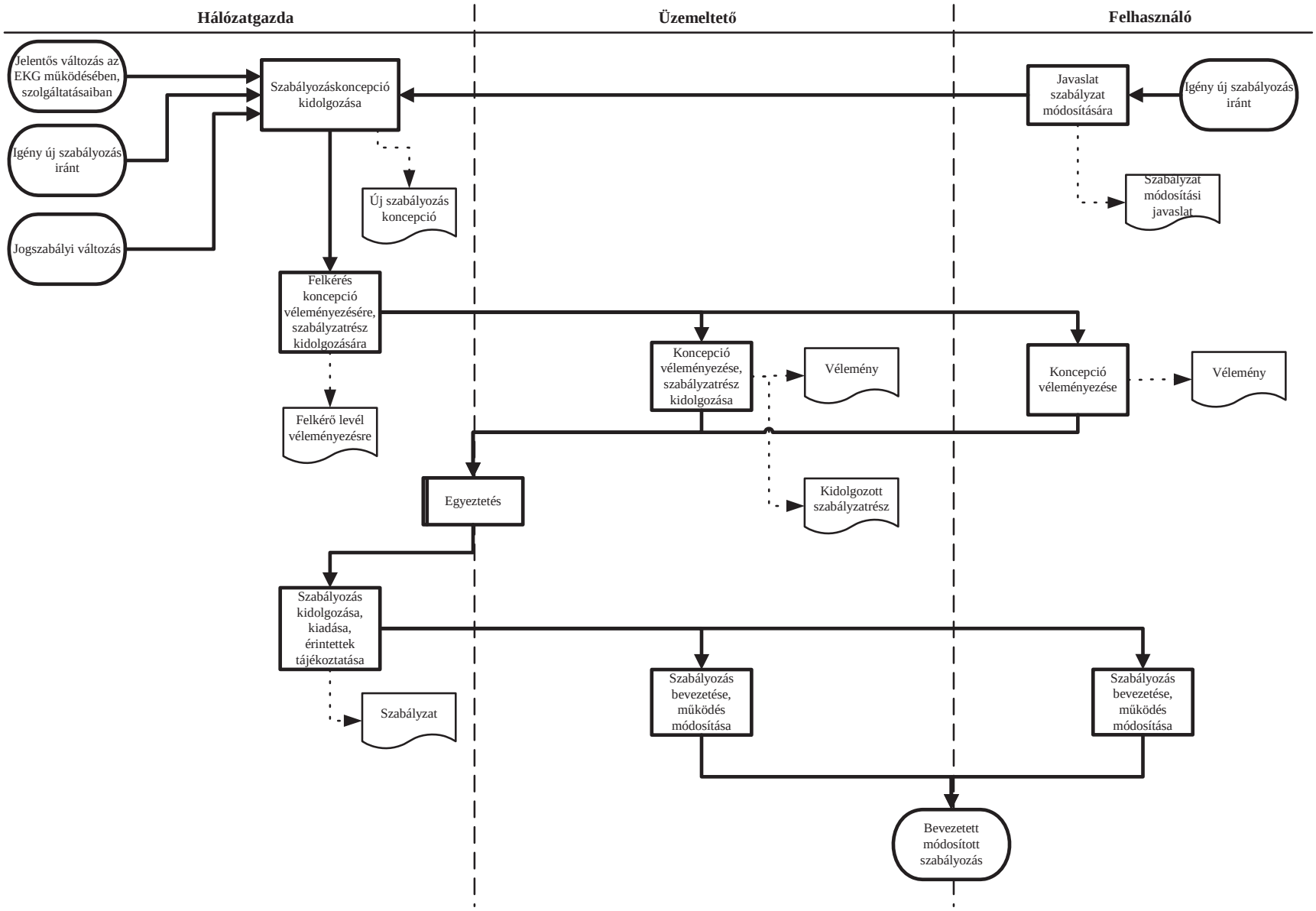
6. Adatcsere kapcsolat létrehozása EU adminisztrációval



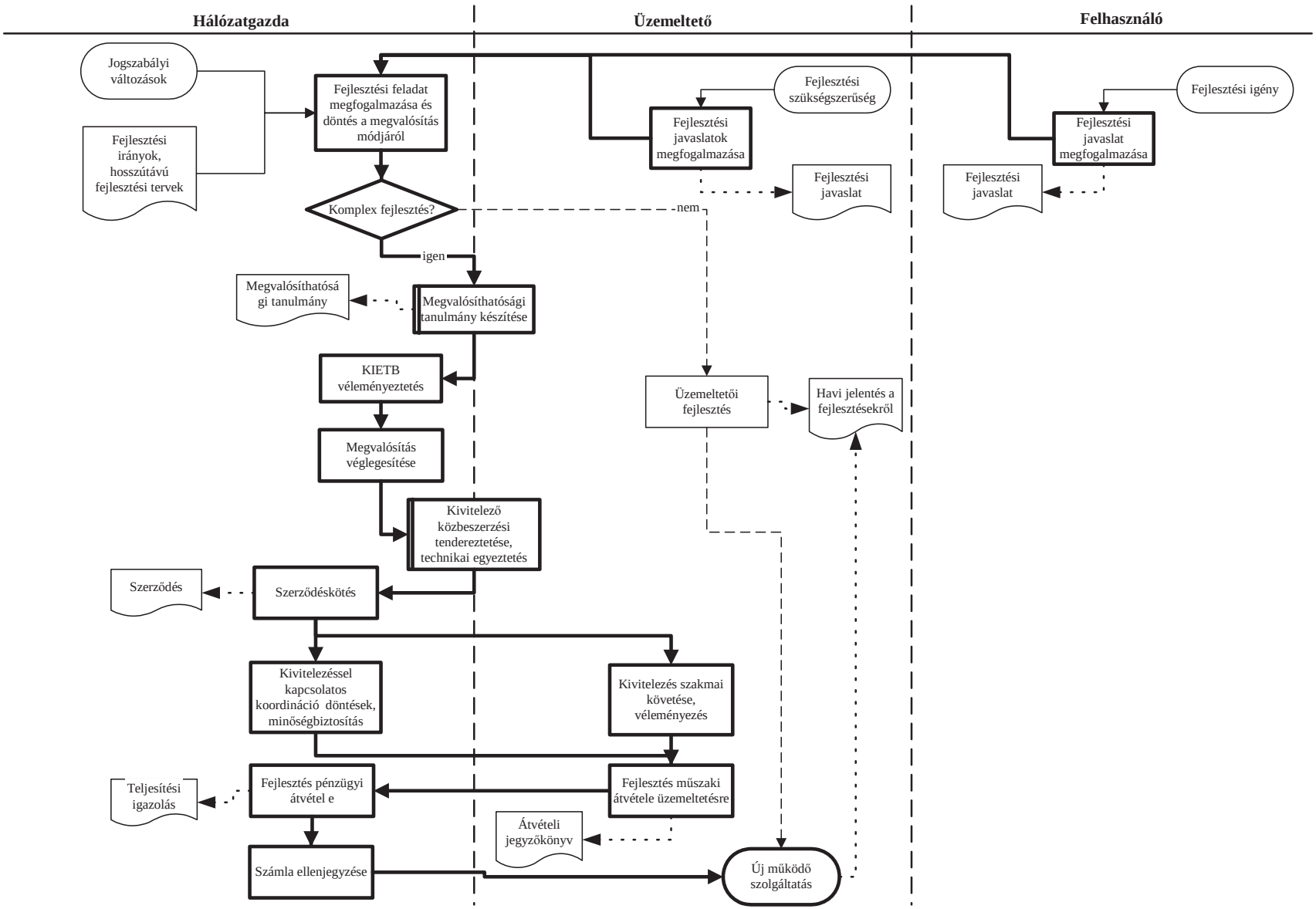
7. Hosting szolgáltatás igénybevétele



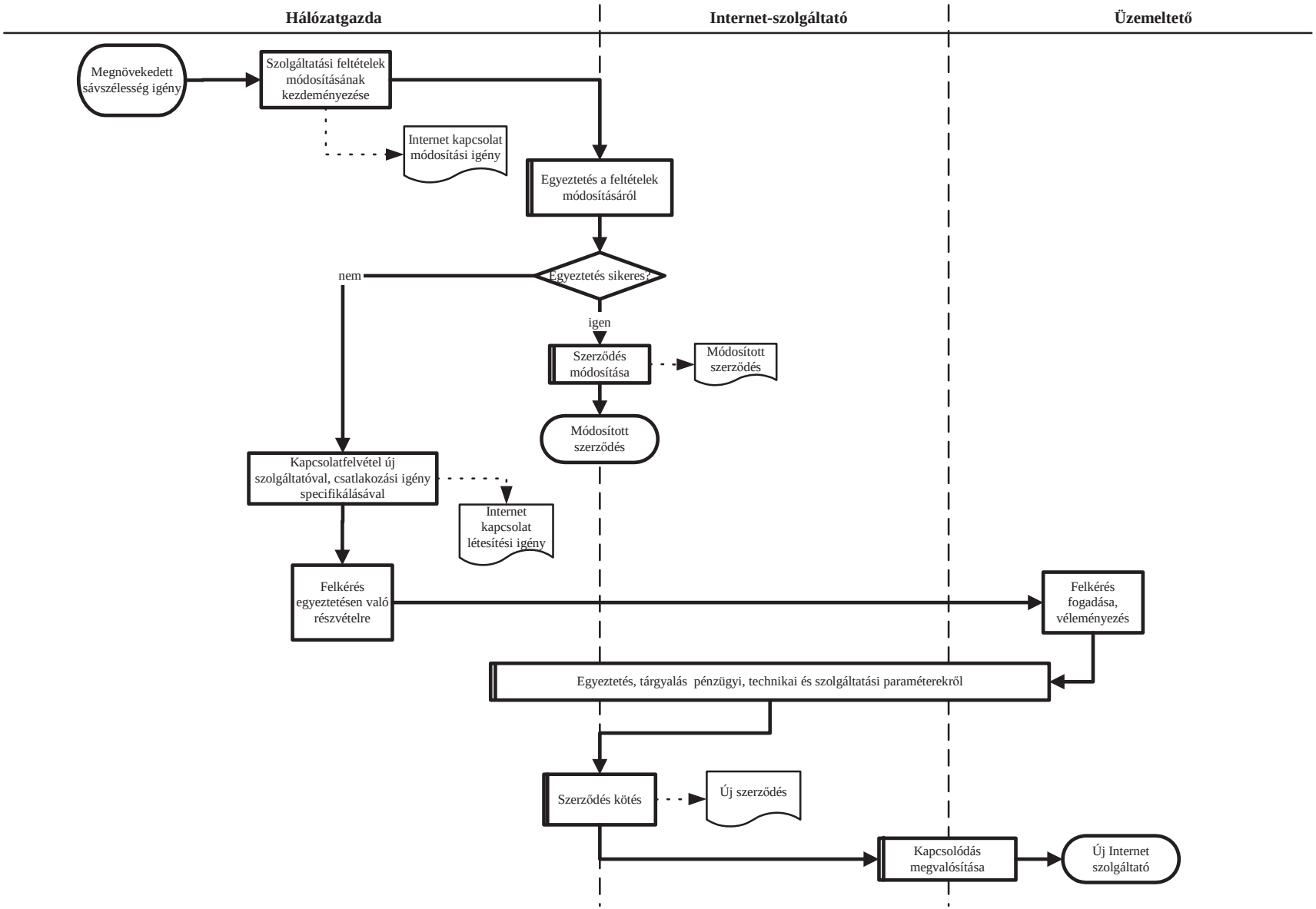
8. Szabályozások, szabályzatmódosítások bevezetése



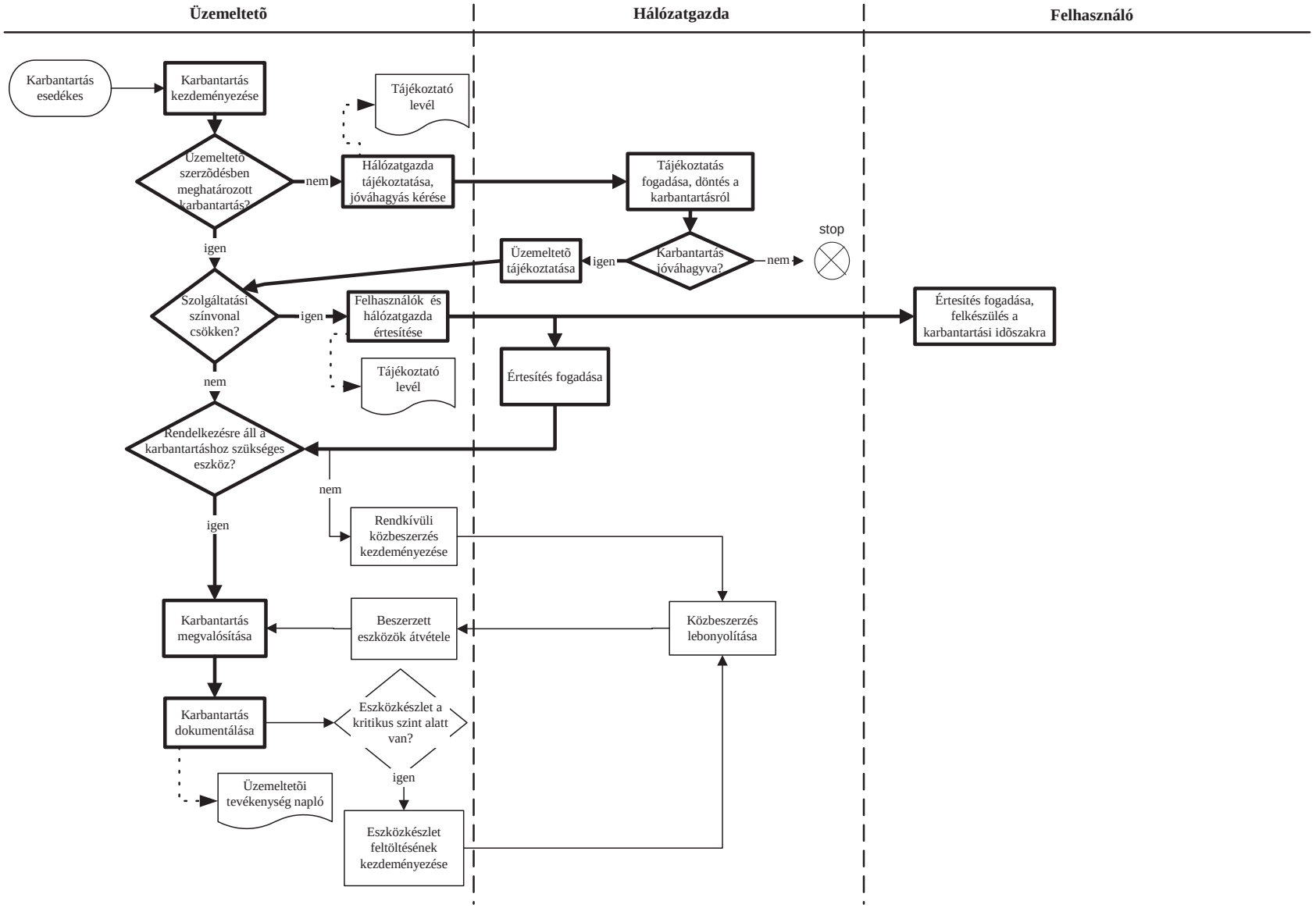
9. Szolgáltatások fejlesztése



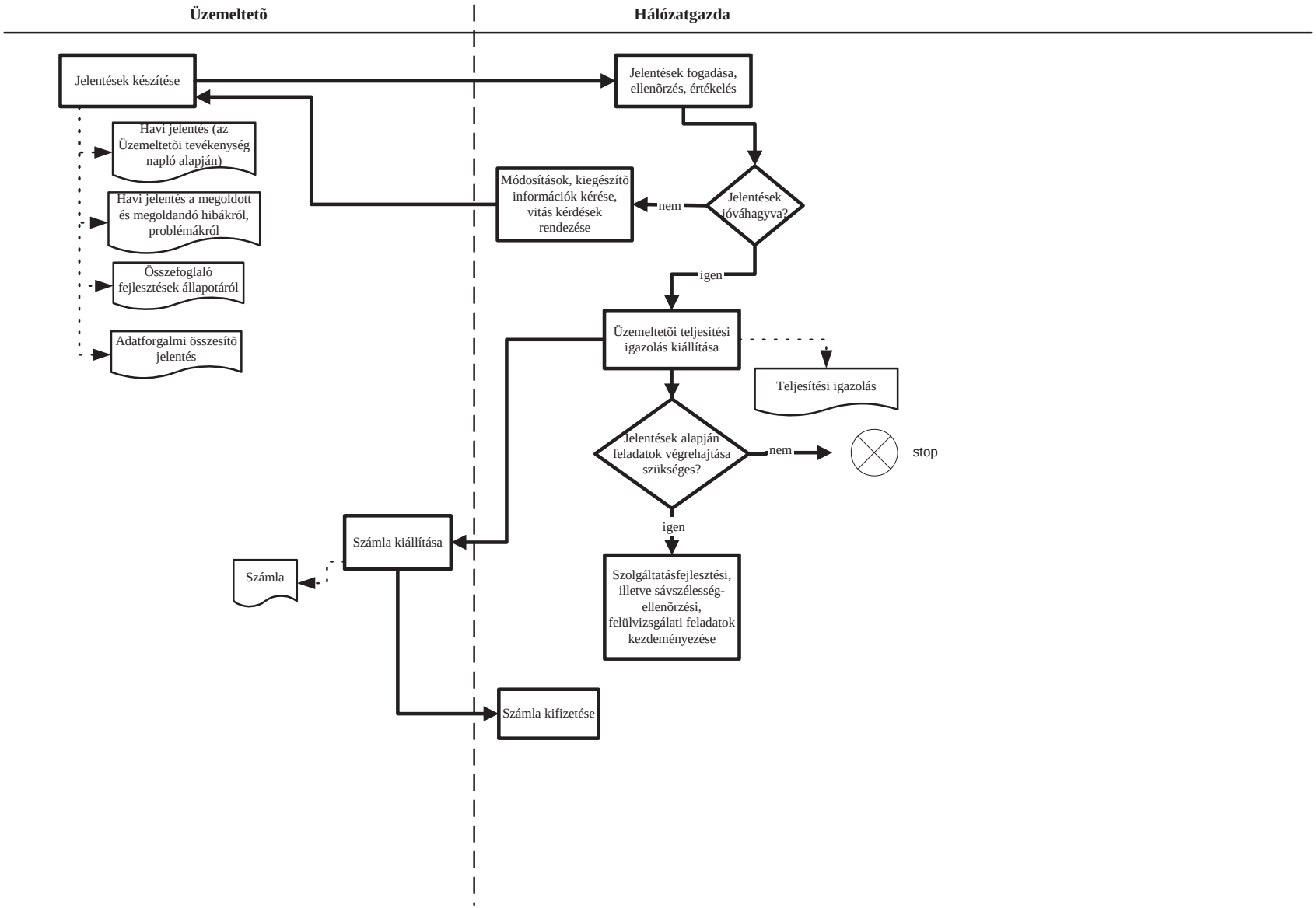
10. EKG-n keresztül megvalósuló internetkapcsolódás sávszélességének bővítése



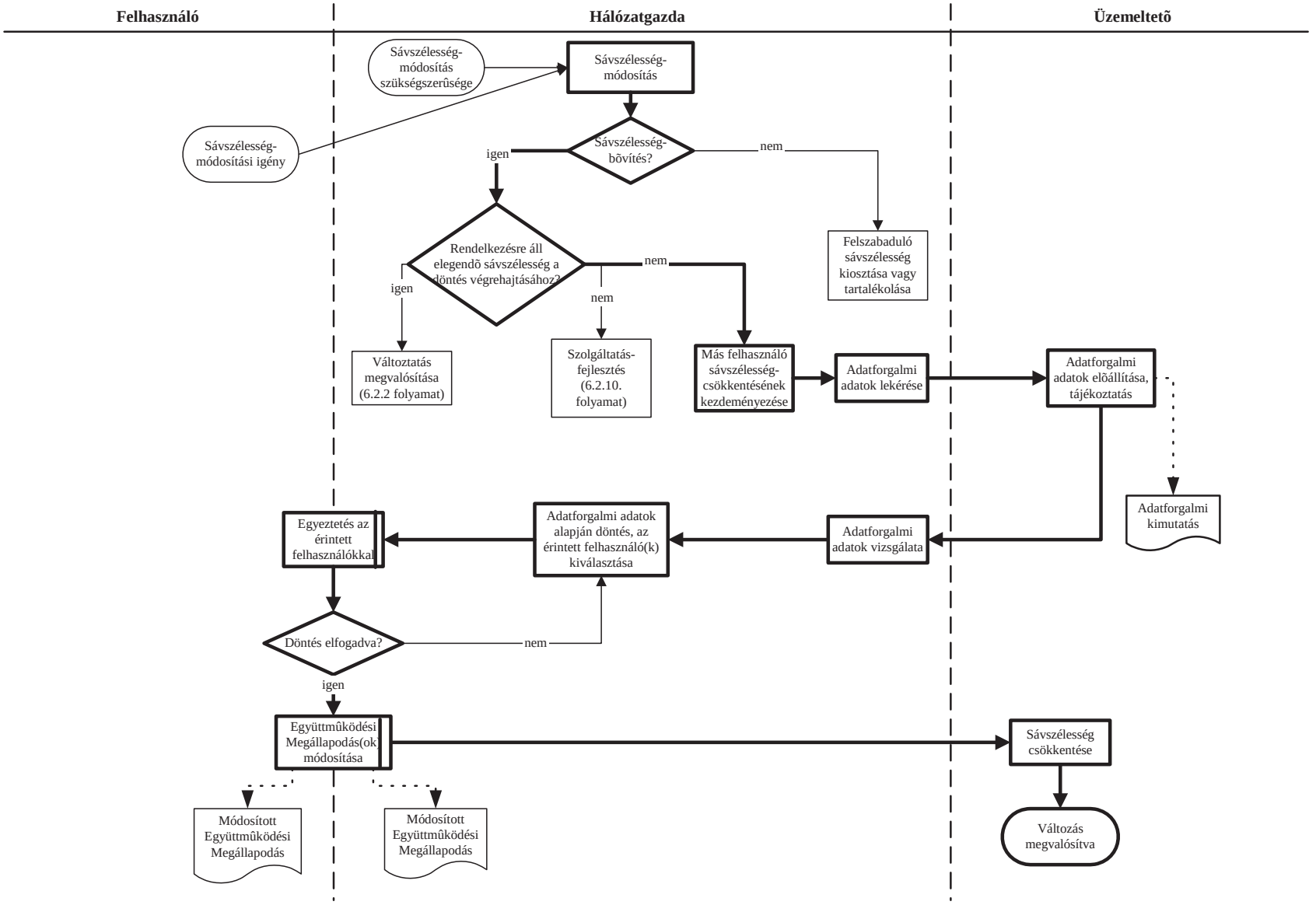
11. Karbantartás



12. Üzemeltetés havi értékelése



13. Sávszélesség-gazdálkodás



3. számú függelék

A jogok, kötelezettségek, felelősségek összefoglalása

Összefoglaló az EKG szolgáltatásban érintett szereplők jogairól, kötelezettségeiről, felelősségeiről

Alany	Jogok	Feladatok, felelősségek
Felhasználó	– EKG-kapcsolat igénylése, tájékoztatás kérése; – Szolgáltatások változtatásának igénylése; – Saját intézményi adatforgalmi adatainak megtekintése; – Elutasított igény esetén a felülvizsgálat kérése; – EKG-val kapcsolatos hiba elhárításának igénylése; – Tájékozódás a hibaelhárítás menetéről, a hibaelhárítás határidejéről; – EKG-kapcsolat megszüntetésének kezdeményezése; – Az EU adatcsere kapcsolat kialakításának kezdeményezése; – Hosting szolgáltatás igénybevételének kezdeményezése; – A meglévő szabályozás módosításának vagy új, még nem szabályozott terület szabályozásának kezdeményezése javaslat formájában; – Az EKG szolgáltatás fejlesztési javaslat benyújtása; – Időben történő tájékozódás a karbantartás okozta várható szolgáltatási szint csökkenésről; – Sávszélesség-módosítás igénylése; – Sávszélesség-csökkentésre kijelölt felhasználóként új adatforgalmi vizsgálat kezdeményezése a KIB-nél; – Felkérés esetén a hálózatgazda szabályzati vagy szabályzat-módosítási koncepciójának vagy a szabályzattervezetnek a véleményezése.	– Csatlakozás létesítésének, esetleges módosításának vagy megszüntetésének kezdeményezése; – A kezdeményezés hálózatgazdával történő egyeztetése; – Igényelt szolgáltatások vagy módosításuk szakszerű specifikálása; – Ráhordó hálózati szolgáltató(k) kiválasztása; – Részvétel az igényelt szolgáltatás, illetve módosítás vagy megszüntetés kivitelezési egyeztetésein; – Az üzemeltetővel folytatott egyeztetések alapján ütemtervek kidolgozása; – Együttműködési megállapodás megkötése, szükség esetén módosítása, megszüntetése; – Ráhordó hálózati szolgáltatás (amennyiben a kapcsolathoz kell) igénybevételéről szóló szolgáltatási szerződés megkötése, szükség esetén módosítása, megszüntetése; – Együttműködés az üzemeltetővel az igény megvalósításának tervezésében és végrehajtásában; – Szükség esetén a ráhordó hálózati szolgáltatás változáshoz illeszkedő módosíttatása; – Az EKG működésével kapcsolatos észlelt probléma bejelentése, a probléma leírása; – Saját eszközök hibáinak elhárítása; – Közreműködés az EKG eszközök csatlakozási hibáinak elhárításában – az üzemeltető irányítása alapján; – Visszajelzés az üzemeltetőnek az elhárított hibáról; – A ráhordó hálózati szolgáltatás (ha létezik) szinkronizálása a mindenkori kapcsolódási ponthoz; – Hosting szolgáltatásnál az üzemeltetendő alkalmazás telepítése, felhasználó oldalról történő távmenedzselés megoldása; – A végleges szabályzat bevezetése; – Karbantartásra vonatkozó tájékoztatás fogadása, felkészülés a karbantartási időszakra; – Kapcsolatfelvétel az EU adminisztrációs adatkapcsolat vonatkozásában az EU adminisztrációs partnerrel; – Együttműködési megállapodás kialakítása az EU adminisztrációs partnerrel; – Az EU adminisztrációs partner felelősségi körébe tartozó feladatok teljesülésének követése, és szükség szerint közreműködés azok végrehajtásában.
Hálózatgazda	– Döntés a csatlakozási igényről; – Az üzemeltető utasítása a csatlakozás előkészítési, megvalósítási feladatainak elvégzésére; – A csatlakozás szakszerűségének elbírálása; – A felhasználók adatforgalmi adatainak vizsgálata; – A változtatási igény elbírálása; – Az üzemeltető utasítása a szükséges feladatok végrehajtására;	– Az EKG rendeltetésének megfelelő működésének biztosítása; – Csatlakozási, szolgáltatás változtatási felhasználói igények jogi, műszaki megvalósíthatóságának vizsgálata; – A felhasználó tájékoztatása az igény teljesítésének lehetőségeiről, technikai paraméterekről; – Az üzemeltető utasítása egyeztetésen való részvételre bonyolult technikai kérdések felmerülése esetén; – Az üzemeltető utasítása – szükség esetén – a kivitelezés tervezését célzó egyeztetésekre; – Kiviteli tervek véleményezése, jóváhagyása vagy módosításuk kezdeményezése;

Alany	Jogok	Feladatok, felelősségek
	– Tájékozódás a hibákról, azok elhárításáról, a megoldásra váró hibákról, esetenként és havi összesítő jelentés alapján; – Kritikus erőforrásokat érintő hiba esetén a normál működésétől való eltérés kezelése; – Koncepcionális hiba esetén a várható probléma megelőzésére vonatkozó EKG fejlesztés kezdeményezése; – A tartalék eszközfelhasználás, az erről készített nyilvántartás ellenőrzése; – Egyeztetések kezdeményezése; – Az EKG auditálásának, csatlakozásának kezdeményezése az EuroDomain szolgáltatónál; – A meglévő szabályozás módosításának vagy új, még nem szabályozott terület szabályozása; – Új EKG internet-kapcsolat igénybevételének kezdeményezése, megnövekedett sávszélesség-igény esetén; – Üzemeltetői szerződés megkötése, módosítása; – Karbantartás elhalasztása; – Az üzemeltetői jelentések elfogadása, elutasítása; – Üzemeltetői teljesítés igazolása; – Üzemeltetői számla ellenjegyzése; – Döntés a sávszélesség-módosítási igényről; – Döntés felszabaduló sávszélesség felhasználásáról; – Felhasználó(k) kiválasztása, melyek sávszélesség-csökkentését kezdeményezi az adatforgalmi vizsgálatok alapján; – A sávszélesség-kapacitás bővítését biztosító szolgáltatásfejlesztési feladatok kezdeményezése.	– Együttműködési megállapodás megkötése, módosítása a felhasználóval; – Üzemeltető tájékoztatása a megkötött, módosított Együttműködési megállapodásról; – Szolgáltatásfejlesztési feladatok kezdeményezése; – Kritikus erőforrásokat érintő hiba esetén a normál működésétől való eltérés kezelése; – Koncepcionális hiba esetén a probléma megelőzésére vonatkozó EKG fejlesztés kezdeményezése, végrehajtása; – A hibaelhárítási tevékenység folyamatos figyelemmel kísérése (monitoring), a vonatkozó jelentések vizsgálata; – A tartalék eszközkészlet feltöltésére irányuló beszerzési eljárás megindítása az üzemeltető kezdeményezésére; – A rendelkezésre álló EKG sávszélesség gazdaságos és hatékony elosztásának biztosítása, figyelembe véve az EKG mindenkori üzembiztonságát (sávszélesség-gazdálkodás); – Sávszélesség-gazdálkodási feladatok keretében döntés a felszabaduló sávszélesség kezeléséről; – Kapcsolattartás az EuroDomain szolgáltatóval; – Az EKG felkészítése az EuroDomain kapcsolódás követelményeire; – Az EuroDomain szolgáltató felelősségi körébe tartozó feladatok teljesülésének követése; – Szabályzat-módosítás koncepciójának kidolgozása és annak véleményeztetése az üzemeltetővel és a felhasználókkal; – A szabályzat véglegesítése és kiadása – az érintettek véleményének figyelembevételével; – EKG infrastruktúrához és szolgáltatásokhoz kapcsolódó, jogszabályokból, felhasználói, üzemeltetői javaslatokból adódó fejlesztések kezdeményezése; – A fejlesztési irányok kijelölése, fejlesztési feladatok megfogalmazása; – Beszerzéses megvalósítás esetén Megvalósíthatósági tanulmány elkészíttetése, KIB általi véleményeztetése, a vállalkozó kiválasztása és a megvalósítás koordinálása; – Teljesítés igazolása, Vállalkozói (szállítói) számla ellenjegyzése; – Szerződéskötés, illetve módosítás az internetkapcsolati pontot nyújtó szolgáltatóval; – Üzemeltetői szerződés megkötése, módosítása; – Döntés a tervszerű vagy rendkívüli karbantartás időpontjairól; – A karbantartáshoz, üzemeltetéshez szükséges eszközök beszerzése, szakmai részvétel a beszerzési eljárásban, a beszerzett eszközök átadása az üzemeltetőnek; – Az üzemeltetői jelentések vizsgálata, döntés elfogadásukról; – Teljesítési igazolás kiállítása;

Alany	Jogok	Feladatok, felelősségek
		– Felhasználó sávszélesség-csökkentésének kezdeményezése, ha a kapacitások szükségessé teszik és az adatforgalmi adatok indokolják; – Egyeztetés a sávszélesség-csökkentésre kijelölt felhasználókkal a csökkentés működésre gyakorolt hatásáról; – Hatékony kommunikációs feladatok megtervezése, végrehajtása, a végrehajtás elemzése.
Üzemeltető	– A hálózat sérülésének kockázata esetén a megelőzés minden lehetséges eszközzel; – Szakmai tanácsadás a felhasználók számára; – Javaslattétel a hálózatgazdának a szükséges eszközbeszerzésekre; – Fejlesztési javaslatok megfogalmazása a hálózatgazda számára; – Javaslat adása a felszabaduló sávszélesség kezelésére; – A meglévő szabályozás módosításának vagy új, még nem szabályozott terület szabályozásának kezdeményezése; – Üzemeltetői szerződés módosításának kezdeményezése; – Számla benyújtása az elfogadott havi jelentések alapján.	– A felhasználóval, igénylővel való technikai egyeztetés – a hálózatgazda utasítására; – Részvétel a kivitelezés részletes tervezésében és a tervezéssel kapcsolatos egyeztetésben – a hálózatgazda utasítására; – Felhasználói ütemtervek véleményezése; – Kiviteli tervek átadása véleményezés és jóváhagyásra felterjesztése a hálózatgazdának; – A hálózatgazda által kiadott feladatok ellátása közben felmerülő, az EKG biztonságos működését veszélyeztető tényezők jelentése a hálózatgazdának; – Adatforgalmi kimutatás összeállítása a hálózatgazda és a felhasználó részére; – Kiegészítő szolgáltatások műszaki megvalósíthatóságának véleményezése a hálózatgazda utasítására; – A megvalósítás keretében a felhasználóval folytatott műszaki-technikai egyeztetések és módosított együttműködési megállapodás alapján a szolgáltatás változtatásához kapcsolódó infrastruktúra-bővítési és eszközkonfigurálási feladatok lebonyolítása; – Hibabejelentések fogadásáért és a hibaelhárítás kezdeményezéséért felelős helpdesk felállítása és működtetése; – Felhasználótól, hálózatgazdától érkezett hibabejelentések fogadása, dokumentálása, illetve a saját maga által észlelt hibák dokumentálása; – Hibajegyek kiállítása; – Hálózatgazda tájékoztatása a hibákról, eseti és havi összesítő jelentés készítése és eljuttatása a hálózatgazdához; – Az EKG közvetett érintettjei (ráhordó hálózati szolgáltatók, EuroDomain hálózatgazda stb.) által felügyelt rendszerek, hálózatok működésében bekövetkezett, üzemeltető által észlelt hiba esetén hibajegy kiállítása, hibajelentés küldése az érintett szolgáltató felé; – Hiba elhárításának megkezdése az üzemeltetői szerződésben meghatározott időn belül; – Hibabejelentő tájékoztatása a hiba elhárításának várható határidejéről, a hibajavítás folyamatáról, illetve a felhasználó, esetleg a hálózatgazda szükséges közreműködéséről; – Felhasználó által elhárítható hiba esetén egyeztetés a felhasználóval a hiba elhárításáról, szakmai irányítás; – Hibaelhárítás, problémamegoldás folyamatának követése, hibajegy vezetése, lezárása; – Tartalék eszközkészlet feltöltésének kezdeményezése a hálózatgazda felé; – Részvétel beérkező tartalék eszközök szállítótól történő átvételében; – Nyilvántartás vezetése a tartalékeszközök felhasználásáról;

Alany	Jogok	Feladatok, felelősségek
		– Felhasználók és hálózatgazda tájékoztatása a hiba elhárításáról; – Az EKG adatforgalmának mérése, Havi jelentés és – szükség esetén – Sávszélesség Módosítási Javaslat készítése, megküldése a hálózatgazda részére; – Hálózati beállítások módosítása a szolgáltatás módosítás esetén, az együttműködési megállapodásnak megfelelően; – Szükség esetén a megszüntetést követő változtatásokra való felkészülés tervezése; – A megszüntetés technikai lebonyolítása a felhasználóval együttműködésben; – Közreműködés az EKG-EuroDomain kapcsolat kiépítésében; – Az EKG oldali hálózati paraméterek beállítása – az EKG felhasználó és az EU adminisztrációs partnerintézmény között létrejött együttműködési megállapodás alapján; – Hosting szolgáltatás igénybevételével kapcsolatos technikai specifikáció kidolgozása; – Szabályzat vagy szabályzatmódosítási koncepció kialakításában vagy tervezet kidolgozásban részvétel vagy véleményezés; A végleges szabályzat bevezetése; – A fejlesztés lebonyolítása – saját hatáskörben történő fejlesztés esetén; – A kivitelezés szakmai követése és műszaki átvétele – külső fejlesztés esetén; – Rendelkezésre állás a fejlesztések technikai egyeztetése céljából, a hálózatgazda felkérésére; – A tervezett karbantartási időpontok kialakítása; – A hálózatgazda és a felhasználók tájékoztatása az üzemeltetői szerződésben meghatározott időszakon kívül eső tervezett és rendkívüli karbantartási feladatokról; – Részvétel a beszerzési eljárásban, az eszközök és szállítók kiválasztásában – igény szerint; – Beszerzett eszközök átvétele, elhelyezése és tárolása; – Karbantartási feladatok végrehajtása, dokumentálása; – A tartalék eszköz – szint kritikus érték alá való csökkenése esetén beszerzési eljárás kezdeményezése a hálózatgazda felé; – Üzemeltetői jelentések összeállítása és megküldése a hálózatgazdának; – Adatforgalmi kimutatás elkészítése; – A kommunikációs terv megvalósításában való közreműködés a hálózatgazda utasítása szerint.
EuroDomain szolgáltató	– EKG Audit	– Megbízás EKG auditra (auditor cég megbízása), majd ezt követően visszajelzés az audit eredményéről a hálózatgazdának; – Az EKG megfelelősége esetén az EuroDomain-EKG kapcsolathoz szükséges összeköttetés kiépítése és kódoló eszközök telepítése; – Az EuroDomain-oldali hálózati paraméterek beállítása, az EKG felhasználó és az EU adminisztrációs partnerintézmény között létrejött együttműködési megállapodás alapján.
EU adminisztrációs partner		– Az érintett EU szolgáltatók értesítése a magyar felhasználó intézmény és az EU adminisztrációs partner közötti együttműködésről – az együttműködési megállapodás megküldésével.

A Kormány 223/2009. (X. 14.) Korm. rendelete az elektronikus közszolgáltatás biztonságáról

A Kormány az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény 31. § (2) bekezdés b) pontjában foglalt felhatalmazás alapján, az Alkotmány 35. § (1) bekezdés b) pontjában meghatározott feladatkörében eljárva a következőket rendeli el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

A rendelet hatálya

1. § (1) E rendelet hatálya az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, az elektronikus közszolgáltatások nyújtásában részt vevő szervezetekre és személyekre, valamint az elektronikus közszolgáltatások igénybe vevőire terjed ki.

(2) Minősített információt kezelő rendszerekben az itt rögzítetteken túlmenő, a tárgykört szabályozó külön jogszabályokban foglaltak alkalmazása is szükséges.

(3) Amennyiben törvény felhatalmazása alapján jogszabály az elektronikus közszolgáltatás nyújtására informatikai biztonsági követelményt ír elő, az elektronikus közszolgáltatás informatikai biztonsági követelményei tekintetében a külön jogszabályban foglaltak alkalmazása is szükséges.

Értelmező rendelkezések

2. § E rendelet alkalmazásában:

a) *adatkezelő:* a kormány által az elektronikus közszolgáltatásról szóló törvény (a továbbiakban: Ekszt.) felhatalmazása alapján az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben a központi rendszerben kezelt adatok kezelésére kijelölt közigazgatási szerv;

b) *audit:* a szervezet, illetve meghatározott program, szolgáltatás vagy alkalmazás folyamataira vonatkozó menedzsment- és üzemeltetési biztonsági intézkedések szabványokban, ajánlásokban, illetve a nemzetközi legjobb gyakorlatokban leírt elvárásoknak való megfelelőségének vizsgálata, és a megfelelés, illetve meg nem felelés tanúsítása;

c) *értékelés:* a hardver eszközök, hálózatok, az ezekből kialakított komplex informatikai rendszerek, és az ezek működtetését, üzemeltetését végző szervezet biztonsági intézkedéseinek, kialakított eljárásrendjeinek Magyarországon elfogadott technológiai értékelési szabványok, követelményrendszerek és ajánlások szerinti megfelelőségi vizsgálata;

d) *felhasználó:* az elektronikus közszolgáltatást igénybe vevő szerv vagy személy;

e) *információbiztonsági fenyegetés:* mindazok az események, amelynek bekövetkezése esetén a rendszerhez fűződő érzékeny információk jogosulatlanul kerülnek más birtokába, vagy válnak megismerhetővé, vagy válnak elérhetetlenné, vagyis sérülnek az e rendeletben megfogalmazott adat- és információbiztonságra meghatározott követelmények;

f) *kritikus infrastruktúra:* olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózata, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában, és ezért meg kell felelniük az alapvető biztonsági, nemzetbiztonsági követelményeknek;

g) *működtető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, az elektronikus közszolgáltatás megvalósítását a központi elektronikus szolgáltató rendszeren lehetővé tevő, a közszolgáltatásokat összehangoló közigazgatási szerv;

h) *szervezet:* valamennyi jogi személyiséggel rendelkező és jogi személyiséggel nem rendelkező jogképes szervezet, valamint az egyéni vállalkozás;

i) *titkosító kulcspár:* a központi rendszerben végzett azonosításról szóló kormányrendeletben meghatározott információvédelmi eszköz;

j) *üzemeltető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, a központi rendszer elemeinek létrehozását, fejlesztését és üzemeltetését a működtető irányításával – szükség esetén más szervezetek bevonásával – közszolgáltatási szerződés keretében ellátó, a rendszer, mint egész működőképességét biztosító szervezet.

II. FEJEZET
AZ INFORMATIKAI BIZTONSÁG IRÁNYÍTÁSA

Az elektronikus közszolgáltatás biztonsági alapkövetelményei

3. § (1) A központi rendszer a kritikus infrastruktúra része, védelmét a kritikus infrastruktúrára vonatkozó, nemzetközileg kialakult biztonsági követelményeknek megfelelően kell kialakítani.

(2) A kritikus infrastruktúra követelményeinek érvényesítésétől csak olyan elektronikus közszolgáltatást nyújtó rendszerek esetében lehet eltérni, ahol a folyamatos rendelkezésre állás hiánya nem veszélyezteti az államszervezet működését, leállása nem terheli túl a központi rendszert, illetve nem okozza pótolhatatlan adatok elvesztését vagy regisztrálásának elmaradását.

(3) Az elektronikus közszolgáltatást nyújtó rendszernek biztosítania kell:

a) a rendszerben található adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása az adatkezelést szabályozó törvényi előírások betartásával történjen (törvényes adatkezelés);

b) a rendszerben kezelt adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhessék meg, használhassák fel, illetve rendelkezhessenek a felhasználásáról (bizalmasság);

c) a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek – ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás megtörténtének bizonyosságát is –, továbbá a rendszerelemek a rendeltetésüknek megfelelően használhatóak legyenek (sértetlenség);

d) a rendszerben kezelt adatokat, illetve az informatikai rendszer elemeit az arra jogosultak a szükséges időpontban és időtartamra használhassák (rendelkezésre állás);

e) érvényesüljön a zárt, teljes körű, folytonos és a kockázatokkal arányos védelem

ea) *zárt védelem:* az összes releváns fenyegetést figyelembe vevő védelem,

eb) *teljes körű védelem:* a rendszer valamennyi elemére kiterjedő védelem,

ec) *folytonos védelem:* az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelem,

ed) *kockázattal arányos védelem:* egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

(4) Elektronikus közszolgáltatás csak az Ekszt. 30. §-ában rögzített tanúsítás megléte, és annak bejelentése esetén folytatható (a továbbiakban: biztonságos informatikai rendszer).

Felelősségi viszonyok

4. § (1) Ha egy elektronikus közszolgáltatást nyújtó rendszer (alrendszer) működtetője szolgáltatását biztonságos informatikai rendszer útján teszi elérhetővé a felhasználók számára, akkor szolgáltatása részeként köteles az eljárási és biztonsági követelmények megismertetéséről – az irányítása alá tartozók esetében elsajátításáról, teljesítéséről – is gondoskodni.

(2) Az elektronikus közszolgáltatást nyújtó rendszer (alrendszer) működtetőjének biztosítania kell, hogy a rendszer belső és külső használói, valamint a külső szolgáltatók tudatában legyenek a rendszerrel szembeni információbiztonsági fenyegetéseknek.

(3) Az elektronikus közszolgáltatást nyújtó, működtető szervezet vezetője köteles biztosítani, hogy az informatikai rendszer az eljárási és biztonsági követelményeknek megfeleljen, függetlenül attól, hogy az üzemeltetést részben vagy egészben harmadik személy végzi.

(4) Az üzemeltető a fokozott veszéllyel járó tevékenység szabályai szerint felelős azért, hogy a működtetőt valamennyi lehetséges kockázatról haladéktalanul tájékoztassa, illetve azok megszüntetéséért, csökkentéséért mindent megtegyen.

(5) E felelősség alól csak akkor mentesül, ha megfelelően dokumentált jelzése ellenére a működtető nem intézkedett időben a probléma megoldására.

(6) Az eljárási és biztonsági követelményeknek való megfelelés nem érinti az elektronikus közszolgáltatást nyújtó szervezet azon kötelezettségét, hogy teljesítse a más jogszabályokban meghatározott követelményeket.

Az informatikai biztonsági felügyelet rendszere

5. § (1) Az elektronikus közszolgáltatást nyújtó rendszerek informatikai biztonságának felügyeletét a közigazgatási informatikáért felelős miniszter (a továbbiakban: miniszter) látja el. A miniszter a feladat ellátására az irányítása alá tartozó informatikai biztonsági felügyelőt jelöl ki.

(2) Az informatikai biztonsági felügyelő ellenőrzi az elektronikus közszolgáltatást nyújtó rendszerek eljárási és biztonsági követelményeknek való megfelelőségét.

(3) Az informatikai biztonsági felügyelő jogosult a központi rendszer üzemeltetőjétől, adatkezelőjétől, valamint az elektronikus közszolgáltatást nyújtó, szolgáltatást nyújtó szervezetektől az eljárási és biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni, a követelményeknek való megfelelőség alátámasztásához szükséges, az elektronikus közszolgáltatást nyújtó alrendszer tervezésével, beszerzésével, előállításával, működésével vagy felülvizsgálatával kapcsolatos adatot, illetve a rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot – különösen az e rendeletben előírt dokumentációt, szabályzatokat – bekérni.

(4) Az informatikai biztonsági felügyelő hatásköre a központi rendszer működtetőjére, adatkezelőjére, üzemeltetőjére, az elektronikus közszolgáltatást nyújtó szervezetek, valamint a számukra a rendszer üzemeltetéséhez szolgáltatást nyújtó szervezetek informatikai biztonsággal összefüggő tevékenységére terjed ki.

6. § (1) Az informatikai biztonsági felügyelő e rendeletben meghatározott biztonsági követelmények érvényesítése érdekében

a) folyamatosan figyelemmel kíséri a központi rendszert üzemeltető szervezetekkel, valamint a központi rendszer számára szolgáltató szervezetekkel kötött megállapodásokban foglalt informatikai biztonsági követelmények betartását;

b) véleményt nyilvánít a központi rendszerhez csatlakozni kívánó szervezetek és szolgáltatások biztonságáról;

c) jogosult a 4. § (4) bekezdése szerint feladatkörébe tartozó szervezet informatikai biztonsággal összefüggő tevékenységének és ellátottságának ellenőrzésére;

d) jóváhagyja a központi rendszer üzemeltetője, adatkezelője biztonsági irányelveit, szabályzatait és eljárásrendjeit;

e) az arra jogosult jóváhagyását megelőzően szakmailag ellenőrzi az elektronikus közszolgáltatást nyújtó szervezetek biztonsági irányelveit, szabályzatait és eljárásrendjeit;

f) határidő tűzésével felhívja az érintett szervezetek vezetőit az ellenőrzés vagy egyéb úton tudomására jutott eltérések felszámolására, ellenőrzi a követelmények megvalósítását;

g) kapcsolatot tart a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) a biztonságos elektronikus szolgáltatásokat nyilvántartó szervezeti egységével;

h) ellenőrzi a biztonságirányítási rendszerek működtetését.

(2) A felügyelő a biztonsági, adatbiztonsági és eljárási követelmények hiányos teljesítése esetén jogosult határidő tűzésével felszólítani az érintett szervezetet a hiányosságok pótlására. A felhívás eredménytelensége esetén kezdeményezi a (4) bekezdésben rögzített eljárást.

(3) Amennyiben a feltárt vagy tudomására jutott hiányosság a központi rendszer biztonságos működését vagy a kezelt adatok biztonságát veszélyezteti, jogosult azonnali hatállyal, végrehajthatóan az elektronikus közszolgáltatást nyújtó alrendszer működését a hiba, hiányosság elhárításáig felfüggeszteni. A felfüggesztés ellen – nem halasztó hatályú kifogással – a miniszterhez lehet fordulni.

(4) Az eljárási és biztonsági követelmények felszólítás ellenére elégtelen teljesülése esetén az informatikai biztonsági felügyelő javaslatára a miniszter értesíti az érintett szervezet felügyeletét – köztestület esetén a törvényességi felügyeletet – ellátó minisztert, helyi önkormányzat esetén a Kormány általános hatáskörű területi államigazgatási szervét, kérve haladéktalan intézkedését.

Intézkedések a biztonsági hiányosságok esetén

7. § (1) Az ellenőrzés, valamint a megtett intézkedések felülvizsgálata során tapasztalt hiányosságok esetében az informatikai biztonsági felügyelő

a) kiemelt kockázatot jelentő – azaz adatvesztés, vagy adatokhoz való jogosulatlan hozzáférés veszélyét felvető – hiányosság esetén a szolgáltatást azonnal felfüggeszti,

b) az a) pontba nem tartozó kockázatot jelentő hiányosság esetén a működtetőt, és – amennyiben a hiányosság elhárítása közvetlenül az üzemeltető feladatát képezi – az üzemeltetőt határidő tűzésével a hiányosság megszüntetésére szólítja fel,

c) amennyiben a hiányosság határidőt követően is fennáll, a szolgáltatás felfüggesztéséről intézkedhet.

(2) Egy rendszerelem üzemeltetésének vagy felfüggesztett szolgáltatásának újraindítása – a hiányosságok megszüntetését követően is – csak az informatikai biztonsági felügyelő engedélyével történhet.

(3) A felfüggesztésről, valamint az újraindítási engedély kiadásáról az informatikai biztonsági felügyelő tájékoztatja a biztonságos működést regisztráló NHH-t.

(4) A szolgáltatás felfüggesztését, az erről szóló döntést követően haladéktalanul, illetve újraindítását annak pontos időpontjával és a korlátozás kiterjedésének megjelölésével a kormányzati portálon az üzemeltetési események között a kormányzati portál üzemeltetője a biztonsági felügyelő közlése alapján közzéteszi.

(5) Az üzemeltető a központi rendszer vagy az elektronikus közszolgáltatás biztonságát súlyosan fenyegető veszély vagy katasztrófa esetén köteles a katasztrófaelhárítási tervnek megfelelően eljárni, és az informatikai biztonsági felügyelőt, valamint a működtetőt erről haladéktalanul értesíteni.

Nemzeti hálózatbiztonsági központ

8. § (1) A kormány a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikáció biztonsága, a vírus- és más támadások káros hatásainak korlátozása érdekében nemzetközi együttműködéssel hálózatbiztonsági központot (a továbbiakban: Központ) működtet.

(2) A Központ nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkező, akkreditált szervezet, mely védi a központi rendszer szolgáltatásait az interneten keresztül érkező támadások ellen. Ezen feladat körében technikai védelmi, megelőző és felvilágosító tevékenységet végez, továbbá képviseli Magyarországot a nemzetközi hálózatbiztonsági és kritikus információs infrastruktúrák védelmére szakosodott együttműködési fórumokon és szervezetekben. Részt vesz az informatikai és a hálózatbiztonságra, valamint a kritikus információs infrastruktúrák védelmére vonatkozó stratégiák és szabályozások előkészítésében.

(3) A Központ a miniszter felügyelete alatt áll, működését az informatikai biztonsági felügyelő ellenőrzi.

(4) A Központ üzemeltetését a Puskás Tivadar Közalapítvány biztosítja közszolgáltatási szerződés keretében az Országos Informatikai és Hírközlési Főügyelet üzemeltetésével párhuzamosan.

(5) A Központ évente jelentést készít tevékenységéről, a potenciális veszélyforrásokról és elhárításuk lehetőségeiről, és azt a következő év február 28-ig közzéteszi.

(6) Nem tartozik a Központ tevékenységi körébe a következő kormányzati hálózatok védelme:

a) a nemzetbiztonsági szolgálatok speciális műveleti hálózatai;

b) a Honvédelmi Minisztérium által működtetett katonai műveleti hálózatok;

c) az Egységes Digitális Rádiótávközlő Rendszer;

d) a Külügyminisztérium által Magyarországon és külképviseleti viszonylatban működtetett diplomáciai információs rendszerek;

e) a Magyar Köztársaság nemzetközi kötelezettségei alapján működtetett nemzetközi hálózatok.

9. § (1) A Központ szolgáltatásai:

a) A Központ a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé magyar Nemzeti Kapcsolati Pontként (a továbbiakban: NKP), kormányzati számítástechnikai sürgősségi reagáló egységként (kormányzati CERT) működik, folyamatos rendelkezésre állással;

b) A Központ, mint NKP ellátja a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé az internetet támadási csatornaként felhasználó beavatkozások kezelését és elhárításának koordinálását;

c) A Központ, mint NKP kezeli a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé a felismert és publikált szoftver sérülékenységeket, a tudomására jutott szoftver sérülékenységeket honlapján, www.cert-hungary.hu magyar nyelven publikálja, illetve a nemzetközi hálózat felé biztosítja a magyar szoftver-sérülékenységekről az angol nyelvű információt;

d) A Központ – a központi rendszer üzemeltetőjétől a központi rendszer működtetője felhatalmazásával átvett információk és adatok alapján – folyamatosan megfigyeli és kiértékeli az internet forgalmat beavatkozásra utaló jeleket keresve, továbbá a folyamatos ügyeleti rendszerén keresztül szükség esetén értesíti a központi rendszer működtetőjét, valamint a hazai és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezeteket a gyanús tevékenységekről.

e) A Központ képviseli és érvényesíti Magyarország érdekeit az informatikai és hálózatbiztonsági, valamint a kritikus információs infrastruktúrák védelmére irányuló nemzetközi együttműködésekben;

f) A Központ részt vesz az informatikai és a hálózatbiztonságra, valamint a kritikus információs infrastruktúrák védelmére vonatkozó stratégiák és szabályozások előkészítésében.

(2) A Központ tevékenységei:

a) A Központ oktatási anyagokat dolgoz ki és tréningeket tart, felvilágosító, szemléletformáló kampányokat szervez, továbbá a tudatosságot növelő honlapot alakít ki és tart fenn az interneten;

b) A Központ együttműködik a magyar informatikai és hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmében érintett bűnüldöző szervekkel, akadémiai és iparági szereplőkkel, ennek keretében gyakorlatokat tart és munkacsoportokat működtet, illetve azokban részt vesz.

10. § (1) A Központ a központi rendszer használói és működtetői számára a 9. § (1) bekezdésében meghatározott szolgáltatásokat a közszolgáltatási szerződés keretében, további díjazás nélkül biztosítja.

(2) A Központ a 9. §-ban foglalt feladatainak maradéktalan ellátása mellett jogosult külön szerződésben meghatározott módon, díjazás ellenében további emelt szintű szolgáltatásokat is nyújtani, mind a központi rendszer használói és működtetői, mind a kritikus információs infrastruktúrával rendelkező szervezetek számára. E tevékenységet egyértelműen el kell különíteni a közszolgáltatási tevékenységtől.

III. FEJEZET
A BIZTONSÁGOS MŰKÖDÉS ALÁTÁMASZTÁSA, MINŐSÉGIRÁNYÍTÁSI KÖVETELMÉNYEK

11. § (1) Az elektronikus közszolgáltatást nyújtó szervezetnek a központi rendszeren keresztül szolgáltatást nyújtó rendszer tervezésére, beszerzésére, megvalósítására (különösen fejlesztésére, testreszabására, paraméterezésére, telepítésére) és felülvizsgálatára kiterjedő, az e §-ban meghatározott feltételeknek megfelelő minőségirányítással kell alátámasztania az eljárási és biztonsági követelmények teljesülését.

(2) A minőségirányítás alapjául szolgáló dokumentációnak alkalmasnak kell lennie arra, hogy az eljárási és biztonsági követelményeknek való megfelelőséget bemutassa. A dokumentációt a biztonsági ellenőrzést végezni jogosultak rendelkezésére kell bocsátani.

(3) Amennyiben az elektronikus közszolgáltatást nyújtó szervezet a szolgáltatásnyújtással összefüggő egyes feladatait – ideértve az üzemeltetést is – közreműködő igénybevételével látja el, a saját dokumentáció helyett csatolhatja a feladatot ellátó közreműködő szervezet vonatkozó dokumentációját, azonban annak a (4) bekezdésben meghatározott követelmények szerinti teljességéért való felelőssége ez esetben is fennáll.

(4) A minőségirányítás alapjául szolgáló dokumentáció

a) a tervezéssel összefüggésben:

aa) meghatározza az előállítandó informatikai célrendszer terveivel kapcsolatos, az eljárási és biztonsági követelmények teljesítését biztosító funkcionális és alkalmassági követelményeket, valamint a tervezés folyamata során és annak befejezésekor elvégzendő ellenőrzéseket és vizsgálatokat,

ab) összefoglaló jelleggel rögzíti az aa) pontban meghatározott egyes ellenőrzések és vizsgálatok eredményét;

b) az egyes elemeinek beszerzésével összefüggésben:

ba) a beszerzést megelőzően rögzíti az eljárási és biztonsági követelmények teljesítését biztosító beszerzési követelményeket, meghatározza a kiválasztás és kiértékelés feltételeit,

bb) kialakítja és alkalmazza azokat az ellenőrzési tevékenységeket, amelyek biztosítják, hogy a beszerzés tárgya megfeleljen az előírt követelményeknek;

c) a rendszer kialakításával összefüggésben:
   ca) munkafolyamatba építve meghatározza a rendszernek az előállítás és a végellenőrzés során ellenőrizendő és vizsgálandó, az eljárási, adatbiztonsági követelmények teljesítését biztosító követelményeit,
   cb) a végellenőrzéshez dokumentálja – amennyiben az előírt – a rendszer hatósági elfogadásának feltételeül előírt követelmények teljesülését,
   cc) rögzíti az egyes ellenőrzések és vizsgálatok eredményét úgy, hogy az alkalmas legyen az előírt – különösen az eljárási, adatbiztonsági – követelmények teljesítésének megítélésére;
d) szabályozza a rendszer elkészülte utáni változáskezelés, rendszeres időközönkénti felülvizsgálat eljárásrendjét, az eljárási, adatbiztonsági és biztonsági követelményeknek való megfelelőség igazolásának módját;
e) igazolja a minőségirányítási rendszer alkalmasságát, teljeskörűségét.

(5) Ha az elektronikus közszolgáltatást nyújtó szervezet olyan, a vonatkozó MSZ ISO/IEC szabványok szerinti, független, erre feljogosított tanúsító szervezet által tanúsított minőségirányítási rendszert működtet, amely az (1) bekezdésben meghatározott területekre, valamint az eljárási és biztonsági követelmények teljesítésére is kiterjed, és azt a rendszer elkészülte utáni audit-jelentéssel igazolja, vélelmezni kell, hogy a minőségirányítással kapcsolatos követelmények e minőségirányítási rendszer útján teljesülnek.

12. § (1) Az elektronikus közszolgáltatást nyújtó szervezet vezetője gondoskodik a 11. § szerinti minőségirányítási dokumentációban foglaltak betartásáról, betartatásáról.

(2) Ha az elektronikus közszolgáltatást nyújtó rendszerre vonatkozó jogi, adatvédelmi vagy biztonsági követelmények megváltoznak, a rendszer (alrendszer) működtetőjének a változás, az új szabályozás ismertté válásától számított 90 napon belül kell gondoskodnia a minőségirányítási dokumentáció módosításáról.

Dokumentáltsági, személyügyi követelmények

13. § (1) Az elektronikus közszolgáltatást működtető szervezetnek – szükség esetén az üzemeltető bevonásával – az elektronikus közszolgáltatási biztonsági minimum követelmény teljesítéséhez legalább a következő informatikai biztonsági követelményeket kell kielégítenie:
a) rendelkezni kell üzemeltetési, valamint informatikai biztonsági szabályzatokkal;
b) üzletmenet-folytonossági, katasztrófaelhárítási tervvel kell rendelkezni a kritikus információkat tartalmazó erőforrások rendkívüli helyzetekben technikailag elérhető folyamatos rendelkezésre állásának biztosítása érdekében;
c) a tárolt és kezelt adatok biztonsága érdekében az elektronikus szolgáltatásra vonatkozóan szolgáltatásműködési szabályzatot kell készíteni, amelyben meg kell határozni a rendszer működéséért felelős, az adatgazda, az adatkezelő, illetőleg az adatfeldolgozó, az üzemeltető és az igénybe vevők jogait és kötelezettségeit, valamint az adatkezelés, adattovábbítás és adatszolgáltatás eljárásrendjét;
d) az elektronikus közszolgáltatás keretében az informatikai rendszerben forgalmazott adatok illetéktelen személy által történő megismerhetőségének megakadályozását elektronikus úton kell biztosítani az adatok keletkezési helyétől azok végső tárolási helyéig bezárólag, beleértve az adatok nyilvános hálózaton történő forgalmazását is;
e) az elektronikus közszolgáltatás keretében gyűjtött, illetőleg keletkezett adatok – személyes adatok tekintetében az adatkezelésre vonatkozó jogszabályi rendelkezésre is figyelemmel – kizárólag a szolgáltatás igénybevételére vonatkozó szerződésben meghatározott esetekben, illetőleg – kizárólag műszaki – hibajavítás céljából, minden esetben dokumentált módon, az annak végrehajtására jogosult személy azonosítása mellett és a változások nyomon követésének, szükség esetén visszaállíthatóságának biztosításával módosíthatók;
f) az elektronikus közszolgáltatás informatikai rendszereinek (alrendszereinek) módosítása előzetesen jóváhagyott változáskezelési szabályzat alapján, az abban foglalt eljárásrend betartásával állítható éles üzembe, melynek során a szoftver összetevőinek változásait verziószámmal és az éles alkalmazásba vétel dátumával ellátva elektronikus adathordozón külön jogszabályban meghatározott ideig, de legalább az elektronikus közszolgáltatás vagy alkalmazás használatának megszüntetését követő öt évig archiválni kell.

(2) Az elektronikus közszolgáltatási biztonsági minimum követelmények teljesülésének igazolására a működtető köteles az elektronikus közszolgáltatást informatikai biztonsági szempontból auditáltatni, illetőleg üzemeltető köteles az elektronikus közszolgáltatáshoz kapcsolódó informatikai rendszert és háttérrendszert informatikai biztonsági szempontból értékeltetni.

(3) Az elektronikus közszolgáltatás működtetőjének belső szabályzatban kell kijelölnie
a) az egyes informatikai biztonsági követelmények teljesítése érdekében ellátandó feladatokat és azok felelőseit,
b) az egyes informatikai biztonsági döntési jogköröket, és azokat, melyek gyakorlásához előzetes döntés szükséges,
c) a rendszer biztonságos működtetéséhez szükséges eszközök rendelkezésre állásáért, folyamatok megvalósulásért felelős vezető személyét,
d) a rendszer használatával kapcsolatos hatásköröket (jogosultsági szinteket),
e) az informatikai biztonsági felelős kiválasztásának módját,
f) a rendszer működtetése szempontjából kritikus feladatköröket, amelyek esetében a 14. § (2) bekezdését kell érvényesíteni.

14. § (1) Az elektronikus közszolgáltatást nyújtó rendszernek rendelkeznie kell
a) a rendszer felépítésére és működésére vonatkozó, naprakész igazgatási, informatikai és üzemeltetési dokumentációkkal, belső utasításokkal és a külső felhasználók számára módszertani segédletekkel,
b) a rendszerben tárolt és feldolgozott adatok tárolási szerkezetének és szintaktikai feldolgozási szabályainak leírásával, a személyes adatok kezelésére vonatkozó adatvédelmi szabályzattal, valamint az adatok kezelésére vonatkozó adatbiztonsági követelményrendszerrel és eljárásrenddel,
c) a rendszer funkcióihoz, az adatokhoz történő hozzáférési (jogosultsági) rend meghatározásával.

(2) A szolgáltatást nyújtó szervezet belső szabályzatában határozza meg az informatikai rendszer üzemeltetésével és ellenőrzésével kapcsolatos egyes munkakörök betöltéséhez szükséges alkalmazási feltételeket és más személyi biztonsági követelményeket. A rendszer működtetése szempontjából kulcsfontosságú, az adatokhoz hozzáférést biztosító munkakörök esetében a fontos és bizalmas munkakörökre vonatkozó követelményeket is – az erre vonatkozó jogszabályban meghatározott garanciális szabályok és eljárásrend szerint – érvényesíteni kell.

(3) Az elektronikus közszolgáltatást nyújtó szervezet vezetője a szolgáltatást működtető szervezeti egységétől független, a közszolgáltatást nyújtó szervezet vezetőjének közvetlen irányítása alá tartozó informatikai biztonsági felelőst jelöl ki, aki személyesen felel a biztonsági követelmények betartásáért. Az informatikai biztonsági felelős e feladatának ellátása körében más vezető által nem utasítható. Amennyiben az informatikai biztonsági felelős – álláspontja szerint – az elektronikus közszolgáltatást nyújtó rendszer biztonságát veszélyeztető utasítást kap, haladéktalanul köteles arról az informatikai biztonsági felügyelőt tájékoztatni, és intézkedését kérni.

(4) Az elektronikus közszolgáltatást nyújtó szervezet vezetője az e szolgáltatást nyújtó rendszer (alrendszer) működtetéséért önállóan felelős személyt nevez ki, valamint kijelöli a kezelt adatok biztonságos tárolásáért felelős szervezeti egységet.

(5) Az elektronikus közszolgáltatást nyújtó szervezet:
a) évente felülvizsgálja a biztonsági irányelveket, a biztonsági szabályzatokat és eljárásrendeket,
b) a szolgáltatással kapcsolatos szervezeti és műszaki változások, illetve biztonsági esemény esetén saját hatáskörben soron kívüli felülvizsgálatot valósít, valósíttat meg, és
c) az a) pont szerinti dokumentációkat, illetve a b) pont szerinti módosított szabályozási tervezetet jóváhagyásra megküldi az informatikai biztonsági felügyelőnek.

(6) A szolgáltatással kapcsolatos szervezeti és műszaki változások esetén, amennyiben az a központi rendszer terhelését érinti, az elektronikus közszolgáltatást nyújtó szervezet külön felhívás nélkül köteles a változásról a központi rendszer működtetőjét előzetesen tájékoztatni. Amennyiben a változás veszélyezteti a központi rendszer egészének működési biztonságát, a központi rendszer működtetője jogosult a változtatást megakadályozni vagy feltételhez kötni. A változás megvalósításának feltétele az elektronikus közszolgáltatások működtetéséről szóló kormányrendelet szerinti együttműködési megállapodás előzetes módosítása, amennyiben a módosítás érinti a rendszer biztonságát.

(7) Az elektronikus közszolgáltatást nyújtó szervezet – a biztonsági követelmények teljesítésének ellenőrzéséhez – a központi rendszer működtetőjének megkeresésére a forgalomról, az alkalmazott hardver és szoftver, valamint biztonsági megoldásokról, eljárásrendekről, szervezeti intézkedésekről adatot szolgáltat.

A folyamatok naplózása

15. § (1) A szolgáltatást nyújtó szervezet az általa működtetett rendszerben vagy annak környezetében vagy mindkettőben gondoskodik a rendszer működése szempontjából meghatározó folyamatok valamennyi kritikus eseményének naplózásáról.

(2) A szolgáltatást nyújtó szervezet a naplózandó események körét, a napló adattartalmának megőrzési idejét – a vonatkozó jogi szabályozás alapján, az adott eljárási cselekmény biztonsági jellegére, érzékenységére tekintettel – határozza meg. A megőrzési időn belül a megbízhatóság megítéléséhez szükséges mértékben valamennyi, az eljárási cselekménnyel kapcsolatos eseménynek rekonstruálhatónak kell lennie. Naplózni kell minden személyes adat továbbítását.

(3) A naplóállomány bejegyzéseit védeni kell az arra jogosulatlan személy általi hozzáféréstől, módosítástól, törléstől, illetve biztosítani kell, hogy a napló tartalma a megőrzési időn belül a jogosult számára megismerhető és értelmezhető maradjon.

(4) A naplóállományokat a 16–17. §-ban szabályozott mentési rendnek megfelelően, a maradandó értékű dokumentumokra vonatkozó szabályok szerint kell tárolni, hogy egy esetleges lokális károsodás ne tegye lehetetlenné a bizonyítást.

(5) A naplóállományok megőrzési idejét – a (2) bekezdésben foglaltak figyelembevételével – a vonatkozó iratkezelési szabályzatok részeként kell meghatározni. A működtető a vonatkozó jogszabály, illetve iratkezelési szabályzat rendelkezésétől függően, a megőrzési határidő lejártával gondoskodik a naplóállományok adathordozóinak levéltári őrizetbe adásáról vagy az adatállományok dokumentált, visszaállítást kizáró megsemmisítéséről.

A mentés és archiválás rendje

16. § (1) Az elektronikus közszolgáltatást nyújtó rendszer működtetőjének a rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan mentési renddel és biztonsági mentésekkel kell rendelkeznie, amelyek biztosítják, hogy az érintett szolgáltatás működése a biztonsági követelményeknek megfelelő helyreállítási időn belül helyreállítható, az éppen folyamatban lévő eljárás, eljárási cselekmény a biztonsági követelményeknek megfelelő helyreállítási időn belül helyreállítható, folytatható legyen. A biztonsági mentéseknek biztosítaniuk kell azt is, hogy a már lefolytatott eljárások, eljárási cselekmények az adott eljárásra vonatkozó követelmények szerint rekonstruálhatóak legyenek.

(2) A mentési rend meghatározza a mentések típusát, módját, a visszatöltési és helyreállítási tesztek rendjét, valamint a mentési eljárásokat.

(3) A mentéseket azok tartalmától függően kockázati szempontból elkülönítetten, az üzletmenet-folytonossági tervben előírt esetben tűzbiztos módon kell tárolni.

17. § (1) Az eljárási cselekmény jellegének megfelelően a rendszer működtetője az üzemi rendszertől műszakilag független, területileg elkülönült, megfelelő biztonsági szaktudással és infrastruktúrával rendelkező szervezetnél köteles biztonsági másolatot elhelyezni olyan nyilvántartásairól, amelyeket papír alapon (eredetiben vagy másolatban) nem őriz meg.

(2) Az (1) bekezdés szerint szükséges biztonsági másolatok kezelése során az adatok elhelyezését és tárolását olyan dokumentáltsággal és módon kell végezni, amely a rendszer teljes megsemmisülése esetén is lehetővé teszi a nyilvántartás azonos funkcionalitású, és lehetőség szerinti legteljesebb adattartalmú újbóli rövid idő alatt történő kialakítását.

(3) A biztonsági őrzés során gondoskodni kell arról, hogy az adatokat az arra jogosult személyen kívül más ne ismerhesse meg, valamint biztosítani kell az adatok jogosulatlan személy általi megsemmisítése, megváltoztatása vagy hozzáférhetetlenné tétele elleni védelmét mind a szervezeten belülről, mind a szervezeten kívülről jövő informatikai és más támadások esetén.

A felhasználók problémáinak kezelése

18. § (1) Az elektronikus közszolgáltatást nyújtó szervezetnek a felhasználók számára – önállóan vagy a központi rendszerrel megállapodás alapján együttműködve – folyamatosan (7-szer 24 órában) rendelkezésre álló, legalább telefonon és interneten elérhető hibakezelési, támogatási hátteret kell biztosítania. Amennyiben a rendszernek belső felhasználói (ügyintézői) vannak, számukra a tényleges használat időszakában kell szakmai és informatikai támogatást biztosítani.

(2) Munkaidőn kívül – megállapodás alapján – a felhasználói hibakezelési, támogatási hátteret az ügyfélvonal biztosíthatja.

(3) A felhasználói támogatásnak mind a szolgáltató által rendelkezésre bocsátott alkalmazás, mind a központi rendszer ehhez felhasznált elemeivel kapcsolatos műszaki, igazgatási, adatkezelési, adatbiztonsági vonatkozásokra is ki kell terjednie.

(4) A felhasználói támogatásnak valós idejű információt kell nyújtania a rendszer állapotáról, terheléséről, válaszidejéről.

(5) A felhasználói, ügyfélszolgálati támogatás elsődleges csatornája a központi ügyfélszolgálat (a továbbiakban: ügyfélvonal). Ennek megfelelően az elektronikus közszolgáltatást nyújtónak a szolgáltatás indítását megelőzően meg kell állapodnia az ügyfélvonal üzemeltetőjével az információszolgáltatás, illetve az információkérés rendjéről.

(6) Az ügyfélvonalon túli támogatás elérhetőségét a szervezet honlapján, az ügyfélszolgálati irodákban és a kormányzati portálon is hozzáférhetővé kell tenni.

Az üzemeltetés kiszervezésével kapcsolatos speciális követelmények

19. § (1) Ha az elektronikus közszolgáltatást biztosító rendszer üzemeltetését harmadik személy végzi, ideértve a rendszer által ellátandó egyes feladatok kiszervezését is, e harmadik személlyel kötött szerződésben biztosítani kell az e rendeletben foglalt ellenőrzési jogosultságok gyakorlását, illetve a működtetőre és üzemeltetőre vonatkozó kötelezettségek teljesítését is.

(2) A szerződésnek biztosítania kell, hogy minden, a rendszer működtetőjével szemben jogszabályban megfogalmazott követelmény az üzemeltető harmadik személy útján is azonos módon teljesüljön.

(3) A rendszer működtetője bármikor igényelheti az adatkezelésébe tartozó, a rendszerben tárolt adatok akár egy meghatározott egyedre vonatkozó, akár részbeni, akár teljes körű átadását a szerződésben meghatározott formátumban. Az igényt legkésőbb 10 munkanapon belül kell teljesíteni, és az adatátadás nem köthető külön díj fizetéséhez a közvetlen költségek megtérítésén túlmenően.

(4) Ha a működtető az üzemeltetés kiszervezése során valamely feladatot olyan harmadik személy által nyújtott szolgáltatás igénybevételével lát el, amelyet a harmadik személy más adatkezelő vagy adatfeldolgozó szervezet számára is nyújt, a szerződésben ki kell kötni, hogy megfelelő műszaki és személyi feltételekkel kell biztosítani a különböző adatállományok elkülönítését, illetve azt, hogy a különböző szervezetek által kezelt adatok jogosulatlan összekapcsolására ne kerülhessen sor.

(5) A kiszervezésre irányuló szerződésben rendelkezni kell az üzemeltetés kiszervezésének megszűnésekor követendő visszavételi eljárásról. A kiszervezés megszüntetése után a korábbi üzemeltetőnek az üzemeltetés során átvett és a rendszereiben tárolt adatokat – megfelelő dokumentálás mellett – haladéktalanul véglegesen, visszaállításra alkalmatlan módon meg kell semmisítenie.

IV. FEJEZET
BIZTONSÁGI KÖVETELMÉNYEK

Védelem a biztonsági kockázatokat jelentő adatoktól

20. § (1) A központi rendszerhez csatlakozott szervezetnek biztosítania kell az informatikai rendszere elégséges, az adatok, illetve a rendszer besorolása alapján meghatározott kockázattal arányos védelmét a számítógépes vírusokkal és más rosszindulatú programokkal – amelyek a rendszer működését vagy az adattartalom integritását veszélyeztetik (a továbbiakban: vírus) – szemben, valamint gondoskodnia kell arról, hogy a rendszer által küldött üzenetek ne tartalmazzanak ilyen programokat.

(2) Amennyiben az elektronikus közszolgáltatást nyújtó vagy a központi rendszerhez csatlakozott szervezet tudomására jut, hogy a saját rendszerében rosszindulatú program fordulhat elő, vagy vírus előfordulásának gyanúja merül fel, haladéktalanul tájékoztatja a központi rendszer üzemeltetőjét, és együttesen – szükség esetén az informatikai biztonsági felügyelő bevonásával – a 7. §-ban foglalt eljárásrendben döntenek a szükséges lépésekről. A hibaelhárítással párhuzamosan, a nagyobb kár elhárításának elősegítése érdekében tájékoztatni kell a központi rendszer helpdesk szolgáltatását is.

(3) Az elektronikus közszolgáltatást nyújtó szervezet által biztosított közszolgáltatások igénybevételéhez szükséges vagy azt elősegítő programot csak megfelelő vírusellenőrzés és a kód változatlanságát ellenőrző eljárás beépítése mellett szabad a felhasználóknak átadni.

(4) A központi rendszer kialakításakor megfelelő védelmet kell biztosítani az olyan, dokumentumokkal, adatcsomagokkal szemben, amelyek azért jelentenek biztonsági kockázatot, mert tömeges küldésük-fogadásuk révén az informatikai

rendszer üzemelését vagy egyes felhasználók hozzáférését akadályozhatják (kéretlen tömeges üzenetek elleni védelem).

Az adattovábbítás bizalmasságának támogatása

21. § (1) Közvetlen adatbázis kapcsolatra épülő, személyes adatokat is tartalmazó adatszolgáltatást vagy adattovábbítást az elektronikus közszolgáltatást nyújtó – a jogszabályi, adatvédelmi feltételek teljesülése esetén is – csak úgy valósíthat meg, ha megfelelő biztonságos csatornát (titkosítási, védelmi eljárást) használva megakadályozza az elektronikus dokumentum illetéktelenek általi megismerését.

