2013. évi L. törvény

az állami és önkormányzati szervek elektronikus információbiztonságáról [1]

A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.

Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. Értelmező rendelkezések

1. § (1) E törvény alkalmazásában

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. *adatfeldolgozás:* az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

3. *adatfeldolgozó:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

4. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

5. *adatkezelő:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

6. *adminisztratív védelem:* a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

7. *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

1 Kihirdetve: 2013. IV. 25.

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

9. *biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

10. *biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

11. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

12. *biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

13. *biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

14. *biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

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

16. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

17. *észlelés:* a biztonsági esemény bekövetkezésének felismerése;

18. *felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre;

19. *fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

20. *fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

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

22. *globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

23. *informatikai biztonságpolitika:* a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

24. *informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

25. *információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

26. *kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez működtetéséhez;

27. *kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

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

29. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

30. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

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

32. *korai figyelmeztetés:* valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

33. *létfontosságú információs rendszerelem:* az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

34. *logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

35. *magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

36. *megelőzés:* a fenyegetés hatása bekövetkezésének elkerülése;

37. *reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

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

39. *sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elekt-

ronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

40. *sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

41. *sérülékenységvizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

42. *számítógépes incidenskezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

43. *szervezet:* az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;

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

45. *üzemeltető:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

46. *védelmi feladatok:* megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

47. *zárt célú elektronikus információs rendszer:* jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

48. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

(2) E törvény alkalmazásában elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese:

a) számítástechnikai rendszerekés hálózatok;

b) helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;

c) rádiós vagy műholdas navigáció;

d) automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);

e) a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

(3) E törvény alkalmazásában egy elektronikus információs rendszernek kell tekinteni az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön (környezeti infrastruktúra, hardver, hálózat), egymással összefüggő eljárásokkal (szabályozás, szoftver és kapcsolódó folyamatok) azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.

2. A törvény hatálya

2. § (1) E törvény rendelkezéseit kell alkalmazni:

a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,

b) a Köztársasági Elnöki Hivatalra,

c) az Országgyűlés Hivatalára,

d) az Alkotmánybíróság Hivatalára,

e) az Országos Bírósági Hivatalra és a bíróságokra,

f) az ügyészségekre,

g) az Alapvető Jogok Biztosának Hivatalára,

h) az Állami Számvevőszékre,

i) a Magyar Nemzeti Bankra,

j) a fővárosi és megyei kormányhivatalokra,

k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,

l) a Magyar Honvédségre.

(2) E törvény rendelkezéseit kell alkalmazni:

a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők,

b) a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,

c) az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek

elektronikus információs rendszereinek védelmére.

(3) A minősített adatokat kezelő elektronikus információs rendszereket érintően

a) e törvény rendelkezéseit a minősített adat védelmére vonatkozó jogszabályokban meghatározott eltérésekkel kell alkalmazni,

b) a 14–18. §¬ban meghatározott feladatok ellátásáról a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

(4) A 14–18. §¬ban meghatározott feladatok ellátásáról:

a) a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat zárt célú elektronikus információs rendszerei, továbbá a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a honvédelemért felelős miniszter,

b) a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek zárt célú elektronikus információs rendszerei esetében a rendvédelmi szervet irányító miniszter,

c) a diplomáciai információs célokra használt zárt célú elektronikus információs rendszerei esetében a külpolitikáért felelős miniszter,

d) a Nemzeti Adó- és Vámhivatalnak az állami költségvetési bevételek biztosítását támogató elektronikus információs rendszerei esetében az adópolitikáért felelős miniszter,

e) az Információs Hivatal esetében a Kormány polgári hírszerzési tevékenység irányításáért felelős tagja,

f) a Nemzeti Média- és Hírközlési Hatóság esetében a Nemzeti Média- és Hírközlési Hatóság elnöke

jogszabályban meghatározottak szerint gondoskodik.

