

## **A Kormány**

### **.../2015. (... ...) Korm. rendelete**

#### **az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról**

A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *a)–c), h) és i)* pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

### **1. Értelmező rendelkezések**

#### **1. § E rendelet alkalmazásában**

1. *felhő alapú számítástechnikai szolgáltatás*: olyan szolgáltatás, amelyet a szolgáltató a felhasználó számára nem egy erre a célra rendelt hardvereszközön, hanem a saját eszközein elosztva, az üzemeltetés részleteit elrejtve üzemelteti, és amelyet a felhasználók interneten keresztül érhetnek el.

### **2. A hatóság**

2. § Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 14. § (1) bekezdése szerinti Nemzeti Elektronikus Információbiztonsági Hatósággént (a továbbiakban: hatóság) a Kormány az e-közigazgatásért felelős minisztert (a továbbiakban: miniszter) jelöli ki.

### **3. A hatósági eljárásra vonatkozó általános rendelkezések**

3. § (1) A (2) bekezdésben foglalt kivételekkel a hatóság eljárásainak általános ügyintézési határideje hatvan nap, amelyet a hatóság vezetője indokolt esetben egy alkalommal, legfeljebb harminc nappal meghosszabbíthat.

(2) A hatóság által lefolytatott hatósági eljárás ügyintézési határideje az általános ügyintézési határidőn túl:

- a)* fizikai védelmi kötelezettség teljesítésére irányuló vizsgálat esetén tizenöt nap,
- b)* adminisztratív védelmi kötelezettség teljesítésére irányuló vizsgálat esetén harminc nap,
- c)* logikai védelmi kötelezettség teljesítésére irányuló vizsgálat esetén hetvenöt nap.

4. § A hatóság az eljárást lezáró döntésének meghozatala előtt az érintett szervezettel – ha ezt azonnali fenyegetés vagy biztonsági esemény, vagy az érintett szervezet ismételt jogsértő magatartása nem zárja ki – egyeztetést folytat le.

**5. § (1)** A hatóság az eljárása során, feladatai ellátása érdekében – az intézkedéssel érintett szervezet működésének és ügyvitelének lehető legkisebb mértékű zavarása mellett – helyszíni ellenőrzés keretében jogosult önállóan, vagy más hatósággal együtt:

*a)* az érintett szervezet információtechnológiai tevékenységével összefüggő helyiségeibe belépni,

*b)* az érintett szervezet számára adatkezelést biztosító, adatfeldolgozást végző, vagy információtechnológiai szempontból érintett helyszínein ellenőrzést tartani, és ennek során bármely, az elektronikus információbiztonsággal kapcsolatos okiratot, dokumentumot, szerződést, aktív, vagy passzív eszközt, információs rendszert, biztonsági intézkedést megismerni, ellenőrizni, az elektronikus információbiztonsággal kapcsolatos okiratokról, dokumentumokról, szerződésekről másolatot készíteni,

*c)* információtechnológiai műszaki vizsgálatokat végezni, szükség esetén az információtechnológiai rendszerhez egyedileg biztosított belépési jogosultsággal.

(2) A hatóság a helyszíni ellenőrzés elrendelése esetén a hatóság ellenőrzést ellátó munkatársa részére megbízólevelet állít ki. A megbízólevélnek tartalmaznia kell az ellenőrzés célját, tárgyát, az elrendelésre okot adó körülményeket, a jogszabályi hivatkozást, az ellenőrzés várható időtartamát, az ellenőrzés módját és az ellenőrzést végző személyek megnevezését.

(3) A helyszíni ellenőrzés elrendeléséről az érintett szervezet vezetőjét előzetesen írásban, az érintett szervezet elektronikus információs rendszereinek biztonságáért felelős személyt elektronikus úton a helyszíni vizsgálat megkezdése előtt 10 nappal értesíteni kell. Az értesítéshez mellékelni kell az ellenőrzést ellátó személy megbízólevelét.

(4) A (3) bekezdés szerinti értesítés mellőzhető, ha

*a)* súlyos fenyegetettség áll fenn,

*b)* súlyos biztonsági esemény történt,

*c)* az *a)* vagy *b)* pont szerinti körülmény bekövetkezése valószínűsíthető, vagy

*d)* az érintett szervezet a rendelkezésre álló adatok alapján a helyszíni ellenőrzés eredményes lefolytatását feltehetően meghiúsítaná.

(5) A helyszíni ellenőrzéssel érintett szervezet vezetője, munkatársa, alkalmazottja, illetve szerződéses jogviszony alapján az elektronikus információbiztonság tekintetében érintett egyéb közreműködő és az elektronikus információs rendszer biztonságáért felelős személy köteles a hatósággal együttműködni.

(6) A helyszíni ellenőrzésről a hatóság jegyzőkönyvet készít, amelyet az ellenőrzés lezárását követő nyolc napon belül az érintett szervezetnek írásban észrevételezésre megküld. Az érintett szervezet azzal kapcsolatban nyolc napon belül írásban tehet – a hatóságot nem kötelező – észrevételeket. Az észrevételek tisztázása érdekében a hatóság egyeztetést kezdeményezhet az érintett szervezettel.