(2) Az elektronikus közszolgáltatást nyújtó biztosítja, hogy a naplózott, az írásbeliség követelményeinek megfelelő, párbeszédes, elektronikus üzenetekre épülő elektronikus ügyintézés során a részére küldött üzenetet megfelelő rejtjelezési eljárással továbbítsák nyilvános adathálózaton.

(3) Amennyiben a felhasználó a szolgáltatást nyújtóval párbeszédre épülő kapcsolatot folytat, és a központi rendszer által biztosított, a szolgáltatók számára hozzáférhető kulcstárban letétbe helyezi nyilvános titkosító kulcsát, a szolgáltatást nyújtó – igény esetén – köteles az igénybe vevőnek szóló üzenetet titkosítva megküldeni.

(4) Az elektronikus közszolgáltatást nyújtó és az azt igénybe vevő egyaránt felelős a saját titkosító magánkulcsa biztonságos és más számára hozzáférhetetlen megőrzéséért. A kulcs bizalmasságának sérülése esetén saját költségére és felelősségére kell azt kicserélnie. Az elektronikus közszolgáltatást nyújtó köteles a titkosító kulcsa bizalmasságának sérüléséből származó, a felhasználónak okozott, bizonyított kárt megtéríteni.

(5) Az elektronikus közszolgáltatást nyújtó olyan biztonságos kulcstároló, letéti rendszert köteles saját magán titkosító kulcsa kezeléséhez kialakítani vagy igénybe venni, amely az eredetileg kijelölt kulcskezelő kiesése vagy a kulcs használt példányának sérülése esetén is biztosítja a biztonságos üzemmenetet.

(6) A központi rendszer működtetője a felhasználók és szolgáltatást nyújtók számára biztosít olyan kulcsgeneráló szolgáltatást, amellyel a biztonsági előírásoknak megfelelő kulcskezelés esetén a központi rendszeren belüli használatra elégséges biztonságú kulcspárok generálhatók.

(7) Az e §-ban meghatározott követelmények nem érintik a minősített adatok védelmével kapcsolatos, a minősített adatok kezelésére vonatkozó jogszabályban meghatározott kötelezettségeket és eljárásrendet.

A szolgáltatást nyújtó rendszer hozzáférési és fizikai biztonsága

22. § (1) A szolgáltatásra, illetve az annak alapját képező adatbázisra vonatkozóan a szükséges adatbiztonsági követelményeket a szolgáltatást nyújtó határozza meg.

(2) Ha az adatbázisban személyes adatok is kezelésre kerülnek, akkor a hozzáférést a 15. §-ban meghatározottak szerint naplózni kell, és a kezelt adatokhoz csak az arra felhatalmazott által biztosított hozzáférési jogosultsággal rendelkező, megfelelően azonosított használók (személyek és folyamatok), kizárólag a hozzáférési jogosultság keretei között férhetnek hozzá.

(3) Az elektronikus közszolgáltatást működtetőnek biztosítania kell, hogy az egyes hozzáférésre jogosultak minden esetben – más személy helyettesítésekor is – saját hozzáférési jogosultságuk keretei között és saját nevükben azonosítottként járhassanak el, és ne férhessenek hozzá más személy azonosításához vagy elektronikus aláírásához használt adatához vagy eszközéhez.

(4) A (2) bekezdésben rögzített naplózási kötelezettség alól kivételt az a felhasználó, igénybe vevő jelent, aki névtelenül, kizárólag nyilvános információhoz fér hozzá.

(5) A központi rendszer a rendszer egyes felhasználói számára megőrzött elektronikus ügyintézéssel kapcsolatos dokumentumaikhoz a hozzáférést – a törvényben biztosított kivétellel – csak az azonosítás után biztosíthatja.

(6) Jogszabályban meghatározott esetekben a hozzáférhetővé tett vagy nyilvánosságra hozott dokumentumok esetében a központi rendszer garantálja azok változatlan tartalommal történő közzé-, illetve hozzáférhetővé tételét.

23. § (1) A jogosulatlan hozzáféréstől fizikailag is védeni kell az informatikai rendszernek az informatikai biztonsági célokat szolgáló elemeit és a 15–17. §-ok szerinti naplókat, mentéseket, illetve az ezeket magukban foglaló helyiségeket.

(2) Az (1) bekezdésben említett helyiségekbe csak az erre feljogosított személyek léphetnek be. A belépésre jogosultak személyét (azonosítását), belépésének, kilépésének időpontját, a végzett tevékenységeket naplóban kell rögzíteni. A védett területen való munkavégzés nyilvántartásának rendjét az informatikai biztonsági szabályzat (illetve annak valamely részszabályzata) tartalmazza.

24. § Az elektronikus közszolgáltatást ellátó informatikai rendszernek más informatikai rendszerrel, hálózattal történő összekapcsolása esetén – az összekapcsolás jogi feltételeinek teljesítésén túlmenően – az elektronikus közszolgáltatást működtető szervezet köteles megkövetelni a kapcsolódó rendszernél is a 11. és 13. § szerinti biztonsági minimum követelmények teljesítését, és ennek erre feljogosítottak általi rendszeres értékeléssel és auditálással történő igazolását.

Az üzemeltetés biztonsága

25. § (1) Az elektronikus közszolgáltatást nyújtó alrendszer megbízható üzemeltetéséhez az elektronikus közszolgáltatást nyújtónak rendelkeznie kell

a) a rendkívüli üzemeltetési helyzetekre kidolgozott eljárásrenddel, amely lehetővé teszi a megbízható üzemmenetnek a rendszer nem működéséből származó veszteségek és a rendszer üzemképességének visszaállításához szükséges ráfordítások optimalizálásával megállapított időn belüli helyreállítását;

b) a rendkívüli helyzetekben folyamatos üzemelést biztosító tartalékberendezésekkel (hálózati, energiaellátási és egyéb tartalék, párhuzamos elemek) vagy e berendezések hiányában az ezeket helyettesítő más megoldásokkal.

(2) Az üzemeltetés során fellépő, a rendszer rendelkezésre állását csökkentő kiesések, megszakítások és más üzemzavarok esetén az elektronikus közszolgáltatást nyújtó biztosítja az elektronikus közszolgáltatás működéséről szóló kormányrendeletben rögzített tájékoztatást, és haladéktalanul intézkedik a hiányosság kiküszöbölésére.

26. § (1) Az elektronikus közszolgáltatás nyújtását biztosító szoftver és hardver rendszerelemek csak egyértelmű azonosítást és tesztelést követően vehetők használatba.

(2) Az elektronikus közszolgáltatás nyújtásához alkalmazási (éles) környezetben használt alapvető rendszerelemeket elkülönítetten kell kezelni és működtetni

a) az elektronikus közszolgáltatással össze nem függő tevékenységekhez használt eszközöktől, és

b) a fejlesztési és tesztelési környezetben használt rendszerelemektől.

(3) Az elektronikus közszolgáltatás nyújtásához használt informatikai eszközök más célra történő felhasználását megelőzően ellenőrizni kell, hogy a rendszerelemek nem tartalmaznak-e olyan adatokat, amelyek az elektronikus közszolgáltatás nyújtásával, az annak részeként kezelt adatokkal összefüggenek, és szükség esetében gondoskodni kell azok törléséről. Biztosítani kell, hogy a törölt adatoknak a más célra felhasznált rendszereken, rendszerelemeken történő visszaállítására ne legyen lehetőség.

(4) A (3) bekezdés szerinti ellenőrzést, illetve az ellenőrzés eredménye alapján végrehajtott intézkedéseket naplózni kell.

27. § Az elektronikus közszolgáltatást nyújtónak gondoskodnia kell a rendszerben felhasznált elektronikus adathordozók szabályozott és biztonságos kezeléséről, megőrzéséről, selejtezéséről és megsemmisítéséről.

V. FEJEZET
SZABÁLYOZÁSI ÉS ELLENŐRZÉSI KÖVETELMÉNYEK

Informatikai biztonsági irányítás és kockázatfelmérés

28. § (1) Az elektronikus közszolgáltatást nyújtó szervezet az informatikai rendszer informatikai biztonsági kockázatait legalább kétévenként felméri, és gondoskodik a rendszer kockázatokkal arányos védelméről a tervezés, a beszerzés, az előállítás, az üzemeltetés és a felülvizsgálat területén.

(2) Az informatikai biztonsági kockázatok feltárását, értékelését, elemzését és a szükséges védelmi intézkedések meghatározását a változáskezelési eljárásba illesztve, folyamatosan kell végezni.

(3) Az elektronikus közszolgáltatást nyújtó az e rendeletben megfogalmazott informatikai biztonsági követelmények kockázatokkal arányos teljesítésének elősegítése, valamint a követelmények teljesülése ellenőrzésének elősegítése céljából informatikai biztonsági irányítási rendszer kialakításáról gondoskodik, amelynek részeként informatikai biztonsági tervet dolgoz ki a következő tartalommal:

a) az informatikai szolgáltatást nyújtó rendszer rendszerszintű biztonsági problémáinak meghatározása;

b) biztonsági célok;

c) a fejlesztésre vonatkozó funkcionális és garanciális biztonsági követelmények;
d) az üzemeltetésre vonatkozó rendelkezésre állási, adatbiztonsági alkalmassági követelmények.

(4) Az elektronikus közszolgáltatást nyújtó szerv kidolgozza és működteti az általa üzemeltetett informatikai rendszer biztonságos működtetését felügyelő informatikai ellenőrző rendszert.

(5) Az informatikai biztonsági irányításnak az e-közszolgáltatás területén alkalmazandó alapkövetelményeinek teljesítéséhez alkalmazható megoldásokat a központi rendszer működtetője a www.ekkk.gov.hu honlapon közzéteszi. A Közigazgatási Informatikai Bizottság a biztonságirányításra vonatkozó ajánlásában szereplő követelmények teljesülése esetén a biztonságirányítására vonatkozó követelmények teljesítését vélelmezni kell.

Biztonsági osztályozás

29. § (1) Az elektronikus közszolgáltatást nyújtó szervezet az általa nyújtott szolgáltatás, illetve adatkezelés egyes elemeit biztonsági osztályokba sorolja annak alapján, hogy az érintett eljárási cselekmény a 28. § szerinti kockázatfelmérés szerint a szolgáltatás nyújtója és igénybe vevője részére milyen informatikai biztonsági kockázatokkal jár.

(2) Az eljárási cselekmény biztonsági osztályba sorolását nemzetközileg elfogadott osztályozási metodika szerint kell végezni. A fenti követelménynek megfelelő megoldásokat a működtető a www.ekk.gov.hu honlapon közzéteszi.

(3) A szolgáltatást nyújtó szervezet a biztonsági osztályba sorolást és annak az adott informatikai rendszerben a (2) bekezdésben meghatározott egyes követelményekkel összefüggő megvalósítását az informatikai biztonsági tervében megjeleníti.

(4) A biztonsági osztályba sorolásnak összhangban kell lennie – amennyiben ilyen létezik – a jogszabályokban meghatározott eljárási követelményekkel, nem okozhat a felhasználó számára a jogszabályban meghatározott kötelezettségekhez képest terhesebb eljárásrendet.

(5) Az elektronikus közszolgáltatást nyújtó kérésére az informatikai biztonsági felügyelő véleményezi az eljárási cselekmények biztonsági osztályba sorolását, valamint a biztonsági osztályba sorolás szerint az egyes informatikai biztonsági követelményeknek az adott informatikai célrendszerben történő megvalósítását, szükség esetén javaslatot tesz pontosításukra, kiegészítésükre.

Biztonságos elektronikus szolgáltatások tanúsítása és regisztrálása

30. § (1) Biztonságosnak a független, a (2) bekezdésben foglalt feltételeknek megfelelő, informatikai rendszerek, elektronikus szolgáltatások értékelésére feljogosított szervezet által auditált elektronikus szolgáltatás tekinthető. Elektronikus közszolgáltatásként kizárólag biztonságos elektronikus szolgáltatás működtethető.

(2) Az informatikai rendszer értékelésére, illetőleg az elektronikus szolgáltatás auditálására az a szervezet jogosult, amely rendelkezik

a) a Nemzeti Akkreditációs Testület (a továbbiakban: NAT), vagy valamely EGT-állam, illetve azzal e területen megállapodás alapján azonos jogállású állam akkreditációs szervezete által kiadott, az adott területen értékelés, illetve auditálás lefolytatására jogosító tanúsítvánnyal, vagy
b) más országban kiadott, a NAT vagy bármely EGT-állam akkreditációs szervezete által kiadottal azonos érvényű tanúsítvánnyal, vagy
c) az informatikai biztonság területén megfelelőségértékelő szervezetek kijelölésére feljogosított bizottság informatikai rendszer értékelésére, illetőleg az elektronikus szolgáltatás auditálására alkalmassá minősítő döntésével.

(3) Az auditált, biztonságos elektronikus szolgáltatást az NHH a szolgáltatás nyújtójának a tanúsításról szóló igazolást tartalmazó írásbeli kérelmére a szolgáltatás rövid leírásával és azonosítójelével haladéktalanul regisztrálja. A nyilvántartás tartalmazza a működtető és az üzemeltető megnevezését és elérhetőségét.

(4) A biztonságos szolgáltatások listájának a www.ekk.gov.hu honlapon történő megjelentetéséről az NHH-tól kapott információk alapján az informatikai biztonsági felügyelő gondoskodik, és ő engedélyezi a regisztráció alapján a szolgáltatás elindítását.

(5) A biztonságos elektronikus szolgáltatás nyilvántartásba vételét követően a működtető köteles a regisztrált adatokban (szolgáltatás leírása; működtető, üzemeltető megnevezése és elérhetősége) bekövetkező változásokról az NHH-t értesíteni, aki az információt közzététel céljából eljuttatja az informatikai biztonsági felügyelőnek.

(6) A biztonságos elektronikus szolgáltatásra vonatkozó audit tényét az NHH által végzett regisztrációt követően a szolgáltatás honlapján elhelyezett, erre utaló logó jelzi.

31. § (1) Az auditálást abban az esetben kell megújítani, ha a technikai eszközökben, a technológiában, az informatikai vagy biztonsági környezetben, illetve az alkalmazásban jelentős változás áll be.

(2) A megújítás szükségességéről dönthet a szolgáltató, javaslatot tehet az értékelés megújítása keretében az értékelő, és annak szükségességét az (1) bekezdésben rögzített változások valamelyike esetén előírhatja az informatikai biztonsági felügyelő is.

(3) Az auditálás és értékelés a jogszabályokban meghatározott informatikai biztonsági dokumentumok meglétére, azok tartalmi megfelelőségére, az abban foglaltak alkalmazhatóságára és gyakorlati megvalósítására terjed ki.

(4) Az informatikai biztonsági dokumentumok tartalmi követelményeit a központi rendszer működtetője a www.ekk.gov.hu honlapon közzéteszi.

32. § Az elektronikus közszolgáltatás auditálása, értékelése, annak kritikus infrastruktúra jellegére tekintettel az alapvető biztonsági, nemzetbiztonsági szempontok figyelembevételével végezhető (végeztethető) az alábbiak szerint:

a) a közbeszerzésről szóló törvény (a továbbiakban: Kbt.) alkalmazására kötelezett szervezetek az elektronikus közszolgáltatás auditálását, illetőleg értékelését végző szervezet kiválasztását az ország alapvető biztonsági érdekével összefüggő beszerzésekről szóló jogszabály rendelkezései szerint folytathatják,

b) a Kbt. hatálya alá nem tartozó, de e rendelet alapján auditálásra illetőleg értékelésre kötelezett szervezet az auditálást, illetőleg értékelést kizárólag olyan szervezettel végeztetheti, amely igazolja, hogy szerepel a nemzetbiztonsági szolgálatok által vezetett, az előzetes nemzetbiztonsági vizsgálaton átesett cégeket tartalmazó jegyzéken.

VI. FEJEZET
KÜLÖNÖS RENDELKEZÉSEK

Alkalmazásszolgáltató központokra vonatkozó speciális követelmények

33. § (1) Az elektronikus közszolgáltatást nyújtó alkalmazásszolgáltató központtól (a továbbiakban: ASP) igénybe vett elektronikus közszolgáltatás esetén a rendelet rendelkezéseit az e cím szerinti kiegészítésekkel kell alkalmazni.

(2) Az ASP-nek biztosítani kell:

a) az alkalmazásokon belül az egyes megrendelők adatainak biztonságos és egyértelmű elkülönítését;

b) az ASP és a megbízó szervezet közötti adatkapcsolatoknak biztonságos adatátviteli csatornán, külső személy által nem értelmezhető, kódolt módon történő megvalósítását;

c) kötelező, folyamatos géptermi jelenlétet, amely kizárja az illetéktelen behatolást;

d) az objektumbiztonság – elektronikus védelem, belépés-ellenőrzés a legmagasabb biztonsági osztályhoz tartozó követelményeinek betartását;

e) katasztrófa-gépterem kialakítását.

(3) Az ASP köteles a fejlesztést és üzemeltetést végző szervezeti egységektől független, az ASP-t szolgáltató szervezet vezetőjének közvetlenül alárendelt informatikai biztonsági felelőst alkalmazni.

(4) Az ASP köteles hibatűrő rendszerekhez legalább két független körös, egyenként is elégséges hűtőrendszert kialakítani, és biztosítani a kábelezés strukturált megvalósítását.

(5) Az ASP az általánosan kötelező szabályzatokon túlmenően köteles kialakítani az alábbiakat:

a) géptermi biztonsági szabályzat;

b) elektronikus levelezéssel összefüggő szabályzat;

c) vírus- és egyéb kártevők elleni védelemmel kapcsolatos szabályzat;

d) rendszer- és adathozzáférési szabályzat;

e) titkosítási szabályzat;
f) szoftverfejlesztési szabályzat;
g) mentési szabályzat.

Az elektronikus kormányzati gerinchálózat speciális biztonsági követelményei

34. § (1) A kormányzati és közigazgatási adatbázisok, informatikai rendszerek jogszabályok által lehetővé, kötelezővé tett összekapcsolása, valamint a különböző szolgáltatások elérhetőségének biztosítása az elektronikus kormányzati gerinchálózat (a továbbiakban: EKG) feladata.

(2) Az EKG, mint infrastrukturális elem – a központi elektronikus szolgáltatási rendszer egyik fő összetevőjeként – távolról is elérhetővé teszi a különféle átfogó alkalmazásokat, számítógépes külső és belső adatszolgáltatásokat, kommunikációs elemeket, amelyek ennek révén egységes egészként funkcionálnak. A központi közigazgatás szervei kizárólag az EKG-n keresztül tarthatnak egymással, illetve az EKG részét nem képező felhasználókkal elektronikus kapcsolatot.

(3) Az EKG biztosítja az egyes intézményi hálózatok között szabályozott kommunikáció, ideértve az internet alapú telefonkapcsolat (VoIP) lehetőségét. Az intézményi hálózatok közötti szabályozott kapcsolat a hálózat fizikai topológiájának megváltoztatása nélkül megvalósítható.

(4) Az EKG biztosítja intézményi hálózatok biztonságos logikai elkülöníthetőségét. E célra virtuális magánhálózatokat használ. Az a szervezet, amelynek hálózata csatlakozik az EKG-hoz, az internethez csak az EKG által biztosítottan csatlakozhat, más internetszolgáltatót e hálózat ellátására nem vehet igénybe.

(5) Az EKG és a központi közigazgatás szervei, valamint az EKG-ra már csatlakozott szervezetek között kapcsolatot az EKG szolgáltatója biztosítja. Más szolgáltató kizárólag az EKG hálózatgazdájának engedélyével vehető igénybe, amennyiben a kapcsolat biztonságos, és más módon gazdaságosan megvalósíthatatlan voltát a bevonni kívánt szolgáltató előzetesen igazolja.

(6) Az EKG alapszolgáltatásai és az EKG emelt szintű szolgáltatásai a hálózatgazda által lebonyolított beszerzési eljárások eredményeként a nemzetbiztonsági szempontból kiemelt fontosságú keretmegállapodásokra vonatkozó szabályok szerint vehetők igénybe.

A központi elektronikus szolgáltató rendszer biztonsági alapdokumentumai

35. § (1) A központi rendszer üzembiztonsága és a kezelt adatok biztonsága érdekében a központi elektronikus szolgáltató rendszer egységes informatikai biztonsági követelményrendszerét az 1. melléklet, a központi elektronikus szolgáltató rendszer informatikai katasztrófaelhárítási tervének alapkövetelményeit a 2. melléklet, az elektronikus kormányzati gerinchálózat biztonsági szabályzatát a 3. melléklet határozza meg.

(2) A központi rendszer és a csatlakozó alrendszerek biztonsági követelményrendszerét a következő dokumentumhierarchiában kell érvényesíteni:
a) biztonsági irányelv, mely meghatározza az informatikai infrastruktúra teljes életciklusára (tervezésnél, beszerzésénél, fejlesztésénél, üzemeltetésénél és selejtezésénél) alkalmazandó általános biztonsági elvárásokat;
b) biztonsági szabályzat, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, a végrehajtás felelősét és a végrehajtás gyakoriságát vagy idejét;
c) végrehajtási eljárásrendek, melyek részletesen leírják a szabályzatban meghatározott feladatok végrehajtásának, ellenőrzésének módját, folyamatát.

(3) A (2) bekezdés szerinti dokumentumokat minden egyes a központi rendszert üzemeltető szervezet, valamint a központi rendszeren keresztül elektronikus közszolgáltatást nyújtó szervezet elkészíti és gondoskodik azok karbantartásáról.

36. § (1) A biztonsági követelményrendszertől, illetve az informatikai katasztrófaelhárítási terv alapkövetelményeitől akkor lehet eltérni, ha a követelmény az adott szolgáltatásra, környezetre nem értelmezhető vagy nem alkalmazható. Ebben az esetben az eltérést indokolni, és a dokumentumokban rögzíteni kell.

(2) A biztonsági követelményrendszerben, illetve az informatikai katasztrófaelhárítási terv alapkövetelményeiben meghatározott követelményeknél kockázatarányosan akkor lehet magasabb követelményszintet megállapítani, ha a kezelt adatok érzékenysége, vagy a felhasználók bizalmának megerősítése ezt szükségessé teszi. A többletkövetelmények alkalmazása esetén az újabb követelményeket a megadott struktúrába kell illeszteni.

(3) A (2) bekezdés szerinti többletelőírások a központi rendszer szolgáltatásait igénybe vevő felhasználó számára csak akkor jelenthetnek többletfeladatot, többletkövetelményt, ha annak teljesítését – a saját biztonsága érdekében – önkéntesen vállalja.

37. § (1) A központi rendszer működési és adatbiztonságának fenntartása a központi rendszer működtetőjének feladata.

(2) A központi rendszer üzemeltetője – a működtető és az informatikai biztonsági felügyelő jóváhagyásával – a központi rendszer egészére vonatkozóan

a) kialakítja az informatikai biztonságirányítási rendszert;

b) rendszeresen, de legalább évente, valamint minden jelentősebb módosítást követően felülvizsgálja a meglévő informatikai biztonsági irányelveket és szabályzatokat, eljárásrendeket, szükség esetén javaslatot tesz azok módosítására.

(3) A központi rendszer működtetője

a) véleményezi a központi rendszert és szolgáltatásait érintő üzemeltetői és szolgáltatói biztonsági irányelveket, szabályzatokat, eljárásrendeket;

b) kidolgozza a biztonsági szabályok alkalmazására és ellenőrzésére szolgáló eljárásrendeket, illetve gondoskodik azok rendszeres aktualizálásáról;

c) ellenőrzi az üzemeltető, valamint a szolgáltató szervezetek biztonsági megfelelőségét, a velük kötött szerződésekben és megállapodásokban érvényesíti a központi rendszerrel kapcsolatos biztonsági elvárásokat;

d) jogosult bekérni az üzemeltetőtől, valamint a közszolgáltatást nyújtó szervezetektől a jelen rendeletben meghatározott biztonsági követelmények teljesítésének értékeléséhez szükséges adatokat és dokumentumokat;

e) szakmai segítséget nyújt a biztonsági dokumentumok elkészítésében.

(4) A központi rendszer működtetője – együttműködve a központi rendszer adatkezelőjével és az üzemeltetővel – biztosítja a központi rendszer egészét átfogó tájékoztatási (ügyfélszolgálati) rendszert, az ügyfélvonalat, amely kiterjed a rendszer üzemállapotára, a benne kezelt adatokra, illetve a felhasználók informatikai és ügyintézési támogatására. Az ügyfélvonal interneten és telefonon egyaránt folyamatosan elérhető.

38. § (1) Az üzemeltető biztosítja a központi rendszer általa üzemeltetett alrendszereinek biztonságos üzemeltetését, és tevékenységével nem veszélyeztetheti a központi rendszer más elemeinek biztonságát.

(2) Az üzemeltető – a működtetővel egyetértésben – meghatározza azon munkaköröket, ahol a rendszer működésének biztonsága, a kezelt adatok védelme érdekében a fontos és bizalmas munkakörökre vonatkozó követelmények érvényesítendők. A működtető felelős a biztonsági ellenőrzések lebonyolíttatásáért, az üzemeltető pedig azért, hogy minden érintett munkakörben megkövetelje a személyi alkalmasságot.

(3) Az üzemeltető a központi rendszer általa üzemeltetett minden egyes alrendszere vonatkozásában a következő biztonsági dokumentumokat készíti el:

a) a biztonsági irányelv;

b) az egyes szolgáltatásokra vonatkozó biztonsági szabályzat;

c) a biztonsági szabályzatok végrehajtásához szükséges eljárásrend.

(4) Az üzemeltető szervezet a (3) bekezdésben meghatározott dokumentumok tervezetét véleményezésre megküldi a központi rendszert működtető szervezetnek, majd a véglegesített tervezetet – jóváhagyásra – az informatikai biztonsági felügyelőnek küldi meg.

(5) A biztonsági szabályzatok rendelkezéseinek érvényesítésére az üzemeltető eljárásrendeket dolgoz ki.

(6) Az üzemeltető

a) félévente tájékoztatást nyújt az informatikai biztonsági eljárásrendek működéséről az informatikai biztonsági felügyelőnek;

b) e rendelet 7. § (1) bekezdés a) pontja szerinti biztonsági esemény esetén
   ba) haladéktalanul felfüggeszti a veszélyt okozó alkalmazást vagy más megoldás hiányában a központi rendszer működését, és jelentést tesz az informatikai biztonsági felügyelőnek,
   bb) az informatikai biztonsági felügyelővel együttműködve értesíti a működtetőt és a korlátozás által érintett szervezeteket,
   bc) igény esetén a működtetővel együttműködve beszámol az Országgyűlés illetékes bizottságának;
c) a működtető kérésére adatokat szolgáltat a biztonsági követelmények teljesítésének ellenőrzéséhez.

(7) Üzemeltetéssel kapcsolatos szervezeti és műszaki változások, illetve biztonsági esemény esetén a (3) bekezdés szerinti dokumentumokat soron kívül kell felülvizsgálni.

39. § Az elektronikus közszolgáltatást nyújtó szervezet köteles gondoskodni arról, hogy az általa nyújtott szolgáltatás, illetve annak igénybevétele ne veszélyeztesse a központi rendszer biztonságát.

40. § A központi rendszer szolgáltatásai biztonságos igénybevételének követelményeit a 4. melléklet határozza meg. A szolgáltatások biztonsági követelményeinek a felhasználó általi megszegése következtében bekövetkező károkozás esetén az üzemeltető és a szolgáltató szervezet – ha ezt igazolja – mentesül a felelősség alól.

VII. FEJEZET
ZÁRÓ ÉS HATÁLYBA LÉPTETŐ RENDELKEZÉSEK

41. § (1) A rendelet – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő 8. napon lép hatályba.

(2) A 8–10. §-ok 2010. január 1-jén lépnek hatályba.

42. § (1) Az elektronikus közszolgáltatásokat igénybe vevő vagy nyújtó, hivatali kapuval rendelkező szervezeteknek, illetve a központi rendszer üzemeltetőjének a biztonsággal kapcsolatos dokumentumaikat 2010. június 30-ig kell e rendelet rendelkezéseivel összhangba hozniuk.

(2) Jogszabályi előírás alapján működésüket 2011. június 30-ig megkezdő, elektronikus közszolgáltatást nyújtó rendszerek esetében a szolgáltatás nyújtását előíró jogszabály, illetve annak felhatalmazása alapján a biztonsági követelményeket előíró jogszabály az e rendeletben vagy a külön jogszabályban foglalt követelmények teljesítésének igazolását a (3) bekezdésben foglalt határidőig ütemezve is előírhatja. Ennek keretében a szolgáltatás működésének megkezdéséhez legalább az e rendelet. 1. mellékletében rögzített biztonsági követelményekre és a 2. melléklet 3.12. pontjában rögzített ellenőrző listára vagy a külön jogszabályban rögzített biztonsági követelményekre és ellenőrző listára vonatkozó önértékelés – a fejlesztésben részt nem vevő független szakértő által igazolt – teljesítését kell az NHH-nak a regisztrációhoz benyújtani.

(3) A jelenleg a központi rendszeren működő szolgáltatások auditálását 2011. december 31-ig kell elvégezni.

43. § (1) Hatályát veszti az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról szóló 195/2005. (IX. 22.) és a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről szóló 84/2007. (IV. 25.) Korm. rendelet.

(2) A 43. § (1) bekezdése 2010. július 1-jén hatályát veszti.

(3) A 43. § (2) Bekezdése 2011. július 1-jén hatályát veszti.

(4) A 43. § (3) bekezdése 2012. január 1-jén hatályát veszti.

Bajnai Gordon s. k.,
miniszterelnök

1. melléklet a 223/2009. (X. 14.) Korm. rendelethez

A központi elektronikus szolgáltató rendszer egységes informatikai biztonsági követelményrendszere

A biztonsági irányelveknek és szabályzatoknak a jelen mellékletben meghatározott tartalmi követelményeket kell kielégíteniük. Ez az alapja az informatikai rendszerek értékelésének és a szolgáltató szervezet auditjának. A kialakítandó informatikai rendszernek, eljárásrendeknek és utasításoknak a mellékletben szereplő tevékenységek egészét vagy meghatározott részét kell átfogniuk a jelen mellékletben megfogalmazottnál nagyobb részletezettséggel, a feladatok megfelelő lebontásával, a végrehajtók támogatásával.

1. A szabályozás azonosító adatai

1.1. A dokumentumok azonosítása	
Cél:	A dokumentum rendelkezzen az egyértelmű azonosításhoz szükséges adattartalommal.
Feladat:	Legalább a következő azonosító adatokkal kell ellátni a dokumentumokat: – A dokumentum címe, (amennyiben van, azonosítója) – Verzió jelölés, – A dokumentum állapotának, státuszának jelölése: munkaanyag, ellenőrzés alatt, végleges dokumentum stb., – A készítő(k) és a jóváhagyó(k) személye, – Hatályba lépés dátuma, – Következő felülvizsgálat legkésőbbi dátuma, – Hatályos mellékletek (azonosításhoz szükséges adatok felsorolása), – Kapcsolódó dokumentumok (azonosításhoz szükséges adatok felsorolása), – Tartalomjegyzék.
Eredmény:	Egyértelműen azonosítható, hogy mely dokumentum milyen állapotában lévő példányáról van szó, ki a felelős a tartalomért és a kiadásáért, mi a minősítése, kire (mire) érvényes, mi az időbeli hatálya.
Felelős:	A szabályzat kiadásáért felelős személy

2. Általános rendelkezések

2.1. Általános tartalmi elemek	
Cél:	A szabályzat környezetének és kapcsolatainak, a készítés körülményeinek
Feladat:	A szabályzat általános része legalább a következő adattartalommal kell – Előzmények, bevezető, összefoglaló, – A szabályzat célja, – A szabályzat szervezeti hatálya, – A szabályzat tárgyi hatálya, – Vonatkozó jogszabályok, szabványok és módszertanok, – Fogalomtár, rövidítések, jelmagyarázat.
Eredmény:	A szabályzatra vonatkozó átfogó ismeretek leírása, amelynek alapján azonosíthatóak annak céljai, a készítés körülményei, az előzmények, kapcsolatok és hivatkozások, és az, hogy kire, illetve mire vonatkozik.
Felelős:	A szabályzat kiadásáért felelős személy

3. Informatikai biztonság szervezete

3.1. Informatikai biztonsági szerepkörök (státuszok) meghatározása	
Cél:	A biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepkörök álljanak rendelkezésre.
Feladat:	A szervezet vezetésének világos iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismertetésével aktív módon támogatnia kell az informatikai biztonságot a szervezeten belül. A kialakításnál figyelembe kell venni, hogy nem lehet összeférhetetlenség az egyes szerepkörök között, és független, közvetlen a felső vezetéshez utalt, neki jelentő szerepkör(ök)et kell létrehozni. Az informatikai biztonsággal összefüggő valamennyi felelősségi kört egyértelműen kell meghatározni. Legalább a következő szerepköröket kell létrehozni: – Informatikai biztonsági felügyelő – a miniszter közvetlen alárendeltségében – felel a központi rendszer informatikai biztonságáért, ellátja az informatikai biztonság ellenőrzését. Összefogja és koordinálja az informatikai biztonsági felelősök szakmai tevékenységét az üzemeltető és a szolgáltató szervezeteknél. – Informatikai biztonsági felelős – az üzemeltető és szolgáltató szervezeteknél – felel a központi rendszer működtetőinél és üzemeltetőinél az informatikai biztonságért.
Eredmény:	Független, jól irányított szervezet, központilag koordinált, folyamatos szakmai tevékenység, világos szerepkörök és feladatok.
Felelős:	A szervezet vezetője

3.2. Külső szolgáltatók igénybevétele	
Cél:	Az informatikai feladatok kiszervezése esetén fenntartani az informatikai biztonság szintjét.
Feladat:	Külső szolgáltatók igénybevételével az informatikai biztonsággal kapcsolatos felelősség nem hárítható át, az a feladatért felelős szervezet első számú vezetőjét terheli. A külső szolgáltatók igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a feladatért felelős szervezet számára a mérés és ellenőrzés feltételeit. A meglévő megállapodásokat, szerződéseket legalább évenként felül kell vizsgálni, és a szükséges módosításokat el kell végezni.
Eredmény:	Informatikai biztonsági követelmények a szolgáltatási megállapodásokban. Éves biztonsági felülvizsgálatok.
Felelős:	A szervezet vezetője

4. Informatikai vagyontárgyak kezelése

4.1. Felelősség az informatikai vagyontárgyakért	
Cél:	Meg kell határozni, hogy a szervezetben ki és milyen módon viseli a felelősséget az informatikai vagyontárgyakért (materiális és immateriális vagyonelemekre egyaránt).
Feladat:	Az informatikai vagyontárgyakat nyilvántartásba kell venni a következő csoportosításban: – Adatok, – Alkalmazások, – Informatikai infrastruktúra (pl. hardverek, szoftverek stb.). A vagyontárgyak azonosításához szükséges adatokat nyilvántartásban kell rögzíteni, biztonsági osztályba kell sorolni, és meg kell nevezni a vagyontárgy felelősét.
Eredmény:	Vagyontárgyak és felelős(ök) listája.
Felelős:	Üzemeltetési vezető

4.2. Az informatikai rendszerben kezelt adatok osztályozása

4.2.1. Osztályozási elvek kialakítása	
Cél:	Az adatok (az informatikailag feldolgozott, meta- és üzemeltetési adatok) osztályozásának célja, hogy azok adatvédelmi és biztonsági súlyának megfelelően kerüljön kialakításra az arányos védelem.

Feladat:	Az adatokat értékük, a jogi előírások, a szervezet szempontjából képviselt érzékenységük és kritikusságuk szempontjából kell osztályozni. Az adatokat az alábbi osztályokba kell sorolni: – Különlegesen védendő (minősített) adatok, amelyekhez a belső és külső hozzáférés csak a vonatkozó törvényi előírások alapján erősen korlátozva, szigorúan ellenőrizve és dokumentálva engedélyezhető (pl. a központi rendszer biztonságát érintő adatok), – Érzékeny adatok, amelyekhez a belső és külső hozzáférést korlátozni, a hozzáférést naplózni kell (pl. elektronikus ügyintézés adatai, állampolgárok személyes adatai stb.), – Belső adatok, amelyekhez a külső hozzáférés nem lehetséges, belső hozzáférés korlátozása nem kritikus, – Nyilvános, közhiteles adatok, ahol a rendelkezésre állás és a megváltoztathatatlanság biztosítása kritikus, – Általános kezelésű adatok. Az alkalmazásokat, és az infrastruktúra elemeit a kezelt adatok biztonsági osztályával összhangban kell besorolni biztonsági osztályokba. A fejlesztők és üzemeltetők a biztonsági besorolásnak megfelelő adminisztratív és technikai védelmet kell, hogy kialakítsanak.
Eredmény:	Az adatok biztonsági besorolása és azok védelmi követelményeinek leírása. Az informatikai erőforrások osztályozása.
Felelős:	Informatikai biztonsági felügyelő/felelős

4.2.2. Adatok jelölése és kezelése	
Cél:	A felhasználók az adatokat (elektronikus és papír hordozójú) biztonsági besorolásának megfelelően kezeljék.
Feladat:	Összhangban a szervezet által elfogadott biztonsági osztályozási rendszerrel, megfelelő eljárásokat kell kidolgozni és bevezetni az adatok (információhordozók) jelölésére és kezelésére.
Eredmény:	Az adatok osztályba sorolásának jelölése és a kezelésre vonatkozó eljárások.
Felelős:	Adatgazda

5. Személyi biztonság

5.1. Ellenőrzött munkatársak alkalmazása	
Cél:	Az informatikai munkaköröket csak megfelelően ellenőrzött munkatársak töltsék be.
Kiinduló adat:	Biztonsági szempontból kritikus munkakörök listája.
Feladat:	Az informatikai munkatársak munkába állását meg kell előzzék a kezelt adatok érzékenységével arányos mélységű, a fontos és bizalmas munkakörökre vonatkozó szabályok szerinti ellenőrzések. A nemzetbiztonsági követelmények szerinti ellenőrzéseken túl a kockázattal arányos mértékben mérlegelni kell a munkatárs egyéni tulajdonságait is (pl. felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség, pánik-tűrőképesség stb.). A biztonsági szempontból kritikus informatikai munkaköröket betöltő munkatársak esetében az alkalmasságot rendszeresen felül kell vizsgálni. Az érintett munkatársakkal olyan – szabályzat szerinti tartalmú – titokvédelmi nyilatkozatot kell aláíratni Külső szolgáltató igénybevétele esetén a szerződésben vagy megállapodásban kell rögzíteni az erre vonatkozó feladatokat a kockázattal arányos módon.
Eredmény:	Munkatársak alkalmazása során gyakorolt biztonsági eljárások.
Felelős:	Humánpolitikai vezető és az informatikai biztonsági felügyelő/felelős

5.2. Feladatok és felelősségi körök meghatározása	
Cél:	A biztonsági intézkedések végrehajtásával kapcsolatos feladatok, felelősségi és hatáskörök legyenek megfelelően rögzítettek.

Feladat:	Munkaköri leírásokban, szabályzatokban kell rögzíteni az egyes munkakörökhöz tartozó feladatokat és felelősségi kört, a szükséges informatikai jogosultságokat. Minden munkakörhöz csak a munkához feltétlen szükséges jogosultságokat kell megadni. Biztonsági oktatást kell tartani a dolgozóknak alkalmazásukkor, új informatikai rendszerek bevezetésekor. A biztonsági szabályok megváltozásakor, de legalább kétévente frissítő oktatást kell tartani minden munkatárs számára.
Eredmény:	Aktuális munkaköri leírások. Biztonsági oktatások.
Felelős:	Informatikai biztonsági felügyelő/felelős

5.3. Személyi biztonság az alkalmazás megszűnése, illetve megváltozása esetén	
Cél:	A munkatársak jogállásának megváltozása esetén fenn kell tartani a biztonsági szintet.
Feladat:	A munkatársak kilépése, tartós távolléte, a munkakör változása esetére eljárást kell kidolgozni a szükséges biztonsági intézkedésekről (jogosultság visszavonása, felfüggesztése, változtatása).
Eredmény:	Eljárás az alkalmazás megszűnése, illetve munkakör megváltozása esetére.
Felelős:	Informatikai biztonsági felügyelő/felelős

6. Fizikai és környezeti biztonság

6.1. Területek védelme, biztosítása

6.1.1. Fizikai biztonsági zónák kialakítása	
Cél:	A védett erőforrások fizikai védelmének kockázatarányos megvalósítása.
Feladat:	Biztonsági zónákat és a hozzájuk tartozó adminisztratív és műszaki védelmi intézkedéseket kell meghatározni. A helyiségeket az alábbi biztonsági kategóriákba kell sorolni: Zárt terület (pl. gépterem), Kiemelt terület (pl. raktárak, áramellátó helyiségek), Ellenőrzött terület (pl. irodák, folyosók), Nyilvános terület (pl. ügyfélszolgálati tér). A zónába sorolásnál tekintettel kell lenni arra, hogy a szomszédos helyiségek, szomszédos biztonsági kategóriába kell tartozzanak.
Eredmény:	Helyiségek biztonsági besorolása. Biztonsági zónák védelmi eljárásai.
Felelős:	Informatikai biztonsági felügyelő/felelős

6.1.2. Belépés- és mozgásellenőrzés	
Cél:	Az erőforrásokhoz való fizikai hozzáférési eljárás ellenőrzése.
Feladat:	A különböző biztonsági zónák közötti mozgást ellenőrizni kell. A biztonsági zónához meghatározott követelményeknek megfelelő adminisztratív és műszaki eljárásokat kell alkalmazni. A telephelyek kiválasztása és kialakítása során törekedni kell a közforgalmú (külső személyek által is használt) területek lehető legnagyobb mértékű elválasztására az üzemi területektől. Azokat a területeket, ahol külső személyek is tartózkodhatnak, nyilvános területként kell kezelni, és a hozzáférési pontokon és zónahatárokon az ennek megfelelő védelmet kell kialakítani. Az ellenőrzési pontok minimálisan a következő intézkedéseket kell megvalósítsák: – Személy azonosságának ellenőrzése, – Be- és/vagy kilépés idejének rögzítése, – Eljárást kell kidolgozni a belépés- és mozgásellenőrző rendszerek működtetésére és használatára.
Eredmény:	Belépés- és mozgásellenőrző rendszer. Eljárás a belépés- és mozgásellenőrző rendszerek működtetésére és használatára.
Felelős:	Informatikai biztonsági felügyelő/felelős

6.2. Informatikai eszközök védelme

6.2.1. Berendezések elhelyezése és védelme	
Cél:	Biztosítani kell a berendezések működőképességét és védelmét az illetéktelen hozzáféréstől.
Feladat:	A berendezések elhelyezésére szolgáló helyiségek kiválasztásánál és kialakításánál figyelembe kell venni a berendezés biztonsági besorolása szerinti követelményeket. Meg kell határozni a környezeti hatások, szándékos támadás és véletlen károkozás kockázatát, és ennek megfelelő fizikai, elektronikai és élőerős védelmet kell biztosítani.
Eredmény:	Berendezések biztonsági besorolása szerinti védelemi követelmények.
Felelős:	Informatikai biztonsági felügyelő/felelős

6.2.2. Közműszolgáltatások biztosítása	
Cél:	A berendezések védelme a közműszolgáltatások kiesésével, valamint működési rendellenességeivel szemben.
Feladat:	A közműszolgáltatások (pl. áram) kiesése esetére a szolgáltatási szint megállapodásokkal és a katasztrófaelhárítási eljárásokkal összhangban kell kiválasztani a szükséges műszaki megoldásokat (pl. áramellátás: szünetmentes áramforrás, többirányú betáplálás, áramtermelő generátor).
Eredmény:	Intézkedési terv a közműszolgáltatások kiesése esetére.
Felelős:	Üzemeltetési vezető

6.2.3. Kábelezés biztonsága	
Cél:	Az informatikai erőforrások által használt kábelek védelme sérülésektől és lehallgatástól.
Feladat:	A kábelek elhelyezésekor, a használt anyagok kiválasztásakor figyelembe kell venni a kiszolgált informatikai erőforrások biztonsági besorolását. A kábeleket a várható fizikai igénybevételnek és a továbbított adatok kritikusságának megfelelően kell védeni, figyelembe véve az elektromágneses sugárzások be-, illetve kijutása (zavar, illetve információ) elleni védelmet is. A kritikus erőforrások között redundáns kapcsolatot kell kialakítani (különböző fizikai útvonalak kijelölésével).
Eredmény:	A biztonsági elvárásoknak megfelelően kialakított és megvalósított kábelezési terv és karbantartási eljárások.
Felelős:	Üzemeltetési vezető

6.2.4. Berendezések karbantartása	
Cél:	A berendezések megbízhatóságának biztosítása, a váratlan hibák elhárítására fordítandó erőforrások minimalizálása.
Feladat:	A berendezések karbantartására karbantartási tervet kell készíteni, amely biztosítja a berendezések előírt (idő vagy igénybevételi) intervallumonként történő szakszerű karbantartását.
Eredmény:	Berendezések karbantartási terve.
Felelős:	Üzemeltetési vezető

6.2.5. Berendezések biztonságos selejtezése és újrafelhasználása	
Cél:	Az adathordozókon tárolt információk ne kerülhessenek illetéktelen kezekbe.
Feladat:	Olyan selejtezési és megsemmisítési eljárásokat kell kidolgozni, amelyek biztosítják, hogy a selejtezett eszközökön tárolt információk visszaállítása ne legyen lehetséges.
Eredmény:	Informatikai berendezések selejtezési eljárásai.
Felelős:	Informatikai biztonsági felügyelő/felelős

7. A kommunikáció és az üzemeltetés irányítása

7.1. Üzemeltetési eljárások és felelősségi körök

7.1.1. Dokumentált üzemeltetési eljárások	
Cél:	Az üzemeltetési tevékenységek végrehajtásának és az ellenőrzés alapjának biztosítása.
Feladat:	Az üzemeltetési feladatok határidőre történő, szabályozott végrehajtása érdekében üzemeltetési szabályzatot és üzemeltetési eljárásokat kell készíteni. Az üzemeltetési szabályzatokban az üzemeltetéssel kapcsolatos feladatokat és felelősségeket kell meghatározni. Az üzemeltetési eljárásokban az üzemeltetési feladatok végrehajtási eljárásait, műszaki leírásait kell meghatározni.
Eredmény:	Üzemeltetési szabályzat. Üzemeltetési eljárások.
Felelős:	Üzemeltetési vezető

7.1.2. Változáskezelési eljárások	
Cél:	Az informatikai rendszer konfigurációján csak előzetesen engedélyezett változások történhessenek.
Feladat:	Ki kell dolgozni a változások kezelésének szabványos folyamatát az igényfelvetéstől az átadás-átvételig. A változáskezelési eljárás tartalmazza legalább az alábbiakat: – Változási igények fogadása, kezelése, – Kockázat elemzése, priorizálás, – Változás dokumentálása és implementálása.
Eredmény:	Változáskezelési eljárás.
Felelős:	Üzemeltetési vezető

7.1.3. Feladatkörök, kötelezettségek elhatárolása	
Cél:	Kerüljenek szétválasztásra a biztonsági szempontból összeférhetetlen feladatkörök.
Feladat:	Meg kell határozni a biztonsági szempontból összeférhetetlen feladatokat, amelyek véletlen vagy szándékos károkozást tesznek lehetővé, és ezek szétválasztását érvényesíteni kell a szervezeti felépítésben valamint a munkakörök kialakításakor. Összeférhetetlen feladatkörök (például): – fejlesztés és üzemeltetés, – üzemeltetés és biztonsági adminisztráció, – üzemeltetés és felhasználás.
Eredmény:	Összeférhetetlen feladatkörök azonosítva és szétválasztva.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.1.4. Fejlesztési, teszt és üzemeltetési berendezések különválasztása	
Cél:	Az üzemeltetési környezethez való jogosulatlan hozzáférés, illetve jogosulatlan módosítás kockázatának csökkentése.
Feladat:	A fejlesztési, tesztkörnyezeteket és üzemi környezetet logikailag és lehetőség szerint fizikailag is szét kell választani egymástól.
Eredmény:	Elkülönített fejlesztési, teszt- és üzemeltetési környezetek.
Felelős:	Informatikai vezető

7.2. Harmadik felek tevékenységének irányítása

7.2.1. Szolgáltatásnyújtás	
Cél:	A külső szolgáltatótól igénybe vett szolgáltatások esetén is biztosítani kell a biztonsági követelmények teljesülését.
Feladat:	Meg kell határozni azokat a szerződéses elemeket és tevékenységeket, amelyeket érvényesíteni kell a harmadik felekkel kötött szolgáltatási szerződésekben. Ki kell dolgozni ezen követelmények teljesülésének ellenőrzési eljárásait.
Eredmény:	Biztonsági követelmények a szolgáltatási megállapodásokban. Ellenőrzési eljárások a biztonsági követelmények érvényesítésére.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.2.2. Harmadik felek szolgáltatásainak figyelemmel kísérése és átvizsgálása	
Cél:	Ellenőrizni kell, hogy a külső féltől igénybe vett szolgáltatások esetén teljesül-e az elvárt szolgáltatási szint.
Feladat:	Ki kell dolgozni a szolgáltatási szintek leírásának, érvényesítésének, a teljesítés dokumentálásának, ellenőrzésének és a nem megfelelő teljesítés szankcionálásának eljárásait.
Eredmény:	Szolgáltatási szint menedzselését biztosító eljárások.
Felelős:	Üzemeltetési vezető és informatikai biztonsági felügyelő/felelős

7.2.3. Harmadik felek szolgáltatásaival kapcsolatos változások kezelése	
Cél:	Biztosítani kell, hogy a változásokat csak a megfelelő jogosultságokkal lehessen kezdeményezni, és a végrehajtás ellenőrzött és dokumentált körülmények között történjen az igény felvetésétől az átadás-átvételig.
Feladat:	Ki kell dolgozni a változáskezelési eljárásokat a külső fél által nyújtott szolgáltatásokra. A változáskezelési eljárásnak biztosítania kell a következőket: – a változások végrehajtása csak a megfelelő jóváhagyás után történjen, – a végrehajtás során is érvényesüljenek a biztonsági követelmények, – az átvétel során ellenőrzésre kerüljön a specifikációban/változási kérelemben leírtak teljesülése.
Eredmény:	Változáskezelési eljárások külső szolgáltatásokra.
Felelős:	Üzemeltetési vezető és informatikai biztonsági felügyelő/felelős

7.3. Rendszertervezés és elfogadás

7.3.1. Kapacitásmenedzsment	
Cél:	A mindenkori erőforrás-igények hatékony kielégítése és a szűk keresztmetszetek kialakulásának elkerülése.
Feladat:	Ki kell dolgozni az erőforrás-kihasználtság figyelésének, elemzésének és a jövőbeli trendek előrejelzésének folyamatait, és ennek eredményét figyelembe kell venni az erőforrás-beszerzések tervezésekor.
Eredmény:	Kapacitás-menedzsment tervek.
Felelős:	Üzemeltetési vezető és informatikai biztonsági felügyelő/felelős

7.3.2. Rendszerek elfogadása, átvétele	
Cél:	Biztosítani kell, hogy az átvett rendszerek tegyenek eleget az elvárt minőségi, mennyiségi, biztonsági és funkcionális követelményeknek.
Feladat:	A rendszerek átvételéhez olyan eljárásokat kell kidolgozni, amelyek biztosítják az elvárásoknak való megfelelés ellenőrzését. Az ellenőrzés módszerei a tesztelés (funkcionális/terheléses stb.), a forráskód-audit, szakértői ellenőrzés stb.
Eredmény:	Átadás-átvételi eljárási rend.
Felelős:	Üzemeltetési vezető

7.4. Védelem a rosszindulatú és mobil kódok ellen

7.4.1. Rosszindulatú kód elleni védelem	
Cél:	Meg kell akadályozni, hogy a szervezet működésében zavart, adatvesztést vagy adatkiszivárgást okozzon bármilyen rosszindulatú kód (vírus, trójai stb.).
Feladat:	Olyan adminisztratív és technikai intézkedéseket kell alkalmazni, amelyek megakadályozzák a rosszindulatú kódokat tartalmazó programok bejutását, alkalmazását.
Eredmény:	Rosszindulatú kód elleni védelem.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.4.2. Mobil kód elleni intézkedések	
Cél:	Meg kell akadályozni, hogy a szervezet működésében zavart, adatvesztést vagy adatkiszivárgást okozzon bármilyen rosszindulatú mobil kód.
Feladat:	Le kell tiltani minden olyan kód futtatását, amelyek nem szükségesek a felhasználók munkájához.
Eredmény:	Biztonságos böngésző beállítások.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.5. Biztonsági mentés

7.5.1. Információk biztonsági mentése	
Cél:	Az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli visszaállítás biztosítása.
Feladat:	Olyan mentési rendet kell kialakítani, ami biztosítja az adatok visszaállíthatóságát a szervezet által meghatározott követelmények szerint (elvárt visszaállítás idő, maximálisan elviselhető adatvesztés stb.). A mentések gyakoriságát, a mentés módját, a használt adathordozót és a tárolási helyet a fentiek figyelembevételével kell kiválasztani, és ki kell dolgozni azokat az eljárásokat, amelyek teljesítik a követelményeket. Az eljárások kidolgozása után az érintettek számára oktatás szükséges, és elengedhetetlen a teljes visszaállítási eljárás tesztelése is. Ki kell dolgozni a mentések ellenőrzésének (ellenőrző visszatöltés) rendjét is (több példányos mentés, külső helyszínen tárolás). A mentési, visszaállítási eljárást évente és releváns változások esetén felül kell vizsgálni, és naprakésszé kell tenni.
Eredmény:	Mentési és visszaállítási eljárások.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.6. Hálózatbiztonság kezelése

7.6.1. Hálózatok védelme	
Cél:	A hálózatokon továbbított adatok biztonságának és a hálózat rendelkezésre állásának védelme.
Feladat:	A hálózatok biztonsági érdekében a következő intézkedések megvalósítása javasolt: a hálózat szegmentációja, tűzfalas védelem (csomag-/alkalmazásszintű), vírusvédelmi eszközök, tartalomszűrés, titkosított adatvédelmi csatornák kialakítása. A hálózati rendelkezésre állás érdekében a hálózati forgalmat rendszeresen mérni és értékelni kell, és biztosítani, hogy a szükséges sávszélesség kellő biztonsággal rendelkezésre álljon. Dokumentálni kell a hálózatokon alkalmazott védelmi intézkedéseket és azok üzemeltetési eljárásait.
Eredmény:	Hálózatbiztonsági intézkedések dokumentációja.
Felelős:	Hálózatbiztonsági szabályzat. Informatikai biztonsági felügyelő/felelős

7.6.2. Hálózati szolgáltatások biztonsága	
Cél:	Az elvárt minőségi, mennyiségi, funkcionális és biztonsági paraméterek megbízható nyújtásának biztosítása a hálózati szolgáltatók részéről.
Feladat:	Dokumentálni kell a hálózati szolgáltatásokkal szemben támasztott biztonsági követelményeket és azok ellenőrzésének, valamint a nem megfelelő teljesítés szankcionálásának eljárásait.
Eredmény:	Hálózati szolgáltatások biztonsági követelményei.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.7. Adathordozók kezelése

7.7.1. Adathordozók kezelése	
Cél:	Biztosítani kell, hogy az adathordozók, illetve a rajtuk tárolt adatok a telephelyről kikerülve se sérülhessenek, módosulhassanak vagy kerülhessenek illetéktelen kezekbe.
Feladat:	Ki kell dolgozni valamennyi adathordozó kezelésének eljárásait, kiemelt figyelmet fordíva a telephelyen kívüli védelemre. A szabályzatnak ki kell terjednie a teljes élettartamra, a nyilvántartásra, a selejtezésre, a frissítésrekre, több példány készítésére. Kiemelt figyelmet kell fordítani az USB eszközökre, a memóriakártyákra.
Eredmény:	Adathordozók kezelési szabályzata.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.7.2. Adathordozók selejtezése	
Cél:	Biztosítani kell, hogy a selejtezett adathordozókon tárolt információk se kerülhessenek illetéktelen kezekbe.
Feladat:	Meg kell határozni azon adathordozók körét, amelyek a rajtuk tárolt adatok miatt selejtezés után sem kerülhetnek ellenőrizetlen körülmények közé. Olyan selejtezési eljárásokat kell kidolgozni, amelyek biztosítják a selejtezett adathordozókon tárolt adatok biztonságos, visszaállítást lehetetlenné tevő megsemmisítését. Minden adathordozó-típusra (mágneses, optikai) ki kell dolgozni a specifikus eljárásrendet. A selejtezés folyamatát dokumentálni kell a későbbi ellenőrizhetőség érdekében.
Eredmény:	Adathordozók biztonsági besorolása. Selejtezési eljárások.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.7.3. Informatikai rendszerekben tárolt adatok kezelési eljárásai	
Cél:	Az adatok biztonsági besorolása szerinti védelem biztosítása.
Feladat:	Minden biztonsági osztályra ki kell dolgozni az adatok tárolási és kezelési eljárásait, amelyek biztosítják a biztonsági osztály által előírt védelmi szintet.
Eredmény:	Adatkezelési eljárások minden biztonsági osztályra.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.7.4. Rendszerdokumentáció védelme	
Cél:	A rendszerdokumentáció rendelkezésre állásának és adatbiztonságának védelme.
Feladat:	Ki kell dolgozni a rendszerek dokumentációinak tárolási és hozzáférési szabályait, ami biztosítja azok rendelkezésre állását és a jogosultsághoz kötött, ellenőrzött hozzáférést. A rendelkezésre állásba bele kell érteni a naprakészséget, a változások átvezetésének folyamatszerű és biztonságos mechanizmusát is. A tárolási rendnek azt is biztosítania kell, hogy szükség esetén az arra jogosultak azonnal hozzáférhessenek a szükséges dokumentációkhoz.
Eredmény:	Rendszerdokumentációk tárolási szabályzata.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.8. Adatcsere, adattovábbítás

7.8.1. Adatcserére, adattovábbításra vonatkozó szabályzatok és eljárások	
Cél:	Biztosítani kell az adatcserének, a továbbított adatoknak a biztonsági osztályuknak megfelelő védelmét.
Feladat:	Ki kell dolgozni a külső szervezetekkel történő adatcsere, a részükre történő adattovábbítás technikai és adminisztratív eljárásait. Az alkalmazott védelmet az átadott információ biztonsági besorolásának megfelelően kell kialakítani. Az eljárásoknak ki kell térnie az adatkéréstől az adat megérkezésének visszaigazolásáig minden lépésre, és egyértelműen definiálnia kell a folyamatban résztvevők felelősségét.
Eredmény:	Kommunikációra vonatkozó biztonsági szabályok.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.8.2. Megállapodások az adatcseréről, adattovábbításról	
Cél:	Más adatkezelésre feljogosított szervezetekkel történő adatcsere biztonságának fenntartása.
Feladat:	Az adatcsere, adattovábbítás biztonságáról a szervezetek között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.
Eredmény:	Adatcsere, adattovábbítás biztonsági eljárásai.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.8.3. Fizikai adathordozók szállítása	
Cél:	Az adathordozók sérülésének, módosulásának és elvesztésének megakadályozása a szállítás során.
Feladat:	Ki kell dolgozni az adathordozók szállítására vonatkozó szabályzatot. A szállításhoz használt eszközt, járművet és adminisztratív védelmet a szállított adat érzékenysége és kritikus volta alapján kell meghatározni.
Eredmény:	Adathordozók szállításának eljárásrendje.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.8.4. Elektronikus üzenetek küldése/fogadása	
Cél:	Az elektronikus üzenetek védelme jogosulatlan hozzáférés és módosítás ellen.
Feladat:	Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.
	Ilyen intézkedés lehet az elektronikus aláírás, időbélyegzés használata, titkosítás.
Eredmény:	Elektronikus üzenetváltás szabályai.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.8.5. Működést támogató információs rendszerek	
Cél:	A szervezet által használt információs rendszerek biztonságának védelme.
Feladat:	Szabályozni kell a rendszerek használatát azok túlterhelésének, üzemzavarának elkerülése, illetve a tárolt információk sérülésének megakadályozása érdekében. Meg kell határozni, hogy az érintett rendszerek ki által, milyen célra és módon alkalmazhatók (pl. internethasználat, e-mail-használat).
Eredmény:	Felhasználói utasítás a kritikus rendszerekre.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.9. Valós idejű, ügyfeleknek biztosított szolgáltatások

7.9.1. On-line üzenetváltások (tranzakciók)	
Cél:	Biztosítani kell az on-line tranzakciók bizalmasságát, sértetlenségét, és meg kell akadályozni az adatvesztést.
Feladat:	Ki kell dolgozni az on-line tranzakciók védelmére vonatkozó követelményeket, és a követelmények teljesítése érdekében végrehajtott technikai és adminisztratív intézkedéseket.
Eredmény:	On-line tranzakciók biztonsági követelményei. On-line tranzakciók biztonsági intézkedései.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.9.2. Nyilvánosan hozzáférhető információk	
Cél:	Biztosítani kell a nyilvánosan hozzáférhető információk sértetlenségét.
Feladat:	Ki kell dolgozni a nyilvánosan hozzáférhető információk (pl. honlapok, nyilvános adatbázisok) sértetlensége érdekében szükséges adminisztratív és technikai intézkedéseket. Ki kell térni az információ változtatásának eljárásrendjére, új információ közzététele előtt követendő eljárásra és egyes információk törlésének eljárásaira is.
Eredmény:	Változáskezelési eljárások a nyilvánosan hozzáférhető információkra. Technikai intézkedések dokumentációja.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.10. Követés (monitoring)

7.10.1. Audit naplózás	
Cél:	A felhasználói tevékenység (jogosult és illetéktelen) figyelemmel kísérése, a támadási kísérletek mielőbbi felfedése érdekében biztosítani kell a naplófájlok biztonságát.
Feladat:	Meg kell határozni, hogy milyen adatok hozzáférése/módosítása esetén van szükség és milyen mélységű naplózásra. Ki kell dolgozni a naplófájlok kezelésére (rögzítés, elemzés) vonatkozó adminisztratív eljárásokat és technikai megoldásokat. A kritikus rendszerek naplófájljait rendszeresen vizsgálni kell az esetleges üzemzavarok és támadási kísérletek felfedése érdekében. Ez a vizsgálat részben automatizálható, amennyiben a naplófájlok mennyisége ezt indokolja.
Eredmény:	Naplófájlok létrehozásának, kezelésének és felhasználásának szabályai. Technikai intézkedések dokumentációja.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.10.2. Rendszerhasználat figyelése	
Cél:	A rendszerek jogosulatlan használatának megakadályozása, és a hibás működés időben történő észlelése.
Feladat:	Ki kell dolgozni a rendszerhasználat figyelésének (adatgyűjtés–elemzés–intézkedés) eljárásait, amelyek biztosítják, hogy a rendellenességek időben feltárásra kerüljenek és kezelhetők legyenek.
Eredmény:	Monitoringeljárások.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.10.3. Naplóinformációk védelme	
Cél:	A rendszer működésére vonatkozó információk rendelkezésre állása.
Feladat:	Ki kell dolgozni a rendszernaplók rögzítésének, tárolásának és elemzésének eljárásait, amelyek biztosítják azok sértetlenségét, megváltoztathatatlanságát és a jogosultsághoz kötött hozzáférést.
Eredmény:	Naplóinformációk kezelési eljárásai.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.10.4. Adminisztrátori és kezelői naplók	
Cél:	Az ellenőrzés, visszakereshetőség és számon kérhetőség biztosítása a rendszerekben végzett tevékenységekkel kapcsolatban.
Feladat:	Ki kell dolgozni az adminisztrátori és operátori naplók rögzítésének és tárolásának eljárásait, amelyek biztosítják azok sértetlenségét, megváltoztathatatlanságát és a jogosultsághoz kötött hozzáférést.
Eredmény:	Rendszerekben végzett tevékenységek naplózásának eljárásai.
Felelős:	Informatikai biztonsági felügyelő/felelős

7.10.5. Hibák naplózása	
Cél:	A hibák nyilvántartása a tanulságok levonása és a hibák jövőbeli elkerülése érdekében.
Feladat:	Ki kell dolgozni a hibákra vonatkozó információk rögzítésének, tárolásának, és elemzésének eljárásait. A hibaelemzések alapján meg kell hozni a szükséges javító intézkedéseket (hiba megkeresése az adott rendszerben, kapacitásbővítés stb.).
Eredmény:	Hibanaplók kezelési rendje.
Felelős:	Informatikai vezető és informatikai biztonsági felügyelő/felelős

7.10.6. Időadatok szinkronizálása	
Cél:	Biztosítani kell, hogy a különböző rendszerekben rögzített adatok (tranzakciók, naplóbejegyzések, üzenetek) időadatai a lehető legteljesebb összhangban legyenek.
Feladat:	Meg kell határozni az órajelek és időadatok szinkronizálásra vonatkozó eljárásait. Az órajelek szinkronizálását a szervezeten belül ugyanazon forráshoz kell igazítani. Összetett, sok elemében időadatokat felhasználó rendszer esetén vizsgálni kell a helyi időszerver üzembe állításának lehetőségét, illetve külső – központi – referenciaforráshoz történő szinkronizálást.
Eredmény:	Egységes időadatok, időbélyegzések a rendszerekben és naplófájlokban.
Felelős:	Informatikai biztonsági felügyelő/felelős

8. Hozzáférés-ellenőrzés

8.1. A hozzáférés-ellenőrzéshez fűződő működési követelmény

8.1.1. Hozzáférés-ellenőrzési szabályzat	
Cél:	A dokumentumokhoz, információkhoz, adatokhoz történő hozzáférés ellenőrzése.
Feladat:	Hozzáférési-ellenőrzési szabályzat kialakítása, bevezetése, betartatása; a szabályzat periodikus felülvizsgálata és módosítása elengedhetetlen. Minden felhasználó csak azokhoz az erőforrásokhoz/információkhoz férhessen hozzá, amelyek a munkájához mindenképp szükségesek.
Eredmény:	Dokumentált információ-hozzáférési szabályozás révén csökken az információk kiszivárgásának és az illetéktelen hozzáférések kockázata.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.2. Felhasználói hozzáférés irányítása

8.2.1. Felhasználók regisztrálása	
Cél:	Az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.
Feladat:	Ki kell dolgozni, be kell vezetni és szigorúan be kell tartatni a felhasználóknak való jogosultságok kiadásának és visszavételének rendszerét; lehetőleg az egyes felhasználók igénybevételi, csatlakozási szerződéséhez – ahol ilyen van – kötve. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.
Eredmény:	A pontosan szabályozott hozzáférési jogok révén csökken az információk kiszivárgásának, illetéktelen hozzáférésének kockázata.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.2.2. Speciális jogosultságok kezelése	
Cél:	A speciális jogosultságok megszerzésének és alkalmazásának korlátozása.
Feladat:	Az általános összeférhetetlenségi szabályoktól való speciális eltérés kockázati tényező, ezért az ilyen jogosultságok kiadását mindenképp kerülni kell. Amennyiben valamilyen elkerülhetetlen ok miatt mégis létre kell hozni ilyent, akkor azt csak dokumentáltan, s csak a feltétlenül szükséges időtartamra szabad adni.
Eredmény:	Csökken annak a kockázata, hogy a speciális jogosultságok nem megfelelő menedzselése miatt a rendszer működésében hibák keletkeznek; vagy illetéktelen helyre kerülnek védendő adatok.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.2.3. Felhasználói jelszavak kezelése, gondozása	
Cél:	A jelszavak kezelésének biztonságos megvalósítása.
Feladat:	A jelszavak, azonosítási eszközök felhasználói kezelését szabályozni kell; figyelve arra, hogy a felhasználók titokban tartsák és megfelelő időközönként változtassák jelszavaikat; valamint biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.
Eredmény:	Felhasználói jelszókezelés szabályozása.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.3. Felhasználói felelősségek

8.3.1. Jelszóhasználat	
Cél:	Megfelelő erősségű jelszavak, azonosítási módszerek használata.
Feladat:	A felhasználók számára olyan használati rendet kell kialakítani, amely biztosítja megfelelő erősségű jelszavak, illetve azonosító eszközök használatát és ezek megfelelő gyakoriságú cseréjét, pótlását.
Eredmény:	Felhasználói jelszókezelés szabályozása.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.3.2. Őrizetlenül hagyott felhasználói berendezések kezelése	
Cél:	Az őrizetlenül hagyott berendezéseken való jogosulatlan hozzáférések megelőzése.
Feladat:	A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat. A belső felhasználókat (alkalmazottakat) kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.
Eredmény:	Felhasználói informatikai biztonsági követelmények.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.4. Hálózati szintű hozzáférés-ellenőrzés

8.4.1. Hálózati szolgáltatások használatára vonatkozó szabályzat	
Cél:	A hálózatra telepített szolgáltatások védelme.
Feladat:	A hálózati szolgáltatások használatáról szabályzatot kell készíteni, s azt be kell tartatni. A szabályzatnak tartalmazni kell, hogy milyen felhasználói kör milyen hálózati területhez férhet hozzá.
Eredmény:	A hálózati szolgáltatások használatára vonatkozó szabályzat.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.4.2. Felhasználó azonosítása, jogosultságkezelése külső hozzáférés esetén	
Cél:	A távoli felhasználók megbízható azonosítása.
Feladat:	A külső összeköttetéseket csak a feltétlenül munkaidőn kívül is elérni szükséges rendszerekhez szabad engedélyezni, s kriptográfiai védelmi módszereket kell alkalmazni.
Eredmény:	A hálózati szolgáltatások használatára vonatkozó szabályzat.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.4.3. Távdiagnosztikai és konfigurációs portok védelme	
Cél:	A távdiagnosztikai és a konfigurációs portok védelmének biztosítása.
Feladat:	A távdiagnosztikai és a konfigurációs portokhoz való fizikai és logikai hozzáférést ellenőrizni, szabályozni kell. A hozzáféréshez a rendszerben alkalmazott legszigorúbb azonosítási eljárásokat és naplózási rendet kell használni.
Eredmény:	A távdiagnosztikai és a konfigurációs portok használatának szabályzata.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.5. Operációs rendszer szintű hozzáférés-ellenőrzés,

8.5.1. Biztonságos bejelentkezési eljárások	
Cél:	Szabályzat az operációs rendszerek hozzáférési eljárásainak beállítására és használatára.
Feladat:	Az operációs rendszerekbe való bejelentkezési eljárásokat – a jogosulatlan hozzáférés, a szándékos károkozás elkerülése érdekében – szabályozni kell. Fontos a különböző szerepköröknek megfelelő hozzáférési jogosultság meghatározása és az ehhez tartozó jogok beállításának szabályozása (igénylés, engedélyezés, beállítás, visszavonás).
Eredmény:	A biztonsági szempontoknak megfelelő hozzáférés az operációs rendszer funkciókhoz.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.5.2. Felhasználó azonosítása és jogosultságkezelése	
Cél:	Az operációs rendszer szintű felhasználók azonosítása és jogosultságkezelése.
Feladat:	A felhasználók egyedi azonosítására, jogosultságainak kiosztására megbízható módszert kell választani, annak használatát szabályzatban kell rögzíteni, használatát szigorúan meg kell követelni. A szabályzatnak ki kell terjednie az azonosítás és jogosultságkezelés teljes életciklusára (igénylés, engedélyezés, beállítás, visszavonás). Meg kell határozni a biztonságos jelszóra, azonosító eszközre vonatkozó követelményeket, szabályozni kell a jelszavak létrehozására, módosítására, tárolására, használatára, visszavonására vonatkozó eljárásokat. A felhasználók a jelszó- és azonosító eszköz használattal kapcsolatos feladatait és kötelezettségeit szintén szabályzatba kell foglalni, és rendszeresen ellenőrizni kell annak betartását.
Eredmény:	Egyértelműen szabályozott felhasználói hozzáférési és hitelesítési rendszer.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.5.3. Rendszer-segédprogramok használata	
Cél:	Átlátható, ellenőrzött, dokumentált, a biztonságot nem veszélyeztető rendszer-segédprogram használat megvalósítása.
Feladat:	A rendszer-segédprogramok használata különös lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázis közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak indokolt esetben engedélyezhető és a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.
Eredmény:	A rendszer-segédprogramok ellenőrzött, biztonságos használata.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.5.4. Az összeköttetés/kapcsolat idejének korlátozása	
Cél:	Annak megakadályozása, hogy a szükséges időn túl aktív maradjon az összeköttetés/kapcsolat.
Feladat:	Szabályozni kell, hogy mekkora az inaktív vagy teljes időtartam, amely után az adatkapcsolatot meg kell szüntetni. Ezt az időintervallumot figyelembe kell venni a rendszerek paraméterezésénél, illetve alkalmazások fejlesztésénél. Az időtartam betartandó attól függetlenül, hogy humán beavatkozásról vagy alkalmazás automatikus aktivitásról van szó.
Eredmény:	Bizonyos inaktív vagy teljes időtartam után az összeköttetés megszakításra (ismételt felépítésre) kerül.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.6. Alkalmazás és adat-szintű hozzáférés-ellenőrzés

8.6.1. Adathozzáférés korlátozása	
Cél:	A konkrét alkalmazás egyes funkciói elérésének, használatának korlátozása.
Feladat:	Alkalmazás funkciónként, illetve egyes adatkörökre (adatminősítés, biztonsági szint stb. szerint) vonatkozó hozzáférés szabályozása, a jogosulatlanok kizárása. Fontos az egyes manipulációk, jogosulatlan kísérletek naplózása, a napló állomány rendszeres értékelése. A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni, ez utólag sokszor nehezen megvalósítható.
Eredmény:	Finoman hangolható, jól naplózott hozzáférési rendszer.
Felelős:	Adatgazda és informatikai biztonsági felügyelő/felelős

8.6.2. Érzékeny adatokat kezelő rendszerek elkülönítése	
Cél:	Az érzékeny adatokat kezelő rendszereknek erre a célra létrehozott, elkülönített számítógépes környezettel kell rendelkezniük.
Feladat:	Az egyes rendszereket kategóriákba kell sorolni az általuk kezelt adatok érzékenységének megfelelően. Az érzékenynek minősített adatokat kezelő alkalmazás elkülönítésével hozható létre a szükséges biztonsági szint. A rendszerek besorolását rendszeresen felül kell vizsgálni és aktualizálni kell.
Eredmény:	Kategóriáknak megfelelő biztonságú elkülönített informatikai környezet.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.7. Mobil számítógép használata és távmunka

8.7.1. Mobil számítógép használata és a vele történő kommunikáció	
Cél:	Mobil számítógép biztonságos használatának szabályozása.
Feladat:	A mobil számítógépek (notebook, palm, pda) biztonságos használatának szabályozása. A hozzáférés, a logikai és fizikai biztonság, az adatmentések megvalósítása, illetve a biztonságos környezeten kívüli munkavégzés szabályrendszere is meghatározandó.
Eredmény:	Biztonságos távoli és helyi mobil számítógép használat.
Felelős:	Informatikai biztonsági felügyelő/felelős

8.7.2. Távmunka	
Cél:	A biztonságos távmunka, távoli elérés megvalósítása.
Feladat:	Szabályozni kell, hogy a biztonságos távoli hozzáférés, illetve munkavégzés érdekében milyen tevékenységek és technikai feltételek szükségesek. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani.
Eredmény:	A biztonsági elvárásokat kielégítő távoli munkavégzés.
Felelős:	Informatikai biztonsági felügyelő/felelős

9. Információs rendszerek beszerzése, fejlesztése és működtetése

9.1. Információs rendszerek biztonsági követelményei

9.1.1. Biztonsági követelmények elemzése és meghatározása	
Cél:	Annak biztosítása, hogy a biztonság az informatikai rendszereknek szerves részét képezze.
Feladat:	A fejlesztés vagy beszerzés kezdete előtt, az információs rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket. Előnyben kell részesíteni azokat az informatikai rendszereket, melyek az adott, technológiai jellegű biztonsági intézkedések teljesítéséről értékeléssel rendelkeznek.
Eredmény:	Az információs rendszerekre vonatkozó biztonsági rendszerterv.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.2. Helyes adatfeldolgozás az alkalmazásokban

9.2.1. Bemenő adatok érvényesítése	
Cél:	Az informatikai rendszerek helyes működéséhez szükséges bemenő adatok megfelelőségének biztosítása.
Feladat:	Az informatikai rendszerek bemenő adatainak ellenőrzése mind tartalmi, mind formai szempontból.
Eredmény:	Adatbeviteli ellenőrzési eljárások.
Felelős:	Adatgazda

9.2.2. Belső feldolgozás ellenőrzése	
Cél:	A belső feldolgozás során mind a szándékos, mind a véletlen károkozás kockázatának minimálisra csökkentése.
Feladat:	Az alkalmazásokba érvényességi ellenőrzéseket kell beépíteni, hogy észlelni lehessen az információk feldolgozási hibákból vagy akár a szándékos cselekedetekből adódó bármilyen sérülését.
Eredmény:	A feldolgozás során bekövetkező hiba esélyének jelentős csökkentése.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.2.3. Üzenetek hitelessége és sértetlensége	
Cél:	Az alkalmazások közötti kommunikáció során a hitelesség és a sértetlenség biztosítása.
Feladat:	Meg kell határozni, hogy az alkalmazások közötti kommunikáció során milyen eszközökkel (például aszimmetrikus kulcsú aláírás, szimmetrikus vagy aszimmetrikus titkosítás, időbélyegek alkalmazásával) lehet biztosítani a sértetlenséget és a hitelességet; illetve hogy ezen óvintézkedés mely üzenettípusok esetén szükséges. Az így meghatározott üzenettípusokra a hitelességet és sértetlenséget biztosító eszközök alkalmazását szabályozni kell.
Eredmény:	A kommunikáció hitelességének és a sértetlenségének biztosítása révén a megbízhatóság jelentős növelése.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.2.4. Kimenő adatok ellenőrzése	
Cél:	A kimenő adatok érvényessége, a tárolt információk későbbi feldolgozása helyes és a körülményeknek megfelelő legyen.
Feladat:	Annak biztosítása, hogy mind az automatikus, mind a manuális illesztő felületeken (interface-eken) a megfelelő időben, a megfelelő (szabályozott) struktúrában és adattartalommal jelenjen meg a kimenő információ.
Eredmény:	Az alkalmazások kimenetén szabványos, sértetlen, megbízható adatok jelentkeznek; javítva a szolgáltatás megbízhatóságát.
Felelős:	Adatgazda

