2013. évi L. törvény

az állami és önkormányzati szervek elektronikus információbiztonságáról

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

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

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

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

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

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

6a. *alapvető szolgáltatásokat nyújtó szolgáltató:* a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 2/A. §-a alapján kijelölt szolgáltató;

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

7a. *bejelentés-köteles szolgáltatás:* az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § *j)* pontjában meghatározott szolgáltatás;

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;

14a. *EGT-állam:* az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott állam;

14b. *elektronikus információs rendszer:*

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

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. *honvédelmi célú elektronikus információs rendszer:* a honvédelmi szervezetek, a honvédelemért felelős miniszter fenntartói irányítása alá tartozó, honvédségi szervezetnek nem minősülő többcélú szakképző intézmény, a honvédelemért felelős miniszter tulajdonosi joggyakorlása alá tartozó gazdasági társaságok, az állami vagyonról szóló 2007. évi CVI. törvény 3. § (2) bekezdés *c)* pontja szerinti gazdasági társaságok, valamint jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok zárt célú elektronikus információs rendszereinek, valamint egyéb - funkciója, rendeltetése, feladatellátása szerint - nyílt elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést;

24.

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;

32a. *kritikus adat:* a személyes adat vagy valamely jogszabállyal védett adat;

33. *létfontosságú információs rendszerelem:* az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt 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 elektronikus 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;

41a. *súlyos biztonsági esemény:* olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

42. *számítógépes eseménykezelő 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 végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

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

45. *üzemeltető:* az a természetes személy, jogi személy 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:* a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja;

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

(2)

(3) E törvény alkalmazásában egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

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 vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek,

d) az alapvető szolgáltatást nyújtó szereplőknek az alapvető szolgáltatás nyújtásában közreműködő,

e) a nemzetbiztonsági védelem alá eső szervek

elektronikus információs rendszereinek védelmére.

(3) A Kormány rendeletében meghatározott, a honvédelmért felelős miniszter vezetése, irányítása alatt álló szervek zárt célú elektronikus információs rendszerei esetében az e törvény szerinti hatósági feladatokat, a biztonsági felügyeletet a Kormány által kijelölt szerv kormányrendeletben meghatározottak szerint látja el.

(4)

(5) A honvédelmi célú elektronikus információs rendszerek esetében, az e törvény szerinti hatósági feladatokat, a biztonsági felügyeletet a honvédelmi ágazaton belül működő, a Kormány által kijelölt szerv kormányrendeletben meghatározottak szerint látja el.

(6)

(7) E törvény rendelkezéseit

a) a minősített adatokat kezelő elektronikus információs rendszereket érintően a minősített adat védelméről szóló törvényben,

b) a médiaszolgáltatási és elektronikus hírközlési tevékenység esetén az elektronikus hírközlésről szóló törvényben, továbbá a médiaszolgáltatásokról és tömegkommunikációról szóló törvényben

meghatározott eltérésekkel kell alkalmazni.

3. § (1) A 2. § (1) bekezdés *a)-h)* és *j)-l)* pontjában megjelölt szervek, valamint - a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfoliókezelési tevékenység keretében kezelt adatok kivételével - a 2. § (1) bekezdés *i)* pontjában megjelölt szerv által kezelt adatok és a 2. § (2) bekezdés *b)* pontjában megjelölt szervezetek által kezelt, a nemzeti adatvagyon részét képező adatok Magyarország területén üzemeltetett és tárolt elektronikus információs rendszerekben, valamint honvédelmi, diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek.

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

(3) A 2. § (1) bekezdés *a)-h)* és *j)-k)* pontjában megjelölt szervek, valamint - a monetáris politika végrehajtásával és a devizatartalék kezelésével kapcsolatos kockázatértékelési és portfoliókezelési tevékenység keretében kezelt adatok kivételével - a 2. § (1) bekezdés *i)* pontjában megjelölt szerv által kezelt adatok az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság (a továbbiakban: hatóság) engedélyével vagy nemzetközi szerződés alapján az EGT-államok 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, illetve független, képesített ellenőr által készített ellenőri jelentéseket 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 a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

(6) Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt

rendszerelemek elektronikus információs rendszerei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztály is megállapítható.