**6. § (1)** A hatóság jogosult bármely, jogszabályban meghatározott hatáskörébe tartozó eljárási cselekményt haladéktalanul – az ügy jellegének megfelelően a kormányzati eseménykezelő központtal, a 15-18. § és a 24-26. § szerinti hatóságokkal közösen – lefolytatni, ha az a magyar

kiberteret, a nemzeti adatvagyon, az állam és polgárai számára kiemelten fontos információs rendszereket súlyosan veszélyeztető fenyegetés elhárítását szolgálja.

(2) A hatóság a kormányzati eseménykezelő központ értesítése alapján tudomására jutott biztonsági eseményeket haladéktalanul megvizsgálja, és annak alapján megteszi a biztonsági eseménnyel kapcsolatos szükséges hatósági intézkedéseket.

#### **4. A hatóság feladatai**

##### **7. § (1) A hatóság**

- a) engedélyezi az érintett szervezetek által az EGT tagállamaiban történő elektronikus információrendszer-üzemeltetést,
- b) ellenőrzi az érintett szervezetek által az EGT tagállamain kívül történő elektronikus információrendszer-üzemeltetést,
- c) ellenőrzi az információtechnológiai fejlesztési projekteknél az információbiztonsági követelmények teljesülését,
- d) nyilvántartja a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályát, valamint az elektronikus információs rendszer osztályba soroláshoz szükséges, jogszabályban meghatározott fizikai, logikai és adminisztratív védelmi intézkedések adatait,
- e) nyilvántartja és honlapján közzé teszi a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítéseket,
- f) jogszabályban meghatározott szempontok szerint, hatósági eljárás keretében lefolytatja a fizikai, logikai és adminisztratív védelmi ellenőrzéseket.

(2) A hatóság az EGT tagállamaiban történő elektronikus információs rendszer üzemeltetése tekintetében engedélyezési eljárást folytat le a 8. § (3) bekezdésében foglaltak kivételével. Az eljárás során a hatóság megvizsgálja

- a) az EGT tagállamaiban történő adatkezelés indokát,
- b) az EGT tagállamaiban kezelt adatok és adatbázisok leírását,
- c) azt, hogy az adatkezelő rendszer, valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy neve, beosztása, elérhetősége ismert-e,
- d) az adatkezelő rendszer technikai és technológiai leírását, ideértve a hardver- és szoftverkomponenseket is,
- e) az adatkezelő rendszer információbiztonságának ismertetését, a rendszerhez kapcsolódó, továbbá az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- f) a kötelezően lefolytatandó biztonsági rendszerfelülvizsgálat eredményét,
- g) a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot és
- h) azt, hogy az üzemeltetés helyszínén illetékes hatóságok jogosultak-e a kezelt adatokba betekinteni.

(3) Nem kell a (2) bekezdés e)–g) pontja szerinti leírásokat megvizsgálni, ha az Ibtv. 4. §-a szerinti, érvényes biztonsági tanúsítvány a kérelem benyújtásakor rendelkezésre áll, és azt a hatóságnak bemutatják.

**8. §** (1) Az engedélyezésre irányuló kérelem tartalmazza a 7. § (2) és (3) bekezdése szerinti adatokat. A kérelmet a külföldön történő adatkezelés megkezdését megelőzően kilencven nappal kell benyújtani a hatóság részére. A 7. § (2) bekezdés *b)*, *e)* és *f)* pontja, és a 7. § (3) bekezdése szerinti dokumentációkat, okiratokat az eredetivel megegyező másolatban, és hiteles magyar fordításban a kérelem mellékleteként csatolni kell.

(2) A hatóság engedélye hiányában az elektronikus információs rendszer EGT tagállamban történő üzemeltetése, továbbá ilyen rendszeren adatfeldolgozói, adatkezelői tevékenység nem kezdhető meg. Az engedély lejártát a benyújtott tanúsítványok érvényességi időtartamához igazodóan kell megállapítani.

(3) Ha a külföldön végzett adatkezelésre vagy rendszerüzemeltetésre olyan nemzetközi szerződés alapján kerül sor, amelyben az állam az egyik szerződő fél, a hatóságot tájékoztatni kell az érintett adatokról, az adatfeldolgozó vagy üzemeltető személyéről, és a szerződéses jogviszony tartalmáról. A hatóság a tájékoztatást további eljárás lefolytatása nélkül tudomásul veszi.

(4) Ha a hatóság tudomására jut, hogy az érintett szervezet az adatkezelést, vagy üzemeltetést – ideértve a nem azonosítható adatkezelési, vagy jogszabály által kizárt helyszínen megvalósuló, felhő alapú számítástechnikai szolgáltatásokat is – jogosulatlanul Magyarországon kívül folytatja, a hatóság a 15. § szerinti jogkövetkezményt alkalmazza.

**9. §** (1) Az európai uniós támogatásból, központi költségvetési támogatásból megvalósuló fejlesztési projektek információbiztonsági követelményeinek teljesítése során a projekt vezetője, a projekt tervezési szakaszában a hatóság részére véleményezésre megküldi a fejlesztendő elektronikus információs rendszerre vonatkozó biztonsági osztályba sorolást, továbbá mindazon dokumentációkat, amelyek alapján a biztonsági követelmények megvalósulása ellenőrizhető a projekt teljes életciklusára nézve, ideértve az átvétel vagy teljesülés után az elektronikus információs rendszer használata során érvényesítendő elvárásokat is.