9.3. Titkosítási intézkedések

9.3.1. Titkosítási eljárások használatára vonatkozó szabályzat	
Cél:	A titkosítási eljárások használatának szabályozása.
Feladat:	Az adatok védelme érdekében ki kell alakítani, és alkalmazni kell a titkosítási eljárások használatára vonatkozó szabályzatot; valamint ezen szabályzat betartását ellenőrizni kell. A védelem szükséges szintjét a kockázatanalízisre, illetve független értékelésre kell alapozni.
Eredmény:	Megbízható titkosítási eljárások; a bizalmasság, a sértetlenség és a hitelesség megléte.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.3.2. Kulcsmenedzsment	
Cél:	A hatályos jogi szabályozásnak megfelelő, lehetőleg az Európai Unió gyakorlatának és ajánlásainak is eleget tevő kriptográfiai technikákon alapuló kulcsmenedzsment-rendszer kialakítása.
Feladat:	A magyar jogi szabályozásnak eleget tevő, lehetőleg a nemzetközi gyakorlatban is bevált kulcsmenedzsment-rendszerek értékelése; az alkalmazandó kulcsmenedzsment-rendszer kiválasztása, a megfelelő szabályzat kialakítása, bevezetése és betartatása szükséges.
Eredmény:	A titkosítási és hitelesítési, illetve visszafejtési eljárások során megbízható kulcsok kerülnek felhasználásra.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.4. Rendszerfájlok biztonsága

9.4.1. Üzemelő szoftverek ellenőrzése	
Cél:	Megbízható szoftverek használata.
Feladat:	Szabályzatba kell foglalni a szoftverek telepítésének és üzemeltetésének elvárt folyamatát; létre kell hozni a központi, illetve intézményi szoftverkatalógust, s csak az abban szereplő (előzetesen bevizsgált) szoftvereket szabad a számítógépekre telepíteni. Biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.
Eredmény:	Megbízható szoftverek használata, az információ kiszivárgási veszélyének csökkentése.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.4.2. Rendszervizsgálat adatainak védelme	
Cél:	A rendszer vizsgálatához szükséges adatok teljes körű védelmének biztosítása.
Feladat:	A vizsgált adatok körét gondosan kell megválasztani, azokat a teljes életútjuk során folyamatosan védeni és ellenőrizni kell. A személyes adatokat tartalmazó üzemeltetési, tesztelési adatbázisok használatát el kell kerülni.
Eredmény:	A rendszer-felügyeleti adatok sérülési, illetéktelen helyre való kerülési kockázatának jelentős csökkenése.
Felelős:	Adatgazda és informatikai biztonsági felügyelő/felelős

9.4.3. Programok forráskódjához való hozzáférés ellenőrzése	
Cél:	A programok forráskódjához való hozzáférés szabályozása.
Feladat:	A használt programok forráskódját biztonságos helyen kell tárolni, a hozzáférést szigorúan korlátozni és naplózni szükséges. Amennyiben a forráskód nem ellenőrizhető, az önmagában egy kockázati tényezőt jelent.
Eredmény:	A programforráskódok kikerülésének; ily módon a rendszer potenciális sebezhetőségi pontjai illetéktelen helyre kerülésének kockázata jelentősen csökken, ugyanakkor az esetleges hibajavításhoz haladéktalanul rendelkezésre áll az éppen használt verzióban.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.5. Biztonság a fejlesztési és támogató folyamatokban

9.5.1. Változáskezelés szabályozási eljárásai	
Cél:	A változtatások megvalósításának ellenőrzés alatt tartása.
Feladat:	A változtatások végrehajtására változáskezelési eljárásokat kell bevezetni, kidolgozni és betartatni. Biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.
Eredmény:	A változtatások felügyelet alatt tarthatók lesznek; így a rendszer részét képező összes szoftver kontrollálható. Ez a káros programok elleni védelem hatékonyságát is növeli.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.5.2. Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően	
Cél:	A változtatás ne okozzon működési zavart a szervezetben és biztonságában.
Feladat:	A használatban levő rendszerek megváltozásakor meg kell vizsgálni, hogy (főleg a működés szempontjából kritikus) alkalmazások működésére az adott változtatás nincs-e káros hatással.
Eredmény:	Csökken a káros hatás kockázata a használat alatt levő rendszerekre.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.5.3. Szoftvercsomagok változásának korlátozása	
Cél:	A szoftvercsomagok módosításának visszaszorítása a feltétlen szükséges esetekre.
Feladat:	Valamennyi változtatás szükségességét, indokoltságát ellenőrizni kell; minél alacsonyabb szinten kell tartani a szoftvercsomagok változtatását. Változtatás esetén az eredeti verziót meg kell őrizni, s a fejlesztést egy másolaton kell végezni. Az új verziót alapos tesztelésnek kell alávetni, éles bevezetése csak ez után lehetséges.
Eredmény:	A szoftvercsomagok egységessége miatt az esetleges sebezhetőségek javítása kisebb ráfordítást igényel, csökken a sebezhetőség kockázata.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.5.4. Veszélyes (forrás)kódok kiszűrése	
Cél:	Meg kell előzni az információk kiszivárgását.
Feladat:	Az információk kiszivárgásának elkerülése érdekében minden rendelkezésre álló forráskódot le kell vizsgálni/vizsgáltatni használat előtt, hogy nincs e benne „hátsó ajtó”. Csak tiszta forrásból szabad programokat beszerezni. Csak szigorú tesztelés után lehet bármely programot a végleges rendszerbe engedni.
Eredmény:	Kisebb eséllyel kerülnek információk illetéktelen kezekbe.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.5.5. Kiszervezett szoftverfejlesztés	
Cél:	A használatba vétel előtt a szervezeten kívüli eredetű (készített, fejlesztett, javított) szoftvereket kiemelt figyelemmel kell ellenőrizni.
Feladat:	Kiemelt figyelemmel kell kísérni a külső szoftver-fejlesztést; s a kapott programot alaposan felül kell vizsgálni/vizsgáltatni. Csak megbízható forrásból származó szoftvert szabad alkalmazni.
Eredmény:	Az alkalmazott szoftverek alapos vizsgálata révén alacsonyabb eséllyel lesz (trójai típusú) támadásnak kitéve a rendszer.
Felelős:	Informatikai biztonsági felügyelő/felelős

9.6. Műszaki sebezhetőség kezelése

9.6.1. A műszaki sebezhetőségek ellenőrzése	
Cél:	A műszaki sebezhetőség minimális szinten tartása.
Feladat:	Fel kell mérni az alkalmazott rendszerek sebezhető pontjait, s az ezekből fakadó kockázatot meg kell szüntetni (illetve minimalizálni a kockázattal arányosan) megfelelő védelmi intézkedések meghozásával.
Eredmény:	A sebezhető pontok megszűnése.
Felelős:	Informatikai biztonsági felügyelő/felelős

10. Informatikai biztonsági események kezelése

10.1. Informatikai biztonsági események és sérülékenységek jelentése	
Cél:	A biztonsági sérülékenységek és események ismertek legyenek, azokra megfelelő választ adjon a szervezet.
Feladat:	A szervezetnek rendelkeznie kell a biztonsági események osztályozására és jelentésére vonatkozó eljárással. A biztonsági események értékelése és osztályozása az alapja a megfelelő védelmi eljárások kialakításának. Ki kell dolgozni a biztonsági események kezelési eljárását, amely legalább a következőket tartalmazza: – a biztonsági sérülékenységek jelentésére vonatkozó eljárást, – a biztonsági események értékelésére vonatkozó eljárást, – a biztonsági eseményről szóló információ eljuttatása biztosított legyen a megfelelő szintre, – legyen a fenti feladatok ellátásáért felelős személy. Az esemény-kezelést be kell illeszteni a működési környezetbe (helpdesk, Informatikai biztonsági irányítási rendszer stb.).
Eredmény:	Nem marad feltáratlan, megfelelően lereagálatlan biztonsági esemény.
Felelős:	Informatikai biztonsági felügyelő/felelős

10.2. Informatikai biztonsági események kezelése	
Cél:	Az informatikai biztonsági események gyors, hatékony kezelése.
Feladat:	A feltárt és dokumentált eseményeket gyűjteni és rendszeresen értékelni kell. Az események okozta hibákat analizálva meg kell határozni a hibák okát. Ki kell dolgozni egy gyors és hatékony eljárást a problémák megismerésére, hogy minél előbb ismertté és kezelhetővé váljanak. Eljárásokat kell kidolgozni és felelősöket kell megnevezni az informatikai biztonsági események kezelésére. Az események kezelése be kell épüljön az üzemeltetés rendjébe. A feltárt események értékelését (osztályozását) biztosító rendszert kell kialakítani. Az események kezeléséhez bizonyítékokat kell gyűjteni, a megtett intézkedéseket dokumentálni kell annak érdekében, hogy később előforduló hasonló eseményeket már a kialakított módon lehessen kezelni, vagy megelőzni.
Eredmény:	Biztonsági események kezelési eljárása.
Felelős:	Informatikai biztonsági felügyelő/felelős

10.3. Informatikai biztonsági problémakezelési eljárás kialakítása	
Cél:	Az informatikai biztonsági problémák megelőzése, illetve hatékony védekezés kialakítása.
Feladat:	Eljárásokat kell kidolgozni és felelősöket kell megnevezni az informatikai biztonsági problémák megállapítására és kezelésére. A fellépő események okozta hibák értékelése mutat rá a hiba okára, vagyis a problémára. A problémák ellen védelmi intézkedéseket kell hozni, az általuk képviselt kockázatok arányában. A teljes eljárást menedzselni kell, vagyis ki kell alakítani a folyamatot, és felelőst kell rendelni hozzá. Gondoskodni kell az esemény-hiba-probléma nyilvántartásáról annak érdekében, hogy a későbbiekben a hasonló események, illetve hibák esetén már a tapasztalatból kiindulva lehessen intézkedni.
Eredmény:	Problémakezelési eljárás kialakítása.
Felelős:	Informatikai vezető és informatikai biztonsági felügyelő/felelős

11. Működés folytonosságának irányítása

11.1. Működésfolytonosság biztosítása	
Cél:	Az informatikai működés folytonosságának biztosítása.
Feladat:	Működésfolytonossági eljárásokat kell kidolgozni és dokumentálni. Azonosítani kell a dokumentumban – a kritikus informatikai szolgáltatásokat, – az informatikai szolgáltatások megengedett kiesési idejét, – minimális szolgáltatási szintet, – átmeneti eljárásokat, – az informatikai szolgáltatás visszaállítási eljárásokat. Meg kell határozni azokat az infrastruktúrákat és szolgáltatásokat, melyeknek működniük kell lokális események/katasztrófák esetén is, hogy ezáltal nyújtsanak informatikai támogatást az esemény elhárításához. Ezekre nézve ki kell alakítani a megfelelő tartalékokat. Szabályozni kell működtetésüket és használatukat, és rendszeresen vizsgálni kell működőképességüket. Az eljárásokat tesztelni kell és a dokumentumot évente, illetve a releváns változások alkalmával felül kell vizsgálni.
Eredmény:	Működésfolytonossági terv (dokumentum). Tesztterv, jegyzőkönyvek.
Felelős:	Üzemeltetési vezető és informatikai biztonsági felügyelő/felelős

11.2. Informatikai katasztrófa-elhárítási terv	
Cél:	A kritikus informatikai erőforrások működésének visszaállítása.
Feladat:	Az informatikai működés sérülhet az informatikai erőforrás katasztrófa jellegű kiesése esetén. A katasztrófaelhárítási terv kiterjed: – a kritikus informatikai erőforrások azonosítására, – az elviselhető kiesési időablak meghatározására, – az erőforrások pótlására/visszaállítására történő eljárások kialakítására az időablakon belül, – a felkészülés, a válasz és a visszaállítás feladatainak meghatározására, felelősök hozzárendelésére. Az eljárásokat tesztelni kell, és a dokumentumot évente, illetve a releváns változások alkalmával felül kell vizsgálni.
Eredmény:	Informatikai katasztrófa-elhárítási terv (dokumentum). Tesztterv, jegyzőkönyvek.
Felelős	Üzemeltetési vezető és informatikai biztonsági felügyelő/felelős

12. Követelményeknek való megfelelés

12.1. Jogi követelményeknek való megfelelés	
Cél:	Jogszerű informatikai működés és szolgáltatások.
Feladat:	Az informatikai működés során fenn kell tartani a jogszabályi megfelelést. Az informatikai működésre hatással lévő jogszabályok azonosítása, és a megfelelés dokumentálása. Eljárás kidolgozása a megfelelés fenntartására, időszakos (évenkénti) felülvizsgálata.
Eredmény:	Vonatkozó jogszabályok listája. A jogszabályoknak megfelelő eljárások. Eljárás a jogszabályi megfelelés fenntartására.
Felelős:	Üzemeltetési vezető

12.2. Biztonsági szabályzatnak és az auditálási követelményeknek való megfelelés, és műszaki megfelelőség	
Cél:	Az informatikai működés megfelelőségének biztosítása érdekében az auditálási követelményeket is figyelembe vevő szabályzatok készítése.
Feladat:	Eljárás kidolgozása a biztonsági szabályzatnak, szabványoknak való megfelelés ellenőrzésére. Éves ütemterv alapján és releváns változások alkalmával ellenőrizni kell a biztonsági eljárások tartalmát és működését. Eljárást kell kidolgozni a biztonsági szabályozás, illetve auditálásra való felkészülés során figyelembe vett szabványok figyelemmel kísérésére és a változások nyomán végrehajtandó teendőkre.
Eredmény:	Eljárás és ütemterv a biztonsági ellenőrzésre. Eljárás a szabványok változásának nyomon követésére.
Felelős:	Informatikai biztonsági felügyelő/felelős

12.2.1. Auditálási szempontok	
Cél:	Biztosítani kell, hogy a védelmi intézkedések a szabályzatokban leírtak szerint megvalósuljanak.
Feladat:	Ki kell dolgozni a védelmi intézkedések felülvizsgálatának rendszerét, kitérve az alkalmazott felülvizsgálati eljárásra, a végrehajtás gyakoriságára és az érintettek felelősségére és feladataira. Javasolt külső, független szakértőt bevonni az ellenőrzésbe.
Eredmény:	A védelmi intézkedések rendszeres, módszeres felülvizsgálata, javító intézkedések. (Független állásfoglalás a védelmi intézkedések megvalósulásáról.)
Felelős:	Informatikai biztonsági felügyelő/felelős

12.2.2. Értékelési szempontok	
Cél:	Biztosítani kell, hogy a műszaki megfelelőségi követelmények az elvárásoknak megfelelően megvalósuljanak.
Feladat:	Amennyiben a beszerzés során a komplett szolgáltatói rendszer értékelését nem nyújtották be, a megfelelőség-értékelésre külön jogszabály alapján feljogosított értékelő szervezettel értékeltetni kell a hardver eszközök, hálózatok, az ezekből kialakított komplex informatikai rendszerek megfelelőségét. Javasolt külső, független szakértőt bevonni az ellenőrzésbe.
Eredmény:	A műszaki védelmi intézkedések megfelelő szintjének garantálása. (Független állásfoglalás a védelmi intézkedések megvalósulásáról.)
Felelős:	Informatikai biztonsági felügyelő/felelős

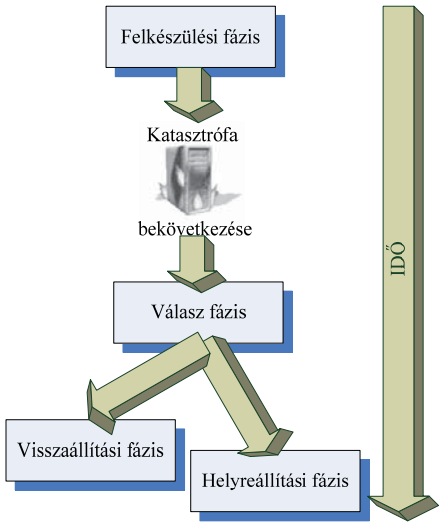
2. melléklet a 223/2009. (X. 14.) Korm. rendelethez

A központi elektronikus szolgáltató rendszer informatikai katasztrófaelhárítási tervének alapkövetelményei

1 Az informatikai katasztrófaelhárítási terv feladata

Az IKeT (informatikai katasztrófaelhárítási terv) célja a központi rendszert üzemeltető szervezet felkészítése arra, hogy kezelni tudja azokat a helyzeteket, amikor az informatikai erőforrások átfogó sérülése miatt a rendszerek folyamatos és rendeltetésszerű működése megszakad.

Az informatikai katasztrófaelhárítási időszakokra bontott feladatai:



1. ábra: Az informatikai katasztrófaelhárítás fázisai

1.1. Katasztrófa előtti felkészülési feladatok

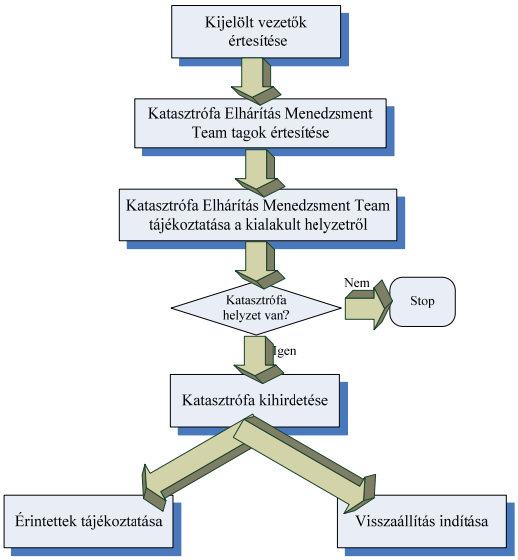
Katasztrófa előtti felkészülési feladatok ellátásakor az üzemeltetőnek meg kell tennie azokat a szükséges intézkedéseket (felkészülési fázis), melyek biztosítják számára, hogy katasztrófahelyzet esetén rendelkezésre álljanak a sikeres elhárításhoz szükséges erőforrások és teljesüljenek a szükséges feltételek.

A felkészülési fázis implementációs tervében felsorolt feladatok végrehajtása biztosítja azt, hogy az üzemeltető szervezet teljesíteni tudja a működtető elvárásait, vagyis az informatikai rendszerek visszaállítását a megjelölt időtartamon belül. A felkészülési fázis meghatározza azokat az adminisztratív, szervezési, illetve technikai intézkedéseket, amelyeket az üzemeltetőnek végre kell hajtania. A felkészülési fázisban kerül sor a szükséges beruházásokra, eszközök beüzemelésére, részletes és konkrét eljárások kidolgozására, tesztelésre, illetve az érintett munkatársak oktatására. A felkészülési fázis főbb feladatai tehát az alábbiak:

– Az informatikai katasztrófaelhárításban részt vevő csoportok létrehozása, tagjaik felelősségi körének meghatározása, és megbízása a feladatok ellátásával.
– Az informatikai katasztrófaelhárításhoz szükséges dokumentációk biztosítása, különös tekintettel a mentés-visszaállítás dokumentációira, majd az egyéb (leltárak, szerződések, értesítési listák stb.) dokumentumok.
– A szállítók rendelkezésre állásának biztosítása.
– Az informatikai katasztrófaelhárítási tevékenységek menedzselésére szolgáló Katasztrófakezelő Központ kijelölése.
– Az informatikai rendszer erőforrásigényének (hardverek, szoftverek, adatok, dokumentációk stb.) biztosítása.
– Az egyes fázisok pénzügyi feltételeinek biztosítása.
– Az Informatikai Katasztrófaelhárítási Terv tesztelése és oktatása.

1.2. Informatikai katasztrófa bekövetkezésekor végrehajtandó feladatok

Katasztrófa utáni feladatok, amikor az üzemeltető mozgósítja az elhárításban részt vevő munkatársait (válasz fázis) és megkezdi az informatikai szolgáltatások lehetőség szerinti tartalék rendszereken való működésbe állítását, (visszaállítási fázis), majd a károk elhárítását követően a rendszerek újraindítását, valamint a normál üzemi állapot helyreállítását (helyreállítási fázis).



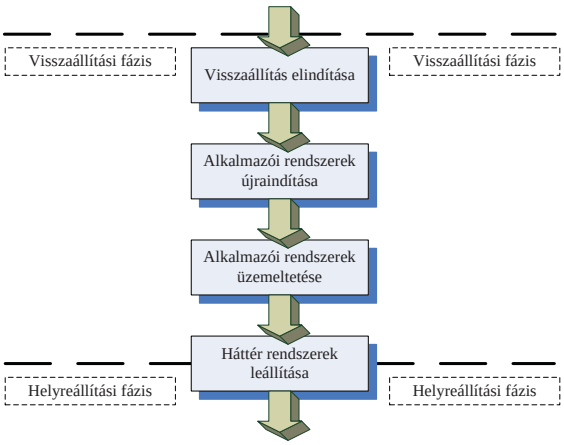
2. ábra: Válasz fázis

1.2.1. Válasz fázis

A válasz fázis során történik a katasztrófa felismerése, az érintettek riasztása, az emberi élet és az eszközök mentése. Előzetes helyzetértékelés alapján kihirdetésre kerül az informatikai katasztrófa. Az érintettek tájékoztatást kapnak a kialakult helyzetről.

1.2.2. Visszaállítási fázis

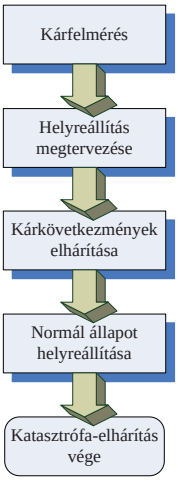
A visszaállítási fázis során történik az informatikai rendszerek lehetőség szerinti átállítása a tartalék eszközökre, illetve a rendszerek helyreállítása a rendelkezésre álló tartalék eszközök felhasználásával a lehető legrövidebb időn belül. Az elsődleges prioritású feladat a már létező párhuzamos alrendszerek bekapcsolása, mely esetben ellenőrizni kell, hogy hibamentesen működnek-e, ezek után – vagy elegendő erőforrás rendelkezésre állása esetén ezzel egy időben – kezdődhet meg a kiesett rendszer(ek) normál üzemi állapotba való helyreállítása.



3. ábra: Visszaállítási fázis

1.2.3. Helyreállítási fázis

A helyreállítási fázis feladata a kritikus folyamatokhoz szükséges, eredetivel azonos funkcionalitású, lehetőség szerint az eredetivel azonos erőforrások biztosítása (beszerzés, üzembe állítás, javítás stb.). Ezen fázis akkor ér véget, amikor az informatikai rendszer az eredetivel legalább azonos módon működőképes.



4. ábra: Helyreállítási fázis

Az Informatikai Katasztrófaelhárítási Terv akkor válik alkalmazhatóvá, amikor a felkészülési fázis feladatait végrehajtották, a tervdokumentumban előírt visszaállítási és helyreállítási lépéseket tesztelték, és a tervet oktatták minden érintett számára.

2. Keretdokumentum

2.1. Informatikai katasztrófaelhárítási terv célja

Az informatikai katasztrófaelhárítási terv alapvető célja, hogy felkészítse a központi rendszert azokra a váratlan hatásokra, amelyek a rendszer folyamatos működését és/vagy az informatikai rendszerek funkcionalitását veszélyeztetik, különös tekintettel a katasztrófahelyzetben történő mentés-visszaállítási feladatokra.

A tervezésnek az a célja, hogy minimalizálja a kockázatokat, az üzemelési stabilitást olyan szinten biztosítsa, amely az informatikai infrastruktúrát érintő katasztrófa esetén a károkhoz mérten optimális költségekkel és gyorsasággal teszi lehetővé a szolgáltatások visszaállítását és helyreállítását, illetve figyelembe vegye a redundáns rendszerfelépítés által biztosított lehetőségeket arra az esetre, hogy lokális katasztrófahelyzetek esetén is egyes szolgáltatások folyamatosan működjenek.

2.2. Az informatikai katasztrófaelhárítási terv hatálya

Az üzemeltető által elkészített IKeT hatálya ki kell terjedjen:

– az üzemeltető által üzemeltetett központi elektronikus szolgáltató rendszer (központi rendszer – KR), informatikai és távközlési eszközeire;
– azon végponti informatikai eszközökre, melyek üzemeltetésére az üzemeltető külön szerződés keretében vállalkozott;
– az üzemeltető és a működtető minden olyan alkalmazottjára, akik a tervben megnevezésre kerültek;
– az üzemeltetővel, illetve a működtetővel a központi rendszerre vonatkozó szerződéses viszonyban tevékenykedő természetes vagy jogi személy(ek)re, jogi személyiséggel nem rendelkező szervezet(ek)re, a velük kötött szerződés alapján;
– a központi rendszer informatikai eszközeinek üzemelési helyszíneire.

2.3. Az informatikai katasztrófaelhárítási terv felépítése

A katasztrófák kezeléséhez rendkívül sok információ és a jól körülhatárolt tevékenység ismerete szükséges. Azon információk és feladatok gyűjteménye az IKeT, amelyek elősegítik a központi rendszer folyamatos működésének megóvását abban az esetben, ha valamilyen, az informatikai infrastruktúrát érintő katasztrófa történne.

Az IKeT elkészítésénél figyelembe kell venni a központi rendszer jellegéből, működéséből, üzemeltetéséből adódó sajátosságokat. Ennek értelmében az informatikai katasztrófaelhárítási tervben az informatikai erőforrásra vonatkozóan a részletes visszaállítási lépések nem, csak a végrehajtási utasítások szintjén kerülnek meghatározásra. Az IKeT

a katasztrófahelyzet esetén történő mentést és visszaállítást tekinti elsődlegesnek, míg a további teendőket tartalmazó dokumentációkat kizárólag meghivatkozza, illetve felkészíti a működtetőt és az üzemeltetőt arra, hogy reagálni, intézkedni tudjon egy esetlegesen bekövetkező, a központi rendszer informatikai infrastruktúráját érintő katasztrófaesemény esetén.

2.3.1. Az informatikai katasztrófaelhárítási tervben megjelenő alkalmazások, rendszerek

Az informatikai katasztrófaelhárítási tervben meg kell jelenjenek mindazon informatikai erőforrások, melyek „Az informatikai katasztrófaelhárítási terv hatálya" című pontban akár közvetetten említésre kerültek.

2.3.2. Az informatikai katasztrófaelhárítási terv kidolgozása során nem érintett rendszerek

Az IKeT célja a központi rendszer működése szempontjából kritikus rendszerek mielőbbi visszaállíthatóságának biztosítása. Ebből kifolyólag az IKeT nem foglalkozik azokkal az informatikai rendszerekkel és szolgáltatásokkal, amelyekre a következő feltételek közül akár egy is teljesül:

– Amely informatikai rendszer nem befolyásolja közvetlenül, kritikus jelleggel a központi rendszer működését, így már a vizsgálat alá vont rendszerek közé sem került be.
– Azon rendszerek, amelyek nem elsődlegesen a központi rendszer informatikai működését szolgálják, hanem egységet képeznek bármilyen más célú irányító, vezérlő, telekommunikációs vagy nem tisztán informatikai vonatkozású rendszerrel.
– Amelyek a központi rendszer működtetésében részt nem vevő irodai (szövegszerkesztés, táblázatkezelés, prezentáció, kép-, zene-, videó-szerkesztés) rendszerek tevékenységét támogatják, illetőleg az EKG működése szempontjából nem a főtevékenységhez kapcsolódó rendszerek (ugyanakkor egy hivatal működésében lehetnek ezek a kritikusak).
– Más a központi rendszerhez kapcsolódó rendszerek esetében eseti elemzéssel kell meghatározni, mely rendszerek szükségesek az alapműködéshez, és melyek sorolhatók hátrább a helyreállítás szempontjából.

3. Kiindulási feltételek

3.1. A változó informatikai környezet hatásai

Az IKeT használatakor figyelembe kell venni, hogy az egy aktuális állapot alapján készült. Fel kell készülni arra, hogy a környezet, a működési folyamatok, és az erőforrások változása befolyásolják annak használhatóságát. Az ismert infrastrukturális változásokat, a terv aktualizálásánál folyamatosan figyelembe kell venni, illetve a tervet folyamatosan aktualizálni kell minden érdemi változásnál.

Az IKeT készítésének időpontjához képest bekövetkező változásokat az IKeT karbantartásáért felelős szervezetnek rendszeresen, illetve jelentős változások esetén ki kell értékelnie, azok alapján a szükséges módosításokat át kell vezetnie az IKeT-ben.

3.2. Kapcsolat a központi rendszer fizikai, tűz- és vagyonvédelmét biztosító szabályzatokkal, dokumentumokkal

Az IKeT az informatikai infrastruktúrát érintő katasztrófaeseményeket tárgyalja. Az informatikai infrastruktúrát is érinthetik az üzemeltető, illetve működtető meglévő általános fizikai, tűz- és vagyonvédelmi szabályzatai. Ezen okokból az IKeT nem foglalkozik kiemelten a címben felsorolt szabályzatok hatálya alá tartozó védelmi intézkedésekkel, ezzel elkerülve az azonos területek többszöri szabályozásából eredő ellentmondások lehetőségét.

A fizikai, tűz- és vagyonvédelemmel kapcsolatos dokumentációk a működtetőnél és az üzemeltetőnél kell megtalálhatók legyenek.

3.3. Biztonsági követelmények biztosítása

Az informatikai biztonsági irányelvekben és az informatikai biztonsági szabályzatban (mely a kapcsolódó szervezetekre is állapít meg követelményeket) meghatározott elveket és biztonsági követelményeket az IKeT folyamatai során, a terv minden fázisában érvényesíteni kell, amely érvényesítés az informatikai biztonsági felügyelő/felelős feladata és felelősségi köre. Az esetlegesen bekövetkező informatikai katasztrófa esetén különösen fontos, hogy a visszaállítás és a helyreállítás szakaszában is ugyanazt a biztonsági szintet kell biztosítani, mint ami az informatikai biztonsági irányelvben elő van írva. Olyan eljárásokat kell kidolgozni a visszaállítás és a helyreállítás időtartamára, hogy ne sérüljenek a szervezési és technikai biztonsági követelmények, és alkalmazhatók legyenek a védelmi intézkedések.

A rendelkezésre állás szempontjából a legösszetettebb és legkritikusabb biztonsági követelmény bizonyos – már az elhárítást tevékenységét is támogató – informatikai rendszerek minimális szinten történő működésének biztosítása. A rendszerek tartalékolását úgy kell kialakítani, hogy minél gyorsabb helyreállítást garantáljon, azaz katasztrófa bekövetkezése esetén a sérült rendszereket minél hamarabb vissza lehessen állítani.

Kezelendő veszélyforrások

Az informatikai és információs rendszereket tekintve a veszélyforrások egy része az informatikai, információ biztonság egy-egy területén jelentkezik, mint részleges, jól behatárolható sérülékenység.

A veszélyforrások másik része globális jellegű. Az ilyen átfogó veszélyforrásokból adódó fenyegetés bekövetkezte az informatikai rendszeren keresztül a szervezet teljes működésére hatással lehet, adott esetben teljesen megbénítva azt. Az IKeT ezekkel, a szervezet egészére kiterjedő veszélyforrásokkal foglalkozik, oly mértékben, hogy feltételezi, nem a teljes informatikai infrastruktúra (informatikai és fizikai környezet) semmisül meg.

3.4. A folyamatos üzemmenet biztosítása

A központi rendszer többek között szolgáltatásokat és informatikai kapcsolatokat biztosít. Az intézmények ezt felhasználva nyújtanak az állampolgárok, más kapcsolódó szervezetek, uniós és más nemzetközi intézmények számára szolgáltatásokat és információkat. Mindezen funkciók biztosítása érdekében a központi rendszer rendszerszolgáltatásainak folyamatos működése szükséges. A szolgáltatások kiesésének megakadályozására biztosítani kell a szükséges erőforrásokat mind humán, mind eszköz oldalról. Az üzemmenet folyamatossága szempontjából kiemelt fontosságú a cél a két telephelyes működés, telephelyenként belsőleg redundáns rendszerekkel, megfelelően képzett tartalék eszközkészlettel, a személyzet kellő felkészítése, valamint a dokumentációk naprakészen tartása.

3.5. Két központos működés feltételei

A központi rendszert alkotó alrendszerek esetében a futtatásra használt hardver környezet kialakításánál cél a hibatűrő felépítés. Ennek érdekében az eszközök belső kialakítása amennyire lehet, redundáns. Az áramszünet miatt bekövetkező adatvesztés kivédését szolgálják a szünetmentes tápegységek és a tartalék tápellátás, amely biztosítja a klímarendszerek folyamatos működését is. Ez a kialakítás jelentősen csökkenti az eszközök meghibásodásából fakadó adatvesztés és esetleges leállás lehetőségét, azonban nem nyújt teljes biztonságot a szolgáltatás leállása ellen. A magas rendelkezésre állású infrastruktúra/szolgáltatás biztosításához szükséges, hogy az egyik eszköz meghibásodása esetén egy másik – átvéve a funkcionalitást – folyamatossá tegye a szolgáltatás működését.

A szolgáltatás kiesését okozhatja természeti katasztrófa is. Ilyen eset (például árvíz) az informatikai rendszer minden elemét érintheti, így az egy központban futó szolgáltatások megszakadása következhet be, ezért szükséges a magas rendelkezésre állást biztosító rendszerek legalább két központba történő területi szétválasztása.

A szolgáltatási központok olyan szintű területi elkülönítése szükséges, amely biztosítja, hogy egyazon esemény lehetőleg ne veszélyeztethesse valamennyi központ működését. A két központos működés kialakításánál figyelembe kell venni, hogy mindkét központban rendelkezésre kell álljon olyan helyiség (kiépített hálózattal, munkahelyekkel, munkaállomásokkal, telefonnal stb. ellátva), ahonnan a rendszereket üzemeltetni lehet.

3.6. Átállás a két központ között

Nem minden szolgáltatás esetén van szükség a teljes tartalékolásra, de jó néhány szolgáltatás (internet-kapcsolat, országos hálózati összeköttetések, DNS, Mail stb.) esetében elengedhetetlen, hogy bármely felmerülő probléma, meghibásodás esetén a másik központ teljes értékűen átvegye az éles üzemi működést. Az egyik központban a szolgáltatás bármely elemének kiesése esetén automatikus kell legyen a rendszer átállása a másik központra. Ilyen esetben a rendszert üzemeltető személyzet csak eseményként érzékeli az átállás tényét, majd riasztást kap a helpdesk ügyeletesen keresztül a rendszer leállásának tényéről.

Az átállás azonban nem csak katasztrófa esetben lehet indokolt, hanem sor kerülhet rá tesztelési jelleggel (katasztrófahelyzet szimulációjaként) vagy tervszerűen, karbantartási folyamatok részeként is. Az ilyen átállási esetek közös jellemzője, hogy a másik központra történő átállást követően a karbantartási tevékenységek végrehajtása idejére csak egy központ biztosítja a szolgáltatást, így megnövekszik a szolgáltatás kiesésének kockázata. Ezért az ilyen tervszerű átállásokat (a karbantartási tervben rögzített időpontokat a terv elfogadásakor kell jóváhagyni) a működtető írásos engedélye alapján ütemezetten (lehetőleg a központi rendszer alacsony kihasználtságú időszakában, pl. éjjel vagy munkaszüneti napon) előre tesztelten, a lehető legrövidebb idő alatt kell végrehajtani.

3.7. A hálózati kapcsolatokat biztosító szolgáltatói követelmények

A központi rendszer folyamatos működtetéséhez megfelelő telekommunikációs kapcsolatok szükségesek. Nem biztosítható a központi rendszer szolgáltatásainak folyamatos elérése az intézmények, más kapcsolódó szervezetek, személyek számára, ha a hálózati kapcsolatok kiesése miatt a központi rendszer nem érhető el. Ennek érdekében a telekommunikációs szolgáltatók kiválasztásakor azok műszaki alkalmasságát elsődleges szempontként kell figyelembe venni. Szükség esetén akár több szolgáltató bevonásával, vagy redundanciák kialakításával kell biztosítani a hálózati kapcsolatok megfelelő szintű rendelkezésre állását.

3.8. Az üzemeltetés és katasztrófaelhárítás személyi és dokumentációs feltételei

3.8.1. A személyzet felkészültsége a rendkívüli helyzetek kezelésére

Az üzemeltető részletes üzemeltetési szabályzattal kell rendelkezzen, melyet folyamatosan karban kell tartania. Az üzemeltetőnek minden új alrendszer indításánál biztosítani kell a szükséges dokumentációkat, és a megfelelő képzésben kell részesíteni munkatársait.

Az informatikai rendszerek karbantartását végző személyzet tagjait a felelősségi területükön folyamatosan képezni kell, az oktatásokról és a megszerzett képesítésekről dokumentációt kell vezetni. A vezetőnek gondoskodniuk kell a megszerzett ismeretek szinten tartásáról és ellenőrzéséről. A rendszer-visszaállítási tesztekről jegyzőkönyvet kell felvenni. Az üzemeltető minden rendszermérnökének rendelkeznie kell a katasztrófahelyzet esetén a visszaállításhoz szükséges ismeretekkel.

3.8.2. Dokumentumkezelés

Az érintett rendszer jellegétől, összetettségétől, a szolgáltatáskiesés súlyától függően kell meghatározni a megkövetelt dokumentumok körét.

A katasztrófaelhárítás szempontjából minimálisan szükséges (folyamatosan karbantartott) dokumentációk köre:

– Informatikai Biztonsági Szabályzat,
– Üzemeltetési szabályzat(ok) és eljárásrendek,
– Informatikai Katasztrófaelhárítási Terv,
– Rendszerdokumentációk,
– Üzemeltetési napló.

Katasztrófahelyzet esetén a dokumentumok többféleképpen állhatnak rendelkezésre:

– a hálózaton egy publikus könyvtárban (hozzáféréssel csak az érintett személyek rendelkeznek) megtalálhatók a jóváhagyott dokumentumok legfrissebb verziói (dátum, valamint verziószám alapján azonosítható),
– az üzemeltető telephelyén, páncélszekrényében megtalálható a központi dokumentációk legfrissebb verziója kinyomtatva,
– a havi mentések során valamennyi, a mentés napján aktuális központi dokumentációt mentenek (a mentésbe a minden aktuális a rendszerrel kapcsolatos dokumentumot szerepeltetni kell), melyet 3 különböző helyen tárolnak.

3.9. Helyreállítási feltételek rendelkezésre állásának vizsgálata

Katasztrófahelyzetben a kockázatok csökkentése érdekében kiemelt fontosságú a meghibásodott rendszer működésének helyreállítása. A helyreállítási időintervallum csökkentésére megfelelő tartalékeszköz készletet kell kialakítani. A meghibásodott hardver helyén a tartalékeszköz üzembe helyezését követően kezdődhet meg szükség esetén a rendszer telepítése, konfigurálása és a szolgáltatás helyreállítása. Ez a művelet a rendszer összetettségétől, illetve konfigurációjától függően akár hosszadalmas is lehet, ezért a rendszerelemekről készített mentések során az adatmentésen kívül (rendszeres időközönként, illetve a rendszer változtatása esetén) rendszermentést, alkalmazásmentést is kell készíteni. A mentésből történő helyreállításhoz rendelkezésre kell állnia minden központban a megfelelően beállított mentési rendszernek és a rendszerekről készített mentéseknek. A mentések sikerességét ellenőrizni kell.

3.10. Alkalmazott mentési rendszer

Egy informatikai katasztrófa bekövetkezte után az informatikai szolgáltatások működőképessé tételéhez alapvetően szükségesek a mentési és kapcsolódó eszközök, illetve a mentéseket tartalmazó adathordozók.

Az adatok és az üzemeltetés biztonsága érdekében, továbbá a jogszabályi előírások következtében az üzemeltetett rendszerek adatairól és programjairól (a továbbiakban: állományok) rendszeresen, illetve egyes tevékenységekhez kapcsolódóan az üzemeltető eseti jelleggel másolatokat készít, és ezeket, a rendszereket kiszolgáló eszközöktől fizikailag elkülönített, biztonságos helyen, hibátlan minőségben őrzi. A mentések célja nem csupán az adatmegőrzés, hanem az is, hogy a rendszerek meghibásodás, hibás feldolgozás vagy katasztrófa után – adott korábbi időpontbeli állapotukban – teljeskörűen reprodukálhatók legyenek.

Egy másolat, vagy egy állapot tényleges megőrzési ideje változó és a biztonsági követelmények alapján kiválasztott mentési megoldás függvénye. A tényleges megoldáshoz különböző módszerek állnak rendelkezésre, ezek közül az üzemeltető – szükség szerint – a normál és a rotációs módszert alkalmazza.

Szükség szerint végezhető teljes vagy különbözeti (inkrementális) mentés. Teljes mentés esetében a kijelölt állományokról készül másolat. A különbözeti mentés esetében csak a változásokról.

A mentés technikáját illetően központi, illetve lokális mentések alkalmazhatóak. A lokális mentés egy másik merevlemezre vagy a számítógépbe épített mobilizálható adathordozóra (optikai lemez, DAT, DLT, LTO stb.) történhet. A központi mentés esetében a hálózaton keresztül egy általában nagykapacitású (DLT/LTO) egységre, egy másik gépre, vagy storage-ra történik a mentés.

A mentési rendszerrel szemben támasztott követelmény, hogy a mentési eljárások során alkalmazott módszerek legyenek függetlenek az operációs és az adatkezelő rendszerektől, ilyen tekintetben legyenek általánosan használhatók. A módszerek legyenek rugalmasak, hogy az eljárások tartalmát és gyakoriságát az egyes rendszerek egyedi követelményeihez lehessen igazítani. A módszereknek – igény szerint – biztosítaniuk kell a kielégítő eseti, munkanaponkénti, heti, havi, éves mentéseket, illetve archiválásokat.

Az eljárások gyakorisága és időpontjai, a másolásra kerülő állományok köre úgy kerüljön meghatározásra, hogy a rendszer egy adott időpontbeli állapotában teljeskörűen reprodukálható legyen. Ennek biztosításához az alkalmazói és rendszermentési eljárásokat tartalmi és időbeni állapotukban is össze kell hangolni.

Mentések:

– Üzemi mentések;
– Rendkívüli mentés (pl. rendszerszoftver váltásakor);
– Archiválás.

Eljárások tartalmi kérdései

Az alkalmazói rendszer jellegű szolgáltatásokhoz kapcsolódó mentési eljárásokkal szembeni követelmények (tartalom, megőrzési idők, példányszámok) a kapcsolódó üzemeltetői dokumentációkban kell szerepeljenek. Nem alkalmazói rendszer jellegű szolgáltatások esetében a szükséges mentési eljárások követelményeit az illetékes rendszer felügyelője határozza meg. A rendszermentés követelményeit a rendszerprogramok (operációs rendszer, adatbázis kezelő) dokumentációja írja elő. A rendszeradatok (pl. jelszó és jogosultsági adatok) mentésére vonatkozó követelményeket – ha azokról a rendszerdokumentáció nem intézkedik – az érintett rendszer felügyelője határozza meg.

A tényleges eljárás részleteit, az eljárás ciklusát és időpontjait, a másolatok példányszámát és megőrzési idejét, valamint az alkalmazandó módszert rendszerekre szabottan a rendszer felügyelője dolgozza ki.

Egy fizikai eljárás több rendszer állományainak másolását is tartalmazhatja. A rendkívüli mentési eljárás sajátossága, hogy az alkalmazói és a rendszerkörnyezetre egyaránt kiterjedhet.

3.10.1. Adathordozók nyilvántartása

A mentés során használt adathordozók tárolását, felhasználását és hozzáférését az üzemeltetőnek nyilván kell tartania.

– Az adathordozók tárolását, felhasználását és hozzáférését szabályozzák, nyilvántartják, rendszeresen és dokumentáltan ellenőrzik. Az ellenőrzés a rendszerfelügyelő feladata.
– Az üzemeltető által üzemeltetett szervereken leltár szerint kiadott, azonosítóval ellátott és nyilvántartásba vett adathordozót kell használni. Az Adathordózók nyilvántartásában vezetni kell a sorszámot, valamint az adathordozó egyéb adatait is.
– Minden mágneses és többször írható optikai adathordozón szerepeltetni kell az első használatba vétel dátumát.
– A használatba vett adathordozón fel kell tüntetni a szerver azonosítóját, nevét és az eljárás fajtáját.
– A rotációs módszerek keretében használt adathordozókat az első alkalommal azonosítóval kell ellátni. A belépő új adathordozó a rotációs táblázat szerinti sorrendben kerül alkalmazásra.
– Az archív státuszba kerülő adathordozót ki kell egészíteni a tartalmának megfelelő dátum, státusz és a kópiaszám adatokkal.
– Az információkat elsődlegesen az adathordozón kell feltüntetni.
– Minden adathordozót újraalkalmazás előtt, felszabadítás, selejtezés után az adatok megsemmisítését eredményező megfelelő eljárásnak kell alávetni. A mágneses adathordozót törölni kell, az optikai és egyéb újra nem írható adathordozót fizikailag alkalmatlanná kell tenni a későbbi felhasználásra. A törléseket szintén dokumentálni kell az Adathordozók Nyilvántartásának megfelelő részébe történő bejegyzéssel. Fel kell tüntetni a törlés vagy megsemmisítés dátumát, okát, az adathordozó azonosítóját, a törlést vagy megsemmisítést végző aláírását.

3.10.1.1. Másolati példányok, adathordozók tárolása és védelme

Az üzemeltetés- és adatbiztonság érdekében a rendkívüli mentésekből és az archivált anyagokból másod- (és harmadpéldányt) is szükséges készíteni, melyekből egy példányt az üzemeltető telephelyén kívül kell tárolni.

Az adatok információvédelmének és az üzemeltetett alkalmazások megbízható működésének biztosításában – és egy esetleges katasztrófa esetén a helyreállításban – nagy szerepet játszik a mentéseket tartalmazó adathordozók és közvetlen dokumentációik fizikai védelme. Ezért biztosítani kell az adathordozók és dokumentációk tűz- és vagyonvédett tárolását. Az üzemeltető telephelyén lehetőleg 24 órás tűz- és vízállóságot biztosító szekrényt, az elkülönített telephelyen jól zárható, lemezszekrényt kell használni.

A rendszerjelszavakat (system password, root password stb.) lezárt – pontosan azonosított – borítékokban szintén két telephelyen szükséges tárolni.

3.10.1.2. Dokumentálás

A mentések elvégzése után a mentést végzőnek, automatikus mentés esetén az ellenőrzést végzőnek a mentéseket papíron is dokumentálni kell az Üzemeltetési Napló megfelelő szakaszában (mentésre vonatkozó bejegyzések). A dokumentumnak tartalmaznia kell a mentés dátumát, a hordozó azonosítóját, a mentést végző nevét és aláírását, valamint a mentésre vonatkozó esetleges megjegyzést – utasítást. Ha a mentés időzített, akkor az előző napi mentés sikerességét minden esetben ellenőrizni kell.

3.10.2. Mentési rend

Az egyes rendszerek/alrendszerek mentéséről részletesen az Informatikai Biztonsági Szabályzat, az Üzemeltetési Szabályzat és a Mentési Eljárások, valamint az egyes rendszerek rendszerdokumentációi kell, hogy tételesen rendelkezzenek.

3.10.3. A két telephelyes mentés kialakítása

Amennyiben létezik, úgy a második központban is szükséges a központi rendszer szerverek naplóállományainak és teljes rendszermentéseinek tárolására szolgáló infrastruktúra, illetve annak archiváló rendszere. A két központ között a megfelelő sávszélességű adatátviteli kapcsolat szükséges.

3.11. Háttér és szállítói stratégia

A rendszer biztonsága szempontjából a szolgáltatási, beszállítói háttérrel való kapcsolatrendszer kritikus jelentőségű a katasztrófaelhárítás szempontjából. Ennek alapján lehet meghatározni a szükséges tartalékolás terjedelmét, természetét, a szükséges saját erőforrásokat. Itt kell dönteni arról, hogy mely funkciók kiesése elviselhető, melyek azok, amelyek azonnali pótlása nélkülözhetetlen.

3.11.1. Szállítói és támogatási szerződések

Minden szállítói és támogatási szerződésből egy-egy másolati példányt el kell helyezni azokon a telephelyeken és helységekben, amelyeket az informatikai katasztrófaelhárítási terv meghatároz.

3.11.2. Szállítók

A szerződésekkel együtt nyilván kell tartani a rendszerek kifejlesztésében közreműködő vállalkozásokat és szállítókat, s azok részvételi kompetenciáit és elérhetőségeiket, hogy katasztrófahelyzet esetén, amennyiben ezt a kialakult helyzet indokolja, a szállítók a helyreállítás feladatába bevonhatók legyenek.

3.12. Ellenőrzőlista

Az alábbi táblázatban található „minta" ellenőrzőlista azt a célt szolgálja, hogy az IKeT karbantartása esetén figyelembe veendő, az informatikai erőforrásokra és szolgáltatásokra vonatkozó vizsgálati kritériumok teljesülését az egyenszilárdság elve alapján ellenőrizni lehessen. A táblázatban felsorolt kritériumok természetesen tetszőlegesen, szabványok, ajánlások, módszertanok vagy egyedi igények alapján bővíthetőek.

Kritérium Rendszer	Rendszer1	Rendszer2	Rendszer3	Rendszer4	Rendszer5	Rendszer6	Rendszer7	Rendszer8
Katasztrófahelyzet bekövetkeztekor a visszaállítás prioritása								
A rendszer hardver és szoftver leltára								
Hardver elemek								
Szoftver elemek								
Egyéb								
Tartalék eszközök (darabszám és típus)								
Tartalék eszközök státusza (hideg, meleg stb.)								
A rendszer egyes elemének kiesése milyen mértékben befolyásolja a szolgáltatási szintet								
A rendszer dokumentációi (és azok tárolási helye)								
Az üzemeltetési kézikönyv tartalmának értékelése								
Van-e kidolgozott mentési-visszaállítási utasítás az üzemeltetési dokumentumban								
A rendszer rendelkezik-e tartalékeszközzel (és annak tárolási helye)								
A rendszer szállítója/szállítói, elérhetőségei, kapcsolattartói								

Kritérium Rendszer	Rendszer1	Rendszer2	Rendszer3	Rendszer4	Rendszer5	Rendszer6	Rendszer7	Rendszer8
A rendszer szállítójának rendelkezésre állása								
SLA								
Van-e támogatási szerződés								
Van-e kidolgozott szállítói támogatás eljárásrend								
Milyen rendszerességgel készül mentés a rendszerről								
A mentések tárolási helye								
Kapcsolódó rendszerek (input)								
Kapcsolódó rendszerek (output)								
Üzemeltetők száma								
Üzemeltetők képzettsége								
Sebezhetőségi ablak								
Kapcsolódó adatkommunikációs vonalak								

3.13. A központi rendszer alrendszereinek, szolgáltatásainak sebezhetőségi ablaka

A sebezhetőségi ablak az az idő- és térbeli tartomány, amelyen belül egy katasztrófa esetén el kell viselni a szolgáltatás rendelkezésre nem állását. Ennek meghatározása az IKeT létrehozásának egyik alapvető kiinduló paramétere. Ennek függvényében lehet a követelményeket megállapítani. A központi rendszer vonatkozásában ennek nagyságát minimalizálni kell, az elfogadhatónak minősített 99,5%-os rendelkezésre állást minél rövidebb időintervallumra vonatkoztatva biztosítani kell.

A központi rendszer Üzemeltetési Szabályzata kell, hogy rendelkezzen arról, hogy hiba esetén – mely lehet bármilyen jellegű, beleértve katasztrófaeseményt is – milyen eszkalációs rendben történjék a hibaelhárítás. Az említett szabályzatban kell dokumentálni az eseményszintű kategóriákat, 1–5-ig tartó skálán meghatározva. A hibakategóriák súlyozva vannak felhasználó és kiesés szempontokból is.

3.14. Kritikus erőforrások

Az üzemeltetőnek rendelkeznie kell az erőforrásokra vonatkozó minden részletre kiterjedő naprakész nyilvántartással – lehetőleg elektronikus formában –, amely az alábbi információkat tartalmazza:

– számítógépes hardverek;
– számítógépes szoftverek;
– számítógépes eszközök ellátásához szükséges anyagok;
– helységek és azon belüli rackszekrények áttekintő ábrája, a rendszerek elhelyezésére vonatkozóan;
– telekommunikáció (eszközök típusa, helye, kapcsolódásai stb.).

Katasztrófahelyzet esetén, ennek alapján megállapítható a kiesett erőforrások köre, melyek kritikussági szintje a rendszer működésfolytonosságában elfoglalt szerep alapján határozható meg a tervezés során.

Az üzemeltetőnek valamennyi rendszeréhez kapcsolódó elektronikus dokumentációját alternatívan elérhető szerveren is tárolnia kell, hogy a katasztrófahelyzet bekövetkezte után is rendelkezésre álljanak a szükséges információk a helyreállításhoz.

3.15. A rendkívüli helyzetek kezelése

A rendkívüli helyzetek, illetve a tömeges leállások kezelésére az üzemeltetőnek rendelkeznie kell a szükséges szabályozásokkal.

Rendkívüli helyzetekben az üzemeltető munkatársaknak nincs mérlegelési lehetőségük, kizárólag a meghatározott eszkalációs eljárás szerint kell eljárniuk. Mérlegelési lehetősége ilyen esetben kizárólag az intézmény vezetőjének, illetve az üzemeltetés vezetőjének van.

Függetlenül attól, hogy az adott esetet mi okozta, minden esetet ki kell vizsgálni, és arról a hibaelhárítás után jelentést kell készíteni, melynek tartalmaznia kell a hiba okát, továbbá az esemény lefolyását részletesen.

3.16. Hardver-karbantartási, problémakezelési és változáskezelési eljárások

Az üzemeltető hatékony hardver-karbantartási, problémakezelési és változáskezelési eljárásokkal kell rendelkezzen a váratlan üzemszünetek megelőzése érdekében, melyekre nézve az üzemeltetési szabályzat szervezeti egységek szerint lebontva kell, hogy részletesen rendelkezzen.

Az üzemeltető a rendszer kialakítása során törekedjen a magas rendelkezésre állású, megbízható rendszerek kialakítására.

A rendelkezésre állás növelése érdekében a kritikus eszközökből az üzemeltetőnek tartalék eszközökkel kell rendelkeznie meghibásodás esetére. A tartalékeszköz-állomány képzésére eljárásrendet kell kialakítani. Az eszközök nyilvántartását naprakész, elektronikus formában kell tárolni.

A rendszerek párhuzamos működése lehetővé teszi mind a tervszerű karbantartási javítási munkálatok, mind a rendkívüli karbantartási javítási feladatok olyan ütemezését, amely mellett folyamatosan biztosítható az üzemszerű működés.

3.17. Az informatikai katasztrófa kihirdetése

A központi szolgáltatásokra vonatkozó üzemeltetési szabályzatnak kell meghatározni, hogy ki és milyen esetekben rendelhet el katasztrófahelyzetet, ki helyettesítheti annak elrendelőjét, illetve ki szüntetheti meg az állapot meghirdetését. Ugyancsak az üzemeltetési szabályzatnak kell részletesen rendelkeznie arról is, hogy mikor kell meghirdetni a katasztrófaelhárítás eszkalációját.

A központi rendszer teljes redundanciával (telephelyi duplikáció) rendelkező szolgáltatásainál a kétközpontos működés tükrében a katasztrófahelyzet a hagyományostól eltérő értelmezést nyer. A kétközpontos működés a szolgáltatás teljes kiesésének valószínűségét alacsony szintre csökkenti, mivel bármely rendszer meghibásodása esetén az éles-üzemi funkció átterhelhető a másik központban megtalálható rendszerekre. Ezek fényében a központi rendszer alrendszereire jelen dokumentum további részében katasztrófahelyzet alatt azt az esetet értjük, amikor az egyik központban valamely rendszer(ek) leállt(ak) és így a szolgáltatást az egyik központ szolgáltatja csak.

3.17.1. A biztonsági események osztályozása

Az erőforrások rendelkezésre állásának megszakadása alapján a biztonsági események a következő kategóriákba sorolhatók:

I. Kategória:

az informatikai erőforrások az érintett központban nem állnak rendelkezésre, az ottani informatikai rendszer működése megszakad.

Ezt okozhatják például a tűz és a víz okozta katasztrófák. Jellegüknél fogva ezek nagy pusztításokat jelentenek a számítástechnikai eszközökben és/vagy a kiszolgáló infrastruktúrában. A helyreállítás időigényes és költséges.

II. Kategória:

az érintett központban egyes erőforrások nem állnak rendelkezésre, és az ottani informatikai rendszer működése megszakad.

Idetartozik például az energiaellátás kiesése. Jellegénél fogva a pusztítás lokalizált, a helyreállítás kevésbé költséges és időigényes, mint az I. Kategóriába sorolt katasztrófák esetében.

A II. Kategóriát az igényeknek és a helyi adottságoknak megfelelően két alkategóriára bontjuk:

II/a Kategória: emberi vagy eszköz erőforrások megsemmisülése, illetve ezek olyan, hosszabb idejű üzem-, munkaképtelensége (kiesése), amely jelentős problémát okoz az informatikai rendszer működésében azáltal, hogy küldetéskritikus vagy lényeges rendszert érint.

II/b Kategória: emberi vagy eszköz erőforrások nem semmisülnek meg, és hosszabb-rövidebb idejű üzem-, munkaképtelensége (kiesése) nem okoz jelentős problémát az informatikai rendszer működésében azáltal, hogy nem küldetéskritikus vagy lényeges rendszert érint.

III. Kategória:

az érintett központban csak erőforráselem(ek) sérül(nek) meg, de az informatikai rendszer működése folyamatos.

A III. kategória veszélyforrásai az Üzemeltetési Szabályzat tárgykörébe esnek. A veszélyforrások képezte fenyegetés bekövetkezése az Üzemeltetési Szabályzatban tárgyalt védelmi intézkedések alkalmazásával előzhetők meg, illetve bekövetkezés esetén ugyancsak ezen védelmi intézkedések alkalmasak a károk mértékének csökkentésére.

Informatikai katasztrófának minősülnek az I. és II/a Kategóriába sorolható események.

Informatikai veszélyhelyzetnek minősülnek a II/b Kategóriába sorolható események.

Nem minősülnek katasztrófának a III. Kategóriába sorolt események.

3. melléklet a 223/2009. (X. 14.) Korm. rendelethez

Az elektronikus kormányzati gerinchálózat informatikai biztonsági szabályzata

1. Informatikai biztonsági szabályzat
   - 1.1. A biztonsági szabályzat hatálya
   - 1.2. Biztonsági szabályzat helye a szabályzatok között
2. Biztonsági intézkedések
   - 2.1. Szervezet
     - 2.1.1. Felelősségi körök
     - 2.1.2. Személyzet
     - 2.1.3. Eljárás rend
     - 2.1.4. Csatlakozás biztonsági feltételei
     - 2.1.5. Beszerzés
     - 2.1.6. Üzemeltetés
     - 2.1.7. Fenntartás
     - 2.1.8. Katasztrófa terv
     - 2.1.9. Biztonsági osztályok
   - 2.2. Infrastruktúra
     - 2.2.1. Általános intézkedések
     - 2.2.2. Számítógéptermek
     - 2.2.3. A számítógéptermeken kívül található eszközök védelme
     - 2.2.4. Üzemelés biztosítása
     - 2.2.5. Villámcsapás- és túlfeszültség-védelem
     - 2.2.6. Tűzvédelem
     - 2.2.7. Vízvédelem
   - 2.3. Hardver eszközök
     - 2.3.1. Szerverek
     - 2.3.2. Munkaállomások
     - 2.3.3. Hálózati hardver eszközök
     - 2.3.4. A csatlakozott intézmények által üzemeltetett eszközök
     - 2.3.5. Hardver eszközök nyilvántartása
     - 2.3.6. Tartalék eszközök
   - 2.4. Szoftverek
     - 2.4.1. Szoftverkarbantartás
     - 2.4.2. Biztonsági mentések
     - 2.4.3. Vírusvédelem
   - 2.5. Hálózat védelme
     - 2.5.1. Rendelkezésre állás biztosítása
     - 2.5.2. Jogosultsági rendszer
     - 2.5.3. MPLS VPN
     - 2.5.4. IP VPN
     - 2.5.5. Tűzfalakra, védelmi intézkedésekre vonatkozó követelmények
     - 2.5.6. Csatlakozott szervezetekre vonatkozó szabályok
     - 2.5.7. Hálózat felügyelete
     - 2.5.8. Rendhagyó (rendkívüli) események jelentése, kezelése
3. Záró rendelkezések
   - 3.1. A biztonsági szabályzat bevezetése, oktatása
   - 3.2. A biztonsági szabályzat hatálybalépése
   - 3.3. A biztonsági szabályzattól való eltérés rendje
   - 3.4. A biztonsági szabályzat aktualizálásának, kiegészítésének rendje

1. Az informatikai biztonsági szabályzat célja

Az informatikai biztonsági szabályzat (a továbbiakban: IBSz) célja az elektronikus kormányzati gerinchálózat (a továbbiakban: EKG) üzembiztonságát megteremtő szabályok és intézkedések meghatározása.

1.1. A biztonsági szabályzat hatálya

Az EKG címzett feladata, hogy a csatlakozott szervezetek közötti elektronikus kommunikáció átviteli közege legyen, így a rajta átfolyó adatok tartalmával nem foglalkozik, azokért nem felel, ez minden esetben az egyes intézmények feladata. Emiatt a biztonsági szabályzat az üzembiztonságról szól, és adatbiztonsággal kapcsolatos kérdésekkel kizárólag akkor foglalkozik, ha azok hatással lehetnek az üzembiztonságra.

A dokumentum hatálya kiterjed:

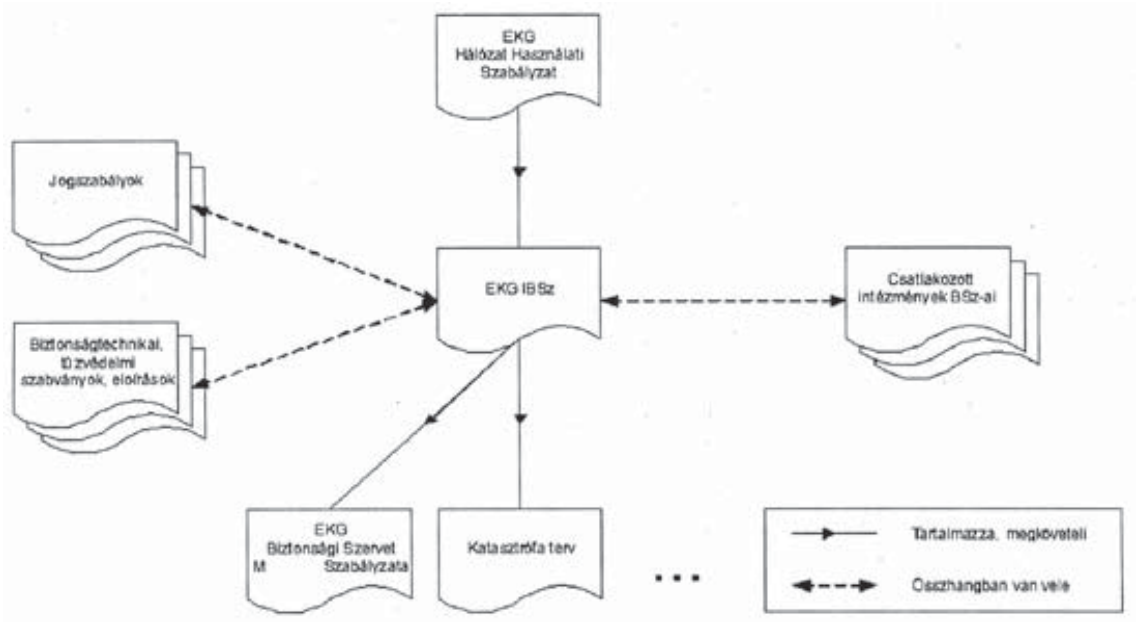
– az EKG hálózatgazdájának feladataira és kötelességeire;
– a hálózat üzemeltetőjének feladataira és kötelességeire;
– a hálózathoz csatlakozott intézmények feladataira és kötelességeire.

1.2. Biztonsági szabályzat helye a szabályzatok között

Az IBSz a biztonsági kérdésekben alapszabályzat, ugyanakkor nem tér ki részletesen az üzembiztonság minden aspektusára, hanem az őt körülvevő szabályozási rendszer szerves része, lehetőség szerint kerülve az átfedéseket. Tartalmazza ugyanakkor a szabályozás további szükséges területeit, amelyek azonban olyan mértékben helyzetfüggőek, hogy jogszabályi szinten szabályozásuk nem kezelhető.

Az IBSz szándékoltan nem áll meg önmagában, hanem szervesen beilleszkedik az őt körülfogó szabályzati rendszerbe, vagyis eredeztethető a megfelelő jogszabályokból (pl. államtitkokról szóló rendeletek stb.) és szabványokból (pl. Országos Építési Szabályzat, ITSEC stb.), kiegészíti az EKG működési szabályzatát és megteremti az alapot az üzembiztonság egyes aspektusaival (pl. biztonsági szervezet működési szabályzata, katasztrófa terv stb.) részletesen foglalkozó szabályzatok létrehozásához.

A biztonsági szabályzatot a hálózatgazdának évente felül kell vizsgálni és szükség esetén aktualizálni, kiegészíteni. A hálózatban bekövetkező jelentős változások esetén a felülvizsgálatot soron kívül el kell végezni.



2. Biztonsági intézkedések

A biztonsági intézkedések alkalmazása szempontjából öt fő kategóriát különböztettünk meg:

szervezet – az EKG biztonságáért felelős szervezetre vonatkozó, illetve az ahhoz kötődő intézkedések;

infrastruktúra – az EKG fizikai védelmét biztosító környezetre vonatkozó intézkedések;

hardver eszközök – az EKG hardver eszközeire vonatkozó intézkedések;

szoftverek – az EKG üzemeltetéséhez és szolgáltatásaihoz szükséges szoftverekre vonatkozó intézkedések;

hálózat védelme – a fenti csoportokba nem besorolható, de a hálózat védelmét szolgáló intézkedések.

Az intézkedések konkrét feladatokat jelentenek, a felelős és a végrehajtás ajánlott gyakoriságával együtt.

A felelős megjelölésénél az IBSz szabályzat a hálózatgazda, az üzemeltető és a csatlakozott/csatlakozandó intézmény szintjén marad (az IBSZ alapfogalmainak értelmezését a szabályzat 1. számú függeléke tartalmazza).

2.1. Szervezet

2.1.1. Felelősségi körök

Biztonságért felelős szervezet kialakítása	
Feladat:	– A biztonságért felelős szervezet felállítása a következő munkakörök kialakításával (munkaköri leírás készítése): *biztonságért felelős vezető* – a hálózat informatikai biztonságáért, és ennek megfelelően magáért a (csatlakozott intézményi, illetve üzemeltetői) biztonsági szabályzat (BSZ) meglétéért, tartalmáért felelős személy *biztonsági felügyelők* – a BSZ betartásának ellenőrzéséért felelős személyek *biztonsági szakértők* – a hálózat biztonságát célzó védelmi intézkedésekért, a káresemények elemzéséért, a BSZ naprakészen tartásáért felelős személyek – A megfelelő személyek körültekintő kiválasztása.
Eredmény:	Biztonságért felelős szervezet.
Felelős:	Hálózatgazda (a szabályzat meglétéért, EKG-ra vonatkozó tartalmáért és a szervezet kialakításáért)
Gyakoriság:	A biztonsági szabályzat hatálybalépésekor, ezt követően szükség szerint (megfelelő munkatárs távozása stb.).
Feladatok és hatáskörök pontos meghatározása és dokumentálása	
Feladat:	– Az EKG-val kapcsolatban pontosan meg kell határozni, hogy mik a feladatok, kinek, milyen felelőssége van, és milyen hatáskörrel bír. Mindezt írásban dokumentálni kell, és gondoskodni kell arról, hogy az EKG-val kapcsolatba kerülő minden szereplő tisztában legyen a rá vonatkozó részekkel.
Eredmény:	Feladatok és hatáskörök pontos leírása.
Felelős:	Hálózatgazda
Gyakoriság:	A biztonsági szabályzat hatálybalépésekor, majd ezt követően legalább évente kell felülvizsgálni, illetve káresemény esetén azonnal.

2.1.2. Személyzet

Személyzet kiválasztása	
Feladat:	– Mivel az EKG nemzetbiztonsági jelentőséggel bír, ezért az azzal kapcsolatba kerülő, annak tervezésében, üzemeltetésében, karbantartásában részt vevő személyeket nagyon körültekintően, az erre vonatkozó jogszabályoknak megfelelően kell kiválasztani. – Külön figyelmet kell fordítani mindazokra, akik az EKG üzemeltetésében adminisztrátori jogosultságokkal rendelkeznek, az ő megbízhatóságuk ellenőrzése kiemelten fontos feladat.
Eredmény:	Körültekintően kiválasztott, megbízható személyzet.
Felelős:	Hálózatgazda, üzemeltető, csatlakozott szervezetek
Gyakoriság:	A biztonsági szabályzat hatálybalépésekor, majd ezt követően szükség szerint (munkatárs távozása stb.).
Személyzet képzése	
Feladat:	– Feladatuk szerint csoportosítva el kell készíteni a személyi állomány képzését segítő anyagokat és meg kell szervezni azok tervszerű és ellenőrzött végrehajtását. – A képzések során fokozott figyelmet kell fordítani biztonsági kérdésekre. – A képzések színvonalát és az elsajátított tudás szintjét ellenőrizni kell.
Eredmény:	Képzett, a feladatait megfelelően ellátni képes, a biztonsági előírásokkal és teendőkkel tisztában lévő személyi állomány.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	A biztonsági szabályzat hatálybalépésekor, majd ezt követően szükség szerint (új munkatárs belépése stb.), rendszeres ismeret karbantartás.

Biztonsági előírások betartásának ellenőrzése	
Feladat:	– A biztonsági felügyelőnek folyamatosan ellenőriznie kell, hogy a személyzet tisztában van a megfelelő biztonsági előírásokkal és be is tartja azokat. – Az ellenőrzéseket dokumentálni kell, a jegyzőkönyveket legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.
Eredmény:	Betartott biztonsági előírások.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Folyamatosan, de nem kiszámítható módon (fontos, hogy ne lehessen rá előre felkészülni).

2.1.3. Eljárás rend

Védelmi intézkedések ellenőrzése és felülvizsgálata	
Feladat:	– Az üzembiztonság érdekében tett védelmi intézkedéseket a biztonsági felügyelőnek rendszeresen kell ellenőriznie és felülvizsgálnia. – Az ellenőrzéseket és felülvizsgálatokat dokumentálni kell, az ezt tartalmazó jegyzőkönyveket legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni. – A felülvizsgálat eredményeképp a felügyelő a védelmi intézkedések módosítását kezdeményezheti.
Eredmény:	Ellenőrzött, visszakövethető és naprakészen tartott védelmi intézkedések.
Felelős:	Hálózatgazda
Gyakoriság:	Félévente, illetve káresemény esetén azonnal.
Káresemény kezelése	
Feladat:	– Az üzembiztonság sérülése esetén a felfedezést követően haladéktalanul meg kell kezdeni az elhárítást és a károk csökkentését (lásd alább a biztonsági események kezelésénél). – A káreseményeket elhárításuk után azonnal elemeznie kell a biztonsági szervezetnek (a biztonsági vezető vezetésével a kijelölt biztonsági szakértők végzik). – Az elemzést dokumentálni kell, a jegyzőkönyvet legalább 5 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni. – Az elemzés eredményeképp a biztonsági szakértők akciótervet dolgoznak ki a hasonló káresemények jövőbeni elkerülésének érdekében. Ebben javaslatot tehetnek a védelmi intézkedések és a felelősségi körök megváltoztatására, kiegészítésére. – Az akciótervet a biztonságért felelős vezető hagyja jóvá, ezt követően haladéktalanul végre kell hajtani.
Eredmény:	Elhárított és elemzett káresemény, a jövőbeli előfordulás elkerülését célzó jóváhagyott és végrehajtott akcióterv.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Káresemény esetén.

2.1.4. Csatlakozás biztonsági feltételei

Csatlakozott/csatlakoztatandó szervezetek biztonsági szabályzata	
Feladat:	– Minden csatlakozó szervezetnek az EKG biztonsági szabályzatával összhangban álló, azzal teljes mértékben harmonizáló biztonsági szabályzatot kell kidolgozni (újonnan csatlakozó szervezet esetén ez alapkövetelmény), melyet a hálózatgazda nevében az EKG biztonsági felelősének véleményeznie kell. Ha a csatlakozott szervezet teljes biztonsági szabályzata nem adható ki véleményezésre, akkor az EKG-t érintő részeket kell véleményezni.
Eredmény:	Az EKG biztonsági felelőse által véleményezett biztonsági szabályzat.
Felelős:	Csatlakozott/csatlakozandó szervezet
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépését követően 6 hónapon belül, illetve a csatlakozás előtt, a csatlakozással hatályba léptetve.

2.1.5. Beszerzés

Beszerzési politika	
Feladat:	– A Hálózatgazdának egységes beszerzési politikát kell kidolgoznia az EKG-ra vonatkozó minden (hardver, szoftver stb.) beszerzési feladatra, a közbeszerzésre vonatkozó jogszabályok maximális figyelembevételével. – A beszerzési politikában lehetőség szerint maximálisan érvényesíteni kell az üzembiztonság fenntartását elősegítő szempontokat. – Amennyire ezt a közbeszerzés szabályai megengedik, törekedni kell arra, hogy az EKG eszközei minél egységesebbek legyenek.
Eredmény:	Egységes beszerzési politika (egységes megbízhatóságú rendszer).
Felelős:	Hálózatgazda
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor aktualizálni a külső tényezők (pl. jogszabályok stb.) megváltozásakor, illetve a piac lényeges változásakor szükséges.

Amortizációs szabályozás	
Feladat:	– A Hálózatgazdának ki kell dolgoznia az EKG minden eszközére (beleértve a hardver és a szoftver eszközöket is) vonatkozó amortizációs szabályokat. – Az amortizációs szabályok kidolgozásakor az eszközöket azonos amortizációs jellemzővel rendelkező kategóriákba kell sorolni, minden egyes kategóriára meghatározva az amortizációs időtartamot és az amortizációs eljárást.
Eredmény:	Amortizációs szabályok.
Felelős:	Hálózatgazda
Gyakoriság:	A biztonsági szabályzat hatálybalépésekor, aktualizálni a külső vagy belső tényezők (pl. technológia stb.) megváltozásakor szükséges.

2.1.6. Üzemeltetés

Eszköznyilvántartás	
Feladat:	– Az üzemeltetőnek naprakész nyilvántartást kell vezetni minden az EKG-hoz tartozó eszközről (hardverek, szoftverek stb.), annak állapotáról, helyéről stb. (a nyilvántartásnak minden olyan adatot tartalmaznia kell, ami alapján az adott eszköz megtalálható, felügyelhető, tervszerűen karbantartható, amortizálható stb.). – A nyilvántartásban már a beszerzési szándéktól fogva meg szükséges jeleníteni az adott eszközt és állapotát (beszerzés alatt, leszállítva, raktárban, tesztelés alatt, installálás alatt, üzemben, meghibásodott, javítás alatt, kivezetés alatt, amortizálva stb.) a teljes életciklus során végigkövetni.
Eredmény:	Naprakész eszköznyilvántartás.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

Tesztelés	
Feladat:	– Az üzemeltetőnek minden eszköztípusra (lehetőség szerint a tömeges, rendszerszerű beszerzés előtt) teszttervet kell készítenie, melynek végrehajtása után az adott típusú eszköz már nagy biztonsággal üzembe helyezhető. – Minden eszközt üzembe helyezése előtt tesztelni kell az előre kidolgozott teszttervek alapján. – Káresemények esetén az elemzések eredménye magával vonhatja a teszttervek kiegészítését.
Eredmény:	Kész teszttervek, csökkentett kockázatú üzembe helyezési folyamat.
Felelős:	Üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor, majd ezt követően folyamatosan.

2.1.7. Fenntartás

Változások	
Feladat:	– Az EKG-ban bekövetkezett bármilyen változást (pl. új tűzfal üzembe helyezése, korszerűtlen eszközök újabbra cserélése, router konfiguráció változtatása stb.) dokumentálni kell, minden a változás visszakövethetőségét elősegítő információval (pl. az esemény leírása, oka, az azt megelőző helyzet, az általa okozott tényleges változások, ezek hatása stb.). – A változások jegyzőkönyvét legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.
Eredmény:	Nyomon követhető változások.
Felelős:	Üzemeltető
Gyakoriság:	Bármilyen az EKG-ban bekövetkező változással egy időben.