(5) E törvény rendelkezéseit médiaszolgáltatási és elektronikus hírközlési tevékenység esetén az elektronikus hírközlésről szóló törvényben és az abban meghatározott elektronikus hírközlésre vonatkozó szabályban, továbbá a médiaszolgáltatásokról és tömegkommunikációról szóló törvényben

és az abban meghatározott médiaigazgatásra vonatkozó szabályban meghatározott eltérésekkel kell alkalmazni.

3. § (1) A 2. § (1) bekezdés *a)–k)* pontjában megjelölt szervek által kezelt adatok és a 2. § (2) bekezdés *b)* pontjában megjelölt szervezetek által kezelt, a nemzeti adatvagyon részét képező adatok Magyarország területén üzemeltetett elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek.

(2) A 2. § (2) bekezdés *c)* pontjában megjelölt elektronikus információs rendszerek – az (1) bekezdésben meghatározott kivétellel – az Európai Unió tagállamai területén üzemeltethetőek.

(3) A 2. § (1) bekezdés *a)–k)* pontjában megjelölt szervek által kezelt adatok elektronikus információs rendszerei az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezeti egység (a továbbiakban: hatóság) engedélyével vagy nemzetközi szerződés alapján az Európai Unió tagállamainak területén belül üzemeltetett elektronikus információs rendszerekben is kezelhetőek.

(4) A törvény hatálya alá tartozó elektronikus információs rendszert működtető, nem Magyarországon bejegyzett vállalkozásnak Magyarország területén működő képviselőt kell kijelölnie, aki az e törvényben foglaltak végrehajtásáért a szervezet vezetőjére vonatkozó szabályok szerint felel.

4. § Az elektronikus információs rendszerekre és eszközökre, szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat a hatóság az eljárása során figyelembe veszi.

II. FEJEZET

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

3. Alapvető elektronikus információbiztonsági követelmények

5. § Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása

zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

6. § Az elektronikus információs rendszernek az 5. §¬ban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

d) a biztonsági események kezelését.

4. Az elektronikus információs rendszerek biztonsági osztályba sorolása

7. § (1) Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.

(2) A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

(3) A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

(4) Az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján kell megvalósítani az 5. és 6. §¬ban előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

(5) A szervezet vezetője az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

8. § (1) A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

(2) A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is el kell végezni, ha a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

(3) A 7. § (2) bekezdésében foglaltakkal összhangban előírt, az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek lehetősége van a biztonsági intézkedések fokozatos kivitelezésére. Ennek keretében az első vizsgálatkor megállapított biztonsági osztályt alapul véve, minden egyes következő, magasabb biztonsági osztályhoz rendelt biztonsági intézkedések kivitelezésére két év áll rendelkezésére.

(4) A szervezet a jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és ennek alapján meghatározza, hogy azok a vizsgálat elvégzésekor melyik biztonsági osztálynak felelnek meg.

(5) Ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet készít a hiányosság megszüntetésére.

(6) A hatóság a szervezet – kivéve a 2. § (3) és (4) bekezdésében meghatározott elektronikus információs rendszerek esetében – által megállapított biztonsági osztályt felülbírálhatja és magasabb, indokolt esetben alacsonyabb szintű osztályba sorolást is megállapíthat.

5. Az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintje

9. § (1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

(2) A szervezet biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább

a) a 2. § (1) bekezdés *b)–d)* , *g)* és *k)* pontjába tartozó szervezetek esetén 2.,

b) a 2. § (1) bekezdés *a)* , *e)* , *f), h)–j)* pontjába tartozó szervezetek esetén 3.,

c) a 2. § (1) bekezdés *l)* pontjába tartozó szervezetek esetén 4.,

d) a 2. § (2) bekezdés *b)* és *c)* pontjába tartozó szervezetek esetén 5.

szintű.

(3) A szervezet az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb szintű besorolást is megállapíthat.

(4) A hatóság – a 2. § (3) és (4) bekezdésében meghatározott elektronikus információs rendszerek esetében az elektronikus információs rendszerek biztonságának felügyeletét és ellenőrzését ellátó ágazati szerv – a szervezet által megállapított biztonsági szintet felülbírálhatja és magasabb, indokolt esetben alacsonyabb szintű besorolást is megállapíthat.