(2) A projekt mérföldköveinek figyelembevételével, az adott projektszakasz zárását megelőző legkevesebb harminc nappal kell a hatóság rendelkezésére bocsátani a kapcsolódó elektronikus információbiztonsági dokumentációt annak érdekében, hogy a hatóság észrevételei vagy kifogásai a projekt terveken, vagy a projekt tárgyán átvezethető és alkalmazható legyen.

(3) A hatvan napnál rövidebb időtartamú projektek esetén az (1) bekezdés szerinti dokumentációt legkésőbb a projekt befejezésekor kell a hatóság rendelkezésére bocsátani.

(4) A hatóság az (1)–(3) bekezdés szerinti dokumentumok tekintetében más hatóság véleményét kikérheti.

**10. §** (1) Az elektronikus információs rendszerek biztonsági osztályba sorolásának ellenőrzése a hatóságnak megküldött információk alapján, jogszabályban meghatározott szempontok szerint történik.

(2) Ha a bejelentett biztonsági osztályba sorolást – ideértve az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál feltárt hiányosság megszüntetésére irányuló cselekvési tervet – a hatóság elfogadja, az erre irányuló döntés a biztonsági osztályba sorolás későbbi önálló, vagy az érintett szervezet, vagy szervezeti egység ellenőrzése során történő felülvizsgálatát nem zárja ki.

(3) Ha a hatóság az eljárása során az érintett szervezet vezetője által megállapított és bejelentett biztonsági osztályba sorolást felülbírálja és magasabb biztonsági osztályt állapít meg, a következő biztonsági osztály elérésére irányadó határidő alkalmazása tekintetében a hatóság döntésének megfelelő szintet kell alapul venni.

(4) Ha a hatóság a bejelentett biztonsági osztályba sorolásnál alacsonyabb osztály alkalmazásának lehetőségét látja, arra az érintett szervezetnek javaslatot tesz.

(5) Ha az érintett szervezet vezetője a biztonsági osztályba sorolás követelményeiről szóló jogszabályban meghatározott biztonsági osztály helyett alacsonyabb osztályt állapít meg, azt részletesen indokolnia kell.

**11. §** (1) Az érintett szervezet, vagy szervezeti egység biztonsági szintbe sorolásának ellenőrzése a hatóságnak megküldött információk alapján, jogszabályban meghatározott szempontok szerint történik.

(2) Ha a hatóság a bejelentett biztonsági szintbe sorolásnál alacsonyabb szint alkalmazásának lehetőségét látja, arra az érintett szervezetnek, vagy szervezeti egységnek javaslatot tesz.

## **5. Az érintett szervezet egyes kötelezettségei**

**12. §** (1) Az érintett szervezet – ha az elektronikus információs rendszer biztonságért felelős személy, szervezet kijelölése vagy az elektronikus informatikai biztonsági szabályzat elkészítése a jogszabályban meghatározott időn belül neki fel nem róható okból nem teljesül – a jogszabályban meghatározott határidőn belül a hatóságot tájékoztatja a teljesítést akadályozó ok és a teljesítés határidejének megjelölésével.

(2) Az elektronikus információs rendszer biztonságáért felelős személy – ideértve az információbiztonsági szolgáltatást nyújtó vállalkozás tagjait és alkalmazottait is – az érintett szervezet igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja

- a) részmunkaidőben,
- b) a vonatkozó szerződésben meghatározott időtartamban, vagy
- c) több érintett szervezetnél.

(3) Az elektronikus információs rendszer biztonságáért felelős személyről szóló tájékoztatás magában foglalja a vonatkozó munka-, megbízási vagy más szerződés másolatának hatóság

kérésére való megküldését, amelyhez csatolni kell az adott személy végzettségét, képzettségét igazoló okirat, vagy a szakterületi gyakorlatot igazoló okirat vagy nyilatkozat másolatát.

(4) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele során a szervezet vezetője nem mentesül a jogszabályban meghatározott azon kötelezettségek alól, amelyek a szervezet felett az információbiztonság tekintetében gyakorolt irányítási és ellenőrzési jogkörébe tartoznak.

## **6. Az ellenőrzési terv**

**13. §** (1) Az éves ellenőrzési tervet a hatóság minden év november 30-ig állítja össze.

(2) A hatóság az ellenőrzési terv végrehajtását az aktuális évet követő év március 1-jéig értékeli.

(3) A hatóság az ellenőrzési tervben foglaltaktól eltérhet, ha olyan azonnali ellenőrzéseket vagy eljárásokat kell lefolytatnia, amelyek a magyar kiberteret, a nemzeti elektronikus adatvagyon, az állam és polgárai számára kiemelten fontos elektronikus információs rendszereket fenyegető súlyos biztonsági események elhárítását szolgálják.

(4) A hatóság az ellenőrzési tervtől való eltérés okát, az ellenőrzési terv értékeléséről szóló jelentésben, az e-közigazgatásért felelős miniszter részére megküldi.

## **7. Jogkövetkezmények**

**14. §** (1) A hatóság az információbiztonsági követelmények teljesülése érdekében – határidő kitűzése mellett – írásban szólítja fel az érintett szervezet vezetőjét az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a biztonságikövetelmény-sértés megszüntetésére, jogszabályban meghatározott kötelezettség teljesítésére, az elvárt intézkedés megtételére.