Külső cégekkel végeztetett javítások, karbantartások	
Feladat:	– Minden esetben, amikor külső céget kell valamilyen javítási vagy karbantartási feladattal megbízni, amely csak a hálózatba „beavatkozva" (helyszíni javítás, illetve távoli elérésen keresztül végzett tevékenységek stb.) végezhető el, az üzemeltető köteles ezt a tevékenységet folyamatosan ellenőrizni, felügyelni és gondoskodni arról, hogy az EKG-ra vonatkozó bizalmas információk (pl. tűzfal konfiguráció stb.) ne kerülhessenek illetéktelen kezekbe.
Eredmény:	A külső cégek bevonásával járó kockázat minimalizálása.
Felelős:	Üzemeltető
Gyakoriság:	Minden esetben, amikor külső cég helyszíni javítást vagy karbantartást végez.

2.1.8. Katasztrófa terv

Katasztrófa terv kidolgozása	
Feladat:	– A Hálózatgazdának és az üzemeltetőnek együttműködve ki kell dolgozni a megfelelő katasztrófa tervet, mely csökkenti a bekövetkezett esemény okozta károkat, segít fenntartani a működést, és hozzájárul az eredeti állapot (vagy a körülményekhez képest az ahhoz legközelebb álló állapot) visszaállításához. – A katasztrófa terv részeként el kell készíteni a végrehajtás feltételeit megteremtő akciótervet, amit jóváhagyás után gyakoroltatni kell. – A katasztrófa tervet évente aktualizálni kell, és tükröznie kell az időközben beállt változásokat. Amennyiben szükséges, úgy ismételten akciótervet kell megfogalmazni és azt gyakoroltatni. – A katasztrófa tervet ismertetni kell az érintettekkel, és gondoskodni kell arról, hogy minden érintett tisztában legyen a rá háruló feladatokkal.
Eredmény:	Katasztrófa terv.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor, majd ezt követően évente, illetve a körülmények lényegi megváltozása esetén kell aktualizálni.

2.1.9. Biztonsági osztályok

EKG-eszközök biztonsági osztályokba történő sorolása	
Feladat:	– Az EKG, illetve az EKG üzemeltetéshez szükséges eszközöket az ITB ajánlásnak megfelelően három biztonsági osztályba kell besorolnia az üzemeltetőnek. A biztonsági osztályokba történő sorolás az ITB 12. ajánlásának 4.1. fejezetében leírt káreseményeknek megfelelően definiált kárérték osztályzás szerint kell, hogy történjen, annak alapján, hogy az adott eszköz kiesése vagy hibás működése mekkora hatással bírna. – A biztonsági osztályokba sorolás támogatja, hogy az adott rendszerelem mennyire fontos a tartalékképzés, a karbantartás és redundancia biztosításának szempontjából. – Az alábbi osztályokba kell sorolni az eszközöket: = A – alapbiztonsági követelmények, ha az elem kiesése vagy hibás működése maximum „2", azaz legfeljebb közepes kárértékű eseményt okozhat;

= F – fokozott biztonsági követelmények, ha az elem kiesése vagy hibás működése maximum „3”, azaz legfeljebb nagy kárértékű eseményt okozhat;

= K – kiemelt biztonsági követelmények, ha az elem kiesése vagy hibás működése „4+”, azaz katasztrofális kárértékű eseményt okoz

Eredmény:	Biztonsági osztályok kialakítása.
Felelős:	Üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor.

2.2. Infrastruktúra

Alábbiakban az EKG fizikai védelmét biztosító infrastruktúra kialakítására és üzemeltetésére vonatkozó intézkedések felsorolása található.

2.2.1. Általános intézkedések

Biztonsági zónák kialakítása	
Feladat:	– Az EKG eszközeit tároló, valamint az üzemeltetéssel más módon kapcsolódó helyiségeket biztonsági zónákra kell felosztani. – Az épületbe való bejutáson túl biztosítani kell, hogy az EKG üzemelést biztosító helyiségekbe (pl. szerverszoba, hálózati felügyeleti szoba) csak azok juthassanak be, akik jogosultak a belépésre. – Definiálni szükséges, hogy melyik helyiségek legyenek védettebbek, mint az épület egyéb helyiségei (pl. szerverszoba).
Eredmény:	Fizikailag elkülönített biztonsági zónák az EKG üzemelését biztosító épületekben.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor.

A biztonsági zónákon belüli közlekedés szabályozása	
Feladat:	– Definiálni szükséges, hogy az egyes helyiségekbe (pl. szerverszoba) ki léphet be. Javasolt, hogy az üzemeltető különböző szakértő csoportjai csak saját helyiségeikbe kapjanak belépést (pl. a hálózati eszközöket tartalmazó terekbe csak a hálózati szakértők juthassanak be).
Eredmény:	A definiált biztonsági zónákba csak a jogosult embereknek, személyeknek van belépési lehetősége.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	A rendszer kiépítésekor, illetve új helyiségek igénybevételekor.

2.2.2. Számítógéptermek

Számítógéptermek	
Feladat:	– Az EKG védett eszközeit (szerverek, menedzsment eszközök stb.) az üzemeltető köteles a hálózatgazda által kijelölt helyiségekben elhelyezni. – A hálózatgazdának gondoskodnia kell arról, hogy a kijelölt helyiségek rendelkezzenek mindazokkal a felszerelésekkel, amelyek a nagy üzembiztonságú rendszerek üzemeltetéséhez kellenek (részletesen lásd az Infrastruktúra fejezet további intézkedéseiben).
Eredmény:	Az EKG eszközeinek a nagy üzembiztonságú működést biztosítani képes környezetben való elhelyezése.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Amikor az EKG bővülése ezt szükségessé teszi.

Számítógéptermek beléptető rendszere	
Feladat:	– Az EKG eszközeinek helyt adó számítógéptermeknek olyan beléptető rendszerrel kell rendelkezniük, melyek lehetővé teszik, hogy kizárólag az arra jogosult személyek juthassanak be. – A számítógéptermekbe való belépéseket, illetve belépési kísérleteket minden esetben naplózni kell, a naplókat legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.

Eredmény:	Az EKG számítógéptermeibe csak a hozzáféréshez jogosult emberek lépnek be, illetéktelenül nem juthatnak be a helyiségekbe.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	A számítógépterem üzembe helyezésekor, illetve a jogosulti kör változásakor haladéktalanul.

Számítógéptermekre vonatkozó belépési jogosultságok kezelése

Feladat:	– Definiálni kell a számítógéptermekbe való belépési jogosultságok menedzselésének módját. Meg kell határozni, hogy kinek adható ki belépési engedély, mikor módosulhat valakinek a hozzáférése, illetve belépési jogosultság megszűnése esetén azonnali hatállyal intézkedést kell tenni a jog megvonására.
Eredmény:	Az EKG számítógéptermeibe csak a hozzáféréshez jogosult emberek, személyek lépnek be.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Számítógépterem üzembe helyezésekor, illetve a jogosulti kör változásakor haladéktalanul.

Számítógéptermek fizikai védelme

Feladat:	– Az üzemeltetőnek gondoskodnia kell arról, hogy az EKG eszközeinek helyt adó számítógéptermek (ideértve a klímaberendezéseket és a szünetmentes tápellátást biztosító eszközöket is) fizikailag is védettek legyenek úgy, hogy mindennemű lopás, manipuláció, külső beavatkozás, támadás lehetőség szerint elkerülhető, illetve legrosszabb esetben legalább észlelhető legyen. – A megyei központokban elsősorban a számítógépszekrények védelmét szükséges megoldani, mivel a számítógépes helyiségek ott nem az EKG tulajdonát képezik.
Eredmény:	Fizikailag védett számítógéptermek.
Felelős:	Az üzemeltető telephelyén az üzemeltető, a hálózatgazda telephelyén lévő helyiségek védelméért a hálózatgazda a felelős. Csak olyan helyiségben lehet EKG eszközt elhelyezni, amelyre annak üzemeltetője garanciát vállal az EKG normáinak megfelelő biztonságáért.
Gyakoriság:	Számítógéptermek kialakításakor 2 évente, illetve átalakításkor felülvizsgálva az intézkedéseket.

Számítógépszekrények védelme

Feladat:	– Az üzemeltető köteles az EKG megyei csatlakozási pontjainál elhelyezett eszközeit az illetéktelen hozzáféréstől számítógépszekrényekkel védeni. – Gondoskodni kell arról, hogy a számítógépszekrények kinyitását kizárólag arra jogosult személy tehesse meg. – A számítógépszekrényekhez való hozzáférést minden esetben naplózni kell, a naplókat legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.
Eredmény:	A területi alközpontokban elhelyezett eszközök megfelelő szintű védelme.
Felelős:	Üzemeltető
Gyakoriság:	Újabb csoportos csatlakozási pontok kialakításakor, 2 évente felülvizsgálva az intézkedéseket.

Belépési eszközök (pl. belépési kártya) használati szabályának előírása

Feladat:	– Rögzíteni (valamennyi használóval ismertetni) kell a belépésre szolgáló eszközök használati szabályait. Ezek a szabályok a következők: eszköz elvesztésének bejelentési kötelezettsége, eszköz másra való átruházásának tiltása, eszköz biztos helyen való őrzése, kilépéskor eszköz visszaadása. – A szabályokat a belépési eszköz használóival ismertetni kell.
Eredmény:	Belépési eszközök rendeltetésének megfelelő használata.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Belépési eszköz kiadásakor.

2.2.3. A számítógéptermeken kívül található eszközök védelme

Számítógéptermeken kívül található eszközök védelme	
Feladat:	– A számítógéptermeken kívül található, távközlési szolgáltatótól bérelt telekommunikációs csatornákat is védeni szükséges. Mivel ezek az eszközök nem az EKG tulajdonát képezik, ezért a távközlési szolgáltatóval kötött szerződésben kell felelősségszintű védelmet biztosítani (rendelkezésre állás, tartalék biztosítása, hibaelhárítási kötelezettség). – Az EKG-hoz csatlakozó intézmények biztonságos üzemelése szempontjából javasolt, hogy az intézmény biztosítson hozzáférést saját az EKG-hoz csatlakozó routeréhez, valamint hiba esetén bejelentési kötelezettsége legyen az üzemeltető felé.
Eredmény:	Számítógéptermeken kívül található eszközök szerződésben meghatározott védelme.
Felelős:	Hálózatgazda
Gyakoriság:	Szerződések megkötésekor.

Üzemeltető raktárának védelme	
Feladat:	– Mivel az üzemeltető a tartalék eszközöket nem a számítógéptermekben tárolja, ezért szükséges a raktárnak is a megfelelő belépési és fizikai védelme. A raktárba csak az üzemeltető léphet be, illetve akinek a hálózatgazda erre külön engedélyt ad.
Eredmény:	Tartalék eszközöket tároló raktár megfelelő védelme.
Felelős:	Üzemeltető
Gyakoriság:	Rendszer kialakításakor.

2.2.4. Üzemelés biztosítása

Eszközök szünetmentes áramellátásának biztosítása	
Feladat:	– Az üzemeltetőnek – a hálózatgazda által biztosított eszközök terhére – gondoskodnia kell arról, hogy az EKG eszközeinek szünetmentes áramellátása biztosítva legyen. Az üzemeltetést biztosító eszközöket redundáns UPS-sel szükséges ellátni. A hosszabb áramszünetek esetére tartalék generátort kell biztosítani az országos központban. A megyei központokban a tervezett áramszünetek esetére mobil generátoros megoldást kell biztosítani (az üzemeltető szakemberei szállítják a helyszínre a generátort). – Az UPS-eket rendszeresen ellenőrizni kell, mert azok akkumulátorai gyakran meghibásodhatnak. Az UPS-ekből ennek megfelelően kellő számú tartalékot kell képezni (lásd 3.3.6. Tartalékgazdálkodás).
Eredmény:	Szünetmentes energiaforrással (UPS) és generátorral ellátott számítástechnikai eszközök.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Számítógéptermek kialakításakor, félévente ellenőrizve az UPS és a generátor állapotát.

Működtetéshez szükséges optimális külső hőmérséklet fenntartása	
Feladat:	– A számítástechnikai eszközök zavarmentes működéséhez folyamatosan optimális hőmérsékletet kell fenntartani. Különösen veszélyeztetett időszak a nyár, amikor a környezeti hőmérséklet magasabb lehet, mint az eszközök tűrőképessége. Az optimális hőmérsékletet klimatizáló készülékekkel szükséges biztosítani. Ez vonatkozik a budapesti központra és a vidéki központokra egyaránt.
Eredmény:	Optimális hőmérséklet a számítástechnikai eszközök zavartalan működéséhez.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Infrastruktúra kiépítésekor, illetve új infrastruktúra igénybevételekor.

Klimatizáló, illetve megfelelő hőmérsékletet biztosító készülékek rendszeres ellenőrzése	
Feladat:	– Az optimális hőmérsékletet biztosító eszközök működését folyamatosan ellenőrizni szükséges. Amennyiben a klíma nem üzemszerűen működik, úgy gondoskodni kell annak javításáról vagy szükség esetén cseréjéről.

Eredmény:	Optimális hőmérséklet a számítástechnikai eszközök zavartalan működéséhez.
Felelős:	Üzemeltető
Gyakoriság:	Félévente.

Környezeti tűréshatárok túllépésének figyelése és kezelése	
Feladat:	– A számítástechnikai eszközök környezeti tűréshatárát folyamatosan monitorozni kell. Amennyiben az eszköz túl magas hőmérsékletnek van kitéve, akkor intézkedni szükséges, amely a körülményektől függően többféle tevékenység is lehet (shutdown, állományok elmentése, tovább üzemelés, körülmények megváltoztatása).
Eredmény:	Az eszközök nem lépik túl fizikai tűréshatárukat, és folyamatosan üzemelnek.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

2.2.5. Villámcsapás- és túlfeszültség-védelem

Túlfeszültség-védelem	
Feladat:	– Fel kell készülni a vihar, illetve villám okozta károkozásokra. Az EKG eszközeit tároló épületeket megfelelő védelemmel kell ellátni, valamint védekezni kell a villám által okozott esetleges feszültségcsúcsokkal (feszültségtüskékkel) szemben is.
Eredmény:	Vihar- és villámvédett épületek, eszközök.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Kiépítéskor.

Túlfeszültség-védelem	
Feladat:	– A villám keltette vagy a hálózati feszültség ingadozásából eredő túlfeszültség meghibásodást okozhat számítógépekben, illetve egyéb hardver eszközökben. Ezeket az eszközöket minden helyszínen védeni kell megfelelően érzékeny, akár többszintű feszültségszabályozó eszközökkel.
Eredmény:	Túlfeszültség elleni védelem.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Eszközök telepítésekor.

2.2.6. Tűzvédelem

Tűzvédelem	
Feladat:	– A tűz ellen minden érintett helységben (budapesti központ, üzemeltető telephelyei, vidéki központok stb.) megfelelő mennyiségű és minőségű füstérzékelő és tűzjelző készüléket szükséges biztosítani. Az érzékelő és riasztó rendszereken túl biztosítani kell a helyszíni oltáshoz szükséges eszközöket. – A szerverszobában tárolt biztonsági mentéseket tartalmazó adathordozók és dokumentáció tűz- és vagyonvédett tárolását is biztosítani kell. Arra is figyelmet kell fordítani, hogy esetleges oltás esetén se sérüljenek. – Ki kell dolgozni a tűzvész esetére a szükséges intézkedéseket, melyeket tűz esetén felül kell vizsgálni.
Eredmény:	Megfelelő tűzvédelemmel ellátott eszközök, illetve helyiségek.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	2 évente, de minden rendszer indításakor, minden új helyiség igénybevétele esetén, valamint tűzeset után.

Tűzjelző készülékek rendszeres ellenőrzése	
Feladat:	– A tűzjelző, illetve füstértékelő készülékeket rendszeresen ellenőrizni szükséges. Ezek közé beleértendő nemcsak a helyiségek tűzvédelmét biztosító eszközök, de a számítógépes szekrények érzékelői is.
Eredmény:	Működőképes tűzjelző készülékek.
Felelős:	Üzemeltető
Gyakoriság:	Félévente, illetve riasztás után.

2.2.7. Vízvédelem

Vízvédelem	
Feladat:	– A szomszédos helyiségekben, illetve az eszközökhöz közel levő falakban történt csőtörés miatt érheti víz az EKG eszközeit. Mivel vízérzékelővel jelenleg nem minden az EKG működtetését szolgáló helyiség rendelkezik, ezért biztosítani kell, hogy ilyen helyiségben az eszközök ne legyenek vízvezeték közelében. – Vízveszély olyan esetben is előfordulhat, amennyiben árvíz fenyegeti az épületet. Amennyiben az EKG eszközeit biztosító eszközök árvízveszélyes helyen vannak (egyes vidéki központokban előfordulhat), úgy gondoskodni kell arról, hogy az eszközök áthelyezhetőek legyenek olyan szintre, ahol az árvíz már nem okoz problémát.
Eredmény:	Vízveszélytől védett EKG-eszközök.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	A „vízbiztos” helyszínek kijelölését a rendszer telepítésekor, illetve konkrét intézkedéseket vízveszély esetén szükséges megtenni.
Vízvédelmet támogató készülékek rendszeres ellenőrzése és karbantartása	
Feladat:	– Amennyiben rendelkezik egy helyiség vagy eszköz vízérzékelő készülékkel (javasolt), akkor ezeket a készülékeket rendszeresen kell ellenőrizni, és rajtuk szükség esetén a megfelelő karbantartási munkálatokat végezni.
Eredmény:	Működőképes vízvédelmet támogató készülékek.
Felelős:	Üzemeltető
Gyakoriság:	Félévente, illetve riasztás után.

2.3. Hardver eszközök

Ebben a fejezetben találhatók mindazok a feladatok és intézkedések, melyek az EKG hardver eszközeire vonatkoznak, illetve azok védelmét szolgálják.

2.3.1. Szerverek

Szerverek üzembe helyezése	
Feladat:	– A szerverek üzembe helyezését meg kell előznie az installálás utáni tesztelésnek, melyek eredményéről jegyzőkönyvet kell írni. Amennyiben a szerver üzembe helyezése csere okán történik, úgy tesztelni kell, hogy a biztonsági mentésből visszaállított programok, fájlok elérhetők-e. – A tesztelési jegyzőkönyveket a szerver üzemből való kivonása után legalább még 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.
Eredmény:	Működőképes új szerverek.
Felelős:	Üzemeltető
Gyakoriság:	Új szerver beüzemelése esetén.
Szerverek karbantartása	
Feladat:	– A szerverek karbantartását és javítását az üzemeltető felügyeli. – Hiba esetén az üzemeltető a tartalékokból biztosít készüléket, majd a szerver szállítójával javíttatja a meghibásodott hardvert. – A szállítókkal kötött szerződésekben mindenképp szerepelnie kell a hardverjavítások időintervallumára vonatkozó megállapodásnak, illetve a tartalékeszközök biztosításáról szóló garanciának (A szállító vállalja a 12 órán belüli hibajavítást, vagy tartalék eszközt kell biztosítani, amelyet 12 órán belül az üzemeltetőnek képes kell lenni konfigurálni és telepíteni). – Folyamatosan vizsgálni kell, hogy az újabb kiadású szoftverek (operációs rendszer, biztonsági szoftverek stb.) futnak-e a szerveren. Amennyiben nem, úgy csere lehet szükséges (lásd Szerverek cseréje).
Eredmény:	Hiba esetén a szerverek gyors helyreállítása.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

Szerverek cseréje	
Feladat:	– Az amortizáció nyomán a régi szervereket ki kell cserélni, hogy a korszerűbb operációs rendszerek, védelmi programok, illetve egyéb szoftverek megfelelően futhassanak rajtuk. Ennek megfelelően a hardverekből kell tartalék. A szerverek cseréjét az üzemeltető kell javasolja írásban, amit a hálózatgazda bírál el. – A régi szervereken levő tartalomról biztonsági mentést kell készíteni. – A kiselejtezett szerverek adattárolóin szereplő adatok megsemmisítéséről minden esetben gondoskodni kell, függetlenül az adatok esetleges minősítésétől.
Eredmény:	Korszerű hardverek, melyeken az újabb fejlesztésű szoftverek is megfelelően futnak.
Felelős:	Szervercsere időben történő igénylése és indokolása: üzemeltető; Szervercseréről döntés: hálózatgazda
Gyakoriság:	Üzemeltető javaslata alapján.

2.3.2. Munkaállomások

Munkaállomásokra vonatkozó korlátozások	
Feladat:	– A munkaállomások jogosultságait az üzemeltetéshez szükséges mértékre kell korlátozni, hogy az azokat ért támadások minél kevesebb eséllyel következzenek be. – Tiltani szükséges mindenféle program öncélú telepítését. Szoftvert csak a rendszergazda telepíthessen a gépekre, az üzemeltető ezért felelős munkatársának jóváhagyása után. – A munkaállomások vírusvédelmét üzemeltetői szinten központilag kell megoldani. – Azokra a munkaállomásokra, amit egy felhasználó használ csak, kizárólag az adminisztrátornak és a felhasználónak legyen belépési jogosultsága.
Eredmény:	Jól ellenőrizhető munkaállomások.
Felelős:	Üzemeltető, csatlakozott szervezetek
Gyakoriság:	Új munkaállomás implementálásakor.

2.3.3. Hálózati hardver eszközök

Hálózati hardver eszközök üzembe helyezése	
Feladat:	– Hálózati eszköz üzembe helyezése esetén az eszközt tesztelni kell, és az eredményről jegyzőkönyvet szükséges felvenni. Biztosítani kell, hogy az új eszköz esetleges működésképtelensége esetén legyen olyan meleg tartalék, amelyik ellátja az eszköz funkcióit. – A tesztelési jegyzőkönyveket az eszköz üzemből való kivonása után legalább még 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni.
Eredmény:	Működőképes hálózati hardver eszközök.
Felelős:	Üzemeltető
Gyakoriság:	Új hálózati eszköz beüzemelésekor.

Hálózati hardver eszközök karbantartása	
Feladat:	– A hálózati hardver eszközök karbantartását és javítását az üzemeltető felügyeli. – Hiba esetén az üzemeltető a tartalékokból biztosít készüléket, majd a hálózati eszköz szállítójával javíttatja a meghibásodott eszközt. – A szállítókkal kötött szerződéseknek mindenképp tartalmazniuk kell a hálózati eszközjavítások időintervallumára vonatkozó megállapodást, illetve a tartalékeszközök biztosítására vonatkozó kötöttségeket (pl. a szállító vállalja a 12 órán belüli hibajavítást, vagy tartalékeszközt kell biztosítani, amelyet 12 órán belül az üzemeltetőnek képes kell lenni konfigurálni és telepíteni).
Eredmény:	Hiba esetén a hálózati eszközök gyors helyreállítása, illetve rendszeres karbantartása.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

Hálózati hardver eszközök cseréje	
Feladat:	– A hálózati eszköz cseréjét az üzemeltető kell javasolja írásban, amit a hálózatgazda bírál el. Ezen túlmenően a hálózatgazda is utasíthatja írásban az üzemeltetőt az eszköz cseréjére. – A javításra külső szervezetnek átadott, illetve leselejtezett hálózati eszközök nem tartalmazhatnak konfigurációs információt. – A csere céljára használt új eszközt előzetesen tesztelni szükséges. – A lecserélt eszköz a körülményektől függően kerülhet selejtezésre, de képezhet tartalékot is.
Eredmény:	Működőképes hálózati hardver eszközök.
Felelős:	Hálózati hardver eszköz cseréjének időben történő jelzése és indoklása: üzemeltető; Eszközcseréről döntés: hálózatgazda.
Gyakoriság:	Üzemeltető javaslata alapján.

2.3.4. A csatlakozott intézmények által üzemeltetett eszközök

Csatlakozott intézmények által üzemeltetett eszközök	
Feladat:	– A csatlakozott szervezetek által üzemeltetett hálózati eszközök rendelkezésre állása az adott intézmény felelőssége, ilyen esetben az üzemeltetőt semmilyen kötelezettség sem terheli. – A csatlakozott intézménytől elvárható, hogy gondoskodjon az adott eszköz folyamatos és zavartalan üzemeléséhez szükséges körülményekről (pl. folyamatos áramellátás, klimatizálás stb.). – Az elektronikus közszolgáltatást nyújtó szervezet köteles gondoskodni az általa üzemeltetett eszköz védelméről (pl. illetéktelen hozzáféréstől, lopástól és manipulációtól való védelem).
Eredmény:	Az elektronikus közszolgáltatást nyújtó szervezetek által üzemeltetett eszközökből eredő biztonsági kockázat csökkenése.
Felelős:	Csatlakozott szervezet
Gyakoriság:	Folyamatosan.

Csatlakozott intézmények által üzemeltetett eszközökkel kapcsolatos hibák	
Feladat:	– Az elektronikus közszolgáltatást nyújtó szervezetek kötelesek az általuk üzemeltetett EKG-hoz kapcsolt eszközökkel kapcsolatos bárminemű hibáról az üzemeltetőt haladéktalanul értesíteni. – A hibák javítása az elektronikus közszolgáltatást nyújtó szervezet feladata, de a hiba igazolt kijavításáig a hiba természetétől függően a hálózatgazdának joga van az üzemeltetővel az adott szervezet hálózati kapcsolatát lezáratni.
Eredmény:	Az elektronikus közszolgáltatást nyújtó szervezetek által üzemeltetett eszközökből eredő biztonsági kockázat csökkenése.
Felelős:	Csatlakozott szervezet
Gyakoriság:	Csatlakozott szervezetek által üzemeltetett eszközök hibája esetén.

Csatlakozott intézmények által üzemeltetett eszközökkel kapcsolatos változások	
Feladat:	– Az elektronikus közszolgáltatást nyújtó szervezetek az általuk üzemeltetett EKG-hoz kapcsolt eszközökről, az azokkal kapcsolatos bármilyen változásról kötelesek az üzemeltetőt haladéktalanul tájékoztatni. – Aktív hálózati hardver elemek esetén az elektronikus közszolgáltatást nyújtó szervezet még a változtatás előtt köteles a tervezett változtatást bejelenteni, és arról az üzemeltető véleményét kérni.
Eredmény:	A csatlakozott szervezetek által üzemeltetett eszközökből eredő biztonsági kockázat csökkenése.
Felelős:	Csatlakozott szervezet
Gyakoriság:	Csatlakozáskor teljes eszközlistáról tájékoztatás, ezt követően változás esetén.

2.3.5. Hardver eszközök nyilvántartása

Hardvernyilvántartás	
Feladat:	– Az üzemeltetőnek az összes EKG hardver eszközről (szerverek, munkaállomások, hálózati eszközök, valamint egyéb elektronikus eszközök) részletes nyilvántartást kell készítenie. – A nyilvántartást biztonságos helyen kell tárolni, melyhez csak megfelelő jogosultsággal férhet hozzá bárki. Gondoskodni kell arról, hogy az aktuális nyilvántartásról mindig legyen biztonsági másolat, melyet az eredetitől elszeparáltan, szintén biztonságos helyen, lopástól és manipulációtól védetten tárolnak. – A hardvernyilvántartás alapján kell történjen a szükséges tartalék eszközök számszerűsítése. – A nyilvántartásban dokumentálni kell a tervezett eszközbeszerzéseket is.
Eredmény:	Pontos hardvernyilvántartás, mely alapján a tartalékképzés tervezhető.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

2.3.6. Tartalék eszközök

Tartalékolási osztályokba sorolás	
Feladat:	– Az EKG eszközöket az alábbi tartalékolási osztályokba kell sorolni: Általános eszközök (normális mennyiségű – lásd köv. pont – tartalék szükséges); üzemeltetés szempontjából kiemelt eszközök (dupla mennyiségű tartalék szükséges)
Eredmény:	Eszközök tartalékolási osztályokba sorolása, amely alapján tervezhető a tartalékképzés.
Felelős:	Üzemeltető
Gyakoriság:	IBSZ érvénybe lépésekor, utána tapasztalatok alapján átsorolni.

Tartalékképzés	
Feladat:	– A tartalékképzés a folyamatos üzemeltetés egyik legfontosabb feladata, ennek megfelelően fokozott figyelmet igényel. – Alapvető szabály, hogy minden EKG-üzemelést biztosító eszközből legyen megfelelő mennyiségű tartalék; és azok üzemképességét folyamatosan kell ellenőrizni. Eszközök, amelyekből tartalékot kell biztosítani: Szerverek, Munkaállomások, hálózati hardver eszközök (switchek, routerek, tűzfalak, hub-ok stb.), Egyéb elektronikus eszközök (UPS, klíma, UPS-akkumulátorok stb.), Egyéb alkatrészek (pl. porszűrő szivacs stb.) – Az általános eszközökből megközelítőleg 5–20%-nyi tartalék szükséges (pl. 10 munkaállomás esetén 1 vagy 2 tartalék munkaállomás). – Az üzemeltetés szempontjából lényeges elemekre megközelítőleg dupla ennyi tartalék (kb. 20–40%) szükséges (pl. 5 router esetén 1 vagy 2 tartalék router). – A tartalékképzésre történő szabály bizonyos esetekben változtatható, a 20% durva becslés. Jelenleg a hálózati eszközökre az alábbi tartalékolási szabály létezik: = 1– 10 darab létezik az eszközből: 1 tartalék eszköz; = 11– 30: 2 tartalék eszköz; = 31– 60: 3 tartalék eszköz; = 61–100: 4 tartalék eszköz; = 100–: 5 tartalék eszköz. – Javasolt megoldás a tartalékok előre történő beszerzésére az éves gazdálkodási terv kialakítása.
Eredmény:	Megfelelő mennyiségű tartalék, mely meghibásodás esetén is biztosítja az EKG üzemelését.
Felelős:	Tartalékképzésért és tartalékok időben történő igényléséért: üzemeltető; Tartalékok beszerzéséért: hálózatgazda.
Gyakoriság:	Folyamatosan.

2.4. Szoftverek

Ez a fejezet tartalmazza az EKG-ban használt szoftverekre vonatkozó, illetve azok védelmét szolgáló feladatokat.

2.4.1. Szoftverkarbantartás

Szoftverek biztonsági frissítéseinek nyomon követése és alkalmazása	
Feladat:	– Az üzemeltető köteles az EKG eszközein használt szoftverek frissítéseit figyelemmel kísérni, és a csatlakoztatott intézmények figyelmét felhívni, illetve azok további működését a szoftverfrissítés után is biztosítani. – A szoftverfrissítéseket (update-ek, service pack-ok) a várható biztonsági hatásuk (pl. kritikus biztonsági probléma javítása stb.) alapján értékelni kell, majd ennek alapján ütemtervet kell meghatározni a bevezetésükre, amennyiben erre tényleg sor kerül. Az ütemtervben meghatározott határidőknek tükrözniük kell a frissítés fontosságát. – Minden használt szoftverre (és azok minden egyes üzemben lévő verzióira) az üzemeltetőnek rendelkeznie kell kidolgozott teszttervekkel. – Minden frissítést az éles rendszeren való telepítés előtt a kidolgozott teszttерveknek megfelelően tesztelni kell. A tesztelés eredménye alapján kell a telepítésre vonatkozó döntést meghozni. – Amennyiben a tesztelés után a telepítés végrehajtását jóváhagyó döntés születik, úgy a megfelelő frissítést a korábban kidolgozott ütemterv szerint telepíteni kell (kritikus frissítés esetén ennek haladéktalanul meg kell történnie). – A szállítókkal kötött szerződésekben mindenképp szerepelnie kell a szoftverfrissítések rendelkezésre állásának, ezzel is biztosítva a szoftverek naprakészségét.
Eredmény:	Biztonsági szempontból naprakész szoftverek.
Felelős:	Üzemeltető
Gyakoriság:	Minden szoftverfrissítés megjelenésekor.

Szoftverek újabb verzióinak nyomon követése és alkalmazása	
Feladat:	– Az üzemeltető köteles figyelemmel kísérni az EKG üzemeltetésében használt szoftverek újabb verzióinak megjelenését. – Új verzió esetén elemezni kell a verzióváltás hatásait (pl. direkt és indirekt költségek, biztonsági szint változása, használhatóság javulása stb.). Az elemzés eredményét dokumentálni kell. Az elemzést lehetőség szerint az új verzió tesztelésével is meg kell támogatni (csak akkor hagyható ki, ha az új verzió nem elérhető, de ebben az esetben az átállási döntésnél figyelembe kell venni a tesztelés hiányából fakadó kockázatokat). – Az elemzés eredménye alapján döntést kell hozni a verzióváltás szükségességéről, és pozitív döntés esetén meg kell határozni az átállás ütemezését. – A kidolgozott ütemezésnek megfelelően el kell végezni a verzióváltást. – Az üzemeltetőnek törekednie kell arra, hogy a használt szoftverek a lehető legnagyobb mértékben egységesek legyenek. – A szállítókkal kötött szerződésekben lehetőség szerint szerepelnie kell a szoftverek verziókövetésének, ezzel is segítve a verzióváltások végrehajtását.
Eredmény:	A lehetőségekhez igazodó, korszerű szoftverpark.
Felelős:	Üzemeltető
Gyakoriság:	A használt szoftverek újabb verzióinak megjelenésekor.

Szoftverek üzemeltetői környezetének folyamatos ellenőrzése és karbantartása	
Feladat:	– Az üzemeltetőnek folyamatosan ellenőriznie kell, hogy minden az EKG üzemeltetésében használt szoftver üzemeltetési feltételei megvannak-e (pl. szükséges memóriamennyiség, szükséges tárterület, naplóállományok számára elegendő tárhely stb.), és mennyire térnek el az optimálistól. – Amennyiben valamely feltétel nem teljesül, úgy haladéktalanul meg kell kezdeni ennek javítását. – Időszakosan (hetente, de legalább kéthetente) gondoskodni kell arról (tárhelyek felszabadítása, megfelelő adatok archiválása stb.), hogy a szükséges környezeti feltételek normális üzemmenet esetén a következő időszakra teljesüljenek.

Eredmény:	A szoftverek üzembiztonságának fenntartása.
Felelős:	Üzemeltető
Gyakoriság:	Ellenőrzés folyamatosan, karbantartás szükség esetén, de legalább kéthetente.

2.4.2. Biztonsági mentések

Biztonsági mentések	
Feladat:	– Az üzemeltetőnek definiálnia kell minden – az EKG-hoz tartozó – adattartalomra (pl. hálózati komponensek konfigurációs állományai, eszköz- és szoftvernyilvántartások, jogosultság adatbázisok, dokumentációk, felhasználói adatok stb.), hogy kell-e róluk biztonsági másolatokat készíteni és milyen sűrűséggel. Ez alapján el kell készíteni a mentési ütemezéseket, forgatókönyveket és ellenőrző listákat. – Az ütemezéseknek megfelelően az üzemeltető köteles a biztonsági mentések elvégzésére. – Amennyiben valamilyen biztonsági esemény ezt szükségessé teszi, úgy az üzemeltető köteles a biztonsági mentésekből az utolsó stabil állapotot visszaállítani.
Eredmény:	Visszaállítható kritikus adattartalom.
Felelős:	Üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor kidolgozott ütemezésnek megfelelően.

Biztonsági mentések tárolása	
Feladat:	– A biztonsági mentéseknek legalább három példányban kell elkészülniük, melyeket egymástól szeparáltan kell tárolni, lehetőség szerint a két budapesti központból és a vidéki tartalékközpontból elérhető helyeken. – Az utolsó 5 biztonsági mentést úgy kell tárolni, hogy azokból a visszaállítás azonnal megkezdhető legyen. – A biztonsági mentéseket legalább 2 évig biztonságosan, lopástól, manipulációtól és illetéktelen hozzáféréstől védve kell megőrizni.
Eredmény:	Többszörösen védett biztonsági másolatok.
Felelős:	Üzemeltető
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor kidolgozott ütemezésnek megfelelően.

2.4.3. Vírusvédelem

Az EKG-n forgalmazott adatok vírusszűrése és mentesítése	
Feladat:	– Mivel az EKG dedikáltan átviteli közeg, ezért sem a hálózatgazdának, sem az üzemeltetőnek nincs jogalapja az adatok tartalmába való betekintésre. Emiatt azok vírusszűrését és mentesítését nem végezheti el. – A fentiek miatt minden csatlakozott szervezet köteles gondoskodni a hozzá tartozó adatok vírusvédelméről, és az ilyen jellegű károkért minden esetben az azt okozó (a nem megfelelő védelemről gondoskodó) intézmény felel.
Eredmény:	Vírusmentesített adatok.
Felelős:	Csatlakozott szervezetek
Gyakoriság:	Folyamatosan.

EKG-ra csatlakozott számítógépek vírusvédelme	
Feladat:	– Az EKG minden szerverén (ahol ilyen megoldás elérhető) gondoskodni kell a folyamatos vírusvédelemről. Ez kiemelten érvényes a Microsoft által forgalmazott operációs rendszereket futtató gépekre. – Minden az EKG-hoz csatlakozott munkaállomáson és szerveren (ahol ilyen megoldás elérhető) gondoskodni kell a vírusvédelemről, ez kiemelten érvényes egyrészt a Microsoft operációs rendszerekre, másrészt azokra a gépekre, amelyekről a hálózat menedzsmentje, üzemeltetése folyik.

Eredmény:	Vírusvédett eszközök.
Felelős:	Üzemeltető, csatlakozott/csatlakozandó szervezetek
Gyakoriság:	Szerverek, munkaállomások üzembe helyezésekor és utána folyamatosan.

A vírusvédelmi eszközök karbantartása	
Feladat:	– Minden az EKG-hoz csatlakozott szerver vagy munkaállomás üzemeltetője (ez vagy a hálózat üzemeltetője, vagy a csatlakozott szervezet) köteles gondoskodni a telepített vírusvédelmi eszközök folyamatos karbantartásáról. – Folyamatosan figyelemmel kell kísérni a vírusvédelmi eszközhöz megjelenő frissítéseket (pl. vírus adatbázis aktualizálás) és azokat haladéktalanul telepíteni kell. – Folyamatosan figyelemmel kell kísérni a vírusvédelmi eszköz újabb verzióinak megjelenését. Új verzió esetén elemezni kell, hogy a verzióváltás milyen hatással járna, el kell dönteni, hogy kell-e verziót váltani, és amennyiben igen, úgy előre kidolgozott ütemterv szerint végre kell hajtani. – A vírusvédelmi eszközök szállítóival kötött szerződésben ki kell kötni, hogy frissítések megjelenése esetén a szállító azt nyomban rendelkezésre bocsátja.
Eredmény:	Naprakész vírusvédelmi eszközök.
Felelős:	Üzemeltető, csatlakozott szervezetek
Gyakoriság:	Folyamatosan.

2.5. Hálózat védelme

Alábbiakban azok az intézkedések szerepelnek, melyek nem köthetők egyértelműen a szoftverekhez vagy a hardver eszközökhöz, hanem inkább a hálózat egészének védelmét szolgálják.

2.5.1. Rendelkezésre állás biztosítása

Szolgáltatási szint megállapodások (SLA)	
Feladat:	– A hálózatgazdának megfelelő szolgáltatási szint megállapodásokat (SLA) kell kötnie az üzemeltetővel és a hálózati kapcsolatokat biztosító távközlési szolgáltatókkal.
Eredmény:	Szolgáltatási szint megállapodások (SLA).
Felelős:	Hálózatgazda
Gyakoriság:	Az üzemeltetési szerződés, illetve a szolgáltatási szerződések megkötésekor, megújításakor.

Hálózati központok	
Feladat:	– Az EKG üzembiztonságának szempontjából a hálózati központok kiesése jelentheti a legnagyobb problémát, ezért a hálózatgazdának gondoskodnia kell arról, hogy két, gyakorlatilag azonos üzemeltetési képességgel rendelkező hálózati központ legyen. – A hálózatgazdának gondoskodnia kell arról is, hogy létezzen olyan vidéki központ, mely ha csökkentett funkcionalitással is, de képes átvenni a hálózat üzemeltetési központjának a szerepét olyan esetben, amikor Budapest nagy területét érintő katasztrófahelyzet következik be. – Amennyiben a hálózatgazda biztosítja az ehhez szükséges eszközöket és helyiségeket, úgy az üzemeltető feladata a központok megtervezése, kialakítása és üzembe helyezése.
Eredmény:	Nagyon megbízható hálózati struktúra.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Az anyagi források rendelkezésre állásától függően.

Redundáns hálózati elemek	
Feladat:	– Az EKG rendelkezésre állási követelményei miatt a hálózat minden elemének redundánsnak kell lennie, nem lehet olyan eszköz vagy hálózati összeköttetés, ami egyedi hibapontnak (single point of failure) minősül. – A redundancia mértékét a szerint kell megválasztani, hogy az adott hálózati elem kiesése a hálózat szolgáltatásának milyen mértékű kiesését veszélyezteti. – Lehetőség szerint a redundanciát úgy kell kialakítani, hogy az egymás kiváltására használt eszközök együtt csak nagyon kivételes esetekben sérülhessenek.
Eredmény:	Nagyon megbízható hálózati struktúra.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	A hálózati elem üzembe állításakor, illetve a hálózat bővítésekor.

2.5.2. Jogosultsági rendszer

Jogosultságokra vonatkozó szabályok	
Feladat:	– A jogosult személyek azonosításának egyértelműnek kell lennie. – A jogosultságokat feladatra vonatkozóan kell meghatározni, és amint szükségtelenné válik haladéktalanul vissza kell vonni. – Az azonosítást és hitelesítést jelszóval vagy egyéb eszközökkel (smart card, token stb.) kell támogatni. – Jelszóhasználat esetén ki kell kötni a jelszavakra vonatkozó szabályokat (minimális hossz, minimális bonyolultság, ciklikusan változó jelszavak kiküszöbölése), és ezeket a jogosultsági rendszernek ki kell kényszerítenie. – Szabályozni kell tudni, hogy az egyes eszközökre (pl. router) milyen IP-címekről lehet bejelentkezni. – Egyéb azonosítást és hitelesítést támogató eszközök esetén meg kell határozni az azok használatára vonatkozó szabályokat (pl. nem átruházható, elvesztés esetén azonnal jelenteni kell, jelentés hiányában az okozott kárért az adott személyt terheli a felelősség stb.). – A szabályokat rendszeresen felül kell vizsgálni és szükség esetén átalakítani.
Eredmény:	A jogosultsági rendszer kijátszásából eredő kockázatok csökkenése.
Felelős:	Üzemeltető, csatlakozott szervezetek
Gyakoriság:	Az informatikai biztonsági szabályzat, illetve a BSZ hatálybalépésével, majd félévente.

Jogosult személyek és alkalmazások nyilvántartása	
Feladat:	– Az üzemeltető köteles a jogosult személyek és alkalmazások nyilvántartására a kapott jogosultságokkal együtt. – A nyilvántartásnak naprakésznek kell lennie, minden változást azonnal át kell vezetni. A változásokat naplózni kell, a naplókat legalább 2 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni. – Lehetőség szerint minden jogosultságokkal kapcsolatos menedzsment feladatot központilag az üzemeltetőnek kell elvégeznie.
Eredmény:	Egyértelmű, naprakész jogosultság-nyilvántartás.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

Jogosultságok kiadásának és visszavonásának folyamata és szabályai	
Feladat:	– Jogosultságok kiadására és visszavonására a hálózatgazda jogosult, melyet utasítására az üzemeltető végez el, csatlakozott intézményeknek bármilyen ezzel kapcsolatos igényüket írásban kell jelezniük. – Jogosultságkérés esetén minden esetben meg kell vizsgálni annak indokoltságát, és ennek eredménye alapján kell meghozni az engedélyezési döntést. – Minden a hálózatban valamilyen szereppel bíró intézmény (csatlakozott intézmények, üzemeltető) haladéktalanul köteles tájékoztatni a hálózatgazdát, ha valamely személy vagy alkalmazás bármilyen jogosultságát vissza kell vonni (pl. dolgozó kilép, új munkakörbe kerül, alkalmazást lecserélik stb.). Ilyen esetben a hálózatgazda köteles azonnal intézkedni.

Eredmény:	Ellenőrzött jogosultság kiadás és visszavonás.
Felelős:	Hálózatgazda, üzemeltető, csatlakozott intézmény
Gyakoriság:	Jogosultsági igény felléptekor vagy megszűnésekor.

Jogosultságok felülvizsgálata	
Feladat:	– Az üzemeltető köteles a jogosultságokat negyedévente felülvizsgálni, és mindazokat a jogosultságokat megszüntetni, melyek már nem indokoltak. – Jogosultság felülvizsgálat alapján történő megvonásáról az adott intézményt előzetesen írásban kell tájékoztatni.
Eredmény:	Naprakész, indokolt jogosultságok.
Felelős:	Üzemeltető
Gyakoriság:	Negyedévente.

Azonosítási és hitelesítési kísérletek naplózása	
Feladat:	– Mind a sikeres, mind a sikertelen azonosítási és hitelesítési kísérleteket naplózni kell. – A naplófájlok 3 hónap elteltével archiválhatók, de az archivált állományokat legalább 2 évig biztonságosan, lopás és manipulációtól védve meg kell őrizni. – A rendszerben lévő naplóállományokhoz csak adminisztrátori jogosultsággal rendelkező személyek, illetve a biztonsági felügyelők férhetnek hozzá. – A naplófájlokat rendszeresen, legalább naponta fel kell dolgozni (ezt a tevékenységet mindenképpen érdemes megfelelő automatikus eszközökkel segíteni), és amennyiben szükséges, úgy haladéktalanul intézkedni kell a jogosultságok korlátozásáról, visszavonásáról vagy a rendszer biztonságának fokozásáról.
Eredmény:	Ismert és minden jogosult által elfogadott eljárásrend.
Felelős:	Hálózatgazda
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor, majd ezt követően évente felülvizsgálva.

Eredménytelen azonosítás, illetve hitelesítés esetén elvégzendő intézkedések rögzítése	
Feladat:	– Meg kell határozni, hogy eredménytelen azonosítás, illetve hitelesítés esetén milyen eljárásrendet kell követni (pl. érvénytelen jelszó vagy felhasználói név beírása után maximum háromszor újra próbálkozhat, ha harmadikra sem sikerül, akkor fél órára zárolódnak a jogosultságai és a rendszer üzenetet küld az adminisztrátornak). – Az eljárásrendet írásban kell rögzíteni és minden jogosultsággal rendelkező személynek vagy alkalmazás felelősének alkalmaznia kell, ellenkező esetben elveszíti a jogosultságait. – Az eljárásrendet évente felül kell vizsgálni és szükség esetén módosítani.
Eredmény:	Ismert és minden jogosult által elfogadott eljárásrend.
Felelős:	Hálózatgazda
Gyakoriság:	Az informatikai biztonsági szabályzat hatálybalépésekor, majd ezt követően évente felülvizsgálva.

2.5.3. MPLS VPN

VPN-csoportok kialakítása	
Feladat:	– Az EKG tagjai közötti biztonságos és garantált sávszélességű kommunikáció miatt a hálózatban VPN-kapcsolatokat szükséges kiépíteni. Az intézményeket kapcsolatok jellegétől függően csoportokba javasolt bontani. A VPN-csoportokat meg kell határozni, és a már csatlakozott intézményeket be kell sorolni ezekbe a kategóriákba. – Meg kell oldani, hogy egy intézmény több VPN-csoportba is tartozhasson. – Ki kell dolgozni a VPN-használat szabályzatát, amely garantálja, hogy több csoportba is tartozó felhasználó révén az érintett VPN-csoportok nem válnak eggyé. A szabályzatot minden érintetthez el kell juttatni.
Eredmény:	Biztonságos, VPN-en keresztül történő kommunikáció.
Felelős:	Hálózatgazda
Gyakoriság:	VPN-ek kialakítása előtt.

Csatlakozó intézmények VPN-csoportba való besorolása, átsorolása	
Feladat:	– Az újonnan csatlakozó intézmények valamelyik VPN-csoportba történő besorolása. – A már csatlakozott intézmény kérésére más VPN-csoportba történő átsorolása, illetve hozzáadása.
Eredmény:	Biztonságos, VPN-en keresztül történő kommunikáció.
Felelős:	Hálózatgazda
Gyakoriság:	Csatlakozáskor, illetve intézmény igénye esetén.

Egy VPN-csoport kiesése nem érintheti más VPN-csoport működését	
Feladat:	– Amennyiben valamelyik VPN-csoport tevékenységét korlátozni kell (pl. az adott VPN-csoportba tartozó intézmények valamelyikét célzott spam támadás éri), úgy gondoskodni kell arról, hogy ez a többi csoport működését csak a lehető legkevésbé zavarja.
Eredmény:	Biztonságosan szeparált és egymástól független VPN-ek.
Felelős:	Üzemeltető
Gyakoriság:	VPN-csoport működésképtelensége vagy korlátozásának szükségessége esetén.

Külső VPN-kapcsolatok engedélyezésének vizsgálata	
Feladat:	– Az üzemeltetés alatt nagy valószínűséggel előfordulnak olyan esetek a jövőben, hogy az EKG-hoz csatlakozott intézmény külső, nem EKG-s IP-címmel kíván VPN-kapcsolatot nyitni. Ilyen esetben erre az adott intézménynek írásban kell engedélyt kérnie a hálózatgazdától, akinek az üzemeltető segítségével meg kell vizsgálnia az adott kapcsolat veszélyeit. A kockázati szint figyelembevételével kell az engedélyezési döntést meghozni. – Engedélyezése esetén az érintett intézménytől igényelni kell a kapcsolat logolását, a logok archiválását és az üzemeltetőnek való átadását. – Az üzemeltető köteles a kapott log fájlokat rendszeresen auditálni és az üzembiztonságot veszélyeztető esemény esetén a kapcsolatot azonnal lezárni. – Ilyen kapcsolatból származó kár esetén a felelősség a kapcsolatot igénylő intézményt terheli.
Eredmény:	Az intézmény oldaláról logolt kapcsolat, melyet az igénylési adminisztráció és a felelősség miatt valószínűleg megfontoltabban kér az intézmény.
Felelős:	Hálózatgazda az engedélyezésért, üzemeltető a felügyeletért
Gyakoriság:	Külső VPN-kapcsolat igénylése esetén.

2.5.4. IP VPN

IP VPN-ek használata	
Feladat:	– A csatlakozott szervezeteknek ajánlott IP VPN-ek kialakítása, mellyel saját tevékenységüket is még biztonságosabbá tehetik. – IP VPN-ek kódolt adatcsomagjainak kicsomagolására az EKG határvédelmi tűzfalán nincs lehetőség, így azok szűréséről a csatlakozott szervezeteknek kell gondoskodniuk. Ezért minden ebből eredő kár az adott intézményt terheli.
Eredmény:	Intézményi IP VPN-ek.
Felelős:	Csatlakozott szervezetek
Gyakoriság:	Csatlakozáskor vagy erre vonatkozó igény esetén.

2.5.5. Tűzfalakra, védelmi intézkedésekre vonatkozó követelmények

Határvédelmi tűzfalak felállítása	
Feladat:	– Az EKG üzembiztonsága megköveteli, hogy hálózati forgalmának zavartalanságát többszintű határvédelmi (a gerinchálózat az internet felé való védelme, amely az üzembiztonságot védi, de a rajta átfolyó adatmennyiség adatbiztonságáért már nem felel) tűzfalrendszer védje. – A felállítandó tűzfalrendszer megtervezéséről, méretezéséről, felállításáról és karbantartásáról az üzemeltetőnek kell gondoskodnia.
Eredmény:	Az EKG tűzfalakkal védett működése.
Felelős:	Üzemeltető
Gyakoriság:	A hálózat kiépítésekor.

Tűzfalak felügyelete és karbantartása	
Feladat:	– Az üzemeltetőnek gondoskodnia kell a tűzfalak zavartalan üzemeléséről. – A tűzfalak konfigurációját időszakosan felül kell vizsgálni, és szükség esetén el kell végezni a megfelelő változtatásokat. A változtatást minden esetben dokumentálni kell, megadva az okot és tényleges változásokat. A jegyzőkönyvet legalább 2 évig biztonságosan, lopástól és manipulációtól védetten meg kell őrizni. – A tűzfalak szállítóival kötött szerződésben ki kell kötni, hogy bármely, a tűzfalakat érintő, nem az üzemeltetésből fakadó hiba esetén köteles annak haladéktalan elhárítására. – A tűzfalaknak minden kapcsolatot naplózniuk kell, a naplófájlokat archiválni kell és legalább 2 évig biztonságosan, lopástól és manipulációtól védetten meg kell őrizni. – A tűzfalak naplófájljait az üzemeltetőnek folyamatosan auditálnia kell.
Eredmény:	Naprakész, felügyelt tűzfalrendszer.
Felelős:	Üzemeltető
Gyakoriság:	Felülvizsgálat negyedévente, illetve betörés esetén; naplófájlok auditja legalább hetente.

Intézmény adott portjának megnyitása	
Feladat:	– Amennyiben valamilyen csatlakozott intézmény tevékenységéhez a tűzfalon egy új portot akar megnyittatni, úgy azt írásban a hálózatgazdával kell engedélyeztetni. – A hálózatgazda az üzemeltető segítségével megvizsgálja, hogy a kérvényezett port megnyitása milyen kockázatokat rejt magában. A vizsgálatról írásos jegyzőkönyvet kell készíteni, melyet legalább 2 évig biztonságos helyen, lopástól és manipulációtól védett módon meg kell őrizni. A kockázati szinttől függően engedélyezhető a port megnyitása. – Az üzemeltető negyedévente köteles felülvizsgálni a megnyitott portokat. Nem használt vagy veszélyforrást jelentő nyitott portok esetén kezdeményezni kell azok lezárását, amit a hálózatgazda hagy jóvá és az üzemeltető végez el. Ilyen esetben előzetesen írásban kell az adott intézményt értesíteni.
Eredmény:	Felügyelt és ellenőrzött port megnyitások.
Felelős:	Csatlakozott intézmény, hálózatgazda, üzemeltető
Gyakoriság:	Port megnyitás kérésekor, illetve a felülvizsgálat negyedévente.

2.5.6. Csatlakozott szervezetekre vonatkozó szabályok

Csatlakozó intézmény egyéb internetkapcsolatainak megszüntetése	
Feladat:	– Az EKG egyik legjelentősebb veszélyforrása az, hogy a csatlakozó intézmények oldaláról érkezik támadás – azok internetes hálózatának nem megfelelő védelme miatt. Ezért az EKG-ra történő csatlakozás alapfeltétele (szerződésben rögzítve), hogy a kapcsolódó intézmény az EKG-ra csatlakozó számítógépeivel, illetve az e számítógépekből álló hálózatával nem kapcsolódhat más külső hálózatra. – Szerződésben szükséges szabályozni, hogy a csatlakozó intézmény felelős az ő oldaláról okozott támadásokért és károkért, legyen az belső (az intézmény alkalmazottjától érkező) vagy külső (az intézmény egyéb hálózati kapcsolatából eredő) támadás.
Eredmény:	Biztonságosan üzemeltethető hálózat.
Felelős:	Hálózatgazda
Gyakoriság:	Csatlakozás esetén.

Csatlakozó intézmény routerének felügyelete	
Feladat:	– A csatlakozó vidéki intézmények nagy száma miatt törekedni kell arra, hogy a csatlakozás minden igényelt kapcsolódási ponton megfelelő router meglétéhez legyen kötve, amelyre az üzemeltetőnek betekintési és menedzselési jogokat kell adni. – Ha a csatlakozó szervezet számára a szükséges routereket az EKG bocsátja rendelkezésre, úgy ezek karbantartása és felügyelete teljes mértékben az üzemeltető feladata, az adott intézmény a routerhez semmilyen jogosultsággal nem rendelkezhet.
Eredmény:	Üzemeltető felügyelete alatt álló routerek.
Felelős:	Felügyeletért az üzemeltető, a betekintési jogok adásáért a hálózatgazda.
Gyakoriság:	Csatlakozás esetén.

Csatlakozó intézmény kapcsolattartóinak megnevezése	
Feladat:	– A csatlakozó intézményektől a szerződés megkötésekor be kell kérni azokat az adatokat, amelyek meghibásodás esetén lehetnek fontosak az EKG üzemeltetésének szempontjából: kapcsolattartók megnevezése (informatikai vezető, illetve technikai szakember), amennyiben a kapcsolat EKG kezelésű eszközzel történik (nem valamely szolgáltató biztosítja a kapcsolatot a megyei alközpontig) pontosan hol helyezkednek el az EKG-hoz kapcsolódó eszközök, klimatizációs lehetőségek, tűzjelző és oltókészülék helye, bejutási lehetőségek adminisztrációja. – Amennyiben ezek az adatok megváltoznak, úgy az intézménynek tájékoztatási kötelezettsége legyen az üzemeltető felé.
Eredmény:	A csatlakozott intézmény főbb – üzemeltetés szempontjából lényeges – adatai.
Felelős:	Hálózatgazda, üzemeltető
Gyakoriság:	Csatlakozás, illetve valamely adat megváltozása esetén.

2.5.7. Hálózat felügyelete

Hálózati események felügyelete	
Feladat:	– Az üzemeltető köteles folyamatos (7×24 órás) hálózati felügyeletet biztosítani. – A hálózat felügyelete magába foglalja a hálózathoz tartozó minden eszköz (amennyiben erre lehetőség van) folyamatos monitorozását, a különböző hálózati események figyelemmel kísérését (pl. terhelések nyomon követése, esetleges kiesések felismerése stb.), azok naplózását, illetve szükség szerint beavatkozást. – A felügyeletet lehetőség szerint a hálózat minél nagyobb részére kiterjedő menedzsment eszközzel kell megtámogatni.
Eredmény:	Felügyelt hálózat.
Felelős:	Üzemeltető
Gyakoriság:	Folyamatosan.

2.5.8. Rendhagyó (rendkívüli) események jelentése, kezelése

Biztonsági események kezelése	
Feladat:	– Üzembiztonságot befolyásoló esemény észlelése történhet a hálózat felügyelet által, illetve felhasználói bejelentésre. – Mindkét esetben haladéktalanul meg kell kezdeni az esemény hatásainak csökkentését és magának az eseménynek az elemzését. – Az elemzés eredményét dokumentálni kell, a jegyzőkönyvet legalább 5 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni. – Az elemzés eredményét felhasználva el kell dönteni, hogy milyen módon kell a hálózatba beavatkozni, az esemény kivédéséhez és az okozott kár minimalizálásához. Ennek megfelelően ki kell alakítani egy akciótervet. – A kialakított akciótervet végre kell hajtani folyamatosan ellenőrizve, hogy közben a hálózatban nem keletkeznek-e újabb biztonságot befolyásoló események.
Eredmény:	Kezelt biztonsági események.
Felelős:	Üzemeltető
Gyakoriság:	Biztonsági esemény bekövetkeztekor.
Incidens menedzsment	
Feladat:	– Incidensnek minősül bármi, ami arra utal, hogy a hálózat nem üzemszerűen, az elvárt módon működik. – Incidens észlelése történhet a hálózat felügyelet által, illetve felhasználói bejelentésre. – Mindkét esetben az incidenst az üzemeltető erre a célra használt rendszerében rögzíteni kell az összes felderítést és elhárítást elősegíthető adattal együtt, majd haladéktalanul meg kell kezdeni az esemény hatásainak csökkentését és magának az eseménynek az elemzését. – Az elemzés eredményét dokumentálni kell, a jegyzőkönyvet legalább 5 évig biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni. – Az elemzés eredményét felhasználva el kell dönteni, hogy milyen módon kell a hálózatba beavatkozni, az esemény kivédéséhez és az okozott kár minimalizálásához. Ennek megfelelően ki kell alakítani egy akciótervet. – A kialakított akciótervet végre kell hajtani folyamatosan ellenőrizve, hogy közben a hálózatban nem keletkeznek-e újabb biztonságot befolyásoló események. – Az üzemeltető incidens követő rendszerének képesnek kell lennie az incidensek életciklusának nyomon követésére, a korábbi incidensek közötti keresés támogatására, a problémák eszkalálására stb.

Eredmény:	Kialakult incidenskezelési folyamat, hálózati problémák gyors, szakszerű megoldása.
Felelős:	Üzemeltető
Gyakoriság:	Incidens bekövetkeztekor.

Nagy felhasználószámú intézmény csatlakozása	
Feladat:	– Amennyiben nagy felhasználószámú intézmény csatlakozik az EKG-hoz, úgy a hálózatgazda értesítse az üzemeltetőt, hogy az fel tudjon készülni a várható terhelésnövekedésre. Ilyen esetben eszközbővítések válhatnak szükségessé.
Eredmény:	Nagyobb intézmény csatlakozása sem okoz negatív változást az üzemeltetés biztonságában.
Felelős:	Hálózatgazda
Gyakoriság:	Nagy felhasználószámú intézmény csatlakozásakor.

3. Záró rendelkezések

3.1. A biztonsági szabályzat bevezetése, oktatása

Az üzemeltetői biztonsági szabályzatot hatálybalépése előtt mind a hálózatgazdának, mind az üzemeltetőnek el kell fogadnia. A csatlakozott szervezet biztonsági szabályzatát az EKG biztonsági felelőse véleményezi, és nem megfelelő szabályozás esetén a hálózatgazda jogosult a csatlakozást felfüggeszteni a szabályozás (illetve a probléma) korrekciójáig.

A hatálybalépés előtt minden érintett személyt tájékoztatásban kell részesíteni. Ehhez szerepekre (pl. rendszeradminisztrátorok, hálózati mérnökök stb.) szabott tájékoztató anyagokat célszerű készíteni, ezáltal lehetővé téve, hogy mindenki tisztában legyen a saját feladatának biztonsági vonzataival.

Mindazok esetében, akik a hálózat üzembiztonságának szempontjából jelentős feladattal (pl. biztonsági vezető, biztonsági felügyelő, rendszeradminisztrátorok, üzemeltetési vezető stb.) bírnak, a tájékoztatást (oktatást) számon kérhető módon kell végrehajtani, és az elsajátított ismeret szintjét ellenőrizni kell.

A hatálybalépés előtt ki kell dolgozni a biztonsági szabályzat betartásához szükséges feltételek megteremtését célzó akciótervet, pontos feladatokkal, határidőkkel és felelősökkel. Ezt az akciótervet a hatálybalépés előtt (illetve a hatálybalépést követően a hálózatgazda által meghatározott türelmi időn belül) végre kell hajtani, amit a hálózatgazdának felügyelnie kell.

3.2. A biztonsági szabályzat hatálybalépése

A biztonsági szabályzat hatálybalépése a csatlakozás időpontja, illetve a korábban csatlakozott szervezetek esetében a jogszabályban meghatározott időpont.

A csatlakozó szervezet biztonsági szabályzata kizárólag akkor léphet hatályba, ha a végrehajtásához szükséges minden alapfeltétel vagy fennáll, vagy meghatározásra került a teljesítés határideje.

3.3. A biztonsági szabályzattól való eltérés rendje

A biztonsági szabályzattól csak rendkívül indokolt esetben, a hálózatgazda jóváhagyásával és előre meghatározott ideig lehet eltérni.

Amennyiben a szabályzat betartása valami okból nem lehetséges, úgy ezt írásban jelezni kell a hálózatgazda felé. A hálózatgazdának ilyen esetben az üzemeltető segítségével meg kell vizsgálnia, hogy a kérés indokolt-e, létezik-e egyéb megoldás, amivel a probléma áthidalható, illetve a kérés jóváhagyása milyen kockázatokat rejt magában. A vizsgálat eredményét írásban dokumentálni kell (a jegyzőkönyvet legalább 5 évig, biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni).

Amennyiben a vizsgálat alapján a kérést a hálózatgazda jóváhagyja, úgy azt is meg kell határoznia, hogy a felmentés meddig állhat fent. Mindezeket jegyzőkönyvezni kell (a jegyzőkönyvet legalább 5 évig, biztonságosan, lopástól és manipulációtól védett módon meg kell őrizni).

Jóváhagyott szabályzattól való eltérés esetén az érintettek kötelesek ezt az állapotot a meghatározott határidő leteltével megszüntetni.

A biztonsági szabály véletlen megsértése esetén, annak észlelését követően az érintettek kötelesek tájékoztatni erről a helyzetről a hálózatgazdát, illetve kötelesek haladéktalanul megkezdeni ennek az állapotnak a felszámolását. Amennyiben az EKG üzembiztonsága ezt megköveteli, úgy a szabálysértés megszüntetéséig a hálózatgazdának joga van a hálózat működőképességének fenntartása érdekében az érintettek hálózati kapcsolatát felfüggeszteni.

3.4. A biztonsági szabályzat aktualizálásának, kiegészítésének rendje

A biztonsági szabályzatot (ideértve az IBSz-t is) legalább évente felül kell vizsgálni, és gondoskodni kell szükség szerinti módosításáról, kiegészítéséről.

A hálózati rendszer jelentős változása esetén a felülvizsgálatot soron kívül el kell végezni.

A biztonsági szabályzat módosításainak bevezetésére és hatályba léptetésére a 3.1. és a 3.2. alfejezetekben leírtak érvényesek.

A szabályzat kiegészítésére, módosítására az üzemeltető és a felhasználók közvetlenül tehetnek javaslatot a hálózatgazdának. A hálózatgazda a módosítás előtt kikéri az üzemeltető és az informatikai biztonsági felügyelő véleményét.

Az üzemeltetői biztonsági szabályzat visszavont rendelkezése esetén a hálózatgazdának meg kell határozni a hatályvesztés pontos időpontját, és erről minden érintettet tájékoztatni kell. A visszavont szabályokat archiválni kell, dokumentálva az okokat, a visszavonás kezdeményezőjét és jóváhagyóját, valamint idejét.

1. számú függelék

A dokumentumban használatos (részben EKG-specifikus) alapfogalmak leírása

Megnevezés	Leírás
Hálózatgazda	A közigazgatási informatikáért felelős miniszter, feladatait az infokommunikációért felelős kormánybiztos látja el.
Üzemeltető	A hálózatgazdával közszolgáltatási szerződéses viszonyban lévő, a hálózat felügyeletéért, és rendelkezésre állásáért felelős szervezet. Külön jogszabály alapján a Kopint-Datorg Zrt.
Távközlési szolgáltatók	Mindazok a távközlési szolgáltatók vagy konzorciumok, amelyek az EKG üzemeltetéséhez szükséges infrastruktúrát biztosítják.
Csatlakozott intézmény	Mindazok a – jellemzően közigazgatási – intézmények, melyek az EKG valamely szolgáltatását igénybe veszik.
Nagy felhasználószámú intézmény	Olyan csatlakozott intézmény, amelyben a munkaállomások száma a 400 darabot meghaladja.
ITSEC	Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok).
UPS	Szünetmentes áramforrás, amely áramkimaradás esetén rövid ideig biztosítja a hozzá kötött eszközök áramellátását.
VPN	Virtuális magánhálózat (Virtual Private Network). Használatával a kapcsolódó felek lényegében úgy kommunikálhatnak, külön titkosítás nélkül a nyilvános hálózatokon, mintha külön bérelt, fizikailag elválasztott magánhálózatot hoztak volna létre.

4. melléklet a 223/2009. (X. 14.) Korm. rendelethez

A központi elektronikus szolgáltató rendszer által nyújtott közszolgáltatások igénybevételének biztonsági feltételei

1. Általános leírás

1.1. Áttekintés

1.1.1. Szolgáltatás terjedelme

A központi elektronikus szolgáltató rendszer (a továbbiakban: KR vagy központi rendszer) feladata többek között az elektronikus közszolgáltatásról szóló 2009. évi LX. törvényben meghatározott, a központi rendszer azonosítási szolgáltatásait igénybe véve megvalósított elektronikus kapcsolattartás lehetővé tétele azáltal, hogy

– a központi rendszert igénybe vevő természetes és jogi személyek (a továbbiakban: felhasználók) által előkészített, kitöltött elektronikus űrlapokból – a központi rendszer elektronikus űrlap formátumára vonatkozó szabályoknak megfelelő – üzenetet állít elő;
– ellenőrzi az elektronikus űrlap formai követelményeknek való megfelelését;
– a formai követelményeknek megfelelő elektronikus beadványokat érkezteti;
– az érkeztetés tényét és időpontját bizonyító elektronikus dokumentumot – visszaigazolást – elkészíti, és a felhasználó részére kézbesíti;
– az érkeztetett elektronikus beadványt kézbesíti a címzett elektronikus közszolgáltatást nyújtó vagy abban részt vevő részére olyan eljárással, hogy a szolgáltató a beküldő személyét a jogszabályban meghatározott módon azonosítani tudja;
– illetve lehetővé teszi a fordított irányú kommunikációt is, ahol biztosítja annak tanúsítását, hogy a címzett átvette-e a neki szóló küldeményt.

A szolgáltatás nem terjed ki

– a felhasználó, illetve harmadik személy tulajdonát képező, a szolgáltatás igénybevételéhez a felhasználó által használt számítástechnikai eszközökre és szolgáltatásokra, beleértve az internetszolgáltatást is;
– az elektronikus ügyintézési folyamat – és ezen keresztül a kitöltött elektronikus űrlapok – tartalmi ellenőrzésére, a tartalmi ellenőrzést, érdemi feldolgozást minden esetben a címzett szervezet végzi el.

1.1.1.1. Szolgáltatás személyi hatálya

A szolgáltatást ügyfélkapuval, illetve hivatali (ennek a vállalkozások számára szolgáló változatával a cégkapuval) rendelkező természetes, illetve jogi személyek vagy jogi személyiséggel nem rendelkező, de közhiteles nyilvántartásban szereplő szervezetek vehetik igénybe.

1.1.1.2. Szolgáltatás területi hatálya

A szolgáltatást magyarországi telephelyről nyújtja a központi rendszer működtetője, a Miniszterelnöki Hivatal, a szolgáltatás nyújtásával kapcsolatban a magyar jogszabályok mérvadók. A szolgáltatás igénybevétele területileg nem korlátozott, azonban az 1.1.1. pontban jelzett funkcionális korlátozás e vonatkozásban is érvényes.

1.1.2. Közzététel

Jelen dokumentum a Magyar Közlönyben kerül az elektronikus közszolgáltatás biztonságáról szóló kormányrendelet mellékleteként kihirdetésre, majd a MeH elektronikus úton hozzáférhetővé teszi a http://www.magyarorszag.hu/segitseg internetes címen.

1.1.3. Értelmező rendelkezések

Központi elektronikus szolgáltató rendszer

Az elektronikus közszolgáltatások nyújtásához felhasznált, a kormányzati portálon keresztül elérhető, szolgáltatást, tájékoztatást és egyéb közhasznú szolgáltatásokat nyújtó informatikai rendszerek összessége, beleértve a felhasználók számára hozzáférhetővé tett nyomtatványkitöltő alkalmazást is.

Központi rendszer működtetője – a Miniszterelnöki Hivatal

A központi rendszer által nyújtott szolgáltatásokért jelen dokumentumban meghatározott korlátozásokkal felelősséget vállaló jogi személy.

1.1.4. Kapcsolódó jogszabályok

– a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.);
– a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.);

– Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (a továbbiakban: Ekszt.) és végrehajtási rendeletei
– A hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről szóló 2009. évi LII. törvény

1.2. Szolgáltatásban részt vevő felek és kötelezettségeik

1.2.1. Miniszterelnöki Hivatal (MeH)

A MeH kötelezettséget vállal arra, hogy mindenkor a jelen dokumentumban meghatározott feltételekkel nyújtja szolgáltatását, különösen tekintettel arra, hogy:

– a rendszer alapszolgáltatásait az ügyfélkapuval rendelkező ügyfelek térítésmentesen vehetik igénybe;
– a MeH által felügyelt informatikai rendszerek folyamatos működését és ezáltal a vállalt szolgáltatási szintet a tőle elvárható gondossággal biztosítja;
– az elektronikus beadványok titkosságát a címzett szervezethez történő beérkezésig biztosítja;
– a MeH az általában elvárható magatartás szerint szabályzatait betartja, illetve a részt vevő felekkel betartatja.

A MeH az ügyfelekkel való kapcsolattartást központi ügyfélszolgálat (ügyfélvonal) telefonos és internetes és internettelefonos (VoIP) szolgáltatásainak igénybevételével biztosítja.

1.2.2. Felhasználók

A központi rendszer szolgáltatásait igénybe vevő természetes és jogi személyek a biztonságos és zavarmentes ügyintézés érdekében kötelezettséget vállalnak arra, hogy jelen dokumentumot megismerik; a dokumentum, valamint a hatályos jogszabályok a felhasználókra vonatkozó rendelkezéseit betartják; vállalják a felelősséget a felhasználói azonosítójukkal végzett tevékenységekért, különösen az általuk az elektronikus közszolgáltatásokat nyújtó szervezetekhez küldött – a központi rendszer által továbbított – elektronikus üzenetek tartalmáért.

1.2.3. Az elektronikus közszolgáltatást nyújtó szervezetek

A központi rendszerhez jogszabályi kötelezés alapján vagy önkéntesen csatlakozott államigazgatási, önkormányzati vagy más közhatalmi szerv, közüzemi szolgáltató vagy más költségvetési szerv, illetve vállalkozás, amely a központi rendszeren át folytatott kommunikációt a törvényekben rögzített eljárásrend mellett bizonyító erejű kommunikációként kezeli, a központi rendszer által nyújtott azonosítást folyamataiban alkalmazza. Elfogadja a központi rendszer által továbbított elektronikus beadvány beérkezésének időpontját, elvégzi az elektronikus beadvány tartalmi vizsgálatát, ellátja a jogszabályokban és belső szabályzatában meghatározottak szerint az ügyfélkapcsolatot, és a felhasználó igénye esetén elektronikusan válaszol a hozzá érkezett üzenetre.

1.2.4. Ügysegéd

Ügysegéd olyan informatikai és/vagy az ügyintézéshez kapcsolódó szakismerettel rendelkező természetes személy, illetve ilyen tevékenységet végző jogi személy vagy jogi személyiséggel nem rendelkező szervezet lehet, amely (aki) az ügyfél megbízásából ügyintézési folyamatokat végez, vagy támogatást ad az ügyek intézéséhez, a központi rendszer használatához. A feladatot elláthatja jogszabályban arra feljogosított hatóság is, amely a Ket. 169. § (1) bekezdése alapján ügyfél képviseletében ügyintézést végez, illetőleg internetes kapcsolati lehetőséget biztosít, szakmai és informatikai segítséget nyújt.

Az ügysegéd minden esetben az ügyfél megbízása alapján, az ügyfél igényének megfelelően köteles eljárni. Az ügysegéd köteles az elektronikus ügyintézés során az ügyfél utasításának maradéktalanul megfelelve eljárni, továbbá köteles felhívni ügyfele figyelmét minden tevékenység végrehajtása előtt azokra a problémákra, amelyeket a döntése okozhat. Az ügysegéd az ügyintézés során önállóan a megbízás kereteit túllépve hozott döntésért a Ptk. alapján felel.

Az ügysegéd kötelessége az elektronikus ügyintézés során a jelen dokumentumban az ügyfelekre vonatkozó rendelkezések betartása az általánosan elvárható gondossággal.

2. A szolgáltatás igénybevételének általános szabályai

Az ügyfelek hozzáférés igénylésének és a szolgáltatás használatának szabályait az Ekszt. rögzíti. A szolgáltatás használójának ugyanakkor tekintettel kell arra lennie, hogy az elektronikus beadványok az interneten nem megbízható átviteli közegben, nem garantált szolgáltatási szinten továbbítódnak. Ennek következménye, hogy a központi rendszeren keresztül a szolgáltatás nyújtójához továbbított elektronikus üzenetét csak akkor tekintheti kézbesítettnek, ha a beérkezés tényét a központi rendszer részére visszaigazolta.

2.1. A használat előfeltétele

2.1.1. Ügyfélkapu létesítése

A központi rendszer azonosítást igénylő szolgáltatásait csak ügyfélkapuval rendelkező felhasználó veheti igénybe az ügyfélkapura történő bejelentkezést követően. Az ügyfélkapu létesítésére vonatkozó szabályok részletesen a www.magyarorszag.hu/ugyfelkapu oldalon érhetők el.

2.1.2. Nyomtatványkitöltő program üzembe helyezése

Az Ekszt 19. § (2) bekezdés b) pontja alapján a rendszer működtetőjének lehetősége van arra, hogy az elektronikus űrlapok és csatolmányaik biztonságos továbbítását lehetővé tevő alkalmazást az ügyfelek rendelkezésére bocsásson. A MeH az elektronikus közszolgáltatást nyújtó szervezetek számára megküldhető elektronikus űrlapok kitöltésére programot bocsát az ügyfelek rendelkezésére, mely

– alkalmas a címzett szervezetek által kibocsátott vagy általánosabb célú elektronikus űrlapok kitöltésére,
– elvégzi az elkészített űrlap elsődleges tartalmi ellenőrzését és előkészítését (titkosítását) az elektronikus elküldéshez. Az űrlapot egyébként ki is lehet nyomtatni, és postán el lehet küldeni, ahol ezt törvény nem zárja ki,
– biztosítja az elektronikus beadvány továbbítását a központi rendszer, és azon keresztül a címzett szervezet felé.

A felhasználó feladata a www.magyarorszag.hu és a www.apeh.hu honlapról a nyomtatványkitöltő és súgó program aktuális verziójának, szükség esetén további – harmadik személy által készített – programkomponenseknek[1] letöltése és telepítése a programokhoz mellékelt telepítési útmutató alapján.

Annak érdekében, hogy a felhasználó a nyomtatványkitöltő program sértetlenségéről és épségéről a telepítést megelőzően meggyőződhessen, a program készítője az általános nyomtatványkitöltő program telepítő csomagját elektronikus aláírással látja el, mely tanúsítja, hogy

– a program a készítőjétől származik,
– a program nem módosult a közzététel során.

A programot a MeH biztosítja az ügyfelek részére, ugyanakkor a számítógépes szoftverek komplex természetéből adódóan nem garantálja, hogy az átadott szoftver teljesen hibamentesen vagy bárminemű zavar nélkül működik, illetve, hogy minden hardver- és szoftver-konfigurációval kompatibilis. A MeH a szoftverekre vonatkozó általános szavatossági feltételekkel összhangban nem vállal felelősséget a szoftver használatából eredendő esetleges károkért, a használatával kapcsolatos adatvesztésért. Ugyanakkor tömeges, illetve típushibák esetén lehetőségei függvényében biztosítja a javítást a programhoz.