10. § (1) A szervezet a jogszabályban meghatározott szempontok alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági szintnek felel meg.

(2) Ha a vizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre a 9. § (2) bekezdésében előírt biztonsági szint, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(3) Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, akkor az 1. szint eléréséhez szükséges intézkedéseket az (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő egy éven belül meg kell valósítani.

(4) A 9. § (2) bekezdésében előírt biztonsági szint teljesítése során a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére – minden egyes szintet érintően, a következő magasabb szintre lépéshez – két év áll rendelkezésére.

(5) A biztonsági szint meghatározását a 9. § (2) bekezdésében előírt biztonsági szint elérését követően legalább háromévenként, szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

(6) Az elektronikus információs rendszer biztonságát érintő változás esetén, illetve új elektronikus információs rendszer bevezetésekor a szervezet biztonsági szintbe sorolását soron kívül meg kell ismételni.

(7) Ha a soron kívüli felülvizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre előírt biztonsági szint, akkora szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(8) A szervezet biztonsági szintbe sorolását a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági szintbe sorolás eredményét a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,

d) kiadja a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját,

e) meghatározza a szervezet elektronikus információs rendszereinek informatikai biztonsági stratégiáját,

f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

(2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője az (1) bekezdés *k)* és *l)* pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

(3) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén az (1) és (2) bekezdésben írt feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírköz-

lési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval és a szervezet vezetőjével.

(4) Az (1) bekezdés *d)* és *e)* pontja tekintetében a szakmai irányítást ellátó miniszter meghatározhatja az elektronikus információs rendszerekre vonatkozó ágazati informatikai biztonságpolitikát és az ágazati informatikai biztonsági stratégiát, melyeket a szervezet vezetője az (1) bekezdésben előírt feladatainak ellátása során köteles figyelembe venni.

12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:

a) a 11. § (1) bekezdés *c)* pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,

b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,

c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja

a hatóság részére.

13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az *a)* pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

(3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

(10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

(11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

III. FEJEZET

AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI FELÜGYELETE

7. Az elektronikus információs rendszerek biztonságának felügyelete

14. § (1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét – a 2. § (3) és (4) bekezdésben meghatározott kivétellel – az informatikáért felelős miniszter látja el a hatóság útján, amely az informatikáért felelős miniszter által vezetett minisztérium szervezeti keretében önálló feladatkörrel és hatósági jogkörrel rendelkező szervezeti egység.

(2) A hatóság feladata:

a) az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,

b) az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,

c) az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,

d) a rendelkezésre álló információk alapján kockázatelemzés elvégzése,

e) a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása,

f) javaslattétel a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére,

g) az információs társadalom biztonságtudatosságának elősegítése és támogatása,

h) együttműködés a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvényben meghatározott elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,

i) kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,

j) kapcsolattartás a Nemzeti Média- és Hírközlési Hatósággal, továbbá a kormányzati eseménykezelő központtal és az ágazati eseménykezelő központokkal, a kormányzati incidens-kezelő munkacsoport irányítása,

k) véleményezési jog gyakorlása a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,

l) együttműködés a kormányzati eseménykezelő központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal,

m) együttműködés a Nemzeti Média- és Hírközlési Hatósággal és a Nemzeti Biztonsági Felügyelettel, ha a biztonsági esemény vagy fenyegetés az 1. § (2) bekezdés *b)* pontjában meghatározott elektronikus információs rendszert vagy az 1. § (2) bekezdés *b)* pontjában meghatározott szolgáltatás nyújtóját érinti,

n) éves és egyedi jelentések készítése a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban.

(3) A hatóság (2) bekezdés *a)* , *b)* és *e)* pontjában meghatározott feladatának ellátása során a Nemzeti Biztonsági Felügyelet szakhatóságként jár el.

(4) A (2) bekezdés *a)* és *b)* pontjában foglalt feladatok ellátása körében a hatóság javaslatára az informatikáért felelős miniszter az e-közigazgatásért felelős miniszter egyetértésével, valamint a minősített adatok védelmének szakmai felügyeletéért felelős miniszter és a katasztrófák elleni védekezésért felelős miniszter javaslatainak figyelembevételével éves ellenőrzési tervet (a továbbiakban: éves ellenőrzési terv) készít.