(2) A hatóság azonnali intézkedések megtételére kötelezi az érintett szervezetet, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget.

(3) A hatóság által kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a hatóság határozatának jogerőre emelkedését követő nyolc napon belül kell befizetni a hatóság Magyar Államkincstárnál vezetett számlájára.

(4) A hatóság a jogkövetkezmények alkalmazása során jogszabályban meghatározottakon túl az alábbi szempontokat veszi figyelembe:

a) az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelménynek a biztonsági osztályba sorolás és biztonsági szint szerinti súlyát,

b) történt-e súlyos biztonsági esemény, vagy fennállt-e ilyen esemény bekövetkeztének veszélye,

- c) a biztonsági esemény hatását, vagy lehetséges hatását az érintett szervezetre, vagy más szervezetekre,
- d) az érintett szervezet magatartását, hatósággal való együttműködését és
- e) az esemény egyedi, vagy ismételt jellegét.

## **8. A zárt célú elektronikus információs rendszerek, valamint a biztonsági felügyeletüket ellátó hatóságok és feladataik**

**15. § (1)** A rendészetért felelős miniszter vezetése, irányítása alá tartozó, az Ibtv. szerinti zárt célú elektronikus információs rendszerek (a továbbiakban: zárt célú elektronikus információs rendszerek) a következő szerveknél működnek:

- a) Belügyminisztérium,
- b) Alkotmányvédelmi Hivatal,
- c) Nemzetbiztonsági Szakszolgálat,
- d) Terrorrelhárítási Központ,
- e) Nemzeti Védelmi Szolgálat,
- f) BM Országos Katasztrófavédelmi Főigazgatóság,
- g) Büntetés-végrehajtás Országos Parancsnokság,
- h) Országos Rendőr-főkapitányság és
- i) Szervezett Bűnözés Elleni Koordinációs Központ.

(2) Az (1) bekezdés szerinti szerveknél működő zárt célú elektronikus információs rendszerek a következők:

- a) rendészeti, nemzetbiztonsági területen titkos információgyűjtést, titkos adatszerzést támogató zárt célú elektronikus információs rendszerek,
- b) rendészeti, nemzetbiztonsági területen belső irodai és iratkezelési célt szolgáló zárt célú elektronikus információs rendszerek, valamint
- c) rendészeti, nemzetbiztonsági területen szakmai feladatok támogatását szolgáló zárt célú elektronikus információs rendszerek.

(3) A (2) bekezdés szerinti zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét jelöli ki.

**16. § (1)** a honvédelemért felelős miniszter vezetése, irányítása alá tartozó szervek zárt célú elektronikus információs rendszerei a következők:

- a) honvédelmi célú közigazgatási döntés-előkészítő és vezetés-irányítási rendszerek,
- b) honvédelmi stacioner és tábori, nemzetközi műveleteket, valamint gyakorlatokat támogató műveleti vezetési rendszerek,

- c) katonai nemzetbiztonsági területen titkos információgyűjtést, illetve titkos adatszerzést támogató rendszerek, valamint
- d) Honvédelmi Tanács és a Kormány speciális működési területén szakmai feladatok támogatását szolgáló kormányzati célú informatikai rendszerek.

(2) Az (1) bekezdés szerinti zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét jelöli ki.

**17. §** (1) A külpolitikaért és külgazdaságért felelős miniszter vezetése, irányítása alá tartozó szervek zárt célú elektronikus információs rendszerei a következők:

.....  
.....

(2) Az (1) bekezdés szerinti zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét jelöli ki.

**18. §** (1) A kormányzati tevékenység összehangolásáért felelős miniszter vezetése, irányítása alá tartozó szervek zárt célú elektronikus információs rendszerei a következők:

.....  
.....

(2) Az (1) bekezdés szerinti zárt célú elektronikus információs rendszerekkel kapcsolatos hatósági, biztonsági felügyeleti feladatok ellátására a Kormány a zárt célú elektronikus információs rendszert működtető szerv vezetőjét jelöli ki.

**19. §** A zárt célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságokra (a továbbiakban: kijelölt hatóság) az Ibtv. 14-17. §-ától eltérően e rendelet 20-22. § szerinti rendelkezéseket kell alkalmazni.

**20. §** A kijelölt hatóság feladata:

a) a zárt célú elektronikus információs rendszerek, illetve a 26. § (1) bekezdésében meghatározott hatóság eljárása során az európai vagy nemzeti létfontosságú rendszerré, létesítménnyé törvény alapján kijelölt rendszerek, létesítmények elektronikus információs rendszereinek (a továbbiakban: kijelölt rendszer) osztályba sorolására és az érintett szervek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,

b) a hozzá érkező, biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása,

c) kapcsolattartás és együttműködés a hatósággal, a Nemzeti Média- és Hírközlési Hatósággal, valamint az eseménykezelő központokkal.