Tekintettel arra, hogy a programot a felhasználó az általa üzemeltetett munkaállomásra telepíti, vagy nyilvános internet-hozzáférési ponton veszi használatba (pl. Teleház, Internetkávézó, E-pont), a felhasználó feladata a nyomtatványkitöltő alkalmazás megbízható üzemeltetési környezetét biztosítani vagy annak meglétéről meggyőződni, beleértve az általános helyes gyakorlatnak megfelelő vírus- és behatolásvédelmi rendszer működtetését is.

Az általános nyomtatványkitöltő program on-line kapcsolat esetén automatikusan ellenőrzi, hogy újabb verzió mind a programból, mind a feltelepített elektronikus űrlapokból kiadásra került-e, s ha hozzáférhető a program újabb verziója, akkor erről tájékoztatja az ügyfelet. Ha nincs on-line kapcsolat, figyelmezteti az ügyfelet erre a lehetőségre. A felhasználó dönt a frissítés telepítéséről, ugyanakkor a MeH javasolja, hogy a frissítéseket a felhasználó rendszeresen telepítse.

2.2. Használat szabályai

2.2.1. Elektronikus űrlap letöltése, frissítése

A felhasználó az elektronikus közszolgáltatást nyújtó szervezet által készített, és hozzá benyújtandó elektronikus űrlap aktuális verzióját a www.magyarorszag.hu honlapról, illetve a címzett szervezet honlapjáról töltheti le és telepítheti. Az űrlapok sértetlenségének ellenőrizhetőségét a kibocsátó biztosítja.

A nyomtatványkitöltő program az elektronikus űrlapok telepítését követően automatikusan ellenőrzi a sértetlenséget, és az űrlap sérüléséről tájékoztatja az ügyfelet. Sérült elektronikus űrlapot ne használjon! Ha nem sikerül az űrlapot hibaüzenet nélkül telepíteni, akkor e tényt kérjük, jelezze a központi ügyfélszolgálaton, mely a 189-es hívószámon érhető el.

Tekintettel arra, hogy a hatóságokkal való kommunikációhoz rendszeresített elektronikus űrlapok tartalma, valamint az elektronikus űrlapokhoz kapcsolódó ellenőrzések változhatnak, a www.magyarorszag.hu honlapon mindig az elektronikus közszolgáltatást nyújtó szervezetek által rendszeresített elektronikus űrlapok legújabb változatát publikálja. A nyomtatványkitöltő program a feltöltéseket megelőzően minden esetben megvizsgálja, hogy a használt elektronikus űrlapból létezik-e újabb verzió, amennyiben létezik, erről tájékoztatja az ügyfelet.

A MeH felelőssége ezzel összefüggésben csak az elektronikus űrlapok biztonságos publikálására korlátozódik. Az elektronikus közszolgáltatást nyújtó szervezet jogosult meghatározni, hogy mely verziójú elektronikus űrlapokat fogadja be a felhasználóktól, ezért a MeH javasolja ügyfeleinek, hogy az esetleges kellemetlenségek elkerülése érdekében – ha szükséges – frissítsék az elektronikus űrlapokat, és a legújabb verziójú elektronikus űrlapot kitöltve intézzék ügyeiket.

---

[1] Jelenleg csak a Java futtató környezet, amely szintén díjtalanul áll rendelkezésre.

2.2.2. Az elektronikus űrlap kitöltése, a kitöltés ellenőrzése

Az elektronikus űrlapot a felhasználó tölti ki, az űrlapon rögzített adatok helyességéért és pontosságáért a felhasználó vállalja a felelősséget függetlenül attól, hogy a nyomtatványkitöltő program által nyújtott alábbi lehetőségek közül melyiket használja:

– az elektronikus űrlapok kitöltését egyedileg a nyomtatványkitöltő alkalmazásban;
– egy megfelelő módon előállított – a címzett szervezet honlapján publikált szintaxisú – XML állományból történő adatbetöltést az elektronikus űrlapra;
– egyszerre több importállományból történő adatbetöltést egy-egy elektronikus űrlapra;
– közvetlenül a nyomtatványkitöltő program XML kimeneti állományának előállítására szolgáló más – a felhasználó vagy általa megbízott harmadik személy által fejlesztett – alkalmazással úgy, hogy a kimeneti állomány formai, logikai ellenőrzése történik csak a nyomtatványkitöltő programmal.

Abban az esetben, ha a felhasználó problémát észlel az űrlap kitöltése vagy tartalmi ellenőrzése során, kérjük ezt közvetlenül jelezze az érintett szervezetnek[2]. A felhasználó – tekintettel arra, hogy az adatok helyességéért teljes felelősséggel tartozik – természetesen jogosult a nyomtatványkitöltő program ellenőrzésének eredményét felülbírálni, illetve figyelmen kívül hagyni (azaz az esetek jelentős részében jogosultak hibajelzés mellett is elküldeni az űrlapot). A szolgáltatást nyújtó szervezetek ugyanakkor bizonyos logikai feltételeknek meg nem felelő űrlapok befogadását jogosultak megakadályozni az értelmezhetetlen adatok feldolgozásának elkerülése érdekében.

Az elkészített és a MeH által publikált elektronikus űrlapokhoz sok esetben külön letölthető egy útmutató, vagy helyzetérzékeny segítő fájl, amely segíti az űrlap kitöltését.

Egyes esetekben az elektronikus űrlap mellé az adott ügyintézéshez szükséges elektronikus mellékletek is csatolhatók

2.2.3. Elektronikus beadvány előkészítése feladásra

A 2.2.2. fejezet szerint elkészített kimeneti állományból az elektronikus küldeményt a nyomtatványkitöltő program állítja elő biztosítva, hogy

– az elektronikus beadvány a központi rendszer által elfogadott formátumú legyen,
– az elektronikus beadványban továbbítandó, az elektronikus űrlapon rögzített adatok titkossága biztosított oly módon, hogy az adattartalomhoz csak a címzett szervezet férhessen hozzá.

Az elektronikus beadvány előállítása a felhasználó kötelessége, amit a nyomtatványkitöltő program erre vonatkozó funkciójával tehet meg. A kezelésre vonatkozó részletes leírást a kormányzati portál tesz közzé.

A központi rendszer az elektronikus beadvány beérkezésekor megvizsgálja, hogy az elektronikus beadvány megfelel-e a formai követelményeknek, a hibás formátumú elektronikus beadványokat a rendszer visszautasítja és a visszautasítás tényéről az ügyfelet értesíti. Ha a felhasználó a nyomtatványkitöltő programmal készítette el azon elektronikus beadványát, melyet feladáskor a központi rendszer visszautasított, és ismeretei szerint minden előírást pontosan betartott, akkor haladéktalanul jelezze a problémát a KÜK felé.

2.2.4. Elektronikus beadvány feladása, érkeztetése

A tényleges küldés megkezdéséhez a felhasználónak be kell lépnie az ügyfélkapun. A felhasználó csak ezt követően jogosult a dokumentum feltöltésére.

A MeH felelősséget vállal azért, hogy a 2.2.3. pontban elkészített elektronikus beadványt tartalmi módosulás nélkül, csak a központi rendszerben használt időbélyegzéssel és érkeztetési számmal ellátva továbbítja a központi rendszeren keresztül a címzett szervezet részére.

A központi rendszer által az elektronikus beadványon elhelyezett időbélyegzés igazolja, hogy az időbélyeg által jelzett időpontban a központi rendszer a feladótól az elektronikus beadványt átvette és a címzett szervezet értesítési tárhelyén elhelyezte.

A címzett szervezet az elektronikus beadvány beérkezésének időpontjaként a központi rendszer által az elektronikus beadványhoz csatolt időbélyegben rögzített időpontot fogadja el.

A felhasználónak kell biztosítania, hogy elektronikus beadványát oly módon adja fel, hogy az – amennyiben ilyen van – a címzett szervezet, hatóság által meghatározott határidő előtt a központi rendszerbe beérkezzen. A felhasználó nem tekintheti elektronikus beadványát a központi rendszer által érkeztetettnek mindaddig, míg erre vonatkozóan a központi rendszer részére visszajelzést nem küldött.

---

[2] Az érintett szervezetek ügyfélszolgálati elérhetőségei a www.magyarorszag.hu honlap hivatalkeresőjében találhatók meg.

A MeH nyomtatékosan felhívja a központi rendszeren át elektronikus űrlapokat küldő felhasználók figyelmét, hogy mind a kimenő állományt, mind a nyomtatványkitöltő program által abból készített elektronikus beadványt rendszeresen – lehetőleg a küldést követően azonnal – archiválják elektronikusan és szükség esetén papír alapon is, hogy később, vitás esetekben, ezen adatok a rendelkezésére álljanak! A megbízható elektronikus archiválás céljára rendelkezésére áll a központi rendszer által biztosított tartós tár is, amelybe a hivatalokhoz megküldött elektronikus űrlapok és a rájuk vonatkozó értesítések helyezhetők csak el. Az archivált példány megőrzési idejét a felhasználó határozza meg, de a MeH javasolja, hogy minden esetben vegye figyelembe a jogszabályok rendelkezéseit, hasonlóan a papír alapú beadványokhoz.

2.2.5. Visszaigazolás

A visszaigazolás birtokában a felhasználó kijelentheti, hogy beadványa a visszaigazoláson szereplő időpontban a címzett szervezethez megérkezett, a benyújtási kötelezettség esetén ennek a visszaigazolásban jelzett időpontban eleget tett. A visszaigazolást a felhasználó kötelessége oly módon tárolni, hogy a címzett szervezettel esetleg felmerülő vitás kérdésben azt mint bizonyítékot felhasználhassa. A központi rendszer üzemeltetője a kibocsátott visszaigazolásokat csak az érkeztető szám alapján visszakereshető módon tárolja. Az igazolás tartalmaz olyan azonosító információt, amely alapján annak változatlansága ellenőrizhető.

A központi rendszer által kiadott visszaigazolás a felhasználó kérése szerint két formátumban kerülhet továbbításra:

– az ideiglenes tárhelyre (lásd 2.2.8 fejezet) PDF formátumú visszaigazolást küld a központi rendszer;
– a felhasználó által az ügyfélkapu nyitásakor megadott (módosítható) elektronikus levelezési címre egyszerű formátumú elektronikus levelet küld a központi rendszer.

2.2.5.1. PDF formátumú visszaigazolás

„Érkeztetés visszaigazolás

Tisztelt <*Felhasználó neve*>!

Ön a(z) <címzett szervezet neve> részére elküldte a ‘<Űrlap típusszáma>’ típusú kitöltött dokumentumát/nyomtatványát. A dokumentumot az elektronikus közigazgatási rendszer befogadta és gondoskodik annak továbbításáról a(z) <címzett szervezet neve> részére.

Az elküldésre került dokumentum file-neve:

<*Fájl neve*>

a befogadott dokumentum érkeztető száma:

<*A központi rendszer által generált, a jogszabályok által meghatározott képzési módot követő érkeztető szám*>

a befogadás hivatalos érkeztetési időpontja:

<*Év*>.<*Hónap*>.<*Nap*>. <*Óra*>:<*Perc*>

a befogadott dokumentum elektronikus lenyomata (SHA256-os algoritmussal és hexadecimális formában):

<*SHA–256 lenyomat hexadecimálisan*>

Segítség a nap 24 órájában

Telefon

Magyarországról hívható kék szám (helyi tarifával hívható): 189

Külföldről hívható telefonszám: +36 1 452-3622

Honlap

Mindent az Ügyfélkapuról:

www.magyarorszag.hu/ugyfelkapu/segitseg

www.ugyfelvonal.hu

E-mail

189@ugyfelvonal.hu

Fax

Magyarországról: 1 452-3621

külföldről: +36 1 452-3621

Üdvözlettel,

Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

Budapest, <dátum>.”

A visszaigazolás tartalmazza:

– az elektronikus beadványban továbbított fájl nevét, így segítve az ügyfelet, hogy a későbbiekben is azonosítani tudja, hogy mely visszaigazolás mely elektronikus beadványra, illetve az abban foglalt dokumentumra vonatkozik;
– az érkeztető számot, mellyel mind a felhasználó, mind a címzett szervezet a későbbiekben hivatkozhat a beadott dokumentumra;
– a beadás időpontját jelző időbélyegzést, mellyel a felhasználó igazolni képes, hogy a központi rendszer mely időpontban érkeztette az elektronikus beadványát.

2.2.5.2. Elektronikus levél, mint visszaigazolás

Az elektronikus levél tartalma megegyezik az előzőekben ismertetettel, azzal az eltéréssel, hogy nincs formázási információ benne.

2.2.6. Többes jóváhagyás kezelése

Egyes adatszolgáltatások, dokumentumok esetében a benyújtó (jellemzően jogi személy) saját szabályzata többes aláírást követel meg. Ebben az esetben a dokumentum csak akkor tekinthető benyújtottnak, ha azt valamennyi aláíró aláírta már. Addig az elektronikus beadvány (az űrlap) benyújtásra vár, már az érintett hivatalnál. Kivétel ez alól, ha az ügyfelek mindegyike saját, közigazgatásban felhasználható elektronikus aláírásával látja el benyújtás előtt az elektronikus dokumentumot.

A többes jóváhagyás technikai feltételeit a címzett szervezet teremti meg, használatának szabályait is ő rögzíti.

A központi rendszer a többes jóváhagyás kezelését azzal támogatja, hogy lehetővé teszi az elektronikus közszolgáltatást nyújtó szervezet számára, hogy a felhasználó elektronikus tárhelyére, illetve elektronikus levélcímére jóváhagyásra felszólító értesítést küldjön.

2.2.7. Elektronikus beadvány feldolgozása

Az elektronikus beadvány feldolgozása a címzett szervezet feladata, a beadvány feldolgozásával kapcsolatban a központi rendszer kizárólag a dokumentum tartalmának változatlan átadásáért felelős.

2.2.8. Értesítési tárhely használata

Az ügyfélkapu létesítésével párhuzamosan a felhasználó részére értesítési tárhelyet biztosít a központi rendszer, melyet a kormányzati portálon a http://www.magyarorszag.hu/allampolgar/szolgaltatasok/tarhely címre bejelentkezve ér el. A értesítési tárhelyen a felhasználónak lehetősége van a beérkezett üzenetek listázására, olvasására, saját számítógépre letöltésére és törlésére, beleértve a központi rendszer által küldött visszaigazolásokat is.

A központi rendszer biztosítja, hogy letöltés esetén az értesítési tárhely kiválasztott üzenetének egy másolati példánya a felhasználó számítógépén jöjjön létre fizikailag.

Az értesítési tárhelyet a MeH átmeneti jelleggel, időben korlátozva bocsátja az ügyfelek rendelkezésére, azaz az üzenetek csak a beérkezéstől számított 30 napig tárolhatók az értesítési tárhelyen.

Az üzenet letöltésével párhuzamosan rendelkezik a felhasználó arról, hogy az értesítési tárhelyről az üzenetet törli, vagy megtartja. A határidőt követően az üzenet automatikusan törlésre kerül!

A MeH felhívja ügyfelei figyelmét, hogy a felhasználó értesítési tárhelyének tartalmát vagy annak valamely részét utólag, a felhasználó által kért vagy határidő lejárata miatti törlés után nem képes visszaállítani.

2.2.9. Tartós tárhely használata

Az elektronikus közszolgáltatásokat ügyfélkapuval igénybe vevő felhasználók számára a Miniszterelnöki Hivatal tartós tárhelyet is biztosít a központi rendszerben. Ez a tárhely az értesítési tárhelyhez kapcsolódva a felhasználó számára érkezett, illetve általa az elektronikus közszolgáltatást nyújtó szervezeteknek megküldött elektronikus dokumentumok tárolását szolgálja. Használata időben nem korlátozott, jelenleg ügyfélkapunként 30 Mb tárhely áll a felhasználó rendelkezésére. Ennél nagyobb tárhely biztosítása csak külön megállapodás és díjfizetés alapján lesz lehetséges.

2.3. Használati jog felfüggesztése, megszüntetése

2.3.1. Hozzáférés megszüntetésének szabályai

Tekintettel arra, hogy a jogszabályi előírások szerint a felhasználó felel minden, a felhasználó által nyitott ügyfélkapun keresztül elérhető szolgáltatás helyes használatáért, valamint a hozzáférési jelszó védelméért, a MeH – a jogszabályi előírásoknak megfelelően – lehetővé teszi a felhasználók számára, hogy a jelszó feltételezhető kompromittálódása esetén a hozzáférés megváltoztatását kezdeményezzék.

2.3.1.1. Elveszett jelszó

Az új jelszót a www.magyarorszag.hu honlap ügyfélkapu bejelentkezési felületének elveszett jelszó menüpontjában lehet igényelni. Az eljárás eredményeként a felhasználó egy újabb egyszer használatos jelszót kap a regisztrációkor bejelentett elektronikus levélcímére, amivel az első regisztrációkor kapott egyszer használatos jelszóhoz hasonlóan kell eljárni. A szolgáltatás egy nap csak három alkalommal vehető igénybe.

2.3.1.2. Jelszó megváltoztatása

Az ügyfélkapu bejelentkezési felületén elérhető jelszó változtatása menüpont – amelyben a jelszót meg lehet változtatni – csak a bejelentkezett felhasználó számára áll rendelkezésre.

2.3.2. Újraérvényesítés módja

Amennyiben a felhasználó nem csak a jelszavát vesztette el, hanem a felhasználói nevét is, vagy mindkettő kompromittálódott, a korrekcióra – éppen a visszaélések kizárása, adatok jogtalan megismerésének korlátozása érdekében kizárólag az okmányirodában való személyes megjelenéssel van lehetőség. Kérjük ezért, hogy a két azonosítóelemet elkülönítetten és különös gondossággal tárolják.

2.3.3. Ügyfélkapu megszűnése

2.3.3.1. A jelszó lejárata

Az ügyfélkapu a létrehozást követően a megszüntetéséig érvényes. Ugyanakkor a jelszó korlátlan idejű használata biztonsági okokból nem támogatott, azt kétévente meg kell újítani. A jelszó érvényességi idejének lejáratát követően az ügyfélkapu hozzáférése automatikusan megszüntetésre kerül. Ekkor a hozzáférés ismételt biztosítására csak az elveszett jelszóra vonatkozó szabályok szerint vagy új ügyfélkapu létesítését követően nyílik lehetőség. Új ügyfélkapu létesítésével azonban a korábbi tartós tárhoz nem lehet hozzáférést biztosítani. Éppen ezért fontos a lejáratra odafigyelni és még az előtt elektronikusan meghosszabbítani az érvényességet.

2.3.3.2. Ügyfél saját kérésére

Személyes megjelenés esetén az ügyfélkapu megszüntetésének eljárásrendje azonos az ügyfélkapu létesítésére vonatkozó eljárásrenddel. A www.magyarorszag.hu bejelentkezési felületén a felhasználó közvetlenül meg tudja szüntetni a saját ügyfélkapuját.

2.4. Speciális szabályok

2.4.1. Ügyfél elektronikus levelezési címének kezelése

A jogszabályi előírásoknak megfelelően a felhasználó kötelessége, hogy az ügyfélkapuhoz rendelt adataiban – különösen az elektronikus levelezési címében – történő változásokat haladéktalanul átvezesse.

A központi rendszer lehetővé teszi a felhasználó számára, hogy az elektronikus levelezési címét, melyre az értesítéseket a központi rendszer küldi, az ügyfélkapura történő bejelentkezést követően megváltoztassa.

A MeH elhárít minden, a felhasználó által megadott elektronikus levelezési címre történő hibás kézbesítésből származó felelősséget, különösen, ha a kézbesítés

– az elektronikus levelezési cím hibás voltából,
– az internet működési zavarából vagy
– az elektronikus levelezési címhez kapcsolódó szolgáltatás üzemavarából fakadóan

hiúsult meg.

3. Szolgáltatás minőségi feltételei

3.1. Szolgáltatás színvonala

A központi rendszer vállalja, hogy

– a szolgáltatást 0–24 órás üzemben 99,9% rendelkezésre állással nyújtja. Az üzemzavar esetére a hatósági ügy esetén a Ket 65. § (8) bekezdésében leírtak alapján vagy automatikusan mentesíti az ügyfelet az ebből származó hátrányok alól, vagy kérésére igazolást ad ki az üzemzavar tényéről. Az üzemzavarra vonatkozó információ a www.magyarorszag.hu kezdőlapján felül lenyíló menüben található;
– egy óra alatt legalább 200 ezer dokumentum fogadását, bejelentkezés kezelését biztosítja;
– a sikeresen feltöltött beadványokat – ha a nyomtatványkitöltő program sikeresnek minősíti a feltöltést – 1 percen belül érkeztetési számmal és időbélyegzéssel látja el és továbbítja a címzett szervezet tárhelyére, valamint a visszaigazolást a felhasználó ideiglenes tárhelyén elhelyezi, illetve erről az értesítő e-mailt elindítja.

3.2. Üzemzavar kezelése

3.2.1. Üzemzavar fogalmi meghatározása

Üzemzavarnak minősül, ha a központi rendszer az ügyfelek folyamatos kiszolgálását 15 percnél hosszabb ideig nem tudja biztosítani, azaz:

– a nyomtatványkitöltő program aktuális verziójával készített elektronikus beadványt a központi rendszer tömegesen elutasítja;
– a központi rendszer bármely okból nem képes fogadni a beadványokat;
– a központi rendszer a befogadott beadványokról nem képes a visszaigazolásokat visszaküldeni.

Jelen szabályzat szempontjából nem számít üzemzavarnak:

– az üzemzavar időtartama nem éri el a 15 percet;
– a címzett szervezet informatikai rendszerének átmeneti vagy tartós működési zavara; ebben az esetben az üzenet befogadásra és visszaigazolásra kerül, csak a szervezet veszi később át;
– a felhasználó által észlelt nem üzemszerű működés, ha ez a felhasználó informatikai rendszerének, illetve az internet vagy az informatikai eszközök működését biztosító környezet átmeneti vagy tartós működési zavarára vezethető vissza, függetlenül attól, hogy ez a felhasználók milyen körét érinti; ebben az esetben a hatósági ügyeknél a Ket. szabályai szerint a helyi szolgáltatótól lehet, illetve kell igazolást kérni a mulasztás kimentéséhez;
– a nyomtatványkitöltő program vagy az elektronikus űrlapok működési hibája, ha a hiba jelentkezésének időpontjában már elérhető a kormányzati portálon vagy a címzett szervezet honlapján a program vagy az elektronikus űrlap újabb verziója, illetve a hiba nem akadályozza az űrlap beküldését.

3.2.2. Tájékoztatás üzemzavarról

Üzemzavar esetén a www.magyarorszag.hu kormányzati portálon információ jelenik meg az üzemzavar kezdő és végidőpontjáról, amit egy hónapon keresztül lehet a honlapon megtalálni. Az érintett csatlakozott szervezeteket a MeH közvetlenül tájékoztatja az üzemzavarról. Ennek megfelelően külön igazolást csak abban az esetben indokolt kérni, ha valamilyen egyedi hiba merült fel, ez azonban csak kivételesen lehet a központi rendszer által igazolható.

3.2.3. Üzemzavar következményei

A Ket. 33. §-a értelmében az üzemzavar az ügyintézési határidőbe nem tartozik bele.

Abban az esetben, ha az üzemzavar az APEH felé határidőre történő kötelezettség teljesítésében akadályozza az ügyfelet, mert az üzemzavar a határidő napján jelentkezik, akkor a határidő automatikusan – külön kérelem nélkül – egy teljes nappal elcsúsztatásra kerül.

Minden más esetben

– a Hatóság saját hatáskörben dönt a határidő megváltoztatásáról, de csak az üzemzavar időtartamával köteles a határidőt módosítani (amennyiben az akadályozza a határidőre történő benyújtást);
– egyedi üzemzavar (dokumentum megsérülése vagy más hibajelenség esetén) a felhasználó kérelmére a MeH igazolást állít ki az üzemzavar tényéről, rögzítve az üzemzavar kezdetének és végének időpontját.

A központi rendszer üzemeltetője a központi rendszer rendelkezésre állását, az üzemzavarok időpontját és időtartamát hitelesen dokumentálja.

3.2.4. Üzemzavar kezelése

Az üzemzavar elhárítását a MeH azonnal megkezdi. Abban az esetben, ha az üzemzavar következményeként adatvisszaállítás szükséges, akkor megvizsgálja, hogy

– az adatvisszaállítás mely időpontra lehetséges, illetve adatvesztés előfordulhatott-e,
– az adatvisszaállítás érinti-e a felhasználói törzsadatokat vagy a benyújtott adatokat.

3.2.4.1. Adatvesztés kezelése

Az elektronikus közszolgáltatást nyújtó szervezet ideiglenes tárhelyét érintő adatvesztés előfordulása esetén a MeH a naplóállományok alapján az ideiglenes tárhelyre és a felhasználó elektronikus levelezési címére együttesen küldött levélben értesíti a visszaállított időpont és az üzemzavar bekövetkezési ideje között a rendszerbe bejelentkezett felhasználókat az általuk küldött elektronikus beadványok esetleges elvesztéséről. A tényről a MeH az érintett csatlakozott szervezeteket is tájékoztatja. A felhasználó kötelessége, hogy megismételje az elektronikus beadvány feladását, ugyanakkor az elektronikus közszolgáltatást nyújtó szervezet felé kötelezettségét az első beküldés időpontjában teljesítette, ha e tényt igazoló visszaigazolás a birtokában van.

A felhasználó ideiglenes tárhelyét a MeH a legutolsó mentett állapotba állítja helyre.

3.2.4.2. Törzsadat visszaállítás

Abban az esetben, ha a felhasználók törzsadatainak visszaállítása szükséges, akkor minden bizonytalan azonosítási állapotú felhasználó jelszavát módosítja új egyszer használatos jelszóra;

– a jelszavakat elküldi a felhasználók elektronikus levelezési címére;
– a felhasználó a következő bejelentkezésnél a regisztrációhoz hasonlóan az új egyszer használatos jelszóval képes bejelentkezni, majd köteles megváltoztatni a jelszavát egy általa választott jelszóra;
– a jelszó változtatását követően a felhasználó a 2.2 pont rendelkezései szerint ismét használhatja a központi rendszer szolgáltatásait.

3.2.5. Bűncselekmény gyanúja esetén követett eljárás

Abban az esetben, ha az üzemzavar feltételezhetően a hatályos jogszabályok értelmében bűncselekménynek tekinthető tevékenység következménye, a MeH büntető feljelentést tesz az illetékes nyomozó hatóságnál.

A MeH a nyomozás hatékony lefolytatása érdekében a nyomozó hatóság által kért minden adatot (lásd 4.4.2. pont) a hatóság rendelkezésére bocsát.

3.3. Panaszkezelés

Az elektronikus közszolgáltatást nyújtó szervezet és a felhasználó közötti vitás ügybe a MeH csak abban az esetben vonható be, ha az információ bizonyíthatóan a központi rendszerbe történt beérkezés és az elektronikus közszolgáltatást nyújtó szervezetnek történt átadás között sérült vagy változott meg. Ez a rendszer működési modelljéből következően a tartalom ismerete nélkül is dokumentálható.

3.3.1. Kapcsolattartás

A MeH a szolgáltatás igénybevétele során felmerülő problémák orvoslására, megválaszolására, reklamációk ügyintézésére központi ügyfélszolgálatot, ügyfélvonalat üzemeltet, melyet a felhasználó telefonon, illetve levélben vagy elektronikus úton kereshet fel.

Az ügyfélszolgálat adatai:

Központi ügyfélszolgálat – ügyfélvonal

Nyitva tartási idő:	0–24 óráig
Elérhetőségek:	
Telefon:	Magyarországról hívható kék szám (helyi díjszabással): 189
	Külföldről hívható telefonszám: +36 1 452 3622
SMS	189
Honlap:	www.magyarorszag.hu/ugyfelvonal
	www.ugyfelvonal.hu
E-mail:	189@ugyfelvonal.hu
Fax:	Magyarországról: 1 452 3621
	külföldről: +36 1 452 3621

A központi ügyfélszolgálat lehetővé teszi a felhasználó számára, hogy

– az elektronikus beadványok kezelésével kapcsolatban tájékoztatást, probléma esetén segítséget kérjen;
– konkrét – hatósági ügyintézéshez kapcsolódó – panasz esetén a felhasználó a címzett hatóság illetékes munkatársának eléréséhez támogatást kapjon.

3.3.2. Panaszok, kifogások intézése

Amennyiben a felhasználó a központi ügyfélszolgálat munkáját nem ítéli kielégítőnek, úgy lehetősége van levélben (cím: 1094 Budapest, Balázs Béla u. 35.) vagy elektronikus levélben (ekelnh@ahiv.hu) megkeresni a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalát, ahol panaszát az erre vonatkozó szabályok szerint kivizsgálják.

3.3.3. Késedelem

Késedelemre visszavezethető vita esetén a felhasználónak rendelkezésére áll a beadványaira a központi rendszer által adott visszaigazolás (lásd 2.2.5. fejezet), mellyel bizonyítja, hogy kötelességének a visszaigazolásban rögzített időpontban eleget tett. Az elektronikus közszolgáltatást nyújtó vagy abban részt vevő szervezetek, hatóságok a visszaigazolásban rögzített időpontot nem kérdőjelezik meg.

3.3.4. Tartalmi problémák

Ha a felhasználó mindenképpen meg kíván bizonyosodni arról, hogy az általa továbbított beadvány sértetlenül érkezett-e meg a szolgáltatást nyújtó szervezethez, akkor jogszabály lehetővé teszi számára, hogy a feladással párhuzamosan saját maga számára is elküldjön egy példányt a feladott dokumentumcsomagból, a saját tartós tárhelyére. Ez kétség esetén bizonyítja, hogy mit küldött el.

Abban az esetben, ha az elektronikus beadványt az elektronikus közszolgáltatást nyújtó szervezet nem képes feldolgozni, akkor a Ket., illetve az adott szervezetre, hatóságra vonatkozó jogszabályokban meghatározott eljárásrend szerint igényelheti a hiánypótlást, a hibás, téves adatok kijavítását, az általa meghatározott ügyrend szerint utasíthatja az ügyfelet az adatok javítására. A hibás adatszolgáltatás következményeit, az alkalmazandó szankciót a Hatóság által alkalmazott gyakorlatot a hatályos jogszabályok határozzák meg.

3.4. Tiltott tevékenységek

Az ügyfél csak a személyéhez rendelt jogosultsággal tevékenykedhet a központi rendszerben, és a felhasználói azonosítójával végrehajtott minden tevékenységért felelősséggel tartozik.

A központi rendszer működtetője a felhasználó jogellenes tevékenysége esetén büntetőeljárás lefolytatását kezdeményezi.

4. Biztonsági intézkedések

Jelen fejezet a MeH informatikai biztonsági elkötelezettségét bizonyítja, az ügyfélkapcsolatra vonatkozó biztonsági óvintézkedéseket rögzíti. A központi rendszer részletes biztonsági eljárási szabályait az üzemeltetők nem nyilvános Informatikai Biztonsági Szabályzatai rögzítik.

4.1. Szervezeti és személyi biztonsági intézkedések

4.1.1. Belső eljárásrendek

4.1.1.1. Általános szabályok

A központi rendszer informatikai eszközeit kizárólag felhatalmazott, a feladat ellátásához szükséges szaktudással rendelkező személyzet működteti. A MeH a működtetés folyamatait belső eljárásrendekben rögzítette, előírva, hogy milyen rendszerességgel, milyen módon kell az üzemeltetési és karbantartási feladatokat végrehajtani.

A központi rendszeren történő minden munkavégzés naplózásra kerül.

A MeH a szolgáltatásban és az azt kiszolgáló informatikai rendszerekben bekövetkező módosítások, változások biztonságos és visszakereshető végrehajtása érdekében dokumentált változáskezelési rendet követ.

4.1.1.2. Biztonsági felülvizsgálatok rendje

A rendszeres információ biztonsági felülvizsgálatok célja a kialakított védelmi rendszer működési hatékonyságának mérése az egyenszilárdságot veszélyeztető hiányosságok és sebezhetőségek feltárása, a szükséges helyesbítő és megelőző védelmi intézkedések kidolgozása, előterjesztések elkészítése.

A MeH a központi rendszer kulcsfontosságú komponenseire rendszeresen – évente legalább egyszer – sebezhetőségi vizsgálatot végeztet, melynek végrehajtása során figyelembe veszi a naplózott események feldolgozása során azonosítható támadási kísérleteket és módokat. A sebezhetőségi vizsgálat célja, hogy az egyes komponensek által hordozott biztonsági kockázatok újraértékelése megtörténjen.

A MeH megkívánja továbbá az egyes szoftver komponensek gyártóitól, hogy sebezhetőségi vizsgálatot végezzenek, és erre vonatkozóan a bizonyítékokat adják át a MeH részére.

A MeH szúrópróbaszerűen egy-egy esemény felülvizsgálatát havonta többször, általános felülvizsgálatot hathavonta, vagy üzemzavart kiváltó rendkívüli eseményt követően azonnal hajt végre, a felülvizsgálatról készült bizonylatokat 15 évig megőrzi. A vizsgálatokat minden esetben a naplóállományokra alapozza.

4.1.2. Fontos és bizalmas munkakörök

4.1.2.1. Biztonsági felelős

Az üzemeltető biztonsági felelőse biztosítja

– a kockázatok csökkentését célzó védelmi intézkedések kidolgozását, bevezettetését;
– a már életbe léptetett eljárásrendekben előírt intézkedések érvényre jutását, betartatását;
– az informatikai rendszerek biztonsági szintjének rendszeres ellenőrzését;

– az üzemeltetői hozzáférési jogok kiadásának és visszavételének kezelését;
– a központi rendszer napló archiválását, rendszeres átvizsgálását, biztonsági események feltárását.

4.1.2.2. Adatvédelmi felelős

A MeH adatvédelmi felelőse látja el az Avtv.-ben rögzített feladatokat, beleértve az ügyfelek személyes adatainak kezelésével kapcsolatos tájékoztatási és ellenőrzési kötelezettségeket is.

4.1.2.3. Üzemeltetésvezető

Az üzemeltetésvezető feladata a központi rendszer működtetésének megszervezése, a működés biztonságához szükséges nyilvántartások naprakészségének biztosítása, az üzemeltetési folyamatok kialakítása, a rendszergazdák és operátorok tevékenységének koordinálása, együttműködés a biztonsági vezetővel a védelmi intézkedések kialakításában.

Az üzemeltetésvezető teljes utasítási joggal rendelkezik üzemeltetés területén.

4.1.2.4. Rendszergazda

A rendszergazda feladata központi rendszer egyes alrendszereinek üzemeltetése, beleértve
– az operátor által nem kezelhető incidensek elhárítását;
– az elkészített adat- és rendszermentések belső szabályok szerinti tárolását, utasításra adatvisszaállítás végrehajtását;
– a belső szabályzatokban előírt rendszeres karbantartási tevékenységek végrehajtását;
– a változások élesítését az üzemi környezetben;
– az üzemeltetői hozzáférési jogok beállítását az informatikai rendszereken a biztonsági felelős utasításainak maradéktalan betartásával.

A rendszergazda köteles tevékenységét a belső szabályzatok előírásai szerint bizonylatolni.

4.1.2.5. Operátor

Az Operátor feladata
– biztonsági események fogadása, elsőszintű kezelése;
– távfelügyeleti rendszeren a központi rendszer működésének folyamatos monitorozása;
– mentések végrehajtása.

A operátor köteles tevékenységét a belső szabályzatok előírásai szerint bizonylatolni.

4.1.3. Személyi biztonság

A személyekre vonatkozó biztonsági intézkedések célja a gondatlanságból elkövetett emberi károkozás, valamint a szándékos visszaélések kockázatának csökkentése.

Tekintettel arra, hogy a fontos és bizalmas munkakört betöltők esetében van lehetőség leginkább a visszaélésekre, ezért ezeket a munkaköröket
– csak erkölcsi bizonyítvánnyal rendelkező, nemzetbiztonsági ellenőrzésen átesett;
– megfelelő szakképesítéssel és szakvizsgával, az adott szakterületre előírt gyakorlattal rendelkező

személy töltheti be.

A MeH hangsúlyt fektet arra, hogy az ilyen munkakört betöltő személyek szakmai felkészültsége mindenkor megfeleljen a kor követelményeinek, ezért a továbbképzések rendjét belső utasításban határozza meg.

Ilyen munkakört betöltő személy által elkövetett visszaélés esetén a MeH a jogszabályok figyelembevételével a lehető legszigorúbb szankciókat alkalmazza.

4.2. Fizikai biztonsági intézkedések

A központi rendszer alapvető informatikai eszközeinek telephelyét és a működésükhöz szükséges infrastruktúrát a MeH biztosítja. A kialakított környezet az
– áramellátás,
– légkondicionálás,
– tűzmegelőzés és tűzvédelem,
– villámvédelem,
– betörésvédelem, beleértve az élőerős védelmet is,

területén a vonatkozó biztonsági előírásoknak maradéktalanul megfelel, a kialakított védelem arányban áll a MeH által kockázatelemzésben azonosított kockázatokkal, és biztosítja, hogy:
– az infrastruktúrát érintő hibák ne veszélyeztessék a vállalt szolgáltatási szintet;
– természetes személyek gondatlanságból vagy szándékosan ne legyenek képesek kárt okozni a központi rendszer működésében, továbbá
– ne legyen módjuk veszélyeztetni a központi rendszer által feldolgozott adatok titkosságát és sértetlenségét.

4.3. Adatbiztonság

4.3.1. Mentés

A központi rendszerben tárolt és feldolgozott minden adatról üzemzavar elhárítása céljából adatmentés készül. Ezen mentések biztosítják, hogy adatvesztéssel járó üzemzavar esetén az adatvesztés mértéke még elfogadható mértékű legyen. A kialakított mentési stratégia olyan, hogy legrosszabb esetben is csak korlátozott adatvesztés lehetséges.

4.3.2. Archiválás

4.3.2.1. Archivált adatkörök és megőrzési idejük

Az ügyfél által végzett tevékenységekről készített naplóállományok megőrzési ideje egy hónap, ezen adatok az előírt időpontig archiválásra kerülnek.

Az ügyfélszolgálati és üzemeltetési tevékenységekről készített naplóállományok megőrzési ideje ugyanez.

A dokumentummozgásokhoz (bevallások, adatszolgáltatások, döntések stb. ügyfelek, illetve hivatalok általi küldése) kapcsolódó adatokat pedig a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény alapján elfogadott levéltári tervek szerint archiváljuk, mivel ezek az iratmozgás alapdokumentumai.

4.3.2.2. Az archivált adatok védelme és hozzáférési szabályok

A MeH az archivált adatok titkosságát és sértetlenségét belső biztonsági szabályzataiban meghatározott módon védi. Az archivált adatokhoz az üzemeltető biztonsági felelőse és az általa feljogosított személyek kizárólag a törvényben meghatározott célokból férhetnek hozzá. A MeH a teljes megőrzési idő alatt biztosítja a jogosultak számára az adatok hozzáférhetőségét és értelmezhetőségét.

4.3.2.3. Az archivált adatok gyűjtésének rendje

Az elektronikusan tárolt adatok naponta kerülnek mentésre oly módon, hogy az adathordozók egy e célra rendszeresített tárolóhelyen kerülnek elhelyezésre.

A nem elektronikus formában keletkező adatok, iratok a MeH irattári tervében meghatározott módon kerülnek tárolásra.

4.4. Logikai biztonsági intézkedések

4.4.1. Üzembiztonság

A központi rendszer szolgáltatásait biztosító informatikai rendszerek ellenállnak az egyszeres hardver meghibásodásnak.

4.4.2. Időforrás és időszinkronizáció

Tekintettel arra, hogy az üzenettovábbító alrendszer által nyújtott szolgáltatás esetében az idő nagy jelentőségű, a központi rendszer minden komponensének belső órája szabványos és hiteles időforráshoz szinkronizált, az időt szolgáltató eszközök a beérkező időadatok egyértelműségét biztosítják.

Az időszinkronizálás jelen szabályzatban meghatározott pontosságánál nagyobb eltérése üzemzavarnak minősül és az eseményt a MeH a 3.2 pont rendelkezései szerint kezeli.

A használt időforrások az UTC-hez képest néhány ezred másodpercet térhetnek el, a rendszer egészének pontossága is jobb, mint az időbélyegzésekben megadott idő.

4.4.3. Az időbélyegzés megoldása

Az időbélyegzés előállítása a központi rendszerben az e célra telepített külön eszközön történik oly módon, hogy az időbélyegzésre használt elektronikus aláíró eszköz megfelel a minősített aláírásra vonatkozó jogszabályi követelményeknek. A minősített időbélyegzés szolgáltatás biztosítása a külön jogszabályban meghatározott feltételek szerint történik.

4.4.4. Határvédelem

A központi rendszert az internettől tűzfal szerverek választják le, melyekre vonatkozó részletes rendelkezéseket a központi elektronikus szolgáltató rendszer informatikai biztonsági szabályzata rögzíti. A határvédelmi rendszer biztosítja az adatáramlás ellenőrzését/szűrését a feldolgozó rendszerek felé megelőzendő a kártékony kódok és szolgáltatásmegtagadás támadások előfordulását, megakadályozza a tiltott adatforgalmat, naplózza mind a tiltott, mind az engedélyezett adatforgalmat.

A határvédelmi rendszer riasztási funkcióval is rendelkezik, mely meghatározott tiltott események bekövetkezése esetén automatikusan jelzést ad. Ezen események rendkívüli eseményként kezelendők. A központi rendszer üzemeltetője folyamatosan monitorozza a központi rendszer adatforgalmát és rosszindulatú tevékenység észlelése esetén értesíti az ezek kezelésére feljogosított hatóságokat.

4.4.5. Biztonsági naplózás

A központi rendszer biztonságos működése csak akkor valósítható meg, ha a rendszerben bekövetkező események visszakereshető és elemezhető módon tárolásra kerülnek. Az ügyfeleknek tudomásul kell venniük, hogy saját és más

ügyfelek biztonsága érdekében az általuk végrehajtott tevékenységek jelentős része naplózásra kerül. A MeH a naplózott eseményt kiváltó látogatókat vagy ügyfeleket a naplózás tényéről külön nem értesíti, indokolt esetben azonban be kívánja vonni őket az esemény kivizsgálásának folyamatába. (A MeH kéri tisztelt ügyfeleit, hogy a kivizsgálásában közreműködni szíveskedjenek.)

A központi rendszer a rendszer aktivitását széles körben és részletesen naplózza, beleértve mind a látogató, mind a bejelentkezett ügyfél és Hatóság, mind az üzemeltetők által végzett tevékenységeket.

A naplóbejegyzések minden esetben tartalmazzák az esemény bekövetkezésének dátumát és időpontját, minden, az esemény utólagos kiértékelése szempontjából fontos adatot, beleértve a végrehajtó személy azonosításához szükséges adatokat.

Tekintettel a központi rendszer egyes komponenseinek naplózás tulajdonságaira, bár a naplóállományok nem egy helyen és azonos formában keletkeznek, de tárolásuk és feldolgozásuk központilag egységes szerkezetben történik.

4.4.5.1. Tárolt események típusai

A központi rendszer minden, a látogatók, és ügyfelek által végzett tevékenységet naplóz, beleértve

- bejelentkezés nélkül elérhető honlapok esetében
  - = a látogatás időpontját,
  - = a látogató számítástechnikai eszközének IP címét,
  - = a böngésző típusát;
- a felhasználó ügyfélkapus bejelentkezésével végezhető eljárások esetében
  - = a felhasználó nevét és e-mail címét (amit egyébként az ügyintéző rendszereknek átadott),
  - = a felhasználó bejelentkezésének és kijelentkezésének időpontját anélkül, hogy az aktivitás természetéről rögzítene további adatokat;
- az előző naplóállománytól teljesen függetlenül tárolja a továbbított üzenetek naplóbejegyzéseit, s benne
  - = feladó nevét;
  - = feladó e-mail címét;
  - = címzett elektronikus közszolgáltatást nyújtó megnevezését;
  - = a továbbított dokumentum típusát (nyomtatványazonosító);
  - = az érkeztető számot;
  - = a fogadás és továbbítás időpontját.

A naplóállományok kezelése a 4.3.2.1. pontban rögzített adatkezelési határidőkig történik, kivéve a dokumentummozgásokhoz (bevallások, adatszolgáltatások, döntések stb. ügyfelek, illetve hivatalok általi küldése) kapcsolódó adatokat, melyek kezelésére a Ket. hatálya alá tartozó eljárási cselekmények Ügyfélkapun keresztül történő intézésekor került sor, s melyek tárolásának időtartama a levéltári törvényben rögzített selejtezési határidőkkel egyezik meg.

Az üzemeltetési tevékenységek és a rendszer belső működésének naplózása szintén megtörténik, beleértve

- rendszermenedzsment tevékenységeket, mint rendszergazdai be-, illetve kijelentkezés, a rendszer vagy komponensének indítása/leállítása, verziófrissítés, adatbázis-menedzsment tevékenységek;
- az audit alrendszer menedzsmentjével kapcsolatos tevékenységeket, mint a naplózási funkció konfigurációjának módosítása, leállítása, újraindítása stb.;
- mentési műveleteket;
- ügyfélszolgálati tevékenységek, mint ügyfél használati jogának felfüggesztése, újraérvényesítése, ügyfél hozzáférésének törlése stb.;
- a központi rendszer egyes komponenseiben bekövetkező, naplózást igénylő eseményeket/hibákat, mint adatbázis események, operációs rendszer események stb.

4.4.5.2. Naplóállomány védelme

A központi rendszer naplóállománya védett a jogosulatlan adatmódosítástól, azaz a naplóbejegyzések sorrendje és a bejegyzések adattartalma, beleértve a bejegyzéshez rendelt időt is, nem változtatható meg, a naplóállományból bejegyzés nem törölhető.

A naplóállományt a gondatlanságból vagy szándékosan elkövetett rongálás ellen biztonsági mentések védik. A MeH minden naplóállomány esetében, beleértve a személyes adatokat tartalmazó naplóbejegyzéseket is, gondoskodik az adatok bizalmas tárolásáról. A naplóállományhoz csak a biztonsági vezető által arra feljogosított személyzet férhet hozzá, szigorúan a hibaelhárításhoz szükséges mértékben. A MeH bűncselekmény gyanúja esetén, hatósági megkeresésre a szükséges adatokat, naplóbejegyzéseket a nyomozó hatóság rendelkezésére bocsátja.

A Kormány 224/2009. (X. 14.) Korm. rendelete a központi elektronikus szolgáltató rendszer igénybevevőinek azonosításáról és az azonosítási szolgáltatásról

A Kormány az elektronikus közszolgáltatások megbízható működése érdekében, az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény 31. § (2) bekezdés c) pontjában foglalt felhatalmazás alapján, az Alkotmány 35. § (1) bekezdés b) pontjában meghatározott feladatkörében a következőket rendeli el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

A rendelet hatálya

1. § (1) E rendelet hatálya kiterjed:

a) a központi elektronikus szolgáltató rendszer (a továbbiakban: központi rendszer) igénybevételével elérhető, azonosításhoz kötött elektronikus közszolgáltatásokra, az azok nyújtásában részt vevő szervezetekre és személyekre,

b) az elektronikus közszolgáltatásokat igénybevevő, illetőleg azok igénybevételéhez szakmai és informatikai támogatást biztosító szervezetekre és személyekre.

(2) E rendelet szabályait a központi rendszer által nyújtott, illetőleg azon keresztül igénybe vett azonosítási és viszontazonosítási szolgáltatásra kell alkalmazni.

(3) Azonosítás szolgáltatás jelleggel csak jogszabályi felhatalmazás alapján nyújtható. Nem vonatkozik e szabály az egy rendszeren belül igénybe vett, illetve az önkéntes hozzájárulás alapján létrehozott és használt azonosítási rendszerekre, adatbázisokra.

Értelmező rendelkezések

2. § E rendelet alkalmazásában:

a) *adatkezelésre feljogosított szervezet:* törvény vagy a szolgáltatás igénybevevője vagy a szolgáltatás alanya által az azonosításhoz szükséges adatok kezelésére feljogosított, a központi rendszerben elektronikus közszolgáltatást nyújtó, vagy a közszolgáltatás nyújtásában adatfeldolgozási megállapodás alapján közreműködő szervezet;

b) *működtető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, az elektronikus közszolgáltatás megvalósítását a központi elektronikus szolgáltató rendszeren lehetővé tevő, a közszolgáltatásokat összehangoló közigazgatási szerv;

c) *regisztrációs adatbázis adatkezelője:* az elektronikus közszolgáltatások működtetéséről szóló kormányrendeletben törvény felhatalmazása alapján a regisztrációs adatbázis kezelésére kijelölt közigazgatási szerv – a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala;

d) *regisztrációs szerv:* ügyfélkapu létesítésére, az azonosításhoz szükséges adatok közhiteles nyilvántartásokkal való egyezésének ellenőrzésére, és annak tanúsítására törvényben vagy kormányrendeletben feljogosított közigazgatási szerv;

e) *szervezet:* valamennyi jogi személyiséggel rendelkező és jogi személyiséggel nem rendelkező jogképes szervezet, valamint az egyéni vállalkozás;

f) *titkosító kulcspár:* a központi rendszerben közlekedő üzenetek védelmére felhasznált aszimmetrikus titkosítást alkalmazó eljáráshoz szükséges két kulcs együttes jelölése;

fa) *titkosító magánkulcs:* a titkosító kulcspár azon része, amely kizárólag a kulcs birtokosának rendelkezésére áll, amelynek segítségével képes a neki címzett üzeneteket titkosítani;

fb) *titkosító nyilvános kulcs:* a titkosító kulcspár a központi rendszer kulcstárában elhelyezett része, melynek segítségével a titkosító magánkulcs birtokosának küldött üzenetet titkosítani lehet. Ez a kulcs a titkosítás feloldására nem alkalmas;

g) *ügyfélkapu:* a központi rendszer természetes személyek részére nyújtott azonosítási szolgáltatásainak belépési, illetve szolgáltatási pontja, ahol a felhasználó közli a rendszerrel az azonosításához rendelkezésére álló információt, tulajdonságot, eszközt, illetve ahol az azonosítást igénylő megkapja a személy azonosságát alátámasztó információt;

h) *üzemeltető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, a központi rendszer elemeinek létrehozását, fejlesztését és üzemeltetését a működtető irányításával – szükség esetén más szervezetek bevonásával – közszolgáltatási szerződés keretében ellátó, a rendszer, mint egész működőképességét biztosító szervezet;

i) *viszontazonosítás:* ellenőrzési folyamat, melynek során a viszontazonosítást kérő elektronikus közszolgáltatást nyújtó szervezet – ideértve a közigazgatási hatósági eljárásról szóló törvény szerinti közreműködő hatóságot is – megküldi az általa jogszerűen kezelt természetes személyazonosító adatokat a központi rendszernek, amely tájékoztatja azoknak a regisztráció során felvett adatokkal való egyezőségéről, illetve az esetleges eltérés tényéről.

Az azonosítás közös szabályai

3. § (1) Az elektronikus kapcsolattartáshoz az eljáró természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező jogképes szervezet azonosságát közhiteles nyilvántartás adataival való egyezésre, illetve azt tanúsító biztonsági (személyazonosításra alkalmas) okmányban szereplő adatok ellenőrzésére kell visszavezetni.

(2) Amennyiben az azonosítás alapja közhiteles nyilvántartás, annak a központi rendszer számára elektronikusan folyamatosan rendelkezésre kell állnia, és folyamatosan a tényleges állapotnak megfelelően kell tanúsítania az azonosításhoz szükséges adatokat.

(3) Amennyiben az azonosítás biztonsági (személyazonosításra alkalmas) okmányra, hatósági bizonyítványra épül, úgy az ellenőrzést végzőnek az ilyen feladatot ellátóktól általában elvárható gondossággal meg kell győződnie az igazolvány, hatósági bizonyítvány hitelességéről és hatályosságáról, valamint az okmány és az adott személy kapcsolatáról.

(4) Nem feladata az azonosság ellenőrzését végzőnek – a nyilvánvaló ellentmondás esetét kivéve – a nyilvántartásban szereplő adat, illetve az igazolvány, bizonyítvány által tanúsított adatok valós voltának ellenőrzése.

(5) Nem alkalmas azonosításra, illetve regisztrációra olyan – egyébként érvényes, és hiteles, akár biztonsági – dokumentum, eszköz, tulajdonság, amely nem tartalmaz az egyértelmű azonosításhoz önmagában elégséges, az azonosítást végző számára hozzáférhető információt.

4. § (1) Természetes személyek azonosítására az ügyfélkapu, szervezetek azonosítására a hivatali kapu szolgál.

(2) A hivatali kapunak az igénybe vevő szervezet jellegétől függő, a szervezet létét közhitelesen tanúsító nyilvántartásra épülő megjelenési formái vannak

a) költségvetési intézmények számára a Magyar Államkincstár által vezetett költségvetési szervek nyilvántartására,

b) társas vállalkozások és egyéni cégek esetén a Cégbíróságok által vezetett cégnyilvántartásra,

c) egyéni vállalkozások esetén a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala által vezetett egyéni vállalkozói nyilvántartásra,

d) társadalmi szervezetek, alapítványok esetében az Országos Igazságszolgáltatási Tanács Hivatala által vezetett társadalmi szervezetek és alapítványok nyilvántartására,

e) nem költségvetési intézményként működő közoktatási intézmények esetében az Oktatási Hivatal által vezetett KIR nyilvántartásra,

f) nem költségvetési intézményként működő felsőoktatási intézmények esetében az Oktatási Hivatal által vezetett FIR nyilvántartásra

épülve.

II. FEJEZET
AZ ÜGYFÉLKAPU

A természetes személyek regisztrációja

5. § (1) A természetes személy a központi rendszer azonosítási szolgáltatásának igénybevételéhez szükséges regisztrációt az ügyfélkapu létesítésére feljogosított regisztrációs szerveknél személyesen, vagy a regisztrációs adatbázis adatkezelőjénél elektronikus űrlapon kezdeményezheti.

(2) A felhasználó személyes megjelenése esetén a regisztrációs szerv a személyes megjelenéskor vagy előzetesen az (1) bekezdésben említett elektronikus űrlapon megadott adatok és a felhasználó által bemutatott, a külön jogszabályban meghatározott személyazonosság igazolására alkalmas hatósági igazolványban szereplő adatok

alapján az ügyfelet azonosítja. A regisztrációs szerv a felhasználó által megadott a természetes személyazonosító adatokat és állampolgárságot összeveti a nyilvántartás adataival, valamint ellenőrzi a személyes megjelenés során bemutatott személyazonosításra alkalmas hatósági igazolvány hatályosságát.

(3) Amennyiben az ügyfélkaput létrehozni szándékozó olyan külföldi, aki nem alanya a személyi adat- és lakcímnyilvántartásnak, úgy az adatok összevetését el kell végezni a központi idegenrendészeti nyilvántartásban is.

(4) Amennyiben az ügyfélkaput létrehozni szándékozó a (3) bekezdés szerinti nyilvántartásban sem szerepel, úgy a regisztrációt az általa bemutatott útlevél, illetve a schengeni övezetbe tartozó EGT részes állam polgára esetén az adott állam által kibocsátott személyazonosításra alkalmas okmány alapján kell elvégezni. Ebben az esetben a bemutatott dokumentum ellenőrzéséhez az okmányminták nyilvántartását kell igénybe venni.

(5) A (2) és (3) bekezdésben meghatározott azonosítás és ellenőrzés sikere esetén a regisztrációt végző átemeli az igénylő természetes személyazonosító adatait a személyi adat- és lakcímnyilvántartásból, illetve a központi idegenrendészeti nyilvántartásból, és rögzíti az igénylő választott felhasználói nevét és elektronikus levelezési címét a regisztrációs adatbázisban. A (4) bekezdésében meghatározott esetben a regisztrációt végző személy – sikeres azonosítást követően – a természetes személyazonosító adatokat rögzíti a regisztrációs adatbázisban.

(6) A (2)–(4) bekezdésben meghatározott azonosítás és ellenőrzés sikertelensége esetén a regisztrációt végző az ügyfélkapu létrehozását megtagadja, és az esetleg már rögzített adatokat helyreállíthatatlanul törli.

6. § (1) Ha a felhasználó az ügyfélkapu létesítését elektronikus űrlapon kezdeményezi, és azt a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra vonatkozó kormányrendeletben meghatározott követelményeknek megfelelő elektronikus aláírással látja el, az ügyfélkapu létesítését megelőzően – az aláírás hitelesítés-szolgáltatójának rendelkezésre állásával összhangban – a központi rendszer haladéktalanul

a) ellenőrzi az elektronikus aláírás érvényességét,

b) szükség esetén a hitelesítés-szolgáltatónál viszontazonosítás útján ellenőrzi a felhasználó természetes személyazonosító adatait, továbbá

c) ellenőrzi az elektronikus űrlapon megadott adatok és az 5. § (2), illetőleg (3) bekezdés szerinti nyilvántartásban szereplő adatok egyezőségét.

(2) Az EGT más részes államának állampolgára, aki nem magyar hitelesítés-szolgáltatótól rendelkezik elektronikus aláírással az (1) bekezdés szerinti elektronikus űrlapot az EU tagállamai által kölcsönösen elfogadott bizalmi listán – melyet a kormányzati portál regisztrációs szekciójában folyamatosan közzétesz – szereplő elektronikus aláírással ellátva nyújthatja be. Álnévre kiállított tanúsítvány itt sem használható. Ez esetben az ellenőrzés kizárólag az aláírás érvényességére, és a tanúsítványban és az űrlapon megtalálható adatok egyezésére terjed ki.

(3) Ha az ellenőrzés sikeres volt, a központi rendszer elektronikus levélben tájékoztatja a felhasználót a regisztráció sikeréről. A regisztráció az elektronikus aláírás ellenőrzési ciklusának megfelelő késleltetéssel lép hatályba. Valós idejű tanúsítványszolgáltatás esetén a kapu az elektronikus válaszüzenet kézbesítését követően haladéktalanul igénybe vehető. Ha az ellenőrzés bármely eleme sikertelen, a regisztráció kérőt a központi rendszer tájékoztatja a regisztráció sikertelenségéről, és az adatokat visszaállíthatatlanul törli.

(4) A felhasználó az ügyfélkapu létesítését elektronikus űrlapon úgy is kezdeményezheti, hogy az nincs elektronikus aláírással ellátva (ideiglenes regisztráció). A központi rendszer az elektronikus űrlap benyújtását követően létrehozza az ügyfélkaput, de az elektronikus kapcsolattartásra csak korlátozottan használható. A kormányzati portál szolgáltatáslistája feltünteti, hogy mely szolgáltatások érhetők el ilyen ideiglenes regisztrációval. Az ideiglenes ügyfélkapuhoz nem tartozik tárhely.

(5) Ha a felhasználó az elektronikus aláírás nélküli elektronikus űrlap elküldésétől számított 30 napon belül nem jelenik meg személyesen egy regisztrációs szerv előtt az azonosítás végett, a központi rendszer az ügyfélkaput törli.

7. § (1) A választott felhasználói névnek egyedinek kell lennie, amely kizárólag a központi rendszer és az adott felhasználó közötti kapcsolatban kerül alkalmazásra. A központi rendszer az egyediséget ellenőrzi. A felhasználói név az ügyfélkapu működése folyamán csak az új ügyfélkapu létesítésének megfelelő eljárással változtatható meg.

(2) A megadott, az értesítésekhez felhasználható elektronikus levelezési címmel szemben követelmény, hogy több azonos nevű felhasználó nem használhat azonos elektronikus levélcímet. A rendszer ezt a regisztrációkor és a név vagy az elektronikus levelezési cím változásakor ellenőrzi, és amennyiben az adott elektronikus levélcímre már történt regisztráció, ezt jelzi.

(3) Azonos elektronikus levélcímre regisztráció csak a korábban regisztráló engedélyének bemutatásával történhet személyesen vagy az adatkezelőhöz küldött formanyomtatványon. Egy személy két vagy több ügyfélkapujához nem használhat azonos elektronikus levélcímet.

(4) A regisztrációs szerv felhívja az ügyfélaput létesítő figyelmét a felhasználói név és a jelszó különös gonddal történő megőrzésére, illetve tájékoztatja a felhasználói név, illetve a jelszó elvesztése, más általi megismerése esetén követendő eljárástól. Az erre vonatkozó tájékoztatást a kormányzati portálon is közzéteszi.

(5) A sikeres regisztrációt követően a regisztrációt végző az ügyfélkapu nyilvántartásban kezelt, rögzített adatokat a felhasználó kérésére kinyomtatja. A kinyomtatott másolatot a felhasználó és a regisztrációt végző aláírja, a regisztrációt végző lebélyegzi, és a felhasználónak átadja.

(6) A felhasználó az ügyfélkapu létrehozásakor megadott elektronikus levélcímének megváltozását a kormányzati portál az ügyfélkapu regisztrációs nyilvántartásában szereplő saját adatainak karbantartására szolgáló felületén vezeti át. A téves vagy nem létező elektronikus levelezési cím megadásából származó következmények elhárítása a felhasználó feladata.

(7) A regisztrált természetes személyazonosító adatokat a felhasználó a kormányzati portál az ügyfélkapu nyilvántartásban szereplő saját adatainak karbantartására szolgáló felületén kiadott utasítására a központi rendszer elektronikusan egyezteti a személyi adat és lakcímnyilvántartással. A változás átvezetése akkor történik meg, ha a nyilvántartásban szereplő történeti adatokkal történő egyeztetés alapján egyértelmű egyezés állapítható meg. Egyértelmű azonosíthatóság hiányában az átvezetést a regisztrációs szervnél a regisztráció általános szabályai szerint lehet kérni.

8. § (1) Amennyiben a regisztrációs adatbázis kezelőjéhez bejelentés érkezik, hogy hibásan megadott, illetve bármilyen okból hibássá vált elektronikus levelezési cím miatt nem az ügyfélkapu felhasználójához érkezik elektronikus levélben az értesítés, a regisztrációs adatbázis kezelője jogosult a hibás elektronikus levelezési címmel rendelkező ügyfélkapu működését felfüggeszteni. Ezt megelőzően a felfüggesztésről értesítést helyez el az érintett ügyfélkapu értesítési tárhelyén.

(2) Amennyiben az értesítést küldő elektronikus közszolgáltató, illetve a központi rendszer üzemeltetője érzékeli, hogy egy elektronikus levelezési cím tartósan, legalább 5 munkanapon keresztül elérhetetlenné, illetve a szolgáltató jelzése szerint nem létezővé vált, elektronikus űrlapon kéri a regisztrációs adatbázis adatkezelőjétől az ügyfélkapu felfüggesztését. A regisztrációs adatbázis adatkezelője erről haladéktalanul intézkedik.

(3) A felfüggesztés a hiba kijavításáig tart. A felfüggesztés nem érinti a korábban a tárhelyen elhelyezett dokumentumokhoz való hozzáférést, csak újabb küldemények nem érkezhetnek az értesítési tárhelyre, illetve nem lehet az ügyfélkapun át feladni sem.

(4) Amennyiben a hibás elektronikus levelezési cím felhasználója azonosítható, a központi rendszer regisztrációs adatbázisának adatkezelője adatot igényel a személyi adat- és lakcímnyilvántartásból, illetve a központi idegenrendészeti nyilvántartásból a lakcím megállapítása és a hibát okozó ügyfélkapu tulajdonosának értesítése érdekében, amit haladéktalanul postai úton megtesz.

(5) A felfüggesztett ügyfélkapu felhasználója a regisztrációs szervnél személyes megjelenéssel vagy írásban közölt új, a feltételeknek megfelelő, kizárólagos felügyelete alatt álló, vagy a 7. § (3) bekezdés szerinti feltételeknek megfelelő elektronikus levelezési címmel – és a hozzá szükséges dokumentumokkal – igényelheti a felfüggesztett ügyfélkapu teljes működésének visszaállítását.

(6) Amennyiben a hibát okozó felhasználó nem azonosítható vagy elérhető, a központi rendszer regisztrációs adatbázisának adatkezelője a kormányzati portál hirdetési felületén hirdetményben teszi közzé a felfüggesztést. A hirdetmény tartalmazza az ügyfélkapu birtokosának nevét és a hibát okozó elektronikus levelezési címet, valamint a hiba első észlelésének időpontját.

(7) A hirdetmény megjelentetésétől számított 1 év eredménytelen letelte után a központi rendszer regisztrációs adatbázisának adatkezelője a felfüggesztett ügyfélkaput, és egyidejűleg a hirdetményi felületről a hirdetményt törli.

9. § (1) Sikeres regisztrációt követően a regisztrációs rendszer a felhasználó részére az általa a regisztráció részeként megadott elektronikus levélcímére elektronikus levélben megküldi az ügyfélkapu megnyitásához szükséges egyszer használható aktiváló kódot. Az aktiváló kód a regisztrációtól számított 5 napig használható fel. Az aktiváló kód lejárata után az elfelejtett jelszóra vonatkozó eljárásrendben lehet új jelszót igényelni.

(2) Az aktiváló kód segítségével a kormányzati portál ügyfélkapu aktiválási felületén a felhasználó elvégzi az ügyfélkapu aktiválást, és ennek részeként lecseréli az aktiváló kódot a saját jelszavára.

(3) Amennyiben a regisztrációtól – ide nem értve az ideiglenes regisztrációt, amelynek lejárata 30 nap – számított 60 napon belül nem történik meg az ügyfélkapu aktiválása, a regisztrációs adatbázis adatkezelője törli a regisztrációt.

(4) A központi rendszerben használható jelszó legalább 8 karakter hosszú és egyaránt tartalmaz kis- és nagybetűket, valamint számokat. Egy jelszó legfeljebb két évig használható. A felhasználó a jelszó megadásakor rövidebb lejáratot is beállíthat. A központi rendszer működtetője legfeljebb 3 alkalommal, a jelszó lejárata előtt 1 hónappal, 1 héttel és 1 nappal elektronikus levélben és az értesítési tárhelyen elhelyezett üzenettel figyelmezteti a felhasználót a jelszócsere szükségességére.

(5) A jelszó lejáratát követően 60 napig az elfelejtett jelszó szabályai szerint lehet új jelszót igényelni, ezt követően a regisztrációs szervnél a regisztrációs adatok ellenőrzésével, az új ügyfélkapu nyitásának megfelelő eljárásrendben lehet a hozzáférést megújítani. Ennek eredményeként az ügyfél a korábbi felhasználói név mellé új egyszer használható aktiváló kódot kap, és ennek segítségével ismét hozzáférhet ügyfélkapujához és a tárhelyen tárolt adataihoz.

10. § (1) A felhasználó jogosult több ügyfélkaput létesíteni és fenntartani. Ezek közül – a (2) bekezdésben meghatározott kivétellel – azonban csak egy létesítése és fenntartása díjmentes. A további ügyfélkapu létesítéséért fizetett igazgatási szolgáltatási díj a regisztrációs szerv bevételét képezi.

(2) Amennyiben a felhasználó egy hivatali kapuval rendelkező, vagy azt létesíteni kívánó szervezet hivatali kapujának működtetéséhez, a hivatali kaput létesítő szervezet igazolásával, és az ennek megfelelő elektronikus levélcímmel igényel újabb ügyfélkaput, ez az ügyfélkapu is díjmentesen létesíthető.

(3) A második vagy további ügyfélkapu létesítéséhez kapcsolódó igazgatási szolgáltatási díj megfizetése a regisztrációs szervnél használható fizetési módokon történhet. A díjfizetés ellenében létrehozott ügyfélkapura vonatkozóan az egyszer használatos aktiváló kódot tartalmazó elektronikus levél megküldésére az igazgatási szolgáltatási díj, illetve az erre vonatkozó visszavonhatatlan fizetési ígéret beérkezését követően haladéktalanul sor kerül.

A regisztráció speciális esetei

11. § (1) Az ügyfélkapuval rendelkező törvényes képviselő – törvényes képviseleti jogosultságának fennállása időtartama alatt – jogosult a korlátozottan cselekvőképes és cselekvőképtelen személy ügyeiben a közigazgatási hatóságokkal való elektronikus kapcsolattartás, más ügyei a központi rendszeren keresztüli elektronikus úton történő intézése, illetve elektronikus közszolgáltatások igénybevétele érdekében az általa képviselt korlátozottan cselekvőképes, illetve cselekvőképtelen személy nevében, azaz az általa képviselt számára speciális ügyfélkapu nyitására, és az a feletti rendelkezésre.

(2) A kapu létesítésekor a regisztrációs szerv meggyőződik a törvényes képviseleti jogosultságról és a képviselt nevén kívül a cselekvőképességnek megfelelő (korlátozottan cselekvőképes – kcs, illetve cselekvőképtelen – csk.) rövidítést feltünteti az e célt szolgáló elkülönített nyilvántartásában.

(3) A törvényes képviselő által a képviselt nevében végrehajtott elektronikus ügyintézés jogosultsági kérdéseit az adott ügy intézésére vonatkozó szabályozás tartalmazza.

(4) Amennyiben egy személynek több törvényes képviselője van, és ügyfélkapuval rendelkezik, ugyanahhoz a speciális ügyfélkapuhoz valamennyi hozzáféréssel rendelkezhet. A speciális ügyfélkapuval az ügyintézés általános szabályainak megfelelően együttes képviselet, illetve a képviselttel együttes eljárás is megvalósítható elektronikusan.

(5) A korlátozottan cselekvőképes vagy cselekvőképtelen személy, illetve a nevében eljáró személyek számára egy speciális ügyfélkapu létesítése díjmentes.

(6) A speciális ügyfélkapu a képviselt és a képviselőként eljáró a 18. § (3) bekezdése szerinti azonosító adatait is továbbítja. A képviseleti jogosultság terjedelmére vonatkozó információt a speciális ügyfélkapu használóira vonatkozóan a központi rendszer nem tart nyilván, annak ellenőrzése az elektronikus közszolgáltatást nyújtó szervezet feladata.

(7) Korlátozottan cselekvőképes személy ügyfélkapu nyitására önállóan is jogosult az általános szabályok szerint.

(8) A korlátozottan cselekvőképes személy az általános szabályok szerint nyitott ügyfélkapuján keresztüli eljárási jogosultságának vizsgálata az elektronikus közszolgáltatást nyújtó szervezet feladata.

12. § (1) A törvényes képviselet tényének igazolására alkalmas elektronikus nyilvántartás működése esetén, amennyiben a nyilvántartás a képviseleti jogot, annak terjedelmét tartalmazza, e nyilvántartásra támaszkodva az ügyfélkapuval már rendelkező törvényes képviselő jogosult a speciális ügyfélkapu személyes megjelenés nélküli, elektronikus űrlappal történő létesítésére.

(2) Amennyiben a törvényes képviselő cselekvőképességét elveszíti, vagy meghal, illetve képviseleti jogosultságát a bíróság megszünteti, az erről való tudomásszerzéstől az új törvényes képviselő kijelöléséig, illetve képviseleti jogosultságának igazolásáig a korlátozottan cselekvőképes vagy cselekvőképtelen személy ügyfélkapujának működését a regisztrációs adatbázis adatkezelője – a 8. § (1) és (3) bekezdésének megfelelő eljárásrendben – felfüggeszti.

13. § A kezelőorvos által kiállított igazolás szerint személyes megjelenésében akadályozott felhasználó esetén a regisztrációs szerv a személyazonosságot a felhasználó lakóhelyén vagy tartózkodási helyén ellenőrzi.

14. § (1) A Magyar Köztársaság konzuli képviseletein a regisztrációs szerv előtt történt azonosítás szabályai szerint lehet ügyfélkapu nyitását kezdeményezni azzal az eltéréssel, hogy a kitöltött elektronikus űrlapot a konzuli tisztviselő kizárólag a bemutatott, személyazonosításra alkalmas hatósági igazolvánnyal veti össze és ellenőrzi a bemutatott dokumentum érvényességét. Ezután feldolgozásra és az ügyfélkapu létrehozására haladéktalanul megküldi a regisztrációs adatbázis adatkezelőjének, aki az adatokat összeveti a személyi adat- és lakcímnyilvántartással, illetve a központi idegenrendészeti nyilvántartással.

(2) Amennyiben az összevetés alapján az ügyfélkapu létrehozását kérő azonosítható, vagy megállapítható, hogy azért nem szerepel egyik nyilvántartásban sem, mert nem tartozik azok hatálya alá, úgy az ügyfélkapu létrehozásra kerül, és az egyszer használatos aktiváló kódot a megadott elektronikus levelezési címre 3 munkanapon belül elküldi a regisztrációs adatbázis adatkezelője.

15. § A regisztrációs adatbázis adatkezelője megállapodás alapján, költségei teljes megtérítése mellett jogosult munkahelyen vagy nyilvános eseményen kihelyezett ideiglenes regisztrációs szervet működtetni.

A felhasználói név és jelszó kezelése

16. § (1) A felhasználónak a felhasználói nevét és jelszavát védenie kell a jogosulatlan hozzáféréstől. Az azonosítók nem megfelelő biztonságú kezeléséből származó kockázatot a felhasználó viseli.

(2) Ha a felhasználó az ügyfélkapujához való hozzáférést biztosító jelszót elfelejti, vagy az jogosulatlan személy tudomására jut, a kormányzati portál elfelejtett jelszó funkciójával haladéktalanul új egyszer használatos aktiváló kódot igényel.

(3) A központi rendszer az új egyszer használatos aktiváló kódot – naponta legfeljebb három alkalommal – a felhasználó elektronikus levélcímére haladéktalanul megküldi.

(4) Ha a felhasználó az ügyfélkapuban használt felhasználói nevét elfelejti, azt a regisztrációs szerv előtti személyes megjelenéssel, személyazonossága igazolására alkalmas hatósági igazolvány bemutatásával, személyazonosítását követően a regisztrációs szerv szóban közli vele. Ezután a felhasználó az elfelejtett jelszóra vonatkozó eljárásrendnek megfelelően megújítja a jelszavát.

17. § (1) Ha a felhasználó ügyfélkapujához használt felhasználói neve jogosulatlan személy tudomására jut, a felhasználó a felhasználói név a regisztrációs szervnél történő lecserélésével állítja helyre ügyfélkapuja biztonságát.

(2) A felhasználó a felhasználói név nyilvánosságra kerülését vagy jogosulatlan személy általi megismerését bejelentheti a központi rendszer ügyfélszolgálatát ellátó ügyfélvonalon, a 189-es telefonszámon, ebben az esetben a bejelentő tájékoztatása után és hozzájárulásával a kommunikáció hangrögzítésre kerül. A biztonság sérülése bejelenthető ezen kívül személyesen – a személyazonosság igazolása mellett – a regisztrációs szervnél, valamint elektronikus űrlapon és -levélben, postai küldeményben is a regisztrációs adatbázis adatkezelőjénél a regisztrációnál megadott adatok közlésével.

(3) A (2) bekezdésben meghatározott esetben az ügyfélvonal kezelője vagy a regisztrációs szerv ügyintézője haladéktalanul a regisztrációs adatbázis adatkezelőjéhez továbbítja a kérést. A regisztrációs adatbázis adatkezelője az ügyfélkapuhoz való hozzáférést haladéktalanul megszünteti.

(4) A felhasználó az ügyfélkapuhoz való hozzáférés megszüntetését követően, a regisztrációs szervnél, kérésére – az 5. § (2) bekezdésében foglalt, sikeres ellenőrzést követően – az ügyfélkapujához való hozzáférés céljából új felhasználói nevet és új, egyszer használatos aktiváló kódot kap.

18. § (1) Ügyfélkapus azonosításhoz a felhasználó a kormányzati portál bejelentkező felületén adja meg a felhasználói nevét és a jelszavát. Helyes adatok esetén a központi rendszer a felhasználót azonosítja, az azonosítás eredménytelensége esetén hibajelzést ad.

(2) A központi rendszer 5 percen belüli ötszöri téves felhasználói név és jelszó adatpár megadása esetén a megadott felhasználói névhez tartozó ügyfélkapu hozzáférést 30 percnyi időtartamra zárolja, amiről a használót azonnal elektronikus levélben értesíti, illetve a központi rendszer üzemeltetőjének naplózott jelzést ad a felhasználó ismert adatainak rögzítésével. 30 perc eltelte után a zárolt ügyfélkapu a helyes adatpár megadásával újra megnyitható.

(3) A felhasználó azonosításához a központi rendszer a felhasználó nevét és elektronikus levelezési címét, egy az azonosítás biztonsági szintjét jelző adatot, valamint egy, a kapcsolat címzettjének megfelelően képzett egyedi ügyfél-azonosító kódot ad tovább az azonosítást igénylő, és arra jogszabályban feljogosított, vagy az üzemeltetővel kötött megállapodás alapján a szolgáltatást igénybevevő szervnek.

(4) Az adatkezelésre törvényben fel nem jogosított szolgáltatónak történő adattovábbítás előtt, megfelelő tájékoztatás mellett, minden esetben kérni kell a felhasználó hozzájárulását az azonosító adatok továbbításához. Az adatok továbbítására csak a felhasználó hozzájárulásával kerül sor. Ennek hiányában az azonosítás nem jön létre, a folyamat leáll, adatok nem kerülnek továbbításra.

(5) Egy adott szervezetnek (személynek) címzett dokumentum küldése esetében a (3) bekezdés szerinti adatok átadására vonatkozó felhasználói hozzájárulást megadottnak kell tekinteni.

Tájékoztatás az ügyfélkapu működéséről és adatkezeléséről

19. § (1) A kormányzati portálon részletes tájékoztatás érhető el az ügyfélkapu igénybevételének jogszabályban rögzített eljárásrendjéről. Emellett a kormányzati portál gyakorlati oktató, ismeretterjesztő anyagot is biztosít a bejelentkezés, a regisztráció, illetve a jelszókezelés folyamatairól. Ez a szolgáltatás ügyfélkapus bejelentkezés nélkül is igénybe vehető.