15. § (1) A hatóság nyilvántartja és kezeli

a) a szervezet azonosításához szükséges adatokat,

b) a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,

c) a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,

d) a szervezet informatikai biztonsági szabályzatát,

e) a biztonsági eseményekkel kapcsolatos bejelentéseket.

(2) Az (1) bekezdésben meghatározott adatok kezelésének célja az elektronikus információs rendszerek védelmével kapcsolatos kötelezettségek teljesítése és hatósági ellenőrzésének biztosítása.

(3) A szervezet az (1) bekezdés *a)–c)* pontjában meghatározott adatokat és ezek változásait megküldi a hatóságnak a nyilvántartásba vétel érdekében.

(4) Az (1) bekezdésben meghatározott nyilvántartásból – ha törvény eltérően nem rendelkezik – adattovábbítás nem végezhető.

(5) Ha a szervezet e törvény hatálya alá tartozó tevékenységet már nem végez, akkor az (1) bekezdésben meghatározott adatokat a hatóság a tevékenység befejezése bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(6) Ha az (1) bekezdésben meghatározott adatok változását a szervezet bejelenti, akkor az eredeti adatokat a hatóság az adat változása bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

16. § (1) A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:

a) az érintett szervezeteknél a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,

b) a követelményeknek való megfelelőség alátámasztásához szükséges dokumentumokat bekérni, illetve a 12. § *b)* pontja alapján megküldött dokumentációt felülvizsgálni,

c) a 7–8. § szerinti biztonsági osztályba sorolást, a 9–10. § szerinti biztonsági szint megállapítását, vagy a védelmi intézkedéseket ellenőrizni, az ott feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,

d) a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását,

e) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervezni,

f) a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviselni Magyarországot,

g) véleményezési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.

(2) A (3) bekezdésben meghatározott kivétellel, ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság

a) köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,

b) ha az *a)* pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető.

(3) Ha a szervezet költségvetési szerv, és a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság

a) köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,

b) ha az *a)* pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, a szervezetet felügyelő szervhez – ha a szervezet azzal rendelkezik – fordulhat és kérheti a közreműködését,

c) ha az *a)* és *b)* pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, információbiztonsági felügyelő kirendelését kezdeményezheti.

8. Információbiztonsági felügyelő

17. § (1) Az információbiztonsági felügyelőt a hatóság javaslatára az informatikáért felelős miniszter a 16. § (3) bekezdése szerinti esetben rendelheti ki.

(2) Az információbiztonsági felügyelő a fenyegetés elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében a Kormány által rendeletben meghatározott intézkedéseket, eljárásokat javasolhat, a szervezet intézkedései tekintetében kifogással élhet. Az információbiztonsági felügyelő pénzügyi kötelezettségvállalásra nem jogosult.

(3) Az információbiztonsági felügyelő határozott időtartamra szóló kirendeléséről és a kirendelés visszavonásáról az informatikáért felelős miniszter gondoskodik. Az információbiztonsági felügyelő tevékenységének szakmai irányítását az informatikáért felelős miniszter látja el.

(4) Az információbiztonsági felügyelő az informatikáért felelős miniszter által vezetett minisztérium kormánytisztviselője, akinek a kormányzati szolgálati jogviszonyára a minisztériumban főosztályvezető-helyettesi munkakörben alkalmazott kormánytisztviselőre vonatkozó szabályokat kell alkalmazni.

(5) Információbiztonsági felügyelőnek az a személy nevezhető ki, aki rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel, valamint legalább 3 év vezetői gyakorlattal.