**21. §** A kijelölt hatóság a zárt célú elektronikus információs rendszerek, illetve a kijelölt rendszerek és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, a zárt célú elektronikus információs rendszer, illetve kijelölt rendszer védelmére vonatkozó intézkedést, amellyel az érintett zárt célú elektronikus információs



rendszert, illetve kijelölt rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:

- a) a jogszabályokban foglalt biztonsági követelmények és az ezekhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
- b) a követelményeknek való megfeleléség alátámasztásához szükséges dokumentumokat bekérni,
- c) a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában az információbiztonsági követelmények megtartását ellenőrizni, azokra ajánlásokat tenni,
- d) a fejlesztési projektek tervezési szakaszában szakmai részvételt biztosítani és a biztonsági követelmények beépülésének ellenőrzésére irányuló tevékenységet folytatni,
- e) a sérülékenységek megszüntetésére vonatkozó intézkedési tervet készíteni.

**22. § (1)** A kijelölt hatóság az Ibtv. hatósági nyilvántartásra vonatkozó szabályai szerinti nyilvántartást vezet.

(2) A zárt célú elektronikus információs rendszert működtető szervezet az Ibtv. szerinti adatokat, valamint ezek változásait 8 napon belül megküldi a kijelölt hatóságnak.

**23. § (1)** A kijelölt hatóság az ellenőrzést a zárt célú elektronikus információs rendszert, illetve a kijelölt rendszert működtető szervezet irányítását ellátó miniszter által jóváhagyott éves ellenőrzési terv vagy egyedi utasítás alapján végzi.

(2) Ha a kijelölt hatóság azt állapítja meg, hogy a zárt célú elektronikus információs rendszert működtető szervezet a biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, akkor az érintettet felszólítja a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére.

**9. A polgári hírszerző tevékenységhez kapcsolódó, a honvédelmi célú elektronikus információs rendszerek, valamint a létfontosságú létesítmények, rendszerek elektronikus információs rendszerei biztonsági felügyeletét ellátó hatóságok és feladataik**

**24. § (1)** A Kormány a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei biztonságának felügyeletét ellátó hatósággént a .....jelöli ki.

(2) Az (1) bekezdés szerinti hatóságra az Ibtv. 14-17. §-a helyett e rendelet 20-22. § szerinti rendelkezéseket megfelelően kell alkalmazni.

**25. § (1)** A Kormány a honvédelmi célú elektronikus információs rendszerek biztonságának felügyeletét ellátó hatósággént a honvédelemért felelős minisztert jelöli ki, aki a felügyeletet

- a) a Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata esetében a hálózatgazda;

b) a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) hálózatai esetében a KNBSZ főigazgatója;

c) a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerek esetében a honvédelmi igazgatás központi döntés-előkészítő és végrehajtás-koordináló szakmai szerv vezetője útján látja el.

(2) Az (1) bekezdés szerinti hatóságra az Ibtv. 14-17. §-a helyett a 20-22. § szerinti rendelkezéseket megfelelően kell alkalmazni.

**26. §** (1) A hatóság, a 15-18. §, valamint a 24. és 25. § szerinti hatóságok hatáskörébe tartozó elektronikus információs rendszerek kivételével, a Kormány az európai vagy nemzeti létfontosságú rendszerré, létesítménnyé törvény alapján kijelölt rendszerek, létesítmények elektronikus információs rendszerei biztonságának felügyeletét ellátó hatóságként a BM Országos Katasztrófavédelmi Főigazgatóságot jelöli ki.

(2) Az (1) bekezdés szerinti hatóságra az Ibtv. 14-17. §-a helyett e rendelet 20-22. § szerinti rendelkezéseket megfelelően kell alkalmazni.

## **10. Az információbiztonsági felügyelő**

**27. §** (1) Információbiztonsági felügyelőként (a továbbiakban: felügyelő) az rendelhető ki, aki a kirendelést vállalja. A felügyelőnek a vezetői gyakorlatára előírt időtartamába beszámítható a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény 8. § (5) bekezdése szerinti munkavégzésre irányuló jogviszonyban szerzett, közigazgatáson kívüli vezetői gyakorlat is. A felügyelő felett a munkáltatói jogokat a miniszter gyakorolja.

(2) A felügyelő egyidejűleg több érintett szervezethez is – ha a kirendelés indokai ezt lehetővé teszik – kirendelhető.

(3) A miniszter a megbízólevél kiállításával a felügyelőt határozott időtartamra rendeli ki az adott szerv elektronikus információbiztonsági tevékenységének felügyeletére. A kirendelés meghosszabbítására a kirendelés idejének lejártá előtt, legfeljebb egy alkalommal kerülhet sor, a folyamatban lévő intézkedések lezárásáig. A kirendelés időtartamának meghatározásakor figyelemmel kell lenni az érintett szervezet kötelezettségzegésének súlyára és a fenyegetés elhárításához szükséges védelmi intézkedésekre. A kirendelésről szóló megbízólevél megfelelően tartalmazza a kirendelés célját, tárgyát, a kirendelésre okot adó körülményeket, jogszabályi hivatkozást, a kirendelés várható időtartamát, az információbiztonsági felügyelő személyazonosításához szükséges adatokat.