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)

(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 által megállapított biztonsági osztályt - a 2. § (5) bekezdésében meghatározott elektronikus információs rendszerek kivételével - felülbírálhatja és magasabb, indokolt esetben alacsonyabb szintű osztályba sorolást is megállapíthat.

(7) Új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

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) Az elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

(3) A szervezet vagy szervezeti egységek biztonsági szintjét a szervezet védelemre való felkészültsége határozza meg.

(4) A szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

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

(6) Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek szervezetei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb, vagy indoklással ellátva alacsonyabb

szintű besorolás is megállapítható.

10. § (1) A szervezet vagy szervezeti egység 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 vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(3) A szervezet vagy a 9. § (2) bekezdése szerinti szervezeti egység biztonsági szintjét a cselekvési tervben szereplő ütemezés szerint kell elérni. Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket az (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő nyolc 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. § (1) 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 vagy szervezeti egység biztonsági szintbe sorolását soron kívül meg kell ismételni.

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

(8) A szervezet vagy felelős szervezeti egység 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 vagy szervezeti egységre irányadó szabályzatban 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 biztonságáért felelős személyt nevez ki vagy bíz meg,

d)-e)

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 meghatározott feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve a központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében. A két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba. Az (1) bekezdés *a)* és *b)* pontjában meghatározott feladatok keretében a szervezeti szintű informatikai biztonsági szabályok kidolgozása abban az esetben is a szervezet vezetőjének felelőssége, ha a jogszabály által kijelölt központosított elektronikus és hírközlési szolgáltatót vesz igénybe.

(4)

(5) A nemzetbiztonsági védelem alá eső állami szervek esetében az elektronikus információs rendszer biztonságáért felelős személy kinevezése tekintetében az eseménykezelő központ előzetes véleményezési jogot gyakorol.

(6) A biztonsági esemény kivizsgálásában részt vevő személy csak az lehet, aki rendelkezik a szervezet vezetője által - az eseménykezelő központ előzetes véleményezésével - kiadott megbízással. A megbízást írásba kell foglalni. A biztonsági esemény kivizsgálásában részt vevő személynek a megbízás előtt részt kell vennie a biztonságiesemény-kezelő eljárásról szóló, eseménykezelő központ által tartott tájékoztató előadáson.

(7) A honvédelmi célú elektronikus információs rendszerek esetében az (5) és (6) bekezdés rendelkezései nem alkalmazhatóak.

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 az 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 biztonsági felügyeletét - a honvédelmi célú elektronikus információs rendszerek, valamint a honvédelmi létfontosságú rendszerelemek és a honvédelmi ágazat hatáskörébe tartozó nemzetbiztonsági védelem alá eső szervek kivételével - a Kormány által kijelölt hatóság látja el.

(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 kivizsgálására irányuló hatósági eljárás megindítása,

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)

h) együttműködés az elektronikus ügyintézés és a bizalmi szolgáltatások 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 19. § (1)-(4) bekezdésében meghatározott eseménykezelő központokkal,

k)-n)

(2a) A hatóság a (2) bekezdés szerinti feladatait a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában - az azokon tárolt adatok megismerése nélkül - kormányrendeletben meghatározottak szerint látja el.

(3) A hatóság eljárásainak általános ügyintézési határideje - a (3a) bekezdésben meghatározott kivétellel - 30 nap.

(3a) A hatóság által lefolytatott hatósági eljárás ügyintézési határideje a logikai védelmi kötelezettség teljesítésére irányuló vizsgálat esetén százhúsz nap.