(2) A felhasználó az ügyfélkapun történt bejelentkezést követően a kormányzati portál, az ügyfélkapu regisztrációs nyilvántartásában rögzített személyes adatok karbantartására szolgáló felületén folyamatosan tájékozódhat a róla kezelt adatokról, illetve az elektronikus levelezési címét, jelszavát és a jelszó megadásakor annak lejárati idejét közvetlenül módosíthatja. A természetes személyazonosító adatok helyesbítésére a polgárok személyi adatainak és lakcímének nyilvántartását, illetve a központi idegenrendészeti nyilvántartást kezelő központi szervnél van lehetőség. A helyesbítés az okmányirodákban is kezdeményezhető.

(3) A felhasználó a regisztrációs adatbázis adatkezelőjénél igényelheti, hogy a rendszer legfeljebb egy évig naplózza az ügyfélkapu belépéseit. A kérés megújítható. A naplóban rögzítettekről kizárólag a felhasználó kaphat tájékoztatást kérelme alapján a tárhelyére.

A megszüntetés szabályai

20. § (1) Az ügyfélkapu megszűnik

a) a felhasználó kérelmére,

b) amennyiben az ügyfélkapu tárhelye üres, a felhasználó haláláról vagy elérhetetlenné válásáról való tudomásszerzést követően haladéktalanul,

c) amennyiben az ügyfélkapu tárhelye nem üres:

ca) a felhasználó haláláról való tudomásszerzést követő 4 hónap elteltével, amennyiben örökösök nem jelentkeztek, vagy nem kérték az eljárás a hagyatékra vonatkozó jogerős döntésig történő felfüggesztését,

cb) ha a felhasználó a rendelkezésre álló adatok alapján személyét illetően nem azonosítható, illetve ismeretlen helyen tartózkodik, ezen tény nyilvántartásba vételét követő 1 év leteltével.

(2) A felhasználó az ügyfélkapu megszüntetését a kormányzati portálról letölthető elektronikus űrlap kitöltésével kezdeményezheti. Az űrlap a kormányzati portál elektronikus űrlapok beküldésére szolgáló felületén, illetve a regisztrációs szervnél személyesen vagy írásban is benyújtható.

(3) Amennyiben az elektronikus tárhely üres, a regisztrációs adatbázis adatkezelője a (2) bekezdés szerint írásban kezdeményezett megszüntetést a kérelem beérkezésétől számított 3 munkanapon belül hajtja végre. A megszüntetendő ügyfélkapun keresztül küldött elektronikus bejelentés esetén a megszüntetést haladéktalanul végrehajtja. A megszüntetés megtörténtéről a felhasználót – a kérelem benyújtásának módjától függően elektronikus levélben vagy írásban – haladéktalanul értesíti a regisztrációs nyilvántartás adatkezelője. A megszüntetésre vonatkozó kérelmet a regisztrációs adatbázis adatkezelője 8 évig megőrzi.

(4) Amennyiben a tárhely nem üres, a regisztrációs adatbázis adatkezelője haladéktalanul figyelmeztető üzenetet küld a felhasználó tárhelyére és elektronikus levelezési címére, melyben 22 munkanapos határidővel kéri a tárhely kiürítését. E határidő leteltével megszünteti az ügyfélkaput és helyreállíthatatlanul törli az ott tárolt adatokat tekintet nélkül arra, hogy a tárhely kiürítésre került-e.

(5) A megszüntetett tárhelyen tárolt információt helyreállíthatatlan módon kell törölni.

21. § A központi rendszer az ügyfélkapuhoz tartozó elektronikus tárhely forgalmát – a dokumentumok átvételének nyomon követése érdekében – folyamatosan naplózza. Ha a napló alapján a regisztrációs adatbázis adatkezelője megállapítja, hogy a tárhelyen 1 éven át nem volt aktivitás, megkeresi a személyi adat- és lakcímnyilvántartást, és tisztázza, hogy az ügyfélkapu tulajdonosa életben van-e. Ezt a tevékenységét évente megismétli.

22. § (1) Amennyiben a személyi adat- és lakcímnyilvántartás közli, hogy az ügyfélkapu tulajdonosa elhunyt, és az ügyfélkapu tárhelye nem üres, a regisztrációs szerv a nyilvántartott elektronikus levélcímre hivatalos értesítést juttat el, hogy az ügyfélkapu megszüntetési eljárását megindítja, és felkéri az esetleges örökösöket, hogy intézkedjenek az ügyfélkapu tárhelyének kiürítésére.

(2) A vélelmezett örökös kérésére az ügyfélkapu működése, valamint a megszüntetési folyamat a hagyatéki eljárás befejezéséig felfüggeszthető. A felfüggesztés időszaka alatt a tárhely nem hozzáférhető.

(3) Az örökösödési eljárásban eljáró közjegyző számára írásbeli kérelmére olvasási jogú hozzáférés biztosítható a hagyatéki eljárásra kijelölő jegyzői döntés alapján.

(4) A hagyatéki eljárás lezárultát követően, az öröklést tanúsító dokumentum alapján, illetve az erre vonatkozóan kiadott közjegyzői végzés alapján a közjegyző végzésében megjelölt örökössel – személyazonosságának az 5. §-ban foglalt eljárásnak megfelelő igazolását követően – a regisztrációs szerv közli a felhasználói azonosítót és a 9. § (1) bekezdésében foglalt eljárás szerint egyszer használatos aktiváló kódot biztosít. Az örökös kérheti a kapcsolatot biztosító elektronikus levelezési cím cseréjét is.

(5) Az ügyfélkapu feletti rendelkezési joggal együtt az örökös hozzáfér az elhunyt titkosító kulcspárjának – amennyiben ilyen volt – a központi rendszer kulcstárában tárolt nyilvános részéhez. A magán kulccsal a központi rendszer nem rendelkezik.

(6) Az örökös számára az ügyfélkapu feletti rendelkezés lehetőségének átvételétől számítva a kiürítésre, megszüntetésre rendelkezésre álló idő 22 munkanap. Ezt követően az ügyfélkapu a 20. § (5) bekezdésének megfelelően megszűnik.

(7) Amennyiben az örökösök az értesítési tárhelyre megküldött értesítés elküldésétől számított 25 munkanapon belül nem jelentkeznek, a regisztrációs adatbázis adatkezelője a felhívást az utolsó nyilvántartott lakcímre postán megismétli, és hirdetményt tesz közzé a kormányzati portál hirdetményi felületén az elhunyt nevének és utolsó ismert lakcímének közlésével.

(8) Amennyiben a felhívás ebben az esetben is eredménytelen, úgy a hirdetmény közzétételétől számított 45 munkanap elteltével a regisztrációs adatbázis adatkezelője intézkedik az ügyfélkapu haladéktalan megszüntetéséről.

III. FEJEZET
A HIVATALI KAPU

A létesítés és használat közös szabályai

23. § (1) A hivatali kapu használója, azon keresztül valamely szervezet nevében tevékenységet végző kizárólag ügyfélkapuval már rendelkező (azonosított) természetes személy lehet.

(2) A hivatali kapu regisztrációja osztott. A központi rendszer kizárólag a hivatali kapu kezelésére az adott szervezetnél felhatalmazott képviselőt tartja nyilván, az adott szervezeten belüli további felhasználók – a szervezet nevében eljárni jogosult személyek – regisztrációját a szervezet által a hivatali kapu kezelésére felhatalmazott képviselő végzi. Ehhez a központi rendszer egységes eszközrendszert (programrendszert) és megfelelően védett tárhelyet biztosít.

(3) Hivatali kapu elektronikus, távolról történő létesítésére csak olyan szervezettípusnál kerülhet sor, amely tekintetében a szervezettípus egyedeinek teljes körű, folyamatosan elektronikusan hozzáférhető, közhiteles nyilvántartása rendelkezésre áll.

(4) Azoknál a szervezettípusoknál, amelyekre a (3) bekezdés nem teljesül, az elektronikus közszolgáltatást nyújtó, illetve nyújtani szándékozó szervezetek számára egyedi megállapodás alapján lehetőség van a költségvetési szervekre kialakított regisztrációs módszer alkalmazására.

(5) A hivatali kapu működőképességéhez szükséges, hogy a szervezet a titkosító kulcspárjának nyilvános részét a kormányzati portál kulcstárában közzétegye.

24. § (1) A hivatali kapu kezelésére felhatalmazott képviselő a részére biztosított regisztrációs felületen a szervezet képviseletére feljogosított személyek nevét és az ügyfélkapu regisztrációnál megadott elektronikus levelezési címét rögzíti az ügyfélkapujuk egyértelmű hozzárendelése érdekében. A regisztráció eredményeként átadja a hivatali kapuhoz tartozó azonosítót és jelszót, illetve – amennyiben ilyen van – azonosító eszközt.

(2) A hivatali kapu kezelésére felhatalmazott képviselő a szervezet nevében eljárni jogosult személyek jogosultságára vonatkozóan korlátozásokat, illetve jogosultságokat is rögzíthet. Korlátozható a jogosultság időben a kommunikációs irányára (fogadás vagy küldés) és a kapcsolat alanyára (szervezetre) vagy ezek kombinációjára vonatkozóan.

(3) A szervezet nevében történő eljárási jogosultság megszűnésekor a hivatali kapu kezelésére felhatalmazott képviselő törli a nyilvántartásból a korábban feljogosított személy azonosító adatait, illetve a hozzáférési jogosultságait. A hivatali kapu kezelésére felhatalmazott képviselő nyilvántartást vezet a szervezet képviseletében hivatali kapu igénybevételével eljárni jogosult személyekről a szervezet saját szervezeti és működési szabályzata szerint. A nyilvántartás alapján tanúsítható, hogy egy adott személy egy adott időszakban jogosult volt-e eljárni az adott szervezet nevében. Ez a dokumentum az adott szervezet által megőrzendő a szervezet iratkezelési szabályzatában a személyi anyagokra meghatározott időtartamig, de legalább 5 évig.

(4) A központi rendszer regisztrációs adatbázisának adatkezelője a hivatali kapu kezelésére felhatalmazott képviselőkről történeti nyilvántartást vezet, hogy tanúsítani lehessen, hogy adott időszakban ki volt feljogosítva a hivatali kapu kezelésére, illetőleg az adott szervezet képviselőinek nyilvántartására. Ez a nyilvántartás a köziratokra és levéltárakra vonatozó szabályok szerint maradandó értékű irat, amelyet – a helyi megőrzést követően – a Magyar Országos Levéltár őriz.

25. § (1) A hivatali kapuval rendelkező szervezetek teljes nevét, rövidített nevét és az elektronikus közszolgáltatás működéséről szóló kormányrendelet szerinti érkeztető számban használt azonosítóját a regisztrációs adatbázis adatkezelője napi frissítéssel a kormányzati portál ügyintézési szekciójában közzéteszi.

(2) A hivatali kapuból küldött dokumentumok, illetve a hivatali kapun keresztül igénybe vett szolgáltatás esetén a központi rendszer által a 18. § (3) bekezdése szerinti adatokon túlmenően az azonosítás érdekében a szervezet (1) bekezdés szerinti, az érkeztető számban használt azonosítója is átadásra kerül a címzett, illetve szolgáltatást nyújtó szervezetnek.

26. § (1) A hivatali kapuhoz csak értesítési tárhely tartozik. A szervezet köteles gondoskodni arról, hogy az értesítési tárhelyre érkezett üzenetek minden munkanapon átvételre kerüljenek.

(2) A hivatali kapuba érkezett üzenetek átvételükkel, de legkésőbb a 30. napon törlésre kerülnek, további tárolásukra az értesítési tárhelyen nincs lehetőség.

(3) Amennyiben a tárhelyen 3 munkanapnál régebben tárolt üzenet van, a munkanap kezdetén a központi rendszer üzenetet küld a hivatali kapu kezelésére feljogosított képviselő elektronikus levelezési címére.

27. § (1) A hivatali kapu megszűnik

a) ha a szervezet a hivatali kapu megszüntetését igényli,

b) ha a szervezet megszűnik.

(2) A hivatali kapu a szervezet, illetve a kapu megszűnésének bejelentésétől, illetőleg a megszűnésnek a központi rendszer tudomására jutásától nem fogad dokumentumokat, és a bejelentéstől, illetve tudomásra jutástól számított 30. napon megszűnik.

(3) Ha a szervezet nem rendelkezik a hivatali kapu kezelésére feljogosított személlyel (illetve a személy nem rendelkezik ügyfélkapuval), a kapu hozzáférése megszűnik, de a kapu változatlan feltételek mellett újra regisztrálható a szervezettípusra vonatkozó szabályok szerint.

Költségvetési szervek hivatali kapuja – Hivatalkapu

28. § (1) A költségvetési szervek hivatali kapu regisztrációját a Miniszterelnöki Hivatal, mint a központi rendszer működtetője végzi.

(2) A regisztráció a kormányzati portálról és a www.ekk.gov.hu honlapról elérhető űrlapon történik elektronikus vagy postai úton. Az űrlap adattartalmát és a regisztráció lépéseit az elektronikus közszolgáltatás működtetéséről szóló kormányrendelet határozza meg.

(3) A regisztráció eredményeként a szervezet hivatali kapujának kezelésére felhatalmazott képviselő a saját ügyfélkapuja értesítési tárhelyére megkapja a hivatali kapu azonosítóját, és jogosultságot kap a részére biztosított regisztrációs felület kezelésére. A költségvetési szervek hivatali kapujára egyebekben a 23–27. § rendelkezéseit kell alkalmazni.

(4) Költségvetési szerv és nonprofit szervezet számára a hivatali kapu létesítése és fenntartása díjmentes.

Vállalkozások hivatali kapuja – Cégkapu

29. § (1) A vállalkozások számára a hivatali kapu regisztrációját az okmányirodák és a polgárok személyi adatainak és lakcímének nyilvántartását kezelő központi szerv végzi.

(2) A regisztráció a kormányzati portálról letölthető elektronikus űrlappal elektronikusan, vagy ugyanennek a kinyomtatott változatával az (1) bekezdés szerinti regisztrációs szervnél személyesen történik.

(3) A cégkapu regisztrációja igazgatási szolgáltatási díj köteles, mely a regisztráló szerv bevételét képezi.

(4) A regisztrációt ügyfélkapuval rendelkező, a vállalkozás önálló képviseletére feljogosított természetes személy végezheti. Amennyiben ilyen nincs a szervezetben, úgy erre a tevékenységre esetileg kell meghatalmazni egy személyt.

30. § (1) Elektronikus regisztráció a hivatali kapu kezelésére felhatalmazott képviselő ügyfélkapuján keresztül végezhető el.

(2) Az elektronikus regisztráció esetén a központi rendszer ellenőrzi a személyi adat- és lakcímnyilvántartásban, hogy a képviseletre jogosultnak kijelölt személy a cégnyilvántartásban is rögzített – név, anyja születési neve – adatpárja csak egy személyt azonosít-e. Amennyiben a vizsgálat negatív eredménnyel zárul, a regisztráció csak személyes megjelenéssel a 29. § (1) bekezdés szerinti regisztrációs szervnél végezhető.

(3) Amennyiben a megadott adatok elégségesek az egyértelmű hozzárendeléshez, a központi rendszer a cégnyilvántartásban ellenőrzi, hogy a személy a cégnyilvántartás szerint jogosult-e önállóan a cég képviseletére.

(4) Amennyiben a (2) és (3) bekezdés szerinti feltételek együttesen teljesülnek, és az igazgatási szolgáltatási díj vagy az arra vonatkozó visszavonhatatlan fizetési ígéret megérkezett, a regisztrációt kérő ügyfélkapuja értesítési tárhelyére haladéktalanul megkapja a hivatali kapu azonosítóját és az egyszer használatos aktiváló kódot.

(5) A cégkapu aktiválását követően a vállalkozás képviseletében eljárni jogosultak adatainak kezelésére felhatalmazott képviselő elkészíti a vállalkozás titkosító kulcspárját, és annak nyilvános kulcsát a hivatali kapun keresztül feltölti a központi rendszer kulcstárába. Ezt követően jogosultságot kap a részére biztosított regisztrációs felület kezelésére. A titkosító kulcspár magánkulcsának biztonságos megőrzése a felhatalmazott képviselő feladata.

31. § (1) Együttes cégképviseleti jogosultság esetén a meghatalmazás alapján történő hivatali kapu nyitásra csak az azt igazoló dokumentumok bemutatásával, személyesen van lehetőség a 29. § (1) bekezdése szerinti regisztrációs szervnél.

(2) Amennyiben az elektronikus regisztráció a 30. § (2) bekezdésében rögzített feltétel teljesülésének hiányában sikertelen volt, a 29. § (1) bekezdése szerinti regisztrációs szervnél személyes megjelenéssel és a céghez való egyértelmű hozzárendelést bizonyító okiratok bemutatásával van lehetőség cégkapu nyitására.

(3) A regisztrációs eljárásra egyebekben a 23–27. §-ok rendelkezéseit kell alkalmazni.

IV. FEJEZET
AZ ELEKTRONIKUS MEGHATALMAZÁSOK KEZELÉSE

32. § (1) Egy ügyfélkapuval rendelkező természetes személy (a továbbiakban: megbízó) a központi rendszerben meghatalmazhat egy másik ügyfélkapuval rendelkező személyt vagy egy hivatali kapuval rendelkező szervezetet, hogy megbízásából elektronikusan eljárjon, amennyiben a megbízott útján való eljárást az adott eljárás szabályozása lehetővé teszi.

(2) Egy hivatali kapuval rendelkező szervezet (megbízó) a központi rendszerben meghatalmazhat egy ügyfélkapuval rendelkező személyt vagy egy hivatali kapuval rendelkező szervezetet, hogy megbízásából elektronikusan eljárjon, amennyiben a megbízott útján való eljárást az adott eljárás szabályozása lehetővé teszi.

33. § (1) A megbízó egy elektronikus űrlap kitöltésével igényel a központi rendszertől egy, a meghatalmazás tényét igazoló tanúsítványt, amelyhez meg kell adnia a felhatalmazás terjedelmét.

(2) A felhatalmazás lehet
- a) egyszeri vagy
- b) meghatározott számú eljárásra szóló,
- c) meghatározott időtartamra szóló.

(3) A felhatalmazásban meg lehet határozni azokat a szervezeteket, amelyeknél a meghatalmazott eljárásra jogosult vagy nem jogosult.

(4) Lehetőség van a (2) és (3) bekezdés szerinti elemek kombinációjára is.

(5) A (2) és (3) bekezdésekben meghatározott meghatalmazási módokat a központi rendszer elektronikusan értelmezhetően továbbítja.

(6) A meghatalmazás során biztosított a lehetőség szöveges korlátozás megadására is – szükség esetén a (2) és (3) bekezdésben felsoroltakkal kombinálva, azonban a szöveges korlátozást a központi rendszer csak a meghatalmazott által indított üzenet címzettjének továbbítja. A korlátozás értelmezése ebben az esetben az üzenetet feldolgozó ügyintéző feladata.

(7) Ha egy meghatalmazás a (2) bekezdés szerinti felhasználhatósága kimerült, a nyilvántartásból haladéktalanul törlésre kerül.

34. § (1) A megfelelően kitöltött meghatalmazást igénylő űrlapra válaszként a központi rendszer adatkezelője egy egyedi véletlen jelsorozatot küld a meghatalmazónak, amelyet a meghatalmazó természetes személyazonosító adataival együtt eltárol.

(2) A meghatalmazó akár a központi rendszeren keresztül, akár más úton átadja a jelsorozatot a meghatalmazottnak.

(3) A meghatalmazott elküldi saját ügyfélkapuján vagy hivatali kapuján keresztül az adott ügyirat mellékleteként a meghatalmazást igazoló jelsorozatot a címzett szervezetnek.

(4) A címzett szervezet – amennyiben szükséges a meghatalmazó személyének ellenőrzése, a jelsorozatot megküldi a központi rendszer adatkezelőjének, és válaszként megkapja a meghatalmazó természetes személyazonosító adatait. A válasz megküldése gépi kapcsolat esetén biztonságos csatornán keresztül, böngésző kapcsolat esetén a biztonságos elektronikus dokumentumtovábbító szolgáltatáson keresztül, védetten történik.

(5) A fel nem használt – el nem küldött és le nem kérdezett – meghatalmazási jelsorozat – amennyiben a meghatalmazó döntése alapján érvényességi ideje nem rövidebb – a kérésétől számított 61. napon a központi rendszerből törlésre kerül, érvényét veszti.

(6) A meghatalmazó a meghatalmazást az erre szolgáló elektronikus űrlap a regisztrációs adatbázis adatkezelőjének történő megküldésével és a meghatalmazási kérelemre kapott véletlen jelsorozat csatolásával bármikor azonnali hatállyal visszavonhatja.

V. FEJEZET
A FELHASZNÁLÓ SZEMÉLYAZONOSSÁGÁNAK ELLENŐRZÉSE A KÖZPONTI RENDSZERBEN NYILVÁNTARTOTT ADATOKKAL TÖRTÉNŐ VISZONTAZONOSÍTÁS ÚTJÁN

35. § (1) Ha az elektronikus közszolgáltatást nyújtó szervezet az általa nyújtott elektronikus szolgáltatás teljesítéséhez a vele az ügyfélkapu útján kapcsolatba lépő, s ily módon azonosított felhasználó adatainak ellenőrzésére jogosult, a viszontazonosítás alapjául szolgáló ellenőrző adattal rendelkező szervezet a központi rendszertől viszontazonosítást igényelhet.

(2) A központi rendszer összeveti a viszontazonosítást kérő által megküldött felhasználói természetes személyazonosító adatokat a felhasználó központi rendszerben tárolt természetes személyazonosító adataival, és azok egyezésének vagy eltérésének tényéről a viszontazonosítást kérőt tájékoztatja.

(3) A viszontazonosítás az ügyfélkapu szolgáltatása, melyet a viszontazonosítást kérő és a központi rendszer között csak védett adathálózati kapcsolaton keresztül lehet megvalósítani.

36. § (1) Azonosítást igénylő elektronikus közszolgáltatás nyújtásának és igénybevételének – jogszabály eltérő rendelkezése hiányában – nem feltétele a központi rendszer által azonosított ügyfél természetes személyazonosító adatainak előzetes ellenőrzése viszontazonosítás útján.

(2) A felhasználó személyazonosító adatainak viszontazonosítás útján történő előzetes ellenőrzése szükséges minden olyan esetben, ahol a már azonosított felhasználó saját személyes vagy különleges adatához, illetve adó-, bank-, biztosítási vagy értékpapírtitkához kíván hozzáférni. Idegen adathoz való hozzáférés esetén az adott eljárásra vonatkozó jogszabályban meghatározott eszközzel kell az elégséges biztonságot létrehozni.

(3) A dokumentum beérkezését követően a beküldő adatainak utólagos viszontazonosítását központi rendszer az elektronikus közszolgáltatást nyújtó szerv igénye alapján csak a biztonságos elektronikus dokumentumtovábbító szolgáltatás útján érkezett dokumentum esetén végezi, a dokumentum befogadásától számított 30 napon belül.

(4) Amennyiben a beküldő nyilvántartott adatai a dokumentum beérkezését követően megváltoztak vagy törlésre kerültek, a viszontazonosítás eredménytelen.

37. § (1) A viszontazonosítás keretében az elektronikus közszolgáltatást nyújtó szervezet megküldi a központi rendszernek

a) a rendelkezésére álló természetes személyazonosító adatokat,

b) a viszontazonosítást kérő számára a központi rendszer által előzetesen a felhasználóról képzett ügyfél-azonosító kódot,

c) a viszontazonosítási kérést azonosító adatot.

(2) A központi rendszer a 35. § (2) bekezdésben foglalt eljárás eredményeként haladéktalanul válaszként megküldi a viszontazonosítást kérő csatlakozott szervezetnek

a) az adatok egyezőségének vagy annak hiányának tényét, valamint

b) a viszontazonosítási kérést azonosító adatot.

(3) A viszontazonosítás akkor is elvégezhető, ha a viszontazonosítást kérőnél nem áll rendelkezésre valamennyi természetes személyazonosító adat, amennyiben a rendelkezésre álló adatokból a viszontazonosítás egyértelmű eredményre vezet.

VI. FEJEZET
ZÁRÓ RENDELKEZÉSEK

38. § (1) E rendelet – a (2)–(4) bekezdésben meghatározott kivételekkel – a kihirdetését követő 8. napon lép hatályba.

(2) A 6. § (2) bekezdése, a 14. § és a 29–31. § 2009. december 28-án lép hatályba.

(3) A 32–34. § 2010. szeptember 1-jén lép hatályba.

(4) A 4. § (2) bekezdés c)–f) pontjai és a 11–12. § külön jogszabály alapján lépnek hatályba.

Bajnai Gordon s. k.,
miniszterelnök

A Kormány 225/2009. (X. 14.) Korm. rendelete az elektronikus közszolgáltatásról és annak igénybevételéről

A Kormány az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény 31. § (2) bekezdés e)–g) és j) pontjaiban foglalt felhatalmazás alapján, az Alkotmány 35. § (1) bekezdés b) pontjában meghatározott feladatkörében eljárva a következőket rendeli el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

A rendelet hatálya

1. § (1) E rendelet hatálya kiterjed

a) az elektronikus közszolgáltatást nyújtó, valamint az elektronikus közszolgáltatáshoz szakmai és informatikai támogatást biztosító természetes és jogi személyekre, valamint jogi személyiség nélküli szervezetekre,

b) a központi elektronikus szolgáltató rendszer (a továbbiakban központi rendszer) útján nyújtott szolgáltatásokra,

c) az elektronikus közszolgáltatásokat igénybevevő szervezetekre és személyekre (a továbbiakban: felhasználó).

(2) E rendelet szabályait a központi rendszeren keresztül nyújtott, vagy igénybe vett elektronikus közszolgáltatásokra kell alkalmazni, függetlenül azok nyújtási és igénybevételi helyétől.

Értelmező rendelkezések

2. § E rendelet alkalmazásában:

a) *általános nyomtatványkitöltő:* a központi rendszer működtetője által biztosított olyan program, amellyel az általános nyomtatványtervezővel tervezett űrlap kitölthető és ellenőrizhető, és a fogadására jogosult csatlakozott szervezet számára a központi elektronikus szolgáltató rendszeren keresztül beküldhető, szükség esetén a kitöltött űrlap kinyomtatható;

b) *általános nyomtatványtervező:* olyan – a központi rendszer működtetője által az elektronikus közszolgáltatást nyújtó szervezetek számára biztosított – program, amellyel elkészíthető és később gondozható az űrlap, amely a fogadására jogosult szervezet számára az általános nyomtatványkitöltővel kitölthető és a központi elektronikus szolgáltató rendszeren keresztül is beküldhető;

c) *egyszer használatos jelszó:* az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (a továbbiakban: Ekszt.) közepes biztonsági fokozatú azonosításánál és szóbeli kapcsolattartásnál használatos olyan azonosítási eszköz, információ, amely csak egyetlen alkalommal, meghatározott időtartamon belül használható fel;

d) *működtető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, az elektronikus közszolgáltatás megvalósítását a központi elektronikus szolgáltató rendszeren lehetővé tevő, a közszolgáltatásokat összehangoló közigazgatási szerv;

e) *nem párbeszédre épülő (off line) elektronikus kapcsolat:* a felhasználó az előzetesen rendelkezésére álló, vagy külön üzenetben rendelkezésére bocsátott adatok felhasználásával hoz létre egy újabb elektronikus dokumentumot, és azt a központi rendszeren keresztül, megfelelő biztonsági és naplózási, illetve visszaigazolási feltételek biztosítása mellett – az üzenetváltást az adott feladat megoldásához szükséges számban ismételve – megküldi a vele kapcsolatban álló elektronikus közszolgáltatást nyújtó szervnek;

f) *párbeszédre épülő (on-line) elektronikus kapcsolat:* kapcsolattartási mód a felhasználó és az adatkezelő szerv között, melynek során a felhasználó az adatkezelő által kezelt adatokhoz (vagy azok e célt szolgáló másolatához) valós időben hozzáférve, azokat kiegészítve, pontosítva hozza létre az ügyintézés tárgyát, amely azonban további intézkedés nélkül nem minősül írásbeli közlésnek;

g) *szervezet:* jogi személyiséggel rendelkező és jogi személyiséggel nem rendelkező jogképes szervezet, valamint az egyéni vállalkozás;

h) *üzemeltető:* az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben kijelölt, a központi rendszer elemeinek létrehozását, fejlesztését és üzemeltetését a működtető irányításával – szükség esetén más szervezetek bevonásával – közszolgáltatási szerződés keretében ellátó, a rendszer, mint egész működőképességét biztosító szervezet.

Az elektronikus közszolgáltatással szembeni általános követelmények

3. § (1) A központi rendszer elektronikus közszolgáltatás nyújtásával biztosítja annak lehetőségét, hogy a közigazgatási és egyéb közfeladatot ellátó szervek, szervezetek, a természetes és jogi személyek valamint jogi személyiség nélküli szervezetek a hatósági és más ügyek intézése, tájékozódási joguk gyakorlása, tájékoztatási kötelezettségük teljesítése, valamint közhitelű nyilvántartások elérése, az ezekbe való betekintés és az ezekből történő adatigénylés, illetve adatszolgáltatás során elektronikus úton eljárhassanak.

(2) A központi rendszer alap és emelt szintű infrastrukturális, hálózati adatátviteli jellegű szolgáltatásai biztosítják az elektronikus közszolgáltatást nyújtók kapcsolattartását a felhasználókkal és egymással, a rendszer útján elérhetővé tett tartalomszolgáltatások elérhetőségét, az ügyek elektronikus úton történő intézésének műszaki lehetőségét, feltételrendszerét valamint a kapcsolattartás során az adatvédelmi és adatbiztonsági követelmények érvényesülését.

4. § (1) A központi rendszer szolgáltatásai magyar nyelven vehetők igénybe, kivéve, ha jogszabály meghatározott eljárásokban az idegennyelv-használat lehetőségének a biztosítását előírja vagy lehetővé teszi.

(2) A központi rendszer működtetője a rendszer működésével, szolgáltatásai igénybevételével kapcsolatosan a magyar nyelvűvel megegyező, illetve az idegen nyelvű felhasználó számára szükséges egyedi, idegen nyelvű információt tehet közzé.

(3) A nyújtott szolgáltatással kapcsolatos eljárási szabályokat, információs követelményeket a közlés nyelvén közzétett információnak megfelelően kell alkalmazni. Az esetlegesen eltérő információért a közzétevő viseli a felelősséget.

5. § (1) A központi rendszer által nyújtott szolgáltatások tekintetében biztosítani kell azok ügyfélbarát jellegét, egyszerű és közérthető használhatóságát, különös tekintettel a gyengébb informatikai felkészültséggel vagy technikai ellátottsággal rendelkezőkre, vakokra, gyengén látókra és színtévesztőkre.

(2) Az elektronikus közszolgáltatások akadálymentes használatát biztosítani kell. Az akadálymentes használat megvalósítására vonatkozó nemzetközi és hazai ajánlásokat a működtető a www.ekk.gov.hu honlapon teszi közzé.

(3) A közszolgáltatást nyújtó honlap működtetője köteles a honlap használatára vonatkozó elektronikus útmutatót, szükség esetén oktatási segédanyagot biztosítani, és a honlapon vagy külön, korlátozás nélkül elérhetően közzétenni.

(4) A központi rendszer által közvetlenül nyújtott elektronikus szolgáltatás naprakészségének és tartalmi pontosságának biztosítása a központi rendszer működtetőjének, a központi rendszeren keresztül elérhetővé tett, vagy szolgáltatásait felhasználó elektronikus szolgáltatás naprakészségének és tartalmi pontosságának biztosítása az elektronikus közszolgáltatást nyújtó szervezet feladata.

6. § (1) A felhasználó és az elektronikus közszolgáltatást nyújtó szervezet közötti írásbeli közlés céljára a központi rendszerben az általános nyomtatványkitöltővel kitölthető űrlap szolgál. A működtető egyetértésével az elektronikus közszolgáltatást nyújtó szervezet a kapcsolattartáshoz az általános nyomtatványkitöltőtől eltérő, a közlések összeállítását szolgáló megoldást biztosíthat.

(2) Ha külön jogszabály írja elő meghatározott tartalmú űrlap használatát, vagy a szervezet saját hatáskörében – a kapcsolattartás megkönnyítése érdekében – rendszeresít űrlapot, azt a kormányzati portálon keresztül is elérhetővé kell tenni.

(3) Törvény vagy kormányrendelet, illetve önkormányzati hatósági ügy esetében önkormányzati rendelet eltérő rendelkezése hiányában az űrlapot elektronikusan továbbíthatóvá, valamint számítógéppel, illetve kézzel kitölthetővé kell tenni.

(4) Ha a szervezet saját honlappal rendelkezik, a kormányzati portálon közzétett űrlappal megegyező elektronikus űrlapot saját honlapján is közzé teheti. A honlap működtetője ez esetben köteles arról gondoskodni, hogy az űrlap folyamatosan aktuális, és a kormányzati portálon közzétettel megegyező legyen. Az űrlap kormányzati portálon való elérhetőségére utaló tájékoztató jellegű információt a saját honlapon minden esetben el kell helyezni.

(5) Ha egy elektronikus közszolgáltatást nyújtó szervezet valamely eljárási cselekmény végzéséhez elektronikus űrlapot rendszeresít, annak tartalmaznia kell az arra vonatkozó kérdéseket, hogy kéri-e a felhasználó

a) az eljárás további szakaszában a papír alapon történő kapcsolattartást;

b) az űrlap elküldésével egyidejűleg annak egy példányának a saját értesítési tárhelyén – amennyiben saját titkosító kulcsát a kulcstárban elhelyezte –, saját titkosító kulccsal titkosítva és időbélyegzéssel ellátva történő elhelyezését;

c) a döntésnek nem minősülő dokumentumok, iratok az értesítési tárhelyére történő megküldését, vagy elegendő számára a 34. § (1) bekezdés c) pontja szerinti értesítés.

(6) Ha az elektronikus közszolgáltatást nyújtó szervezet egy űrlapot papír alapon is hozzáférhetővé, kitölthetővé tesz, ebben az esetben is biztosítani kell az aktualizálást és egyezést a kormányzati portálon közzétett példánnyal. A kormányzati portálon közzétett űrlaptól eltérő, a szervezetnél fellelhető példányokat be kell vonni és meg kell semmisíteni. A papír alapú űrlap minden változatából egy-egy példányt a szervezet irattári szabályzatában foglaltak szerint meg kell őrizni.

(7) A kormányzati portálon a bejelentések, közlések és válaszok értelmezéséhez, az archív jelleget jelezve – az e rendelet hatálybalépését követően használt valamennyi űrlapot hozzáférhetővé kell tenni, és azt a használatban lévő űrlapoktól el kell különíteni. Jelezni kell, hogy az adott űrlap mikortól meddig volt használatban. Az archív űrlapokat a kormányzati portálról a használatuk megszűnését követő 8 év eltelte után szabad eltávolítani.

(8) Az általános nyomtatványkitöltő valamennyi az (1) bekezdésben megjelölt követelménynek megfelelő, e rendelet hatálybalépése után elfogadott elektronikus űrlapot kezeli.

II. FEJEZET
AZ ELEKTRONIKUS KÖZSZOLGÁLTATÁS ÉS ANNAK IGÉNYBEVÉTELE

A kormányzati portál

7. § (1) A kormányzati portál a közszolgálat – ideértve a közigazgatást, a közszolgáltatásokat és az elektronikus közszolgáltatást önként nyújtó szervezeteket is – központi elektronikus tájékoztatási és szolgáltatási felülete, amely az interneten a www.magyarorszag.hu címen érhető el. A kormányzati portál biztosítja, hogy felületéről valamennyi nyilvános elektronikus közszolgáltatás elérhető legyen.

(2) A kormányzati portál állandó szolgáltatásai:

a) a központi, területi és helyi közigazgatási szervek, közszolgáltatók, valamint a központi rendszerhez csatlakozott további szervezetek elérhetőségi adatai [postai és elektronikus cím(ek), telefonszámok (központ és ügyfélszolgálat), ügyfélfogadási idő];

b) ügyleírások, letölthető űrlapok, minták;

c) az elektronikus közszolgáltatások katalógusa, amely tartalmazza a szolgáltatást nyújtó szervek megnevezését, és elektronikus elérhetőségét;

d) személyes ügyintézési felület kialakításának lehetősége;

e) biztonságos elektronikus dokumentumtovábbító szolgáltatás (a továbbiakban BEDSZ) indítási és fogadási pontja;

f) személyes azonosítással igénybe vehető fórum;

g) bejelentések, közlések felülete, mely a jogszabály alapján itt közzétett hatósági hirdetmények megjelenítését szolgálja;

h) hatályos jogszabályok elektronikus gyűjteménye és a Magyar Közlöny hiteles elektronikus közzétételi felülete;

i) pályázatok közzététele;

j) a helyi ügyekbe bekapcsolódni kívánó civil szervezetek mutatója, bejelentkezési helye;

k) jogszabálytervezetek véleményezésének elérhetőségi mutatói;

l) értesítési tárhely, tartós tár;

m) kulcstár.

(3) Az (2) bekezdés szerinti szolgáltatásokra, azok igénybevételére vonatkozó általános tájékoztatást, az alapvető ügyintézéshez szükséges tájékoztatókat a kormányzati portálon a magyar mellett legalább angol nyelven is hozzáférhetővé kell tenni.

(4) A (2) bekezdés a)–c), g), i) és k) pontjaiban meghatározott információk naprakészségének és pontosságának biztosítása a hatáskörrel rendelkező közigazgatási vagy közszolgáltató intézmény feladata. A közzétett információ helyi sajátosságokkal történő kiegészítése a területileg illetékes államigazgatási szerv vagy önkormányzati hatóság feladata.

(5) A központi rendszer működtetőjének feladata a (2) bekezdés d), e), h) l) és m) pontjaiban rögzített szolgáltatások naprakészségének és pontosságának biztosítása. A működtető feladata, hogy a b) pontban meghatározott szolgáltatás azon részének naprakészségét és pontosságát biztosítsa, amelynek gondozása nem tartozik egyetlen csatlakozott, illetve a 8. § (4) bekezdése szerinti feladatot ellátó szervezet hatáskörébe sem.

(6) A központi rendszer üzemeltetője felel az f) pontban meghatározott szolgáltatásért és – az érintett szervektől kapott tájékoztatás alapján – a (3) bekezdés szerinti idegen nyelvű tájékoztató frissítéséért.

Az információk naprakészségének biztosítása

8. § (1) A központi költségvetési szerv feladata, hogy az adatváltozásokat a lehetőség szerint a változást megelőzően, de legkésőbb változástól számított 2 munkanapon belül átadja a kormányzati portál üzemeltetőjének, aki az adatváltozást 1 munkanapon belül átvezeti a kormányzati portálon.

(2) Ha a működtető vagy az üzemeltető észleli, vagy egyéb módon tudomására jut, hogy a kormányzati portálon közölt adat vagy információ elavult, téves, hiányos vagy más okból elégtelen, a működtető haladéktalanul felhívja az érintett szervezetet annak helyesbítésére, kiegészítésére. Amennyiben a helyesbítésre a felhívás megérkezésétől számított 2 munkanapon belül nem kerül sor, a központi rendszer működtetőjének döntése alapján az üzemeltető a kormányzati portálon jelzi az adat vagy információ elavult, téves, elégtelen voltát és közli, mely szerv feladata az adatok naprakészségének biztosítása.

(3) A központi rendszerhez csatlakozott, de a kormány irányítása alá nem tartozó szervekre vonatkozó információk naprakészségének és pontosságának biztosítása az érintett szervezettel kötött megállapodásban foglaltak alapján történik.

(4) A kormány irányítása alá nem tartozó s a központi rendszerhez sem csatlakozott szervezetek esetében a feladatkör szerint érintett központi közigazgatási szerv gondoskodik az ágazatot érintő információk naprakészségéről és helyességéről.

(5) A központi rendszerhez csatlakozott közüzemi vagy egyetemes szolgáltató (a továbbiakban együtt közüzemi szolgáltató) a kormányzati portál útján közzé tett, a fogyasztók tájékoztatására szolgáló információk tartalmi megfelelőségét, naprakészségét az 5. § (4) bekezdésében foglalt feladatmegosztás szerint, illetve a rá irányadó jogszabályok szerint biztosítja.

A kormányzati portál igénybevételével nyújtott szolgáltatások feltételei

9. § (1) Ha az elektronikus közszolgáltatást nyújtó szervezet párbeszédre épülő szolgáltatást kíván a kormányzati portálról elérhetővé tenni, legalább a következő feltételeket biztosítania kell:

a) az általa nyújtott elektronikus közszolgáltatás folyamatos, a 25. § (4) bekezdésben foglaltak figyelembevételével, havi szinten legalább 99,5%-os elérhetőségét;

b) az alkalmazásfelügyelet és egyéb infokommunikációs támogatás folyamatos készenlétét;

c) az elektronikus szolgáltatáshoz kapcsolódó naprakész elektronikus dokumentációt és tájékoztató segédanyagot;

d) a központi ügyfélszolgálattal való együttműködést.

(2) Ha az elektronikus közszolgáltatást nyújtó szervezet nem párbeszédre épülő szolgáltatást kíván a kormányzati portál útján nyújtani, az (1) bekezdés c) és d) pontjaiban meghatározottakon túlmenően legalább a következő feltételeket kell biztosítania:

a) az általa nyújtott elektronikus közszolgáltatás a jogszabályokban meghatározott ügyintézési határidőn belüli ügyintézést biztosító üzemeltetését;

b) az ügyintézést kiszolgáló rendszer üzemidőben fellépő hibáinak kezelését;

c) a központi rendszeren keresztül érkezett üzenetek minden munkanapon elvégzett átvételét.

Panaszok, bejelentések kezelése

10. § (1) A központi rendszer, különösen a kormányzati portál, az ügyfélkapu és a központi ügyfélszolgálat működésével, működtetésével kapcsolatos panaszokat, kérdéseket, a felhasználók az erre szolgáló elektronikus űrlapon vagy elektronikus levélben a 189@ugyfelvonal.hu címre, illetve a központi ügyfélszolgálat 189-es kék telefonszámán szóban jelenthetik be. Személyes bejelentést munkaidőben az ügyfélközpont fogad.

(2) Az (1) bekezdés szerinti panaszokra és kérdésekre a működtető 15 munkanapon belül a kormányzati portál fórumán válaszol.

(3) Amennyiben a panasz, közérdekű bejelentés vagy kérelem nem a központi rendszer működtetésével kapcsolatos, a működtető azt 1 munkanapon belül a feladat és hatáskörrel rendelkező szervnek továbbítja és erről a bejelentőt a kormányzati portál fórumán keresztül tájékoztatja.

(4) Ha a bejelentés a közérdekű kérelmekkel, panaszokkal és bejelentésekkel kapcsolatos, az európai uniós csatlakozással összefüggő egyes törvénymódosításokról, törvényi rendelkezések hatályon kívül helyezéséről, valamint egyes törvényi rendelkezések megállapításáról szóló 2004. évi XXIX. törvény 142. §-a szerint nem igényel választ, ezt a tényt

közvetlenül a bejelentéshez kapcsoltan rögzíti a működtető a megfelelő jogszabályi hivatkozással, és a bejelentést az irattári szabályok szerint kezeli a továbbiakban.

Hirdetmények közzététele

11. § (1) A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvényben előírt esetekben a hirdetményt a kormányzati portál a 7. § (2) bekezdés g) pontja szerinti hatósági hirdetmények egységes megjelenítését szolgáló felületén kell közzé tenni.

(2) Az (1) bekezdés szerinti felületen külön kereső működik, amely lehetővé teszi a hozzáférhető hirdetmények között kategória, időszak, forrásintézmény, tárgy, eljáró hatóság, kérelmező, ügyiratszám, település, ügyintéző alapon és bármely jelsorozatra történő keresést.

(3) Az (1) bekezdésben meghatározott célra szolgáló elektronikus űrlap a kormányzati portálról letölthető. A hirdetménynek a kormányzati portál üzemeltetőjéhez határidőben történő megküldéséről a hirdetményi közlésért felelős szerv a hivatali kapuján keresztül gondoskodik.

(4) A hirdetmény a beküldött elektronikus űrlapon közölt szöveggel a hirdetmenyek.magyarorszag.hu felületen jelenik meg, azt a működtető vagy üzemeltető nem módosíthatja, a tartalomért a hirdetmény beküldője felel.

(5) Ha az eredeti űrlapot kijavításra, vagy kiegészítésre vonatkozó jelzéssel ismét megküldik, a hirdetményt módosított tartalommal kell megjeleníteni. Ez esetben – ha jogszabály eltérően nem rendelkezik – a hirdetményt közzétevő döntése alapján lehetőség van a módosított tartalomnak az eredeti határidővel vagy annak megküldését követően az új közzétételi dátumtól számított határidővel történő megjelentetésére és határidő-számításra.

A központi ügyfélszolgálat

12. § (1) A működtető szervezet az elektronikus tájékoztatás és ügyintézés elősegítésére központi ügyfélszolgálatot, ügyfélvonalat, ügyféltájékoztató központot tart fenn.

(2) A felhasználók számára folyamatosan, napi 24 órán át az ügyfélvonal által biztosított elektronikus tájékoztató szolgáltatás a 189-es hívószámon áll rendelkezésre, amely az országon belül helyi díjazású tarifával hívható. Az elektronikus tájékoztató szolgáltatás

a) telefonon,
b) rövid szöveges üzenet útján (a továbbiakban: SMS),
c) telefaxon,
d) elektronikus levélben,
e) internet-telefonon (VoIP)

érhető el.

(3) Az ügyfélvonal alaptevékenysége keretében nyújtott szolgáltatások:

a) a közigazgatási és elektronikus közszolgáltatást nyújtó szervek elérési adatai, feladat- és hatásköre, illetékességi területe, az általuk intézett ügytípusok intézésének folyamata;
b) tájékoztatás az egyes ügyekre vonatkozó jogszabályokról és azok tartalmáról;
c) egyedi ügyben a segítséget igénylő hívásának illetékes szervhez történő átirányítása;
d) előzetes időpontfoglalás az ügyfélfogadást biztosító elektronikus közszolgáltatást nyújtó szerveknél;
e) állampolgári panaszok, bejelentések fogadása és az illetékes elektronikus közszolgáltatást nyújtó, illetve elektronikus közszolgáltatás nyújtására jogszabály által kötelezett szervhez történő továbbítása;
f) technikai segítségnyújtás az elektronikus ügyintézés kérdéseiben;
g) az elektronikus ügyintézéssel kapcsolatos technikai hibabejelentések fogadása, informatikai ügyfélszolgálat tevékenységének biztosítása, továbbá a hibajelzés és informatikai kérdés illetékes csatlakozott szervezet technikai ügyeletéhez történő továbbítása;
h) törvény felhatalmazása esetén a kérelem, adatszolgáltatás telefonon történő benyújtása, fogadása, hatáskörrel és illetékességgel rendelkező közigazgatási szervhez vagy közszolgáltatóhoz való továbbításához szükséges cselekmények elvégzése, és a kérelem vagy adatszolgáltatás továbbítása;
i) közreműködés egy konkrét ügy intézésére vonatkozó tájékozódás biztosításában;
j) tájékoztatás időszakosan előforduló, az állampolgárok jelentős csoportjait érintő kérdésekben.

(4) A (3) bekezdés h)–i) pontjai szerinti szolgáltatások csak a felhasználó külön jogszabály szerinti azonosítását követően vehetők igénybe.

(5) Az ügyfélvonal szolgáltatásait elsősorban a 7. §, a 9. § (1) bekezdés és a 10. és 11. §-ban meghatározott, az elektronikus közszolgáltatást nyújtó szervezetek által rendelkezésre bocsátott információk felhasználásával, valamint az elektronikusan elérhető nyilvános adatok és saját információbázisa alapján biztosítja.

Személyes adatok kezelésének módja

13. § (1) Telefonos szolgáltatás igénybevételével nyújtott ügyfél-tájékoztatás esetén a felhasználó neve és elérhetőségei (elektronikus levélcím, telefonszám, központi rendszer cím) csak akkor kérhető, ha

a) a felhasználó bejelentést tesz,

b) visszahívást kér,

c) elektronikus irat vagy űrlap küldését kéri.

(2) Az (1) bekezdésben foglalt esetben a telefonos szolgáltatás igénybevétele során fel kell hívni a felhasználó figyelmét, hogy ügye intézése nevének és elérhetőségének rögzítését és tárolását teszi szükségessé.

(3) Az (1) bekezdésben foglalt adatok abban az esetben kezelhetők – rögzíthetők, tárolhatók és kizárólag az ügy intézése érdekében továbbíthatók kizárólag az ügy intézésére jogosult szervnek –, ha azt a felhasználó a telefonos szolgáltatás igénybevétele során – kifejezetten és a hangrögzítésre irányuló, szóban közölt engedélyét követően – hangfelvételen rögzítve engedélyezte.

(4) A felhasználó (1) bekezdésben foglalt adatait a szolgáltatás teljesítésének visszaigazolását követően haladéktalanul, de legkésőbb 3 munkanapon belül törölni kell.

(5) Ha a (1) bekezdés szerinti esetben a felhasználó a telefonos szolgáltatás során – szóbeli közlése szerint – nem kíván hozzájárulni az ügye intézéséhez szükséges adatok kezeléséhez, a telefonos szolgáltatás során hangrögzítésre nem kerül sor. Ebben az esetben azonban – adatkezelési hozzájárulás hiányában – a felhasználó személyes elérhetőségét, illetve azonosítását igénylő szolgáltatások nem válnak a felhasználó számára elérhetővé.

(6) A központi rendszer szolgáltatásainak igénybevételéről keletkezett adatok személyazonosításra alkalmatlan módon statisztikai célra felhasználhatók.

Tájékoztatáskérés az ügyfélvonal útján

14. § (1) Telefonon keresztül történő információkérés esetén az ügyfélvonal először az automatikus hívásfogadó rendszerben kínál fel a felhasználó számára választási lehetőséget előzetesen rögzített szöveg meghallgatásra vagy az ügyfélvonal kezelőjétől kapott szóbeli tájékoztatásra. Ha a kért információ nem áll közvetlenül rendelkezésre, a kezelő az ügyfélvonal saját szakértőjétől kér támogatást átkapcsolással, vagy – amennyiben a hatáskörrel rendelkező szerv ügyfélszolgálata, vagy ügyfélszolgálatra kijelölt munkatársa elérhető – átkapcsol hozzá.

(2) Amennyiben az ügy bonyolultsága indokolja, az ügyfélvonal kezelője – szükség esetén szakértő bevonásával – legfeljebb 2 órán belül ad választ visszahívás, illetve elektronikus levél útján.

(3) Elektronikus levélben vagy SMS formájában történő információkérés esetén az ügyfélvonal a kérdés beérkezését – a kérdésnek megfelelő formában – haladéktalanul visszaigazolja, majd legfeljebb 2 órán belül ad tájékoztatást – a felhasználó igénye és a válasz méretétől függően – rövid szöveges üzenet formájában, vagy – amennyiben a felhasználó a válaszcímet megadta – elektronikus levélben.

(4) Ha a (2) és (3) bekezdés szerinti kérdésre a részletes válasz hosszabb időt igényel, a kezelő erről tájékoztatja a felhasználót a várható válaszadási határidő megadásával, ami nem lehet hosszabb, mint a kérdést követő első munkanap.

(5) A feladat- és hatáskörrel rendelkező szerv a lehető legrövidebb kapcsolási, illetve válaszadási idő mellett biztosítja az ügyfélvonal által hozzá átirányított hívásokra történő pontos válaszadást. A kezelő az információszolgáltatásban érintett szerv adatszolgáltatása alapján jár el, ad tájékoztatást, és erről tájékoztatja a felhasználót.

(6) Az elektronikus közszolgáltatást nyújtó szervezetek ügyfélszolgálati feladatot ellátó szervezeti egységei az ügyfélvonallal való együttműködésük keretében folyamatosan biztosítják az ügyfélvonal munkájához szükséges, nyilvános, közérdekű, naprakész, az elektronikus közszolgáltatást nyújtó szerv szervezetére, tevékenységére, működésére és gazdálkodására vonatkozó általános információkat. Ezekre az adatokra irányuló igény esetén a válaszadást lehető legrövidebb idő alatt – lehetőség szerint 1 munkanapon belül –, legfeljebb azonban 15 munkanapon belül kell teljesíteni.

15. § (1) Az ügyfélvonal a felhasználó igénye alapján – az érintett közigazgatási szerv ügyfélfogadási rendjére, az ügyfélszolgálaton intézhető ügyfajtákra figyelemmel – a közigazgatási szervvel egyeztetve a felhasználó számára ügyeik intézéséhez 10 munkanapon belüli időpontra ügyfélfogadási időpontot foglalhat. A lefoglalt időpontban a közigazgatási szerv a felhasználót köteles fogadni. Az időpontfoglalásról a felhasználót az ügyfélvonal kezelője értesíti.

(2) Az időpontfoglalás lehetőségét a közigazgatási szerveken túlmenően valamennyi, a központi rendszeren keresztül elektronikus közszolgáltatást nyújtó szolgáltatónak a rá vonatkozó jogszabály szerinti határidőn belül biztosítania kell.

(3) Amennyiben egy elektronikus közszolgáltatást nyújtó vagy nyújtására kötelezett szervezet nem biztosítja a jogszabályi határidőn belül az ügyfélfogadás lehetőségét, a központi rendszer működtetője megkeresi az ügyben az érintett szervezetet felügyelő szervet.

Panaszok, bejelentések

16. § (1) Az ügyfélvonal a hozzá beérkezett, a közigazgatási szerv, illetve közüzemi szolgáltató működésével kapcsolatos panaszt a beérkezéstől számított 1 munkanapon belül az illetékes közigazgatási szervhez, illetve közüzemi szolgáltatóhoz továbbítja.

(2) Az ügyfélvonal által az illetékes közigazgatási szervhez, illetve közüzemi szolgáltatóhoz továbbított kérdés, panasz vagy bejelentés esetén az illetékes szerv közvetlenül intézkedik vagy válaszol a felhasználónak, melynek tényéről az ügyfélvonalat egyidejűleg tájékoztatja.

(3) Ha a továbbított panasz megválaszolására vonatkozóan 15 munkanapon belül nem érkezik visszajelzés, az ügyfélvonal kérdést intéz a közigazgatási szervhez, illetve a közüzemi szolgáltatóhoz az adott panasz elintézésének helyzetéről. Ha az első megkereséstől számított 22 munkanap elteltével nem érkezik meg a panaszra adott válasz vagy annak jelzése, hogy a panasz elbírálása előreláthatólag tovább tart, az ügyfélvonal tájékoztatja a panaszost a válasz hiányáról.

(4) Amennyiben a panaszos hozzájárul panasza továbbításához, az ügyfélvonal továbbítja a panaszt az illetékes közigazgatási szerv felettes szervéhez, illetve közüzemi szolgáltató felett a szakmai felügyeletet gyakorló közigazgatási szervhez, és ennek tényéről a felhasználót tájékoztatja.

(5) Ha a bejelentés, panasz a közérdekű kérelmekkel, panaszokkal és bejelentésekkel kapcsolatos, az európai uniós csatlakozással összefüggő egyes törvénymódosításokról, törvényi rendelkezések hatályon kívül helyezéséről, valamint egyes törvényi rendelkezések megállapításáról szóló 2004. évi XXIX. törvény 142. §-a szerint nem igényel választ, ezt a tényt a kezelő a bejelentés témájával és időpontjával együtt személyazonosító adatok nélkül rögzíti, és a naplót a működtető 6 hónapig tárolja.

Eljárási cselekmény telefonos intézése

17. § (1) Ha törvény közigazgatási eljárásban lehetővé teszi kérelem benyújtásának, adatközlésnek vagy más eljárási cselekménynek a telefonon történő elvégzését, erre a 13. § (3) bekezdésében meghatározott adatok rögzítésén túlmenően csak abban az esetben kerülhet sor, ha a felhasználó rendelkezik a központi rendszerben kezelt egyszer használatos jelszóval, azt a kezelőnek megadja, és a kezelő sikeres azonosítást végez.

(2) Ha elektronikus közszolgáltatást nyújtó nem közigazgatási szervezet és az ügyfélvonal megállapodása lehetővé teszi ügyintézési lépések telefonon történő lebonyolítását, és a felhasználó az (1) bekezdés szerint vagy az adott közszolgáltatás fogyasztói szerződésében rögzített módon azonosította magát, az ügyfélvonal ezen cselekményeket is elláthatja telefonon keresztül.

(3) Az ügyfélvonal adott ügy intézését végző kezelője a – törvény rendelkezése alapján a kérelemmel azonos joghatással bíró – hangfelvételt és az azonosítás érdekében az ügyfélkapuval rendelkező használó nevét és e-mail címét egy e célra rendszeresített elektronikus űrlapra felvezeti, és a hozzá kapcsolt felvétellel együtt elektronikus aláírásával hitelesíti. Az így elkészített dokumentumot haladéktalanul továbbítja az ügyben hatáskörrel és illetékességgel bíró szerv hivatali kapujába.

(4) Az ügyfélvonal rendszeréből a felvétel a címzett szerv átvételi igazolásának megérkezését követően haladéktalanul törlésre kerül.

18. § Ha a felhasználó a 12. § (2) bekezdés i) pontja szerinti tájékoztatást igényel telefonon, az azonosítás a 17. § (1) bekezdése szerint történik.

III. FEJEZET
AZ ELEKTRONIKUS KÖZSZOLGÁLTATÁS IGÉNYBEVÉTELE

Általános szabályok

19. § (1) A központi rendszer szolgáltatásai elektronikus úton, interneten vagy telefon használatával, illetőleg az elektronikus kapcsolattartáshoz személyes közreműködést nyújtó ügysegéd révén vehetők igénybe.

(2) A központi rendszer szolgáltatásainak igénybevétele az Ekszt. 10. § (2) bekezdése szerinti eseteket kivéve a felhasználó azonosításához nem köthető.

(3) A felhasználó az igénybevétel során az elektronikus közszolgáltatás biztonságáról szóló kormányrendeletben meghatározott műszaki-biztonsági követelményeknek megfelelő módon köteles eljárni. Amennyiben e követelmények nem teljesülnek, a felhasználó hozzáférését a központi rendszer védelmi eszközei korlátozhatják.

A központi rendszer útján nyújtott tájékoztató szolgáltatások és az adatszolgáltatási kötelezettségének teljesítése

20. § (1) Az állami, önkormányzati és az Ekszt.-ben meghatározott egyéb közfeladatot ellátó szerv az elektronikus közzétételre vonatkozó, így különösen a közérdekű adatok nyilvánosságáról és az elektronikus információszabadságról szóló törvényekből fakadó kötelezettségét a központi rendszer útján is teljesíti. A központi rendszer az e bekezdés szerint közzétett adatok leíró (meta)adatait is közzéteszi a kereshetőség érdekében.

(2) A közszolgáltatást nyújtó szerv a tevékenységére, így különösen a szervezetére, szolgáltatásaira, működésének szabályozására, gazdálkodására vonatkozó közérdekű és közérdekből nyilvános adatainak közzétételére irányuló kötelezettségét a központi rendszeren keresztül is teljesíti.

(3) Az (1) és (2) bekezdésben meghatározott kötelezettségek nem érintik az érintett szervezetek egyéb jogszabályokban meghatározott adatszolgáltatási kötelezettségét, és nem jelentenek külön megjelenítési kötelezettséget. Amennyiben azonban az érintett szervezet nem biztosítja az elérhetőséget, akkor a központi rendszer működtetője jogosult a felügyeleti szerv intézkedését kérni a közzététel lehetővé tétele érdekében.

(4) Az (1) és (2) bekezdésben említett szerv gondoskodik arról, hogy felhasználói – ha törvény másként nem rendelkezik – megfelelő azonosítás után az ügyfélkapun keresztül, hozzáférhessenek azokhoz az adatokhoz, melyeket a szerv a felhasználóról kezel.

(5) A központi rendszer minden azonosított felhasználója számára biztosítani kell, hogy a róla nyilvántartott adatokat a központi rendszeren keresztül is megismerhesse, és – a helyesbítendő adatra vonatkozó szabályok szerint – elektronikusan is igényelhesse a róla nyilvántartott adatok helyesbítését.

21. § (1) A felhasználó az Ekszt. 24. § (1) bekezdése szerinti adathozzáférési jogosultságait a kormányzati portálon elérhető adathozzáférési űrlapok kitöltésével, és az érintett szerv részére a központi rendszer útján történő megküldésével gyakorolhatja. Tájékoztatás párbeszédre épülő kapcsolat útján is biztosítható.

(2) Az elektronikus közszolgáltatást nyújtó szervezetek kötelesek az általuk vezetett elektronikus nyilvántartásokhoz, illetve az ügyintézésük során elektronikusan keletkezett vagy elektronikus másolatban rendelkezésre álló iratokhoz történő hozzáféréshez szükséges űrlapok rendszeresítéséről és azok kormányzati portálon történő közzétételéről gondoskodni.

(3) Az űrlapokat legkésőbb az elektronikus közszolgáltatást nyújtó szervezet központi rendszerhez történő csatlakozásától számított 15 napon belül kell közzétenni.

22. § (1) Törvény eltérő rendelkezése hiányában az elektronikus közszolgáltatást igénybe vevő természetes személy számára az ügyei elektronikus intézése során elektronikusan keletkezett vagy rendelkezésre álló iratok elektronikus rendelkezésre bocsátása ingyenes, ezzel összefüggésben semmilyen költséget, díjat felszámítani nem lehet.

(2) Ha a jogi személy vagy a jogi személyiség nélküli szervezet jogszabály alapján a közigazgatási hatóság által elektronikusan vezetett nyilvántartásokban róla kezelt adatokhoz az adattovábbítás költségeinek megfizetése ellenében férhet hozzá, az elektronikus közszolgáltatást nyújtó szervezet az adattovábbítás költségét a központi rendszer útján is köteles közzétenni.

23. § (1) A 22. § (1) bekezdése alapján igényelt adatokat – eredményes viszontazonosítás esetén – haladéktalanul, de legkésőbb az adathozzáférési űrlap beérkezésétől számított 3 munkanapon belül elektronikusan, a központi rendszer útján kell az adathozzáférést igénylő számára megküldeni.

(2) Amennyiben az (1) bekezdés szerinti viszontazonosítás nem vezetett eredményre, az adathozzáférési igényt – az eredménytelenségi ok közlése mellett – vissza kell utasítani.

A személyes ügyintézési felület kialakítása

24. § (1) A felhasználó jogosult arra, hogy tartós tárhelyén a működtető által rendelkezésre bocsátott alkalmazás segítségével biztonságosan akár egyenként, akár összevontan tárolja az ügyfélkapuihoz, illetve ilyen megbízatása esetén a hivatal kapuihoz tartozó azonosítókat, és azokból a kormányzati portál erre szolgáló, csak általa elérhető felületén személyes ügyintézési felületet kialakítani.

(2) A személyes ügyintézési felületen – a felhasználó döntése alapján – egyidejűleg biztosítani kell az adott személyhez tartozó valamennyi tárhelyéhez ügyfél- és hivatali kapujához hozzáférést.

(3) A személyes ügyintézési felületre a felhasználó összeválogathatja azon elektronikus közszolgáltatások elérhetőségére vonatkozó információkat, amelyeket gyakrabban használ, és azokat is a bejelentkezési információval együtt a rendszer számára tárhelyén védetten tárolja. Az információk utóbb a felhasználó által módosíthatók.

A rendszer működtetése, karbantartása

25. § (1) A központi rendszer működéséről, rendelkezésre állásáról, a központi rendszer, illetve a hozzá csatlakozott elektronikus közszolgáltatást nyújtó szervezetek által biztosított szolgáltatások elérhetőségéről a működtető, a rendszer üzemeltetéséről a külön jogszabályban kijelölt üzemeltető gondoskodik.

(2) A kormányzati portál üzemeltetője biztosítja az elektronikus közszolgáltatás folyamatos, havi szinten legalább 99,5%-os szintű elérhetőségét:

a) a kormányzati portálon,

b) az elektronikus szolgáltatás személyazonosítást igénylő elemeinek működőképességét az ügyfélkapun keresztül, valamint

c) az elektronikus közszolgáltatás ügyfélszolgálati támogatását az ügyfélvonalon keresztül.

(3) A központi rendszer folyamatosan, napi 24 órán keresztül biztosítja a dokumentumok folyamatos fogadását.

(4) A rendelkezésre állási időbe a kormányzati portálon – a megkezdését legalább 3 nappal megelőzően – meghirdetett karbantartási célú üzemszünet nem számítandó bele. E szabály vonatkozik a központi rendszer útján vagy a központi rendszer szolgáltatási igénybevételével elektronikus közszolgáltatást nyújtó szervezet tervezett és az üzemeltetővel előzetesen egyeztetett időpontban megvalósuló karbantartására is.

Üzemzavar

26. § (1) Az elektronikus közszolgáltatást érintő üzemzavar esetén a szolgáltatást nyújtó szervezet az észlelést követően haladéktalanul értesíti az üzemeltetőt az üzemzavar bekövetkeztéről, annak vélelmezett okáról, előre látható időtartamáról, illetve annak megszűnéséről. Az üzemeltető az üzemzavarról haladéktalanul értesíti a működtetőt, és az üzemzavar elhárításáig folyamatosan tájékoztatja a megtett intézkedésekről.

(2) A működtető az elektronikus közszolgáltatás üzemzavarának észlelését, illetve csatlakozott szervezet által nyújtott szolgáltatásban beállott üzemzavarra vonatkozó tudomásszerzését követően haladéktalanul tájékoztatást tetet közzé a kormányzati portálon. A közzétételi kötelezettség nem vonatkozik az elektronikus szolgáltatások a kormányzati portálon megjelenített elektronikus mutatója útján elérhető elektronikus szolgáltatások körére.

(3) Az üzemeltető szervezet a (2) bekezdésben foglaltakkal egy időben SMS útján értesíti az üzemzavarral érintett szervezeteket az üzemzavar bekövetkeztéről, amennyiben ismert, előre látható időtartamáról, illetve az üzemzavar megszűntét követően haladéktalanul értesíti a szolgáltatás helyreállításáról.

(4) A 15 percet meghaladó időtartamú üzemzavarról szóló tájékoztatás a kormányzati portálon az üzemeltetési információk között jelenik meg. A működtető az üzemzavarról szóló tájékoztatás hozzáférhetőségét a hiba elhárítását követő harmincadik napon megszünteti. A bekövetkezett üzemzavarról az üzemeltető elektronikus naplót vezet, melyet 8 évig megőriz, és megkeresés esetén 3 munkanapon belül az igénylőnek igazolást ad az üzemzavar tényéről.

(5) A működtető vezetője a rendszer túlterheltsége esetén – az üzemeltető véleményének kikérésével – a túlterhelés időszakában legfontosabb szolgáltatásokra szűkítheti az elérhető szolgáltatások körét az elkerülhetetlen társadalmi veszteség minimalizálása céljából, elsődlegesen a határidős kötelezettségek teljesítését biztosító szolgáltatások

fenntarthatósága érdekében, a korlátozott szolgáltatások átlagos igénybevételi gyakoriságának és a kapcsolattartás korlátozásával esetlegesen okozható kárnak a figyelembevételével.

(6) Az ilyen időszakban nem elérhető szolgáltatásokra az üzemzavarra vonatkozó szabályok irányadók. A túlterhelés megszűntével a korlátozott szolgáltatásokat haladéktalanul elérhetővé kell tenni.

Karbantartás, üzemszünet

27. § (1) A központi rendszer karbantartás miatti leállítását megelőzően a működtető szervezet a karbantartási igény felmerülésekor, de a karbantartás megkezdése előtt legalább 3 nappal a kormányzati portál útján tájékoztatja a felhasználókat és az elektronikus közszolgáltatást nyújtó szervezeteket a karbantartási célú üzemszünet várható kezdeti időpontjáról és tervezett időtartamáról, valamint a karbantartásban érintett és így időszakosan elérhetetlenné váló szolgáltatások köréről.

(2) A működtető jogosult heti egyszeri karbantartási üzemszüneti időpont kijelölésére olyan módon, hogy az a szolgáltatások igénybevételét a lehető legkevésbé zavarja. A karbantartás által érintett szervezeteket a karbantartás időpontjáról és időtartamáról a karbantartás elrendelésekor haladéktalanul, a felhasználókat pedig az (1) bekezdésben foglaltak szerint tájékoztatja a működtető. Tervezett karbantartás miatti üzemszünet az éjszakai forgalomminimum időszakára vagy hétvégére jelölhető ki.

(3) Ha a központi rendszer egésze vagy egyes szolgáltatásai egy közigazgatási eljárási cselekmény jogszabályban meghatározott határnapján vagy határnapjára is kiterjedően legalább 1 órán át folyamatosan nem voltak elérhetők, és az erre vonatkozó információ a 26. § (4) bekezdése szerint meghirdetésre került, az érintett közigazgatási eljárásban az ügyintézési határidő külön igazolás nélkül az üzemzavar elhárítását követő első munkanap lesz.

(4) Az (1) bekezdésben foglaltak alkalmazandók egy, a központi rendszeren keresztül elérhető elektronikus közszolgáltatás karbantartás miatti leállása esetében is. Az elektronikus közszolgáltatást nyújtó szervezet a központi rendszerrel összekapcsolt informatikai rendszerein a karbantartásokat a központi rendszer üzemeltetőjével előzetesen egyeztetett időpontban végezheti el.

(5) A működtető a rendszer kapacitásainak egyenletesebb kihasználásának előmozdítása végett

a) adatszolgáltatást kérhet az egyes szervezetektől a terhelési határidőkre vonatkozóan,

b) a teljesítménycsúcsok mérséklése érdekében jogosult a kormánynál kezdeményezni az egyes egybeeső határidők módosítását.

(6) Ha egy felhasználó az elektronikus kapcsolattartáshoz általa igénybe vett, nem saját ellenőrzése alatt álló informatikai rendszer a (3) bekezdés szerinti feltételeknek megfelelő időpontbeli és időtartamú üzemzavara vagy karbantartási leállása miatt nem tudta határidőben teljesíteni kötelezettségét, igazolási kérelemnek van helye, amiben a felhasználó a szolgáltatótól, illetve az Országos Informatikai és Hírközlési Főügyelettől kapott ténytanúsítással bizonyíthatja vétlenségét.

Az ügyek intézéséhez szükséges azonosítás

28. § (1) A természetes személy felhasználó az ügyfélkapu létesítését a regisztrációs feladat ellátására jogosult szerveknél (a továbbiakban: regisztrációs szerv) a központi elektronikus szolgáltató rendszer igénybevételével végzett azonosításról szóló kormányrendelet szerinti eljárásrendben kezdeményezheti, illetve gyakorolhatja megszerzett jogosultságát.

(2) Az ügyfélkapunál használt jelszó alapján történő azonosítás az Ekszt. szerinti alacsony biztonsági fokozatú azonosítás. A jelszó használatára vonatkozó szabályokat az (1) bekezdés szerinti jogszabály tartalmazza.

29. § (1) Hivatali kapu szolgál a szervezetek az elektronikus közszolgáltatásokhoz való hozzáférésének, illetve elektronikus közszolgáltatások nyújtásának biztosítására. A használó szervezetek jogállása szerint megkülönböztethetők a hivatali kapun belül altípusok, ezek működési rendszere a szervezettípus sajátosságaihoz igazodik. A hivatali kapu létrehozásának és működésének eljárásrendjét a 28. § (1) bekezdése szerinti jogszabály tartalmazza.

(2) Az elektronikus közszolgáltatás nyújtására is alkalmas hivatali kapu létrehozásának feltétele a hivatali kapu nyitásán túlmenően az elektronikus közszolgáltatás működtetéséről szóló kormányrendelet szerinti megállapodás megkötése a működtetővel, illetve szerződés megkötése az üzemeltetővel.

(3) A központi rendszer üzemeltetője a hivatali kapuval rendelkező szervezet számára elektronikus szervezeti postafiókot hoz létre.

(4) A központi rendszer a BEDSZ igénybevételével teszi lehetővé az elektronikus közszolgáltatást nyújtó szervezet számára a felhasználó által hozzá intézett dokumentum fogadását és válaszdokumentum küldését. Ha jogszabály vagy az ügyfél erre az elektronikus közszolgáltatást nyújtót felhatalmazta, saját kezdeményezésből is megkeresheti a felhasználót.

(5) Internetes böngésző programmal történő hozzáférés esetén a hivatali kapu (a szervezet) azonosítása hivatali kapura vonatkozó azonosítási eljárással, illetve a szervezet hivatali kapujához hozzáférési joggal rendelkező személy azonosítása az adott személy ügyfélkapu azonosításának felhasználásával történik.

(6) A szervezet hivatali kapujához hozzáférésre jogosultak nyilvántartásának vezetésére felhatalmazott képviselők nyilvántartásának vezetését – a hivatali kaput használó szervezet adatszolgáltatása alapján – az elektronikus közszolgáltatás működtetéséről szóló kormányrendeletben feljogosított adatkezelő végzi.

(7) Az elektronikus közszolgáltatást nyújtó szervezet a központi rendszer által biztosított alkalmazás segítségével, a 28. § (1) bekezdésében említett jogszabály szerint maga végzi a képviseletében eljárni jogosult személyek regisztrációját, illetve jogosultságaik nyilvántartását.

30. § (1) Ha a csatlakozott szervezet nem böngészőn keresztül, hanem erre szolgáló célrendszerrel, automatizáltan fogadja, illetve küldi a küldeményeket, a BEDSZ szolgáltatásai a hivatali kapun keresztül csak biztonságos csatorna használatával vehetők igénybe.

(2) Automatizált hozzáférés esetén a szervezeti postafiókhoz hozzáférést biztosító azonosító bizalmas kezeléséről az elektronikus közszolgáltatást nyújtó szervezet gondoskodik.

31. § A közigazgatási szerv hivatali kapujához a 29. § (7) bekezdésben foglaltak szerint hozzáférési joggal rendelkező köztisztviselő – ideértve a jegyzőt is – a közigazgatási hatósági eljárási törvény elektronikus szolgáltatásra vonatkozó szabályai figyelembevételével meghatalmazás alapján jogosult a felhasználó nevében eljárni. A meghatalmazást a hivatali kapuval rendelkező szervezet az iratkezelési szabályok szerint kezeli.

A biztonságos elektronikus dokumentumtovábbító szolgáltatás

32. § (1) A BEDSZ

a) fogadja és elektronikus úton a címzett szervezet postafiókjába továbbítja a felhasználó által az elektronikus űrlapok fogadására feljogosított szervezetekhez intézett elektronikus dokumentumokat,

b) fogadja és a címzett felhasználóhoz továbbítja az elektronikus közszolgáltatást nyújtó szervezet az a) pont szerinti dokumentumok összefüggésében küldött válaszait, továbbá

c) mindkét irányban megfelelő bizonyító erővel dokumentálja a küldés tényét, időpontját, a küldő és címzett személyét, és lehetővé teszi a küldött dokumentum azonosítását.

(2) A BEDSZ az ügyfélkapun keresztül csak az általános nyomtatványtervezővel és általános nyomtatványkitöltővel készített, vagy annak megfelelő formátumú és a központi rendszerben előzetesen regisztrált elektronikus űrlapot fogadja.

(3) Az űrlapot a beküldő a dokumentum esetleges utólagos megváltozásának kimutathatóvá tétele érdekében elektronikus aláírással láthatja el, amire az általános nyomtatványkitöltő lehetőséget biztosít. A BEDSZ az aláírt dokumentumot változatlanul, az aláírás ellenőrzésére alkalmas formában továbbítja.

(4) A működtető hozzájárulhat ahhoz, hogy az elektronikus közszolgáltatást nyújtó szervezet a BEDSZ szolgáltatását a (2) bekezdésben foglaltaktól eltérő feltétellel használja, ha az gazdaságos, a felhasználók érdekeit szolgálja, összhangba hozható a BEDSZ működési modelljével és biztosítja a visszaigazoláshoz szükséges információkat.

(5) A BEDSZ a természetes személyek számára az ügyfélkapun keresztül, a szervezetek számára pedig a hivatali kapun keresztül érhető el.

33. § (1) A hivatali kapuval rendelkező csatlakozott szervezet az elektronikus űrlapokat és az azokhoz csatolt egyéb elektronikus dokumentumokat (a továbbiakban együtt: elektronikus küldemény) a BEDSZ útján, hivatali postafiókján keresztül fogadja.

(2) A befogadott elektronikus küldemény változatlan formában és tartalommal, – a rendszerbe történő befogadást követő – haladéktalan továbbítását – a címzettként megjelölt szervezet szervezeti postafiókjába, illetve a felhasználó értesítési tárhelyére – az üzemeltető biztosítja.

(3) A BEDSZ elvégzi a benyújtott elektronikus küldemény sérülésmentességének, valamint formai követelményeknek való megfelelőségének ellenőrzését. Biztonsági kockázat vagy az átvitel hiányosságának észlelése esetén a rendszer megtagadja az elektronikus küldemény befogadását, és a megtagadás tényéről – annak okának feltüntetése mellett – a felhasználót tájékoztatja.

(4) A csatlakozott szervezet által befogadott és aláírásával ellátott dokumentumnak minősül a felhasználó által küldött és a központi rendszer által befogadott olyan elektronikus küldemény, melyet a felhasználó az elküldéssel párhuzamosan a BEDSZ igénybevételével a tartós tárába is feltöltött.