(4) Felügyelőnek nem rendelhető ki az a személy, aki

a) az érintett szervezettel munkavégzésre irányuló jogviszonyban áll,

b) a kirendelést megelőző három évben az adott szervezettel munkavégzésre irányuló jogviszonyban állt,

- c) a kirendeléskor, vagy a kirendelést megelőző három évben az adott szervezetnél rendszeres és tartós megbízási vagy vállalkozási jogviszonyban áll, vagy állt,
- d) az adott szerv vezetőjének, gazdasági vezetőjének vagy alkalmazottjának hozzátartozója e minőségének fennállása alatt,
- e) az adott szervezet képviselője e minőségének fennállása alatt, és annak megszűnésétől számított három évig, továbbá
- f) az, akitől az adott helyzet tárgyilagos megítélése üzleti érdekeltségből vagy egyéb okból nem elvárható (elfogultság).

(5) A felügyelő kirendelésének megszűnésére a megbízólevélben meghatározott időtartam letelte előtt akkor kerülhet sor, ha

- a) a kirendelés oka elhárult és a felügyelő összefoglaló beszámolóját a hatóság elfogadta, vagy
- b) a felügyelőt a miniszter visszahívja.

(6) A felügyelőt a miniszter visszahívja, ha

- a) a hatóság megállapítja, hogy az adott szervnél a felügyelőnek felróhatóan nem érvényesülnek a biztonsági követelmények, vagy
- b) az (4) bekezdés szerinti, kizárásra okot adó körülmény merül fel, vagy a fennálló, a kizárásra okot adó körülmény a miniszter tudomására jut.

(7) A miniszter jogosult az (5) bekezdés b) pontja esetén új felügyelőt kirendelni.

(8) Az új felügyelő kirendelésére a hatóság vezetője tesz javaslatot.

(9) A felügyelő kirendelésének megszűnéséről a hatóság vezetője írásban haladéktalanul tájékoztatja az érintett szervezet vezetőjét.

**28. § (1)** A felügyelő jogosult a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok betartásával, teljesítésével összefüggésben

- a) az adott szerv vezetőitől és bármely dolgozójától írásbeli és szóbeli tájékoztatást, adatszolgáltatást kérni,
- b) az érintett szervezet információtechnológiával kapcsolatos valamennyi dokumentumába, okiratába betekinteni, arról másolatot, kivonatot készíttetni,
- c) az érintett szervezet valamennyi információtechnológiával kapcsolatos helyiségébe belépni,
- d) azonnali intézkedést javasolni a szerv vezetőjének a közvetlen fenyegetés elhárításához (működés korlátozása, leállítása),
- e) intézkedést javasolni a jogszabályszerű működés kialakításához vagy helyreállításához, ennek keretében különösen az érintett szabályzatok felülvizsgálatát kezdeményezni,
- f) előzetesen véleményezni a működéssel kapcsolatos elektronikus információbiztonságot is érintő intézkedéseket és
- g) kifogással élni az érintett szervezet által az Ibtv. alapján megtett vagy elmulasztott intézkedései, döntései tekintetében.

(2) A felügyelő köteles

- a) az érintett szervezetnél megbízólevelét bemutatni,

b) figyelemmel kísérni megbízatásának időpontjától kezdve az adott szervnél a jogszabályokban foglalt biztonsági követelmények és eljárások megvalósulását, a jogszabályokban előírt feladatok ellátását,

c) feltárni azokat az okokat, amelyek a kötelezettség nem teljesítéséhez vagy esetleg a fenyegetés kialakulásához vezettek,

d) a c) pontban foglaltak és az érintett szervezet működésének ismert feltételei alapján a szükséges intézkedések végrehajtására irányuló intézkedési tervet készíteni a szerv részére,

e) azonnali intézkedéseket kezdeményezni úgy, hogy azok bevezetése nem lehetetleníti el az alaptevékenység ellátását, valamint azokról haladéktalanul értesíti a hatóságot,

f) betartani a titoktartási kötelezettségre vonatkozó szabályokat,

g) a megtett intézkedésekről a hatóságnak folyamatosan beszámolni, a beszámolóban számot kell adni a megtett intézkedésekről, a biztonsági követelmények teljesüléséről, az elektronikus információbiztonság fejlődéséhez szükséges további intézkedésekről,

h) a megbízatásának megszűnésekor összefoglaló beszámolót készíteni a működéséről, ideértve a megtett intézkedéseket és azok eredményét, és a javasolt további intézkedéseket, amely elfogadásáról a hatóság dönt.

## **11. Jogorvoslat**

**29. § (1)** A hatóság határozatai ellen újrafelvételi eljárásnak nincs helye.

(2) A hatóság határozatainak felügyeleti jogkörben való visszavonására, módosítására nincs lehetőség.

## **12. A hatóságra vonatkozó vegyes rendelkezések**

**30. § (1)** Az elektronikus információbiztonsági szabályok érvényesülésének biztosítására az európai és nemzeti létfontosságú rendszerelemek nyilvántartására és a nyilvántartás adatainak kezelésére kijelölt szerv és a hatóság, valamint a kormányzati eseménykezelő központ kölcsönösen tájékoztatják egymást az európai vagy hazai létfontosságú rendszerek és rendszerelemek kapcsán feltárt, az elektronikus információbiztonságot érintő megállapításaikról.