9. A Nemzeti Biztonsági Felügyelet feladatai az elektronikus információs rendszerek biztonsága vonatkozásában

18. § A Nemzeti Biztonsági Felügyelet

a) éves ellenőrzési terv alapján, és az e törvény 14. § (2) bekezdés *a)* , *b)* és *e)* pontjában foglaltakra tekintettel:

a) szakhatóságként a hatóság megkeresésére, továbbá

b) egyedi esetekben a hatóság felkérésére

az érintett szervezet vezetőjét előzetesen tájékoztatva sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,

b) a szervezetek elektronikus információs rendszerében a szervezet felkérésére sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,

c) a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálat lezárását követően haladéktalanul tájékoztatja a vizsgált szervezet vezetőjét,

d) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez,

e) a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot,

f) véleményezési jogot gyakorol a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,

g) az *a)–c)* pontban foglalt feladatok végrehajtásáról a hatóság részére tájékoztatást ad,

h) együttműködik a kormányzati eseménykezelő központtal.

10. A kormányzati eseménykezelő központ

19. § (1) A Kormány az e törvényben foglalt biztonsági események kezelése érdekében kormányzati eseménykezelő központot működtet a katasztrófák elleni védekezésért felelős miniszter irányítása alatt. A kormányzati eseménykezelő központhoz a 2. § (1) bekezdésben meghatározott szervek tartoznak.

(2) A 2. § (4) bekezdésében meghatározott szervezetek és az önálló szabályozó szervek az eseménykezelési feladatok ellátása érdekében ágazati eseménykezelő központot hozhatnak létre.

(3) Az ágazati eseménykezelő központ a biztonsági eseményekhez kapcsolódó és az (5) bekezdés szerinti együttműködés során tudomására jutott biztonsági események adatait köteles haladéktalanul a kormányzati eseménykezelő központ részére továbbítani.

(4) A kormányzati eseménykezelő központ az európai kormányzati eseménykezelő csoport által akkreditált nemzeti eseménykezelő központként részt vesz a kormányzati eseménykezelő központok nemzetközi együttműködésében.

(5) Az ágazati eseménykezelő központok a fenntartó döntése alapján részt vehetnek az eseménykezelő központok nemzetközi együttműködésében, és e célból akkreditálhatóak.

(6) Az ágazati eseménykezelő központok a kormányzati eseménykezelő központtal, mint nemzeti eseménykezelési koordinátorral, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal együttműködnek.

20. § (1) A kormányzati eseménykezelő központ ellátja a következő feladatokat:

a) az ágazati eseménykezelő központok szakmai támogatása,

b) a nemzetközi eseménykezelési együttműködésekben Magyarország képviselete és az ágazati eseménykezelő központok tájékoztatása a nemzetközi szervezetektől tudomására jutott információbiztonságot érintő eseményekről, fenyegetésekről,

c) a szervezetekkel való kapcsolattartás a bejelentett biztonsági események fogadására, valamint az azok kezeléséhez szükséges operatív intézkedések megtétele és koordinálása,

d) napi rendszerességű hálózatbiztonsági helyzetértékelések elvégzése,

e) folyamatosan elérhető 24 órás ügyelet működtetése,

f) a biztonsági események kivizsgálása során a jogszabályban meghatározottak szerint a biztonsági események adatai műszaki vizsgálatának elvégzése,

g) a szervezeteknél előforduló biztonsági események adatainak gyűjtése, ezekről negyedévente jelentés készítése a Nemzeti Kiberbiztonsági Koordinációs Tanács részére,

h) elemzések, jelentések készítése a Nemzeti Kiberbiztonsági Koordinációs Tanács részére a hazai és nemzetközi információbiztonsági irányokról,

i) azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági eseményekről, ezek magyar nyelvű megjelenítése,

j) a nemzetközileg publikált sérülékenységek közzététele a honlapján,

k) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatok szervezése,

l) felkérésre részvétel a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon,

m) együttműködés a hatósággal és a Nemzeti Biztonsági Felügyelettel.

(2) Az ágazati eseménykezelő központok – az (1) bekezdés *a)* és *b)* pontban meghatározottak kivételével – az általuk támogatott ágazatok tekintetében ellátják a kormányzati eseménykezelő központ feladatait.

11. A kormányzati koordináció biztosítása

21. § (1) A Miniszterelnökséget vezető államtitkár által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) a Kormány javaslattevő, véleményező szerveként gondoskodik a 2. § (1)–(4) bekezdésében meghatározott szervezetek e törvényben és végrehajtási rendeleteiben meghatározott tevékenységeinek összehangolásáról.