34. § (1) A BEDSZ igénybevételével a benyújtott elektronikus küldeményre a befogadás során azonnal érkeztető szám és időbélyegző kerül. Az érkeztető szám lehetővé teszi az egyértelmű azonosítást, az időbélyegző pedig az elektronikus küldeményre és a benyújtás körülményeire jellemző egyedi lenyomatként tanúsítja az elektronikus küldemény beérkezésének megtörténtét, a beérkezés időpontját és biztosítja az elektronikus küldemény változatlansága utólagos ellenőrzésének lehetőségét.

(2) Az elektronikus közszolgáltatást nyújtó szervezetnek küldött elektronikus küldeményt a központi rendszer által az (1) bekezdés szerinti tartalommal kiadott befogadási igazolásban rögzített időponttól kell benyújtottnak tekinteni.

(3) A BEDSZ szolgáltatásait felhasználó által küldött elektronikus küldemény esetében az utólagos viszontazonosítás elvégzését lehetővé tevő ügyfél-azonosító kódot a BEDSZ csatolja a címzett szervezet szervezeti postafiókjában elhelyezett elektronikus küldeményhez.

35. § (1) A BEDSZ által a felhasználónak biztosított szolgáltatások:

a) az elektronikus úton érkezett küldemények fogadása, időbélyeggel való ellátása, címzett érkeztetési tárába való továbbítása, majd ott biztonságos ideiglenes, vagy természetes személy felhasználó számára hosszú távú tárolási lehetőség biztosítása;

b) a befogadott elektronikus küldeményekről a befogadás időpontját és a befogadott elektronikus küldemény érkeztető számát és lenyomatát igazoló befogadási igazolás kiállítása és visszaküldése az elektronikus küldemény feladójának;

c) értesítő elektronikus levél, illetőleg – az ügyfél és elektronikus hírközlési szolgáltatója előzetes megállapodása esetén – rövid üzenetküldési szolgáltatás segítségével értesítés kiküldése a felhasználó ügyfélkapu-nyilvántartásban szereplő elektronikus levélcímére, illetőleg – az SMS díjának vállalása esetén – telefonszámára, ha az értesítési tárhelyre dokumentum érkezett;

d) általános nyomtatványkitöltő alkalmazás biztosítása a kormányzati portálról történő letöltési lehetőséggel a nyomtatványok hagyományos és elektronikus kitöltéséhez, tikosításához, küldésre előkészítéséhez;

e) kulcsgeneráló és rejtjelező szolgáltatás biztosítása az általános nyomtatványkitöltő részeként aszimmetrikus titkosító kulcspár generálásához, valamint dokumentumok rejtjelezéséhez és visszaállításához;

f) a megadott formátumú rejtjelező kulcsok kulcstárba történő feltöltésének, majd feltöltés után törlésének és újrafeltöltésének, illetve megőrzésének biztosítása;

g) a felhasználó igénye és hozzájárulása esetén törzsadatok kezelése, melynek keretében lehetővé válik, hogy az elektronikus űrlapokon a felhasználó adatai a személyi adat- és lakcímnyilvántartásból vagy a központi idegenrendészeti nyilvántartásból átemelt adataival kerülhessenek kitöltésre.

(2) Az (1) bekezdés e) pontja szerinti a kulcsgeneráló szolgáltatással létrehozott titkosító kulcspár magán kulcsának megőrzése, illetve a nyilvános részének a kulcstárban való elhelyezése a felhasználó felelőssége. E kulcsokat megsemmisülésük esetén a központi rendszer üzemeltetője nem pótolja.

(3) Az elektronikus közszolgáltatást nyújtó szervezet részére biztosított szolgáltatások:

a) szervezeti postafiók létrehozása, ahol a felhasználótól származó elektronikus dokumentumok kerülnek letöltésig tárolásra, de legkésőbb 30 napig;

b) a szervezeti postafiókban található 3 munkanapon belül át nem vett küldemény esetén figyelmeztetés küldése a hozzáférésre jogosultak nyilvántartásának vezetésére felhatalmazott képviselő ügyfélkapujába;

c) a felhasználó számára küldött és az átvételről visszaigazolást igénylő dokumentum a felhasználó általi átvételét vagy 5 munkanapon belül át nem vételét visszaigazoló értesítés;

d) automatizált rendszerrel vagy az interneten böngészővel történő hozzáférés a saját szervezeti postafiókhoz;

e) támogatás a rejtjelezett dokumentumforgalmazáshoz (dokumentum rejtjelezés, visszaállítás);

f) kulcstár hozzáférés biztosítása a csatlakozott szervezet számára a felhasználó részére küldendő dokumentum – a felhasználó igénye alapján történő – rejtjelezéséhez;

g) általános nyomtatványtervező biztosítása az általános nyomtatványkitöltővel kitölthető elektronikus (és hagyományos) nyomtatványok tervezéséhez;

h) proaktív, a lehetőség vagy szükséglet felmerülésére személyre szabottan figyelmet felhívó ügyfél-tájékoztatás támogatása.

(4) Az elektronikus közszolgáltatást nyújtó szervezet a tájékoztató szolgáltatása keretében tájékoztatja a felhasználót a dokumentum elektronikus úton történő benyújtásának lehetőségéről, a kormányzati portál pedig oktatási anyagot biztosít az eszköz, illetve szolgáltatás használatához.

36. § (1) Az elektronikus közszolgáltatást nyújtó szervezetnek küldött dokumentum, amennyiben a felhasználó azt feltöltéskor igényli, és saját nyilvános titkosító kulcsát a kulcstárba feltöltötte, tárolásra kerül a felhasználó tartós tárában is. A tartós tárba a felhasználó az érkezési tárhelyről is tölthet be dokumentumot.

(2) A címzett elektronikus közszolgáltatást nyújtó szervezet a felhasználó dokumentumára küldött válaszdokumentumot, ha erről a felhasználó a dokumentuma benyújtásakor rendelkezett, köteles a felhasználó kulcstárban elhelyezett nyilvános rejtjelező kulcsával rejtjelezni. Amennyiben a felhasználó a rejtjelező kulcsát a rendszerbe nem töltötte fel, úgy a válaszdokumentumot – amennyiben jogszabály azt nem zárja ki – titkosítás nélkül kell a tárhelyére megküldeni. Amennyiben jogszabály kizárja a titkosítatlan megküldést, úgy azt írásos formában, levélben, a kérelemben megjelölt lakcímre kell megküldeni.

(3) Ha a felhasználó értesítési tárhelyére kérte a választ, de annak megérkezése előtt az ügyfélkapuja megszűnik, az elektronikus közszolgáltatást nyújtó szervezet – a regisztrációs nyilvántartást vezető szerv értesítése alapján – a hivatalos iratot írásos formában, papír alapon, postai úton a felhasználó lakcímére küldi meg.

(4) Az elektronikus dokumentum átvételének visszaigazolását a felhasználó részéről teljesítettnek kell tekinteni azzal, hogy a felhasználó az értesítési tárhelyére érkezett dokumentumot megnyitja vagy azt tartós tárhelyére áthelyezi. Az átvétel időpontját a központi rendszer nyugtázza és az időpontot elektronikusan, a hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről szóló törvényben rögzített adattartalommal haladéktalanul közli a küldeményt indító szervezettel.

37. § A központi rendszer a rendszerbe érkezett dokumentumhoz érkeztető számot képez. Az érkeztető szám szerkezetét e rendelet melléklete tartalmazza. Az érkeztető számot a központi rendszer visszajuttatja a küldemény feladójához, és hozzácsatolja a küldeményhez.

Elektronikus tárhely és központi cím

38. § (1) Az ügyfélkapu részét képező tartós elektronikus tárhely mérete 30 Mb. Ezt meghaladó kapacitású tartós tár külön díjazás mellett vehető igénybe.

(2) A hivatali kapu szervezeti postafiókja csak értesítési tárhelyet biztosít.

(3) Az (1) bekezdés szerinti méretet meghaladó tárhely díjszabását az üzemeltető a kormányzati portálon teszi közzé.

(4) Az igénybe venni kívánt többlet tárhely mennyiségét a felhasználó az erre a célra rendszeresített és a kormányzati portálon hozzáférhetővé tett elektronikus űrlap kitöltésével a központi rendszer üzemeltetőjénél jelentheti be.

(5) Az üzemeltető a tárhely kapacitásának bővítését – szabad kapacitás esetén – a befizetés megérkezésétől számított 3 munkanapon belül végzi el. A megnövelt kapacitású tárhely hozzáférhetőségéről a működtető szervezet haladéktalanul automatikus értesítést küld a felhasználó értesítési tárhelyére.

39. § (1) A központi rendszer működtetője a felhasználók számára a magyarorszag.hu címtartományban egy-egy, a természetes személyazonosító adatokkal és a törvény által rendszeresített azonosító kódokkal kapcsolatban nem álló véletlenszerű központi rendszer címet biztosít, amelyet a felhasználó tetszése szerinti időpontban lecserélhet egy másik, szintén a központi rendszer által rendelkezésre bocsátott véletlenszerű címre.

(2) Az (1) bekezdés szerinti cím kizárólag ügyfélkapuval vagy hivatali kapuval rendelkező felhasználók által érhető el, csak a központi rendszeren belüli kommunikációra használható. Visszaélés észlelése esetén a címet a központi rendszer működtetője a kommunikációból kizárhatja.

(3) Ha a felhasználó egyedi információt kíván közzé tenni, vagy erre törvény kötelezi, az (1) bekezdésben foglalt követelményeknek megfelelő, csak a felhasználó által írható és mindenki más által olvasható egyszer használatos címet igényelhet.

(4) A (3) bekezdés szerinti cím reklámtevékenységre nem használható fel. Megalapozott bejelentés esetén az ilyen közléseket az üzemeltető – az ok megjelölésével – hozzáférhetetlenné teszi.

IV. FEJEZET
AZ ÜGYINTÉZÉSHEZ KAPCSOLÓDÓ ELJÁRÁSOK

Fizetési kötelezettségek teljesítése

40. § (1) Ha az elektronikus közszolgáltatást igénybe vevő felhasználó olyan eljárást kezdeményez, amelyben az illeték- vagy az igazgatási szolgáltatási díj fizetési kötelezettsége keletkezik, e kötelezettségét:
a) államigazgatási eljárási illeték esetében a Magyar Államkincstárnál vezetett eljárási illetékbevételi számla javára,
b) igazgatási szolgáltatási díj esetében a vonatkozó jogszabályban megjelölt számla javára,
c) szolgáltatási díj esetében az elektronikus közszolgáltató által megjelölt számlára
átutalással teljesíti.

(2) A banki átutalás „közlemény" rovatában, illetve a készpénz-átutalási megbízás befizető azonosító rovatában fel kell tüntetni a központi rendszer által adott 27 jegyű érkeztető számot, valamint illeték vagy szolgáltatási díj esetében az eljárást azonosító kódot, amelyet az eljárás űrlapján jól láthatóan fel kell tüntetni.

(3) Ha az elektronikus közszolgáltatást igénybe vevő felhasználó az eljárási illeték előzetes megfizetését lehetővé vagy kötelezővé tevő elektronikus hatósági ügyet indít, a készpénz-átutalási megbízás feladóvevényén szereplő „azonosító" számot (8 számjegyű azonosító), a megfizetett eljárási illeték összegét, a befizetés időpontját fel kell tüntetnie az eljárást indító elektronikus űrlap erre szolgáló rovatában.

(4) Ha az elektronikus kapcsolattartást lehetővé tevő eljárásban a befizetés megérkezésének igazolása került előírásra az eljárás indításának feltételeként úgy az eljárást indító űrlaphoz kell csatolni a Magyar Államkincstár elektronikus visszaigazolását.

(5) Az eljárási illetéket, ha azt a kérelem előterjesztését megelőzően az elektronikus kapcsolattartást kezdeményező felhasználó nem fizette meg vagy az igazgatási szolgáltatási díjról szóló jogszabály másként nem rendelkezik, az illetéket vagy igazgatási szolgáltatási díjat legkésőbb a központi rendszer által kiküldött ügyazonosító átvételét követő munkanapon kell megfizetni.

(6) Amennyiben az illeték (igazgatási szolgáltatási díj) megfizetése a kérelem elektronikus benyújtása esetén az (5) bekezdésben meghatározott időpontig nem történt meg, akkor az eljáró szerv elektronikus úton felhívja az ügyfelet, hogy nyolc napon belül fizesse meg az eljárásért fizetendő eljárási illetéket vagy igazgatási szolgáltatási díjat. A fizetési kötelezettség mértékéről, módjáról és határidejéről, valamint a mulasztás jogkövetkezményéről az eljáró szerv a kérelmezőt egyidejűleg tájékoztatja.

(7) A fizetési kötelezettséget eredményező eljárásnál alkalmazott elektronikus űrlapon fel kell tüntetni a fizetési kötelezettség teljesítésének lehetséges módjait, a bankszámlaszámot, az eljárás azonosító kódját, a feltüntetendő további adatokat és a befizetés a kérelem benyújtásához viszonyított időpontját.

41. § (1) A Magyar Államkincstár a 40. § (2), (5) és (6) bekezdése szerint befizetett ügyazonosító számot tartalmazó befizetés megtörténtéről az ügyazonosító számot, a megfizetett illeték összegét és a befizetés időpontját tartalmazó listát küld az ügyben eljáró közigazgatási szerv részére, mely az ügyfél által benyújtott elektronikus űrlaphoz csatolja a befizetési információt, valamint a könyvelési rendszerbe átadja azt.

(2) Az eljárási illeték előzetes megfizetésével indított ügyben az eljáró szerv a befizetés tényét a Magyar Államkincstár megkeresésével ellenőrzi. A Magyar Államkincstár a megkeresésre – csekken történt befizetés esetén a 8 számjegyű azonosító szám, banki átutalás esetén a banki átutalás azonosító száma alapján – közli a megfizetett illeték összegét, a megfizetés időpontját és azt a tényt, hogy az adott azonosító számra érkezett-e korábban megkeresés más szervtől. Az eljáró közigazgatási szerv az (1) bekezdés szerint kezeli a befizetéssel kapcsolatos adatokat.

(3) Ha az azonosító számra más szervtől már érkezett megkeresés, akkor az eljáró szerv a 40. § (6) bekezdésben foglaltak szerint felszólítja az ügyfelet a teljesítésre.

(4) Ha jogszabály igazgatási szolgáltatási díj fizetési kötelezettség esetén az elektronikusan eljáró ügyfél számára lehetővé teszi, legkésőbb a közigazgatási eljárást lezáró határozat, igazolvány, vagy hatósági bizonyítvány személyes átvételével egyidejűleg fizethető meg az igazgatási szolgáltatási díj, a jogszabályban meghatározott módon.

(5) Közigazgatási hatóságok esetén az igazgatási szolgáltatási díj, más elektronikus közszolgáltatást nyújtó szervezetek esetében a szolgáltatás ellenértékének kezelése a szervezetre vonatkozó számviteli szabályok szerint történik.

42. § (1) Amennyiben az elektronikus közszolgáltató rendelkezik bankkártyás fizetést fogadni képes terminállal, a fizetés bankkártyával is teljesíthető.

(2) A befizetést a 40. § eljárásainak alkalmazásával kell nyilvántartani és kezelni.

43. § A távolról történő elektronikus kapcsolattartáshoz, ügyintézéshez kapcsolódó elektronikus fizetés szabályairól külön jogszabály rendelkezik.

Az elektronikus dokumentum zárt kezelése

44. § (1) Ha a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény szerint adatok zárt kezelése szükséges, megfelelő megoldásnak kell tekinteni az olyan informatikai megoldást, amely csak a törvényben meghatározott személyek részére teszi megismerhetővé a zárt kezelésű adatokat.

(2) Az (1) bekezdésben meghatározott megoldás különösen a külön jogszabály szerinti követelményeknek megfelelő rejtjelezés és rejtjelezett formában történő tárolás, amely biztosítja, hogy a rejtjelezett elektronikus dokumentumból az eredeti elektronikus dokumentumot kizárólag a megismerésre jogosult részére lehet visszaállítani.

(3) A (2) bekezdés szerinti rejtjelezést a hatósághoz mint szervezethez és nem meghatározott természetes személyhez rendelt rejtjelező kulcs útján kell elvégezni.

Az elektronikus dokumentumra történő rávezetés, feljegyzés, kijavítás, záradékolás, felülhitelesítés

45. § Ahol jogszabály valamely jognak, döntésnek, ténynek vagy más adatnak iratra történő feljegyzését vagy rávezetését rendeli el, illetve valamely irat záradékolásáról vagy kijavításáról rendelkezik, (e bekezdésben együtt feljegyzés) azon érteni kell a feljegyzéssel érintett, módosított elektronikus dokumentumot is, ha a módosított elektronikus dokumentumból egyértelműen kitűnik:

a) az eredeti elektronikus dokumentum teljes tartalma,

b) a feljegyzés ténye, időpontja és a feljegyző személye és

c) a feljegyzés tartalma.

V. FEJEZET
ZÁRÓ RENDELKEZÉSEK

46. § (1) E rendelet – a (2) bekezdésben meghatározott kivétellel – a kihirdetését követő 8. napon lép hatályba.

(2) A 6. § (2) és (7) bekezdése, a 20. § (2) bekezdése, a 38–39. §, valamint a 35. § (1) bekezdés c) pontjában az „illetőleg – az SMS díjának vállalása esetén – telefonszámára," szövegrész 2010. január 1-jén lép hatályba.

(3) Az elektronikus ügyintézés részletes szabályairól szóló 193/2005 (IX. 22.) és a központi elektronikus szolgáltató rendszerről szóló182/2007 (VII. 10) Korm. rendelet hatályát veszti.

Bajnai Gordon s. k.,
miniszterelnök

Melléklet a 225/2009. (X. 14.) Korm. rendelethez

Az érkeztető szám képzése

1–9	A szervezet a hivatali kapu nyilvántartásban kapott, nem változó és egyedi azonosítója
10–17	Az érkezés dátuma (éééé hhnn)
18–21	Az érkezés időpontja (óópp)
22–27	A központi rendszer által meghatározott, az érkeztetett beadványt azonosító sorszám, mely naponta egyről indul

A Kormány 226/2009. (X. 14.) Korm. rendelete a Svájci–Magyar Együttműködési Program végrehajtási rendjéről szóló 237/2008. (IX. 26.) Korm. rendelet módosításáról

A Kormány az Alkotmány 35. § (2) bekezdésében megállapított eredeti jogalkotói hatáskörében, valamint az államháztartásról szóló 1992. évi XXXVIII. törvény 124. § (2) bekezdés v) pontjában kapott felhatalmazás alapján, az Alkotmány 35. § (1) bekezdés a) és b) pontjában megállapított feladatkörében eljárva a következőket rendeli el:

1. § A Svájci–Magyar Együttműködési Program végrehajtási rendjéről szóló 237/2008. (IX. 26.) Korm. rendelet (a továbbiakban: R.) 2. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) E rendelet alkalmazásában

1. *állami támogatás:* az Európai Közösséget létrehozó Szerződés (a továbbiakban: EK Szerződés) 87. cikkének (1) bekezdése és az EK Szerződés 87. és 88. cikkének a csekély összegű támogatásokra való alkalmazásáról szóló 2006. december 15-i 1998/2006/EK bizottsági rendelet szerinti támogatás;

2. *általános elvek:* a Keretmegállapodás 1. mellékletében rögzített irányelvek és stratégiák;

3. *Értékelő Bizottság:* a Keretmegállapodásban létrehozott, külön szabályzatban meghatározott összetételű szerv, amely megvizsgálja a Projekttervezetet a Keretmegállapodásban rögzített és az egyes pályázati felhívásokban meghatározott kritériumok alapján;

4. *forráslehívás:* azon tevékenységek elnevezése, melyek eredményeképpen a támogatás összege rendelkezésre áll a lebonyolítási bankszámlákon annak érdekében, hogy a Projekt Végrehajtó támogatásra jogosult számlái vagy egyéb, a gazdasági eseményt hitelesen dokumentáló bizonylatai alapján őt megillető támogatás összege, illetve a folyósítandó előleg átutalásra kerüljön;

5. *földrajzi összpontosítás:* összpontosítás a két periférikus és kevésbé fejlett régióra (Észak-Magyarország és Észak-Alföld), amelyekben a Hozzájárulás legalább 40%-a kerül felhasználásra;

6. *gazdálkodó szervezet:* a Polgári Törvénykönyvről szóló 1959. évi IV. törvény 685. §-ának c) pontjában meghatározott szervezet;

7. *Hozzájárulás:* a Svájc által biztosított, vissza nem térítendő pénzügyi hozzájárulás;

8. *igazolási jelentés:* a projektenkénti elszámoláshoz kapcsolódó ellenőrzési dokumentáció, amelyben a Közreműködő szervezetek a Nemzeti Koordinációs Egység számára tanúsítják a projektenkénti elszámolási dokumentáció valódiságát alátámasztó ellenőrzések eredményeképpen az abban szereplő költségek elszámolási szabályok szerinti megfelelőségét;

9. *intézményfejlesztési projekt:* különösen képzésre, tanácsadásra, konferencia szervezésére irányuló projekt;

10. *Keretmegállapodás:* a kibővült Európai Unió gazdasági és társadalmi egyenlőtlenségei csökkentését célzó, a Svájci Szövetségi Tanács és a Magyar Kormány között létrejött Svájci–Magyar Együttműködési Program végrehajtásáról szóló Keretmegállapodás kihirdetéséről szóló 348/2007. (XII. 20.) Korm. rendelettel kihirdetett Keretmegállapodás, amely a Svájci–Magyar Együttműködési Program megvalósítására vonatkozó főbb keretszabályokat tartalmazza;

11. *Kifizető Hatóság:* a Keretmegállapodás 2. mellékletében felsorolt feladatok ellátására létrehozott szerv, amely a Pénzügyminisztérium szervezeti keretei közt működik;

12. *Közbeszerzési eljárás:* a közbeszerzésről szóló 2003. évi CXXIX. törvény (a továbbiakban: Kbt.) és annak végrehajtási rendeletei szerinti eljárás;

13. *Közreműködő szervezet (a továbbiakban: KSz):* a Projektek végrehajtását végző Projekt Végrehajtók tekintetében bármely, a Nemzeti Koordinációs Egység felelőssége alatt vagy a Nemzeti Koordinációs Egység nevében eljáró köz- vagy magánszférába tartozó személy vagy szervezet. A Keretmegállapodás 2. és 3. mellékletében felsorolt, a közreműködő szervezet hatáskörébe tartozó feladatokat a VÁTI Magyar Regionális Fejlesztési és Urbanisztikai Nonprofit Korlátolt Felelősségű Társaság látja el;

14. *négy szem elve:* minden végrehajtási és pénzügyi tranzakció engedélyezését megelőzően az adott feladatot ellátó személy munkáját egy másik személy teljeskörűen felülvizsgálja, beleértve az ellenőrzési listák és a kitöltési útmutatók alkalmazását is;

15. *Nemzeti Koordinációs Egység (a továbbiakban: NKE):* a Keretmegállapodásban rögzítetteknek megfelelően Magyarországon a Svájci–Magyar Együttműködési Program koordinációjáért felelős egység, mely feladatot a Nemzeti Fejlesztési Ügynökség (a továbbiakban: NFÜ) elnöke által kijelölt szervezeti egység látja el;

16. *önálló projekt:* meghatározott célra rendelt, meghatározott szerepet betöltő feladatok egy egységet képező sorozata;

17. *Pályázati Alap:* egy világosan meghatározott cél érdekében létrehozott, szervezeteknek vagy intézményeknek támogatást nyújtó alap, mely elsősorban a több kis projektet tartalmazó programok költséghatékony adminisztrációját biztosítja. A támogatási összeget egy támogatásközvetítő szervezet osztja szét további pályáztatással;
18. *partner:* több jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság által közösen megvalósítandó projekt esetén a megvalósításban részt vevő, illetőleg a Svájci–Magyar Együttműködési Programból támogatásban részesülő fél;
19. *pénzügyi ellenőrzési szervezet:* a Keretmegállapodás 2. mellékletének 5.6. pontjában rögzített ellenőrzési szervezet;
20. *prioritási területek:* a Keretmegállapodás 1. mellékletében meghatározott prioritási területek;
21. *Projekt Előkészítési Megállapodás:* a Projekt Előkészítési Alap tekintetében a projekttervezet benyújtója és a KSz között kötött szerződés;
22. *Projekt Előkészítési Támogatás:* Projekt Előkészítési Alap terhére megítélt, a Projekt Előkészítési Megállapodásban rögzített támogatás;
23. *Projekt Megállapodás:* egyrészről a Svájci Fejlesztési és Együttműködési Ügynökség (a továbbiakban: SFEÜ), illetve a Gazdasági Államtitkárság (a továbbiakban: GÁ), másrészről az NKE vagy további szerződő felek között létrejött megállapodás, amely adott projektre vonatkozóan rögzíti a támogatás és a projektvégrehajtás feltételeit;
24. *Projekt Végrehajtó:* a Keretmegállapodás értelmében egy adott projekt végrehajtásával megbízott bármely állami hatóság, bármely köz- vagy magántestület, melyet elismernek a felek és megbíznak a Keretmegállapodás hatálya alá tartozó projekt végrehajtásával. Az állami támogatásokra vonatkozó szabályok esetén Projekt Végrehajtón a projektgazdát is érteni kell;
25. *Projekttervezet:* a projektkiválasztás alkalmával az első fordulóban benyújtott projekttervezet tartalmazza valamennyi szükséges információt annak érdekében, hogy a javasolt projekt általános értékelése megvalósítható legyen és egy elvi döntésre kerülhessen sor;
26. *svájci hatóság:* a donor fél részéről eljáró hatóság, egyrészt a SFEÜ-n keresztül eljáró Svájci Szövetségi Külügyminisztérium és a GÁ-n keresztül eljáró Szövetségi Gazdasági Minisztérium, másrészt az NKE-vel történő kapcsolattartásért felelős Svájci Nagykövetség, valamint az annak keretén belül működő Svájci Hozzájárulás Hivatala Budapest;
27. *Svájci Hozzájárulás Hivatala Budapest:* a budapesti Svájci Nagykövetség keretén belül működő, a Svájci Hozzájárulás lebonyolítását illetően a magyar intézmények és Svájc közötti kapcsolattartásért felelős iroda;
28. *támogatási ajánlat:* az NKE által támogatásra javasolt és donor svájci hatóság által elfogadott pályázatokra vonatkozó, a donor által megküldött, a támogatás nyújtásának részletes feltételeit tartalmazó dokumentum;
29. *Támogatási Szerződés:* adott Támogatásközvetítő Szervezet és az általa további pályáztatással kiválasztott Projekt Végrehajtók által kötött, a pályázati alapból elnyert támogatás felhasználását szabályozó szerződés;
30. *Támogatásközvetítő Szervezetek (a továbbiakban: TKSz):* nyílt eljárás keretében kiválasztott szervezet, melynek feladata a Pályázati Alap és Ösztöndíj Alap esetén a Pályázati Alap és Ösztöndíj Alap keretében rendelkezésre álló támogatás további pályáztatással történő szétosztása;
31. *technikai segítségnyújtás projekt:* a Technikai Segítségnyújtási Alap keretében megvalósuló projekt;
32. *tematikai összpontosítás:* legfeljebb nyolc prioritási területre történő összpontosítás, amely területeken a Hozzájárulás legalább 70%-a kerül felhasználásra;
33. *Végleges Projektjavaslat:* a projektkiválasztás alkalmával a sikeres első forduló esetén kezdődhet meg a második forduló, amelyben egy Végleges Projekttervezet kerül benyújtásra;
34. *Végrehajtási Megállapodás:* a KSz és a Projekt Végrehajtó között a Projekt Megállapodás alapján kötött szerződés, amely rögzíti a felek jogait és kötelezettségeit a projekt végrehajtására vonatkozóan."

2. § Az R. 7. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) Az igényelhető támogatás összege egyedi projektszemlélet megközelítés értelmében, egyedi projekt formában benyújtott pályázat esetén legalább 1 millió svájci frank lehet, a 3. számú prioritási területet kivéve, ahol ez a határ 5 millió svájci frank, figyelemmel a Keretmegállapodás 1. mellékletében rögzített prioritásterületekhez kapcsolódó támogatási összegre és a pályázati felhívásra. Ettől a svájci hatóság döntése alapján el lehet térni."

3. § Az R. 13. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) A Hozzájárulás felhasználása során a Keretmegállapodásban rögzített alapelveket figyelembe kell venni."

4. § Az R. 21. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) Amennyiben a végrehajtás figyelemmel kísérése során a KSz tudomására jut, hogy az (1) bekezdés a)–c) pontjában felsorolt esetek valamelyike áll fenn, és a Projekt Végrehajtó a Végrehajtási Megállapodás, illetve a Projekt

Megállapodás módosítását nem kezdeményezte, azok módosítását a KSz a Projekt Végrehajtó előzetes tájékoztatását követően kezdeményezi."

5. § Az R. 22. § (2) és (3) bekezdése helyébe a következő rendelkezés lép:

„(2) Amennyiben a végrehajtás figyelemmel kísérése során a KSz tudomására jut, hogy az (1) bekezdés a) és b) pontjában felsorolt esetek valamelyike áll fenn, és a Projekt Végrehajtó a Végrehajtási Megállapodás módosítását nem kezdeményezte, a módosítást a KSz kezdeményezi.

(3) A Végrehajtási Megállapodás (1) bekezdés a) és b) pontjában meghatározott módosításának jóváhagyásáról a KSz saját hatáskörében dönt. E döntéséről, annak indokolásával együtt a KSz azonnal tájékoztatja az NKE-t."

6. § (1) Az R. 27. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) Az NKE pénzügyi lebonyolításhoz kapcsolódó feladatai tekintetében

a) elkülönített folyószámlát (a továbbiakban: programszámla) nyit a Magyar Államkincstárban (a továbbiakban: Kincstár) a svájci hatóság által átutalt támogatások fogadására és visszafizetésére,

b) intézkedik a svájci hatóság által átutalt támogatások fejezeti kezelésű előirányzat-felhasználási keretszámlára (a továbbiakban: EFK) történő továbbutalásáról,

c) biztosítja a kifizetendő támogatás összegének rendelkezésre állását a lebonyolítási forint bankszámlán, annak érdekében, hogy a Projekt Végrehajtó, illetőleg partnere jóváhagyott kifizetési igénylése alapján a támogatás összege, illetve a folyósítandó előleg átutalásra kerülhessen,

d) hitelesíti a KSz által benyújtott elszámolásokat, és továbbítja azokat a svájci hatóság felé,

e) ellenőrzi a pénzügyi lebonyolítás menetét."

(2) Az R. 27. § (4) bekezdés g)–n) pontja helyébe a következő rendelkezés lép:

[A KSz]

„g) beszámol a végrehajtás előrehaladásáról az éves megbeszélésen,

h) tekintettel arra, hogy a közbeszerzési eljárások lebonyolítását a Projekt Végrehajtó végzi el, a KSz a közbeszerzési eljárás megindítása előtt, majd az eredményhirdetést megelőzően ellenőrzi a közbeszerzési dokumentumokat a közbeszerzésekre vonatkozó jogszabályoknak való megfelelés és a műszaki minőségbiztosítás szempontjából,

i) megfigyelőként jelen lehet a közbeszerzési ajánlatok bontása és bírálata során,

j) a Pályázati Alap esetén a pályázat közzétételét megelőzően ellenőrzi a pályázati dokumentációt, megfigyelőként jelen lehet a pályázatok értékelése során,

k) a projekt végrehajtásáról rendszeresen jelent az NKE részére,

l) adatot szolgáltat a programszintű Éves Jelentéshez,

m) kifizeti a Projekt Végrehajtóknak, illetőleg a partnereknek az előlegeket, valamint a támogatások összegét a projektekre benyújtott elszámolások alapján, továbbá a megítélt projekt előkészítési támogatást,

n) eljárásrendjének megfelelő mértékben ellenőrzi a kifizetési kérelmeket, majd összeállítja a közös eljárásrend szerinti dokumentumokat."

(3) Az R. 27. § (6) bekezdése a következő e) ponttal egészül ki:

[A Kifizető Hatóság]

„e) a megfelelő pénzügyi ellenőrzések biztosítása érdekében a támogatások lebonyolításában érintett szervezeteknél helyszíni vizsgálatot végezhet."

7. § Az R. 29. §-a helyébe a következő rendelkezés lép:

„29. § (1) A Svájci–Magyar Együttműködési Program által támogatott projektek közbeszerzési eljárásai tekintetében a Projekt Végrehajtó jár el ajánlatkérőként.

(2) A KSz ellenőrzi – a Technikai Segítségnyújtás kivételével – a közbeszerzési eljárások lebonyolítását a közbeszerzésre vonatkozó jogszabályoknak való megfelelés és a műszaki minőségbiztosítás szempontjából. Annak érdekében, hogy a KSz e feladatát el tudja látni, a Projekt Végrehajtó együttműködik a KSz-szel. Ennek során benyújtja a KSz-hez a közbeszerzési eljárás dokumentumait előzetes ellenőrzésre a közbeszerzési eljárás megindítását, valamint az eredményhirdetést megelőzően.

(3) Az (1) és (2) bekezdés szerinti eljárás során a Projekt Végrehajtó biztosítja, hogy a KSz a közbeszerzési ajánlatok bontása és bírálata során megfigyelőként jelen lehessen. A KSz megfigyelője a bírálat menetéről jelentést készít a KSz vezetője számára, a jelentést egyidejűleg a Projekt Végrehajtónak is megküldi.

(4) Amennyiben a (2) bekezdés szerinti eljárásban a KSz megfigyelője eljárásrendi szabálytalanságot észlel, ezt jelentésében jelzi a KSz vezetőjének és a közbeszerzési bíráló bizottság elnökének.
(5) A közbeszerzési eljárások lebonyolítása során a KSz és a Projekt Végrehajtó további feladatait és kötelezettségeit a Végrehajtási Megállapodás mellékletét képező megállapodás rendezi."

8. § (1) Az R. 31. § (2) bekezdés c) pontja helyébe a következő rendelkezés lép:
[Az Időközi jelentések tartalmazzák]
„c) a közbeszerzéssel, valamint a tájékoztatással és nyilvánossággal kapcsolatos kötelezettségek teljesítését,"
(2) Az R. 31. § (2) bekezdés f) pontja helyébe a következő rendelkezés lép:
[Az Időközi jelentések tartalmazzák]
„f) az alátámasztó bizonylatok megfelelőségéről szóló, 75. § szerinti könyvvizsgálói ellenőrzési jelentést a Végrehajtási Megállapodásban meghatározottak szerint,"

9. § Az R. 37. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) A programszintű Éves Jelentést legkésőbb az éves monitoring megbeszélés előtt egy hónappal meg kell küldeni az éves ülés minden résztvevőjének."

10. § Az R. 40. §-a helyébe a következő rendelkezés lép:
„40. § A Pályázati Alap támogatási forma célja olyan, a Keretmegállapodás 1. mellékletében meghatározott célterületekhez illeszkedő nonprofit jellegű kis projektek támogatása, amelyek támogatási igénye 10 000 és 100 000 svájci frank között van. Ettől a svájci hatóság döntése alapján el lehet térni. E projektek támogatása az NKE által meghirdetett kétlépcsős eljárással kiválasztott Pályázati Alap TKSz közreműködésével történik."

11. § Az R. 49. §-a helyébe a következő rendelkezés lép:
„49. § Az Ösztöndíj Alapból egyrészt a svájci felsőfokú és másoddiplomás programokra, másrészt magyar hátrányos helyzetű és marginalizált csoportbeli hallgatók számára nyújtható pénzügyi támogatás."

12. § Az R. 54. §-a a következő (3) bekezdéssel egészül ki:
„(3) A Svájci–Magyar Együttműködési Program keretében finanszírozott projektek esetén a Projekt Végrehajtóknak az EFK-ról utalt előleg mértéke
a) egyedi projekt támogatási forma esetén a Svájci–Magyar Együttműködési Programból származó támogatás 25%-a,
b) Pályázati Alap támogatási forma esetén a Svájci–Magyar Együttműködési Programból származó támogatás 50%-a,
c) a svájci hatóság, illetőleg az NKE egyedi döntése alapján, a pénzügyminiszter egyetértésével az a) és b) pontban meghatározottakat meghaladó mértékű is
lehet."

13. § Az R. 57. §-a helyébe a következő rendelkezés lép:
„57. § (1) Az NFÜ EFK-t nyit a Kincstárban, amely előfinanszírozásra szolgál.
(2) Az EFK vezetésével kapcsolatos bárminemű költség elszámolása közvetlenül a központi költségvetés, Pénzügyminisztérium fejezet terhére történik.
(3) A Kincstár a bankszámlakivonatot egy eredeti példányban állítja elő, amelyet az NFÜ-nek küld meg."

14. § Az R. az 57. §-t követően a következő 57/A. §-sal egészül ki:
„57/A. § (1) Az NFÜ forint lebonyolítási számlákat nyit a Kincstárban, amelyekről a támogatás a Projekt Végrehajtó, illetőleg partnere számára kiutalásra kerül, illetve a Technikai Segítségnyújtás keret felhasználása esetén a szállítók részére történő kifizetés teljesítésre kerül.
(2) A lebonyolítási számla felett az NFÜ a KSz részére rendelkezési jogosultságot biztosíthat.
(3) A lebonyolítási számla vezetésével kapcsolatos bárminemű költség elszámolása közvetlenül a központi költségvetés, Pénzügyminisztérium fejezet terhére történik.
(4) A Kincstár a bankszámlakivonatot két eredeti példányban állítja elő. Egy példányt az NFÜ-nek, egy példányt pedig a KSz részére küld meg.
(5) A Technikai Segítségnyújtás keret felhasználására külön lebonyolítási számla kerül megnyitásra."

15. § Az R. 59. §-a helyébe a következő rendelkezés lép:
„59. § Az 56–57/A. §-okban meghatározott (bank)számlákhoz kapcsolódó, a Kincstár által kiállított (bank)számlakivonatok adatait a bankszámla felett rendelkezőknek az információtechnológiai rendszerben a kézhezvételt követő 5 munkanapon belül rögzítenie kell.”

16. § Az R. az 59. §-t követően a következő alcímmel és 59/A. §-sal egészül ki:
„**Forráslehívás**
59/A. § (1) Az NKE biztosítja a támogatás összegének rendelkezésre állását a lebonyolítási bankszámlákon, annak érdekében, hogy a Projekt Végrehajtó támogatásra jogosult számlái vagy egyéb, a gazdasági eseményt hitelesen dokumentáló bizonylatai alapján őt megillető támogatás összege, illetve a folyósítandó előleg átutalásra kerüljön.
(2) A támogatás terhére elszámolható költségeket, és ezek alapján a kiutalandó támogatás összegét minden esetben forintban kell megállapítani.
(3) Minden egyes forráslehívási folyamat során a KSz forintban összeállítja a forráslehívási dokumentációt, amely a még le nem hívott támogatásra jogosult pénzügyi elszámolások adatainak összesítését jelenti. A forráslehívási dokumentáció elkészültéről a KSz haladéktalanul tájékoztatja az NKE-t. Az elektronikusan összeállított forráslehívási dokumentációt a KSz kinyomtatja és aláírja. Az NKE a KSz által benyújtott, nyomtatott dokumentáció alapján jóváhagyja a forráslehívást, amelyet aláírással igazol.
(4) A forráslehívási dokumentáció benyújtását követő 5 munkanapon belül az NKE intézkedik a jóváhagyott támogatási összeg EFK-ról a lebonyolítási számlára történő utalásáról.
(5) Technikai segítségnyújtás esetén az NKE állítja össze forintban a forráslehívási dokumentációt.”

17. § Az R. 60. §-a és az azt megelőző alcíme helyébe a következő rendelkezés és alcím lép:
„**Kifizetés és elszámolás a Projekt Végrehajtóval**
60. § A KSz a Projekt Végrehajtók kifizetési kérelme alapján gondoskodik az előleg lebonyolítási számláról történő átutalásáról.”

18. § Az R. 61. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) A KSz az igazolást követően utólagos finanszírozásra jóváhagyja a Projekt Végrehajtó által benyújtott Időközi jelentést és annak részeként az elszámolható költségeket tartalmazó pénzügyi elszámolást, továbbá gondoskodik a támogatások összegének a lebonyolítási számláról a Projekt Végrehajtó, illetőleg partnere (bank)számlájára történő átutalásáról.”

19. § Az R. 63. §-a helyébe a következő rendelkezés lép:
„63. § Az NKE a Projekt Végrehajtók forintösszeget tartalmazó kifizetési kérelmét – a 35. § (3) bekezdésben rögzítettek szerint – továbbítja a Kifizető Hatóságnak rávezetve a továbbküldés napján érvényben lévő, a Magyar Nemzeti Bank által közzétett devizaárfolyam szerinti svájci frank összeget. A Kifizető Hatóság a visszatérítési kérelmet formai ellenőrzés után eljuttatja a svájci hatóság részére.”

20. § Az R. 65. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) Az NKE a 35. § (3) és (4) bekezdés szerint a jóváhagyott Időközi jelentéseket és Projektzáró jelentéseket a visszatérítési kérelemmel együtt eljuttatja a Kifizető Hatóság részére, amely 10 munkanapon belül megküldi azokat a svájci hatóság részére.”

21. § Az R. 66. §-a helyébe a következő rendelkezés lép:
„66. § A visszatérítési kérelem alapján a svájci hatóság a programszámlára utalja a támogatást.”

22. § Az R. 67. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) Az NKE a hitelesítési tevékenységének alátámasztása érdekében helyszíni látogatást tehet a pénzügyi lebonyolításban részt vevő KSz-nél. Az NKE előzetes értesítése alapján a KSz hozzáférést biztosít az NKE által írásban felhatalmazott személyek részére az elektronikus és papír formában rendelkezésre álló, a KSz igazoláshoz kapcsolódó dokumentumaihoz és adataihoz.”

23. § Az R. 69. § (2) bekezdés felvezető szövege helyébe a következő rendelkezés lép:
„A KSz által kiállított forráslehívási dokumentáció tanúsítja, hogy”

24. § Az R. 70. és 71. §-a helyébe a következő rendelkezés lép:
„70. § A Technikai Segítségnyújtási Alap esetén a hitelesítési tevékenységet az NKE látja el a 67. és 68. §-ban meghatározott eljárásrend szerint.
71. § A Technikai Segítségnyújtási Alap esetén az igazolási tevékenységet az NKE látja el.”

25. § Az R. 72. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) A pénzügyi irányítási és kontroll tevékenység tekintetében az Áht., valamint – az e rendeletben foglalt eltérésekkel – az Ámr. és a költségvetési szervek belső ellenőrzéséről szóló 193/2003. (XI. 26.) Korm. rendelet előírásai az irányadók.”

26. § Az R. 75. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) Amennyiben a Projekt Megállapodás másként nem rendelkezik – a Technikai Segítségnyújtás Alap, a Projekt Előkészítési Alap és a Pályázati Alap kivételével –, egy pénzügyi ellenőrzési szervezet időközi könyvvizsgálói ellenőrzés(eke)t végez a két évnél tovább tartó és az 500 000 svájci frank keretösszeget meghaladó projektek esetében, és egy, a nemzetközi audit szabványoknak megfelelő végső pénzügyi ellenőrzést végez az összes projekt esetében.”

27. § Az R. 76. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) Az NFÜ belső ellenőrzési egysége, valamint a KSz és a TKSz belső ellenőrzési részlegei az általuk lefolytatott ellenőrzésekről szóló jelentést az NKE-n keresztül 40 napon belül megküldik a KEHI részére.”

28. § Az R. 77. § (2) és (3) bekezdése helyébe a következő rendelkezés lép:
„(2) A KEHI az (1) bekezdésben meghatározottak mellett elvégzi a teljes hitelesített kiadások 15%-os mintavételes ellenőrzését.
(3) A Technikai Segítségnyújtás Alap, a Projekt Előkészítési Alap és a Pályázati Alap tekintetében – a 75. § (1) bekezdéssel összhangban – az ellenőrzéseket a KEHI folytatja le. Ezen ellenőrzéseket a KEHI legalább kétévente elvégzi.”

29. § Az R. 85. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) A KSz a lebonyolítási számlán történt jóváírásról szóló bankszámlakivonat kézhezvételét követő 5 munkanapon belül visszautalja a behajtott összeg Svájci–Magyar Együttműködési Programra jutó részét az EFK-ra.”

30. § Az R. 86. § (2) bekezdése a következő h) ponttal egészül ki:
[Az (1) bekezdésben meghatározottakon túl az adott támogatási kategóriára vonatkozóan az alábbi előírásokat, az ott meghatározottak szerint kell alkalmazni:]
„h) pénzügyi válság kapcsán nyújtandó átmeneti támogatás (a továbbiakban: átmeneti támogatás) esetében az EK Szerződés 87. cikkének (1) bekezdése szerinti állami támogatásokkal kapcsolatos eljárásról és a regionális támogatási térképről szóló 85/2004. (IV. 19.) Korm. rendelet 23/A. és 23/D. §-ában, valamint e rendelet 112/A. és 112/B. §-ában foglaltak az irányadók.”

31. § Az R. 87. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) E rendelet alapján támogatás csak akkor ítélhető meg, ha a kedvezményezett még a beruházás megkezdése előtt a támogatás iránti kérelmét benyújtja. Egyedi támogatás megítélését megelőzően nagyvállalkozások esetében a fentieken kívül a kedvezményezettek kötelesek bizonyítani azt, hogy az alábbiak közül egy vagy több kritérium teljesül:
a) a támogatás segítségével lényegesen megnövekszik a projekt mérete,
b) kiszélesedik a tevékenység köre,
c) növekszik a kedvezményezett által a projektre fordítandó összeg,
d) lényegesen felgyorsult a projekt végrehajtási üteme,
e) vagy regionális beruházási támogatás esetében a projekt a támogatás hiányában nem az érintett támogatott régióban valósult volna meg.”

32. § Az R. 90. § (2) és (3) bekezdése helyébe a következő rendelkezés lép:
„(2) Elszámolható költségek:
a) a beruházás célját szolgáló
aa) tárgyi eszköznek a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Sztv.) szerinti bekerülési értéke,
ab) tárgyi eszköz vételára létesítmény felvásárlásakor,

ac) immateriális javak közül a találmány, a szabadalom, a licenc és a know-how Sztv. szerinti bekerülési értéke (a továbbiakban: támogatható immateriális javak); vagy

b) a beruházás üzembe helyezését követő harmadik év végéig újonnan létrehozott munkakörökben foglalkoztatott munkavállalókra vonatkozó, a munkáltató által viselt – Sztv. 79. §-a szerint elszámolható – személyi jellegű ráfordításának 24 havi összege, a munkakör létrehozásának napjától számítva.

(3) A (2) bekezdésben meghatározott elszámolható költségek részletes felsorolását a pályázati dokumentáció tartalmazza. A pályázati dokumentáció az elszámolható költségek körét az (1) és (2) bekezdésben meghatározottaktól szűkebben is meghatározhatja."

33. § Az R. a 112. §-t követően a következő alcímmel, valamint 112/A. és 112/B. §-sal egészül ki:

„**Az átmeneti támogatásokra vonatkozó szabályok**

112/A. § (1) Az átmeneti támogatásként nyújtott összes támogatás támogatástartalma vállalkozásonként nem haladhatja meg az 500 000 eurónak megfelelő forintösszeget, figyelemmel a (2) bekezdésben foglaltakra.

(2) A több részletben fizetendő támogatást az odaítélése időpontjában érvényes értékre kell diszkontálni.

(3) Egy vállalkozásnak 2008. január 1-je és 2010. december 31-e között odaítélt átmeneti támogatás és csekély összegű támogatás támogatástartalma együttesen nem haladhatja meg az 500 000 eurónak megfelelő forintösszeget.

(4) Azonos elszámolható költségek tekintetében az átmeneti támogatás nem halmozható csekély összegű támogatással.

(5) Azonos elszámolható költségek tekintetében az átmeneti támogatás nem halmozható állami támogatással, ha az ilyen jellegű kumuláció olyan támogatási intenzitást eredményezne, amely túllépi az adott állami támogatásra vonatkozóan rögzített támogatási intenzitást.

112/B. § (1) Átmeneti támogatás nem nyújtható:

a) a halászati és akvakultúra-termékek piacának közös szervezéséről szóló 1999. december 17-i 104/2000/EK tanácsi rendelet hatálya alá tartozó, halászathoz vagy akvakultúrához kapcsolódó tevékenységet végző vállalkozásnak;

b) az EK Szerződés I. Mellékletében felsorolt mezőgazdasági termékek elsődleges termelésével foglalkozó vállalkozásoknak;

c) az EK Szerződés I. Mellékletében felsorolt mezőgazdasági termékek feldolgozásában és forgalmazásában tevékeny vállalkozásoknak,

ca) amennyiben a támogatás összege az elsődleges termelőktől beszerzett vagy az érintett vállalkozások által forgalmazott ilyen termékek ára vagy mennyisége alapján kerül rögzítésre,

cb) amennyiben a támogatás az elsődleges termelőknek történő teljes vagy részleges továbbítástól függ;

d) harmadik országokba vagy tagállamokba irányuló exporttal kapcsolatos tevékenységekhez, nevezetesen amikor a támogatás mértéke az exportált mennyiségekhez közvetlenül kapcsolódik; illetve értékesítési hálózat kialakításához és működtetéséhez vagy exporttevékenységgel összefüggésben felmerülő egyéb folyó kiadásokhoz kapcsolódik;

e) amennyiben az átmeneti támogatás az importáruk helyett hazai áru használatától függ.

(2) Átmeneti támogatással csak olyan vállalkozás támogatható, amely 2008. július 1-jén nem minősült nehéz helyzetben lévő vállalkozásnak.

(3) A támogatás nyújtását megelőzően a vállalkozás írásban tájékoztatja a támogatást nyújtót az átmeneti támogatás, illetve csekély összegű támogatás formájában 2008. január 1-jét követően neki odaítélt támogatásokról és a még el nem bírált támogatási kérelmeiről.

(4) A támogatást nyújtó kötelessége, hogy felhívja a kedvezményezett figyelmét arra, hogy pénzügyi válság kapcsán nyújtandó átmeneti támogatásban részesült, és egy vállalkozásnak 2008. január 1-je és 2010. december 31-e között odaítélt átmeneti támogatás és csekély összegű támogatás támogatástartalma együttesen nem haladhatja meg az 500 000 eurónak megfelelő forintösszeget.

(5) A kedvezményezett köteles az átmeneti támogatáshoz kapcsolódó minden iratot az odaítélést követő 10. évig megőrizni, és a támogatást nyújtó ilyen irányú felhívása esetén köteles azokat bemutatni."

Záró rendelkezések

34. § Ez a rendelet a kihirdetését követő 5. napon lép hatályba, és a hatálybalépését követő napon hatályát veszti.

35. § E rendelet hatálybalépésével egyidejűleg hatályát veszti az R. 9. §-a.

Bajnai Gordon s. k.,
miniszterelnök

IV. A Magyar Nemzeti Bank elnökének rendeletei

A Magyar Nemzeti Bank elnökének 25/2009. (X. 14.) MNB rendelete a „Kazinczy" arany emlékérme kibocsátásáról

A Magyar Nemzeti Bankról szóló 2001. évi LVIII. törvény 60. §-a (1) bekezdésének d) pontja alapján fennálló jogkörömben eljárva a következőket rendelem el:

1. § (1) A Magyar Nemzeti Bank – Kazinczy Ferenc születésének 250. évfordulója alkalmából – „Kazinczy" megnevezéssel 50 000 forintos címletű arany emlékérmét bocsát ki.

(2) A kibocsátás időpontja: 2009. október 27.

2. § (1) Az emlékérme 968 ezrelék finomságú aranyból készült, súlya 10 gramm, átmérője 25 mm, széle sima.

(2) Az emlékérme előlapján, a középmezőben a széphalmi Kazinczy Emlékcsarnok klasszicista épületének ábrázolása látható. Az emlékcsarnok ábrázolása alatti négy vízszintes sorban a „Széphalom" felirat, az „50000" értékjelzés, a „FORINT" felirat és a „2009" verési évszám, az épület ábrázolása mellett, jobb oldalon pedig a „BP." verdejel olvasható. Az emlékérme szélén, felső köriratban a „MAGYAR KÖZTÁRSASÁG" felirat olvasható. Az emlékérme előlapjának képét e rendelet 1. melléklete tartalmazza.

(3) Az emlékérme hátlapján Kazinczy Ferenc – J.V. Kiminger rézmetszete alapján készült – portréja látható. A portrétól jobbra, három vízszintes sorban Kazinczy Ferenc aláírása, valamint az „1759–1831" felirat olvasható. Az emlékérme szélén, jobb oldalon lent található Szöllőssy Enikő tervezőművész mesterjegye. Az emlékérme hátlapjának képét e rendelet 2. melléklete tartalmazza.

3. § Az emlékérméből 5000 darab készíthető, különleges – ún. proof – technológiával.

4. § Ez a rendelet 2009. október 27-én lép hatályba.

Simor András s. k.,
a Magyar Nemzeti Bank elnöke

1. melléklet a 25/2009. (X. 14.) MNB rendelethez

Az emlékérme előlapjának képe:

2. melléklet a 25/2009. (X. 14.) MNB rendelethez

Az emlékérme hátlapjának képe:

A Magyar Nemzeti Bank elnökének 26/2009. (X. 14.) MNB rendelete a „Kazinczy" ezüst emlékérme kibocsátásáról

A Magyar Nemzeti Bankról szóló 2001. évi LVIII. törvény 60. §-a (1) bekezdésének d) pontja alapján fennálló jogkörömben eljárva a következőket rendelem el:

1. § (1) A Magyar Nemzeti Bank – Kazinczy Ferenc születésének 250. évfordulója alkalmából – „Kazinczy" megnevezéssel 3000 forintos címletű ezüst emlékérmét bocsát ki.

(2) A kibocsátás időpontja: 2009. október 27.

2. § (1) Az emlékérme 925 ezrelék finomságú ezüstből készült, súlya 10 gramm, átmérője 30 mm, széle: recézett.

(2) Az emlékérme előlapján, a középmezőben, fényes téglalapban megjelenő papírtekercs látható lúdtollal, amelyet középen egy zsinórhurok köt át. A zsinórhurok feszített szárai vízszintes irányban, finom aszimmetriával kettéosztják az érme előlapját. A zsinór fölött bal oldalon a „3000" értékjelzés, jobb oldalon a „FORINT" felirat olvasható. A zsinór alatt bal oldalon a „2009" verési évszám, jobb oldalon a „BP." verdejel látható. Az emlékérme szélén, köriratban felül a „MAGYAR", alul a „KÖZTÁRSASÁG" felirat olvasható. Az emlékérme előlapjának képét e rendelet 1. melléklete tartalmazza.

(3) Az emlékérme hátlapján Kazinczy Ferenc szembenéző portréja látható. Az emlékérme szélén, köriratban a „KAZINCZY FERENC 1759–1831" felirat olvasható. A portrétól jobbra található Soltra E. Tamás tervezőművész mesterjegye. Az emlékérme hátlapjának képét e rendelet 2. melléklete tartalmazza.

3. § Az emlékérméből 12 000 darab készíthető, ebből 7000 darab különleges – ún. proof – technológiával verhető.

4. § Ez a rendelet 2009. október 27-én lép hatályba.

Simor András s. k.,
a Magyar Nemzeti Bank elnöke

1. melléklet a 26/2009. (X. 14.) MNB rendelethez

Az emlékérme előlapjának képe:

2. melléklet a 26/2009. (X. 14.) MNB rendelethez

Az emlékérme hátlapjának képe:

A Magyar Nemzeti Bank elnökének 27/2009. (X. 14.) MNB rendelete a „Kálvin” emlékérme kibocsátásáról

A Magyar Nemzeti Bankról szóló 2001. évi LVIII. törvény 60. §-a (1) bekezdésének d) pontja alapján fennálló jogkörömben eljárva a következőket rendelem el:

1. § (1) A Magyar Nemzeti Bank – Kálvin János születésének 500. évfordulója alkalmából – „Kálvin” megnevezéssel 5000 forintos címletű ezüst emlékérmét bocsát ki.

(2) A kibocsátás időpontja: 2009. október 29.

2. § (1) Az emlékérme 925 ezrelék finomságú ezüstből készült, súlya 31,46 gramm, átmérője 38,61 mm, széle recézett.

(2) Az emlékérme előlapján, körvonallal ellátott külső gyűrűben, felső köriratban a „MAGYAR KÖZTÁRSASÁG” felirat olvasható. A középmezőben a Debreceni Református Kollégium szószéktartóján található Krisztus-monogram ábrázolása látható. Az ábrázolás alatti két vízszintes sorban az „5000” értékjelzés és a „FORINT” felirat olvasható. Az emlékérme bal alsó részén a „BP.” verdejel, a jobb alsó részén a „2009” verési évszám olvasható. Az emlékérme előlapjának képét e rendelet 1. melléklete tartalmazza.

(3) Az emlékérme hátlapján, körvonallal ellátott külső gyűrűben, felső köriratban a „SOLI DEO GLORIA”, alsó köriratban a „KÁLVIN JÁNOS 1509–1564” felirat olvasható. A középmezőben Kálvin János – Hans Holbein festménye alapján készült – portréja látható. A portrétól balra az „EUROPA” nemzetközi emlékérme-sorozat közös emblémája, az ún. „Euro-Star” jel látható, míg a portrétól jobbra Csikai Márta tervezőművész mesterjegye található. Az emlékérme hátlapjának képét e rendelet 2. melléklete tartalmazza.

3. § Az emlékérméből 12 000 darab készíthető különleges – ún. proof – technológiával.

4. § Ez a rendelet 2009. október 29-én lép hatályba.

Simor András s. k.,
a Magyar Nemzeti Bank elnöke

1. melléklet a 27/2009. (X. 14.) MNB rendelethez

Az emlékérme előlapjának képe:

2. melléklet a 27/2009. (X. 14.) MNB rendelethez

Az emlékérme hátlapjának képe:

V. A Kormány tagjainak rendeletei

Az egészségügyi miniszter 30/2009. (X. 14.) EüM rendelete a fertőző betegségek és a járványok megelőzése érdekében szükséges járványügyi intézkedésekről szóló 18/1998. (VI. 3.) NM rendelet, valamint az emberi felhasználásra kerülő gyógyszerek rendeléséről és kiadásáról szóló 44/2004. (IV. 28.) ESZCSM rendelet módosításáról

Az egészségügyről szóló 1997. évi CLIV. törvény 247. § (2) bekezdés d) pont df)–dg) alpontjában, az emberi alkalmazásra kerülő gyógyszerekről és egyéb, a gyógyszerpiacot szabályozó törvények módosításáról szóló 2005. évi XCV. törvény 32. § (5) bekezdés o) pontjában, valamint az egészségügyi hatósági és igazgatási tevékenységről szóló 1991. évi XI. törvény 15. § (11) bekezdés a) pontjában foglalt felhatalmazás alapján, az egészségügyi miniszter feladat- és hatásköréről szóló 161/2006. (VII. 28.) Korm. rendelet 1. § a) pontjában megállapított feladatkörömben eljárva a következőket rendelem el:

1. § A fertőző betegségek és a járványok megelőzése érdekében szükséges járványügyi intézkedésekről szóló 18/1998. (VI. 3.) NM rendelet (a továbbiakban: R.) 4. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) Az oltás végrehajthatóságának megítéléséről a kezelőorvos dönt. Orvosi felügyelet mellett egészségügyi szakdolgozók is végezhetnek védőoltást."

2. § Az R. 5. § (8) bekezdésének felvezető szövege helyébe a következő rendelkezés lép:

„Azoknál a gyermekeknél, akiknél bármelyik kötelezően előírt védőoltás elmaradt, az elmaradt védőoltást a legrövidebb időn belül pótolni kell. Azok az orvosok, akik bölcsődébe, óvodába, nevelőszülőkhöz, gyermekotthonba, illetőleg egyéb gyermekközösségbe, továbbá alap-, közép- és felsőfokú oktatási intézménybe kerülő gyermekek vizsgálatát végzik, kötelesek az életkor szerint esedékessé vált oltások megtörténtét ellenőrizni. A hiányzó oltásokat az oltás végzésére jogosultaknak pótolniuk kell. Az oltási kötelezettség"

[a) a torokgyík, a szamárköhögés és a merevgörcs elleni elmaradt első, második és harmadik védőoltásra a 7. életév,

b) a torokgyík, a merevgörcs elleni elmaradt negyedik, továbbá a gyermekbénulás elleni elmaradt védőoltásokra a 14. életév,

c) a kanyaró, a rózsahimlő, a mumpsz és a Hepatitis B elleni elmaradt védőoltásokra a 20. életév,

d) a Hib elleni elmaradt védőoltásokra az 5. életév

betöltéséig áll fenn.]

3. § (1) Az R. 13. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) Ha a gyermek oltását nem a területileg illetékes háziorvos vagy házi gyermekorvos végzi, az elvégzett oltásokra vonatkozó adatokat az oltóorvos az oltás beadásának napján írásban vagy elektronikus úton köteles jelenteni a kistérségi intézetnek."

(2) Az R. 13. § (7) bekezdése helyébe a következő rendelkezés lép:

„(7) A védőoltást követő nemkívánatos eseményeket, beleértve az oltási reakciókat (mellékhatásokat) és oltási baleseteket

a) az oltó-, illetve észlelő orvos a kistérségi intézetnek, és egyidejűleg az Országos Gyógyszerészeti Intézetnek,

b) a kistérségi intézet a regionális intézetnek,

c) a regionális intézet az OEK-nek

haladéktalanul jelenti."

4. § (1) Az R. 15. § (2) bekezdés a)–b) pontja helyébe a következő rendelkezés lép:

[Az oltóorvos]

„a) nyilvántartást vezet a területi ellátási kötelezettségéhez tartozó oltandó személyekről,

b) az a) pont szerinti oltandó személyek számára az életkorhoz kötött oltáshoz szükséges oltóanyag (a hozzá bejelentkezettek neve és TAJ-száma szerinti) igénylését – a védőnővel együttműködve – a rendelő székhelye szerint illetékes kistérségi intézetnek megküldi,"

(2) Az R. 15. § (2) bekezdés h) pontja helyébe a következő rendelkezés lép:
[Az oltóorvos]
„h) a 13. § (7) bekezdés a) pontja szerinti jelentési kötelezettségének eleget tesz,"

5. § Az R. 17. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) A 18–21. §-ban foglalt esetekben, amennyiben a szűrővizsgálatra kötelezett személy a szűrővizsgálaton nem jelenik meg, a kistérségi intézet az Eütv. 60. § (2) bekezdésében foglaltak szerint a szűrővizsgálatot elrendeli."

6. § Az R. 27. § (5) bekezdése helyébe a következő rendelkezés lép:
„(5) Amennyiben az 1. számú mellékletben nevesített fertőző megbetegedésben szenvedő személy nem veti magát alá a gyógykezelésnek, a kistérségi intézet az Eütv. 56. § (2) bekezdésében foglaltak alapján az érintettet a gyógykezelésre kötelezheti."

7. § Az R. 37. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) Minden egészségügyi, szociális és oktatási dolgozó, aki az elvégzett vizsgálatok során tetvesség fennállását észleli, vagy arról hivatásának gyakorlása közben tudomást szerez, köteles annak megszüntetéséről haladéktalanul gondoskodni. Amennyiben ezt a tetvesség mértéke, jellege vagy bármi más ok miatt hatáskörében nem tudja biztosítani, köteles az esetről a kistérségi intézetet tájékoztatni, amely a tetvetlenítést elvégezteti."

8. § Az R. 41. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) A mikrobiológiai vizsgálatot végző laboratórium a fertőző betegségre gyanús személyek mikrobiológiai vizsgálati eredményeit a természetes személyazonosító adataikkal együtt továbbítja a regionális intézet járványügyi vagy epidemiológiai osztályára."

9. § Az R. 4. számú melléklete 2. pontja helyébe a következő rendelkezés lép:
„2. Szúnyogok
Szúnyogirtó szer és szúnyoglárvairtó szer légi úton csak az OTH engedélyével juttatható ki a környezetbe.
Légi úton történő szúnyogirtás és szúnyoglárvairtás egészségügyi gázmester szakmai irányításával végezhető.
A légi úton történő szúnyoglárvairtáshoz entomológiai szakképzettséggel rendelkező személy részvétele is szükséges.
Az engedélyes köteles a kezelések tényleges időpontját és helyét a regionális intézetnek az egészségügyi hatósági és igazgatási tevékenységről szóló törvényben meghatározottak szerint bejelenteni."

10. § Az emberi felhasználásra kerülő gyógyszerek rendeléséről és kiadásáról szóló 44/2004. (IV. 28.) ESZCSM rendelet 16. § (3) bekezdés c) pontja helyébe a következő rendelkezés lép:
[Orvosnak, állatorvosnak és gyógyszerésznek – amennyiben végzettségét hitelt érdemlően igazolni tudja – vényköteles gyógyszer legfeljebb harminc napra elegendő mennyiségben vény nélkül kiadható. Orvosnak, állatorvosnak és gyógyszerésznek is csak vényre adható ki]
„c) az alkalmazási előírása szerint az influenzavírus okozta megbetegedések megelőzésére és kezelésére szolgáló gyógyszerkészítmény, legfeljebb az alkalmazási előírása szerinti terápiás alkalmazáshoz szükséges mennyiségben."

11. § (1) E rendelet a kihirdetését követő napon lép hatályba.
(2) Az R.
a) 2. § (1) bekezdésében az „A népjóléti" szövegrész helyébe az „Az egészségügyért felelős" szöveg,
b) 5. § (6) bekezdésében az „egészségügyi hatósági elrendelésre" szövegrész helyébe az „az egészségügyi államigazgatási szerv elrendelésére" szöveg,
c) 15. § (2) bekezdés e) és f) pontjában a „rendelő helye" szövegrész helyébe a „rendelő székhelye" szöveg,
d) 16. § (4) bekezdés a) pontjában az „egészségügyi miniszternek" szövegrész helyébe az „egészségügyért felelős miniszternek" szöveg,
e) 41. § (2) bekezdés c) pontjában a „regionális intézetének" szövegrész helyébe a „regionális intézetnek" szöveg,
f) 41. § (4) bekezdés f) pontjában a „regionális intézetének" szövegrész helyébe a „regionális intézetnek" szöveg
lép.

(3) Hatályát veszti az R.
   a) 3. § (1) bekezdésében a „területileg illetékes" szövegrész,
   b) 5. § (10) bekezdése,
   c) 8. § (5) bekezdésében a „területileg illetékes" szövegrész,
   d) 8. § (8) bekezdésében a „területileg illetékes" szövegrész,
   e) 15. § (1) bekezdés b) pontjában a „területileg illetékes" szövegrész,
   f) 16. § (1) bekezdés a) pontjában az „illetékességi területén" szövegrész,
   g) 16. § (1) bekezdés f) pontjában a „határozattal" szövegrész,
   h) 16. § (2) bekezdés a) pontjában az „illetékességi területén" szövegrész,
   i) 19. § (10) bekezdésében a „területileg illetékes" szövegrész,
   j) 21. § (1) bekezdésében a „területileg illetékes" szövegrész,
   k) 29. § (2) bekezdésében a „határozattal" szövegrész,
   l) 30. § (1) bekezdésében a „határozattal" szövegrész,
   m) 30. § (5) bekezdésében a „határozattal" szövegrész,
   n) 33. § (1) bekezdésében a „határozattal" szövegrész,
   o) 36. § (1) bekezdésében az „az Eütv. 73. § (1) bekezdése szerint" szövegrész,
   p) 36. § (5) bekezdésében a „határozattal" szövegrész,
   q) 36. § (6) bekezdésében a „határozatban" szövegrész,
   r) 37. § (4) bekezdésében a „határozatban" szövegrész.

(4) A háziorvosi szolgálat a betegforgalmi tevékenység külön jogszabály szerinti jelentése alapján, új influenzavírus elleni védőoltással történő immunizálásért oltásonként 200 forintra jogosult, melyet az Egészségügyi Minisztérium és az Országos Egészségbiztosítási Pénztár között létrejött megállapodásban foglaltaknak megfelelően az Országos Egészségbiztosítási Pénztár utal.

(5) Az 1–10. §, valamint az (1)–(3) bekezdés az e rendelet hatálybalépését követő napon hatályát veszti. E bekezdés az e rendelet hatálybalépését követő második napon hatályát veszti.

Dr. Székely Tamás s. k.,
egészségügyi miniszter

A földművelésügyi és vidékfejlesztési miniszter 132/2009. (X. 14.) FVM rendelete az Európai Mezőgazdasági Garancia Alapból finanszírozott egységes területalapú támogatás (SAPS), valamint az ahhoz kapcsolódó kiegészítő nemzeti támogatások (top up) 2009. évi igénybevételével kapcsolatos egyes kérdésekről szóló 37/2009. (IV. 3.) FVM rendelet egyes jogcímeihez kapcsolódó támogatási összegekről

A mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 81. § (3) bekezdés a) pontjában kapott felhatalmazás alapján, a földművelésügyi és vidékfejlesztési miniszter feladat- és hatásköréről szóló 162/2006. (VII. 28.) Korm. rendelet 1. § a) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

I. FEJEZET
EGYSÉGES TERÜLETALAPÚ TÁMOGATÁS

1. § Az Európai Mezőgazdasági Garancia Alapból finanszírozott egységes területalapú támogatás (SAPS), valamint az ahhoz kapcsolódó kiegészítő nemzeti támogatások (top up) 2009. évi igénybevételével kapcsolatos egyes kérdésekről szóló 37/2009. (IV. 3.) FVM rendelet (a továbbiakban: R.) alapján járó egységes területalapú támogatás jogcímen hektáronként legfeljebb 42 941,60 Ft vehető igénybe. A támogatásra jogosult országos bázisterület nagysága

4 829 000 ha. A támogatási keretek túllépése esetén az igényelt támogatás összege – az érintett mezőgazdasági termelőnél a túllépés mértékével megegyezően – arányos visszaosztás alkalmazásával csökkentésre kerül.

II. FEJEZET
EGYSÉGES TERÜLETALAPÚ TÁMOGATÁSHOZ KAPCSOLÓDÓ KIEGÉSZÍTŐ NEMZETI TÁMOGATÁS

Hízottbika-támogatás

2. § Az R. 25. §-a alapján történelmi bázis jogosultságonként legfeljebb 56 000 Ft támogatás vehető igénybe.

Tejtámogatás

3. § Az R. 26. §-a alapján a tejtermelő történelmi bázis jogosultságonként legfeljebb 8,30 Ft támogatásra jogosult.

Anyatehéntartás támogatása

4. § Az R. 28–32. §-a alapján anyatehenenként – termeléshez kötötten – legfeljebb 30 000 Ft, az R. 27. §-a alapján termeléstől elválasztva – történelmi bázis jogosultságonként – legfeljebb 18 000 Ft támogatás vehető igénybe.

Extenzifikációs szarvasmarha-támogatás

5. § Az R. 33. §-a alapján történelmi bázis jogosultságonként legfeljebb 18 500 Ft támogatás vehető igénybe.

Anyajuhtartás támogatása

6. § Az R. 34–38. §-a alapján anyajuhok után, egyedenként legfeljebb 1700 Ft támogatás vehető igénybe. Ha a mezőgazdasági termelő juhtejet vagy juhtejterméket értékesít, akkor a támogatás mértéke az anyajuhok után, egyedenként legfeljebb 1400 Ft.

Kedvezőtlen adottságú területeken nyújtandó anyajuh kiegészítő támogatás

7. § Az R. 39. §-a alapján történelmi bázis jogosultságonként legfeljebb 1600 Ft anyajuh kiegészítő támogatás vehető igénybe.

Dohánytermesztés támogatása

8. § (1) Az R. 43–47. §-a alapján a Burley dohány termesztése támogatásának keretében termeléshez kötötten – hektáronként – legfeljebb 750 000 Ft, az R. 48. §-a alapján termeléstől elválasztva – történelmi bázis jogosultságonként – legfeljebb 300 000 Ft támogatás vehető igénybe.

(2) Az R. 43–47. §-a alapján a Virginia dohány termesztése támogatásának keretében termeléshez kötötten – hektáronként – legfeljebb 940 000 Ft, az R. 48. §-a alapján termeléstől elválasztva – történelmi bázis jogosultságonként – legfeljebb 380 000 Ft támogatás vehető igénybe.

Héjas gyümölcsűek termesztésének támogatása

9. § Az R. 49. §-a alapján héjas gyümölcsűek termesztésének támogatása jogcímen hektáronként legfeljebb 32 000 Ft támogatás vehető igénybe.

Rizs termesztésének támogatása

10. § Az R. 50–52. §-a alapján a rizs termesztésének támogatása jogcímen termeléshez kötötten – hektáronként – legfeljebb 62 000 Ft, termeléstől elválasztva – történelmi bázis jogosultságonként – legfeljebb 25 000 Ft támogatás vehető igénybe.

11. § (1) Ez a rendelet a kihirdetése napján lép hatályba.

(2) Hatályát veszti az Európai Mezőgazdasági Garancia Alapból finanszírozott egységes területalapú támogatás (SAPS) 2008. évi igénybevételével kapcsolatos egyes kérdésekről szóló 39/2008. (III. 29.) FVM rendelet és az Európai Mezőgazdasági Garancia Alapból finanszírozott egységes területalapú támogatásokhoz (SAPS) kapcsolódó 2008. évi kiegészítő nemzeti támogatások (top up) igénybevételével kapcsolatos egyes kérdésekről szóló 42/2008. (IV. 4.) FVM rendelet egyes jogcímeihez kapcsolódó támogatási összegekről szóló 107/2008. (VIII. 27.) FVM rendelet azzal, hogy rendelkezéseit a folyamatban lévő ügyekben alkalmazni kell.

12. § (1) Az R. a 22. §-át követően a következő alcímmel és 22/A. §-sal egészül ki:

„**Levonások, kizárások**

22/A. § A kölcsönös megfeleltetés ellenőrzései megállapításaihoz kapcsolódó levonások az e rendeletben meghatározott kiegészítő nemzeti támogatásokra nem alkalmazandók. Ha a termelőnél a kölcsönös megfeleltetés ellenőrzései során olyan mértékű szándékos meg nem felelés kerül megállapításra, hogy emiatt a termelőt az egységes területalapú támogatásból kizárják, akkor a támogatásból való kizárás alkalmazandó valamennyi, e rendeletben meghatározott kiegészítő nemzeti támogatásra is."

(2) Az R. 25. § (4) bekezdése helyébe a következő rendelkezés lép:

„(4) Ha a mezőgazdasági termelő más szarvasmarhatartás-támogatásban is részt vesz, az ellenőrzések során a támogatási feltételeknek való meg nem felelés esetén a támogatási összeg meghatározására, kizárólag az áthúzódó szankció levonása tekintetében, a 796/2004/EK bizottsági rendelet 57., 59. és 69. cikke szerinti eljárást kell alkalmazni."

(3) Az R. 27. § (4) bekezdése helyébe a következő rendelkezés lép:

„(4) Ha a mezőgazdasági termelő más szarvasmarhatartás-támogatásban is részt vesz, az ellenőrzések során a támogatási feltételeknek való meg nem felelés esetén a támogatási összeg meghatározására, kizárólag az áthúzódó szankció levonása tekintetében, a 796/2004/EK bizottsági rendelet 57., 59. és 69. cikke szerinti eljárást kell alkalmazni."

13. § A kölcsönös megfeleltetés körébe tartozó ellenőrzések lefolytatásával, valamint a jogkövetkezmények alkalmazásával kapcsolatos szabályokról szóló 81/2009. (VII. 10.) FVM rendelet 1. § (2) bekezdés felvezető szövegrésze helyébe a következő rendelkezés lép:

„A kölcsönös megfeleltetési szabályok betartását az Európai Mezőgazdasági Vidékfejlesztési Alapból és az Európai Mezőgazdasági Garancia Alapból finanszírozott alábbi intézkedésekben részt vevő ügyfelek esetében kell vizsgálni:"

14. § (1) A 11. § (2) bekezdése 2011. december 31-én hatályát veszti.

(2) Hatályát veszti az R. 41. § (2) bekezdése.

15. § A 12–14. § 2012. január 1-jén hatályát veszti. E § 2012. január 2-án hatályát veszti.

Gráf József s. k.,
földművelésügyi és vidékfejlesztési miniszter

A földművelésügyi és vidékfejlesztési miniszter 133/2009. (X. 14.) FVM rendelete az Európai Mezőgazdasági Vidékfejlesztési Alapból a mezőgazdasági termelők gazdaságátadásához nyújtandó támogatás részletes feltételeiről szóló 83/2007. (VIII. 10.) FVM rendelet módosításáról

A mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 81. § (3) bekezdés a) pontjában kapott felhatalmazás alapján, a földművelésügyi és vidékfejlesztési miniszter feladat- és hatásköréről szóló 162/2006. (VII. 28.) Korm. rendelet 1. § a) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § Az Európai Mezőgazdasági Vidékfejlesztési Alapból a mezőgazdasági termelők gazdaságátadásához nyújtandó támogatás részletes feltételeiről szóló 83/2007. (VIII. 10.) FVM rendelet (a továbbiakban: R.) 2. §-ának helyébe a következő rendelkezés lép:

„2. § E rendelet alkalmazásában:

1. *saját jogú nyugellátás:* a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény 6. § (1) és (4) bekezdése szerinti nyugellátás,

2. *segítő családtag:* a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 4. § g) pontjában ekként meghatározott fogalom,

3. *munkavállaló:* aki nem minősül egyéni, illetve társas vállalkozónak, és biztosítással járó jogviszony keretében, mezőgazdasági tevékenység végzésére foglalkoztatják,

4. *állategység:* az egységes területalapú támogatások és egyes vidékfejlesztési támogatások igényléséhez teljesítendő „Helyes Mezőgazdasági és Környezeti Állapot" fenntartásához szükséges feltételrendszer, valamint az állatok állategységre való átváltási arányának meghatározásáról szóló 50/2008. (IV. 24.) FVM rendelet 5. számú mellékletében meghatározott technikai mértékegység,

5. *gazdaság:* a támogatási kérelem benyújtásakor az átadó tulajdonában, illetve használatában lévő termőföld, állatállomány, továbbá a mezőgazdasági termelő tevékenységhez kapcsolódó kvóták, támogatási jogosultságok és kötelezettségek összessége,

6. *átadás időpontja:* a kifizetési kérelem benyújtásának időpontja,

7. *főtevékenység:* az egyéni vállalkozói igazolványban főtevékenységként megjelölt, a gazdasági tevékenységek egységes ágazati osztályozási rendszeréről kiadott TEÁOR'03 és TEÁOR'08 közötti fordítókulcsról szóló 9002/2007. (SK. 3.) KSH Közlemény (a továbbiakban: TEÁOR'08) szerinti 0111-0150 és 0170 tevékenység,

8. *üzleti célú növénytermesztési, állattenyésztési, vegyes gazdálkodási mezőgazdasági tevékenység:* a TEÁOR'08 szerinti 0111-0170 tevékenység."