(2) Az (1) bekezdés szerinti tájékoztatást haladéktalanul meg kell tenni, ha annak tárgya az elektronikus információbiztonságot fenyegető veszélyforrást tár fel, vagy biztonsági eseményre utal. Az értesítés alapján az érintett szervezetek a hatáskörükbe tartozó intézkedést – egymással koordinálva – azonnal megkezdik.

## **13. Záró rendelkezések**

**31. § (1)** Ez a rendelet – a (2) bekezdésben foglalt kivétellel – 2015. július 1-jén lép hatályba.

(2) A 33. § a) pontja 2016. január 1-jén lép hatályba.

**32. §** A 26. § szerinti hatóság feladatait 2016. január 1-jéig a hatóság látja el.

**33. §** Hatályát veszti

- a) a 32. §,
- b) a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet,
- c) a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet,
- d) a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet,
- e) a diplomáciai információs célokra használt zárt célú elektronikus információs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 3/2014. (II. 26.) KüM rendelet,
- f) a Nemzeti Adó- és Vámhivatal elektronikus információs rendszerei biztonságának felügyeletéről és ellenőrzéséről szóló 34/2013. (VIII. 30.) NGM rendelet,
- g) az Információs Hivatal elektronikus információs rendszereinek biztonsági felügyeletéről és ellenőrzéséről szóló 12/2015. (III. 6.) MvM rendelet.

## **Indoklás**

### **Az 1. alcímhez**

Az értelmező rendelkezés elsődleges célja a joganyag könnyebb kezelhetősége. A rendelkezés az IT világában ismert, de a magyar joganyagban még újdonságnak számító fogalmat határoz meg, amely jogszabályi intézményesítése fontos előrelépés a biztonság területén.

### **A 2-3. alcímhez**

A hatóság kijelölését eljárási szabályait tartalmazza. Az eljárási határidő a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvénytől (továbbiakban: Ket.) eltérő szabályozása azon alapul, hogy az információbiztonsággal kapcsolatos dokumentációk értékelése, az esetleg szükséges (akár műszaki) vizsgálatok elvégzése jelentős időtartamot vehet igénybe, különös tekintettel arra, hogy a Javaslat az információbiztonság szintjének emelését, a biztonsági intézkedések tudatos kialakítását tekinti elsődleges szempontnak, ezért elsősorban a hatóság és az érintett szervezetek közötti párbeszédre törekszik. Azonnali eljárási cselekmények bevezetésére elsősorban akkor kerül sor, ha azt a kialakult veszélyhelyzet, vagy veszély megköveteli.

Fontos, hogy a hatóság széles spektrumú jogosítványokkal rendelkezzen, de az IT biztonság érdekében – tekintettel a biztonsági események gyors bekövetkezésére, és hatásainak rendkívül gyors továbbgyűrűzésére – azonnali beavatkozási lehetőségekkel is bírjon.

Garanciális elem, hogy a helyszíni és egyéb ellenőrzés keretei szabályozottak, és ügyfélcentrikusak, ugyanakkor a kibertér védelme érdekében kellően célhoz kötöttek.

Az eljárási cselekmények a Ket.-re épülnek, de attól – a jogterület specialitásai, illetve az eljárás tárgyának jellegzetességei miatt – el is térnek, a hatóság eljárását az IT területre szűkítik.

#### **A 4. alcímhez**

A külföldön történő adatkezelés információvédelmi szempontból igen kényes terület, ezért fontos részletesen szabályozni az Ibtv. céljainak teljesülése érdekében.

Magyarország érdeke, hogy a nemzeti adatvagyon kulcsfontosságú rendszerei nyomon követhetők, ellenőrizhetők legyenek a biztonság érdekében. Fontos az is, hogy az ezzel kapcsolatos tevékenység elsősorban itthon történjen a hazai kapacitások kihasználása érdekében, ugyanakkor az EU-ban történő adatfeldolgozás, üzemeltetés nem zárható ki.

Az Ibtv. szövegéből következik, hogy az EU-n kívüli adatfeldolgozás, üzemeltetés nem lehetséges, mivel az jelentős biztonsági kockázatot jelent.

Az ilyen tevékenységet be kell jelenteni, hogy az a hatóság tudomására jusson, és ellenőrizhesse a jogszabályi kötelezettségek teljesülését.

Ugyancsak be kell jelenteni az egyébként legálisan, nemzetközi szerződés alapján megvalósuló üzemeltetést, adatkezelést, mivel fontos cél a teljes kibertér feltérképezése. Természetesen az ilyen bejelentés elmaradását szankcionálni nem lehet, illetve ezekkel kapcsolatban a hatósági döntés meghozatala indokolatlan.

Fontos, hogy az információtechnológiai fejlesztések, beszerzések során a biztonsági követelmények maradéktalanul teljesüljenek, és azok a rendszer életében fennálljanak, ami napjainkban még nem természetes. Az Ibtv. ezt kógens szabályként iktatta be. Ugyanakkor a tervezet a reális folyamatokhoz igazodva határozza meg a követelményeket.

A biztonsági osztályba sorolás, illetve biztonsági szint meghatározásának ellenőrzése az érintett szervezetek jogkövető magatartását feltételező adminisztratív eljárás. Hatósági beavatkozásra csak akkor kerül sor, ha a törvényi kötelezettségek nem teljesülnek.