(2) A Tanács a Miniszterelnökséget vezető államtitkár vezetésével és a Miniszterelnökség által delegált kiberkoordinátor támogatásával:

a) összehangolja a törvény hatálya alá tartozó szervezetek együttműködését a kiberbiztonsággal összefüggő feladatok ellátásában;

b) elősegíti a kiberbiztonság szabályozását, valamint a kiberbiztonság ágazati munkacsoportjainak munkáját;

c) támogatja a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) munkáját;

d) támogatja a források hatékony felhasználását;

e) figyelemmel kíséri Magyarország Nemzeti Kiberbiztonsági Stratégiájának végrehajtását és erről jelentést tesz a Nemzetbiztonsági Kabinetnek;

f) elősegíti a kiberbiztonságot érintő egységes magyar kormányzati álláspont kialakítását és hozzájárul Magyarország nemzetközi politikai képviseletéhez.

(3) A Tanács munkáját az általa felkért szakmai, illetve nem kormányzati gazdasági vezetőkből álló Fórum és az ágazati kormányzati és nem kormányzati együttműködést biztosító kiberbiztonsági munkacsoportok segítik javaslattételi joggal és véleményezési lehetőséggel.

(4) A külpolitikáért felelős miniszter figyelemmel kíséri és a kormány feladat- és hatáskörrel rendelkező szervei, valamint a Tanács felé jelzi az európai uniós kibertér-politikával kapcsolatos eseményeket és döntéseket, és a külpolitikáért való felelőssége körében képviseli a magyar álláspontot a nemzetközi fórumokon és a kétoldalú kapcsolatokban.

12. Adatvédelmi rendelkezések

22. § (1) [2]A hatóság, a Nemzeti Biztonsági Felügyelet, a kormányzati eseménykezelő központ és az ágazati eseménykezelő központ munkatársai az e törvényben meghatározott, az elektronikus információs rendszerek védelmével összefüggő feladataik ellátása során megismert minősített adatot, személyes adatot vagy különleges adatot, üzleti titkot, banktitkot, fizetési titkot, biztosítási titkot, értékpapírtitkot, pénztártitkot, orvosi titkot és más hivatás gyakorlásához kötött titkot kizárólag a feladat ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével jogosultak kezelni. A feladatellátás befejezését követően a feladatellátáshoz kapcsolódóan rögzített adatokat kötelesek az elektronikus információs rendszereikből és adathordozóikról törölni.

(2) A hatóság, a Nemzeti Biztonsági Felügyelet, a kormányzati eseménykezelő központ és az ágazati eseménykezelő központ munkatársait az (1) bekezdés szerint megismert adatok tekintetében titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követően is fennmarad.

IV. FEJEZET

OKTATÁS-KÉPZÉS, KUTATÁS-FEJLESZTÉS

23. § A Nemzeti Közszolgálati Egyetem a képzési tevékenység ellátásával összefüggésben

a) a 11. § (1) bekezdés *g)* pontjában, a 13. § (8) bekezdésében meghatározott képzés érdekében kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját,

b) kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a 13. § (8) bekezdésében meghatározott képzettségi követelményeket,

c) gondoskodik a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről,

d) közreműködik az információbiztonsági, kibervédelmi, létfontosságú információs rendszer védelmi gyakorlatokon.

V. FEJEZET

ZÁRÓ RENDELKEZÉSEK

2 Módosította: 2013. évi CCXXXVI. törvény 155. §.

13. Felhatalmazó rendelkezések

24. § (1) Felhatalmazást kap a Kormány, hogy rendeletben meghatározza

a) a hatóság feladatának részletes szabályait, a hatósági ellenőrzés lefolytatásának részletes eljárási szabályait, [3]

b) a hatóság által kiszabható bírság mértékét, a bírság kiszabásának és befizetésének részletes eljárási szabályait, [4]

c) az információbiztonsági felügyelő kirendelésének szabályait, feladatkörét és eljárásának rendjét, [5]

d) a Nemzeti Biztonsági Felügyelet szakhatósági feladat- és hatáskörét, [6]

e) a kormányzati eseménykezelő központ és az ágazati eseménykezelő központok feladat- és hatáskörét, és [7]

f) a 21. § szerinti Tanács, Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokat, feladat- és hatáskörüket. [8]