2. § (1) Az R. 3. § (1) bekezdés a) pont aa) alpontja helyébe a következő rendelkezés lép:

[E rendelet alapján jövedelempótló típusú támogatást vehet igénybe

a) aki mezőgazdasági termelő tevékenységet végez, és]

„aa) a TEÁOR'08 szerinti 0111-0150 tevékenységet végző egyéni vállalkozó, vagy"

(2) Az R. 3. §-a a következő (3) bekezdéssel egészül ki:

„(3) Az Európai Mezőgazdasági Vidékfejlesztési Alap társfinanszírozásában megvalósuló támogatások igénybevételének általános szabályairól szóló 23/2007. (IV. 17.) FVM rendelet (a továbbiakban: Vhr.) 10. §-ától eltérően a támogatás nem ruházható át kötelezettségátadás, illetve jogutódlás keretében."

3. § (1) Az R. 4. § (3) bekezdés b) pontja helyébe a következő rendelkezés lép:

[Az üzemméret számításánál az átadó gazdaságából figyelembe vehető:]

„b) az az állatállomány,

ba) amely a támogatási kérelem benyújtásakor az átadó gazdálkodó tulajdonában van,

bb) amely a kifizetési kérelem benyújtásáig az átvevő tulajdonába átkerül, de a kifizetési kérelemben figyelembe vett állatlétszámból számított EUME érték nem haladhatja meg a támogatási kérelem benyújtásakor meglévő állatlétszámból számított EUME értéket, és

bc) amelyre vonatkozóan az átadó a tartási helyek, a tenyészetek és az ezekkel kapcsolatos egyes adatok országos nyilvántartási rendszeréről szóló 119/2007. (X. 18.) FVM rendelet alapján vezetett nyilvántartásban az állatállomány tartójaként szerepel, valamint eleget tesz

1. a szarvasmarhafélékre vonatkozóan a szarvasmarha-fajok egyedeinek jelöléséről, valamint Egységes Nyilvántartási és Azonosítási Rendszeréről szóló 99/2002. (XI. 5.) FVM rendeletben előírt,

2. a lófélékre vonatkozóan az egyes állatfajok egyedeinek Egységes Nyilvántartási és Azonosítási Rendszeréről szóló 29/2000. (VI. 9.) FVM rendeletben előírt,

3. a juh-, kecskefajokra vonatkozóan a juh- és kecskefajok egyedeinek Egységes Nyilvántartási és Azonosítási Rendszeréről szóló 47/2005. (V. 23.) FVM rendeletben előírt, az állatállományra vonatkozó bejelentési kötelezettségeknek."

(2) Az R. 4. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) A támogatási összeg alapját képező, átadásra került földterületekre vonatkozó EUME értéket a (3) bekezdés a) pont aa) alpontjában meghatározott időszak hasznosítási típusa alapján, a két év hasznosítási típusának területe szerint súlyozott átlagával kell megállapítani."

(3) Az R. 4. §-a a következő (5) bekezdéssel egészül ki, egyidejűleg az eredeti (5)–(7) bekezdések számozása (6)–(8) bekezdésekre változik:
„(5) A támogatási összeg alapját képező, átadásra került állatállományra vonatkozó EUME érték a támogatási kérelemben megadott állatlétszám alapján kalkulált, és a kifizetési kérelemben jelölt, átadásra került állatlétszám alapján számolt alacsonyabb EUME érték."

4. § (1) Az R. 5. § (1) bekezdés d)–h) pontjai helyébe a következő rendelkezések lépnek:
[Az átadó gazdálkodó akkor jogosult támogatásra, ha]
„d) a támogatási kérelem benyújtásakor legalább 3 hektár földterületen gazdálkodik;
e) a támogatási kérelem benyújtásakor a tulajdonában lévő termőföldet – kivéve az önellátásra szolgáló földterületet – a kifizetési kérelem benyújtásáig az átvevőre per- és igénymentesen átruházza, továbbá a haszonbérletet végleg megszünteti;
f) a kifizetési kérelem benyújtásáig átadja az 1. számú mellékletben meghatározott önellátást biztosító mennyiségen felüli állatállományt;
g) legkésőbb a kifizetési kérelem hiánypótlásának benyújtásáig kezdeményezi a gazdaságban végzett mezőgazdasági termelő tevékenységhez kapcsolódó kvóták, támogatási jogosultságok és kötelezettségek átruházását;
h) a kifizetési kérelem benyújtásáig véglegesen felhagy minden – az önellátásra történő termelés kivételével – üzleti célú növénytermesztési, állattenyésztési, vegyes gazdálkodási mezőgazdasági tevékenységgel;"

(2) Az R. 5. § (3) bekezdés e) pontja helyébe a következő rendelkezés lép:
[Az átadó gazdálkodó munkavállalója akkor jogosult támogatásra, ha]
„e) a kifizetési kérelem benyújtásáig véglegesen felhagy az üzleti célú mezőgazdasági tevékenységgel és a mezőgazdasági munkavállalással."

(3) Az R. 5. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) A támogatás igénybevételének további feltétele, hogy a gazdaságot egy olyan természetes személy vegye át, aki
a) egyéni vállalkozóként főtevékenységet végez vagy kíván végezni, és ezt legkésőbb a kifizetési kérelemhez csatolt egyéni vállalkozói igazolványának hiteles másolatával igazolja,
b) az átadás időpontjában még nem tölti be a 40. életévét,
c) az Európai Mezőgazdasági Vidékfejlesztési Alapból a fiatal mezőgazdasági termelők indulásához a 2009. évtől nyújtandó támogatások részletes feltételeiről szóló 113/2009. (VIII. 29.) FVM rendelet [a továbbiakban: 113/2009. (VIII. 29.) FVM rendelet] 1–4. számú mellékleteiben meghatározott végzettségek valamelyikével rendelkezik, valamint
d) az átvételt a gazdaság méretének növelése céljából valósítja meg."

5. § (1) Az R. 7. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) A támogatási kérelmet 2010. március 1. és március 31. között lehet benyújtani."

(2) Az R. 7. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) Egy támogatási kérelmet kell benyújtani akkor is, ha egy gazdaságot több gazdálkodó ad át, vagy ha a támogatást az átadó gazdálkodó munkavállalója is kérelmezi. Ilyen esetekben a támogatási kérelmet a kérelmezők egymás közül választott képviselő útján nyújtják be."

(3) Az R. 7. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) A támogatási kérelmet a Mezőgazdasági és Vidékfejlesztési Hivatal (a továbbiakban: MVH) honlapján közzétett formanyomtatványon postai úton, vagy az MVH honlapján keresztül elektronikus úton is be lehet nyújtani az MVH-hoz."

(4) Az R. 7. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) A (3) bekezdés szerinti formanyomtatvány az alábbi adatokat tartalmazza:
a) az átvevő ügyfél végzettségére vonatkozó adatok,
b) az átadó gazdálkodó nyilatkozata arról, hogy nem részesül saját jogú nyugellátásban,
c) a munkavállaló nyilatkozata arról, hogy nem részesül saját jogú nyugellátásban,
d) az átadó gazdálkodó nyilatkozata arról, hogy az átadást követően felhagy minden üzleti célú növénytermelési, állattenyésztési, vegyes-gazdálkodási mezőgazdasági tevékenységgel,
e) a munkavállaló nyilatkozata arról, hogy véglegesen felhagy az üzleti célú mezőgazdasági tevékenységgel és mezőgazdasági munkavállalással,
f) az átadó gazdálkodó által átadásra kerülő saját tulajdonú termőföldre, az állatállományra, valamint a gazdaság részét képező, de a támogatásba be nem vonható földterületre vonatkozó adatok,
g) az átvevő gazdálkodó nyilatkozata arról, hogy az átvétel a meglévő gazdaság méretének növelése céljából történik."

(5) Az R. 7. § (5) bekezdés d) pontja helyébe a következő rendelkezés lép:
[A támogatási kérelemhez mellékelni kell:]
„d) a 3. számú melléklet szerinti, a támogatási kérelemhez szükséges igazolásokat, okiratokat."

6. § Az R. 8. §-ának helyébe a következő rendelkezés lép:
„8. § A támogatási kérelmet az MVH bírálja el, és a 2. számú mellékletben meghatározott pontozási rendszer alapján végzett értékeléssel, valamint a Tv. 32. § (1) bekezdés c) pontja szerinti rangsor állításával hoz döntést."

7. § (1) Az R. 9. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) Kifizetési kérelmet a támogatási kérelmet jóváhagyó határozat jogerőre emelkedésétől számítva legkésőbb a második kifizetési időszak végéig, 2009-ben november 2. és december 1. között, 2010-től évente február 1. és február 28., valamint augusztus 1. és augusztus 31. között lehet benyújtani az MVH honlapján közzétett formanyomtatványon. Egy kifizetési kérelmet kell benyújtani – a 7. § (2) bekezdése alapján választott képviselő útján – akkor is, ha egy gazdaságot több gazdálkodó ad át, vagy ha a támogatást az átadó gazdálkodó munkavállalója is kérelmezi. A formanyomtatványnak tartalmaznia kell a kötelezettségek teljesítését igazoló adatokat."

(2) Az R. 9. § (2) bekezdés a)–d) pontjai helyébe a következő rendelkezések lépnek:
[A kifizetési kérelemhez mellékelni kell:]
„a) az átadó gazdálkodó 30 napnál nem régebbi teljes földhasználati lapját,
b) a Mezőgazdasági Szakigazgatási Hivatalnak (a továbbiakban: MgSzH) a kérelmező lakóhelye szerint illetékes területi szerve által kiállított hatósági bizonyítvány hiteles másolatát arról, hogy a mezőgazdasági őstermelői igazolványról szóló 228/1996. (XII. 26.) Korm. rendelet 4. § (2) bekezdése alapján az őstermelői igazolvány visszavonásra került, illetve az egyéni vállalkozói igazolvány hiteles másolatát, melyből törlésre került a TEÁOR'08 szerinti 0111-0170 tevékenység,
c) az átadó gazdálkodó munkavállalójára vonatkozóan az MgSzH-nak a munkavállaló lakóhelye szerint illetékes területi szerve által kiadott hatósági bizonyítványt arról, hogy a munkavállaló nem rendelkezik őstermelői igazolvánnyal,
d) az átvevő egyéni vállalkozói igazolványának hiteles másolatát,"

(3) Az R. 9. § (2) bekezdése a következő e)–f) pontokkal egészül ki:
[A kifizetési kérelemhez mellékelni kell:]
„e) az átadó gazdálkodó nyilatkozatát a megtartott földterület nagyságáról, illetve a megtartott állatállományról és tartási helyéről,
f) az átvevő gazdálkodó 30 napnál nem régebbi teljes földhasználati lapját."

(4) Az R. 9. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) A támogatás folyósítása az átadás időpontjától naptári év szerint negyedévente, a kifizetés alapjául szolgáló negyedévet követően történik. Az átadás időpontjától függően a kifizetés első és utolsó részlete nem teljes negyedévre is vonatkozhat."

(5) Az R. 9. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) A kifizetés feltétele, hogy az átadott támogatási jogosultságoknak és kötelezettségeknek, valamint kvótáknak az átvevőre történő átruházására vonatkozó kérelmét a külön jogszabályokban meghatározottak szerint az átadó gazdálkodó legkésőbb a kifizetési kérelem hiánypótlásáig benyújtsa az MVH-hoz.”

8. § (1) Az R. 1. számú melléklete helyébe az 1. melléklet lép.
(2) Az R. 2. számú melléklete a 2. melléklet szerint módosul.
(3) Az R. 3. számú melléklete helyébe a 3. melléklet lép.

9. § (1) Ez a rendelet a kihirdetése napján lép hatályba.
(2) Az R. e rendelettel megállapított rendelkezései – a (3) bekezdésben meghatározott kivétellel – az e rendelet hatálybalépését követően benyújtott kérelmek esetében alkalmazhatók.
(3) Az R. e rendelettel megállapított 2. § 6. pontjában, 5. § (1) bekezdés e) és g) pontjaiban, valamint 9. § (1) bekezdésében foglalt szabályokat a 2007. december 3. és 2008. január 15. között benyújtott támogatási kérelmekhez kapcsolódó kifizetési kérelmek esetében is alkalmazni kell.
(4) Az R. 6. §-a és az R. 7. § (5) bekezdés a) pontja hatályát veszti.

10. § Az Európai Mezőgazdasági Vidékfejlesztési Alapból a fiatal mezőgazdasági termelők indulásához a 2009. évtől nyújtandó támogatások részletes feltételeiről szóló 113/2009. (VIII. 29.) FVM rendelet 5. § (1) bekezdése helyébe a következő rendelkezés lép:
„(1) A támogatási kérelmet évente szeptember 15. és október 31. között postai úton lehet benyújtani az MVH honlapján közzétett formanyomtatványon az MVH-hoz.”

11. § Az 1–8. §, a 9. § (4) bekezdése, a 10. §, valamint az 1–3. melléklet az e rendelet hatálybalépését követő napon hatályát veszti. Ez a § az e rendelet hatálybalépését követő napon hatályát veszti.

Gráf József s. k.,
földművelésügyi és vidékfejlesztési miniszter

1. melléklet a 133/2009. (X. 14.) FVM rendelethez
„1. számú melléklet a 83/2007. (VIII. 10.) FVM rendelethez

Önellátásra megtartható állatok

Megtartható állategység összesen: 8 ÁE tetszőleges állatfajonkénti eloszlásban, de legfeljebb

Állatfaj	Megtartható állategység
Szarvasmarha	3
Bivaly	3
Juh	3
Kecske	3
Sertés	3
Tojótyúk	1
Egyéb baromfi	1
Nyúl	1

Megtartható 4 méhcsalád, a lófélék korlátozás nélkül megtarthatók.
1 db nyúl 0,02 ÁE-nek felel meg.”

2. melléklet a 133/2009. (X. 14.) FVM rendelethez

Az R. 2. számú mellékletében szereplő „Értékelési szempontok" táblázat „Horizontális szempontok" rész a „Termelői szervezeti tagság az átvevő tagsága", valamint „Az átvevő végzettsége" sorai helyébe a következő rendelkezések lépnek:

„Termelői szervezeti tagság az átvevő tagsága	Az MVH honlapján közzétett formanyomtatványon benyújtott elismert termelői csoport, zöldség-gyümölcs termelői csoport vagy termelői szervezet által kiadott igazolást arról, hogy az átvevő a csoport tagja.	4 pont
Az átvevő végzettsége	A 113/2009. (VIII. 29.) FVM rendelet 2–4. számú mellékleteiben meghatározott felsőfokú agrár végzettség. Csatolni kell a felsőfokú oktatási intézményben szerzett oklevél, diploma hiteles másolatát.	10 pont"

3. melléklet a 133/2009. (X. 14.) FVM rendelethez

„3. számú melléklet a 83/2007. (VIII. 10.) FVM rendelethez

A támogatás iránti kérelemhez szükséges igazolások listája

A) A gazdaságot átadó mezőgazdasági termelőre vonatkozóan

Az átadó a támogatási kérelem benyújtását megelőző 10 év során folytatott mezőgazdasági termelő tevékenységének igazolására szolgáló dokumentumok az alábbiak:

– egyéni vállalkozói igazolvány hiteles másolata, amely tartalmazza a TEÁOR'08 szerinti 0111-0150 növénytermelési, állattenyésztési, vegyes gazdálkodási tevékenységet,

– őstermelői igazolvány hiteles másolata, értékesítési betétlapokkal együtt,

– a Mezőgazdasági és Szakigazgatási Hivatal területi szerve által – a falugazdász a tevékenysége során szerzett információja alapján – a kérelmező mezőgazdasági termelő tevékenység folytatásáról kiadott hatósági bizonyítványa,

– munkavállalóként végzett mezőgazdasági termelő tevékenység igazolása munkakör megjelölését is tartalmazó munkaszerződés másolatával és egyéb dokumentummal, illetve

– adott évre vonatkozó Nyugdíjbiztosítási Egyéni Nyilvántartó Lap (a továbbiakban: NYENYI lap) másolata

B) A gazdaságot átadó munkavállalójára vonatkozóan

Igazolás, hogy a támogatási kérelem benyújtását megelőző öt év során munkaidejének legalább a felét mezőgazdasági munkával, az átadó gazdálkodó gazdaságában töltötte:

– a kérelem benyújtását megelőző öt évre vonatkozó NYENYI lap másolata, illetve

– mezőgazdasági termelő tevékenység igazolása munkakör megjelölését is tartalmazó munkaszerződés másolatával és egyéb dokumentummal

C) A gazdaságot átvevő természetes személyre vonatkozóan

– az 5. § (4) bekezdés c) pontjában meghatározott végzettséget igazoló dokumentum hiteles másolata"

A földművelésügyi és vidékfejlesztési miniszter 134/2009. (X. 14.) FVM rendelete a szőlőültetvények szerkezetátalakítására és -átállítására vonatkozó szabályozásról szóló 161/2008. (XII. 18.) FVM rendelet módosításáról

A mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 81. § (3) bekezdés a) és b) pontjában, a szőlőtermesztésről és a borgazdálkodásról szóló 2004. évi XVIII. törvény 57. § (1) bekezdés b), d), e), g), h), i), j), m) pontjaiban, valamint a hegyközségekről szóló 1994. évi CII. törvény 65. § b) és c) pontjaiban kapott felhatalmazás alapján, a földművelésügyi és vidékfejlesztési miniszter feladat- és hatásköréről szóló 162/2006. (VII. 28.) Korm. rendelet 1. § a) pontjában meghatározott feladatkörömben eljárva, a következőket rendelem el:

1. § A szőlőültetvények szerkezetátalakítására és -átállítására vonatkozó szabályozásról szóló 161/2008. (XII. 18.) FVM rendelet (a továbbiakban: R.) 4. § (2)–(4) bekezdései helyébe a következő rendelkezések lépnek:

„(2) A mezőgazdasági piacok közös szervezésének létrehozásáról, valamint egyes mezőgazdasági termékekre vonatkozó egyedi rendelkezésekről (az egységes közös piacszervezésről szóló rendelet), 2007. október 22-i 1234/2007/EK tanácsi rendelet (a továbbiakban: Tanácsi rendelet) 103k. cikk szerint elkészített és az Európai Bizottság részére benyújtott Nemzeti Támogatási Program 1. számú mellékletében foglaltaknak megfelelően a 2009/2010. borpiaci évre vonatkozóan az e rendelet alapján kifizethető támogatási keretösszegről az agrárpolitikáért felelős miniszter (a továbbiakban: miniszter) tájékoztatja a Mezőgazdasági és Vidékfejlesztési Hivatalt (a továbbiakban: MVH), amely a keretösszegről közleményt tesz közzé.

(3) A támogatási keretösszeg meghatározásakor a forintra történő átszámítást a támogatás kifizetésének borpiaci éve első napján érvényes, az Európai Központi Bank által jegyzett forint/euró átváltási árfolyam alapján kell elvégezni.

(4) Az MVH a kifizetéseket úgy teljesíti, hogy 2010. október 15-ig az összes kifizetés átlaga a 12 500 euró/ha összeget ne haladja meg."

2. § (1) Az R. 5. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A támogatás igénybevételének feltétele, hogy a hegyközségi tanács Borvidéki tervet készítsen a 3. számú melléklet szerint."

(2) Az R. 5. § (2) bekezdésének a) pontja helyébe a következő rendelkezés lép:

[A Borvidéki terv tartalmazza:]

„a) tevékenységenkénti bontásban a borkészítésre alkalmas szőlőfajták osztályba sorolásáról szóló 98/2009. (VII. 30.) FVM rendeletben engedélyezett kategóriába sorolt, illetve a borvidéki rendtartás szerinti azon szőlőfajtákat, amelyekre támogatás igényelhető,"

(3) Az R. 5. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) A fajtalista összeállításánál, illetve a művelésmódok meghatározásánál figyelembe kell venni azokat az ökológiai, termesztéstechnológiai feltételeket, amelyek alapján biztosítható a magasabb minőségi követelményeknek való megfelelés vagy a nagyobb piaci keresettségű borászati termék készítése. A Borvidéki tervben szerepeltethetők azok a szőlőfajták is, amelyeket a szőlőtermesztésről és a borgazdálkodásról szóló 2004. évi XVIII. törvény 2. § 9. pontjának megfelelően a minőségi bortermelést szolgáló kísérleti ültetvény létesítésére szánnak."

(4) Az R. 5. § (5) bekezdése helyébe a következő rendelkezés lép:

„(5) A szerkezetátalakítás során kialakítható sortávolság nem lehet kevesebb 1 méternél, illetve több 3,5 méternél. A szerkezetátalakítás során kialakítható tőtávolság nem lehet kevesebb 0,6 méternél, illetve több 1,2 méternél. Ikersoros ültetvények esetén az átlagos sortávolságot kell figyelembe venni."

3. § Az R. 6. § (2)–(4) bekezdései helyébe a következő rendelkezések lépnek:

„(2) A HNT a véleményével ellátott Borvidéki tervet minden év május 15-ig átadja a miniszter részére jóváhagyásra.

(3) Az 5. § (2)–(6) bekezdéseiben foglaltaknak nem megfelelő Borvidéki tervek hiányosságainak pótlására 2010. június 30-ig van lehetőség. A Borvidéki terveket a miniszter hagyja jóvá, és a miniszter döntését 2010. július 15-ig közli az MVH-val és HNT-vel. A miniszter által jóvá nem hagyott Borvidéki tervek alapján támogatás nem igényelhető.

(4) Az MVH a Borvidéki terveket a miniszter döntésének közlését követő hét munkanapon belül a honlapján közzéteszi."

4. § Az R. 7. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) Az Egyéni tervben szerepeltetni kell a hegybíró arra vonatkozó nyilatkozatát, hogy az Egyéni terv megfelel a Borvidéki tervben foglaltaknak.”

5. § Az R. 8. §-a helyébe a következő rendelkezés lép:
„8. § (1) Támogatási, illetve előzetes kifizetés iránti kérelmet nyújthat be az a természetes személy vagy gazdálkodó szervezet, aki (amely) a szerkezetátalakításban részesíteni kívánt (részesített) ültetvény használója.
(2) A támogatási kérelem az alábbi adatokat tartalmazza:
a) a kérelmező azonosításához szükséges adatok (ügyfél regisztrációs szám, név, cím, kapcsolattartási információk);
b) a tevékenység megjelölése;
c) a tevékenységgel érintett ültetvény részletezése (borvidék, helység, helyrajzi szám, a helyrajzi számhoz tartozó telepítési engedély száma, a tevékenységgel érintett területnagyság);
d) a tevékenység végrehajtása során elvégzett műveletek.
(3) Az előzetes kifizetés iránti kérelem az alábbi adatokat tartalmazza:
a) a kérelmező azonosításához szükséges adatok (ügyfél regisztrációs szám, név, cím, kapcsolattartási információk);
b) a tevékenység megjelölése;
c) nyilatkozat a támogatási kérelem következő borpiaci évre történő átviteléről;
d) a tevékenységgel érintett ültetvény részletezése (borvidék, helység, helyrajzi szám, a helyrajzi számhoz tartozó telepítési engedély száma, a tevékenységgel érintett területnagyság);
e) a tevékenység végrehajtása során elvégezni kívánt műveletek.”

6. § (1) Az R. 9. § h) pontja helyébe a következő rendelkezés lép:
[Nem igényelhető támogatás az olyan ültetvényre,]
„h) amelyet nem érvényes vagy hatályos telepítési engedély alapján telepítettek,”
(2) Az R. 9. §-a a következő k) ponttal egészül ki:
[Nem igényelhető támogatás az olyan ültetvényre,]
„k) amelyre vonatkozóan kiállított telepítési engedélyhez igénybe vett újratelepítési jog termőhelyi kataszteri osztálya vagy pontértéke az MVH által vezetett, külön jogszabály által meghatározott nyilvántartásban nem szerepel.”

7. § (1) Az R. 10. § (2) és (3) bekezdései helyébe a következő rendelkezések lépnek:
„(2) A támogatási kérelmeket 2009. december 1. és 2010. április 30. közötti időszakban lehet benyújtani, a benyújtás időpontjának a kérelem postára adásának napja minősül.
(3) A kérelmeket az MVH Központ honlapján közzétett formanyomtatványon kell benyújtani.”
(2) Az R. 10. § (4) bekezdésének j) pontja helyébe a következő rendelkezés lép:
[A támogatási kérelemhez csatolni kell:]
„j) szaporítóanyag-felhasználás esetén a felhasznált szaporítóanyagra vonatkozó származási igazolás másolatát,”

8. § Az R. 11. § (3) bekezdése helyébe a következő rendelkezés lép:
„(3) A 16. § (4) bekezdése szerinti két borpiaci év alatt történő végrehajtás esetén a második borpiaci évre benyújtott kérelemhez nem kell mellékelni a 10. § (4) bekezdés a)–f) és h) pontjaiban meghatározott dokumentumokat.”

9. § Az R. 12. § (2) és (3) bekezdései helyébe a következő rendelkezések lépnek:
„(2) Az előzetes kifizetés iránti kérelmeket 2009. december 1. és 2010. április 30. közötti időszakban lehet benyújtani, a benyújtás időpontjának a kérelem postára adásának napja minősül.
(3) A kérelmeket az MVH Központ honlapján közzétett formanyomtatványon kell benyújtani.”

10. § Az R. 14. §-a helyébe a következő rendelkezés lép:
„14. § (1) A biztosíték-feloldás iránti kérelmeket egy eredeti példányban postai úton az MVH PKI részére kell benyújtani.
(2) A biztosíték-feloldás iránti kérelmek benyújtásának határideje az előzetes kifizetést követő második borpiaci év vége. A benyújtás időpontjának a kérelem postára adásának napja minősül, a benyújtási határidő elmulasztása esetén a biztosíték teljes összege visszatartásra kerül.

(3) A biztosíték-feloldás iránti kérelmeket az MVH Központ által rendszeresített és honlapján közzétett formanyomtatványon kell benyújtani, amely az alábbi adatokat tartalmazza:
a) a kérelmező azonosításához szükséges adatok (ügyfél regisztrációs szám, név, cím, kapcsolattartási információk);
b) a feloldani kívánt biztosíték részletezése (a feloldani kívánt biztosíték MVH határozatának vonalkódja, a feloldani kívánt biztosíték összege).
(4) A biztosíték-feloldás iránti kérelemhez csatolni kell:
a) a tevékenységek végrehajtását követő állapotra vonatkozó ültetvényleltárt a 6. számú melléklet szerint,
b) szaporítóanyag-felhasználás esetén a felhasznált szaporítóanyagra vonatkozó származási igazolás másolatát,
c) a kérelmezőnek a 7. számú melléklet szerinti nyilatkozatát arra vonatkozóan, hogy a biztosíték-feloldás iránti kérelem jóváhagyása esetén kéri a készpénz biztosíték visszautalását, bankgarancia esetében annak megszüntetését, és az eredeti példány visszaküldését.
(5) Az MVH a biztosíték feloldásáról a helyszíni ellenőrzést követő 30 munkanapon belül dönt."

11. § Az R. 17. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) A 2. § c)–d) pontjai szerinti tevékenységekhez tartozó tőkepótlás műveletre kizárólag abban az esetben adható támogatás, amennyiben a pótolt tőkék aránya meghaladja az ültetvény tőkeállományának 5%-át."

12. § Az R. 21. §-a a következő (2) bekezdéssel egészül ki és az eredeti (2) bekezdés számozása (3) bekezdésre változik:
„(2) A támogatási keret túligénylése esetén, az (1) bekezdésben meghatározottakra tekintettel, a keretkimerülés napján beérkezett kérelmek közötti sorrend a kérelmekben szereplő területnagyság növekvő sorrendjével azonos."

13. § Az R. 22. §-a helyébe a következő rendelkezés lép:
„22. § (1) Amennyiben a 2009/2010. borpiaci év vonatkozásában benyújtott kérelmek alapján az összesített támogatási igény a 4. § (2) bekezdésben meghatározott keretösszeget meghaladja, úgy a keretösszegen felüli, jogos támogatási igényt tartalmazó, a 10. § (2) bekezdésben jelölt határidőig beérkező támogatási kérelmek kapcsán a kifizetésre 2010. október 16. után kerül sor a 2010/2011. borpiaci évre meghatározott keretösszeg terhére.
(2) A 2009/2010. borpiaci évre meghatározott keret kimerülése esetén a keretösszegen felül, a 12. § (2) bekezdésben jelölt határidőig beérkező előzetes kifizetés iránti kérelmek a következő borpiaci évre átvihetőek az előzetes kifizetés iránti kérelemben feltüntetett nyilatkozat alapján. A kifizetésre 2010. október 16. után kerül sor a 2010/2011. borpiaci évre meghatározott keretösszeg terhére.
(3) Amennyiben a kérelmező az előzetes kifizetés iránti kérelemben nem nyilatkozik arról, hogy a 4. § (2) bekezdésében megállapított támogatási keret kimerülése esetén kérelmét a következő borpiaci évre vonatkozóan is fenntartja, úgy a kereten felüli előzetes kifizetés iránti kérelem elutasításra kerül.
(4) A 21. § (1) bekezdés figyelembevételével a 2009/2010. borpiaci évre átvitt kérelmek előnyt élveznek a 2009/2010. borpiaci évben benyújtott kérelmekkel szemben.
(5) A 2009/2010. borpiaci évre meghatározott keret kimerülése esetén a kereten felül benyújtott előzetes kifizetés iránti kérelmek tekintetében az előzetes kifizetés iránti kérelemhez mellékelt, a 12. § (4) bekezdés i) pontja szerinti biztosíték visszaszolgáltatását kérheti az ügyfél az előzetes kifizetés iránti kérelem átvitelére vonatkozó döntés jogerőre emelkedését követően.
(6) A 2010/2011. borpiaci évre átvitt kérelmek előzetes kifizetési kérelmek elbírálása során az MVH a 12. § (4) bekezdés i) pontja szerinti biztosíték hiánya esetén a kérelmezőt hiánypótlásra szólítja fel. A hiánypótlást a felszólító végzés közlésétől számított 8 munkanapon belül kell teljesíteni."

14. § Az R. 24. § (2) bekezdése helyébe a következő rendelkezés lép:
„(2) Az e rendelet szerinti nyomtatványokat, a nyilatkozatmintákat, a vázrajzokat, valamint az ültetvényleltár mintáját az MVH honlapján letölthető formában közzéteszi legkésőbb 2009. december 1. napján."

15. § (1) Az R. 1. számú melléklete helyébe e rendelet 1. számú melléklete lép.
(2) Az R. 3. számú melléklete helyébe e rendelet 2. számú melléklete lép.
(3) Az R. 6. számú melléklete helyébe e rendelet 3. számú melléklete lép.
(4) Az R. e rendelet 4. számú melléklete szerinti 7. számú melléklettel egészül ki.

16. § A szőlőtermelési potenciálról szóló 86/2009. (VII. 17.) FVM rendelet [a továbbiakban: 86/2009. (VII. 17.) FVM rendelet] 4. § (4) bekezdésének g) pontja helyébe a következő rendelkezés lép:

[A kérelemhez csatolni kell:]

„g) telepítési, pótlási, fajtaváltási engedély iránti kérelemhez a külön jogszabályban előírt – öt évnél nem régebbi – ültetvénytelepítést megalapozó talajvédelmi terv másolatát, amely gyökérnemes (saját gyökerű) szaporítóanyag felhasználása esetén tartalmazza a talaj filoxéra ellenállóságának igazolását;"

17. § (1) A szőlészeti és a borászati adatszolgáltatás, valamint a származási bizonyítványok kiadásának rendjéről, továbbá a borászati termékek előállításáról, forgalomba hozataláról és jelöléséről szóló 127/2009. (IX. 29.) FVM rendelet [a továbbiakban: 127/2009. (IX. 29.) FVM rendelet] 61. § (5) bekezdése helyébe a következő rendelkezés lép:

„(5) A 31. § (2) bekezdését a 67. § (1) bekezdésében meghatározott borok esetében 2010. január 1-jétől kell alkalmazni."

(2) A 127/2009. (IX. 29.) FVM rendelet 10. és 11. számú mellékleteiben a „479/2008/EK tanácsi rendelet IV. számú melléklete" szövegrész helyébe az „1234/2007/EK tanácsi rendelet XIb. melléklete" szövegrész lép.

18. § (1) Ez a rendelet a kihirdetése napján lép hatályba.

(2) Az R. 5. § (2) bekezdésének b) pontja, a 10. § (4) bekezdésének k) pontja, a 19. §, valamint a 19. §-t megelőző alcím, 20. § (1) bekezdése, a (2) bekezdésének a)–b), t), v) pontja, a 86/2009. (VII. 17.) FVM rendelet 4. § (4) bekezdésének f) pontja, továbbá a 127/2009. (IX. 29.) FVM rendelet 13. és 14. számú mellékleteiben a „– ha nem megfelelt, akkor legyen indoklás!" szövegrész hatályát veszti.

(3) A 11. §, valamint a 15. § rendelkezéseit e rendelet hatálybalépését követően benyújtott kérelmekre kell alkalmazni.

(4) Az 1–17. §, az 1–4. számú mellékletek, valamint a (2) bekezdés e rendelet hatálybalépését követő harmadik napon hatályát veszti. E bekezdés e rendelet hatálybalépését követő negyedik napon hatályát veszti.

19. § Ez a rendelet a következő közösségi előírások végrehajtásához szükséges rendelkezéseket állapítja meg:

a) az egyes mezőgazdasági termékekre vonatkozó egyedi rendelkezésekről („az egységes közös piacszervezésről") szóló, 2007. október 22-i 1234/2007/EK tanácsi rendelet 103q. cikke, valamint

b) a borpiac közös szervezéséről szóló 479/2008/EK tanácsi rendeletnek a támogatási programok, a harmadik országokkal folytatott kereskedelem, a termelési potenciál és borágazat ellenőrzése tekintetében történő végrehajtására vonatkozó részletes szabályok megállapításáról szóló, 2008. június 29-i 555/2008/EK bizottsági rendelet 6–10. cikke.

Gráf József s. k.,
földművelésügyi és vidékfejlesztési miniszter

1. számú melléklet a 134/2009. (X. 14.) FVM rendelethez

„1. számú melléklet a 161/2008. (XII. 18.) FVM rendelethez

A hektáronkénti támogatási összegek fajtaváltás tevékenység esetében

Művelet megnevezése	Igénybe vehető maximális támogatási összegek 75%-os támogatási szint esetében (Ft/ha)	Igénybe vehető maximális támogatási összegek 50%-os támogatási szint esetében (Ft/ha)
erózióvédelem*	180 000	120 000
régi ültetvény felszámolása	150 000	100 000
ültetési munkák elvégzése (gyökeres oltvány, 5000 tő/ha tőszám alatt)	1 710 000	1 140 000
ültetési munkák elvégzése (gyökeres oltvány, 5000 tő/ha tőszám és a felett)	1 980 000	1 320 000
ültetési munkák elvégzése (gyökeres dugvány, 5000 tő/ha tőszám alatt)	1 335 000	890 000

Művelet megnevezése	Igénybe vehető maximális támogatási összegek 75%-os támogatási szint esetében (Ft/ha)	Igénybe vehető maximális támogatási összegek 50%-os támogatási szint esetében (Ft/ha)
ültetési munkák elvégzése (gyökeres dugvány, 5000 tő/ha tőszám és a felett)	1 530 000	1 020 000
átoltási munkák elvégzése (5000 tő/ha tőszám alatt)	750 000	500 000
átoltási munkák elvégzése (5000 tő/ha tőszám és a felett)	900 000	600 000
támrendszer létesítés elvégzése** (2,4 m átlagos sortávolság és a felett)	1 125 000	750 000
támrendszer létesítés elvégzése** (2,4 m átlagos sortávolság alatt)	1 350 000	900 000

* Az erózióvédelem költségei kizárólag átlagosan 3%-nál nagyobb lejtésű terület esetén számolhatók el.

** Két borpiaci év alatt történő végrehajtás esetén az első borpiaci évben nem számolható el.

A hektáronkénti támogatási összegek ültetvény áttelepítése tevékenység esetében

Művelet megnevezése	Igénybe vehető maximális támogatási összegek 75%-os támogatási szint esetében (Ft/ha)	Igénybe vehető maximális támogatási összegek 50%-os támogatási szint esetében (Ft/ha)
erózióvédelem*	180 000	120 000
régi ültetvény felszámolása**	150 000	100 000
ültetési munkák elvégzése (gyökeres oltvány, 5000 tő/ha tőszám alatt)	1 710 000	1 140 000
ültetési munkák elvégzése (gyökeres oltvány, 5000 tő/ha tőszám és a felett)	1 980 000	1 320 000
ültetési munkák elvégzése (gyökeres dugvány, 5000 tő/ha tőszám alatt)	1 335 000	890 000
ültetési munkák elvégzése (gyökeres dugvány, 5000 tő/ha tőszám és a felett)	1 530 000	1 020 000
támrendszer létesítés elvégzése*** (2,4 m átlagos sortávolság és a felett)	1 125 000	750 000
támrendszer létesítés elvégzése*** (2,4 m átlagos sortávolság alatt)	1 350 000	900 000

* Az erózióvédelem költségei kizárólag átlagosan 3%-nál nagyobb lejtésű terület esetén számolhatók el.

** Vásárolt újratelepítési jog esetén a művelet költségei nem számolhatók el.

*** Két borpiaci év alatt történő végrehajtás esetén az első borpiaci évben nem számolható el.

A hektáronkénti támogatási összegek ültetvény támrendszerének létesítése tevékenység esetében

Művelet megnevezése	Igénybe vehető maximális támogatási összegek 75%-os támogatási szint esetében (Ft/ha)	Igénybe vehető maximális támogatási összegek 50%-os támogatási szint esetében (Ft/ha)
tőkepótlás elvégzése	210 000	140 000
támrendszer létesítés elvégzése (2,4 m átlagos sortávolság és a felett)	1 125 000	750 000
támrendszer létesítés elvégzése (2,4 m átlagos sortávolság alatt)	1 350 000	900 000

A hektáronkénti támogatási összegek ültetvény támrendszerének korszerűsítése tevékenység esetében

Művelet megnevezése	Igénybe vehető maximális támogatási összegek 75%-os támogatási szint esetében (Ft/ha)	Igénybe vehető maximális támogatási összegek 50%-os támogatási szint esetében (Ft/ha)
régi támrendszer elemeinek bontása	90 000	60 000
tőkepótlás elvégzése	135 000	90 000
támrendszer korszerűsítés elvégzése	450 000	300 000

”

2. számú melléklet a 134/2009. (X. 14.) FVM rendelethez
„3. számú melléklet a 161/2008. (XII. 18.) FVM rendelethez

„Borvidéki szerkezetátalakítási és -átállítási terv
..... Borvidék
A 2010/2011. borpiaci évtől érvényes borvidéki követelményrendszer a szőlőültetvények szerkezetátalakítási és -átállítási támogatásához

A Borvidéki terv a hegyközségekről szóló 1994. évi CII. törvény, a szőlőültetvények szerkezetátalakítására és -átállítására vonatkozó szabályozásról szóló 161/2008. (XII. 18.) FVM rendelet, valamint a borkészítésre alkalmas szőlőfajták osztályba sorolásáról szóló 98/2009. (VII. 30.) FVM rendelet alapján készült.

1. Támogatható tevékenységek a Borvidéken:
– Fajtaváltás,
– Ültetvény áttelepítése,
– Ültetvény támrendszerének létesítése,
– Ültetvény támrendszerének korszerűsítése.

2. Termőhelyi kataszteri feltételek

2.1. Fajtaváltás
Fajtaváltást csak a Borvidék (I., II/1., II/2.) ..... termőhelyi kataszteri besorolású területein lehet végrehajtani.

2.2. Ültetvény áttelepítése
Ültetvény áttelepítése tevékenység keretében áttelepíteni a Borvidék I. termőhelyi kataszteri osztályú területein belül korlátozás nélkül, a Borvidék (II/1., II/2.) ..... kataszteri osztályú területeiről csak magasabb termőhelyi kataszteri pontértékű területre lehet.
Szőlőtermesztésre alkalmatlan, vagy termőhelyi kataszterbe nem sorolt területről ültetvényt áttelepíteni I., II/1., II/2. termőhelyi kataszteri osztályú területre lehet.

2.3. Ültetvény támrendszerének létesítése és ültetvény támrendszerének korszerűsítése
Ültetvény támrendszerének létesítése és ültetvény támrendszerének korszerűsítése tevékenységeket csak a Borvidék (I., II/1., II/2.) ..... termőhelyi kataszteri besorolású területén lévő ültetvényeken lehet végrehajtani.

3. Fajtalista

3.1. Fajtaváltás és ültetvény áttelepítése esetén az alábbi fajták részesülnek támogatásban:
..... körzet:

Engedélyezett fajták	Fajtanév
Fehérborszőlő-fajták	
Vörösborszőlő-fajták	

3.2. Ültetvény támrendszerének létesítése és ültetvény támrendszerének korszerűsítése esetén az alábbi fajtájú ültetvények részesülnek támogatásban:
..... körzet:

Engedélyezett fajták	Fajtanév
Fehérborszőlő-fajták	
Vörösborszőlő-fajták	

4. Ültetvényszerkezet

4.1. Ültetvényszerkezet fajtaváltás és ültetvény áttelepítése esetében
– A tőkehelyek száma nem lehet alacsonyabb mint ..... db/ha.
– A szerkezetátalakítás során kialakítható sortávolság nem lehet kevesebb mint ... méter, illetve több mint ... méter,
– A szerkezetátalakítás során kialakítható tőtávolság nem lehet kevesebb mint ... méter, illetve több mint ... méter,

– Kialakítható művelésmódok:
  = ...
  = ...
  = ...
  = ...

4.2. Ültetvényszerkezet ültetvény támrendszerének létesítése és ültetvény támrendszerének korszerűsítése esetében
– A tőkehelyek száma nem lehet alacsonyabb mint ..... db/ha.
– A szerkezetátalakítás során kialakítható sortávolság nem lehet kevesebb mint ..... méter, illetve több mint ..... méter,
– A szerkezetátalakítás során kialakítható tőtávolság nem lehet kevesebb mint ... méter, illetve több mint ... méter,
– Kialakítható művelésmódok:
  = ...
  = ...
  = ...
  = ...

5. Az elmúlt 15 évben, a tőkeállomány 30%-ánál nagyobb mértékű pusztulást szenvedett szőlőterületek a következők:

Település	30% feletti kipusztulást szenvedett terület	
	hrsz.	ha

A 2010/2011. borpiaci évtől érvényes borvidéki szerkezetátalakítási és -átállási tervet a Borvidék Hegyközségi Tanácsa .../2010. számú határozatával fogadta el.

Helység, dátum .....

....
elnök titkár”

3. számú melléklet a 134/2009. (X. 14.) FVM rendelethez
„6. számú melléklet a 161/2008. (XII. 18.) FVM rendelethez

Ültetvényleltár

Ültetvény helye (helység és helyrajzi szám): .....
Sortávolság: ..... méter
Tőtávolság: ..... méter
Művelésmód: .....

Sorok száma	Tőállomány	
	Elültetett/pótolt szaporítóanyag db	Tőkehelyek száma* db
1		
2		
3		
4		
5		
6		
Összesen:		

* A tőkehelyek számát a 161/2008. (XII. 18.) FVM rendelet 2. § c)–d) pontjai szerinti tevékenységek esetén is ki kell tölteni!”

4. számú melléklet a 134/2009. (X. 14.) FVM rendelethez
„7. számú melléklet a 161/2008. (XII. 18.) FVM rendelethez

Nyilatkozat

Alulírott ..... (név) (MVH regisztrációs szám: ....., cím: .....) a jelen nyilatkozathoz tartozó a biztosítékfeloldás iránti kérelemnek az MVH által történő jóváhagyása esetén kérem a kapcsolódó
a) ..... Ft összegű készpénz biztosíték visszautalását az MVH ügyfél-nyilvántartási rendszerben rögzített pénzforgalmi bankszámlámra.
b) ..... számú bankgarancia megszüntetését, és a bankgarancia eredeti példányának ..... (ügyfél vagy pénzintézet) részére ..... címre történő visszaküldését.

Kelt: ..... (helység, dátum)

.....
aláírás”

A földművelésügyi és vidékfejlesztési miniszter 135/2009. (X. 14.) FVM rendelete a szeszesital-piac ellátását szolgáló újbor lepárlásához a 2009/2010. borpiaci évben nyújtott támogatás feltételeiről

A mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 81. § (3) bekezdésének a) pontjában kapott felhatalmazás alapján, a földművelésügyi és vidékfejlesztési miniszter feladat- és hatásköréről szóló 162/2006. (VII. 28.) Korm. rendelet 1. § a) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

A támogatás jogosultja

1. § Támogatást igényelhet az a természetes személy vagy gazdálkodó szervezet (a továbbiakban: kérelmező), aki vagy amely:

a) saját termelésű, vagy vásárolt, 2009. évben Magyarországon termett szőlőből általa készített borát szeszfőzdével vagy mezőgazdasági eredetű termékek lepárlását kereskedelmi céllal végző alkoholtermék adóraktárral (a továbbiakban: lepárlóüzem) kötött szállítási szerződés (a továbbiakban: szerződés) alapján lepárlásra beszállítja és

b) telephelyén működő természetes személy, gazdasági társaság vagy egyéni vállalkozó ellen a borászati hatóság a 2007/2008., a 2008/2009. vagy a 2009/2010. borpiaci év során az alábbi jogerős intézkedések egyikét sem foganatosította:

ba) a borászati üzem legfeljebb 30 napra történő ideiglenes bezárása, gép, felszerelés, berendezés működésének, csomagolóanyag felhasználásának, tárolóhely vagy szállítóeszköz használatának megtiltása, újbóli működésének, használatbavételének, használatban tartásának feltételhez kötése,

bb) a borászati üzem területén talált közfogyasztásra, továbbfeldolgozásra alkalmatlan borászati termék megsemmisítésének vagy lepárlásának elrendelése.

A támogatási keretösszeg, a támogatás mértéke

2. § (1) E rendelet alapján a szeszesital-piac ellátását szolgáló borlepárlás támogatására fordítható keretösszeg 1 850 000 eurónak megfelelő forintösszeg.

(2) A támogatási kérelmek elbírálása a beérkezés sorrendjében történik, legkésőbb 2010. január 31-ig.

(3) A támogatási keret túligénylése esetén a keretkimerülés napján beérkezett kérelmek közötti sorrendet az alábbi szempontok figyelembevételével kell kialakítani:

a) elsőbbséget élveznek a szőlő-bor ágazatban működő, a termelői csoportokról szóló 81/2004. (V. 4.) FVM rendelet alapján elismert termelői csoportok kérelmei,

b) amennyiben az a) pont szerinti kérelmezők részére megállapított támogatási összeg nem meríti ki a rendelkezésre álló támogatási keretösszeget, úgy a kérelmek közötti sorrend a kérelmezők által lepárlásra felajánlott bor térfogatszázalékban kifejezett alkoholtartalma szerinti növekvő sorrenddel azonos.

(4) Amennyiben egy kérelmező több, eltérő alkoholtartalmú bortételt is felajánlott lepárlásra, úgy a bortételek alkoholtartalmának az egyes bortételek hektoliterben kifejezett mennyiségével súlyozott átlagát kell figyelembe venni a sorrend felállításánál.

(5) Támogatás a beszállított bormennyiség termőterülete után, 1260 €/ha-nak megfelelő forintösszegben jár azzal, hogy hektáronként legalább 70, de legfeljebb 84 hl bor támogatott lepárlása kérelmezhető. A hektáronként beszámított alkohol mennyisége legalább 840 hektoliterfok kell, hogy legyen.

A szerződés

3. § (1) Támogatás csak akkor nyújtható, ha a kérelmező és a lepárlóüzem szerződést kötött. Egy kérelmező egy borpiaci évben legfeljebb egy szerződés alapján jogosult támogatásra, amelynek meg kell felelnie a (2)–(3) bekezdésben foglaltaknak.

(2) Támogatás a rendelet hatálybalépését követően, 2010. január 10-ig terjedő időtartam alatt megkötött szerződés alapján nyújtható. A támogatási kérelem vonatkozásában hiánypótlásnak nincs helye.

(3) A szerződés alapján akkor nyújtható támogatás, ha az legalább a következőket tartalmazza:

a) a szerződő felek neve (cégneve), a mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 28. §-ának (1) bekezdésében meghatározott regisztrációs száma, valamint adóazonosító jele vagy adószáma,

b) a szállítandó bor mennyisége hektoliterben, valamint alkoholtartalma térfogatszázalékban kifejezve,

c) a szállítandó bor nettó átvételi ára, amely nem lehet kevesebb, mint 200 Ft/hektoliterfok,

d) a szállítandó borra vonatkozó, a borászati hatóság által kiállított minősítési határozat száma,

e) a lepárlóüzem kötelezettségvállalása arra vonatkozóan, hogy a részére beszállított bort 2010. május 31-ig lepárolja,

f) a szállítandó bor átvételének helye,

g) az alábbiakra vonatkozó kitételeket:

ga) a szerződés a Mezőgazdasági és Vidékfejlesztési Hivatal (a továbbiakban: MVH) támogatási kérelmet jóváhagyó határozatának jogerőre emelkedése napján lép hatályba,

gb) az MVH határozatában megjelölt bormennyiséget a kérelmezőnek 2010. május 15-ig teljes mértékben be kell szállítania a lepárlóüzembe,

gc) a beszállítás ütemezését azzal, hogy az 500 hl-t meghaladó bortételek esetében a beszállítás sorrendjét a támogatás odaítéléséről rendelkező MVH határozat kiadásának dátuma szerinti, időrendben növekvő sorrend határozza meg, valamint az így kialakult sorrendtől csak az érintett, soron következő termelő írásbeli nyilatkozata alapján lehet eltérni,

h) a szállítandó bor mennyiségét, amely nem haladhatja meg a 15 000 hl-t,

i) az 5. § szerint beszállított, de az e) pontban meghatározott határidőt követően lepárolt bortételre eső támogatásnak megfelelő összeget a lepárlóüzem a kérelmező részére kifizeti.

A támogatási kérelem benyújtása

4. § (1) A támogatási kérelmet egy eredeti példányban postai úton az MVH Piaci Támogatások és Külkereskedelmi Intézkedések Igazgatósága (a továbbiakban: MVH PKI) részére kell benyújtani az MVH által az alábbi adattartalommal rendszeresített és az MVH Központ honlapján közzétett formanyomtatványon:

a) a kérelmező azonosításához szükséges adatok (név, regisztrációs szám és telephelyének címe),

b) a szerződésben foglalt bor teljes mennyiségére vonatkozó szőlő és bor származási bizonyítványok alapján a borászati hatóság kiadott hatósági bizonyítványban meghatározott termőterület nagysága,

c) a szerződésben foglalt bor mennyisége hektoliterben,
d) a szerződésben foglalt bor alkoholtartalma térfogatszázalékban,
e) a 2. § (3) bekezdés a) pontja szerinti termelői csoportok esetében az elismerésről rendelkező határozat száma.

(2) A támogatási kérelmet e rendelet hatálybalépésének napjától 2010. január 10-ig lehet benyújtani.

(3) A támogatási kérelemhez mellékelni kell:
a) a szerződés egy eredeti példányát,
b) a szerződésben foglalt bor teljes mennyiségére vonatkozóan a borászati hatóság által kiállított minősítési határozatot, amely igazolja, hogy a lepárlásra szánt bor minősége megfelel a mezőgazdasági piacok közös szervezésének létrehozásáról, valamint egyes mezőgazdasági termékekre vonatkozó egyedi rendelkezésekről („az egységes közös piacszervezésről szóló rendelet") szóló, 2007. október 22-i 1234/2007/EK tanácsi rendelet (a továbbiakban: tanácsi rendelet) XIb. melléklete 1. pontjában meghatározott feltételeknek,
c) a borászati hatóság által kiállított, az 1. számú mellékletben meghatározott tartalmú hatósági bizonyítványt.

(4) A (3) bekezdés b) pontja szerinti minősítési határozat kiadásakor a borászati hatóság az alábbi paramétereket vizsgálja:
a) sűrűség 20 °C-on,
b) tényleges alkoholtartalom,
c) összes alkoholtartalom,
d) összes extrakttartalom,
e) cukormentes extrakttartalom,
f) invertcukor-tartalom,
g) titrálhatósav-tartalom borkősavban kifejezve,
h) illósavtartalom ecetsavban kifejezve,
i) összes kénessavtartalom,
j) szabad kénessavtartalom,
k) hamutartalom,
l) pH érték,
m) érzékszervi vizsgálat,
n) malvidin-diglükozid-tartalom (vörösborok esetén).

(5) A minősítési határozatot a borászati hatóság a legalább két litert kitevő borminta benyújtását követő 22. munkanapon adja ki, a kérelmező előzetes nyilatkozatának megfelelően személyesen (a hatóság székhelyén) vagy postai úton.

(6) A (3) bekezdés c) pontja szerinti hatósági bizonyítványt a borászati hatóság a kérelem benyújtását követő 22. munkanapon adja ki, a kérelmező előzetes nyilatkozatának megfelelően személyesen (a hatóság székhelyén) vagy levélben. A hatósági bizonyítvány iránti kérelemhez mellékelni kell:
a) a szerződésben foglalt bor teljes mennyiségére vonatkozó bor származási bizonyítványok másolatait, összevont bor származási bizonyítvány esetében kiegészítve azokkal a bor származási bizonyítvány másolatokkal is, amelyek alapján az összevont bor származási bizonyítvány kiállításra került,
b) az a) pont szerinti bor származási bizonyítványokhoz tartozó szőlő származási bizonyítványok másolatait,
c) a szerződésben foglalt bor teljes mennyiségére vonatkozóan a borászati termékek egységes bizonylatolási, nyilvántartási és elszámolási rendjéről szóló rendelet szerinti pincekönyv Hitelesítési részének és Termék-előállítás nyilvántartó lapjának másolatát,
d) amennyiben a szerződésben foglalt bor nem a kérelmező adóraktárában került előállításra, úgy a bérfeldolgozásra vonatkozó szerződés másolatát,
e) amennyiben a szerződésben foglalt bor bértárolásban van, úgy a bértárolásra vonatkozó szerződés másolatát.

(7) A borászati hatóság a (3) bekezdés c) pontjában meghatározott hatósági bizonyítvány kiadását megelőzően helyszíni szemlén vizsgálhatja az (6) bekezdés a)–e) pontjában foglalt dokumentumok megfelelőségét.

(8) Az MVH a támogatási kérelmet elutasítja, amennyiben
a) a kérelmező nem felel meg az 1. §-ban foglaltaknak,
b) a szerződés nem felel meg a 3. §-ban foglaltaknak,
c) a támogatási kérelem nem tartalmazza a (3) bekezdésben meghatározott benyújtandó mellékletek valamelyikét vagy
d) a borászati hatóság által kiállított minősítési határozat alapján a lepárlásra szánt bor minősége nem felel meg a tanácsi rendelet XIb. melléklete 1. pontjában meghatározott feltételeknek.

(9) Támogatás csak a szőlő, illetve bor származási bizonyítvány alapján megállapított területnagyságra nyújtható.

A szerződésben foglalt borok beszállítása

5. § Az MVH határozatában megjelölt bormennyiség akkor tekinthető teljes mértékben beszállítottnak, amennyiben

a) a lepárlóüzembe történő betárolás a 3. § (3) bekezdés g) pont gb) alpontjában meghatározott határidőn belül lezárult,

b) a beszállított bormennyiség legfeljebb 2%-os mértékben tér el az MVH határozatában megjelölt bormennyiségtől.

A szerződésben foglalt borok lepárlása

6. § (1) A lepárlóüzem a szerződésenként beszállított teljes bormennyiség lepárlását követően, a lepárlás befejezésétől számított 3 munkanapon belül, faxon bejelenti a lepárlás megtörténtét az MVH PKI és a borászati hatóság részére.

(2) Az (1) bekezdésben foglalt értesítéssel egyidejűleg a lepárlóüzem megküldi az MVH PKI részére a 2. számú mellékletben meghatározott tartalmú nyilatkozatot.

A támogatás kifizetése, utólagos ellenőrzés

7. § (1) Az MVH a kérelmezőtől átvett bormennyiség lepárlására és a támogatási feltételek teljesülésére vonatkozó ellenőrzése kiterjed:

a) a jövedéki adóról és a jövedéki termékek forgalmazásának különös szabályairól szóló 2003. évi CXXVII. törvény (a továbbiakban: Jöt.) által előírt, a szerződésben foglalt borok átvételére vonatkozó nyilvántartásokra, valamint szállítási okmányokra,

b) a Jöt. által előírt, a szerződésben foglalt borok lepárlására vonatkozó jövedéki nyilvántartásokra (termékmérleg nyilvántartás, termelési napló).

(2) Az MVH az ellenőrzése során figyelembe veszi a Jöt. rendelkezései szerint vezetett és a Vám- és Pénzügyőrség Országos Parancsnokság által ellenőrzött nyilvántartásokat és dokumentációkat.

(3) A támogatás kifizetése az (1) bekezdés szerinti ellenőrzést követően kezdődhet meg.

(4) Az MVH legkésőbb 2010. október 15-ig, forintban folyósítja a támogatást.

(5) A támogatási összeg meghatározásakor a forintra történő átszámítást az első borbeszállítás hónapjának első napján érvényes, az Európai Központi Bank által jegyzett forint/euró átváltási árfolyam alapján kell elvégezni.

(6) A borászati hatóság a lepárlás időszakában legalább havonta egy alkalommal a lepárlóüzem telephelyén ellenőrzést végez. Az ellenőrzésnek a lepárlással előállított bordesztillátumnak vagy borpárlatnak a szeszes italok meghatározásáról, megnevezéséről, kiszereléséről, címkézéséről és földrajzi árujelzőinek oltalmáról, valamint az 1576/89/EK tanácsi rendelet hatályon kívül helyezéséről szóló, 2008. január 15-i 110/2008/EK európai parlamenti és tanácsi rendeletben meghatározott feltételeknek való megfelelőségére kell vonatkoznia.

(7) A borászati hatóság a (6) bekezdés szerinti ellenőrzések eredményét tartalmazó jegyzőkönyveket az ellenőrzés elvégzését követő 5 munkanapon belül megküldi az MVH PKI részére.

Jogkövetkezmények

8. § (1) Támogatás nem folyósítható:

a) nem teljes mértékben beszállított bormennyiség után, vagy

b) olyan bortétel után, amelyet a lepárlóüzem a 3. § (3) bekezdésének e) pontjában meghatározott határidőt követően párolt le,

c) amennyiben az MVH vagy a borászati hatóság ellenőrzése során megállapítja, hogy a támogatási kérelemben megjelölt, illetve bármely beszállított bortétel nem tételazonos.

(2) Amennyiben az MVH vagy a borászati hatóság a kérelmezőnél végzett utólagos ellenőrzése során azt állapítja meg, hogy a kérelmező nem a támogatási kérelemben megjelölt bortételt szállította be lepárlásra, úgy az igénybe vett támogatás teljes összege jogosulatlanul igénybe vett támogatásnak minősül.

(3) Az a kérelmező, aki a szőlészeti és a borászati adatszolgáltatás, valamint a származási bizonyítványok kiadásának rendjéről, továbbá a borászati termékek előállításáról, forgalomba hozataláról és jelöléséről szóló 127/2009. (IX. 29.) FVM rendeletben [a továbbiakban: 127/2009. (IX. 29.) FVM rendelet] meghatározott szüreti, termelési vagy

készlet-jelentési kötelezettségének határidőben nem tesz eleget, nem jogosult az e rendelet szerint támogatás igénybevételére, sem a kötelezettség nem teljesítésének borpiaci évében, sem az azt követő borpiaci évben.

(4) Azon kérelmező esetében, aki a 127/2009. (IX. 29.) FVM rendeletben meghatározott szüreti, termelési vagy készlet-jelentési kötelezettségét a határidő lejárta után, de legfeljebb 10 munkanapon belül pótolja, a megítélhető támogatás összegét az MVH PKI késedelmes munkanaponként a megítélhető támogatási összeg 1/11-ed részével csökkenti. A csökkentés alapját az az összeg képezi, amelyre a kérelmező a határidőig benyújtott jelentés esetén lett volna jogosult.

(5) Azon kérelmező, aki az 5. §-ban foglalt beszállítási kötelezettségének legalább 90%-os mértékben nem tesz eleget, 2011. július 31-ig nem kérelmezhet a tanácsi rendelet 103o–103u., valamint 103w–103y. cikkei alapján folyósított támogatást.

(6) A (3) és (4) bekezdésekben foglalt szüreti, termelési vagy készlet-jelentési kötelezettségek teljesítését az MVH PKI a külön jogszabályban meghatározott integrált szőlészeti és borászati nyilvántartó rendszer segítségével ellenőrzi.

Záró rendelkezések

9. § (1) Ez a rendelet 2009. november 10-én lép hatályba.

(2) A 4. § (1) bekezdés szerinti formanyomtatványt az MVH Központ honlapján letölthető formában közzéteszi legkésőbb a rendelet hatálybalépésének napján.

(3) Ez a rendelet a következő európai uniós jogi aktusok végrehajtásához szükséges rendelkezéseket állapítja meg:

a) a mezőgazdasági piacok közös szervezésének létrehozásáról, valamint egyes mezőgazdasági termékekre vonatkozó egyedi rendelkezésekről szóló 2007. október 22-i 1234/2007/EK tanácsi rendelet („az egységes közös piacszervezésről szóló rendelet") 103w. cikke, valamint

b) a borpiac közös szervezéséről szóló 479/2008/EK tanácsi rendeletnek a támogatási programok, a harmadik országokkal folytatott kereskedelem, a termelési potenciál és borágazat ellenőrzése tekintetében történő végrehajtására vonatkozó részletes szabályok megállapításáról szóló, 2008. június 29-i 555/2008/EK bizottsági rendelet 26–27. cikke.

Gráf József s. k.,
földművelésügyi és vidékfejlesztési miniszter

1. számú melléklet a 135/2009. (X. 14.) FVM rendelethez

A borászati hatóság által kiadott hatósági bizonyítvány tartalmazza:

1. „A ..... (név) által ..... napján beérkezett írásbeli kérelem alapján az alábbiakat igazolom."
2. „A ..... sorszámú minősítési határozaton megjelölt kérelmező telephelyén működő gazdasági társaság vagy egyéni vállalkozó ellen a borászati hatóság a 2007/2008., 2008/2009., 2009/2010. borpiaci év során az alábbi kérdésekben:
   – a borászati üzem legfeljebb 30 napra történő ideiglenes bezárása, gép, felszerelés, berendezés működésének, csomagolóanyag felhasználásának, tárolóhely vagy szállítóeszköz használatának megtiltása, újbóli működésének, használatbavételének, használatban tartásának feltételhez kötése;
   – a borászati üzem területén talált borászati termék közfogyasztásra, továbbfeldolgozásra alkalmatlan termék megsemmisítésének vagy lepárlásának elrendelése

   intézkedést nem foganatosítottam."
3. „A fenti sorszámú minősítési határozaton megjelölt ..... hl bormennyiség származási országa Magyarország."
4. „A fenti sorszámú minősítési határozaton megjelölt ..... hl bormennyiség borszármazási bizonyítvánnyal igazolt termelője a: ....."
5. „A fenti sorszámú minősítési határozaton megjelölt ..... hl bormennyiség 2009. évben szüretelt szőlőből készült."
6. „A fenti sorszámú minősítési határozaton megjelölt ..... hl bormennyiség hektárban kifejezett szőlőtermő-területe: ..... ha."

2. számú melléklet a 135/2009. (X. 14.) FVM rendelethez

A lepárlóüzem nyilatkozata

„Alulírott ..... a ..... (lepárlóüzem) képviseletében tudomásul veszem, hogy amennyiben az MVH vagy a borászati hatóság ellenőrzése során azt állapítja meg, hogy az üzemünkben a szeszesital-piac ellátását szolgáló borlepárlás támogatásának feltételeiről szóló 135/2009. (X. 14.) FVM rendelet szerinti támogatásban részesült borból lepárlással előállított bordesztillátum vagy borpárlat nem felel meg a szeszes italok meghatározásáról, megnevezéséről, kiszereléséről, címkézéséről és földrajzi árujelzőinek oltalmáról, valamint az 1576/89/EK tanácsi rendelet hatályon kívül helyezéséről szóló 110/2008/EK európai parlamenti és tanácsi rendelet előírásainak, akkor a 2010/2011. borpiaci év folyamán üzemünk nem vehet részt a mezőgazdasági piacok közös szervezésének létrehozásáról, valamint egyes mezőgazdasági termékekre vonatkozó egyedi rendelkezésekről szóló 2007. október 22-i 1234/2007/EK tanácsi rendelet („az egységes közös piacszervezésről szóló rendelet") II. cím I. fejezete, 103w., valamint 103x. cikkében meghatározott támogatási intézkedések végrehajtásában."

Cégszerű aláírás, dátum

A közlekedési, hírközlési és energiaügyi miniszter 55/2009. (X. 14.) KHEM rendelete egyes miniszteri rendeletek módosításáról

A közlekedési, hírközlési és energiaügyi miniszter feladat- és hatásköréről szóló 133/2008. (V. 14.) Korm. rendelet 1. §-a (1) bekezdésének a) és c) pontjaiban meghatározott hatáskörömben eljárva,

az utak forgalomszabályozásáról és a közúti jelzések elhelyezéséről szóló 20/1984. (XII. 21.) KM rendelet módosítása tekintetében a közúti közlekedésről szóló 1988. évi I. törvény 48. §-ának (3) bekezdése b) pontjának 5. alpontjában,

a bányaüzem felelős műszaki vezetője és helyettese kijelölésének feltételeiről szóló 25/1994. (X. 14.) IKM rendelet módosítása tekintetében a bányászatról szóló 1993. évi XLVIII. törvény 50/A. §-a (2) bekezdésének a)–b) pontjában,

az egyes használt vagy sérült gépjárművek vámkezelését megelőző vizsgálatról szóló 3/1999. (I. 18.) KHVM–KöM–PM együttes rendelet tekintetében a közúti közlekedésről szóló 1988. évi I. törvény 48. §-ának (3) bekezdése b) pontjának 15. alpontjában,

a hajózási tevékenység engedélyezésének rendjéről szóló 28/2000. (XII. 18.) KöViM rendelet módosítása tekintetében a víziközlekedésről szóló 2000. évi XLII. törvény 88. §-a (2) bekezdésének a) pontjában,

a belföldi és a nemzetközi közúti árufuvarozás szakmai feltételeiről és engedélyezési eljárásáról szóló 14/2001. (IV. 20.) KöViM rendelet tekintetében a közúti közlekedésről szóló 1988. évi I. törvény 48. §-ának (3) bekezdése b) pontjának 1. alpontjában,

a hajózási képesítésekről szóló 15/2001. (IV. 27.) KöViM rendelet módosítása tekintetében a víziközlekedésről szóló 2000. évi XLII. törvény 88. §-a (2) bekezdésének s) pontjában,

a tengeri személyhajókra vonatkozó biztonsági követelményekről szóló 12/2002. (II. 7.) KöViM rendelet tekintetében víziközlekedésről szóló 2000. évi XLII. törvény 88. §-a (2) bekezdésének b) pontjában,

a 24 méter és annál nagyobb hosszúságú tengeri halászhajókra vonatkozó biztonsági követelményekről szóló 22/2002. (IV. 27.) KöViM rendelet tekintetében a víziközlekedésről szóló 2000. évi XLII. törvény 88. §-a (2) bekezdésének b) pontjában,

a víziközlekedés irányítására és a hajóút kitűzésére szolgáló jelekről, valamint e jelek létesítéséről, üzemeltetéséről, módosításáról és megszüntetéséről szóló 27/2002. (XII. 5.) GKM rendelet tekintetében a víziközlekedésről szóló 2000. évi XLII. törvény 88. §-a (2) bekezdésének j) pontjában,

a nagysebességű transzeurópai vasúti rendszer kölcsönös átjárhatóságáról szóló 37/2006. (VI. 21.) GKM rendelet tekintetében a vasúti közlekedésről szóló 2005. évi CLXXXIII. törvény 88. §-a (2) bekezdésének 19. pontjában,

a vasúti társaságok működésének engedélyezéséről szóló 45/2006. (VII. 11.) GKM rendelet tekintetében a vasúti közlekedésről szóló 2005. évi CLXXXIII. törvény 88. §-a (2) bekezdésének 1. pontjában

foglalt felhatalmazás alapján a következőket rendelem el:

1. § A bányaüzem felelős műszaki vezetője és helyettese kijelölésének feltételeiről szóló 25/1994. (X. 14.) IKM rendelet 6. §-a (2) bekezdésének a) pontjában a „nevét" szövegrész helyébe a „természetes személyazonosító adatait" szöveg lép.

2. § A hajózási képesítésekről szóló 15/2001. (IV. 27.) KöViM rendelet 10. §-ának (3) bekezdésében a „Gazdasági és Közlekedési Minisztériumot (a továbbiakban: minisztérium)" szöveg helyébe a „minisztériumot" szöveg lép.

3. § A tengeri személyhajókra vonatkozó biztonsági követelményekről szóló 12/2002. (II. 7.) KöViM rendelet 14. §-a helyébe a következő rendelkezés lép:
„14. § Ez a rendelet a – az e rendelet 2. §-ában hivatkozott nemzetközi egyezményeket, illetve szabályzatokat kihirdető külön jogszabályokkal együtt – a személyhajókra vonatkozó biztonsági előírásokról és követelményekről szóló 1998. március 17-i 98/18/EK tanácsi irányelvének való megfelelést szolgálja."

4. § A 24 méter és annál nagyobb hosszúságú tengeri halászhajókra vonatkozó biztonsági követelményekről szóló 22/2002. (IV. 27.) KöViM rendelet 2. számú melléklete e rendelet melléklete szerint módosul.

5. § A víziközlekedés irányítására és a hajóút kitűzésére szolgáló jelekről, valamint e jelek létesítéséről, üzemeltetéséről, módosításáról és megszüntetéséről szóló 27/2002. (XII. 5.) GKM rendelet 8. §-ának (1) bekezdésében a „környezetvédelmi, természetvédelmi és vízügyi felügyelőség" szövegrész helyébe a „vízügyi hatóság" szöveg, 10. §-ának (2) bekezdésében a „területileg illetékes környezetvédelmi, természetvédelmi és vízügyi felügyelőséghez" szövegrész helyébe a „vízügyi hatósághoz" szöveg, 14. §-ának (2) bekezdésében a „környezetvédelmi és vízügyi igazgatóság" szövegrész helyébe a „vízügyi igazgatási szerv" szöveg lép.

6. § A nagysebességű transzeurópai vasúti rendszer kölcsönös átjárhatóságáról szóló 37/2006. (VI. 21.) GKM rendelet 13. §-ának (5) bekezdésében az „az NKH Közép-magyarországi Regionális Igazgatóságának" szövegrész helyébe az „a vasúti közlekedési hatóságnak" szöveg lép.

7. § A vasúti társaságok működésének engedélyezéséről szóló 45/2006. (VII. 11.) GKM rendelet 9. §-ának (4) bekezdésében az „az engedélyt kérő" szövegrész helyébe az „a kérelmező" szöveg lép.

8. § Hatályát veszti

a) az utak forgalomszabályozásáról és a közúti jelzések elhelyezéséről szóló 20/1984. (XII. 21.) KM rendelet 2. §-ának (8) bekezdésében az „előzetes" szövegrész,

b) az egyes használt vagy sérült gépjárművek vámkezelését megelőző vizsgálatról szóló 3/1999. (I. 18.) KHVM–KöM–PM együttes rendelet 2. §-a (1) bekezdésének a) pontja és (2) bekezdése, 4. §-ában a „területileg illetékes" szövegrész, 5. §-ának (1) és (2) bekezdésében az „eljáró" szövegrész, 8. §-ának (1) bekezdésében az „ , egyidejűleg hatályát veszti az egyes gépjárművek vámkezelését megelőző vizsgálatról szóló 2/1993. (I. 27.) KHVM–KTM együttes rendelet, valamint az azt módosító 27/1997. (XII. 12.) KHVM–KTM együttes rendelet és a 15/1998. (VI. 25.) KHVM–KTM együttes rendelet" szövegrész,

c) a hajózási tevékenység engedélyezésének rendjéről szóló 28/2000. (XII. 18.) KöViM rendelet 12. §-ának (3) bekezdésében a „nevét, székhelyét (telephelyét) vagy lakóhelyét, továbbá" szövegrész,

d) a belföldi és a nemzetközi közúti árufuvarozás szakmai feltételeiről és engedélyezési eljárásáról szóló 14/2001. (IV. 20.) KöViM rendelet 12. §-a (1) bekezdésének második mondata.

9. § Ez a rendelet a kihirdetését követő napon lép hatályba és a hatálybalépését követő második napon hatályát veszti.

Hónig Péter s. k.,
közlekedési, hírközlési és energiaügyi miniszter

Melléklet az 55/2009. (X. 14.) KHEM rendelethez

A 24 méter és annál nagyobb hosszúságú tengeri halászhajókra vonatkozó biztonsági követelményekről szóló 22/2002. (IV. 27.) KöViM rendelet 2. számú mellékletében a „Mentesítési bizonyítvány" mintájában a
„Kiállítva a
Issued under the provisions of the
22/2002. (IV. 27.) KöViM rendelet alapján
decree 22/2002. (IV. 27.) KöViM of the Minister of Transport and Water Management
annak igazolásául, hogy az alábbiakban megnevezett hajó megfelel a Tanácsnak a 24 méter és annál hosszabb halászhajók biztonsági rendszerének harmonizálásáról szóló 97/70/EK irányelvében foglalt rendelkezéseknek
and confirming compliance of the vessel named hereafter with the provisions of Council Directive 97/70/EC setting up harmonised safety regime for fishing vessels of 24 metres in length and over
a MAGYAR KÖZTÁRSASÁG közlekedési és vízügyi miniszterének felhatalmazása alapján
under the authority of the Minister of Transport and Water Management of the REPUBLIC OF HUNGARY
a
.....
by
[a 10/2000. (X. 31.) KöViM rendelet alapján kijelölt szervezet neve]
(full official designation of the competent organisation recognised under the provisions of Council Directive 94/57/EC)"
szövegrész helyébe a
„Kiállítva a
Issued under the provisions of the
22/2002. (IV. 27.) KöViM rendelet alapján
decree 22/2002. (IV. 27.) KöViM
annak igazolásául, hogy az alábbiakban megnevezett hajó megfelel a Tanácsnak a 24 méter és annál hosszabb halászhajók biztonsági rendszerének harmonizálásáról szóló 97/70/EK irányelvében foglalt rendelkezéseknek
and confirming compliance of the vessel named hereafter with the provisions of Council Directive 97/70/EC setting up harmonised safety regime for fishing vessels of 24 metres in length and over
a MAGYAR KÖZTÁRSASÁG kormányának felhatalmazása alapján
under the authorization of the Government of the REPUBLIC OF HUNGARY
a Nemzeti Közlekedési Hatóság által.
by the National Transport Authority."
szöveg lép.

IX. Határozatok Tára

A köztársasági elnök 133/2009. (X. 14.) KE határozata dandártábornok szolgálati viszonyának megszüntetéséről és nyugállományba helyezéséről

Az Alkotmány 30/A. § (1) bekezdés i) pontjában biztosított jogkörömben, a honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény 49. § (2) bekezdésének b) pontja alapján *Kocsis István* dandártábornok szolgálati viszonyát 2009. október 5-én megszüntetem és 2009. október 6-ai hatállyal nyugállományba helyezem.

Budapest, 2009. szeptember 22.

Sólyom László s. k.,
köztársasági elnök

Ellenjegyzem:

Budapest, 2009. szeptember 24.

Dr. Szekeres Imre s. k.,
honvédelmi miniszter

KEH ügyszám: IV-6/03704/2009.

A Magyar Közlönyt a Szerkesztőbizottság közreműködésével a Miniszterelnöki Hivatal szerkeszti.
A Szerkesztőbizottság elnöke: dr. Petrétei József, a szerkesztésért felelős: dr. Tordai Csaba.
A szerkesztőség címe: Budapest V., Kossuth tér 1–3.
A Határozatok Tára hivatalos lap tartalma a Magyar Közlöny IX. részében jelenik meg.
A Magyar Közlöny hiteles tartalma elektronikus dokumentumként a http://kozlony.magyarorszag.hu honlapon érhető el. Felelős kiadó: dr. Tordai Csaba.
A Magyar Közlöny oldalhű másolatát papíron kiadja a Magyar Közlöny Lap- és Könyvkiadó.
Felelős kiadó: dr. Kodela László elnök-vezérigazgató.