#### **Az 5. alcímhez**

A tervezet tisztázza az ügyfél feladatait abban az esetben, amikor egyes törvényi kötelezettségeinek nem tud eleget tenni. Egyértelműsíti a törvény szövegéből kiindulva, hogy nem köteles minden egyes érintett szervezet a biztonságért felelős főállású személyt alkalmazni, iránymutatást ad egyes kötelezettségek teljesítésének módjára. A biztonsági események bejelentése fontos kötelezettség, ugyanakkor az adminisztratív terheket elviselhetetlenné tenné, ha minden, jelentéktelen biztonsági eseményt be kellene jelenteni. Ugyanakkor minden – jellegétől független – biztonsági eseményt nyilván kell tartania az érintett szervezetnek, de ez pusztán technológiai napló, amelynek kialakítása az érintett szervezet egyéni megoldásán alapul (pl.: akár egy géptermi napló is alkalmas lehet erre a célra).

#### **A 6. alcímhez**

Az ellenőrzési terv szempontjából lényeges, hogy széleskörű egyeztetésen alapul, figyelembe veszi a tapasztalatokat. Lehetőséget kell azonban biztosítani arra, hogy a kibervilágban nem szokatlan, jelentős erőforrásokat lekötő váratlan események prioritást kapjanak az előzetesen

rögzített ellenőrzési tervhez képest, de ennek meg legyen a megfelelő visszacsatolása az érintett miniszterek felé.

#### **A 7. alcímhez**

Kiemelt szempont – mivel a kiberbiztonság megteremtése az elsődleges – hogy a hatóság ne a büntetésre, hanem biztonság, mint cél elérésére összpontosítson. Ezt szolgálja az ügyféllel való egyeztetés, a bírság kereteinek szélesre nyitása, a mérlegelési szempontok megállapítása.

#### **A 8-9. alcímhez**

A tervezet meghatározza a zárt célú elektronikus információs rendszereket. A rendelet kijelöli az egyes területekért felelős hatóságokat. A zárt célú elektronikus információs rendszerek biztonsági felügyeletével, valamint ellenőrzésével kapcsolatban kijelölt hatóság működésére, feladatára vonatkozó speciális szabályok kerülnek meghatározásra.

A tervezet kijelöli a polgári hírszerző tevékenységhez kapcsolódó, a honvédelmi célú elektronikus információs rendszerek, valamint a létfontosságú létesítmények, rendszerek elektronikus információs rendszerei biztonsági felügyeletét ellátó hatóságokat, és meghatározza rájuk vonatkozó, az általánostól eltérő speciális szabályokat.

#### **A 10. alcímhez**

Az információbiztonsági felügyelő kirendelése kényszerintézkedés. Ezért arra nem alkalmazhatók a közszolgálati tisztviselőkről szóló 2011. évi CXCV. törvény (a továbbiakban: Kttv.) kirendelésről szóló rendelkezései. Jelen esetben ugyanis a „kirendelt”, vagy kijelölt személy számára az utasítás adási jogot a kijelölő gyakorolja a felügyelő felé, és a felügyelő is a kirendelő felé tartozik beszámolási kötelezettséggel. A kirendelés megbízólevéllel történik. Az érintett szervezet semmilyen jogot nem gyakorolhat a felügyelő fölött, azzal együttműködni köteles. Fontos elem a felügyelő kijelölésének feltételrendszere, illetve a jogainak és kötelemeinek pontos szabályozása. A felügyelő széles körű jogosultságokkal rendelkezik annak érdekében, hogy az érintett szervezet kötelezettségei teljesüljenek.

#### **A 11. alcímhez**

Tekintettel a hatóság szervezeten belüli státuszára, a jogorvoslat bírói útra terelése a kívánatos. A hatóság döntéseinek gyors végrehajtása az IT biztonság szempontjából kívánatos.

#### **A 12. alcímhez**

A magyar információs társadalom, a kibertér védelme nem egyes szervek és szervezetek külön-külön eljárásáról szól, hanem azok egymás felé irányuló kölcsönös támogatásáról, a szükséges

információk rendelkezésre bocsátásáról, az együttműködésről. Az információbiztonság szervezetrendszerének egységes egészként kell működnie.

Az információbiztonsági operatív munkacsoportot törvényi felhatalmazás alapján lehetőséget biztosít az érintett szervezetekkel való konzultációra, a tudás, a „best practice” átadására, véleménynyilvánításra, egyeztetésre, illetve a gyors, összehangolt fellépésre. Ez a munkacsoport már napjainkban is működik, jellegét tekintve nagyban hasonlít a katasztrófa védelem operatív törzsére. Mivel ez a munkacsoport nem hatóság, tevékenységének szabályozása nem lehet az előterjesztés tárgya.

### **A 13. alcímhez**

A jelenleg hatályos, a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII. 29.) Korm. rendelet módosításának mértékére tekintettel új kormányrendelet megalkotása és a korábbi rendelet hatályon kívül helyezése vált indokolttá. Az Ibtv.-módosítás eredményeként kormányrendeletben kell meghatározni az egyes speciális elektronikus információs rendszerek tekintetében eljáró hatóságokat, eseménykezelő központokat és feladataikat. Erre tekintettel hatályon kívül kell helyezni az e rendszerekre vonatkozó szabályozást tartalmazó miniszteri rendeleteket.