(2) Felhatalmazást kap

a) az informatikáért felelős miniszter, hogy az e-közigazgatásért felelős miniszterrel és a minősített adatok védelmének szakmai felügyeletéért felelős miniszterrel egyetértésben meghatározza az 5. § és 6. §¬ban előírt technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre vonatkozó követelményeket, továbbá a 7–8. § szerinti biztonsági osztályba sorolás és a szervezetek 9–10. § szerinti biztonsági szintbe sorolásának követelményeit, [9]

b) a közigazgatás-fejlesztésért felelős miniszter, hogy az informatikáért felelős miniszterrel egyetértésben az e törvényben meghatározott vezetői, az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmát, [10]

c) az informatikáért felelős miniszter, hogy a szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjét [11]

rendeletben határozza meg.

(3) Felhatalmazást kap

a) a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat, továbbá a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a honvédelemért felelős miniszter, [12]

b) a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek esetében a rendvédelmi szervet irányító miniszter, [13]

c) a diplomáciai információs célokra használt rendszer esetében a külpolitikáért felelős miniszter,

d) a Nemzeti Adó- és Vámhivatal esetében az adópolitikáért felelős miniszter, [14]

3 Lásd: 301/2013. (VII. 29.) Korm. rendelet.
4 Lásd: 301/2013. (VII. 29.) Korm. rendelet.
5 Lásd: 301/2013. (VII. 29.) Korm. rendelet.
6 Lásd: 301/2013. (VII. 29.) Korm. rendelet.
7 Lásd: 233/2013. (VI. 30.) Korm. rendelet.
8 Lásd: 484/2013. (XII. 17.) Korm. rendelet.
9 Lásd: 77/2013. (XII. 19.) NFM rendelet.
10 Lásd: 26/2013. (X. 21.) KIM rendelet.
11 Lásd: 73/2013. (XII. 4.) NFM rendelet.
12 Lásd: 16/2013. (VIII. 30.) HM rendelet.
13 Lásd: 36/2013. (VII. 17.) BM rendelet.
14 Lásd: 34/2013. (VIII. 30.) NGM rendelet.

e) az Információs Hivatal esetében a Kormány polgári hírszerzési tevékenység irányításáért felelős tagja,

f) a médiaszolgáltatási és az elektronikus hírközlési tevékenység esetében a Nemzeti Média- és Hírközlési Hatóság elnöke,

g) a minősített adatokat kezelő elektronikus információs rendszerek esetében a minősített adatok védelmének szakmai felügyeletéért felelős miniszter,

hogy az elektronikus információs rendszer biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokat rendeletben határozza meg.

14. Hatálybalépés

25. § Ez a törvény 2013. július 1-jén lép hatályba.

15. Átmeneti rendelkezések

26. § (1) A szervezetnek a már működő elektronikus információs rendszerei 7. § szerinti biztonsági osztályba sorolását első alkalommal az e törvény hatálybalépését követő egy éven belül el kell végezni.

(2) A szervezetnek a szervezet 10. § szerinti biztonsági szintbe sorolását első alkalommal az e törvény hatálybalépését követő egy éven belül el kell végezni.

(3) A szervezet a 15. § (1) bekezdés *a)* és *c)* pontjában foglalt adatokat az e törvény hatálybalépésétől számított 60 napon belül, a 15. § (1) bekezdés *d)* pontjában foglalt szabályzatot az e törvény hatálybalépésétől számított 90 napon belül nyilvántartásba vétel céljából köteles bejelenteni a hatóságnak.

(4) A törvény hatálybalépésekor az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó személyeknek a 13. § (8) bekezdésben előírt képzési követelményeknek a hatálybalépést követő öt éven belül kell eleget tenniük.

16. [15]

27 - 29. § [16]

15 Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2013. VII. 2-től.
16 Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2013. VII. 2-től.