(3b) A hatóság eljárásaiban

a) az ügyfél értesítése az eljárás megindításáról mellőzhető,

b) a szervezet köteles a szakértői eljárásban közreműködni.

(4) A (2) bekezdés *a)* és *b)* pontjában foglalt feladatok ellátása körében a hatóság javaslatára az e-közigazgatásért felelős miniszter az informatikáért 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, az eseménykezelő központtól kapott értesítéseket.

(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, valamint az (1) bekezdés *d)* pontja szerinti szabályzatot megküldi a hatóságnak a nyilvántartásba vétel érdekében.

(4) Az (1) bekezdésben meghatározott nyilvántartásból - ha jogszabály eltérően nem rendelkezik - adattovábbítás kizárólag a 19. § (1)-(4) bekezdésében meghatározott eseménykezelő központok részére 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, kibervédelmi gyakorlatokat szervezni,

f) a nemzetközi információbiztonsági, kibervédelmi gyakorlatokon felkérésre képviselni Magyarországot,

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

h) eljárása során független, képesített ellenőrt igénybe venni, és az általa végzett ellenőrzés eredményét figyelembe venni,

i) a minimálisan elvárt biztonsági követelményeket meghatározni.

(1a) A 2. § (5) bekezdése szerinti szerv az általa felügyelt ágazat tekintetében ellátja az (1) bekezdés *a), b), c), d)* és *i)* pontja szerinti feladatokat.

(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,

d) jogosult bírságot kiszabni külön kormányrendeletben meghatározottak szerint.

(4) Ha az elektronikus információs rendszert olyan

a) súlyos biztonsági esemény éri vagy

b) súlyos biztonsági esemény közvetlen bekövetkezése fenyegeti,

amely a rendszert működtető szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, az eseménykezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a szervezetet, hogy a súlyos biztonsági esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg.

(5) Ha a szervezethez információbiztonsági felügyelő van kirendelve, a (4) bekezdés szerinti körülmények felmerüléséről az eseménykezelő központot haladéktalanul tájékoztatja. Azonnali beavatkozást igénylő esetben az eseménykezelő központ - az információbiztonsági felügyelő útján - az információk sérülésének elkerüléséhez szükséges mértékben ideiglenes intézkedést alkalmazhat.

(6) Ha a (2) bekezdés *a)* pontjában és a (3) bekezdés *a)* pontjában meghatározott felszólítást az érintett szervezet figyelmen kívül hagyja, vagy a hatóság által javasolt védelmi intézkedéseket önhibájából nem teljesíti és ezzel a (4) bekezdés *a)* vagy *b)* pontja szerinti biztonsági esemény áll vagy állhat elő, a hatóság a biztonsági esemény bekövetkezésének elhárítására fordított költségének megtérítésére kötelezi.

8. Információbiztonsági felügyelő

17. § (1) Az információbiztonsági felügyelőt a hatóság javaslatára az e-közigazgatásért 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 e-közigazgatásért felelős miniszter gondoskodik. Az információbiztonsági felügyelő tevékenységének szakmai irányítását az e-közigazgatásért felelős miniszter látja el.

(4) Az információbiztonsági felügyelő az e-közigazgatásért 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. Sérülékenységvizsgálat, biztonsági esemény vizsgálata

18. § (1) A hatóság az érintett szervezetet kötelezheti arra, hogy sérülékenységvizsgálatot végeztessen, valamint a biztonsági eseményt kivizsgáltassa. Ha a hatóság kötelezésének az érintett szervezet nem tesz eleget, a hatóság eljárási bírságot szab ki.

(2) A törvény hatálya alá tartozó szervezet sérülékenységvizsgálatot, biztonsági esemény vizsgálatát a hatóság felhívása nélkül is kezdeményezhet.

(2a) A kormányrendeletben meghatározott, sérülékenységvizsgálat lefolytatására jogosult szerv saját hatáskörben maga is indíthat és lefolytathat sérülékenységvizsgálatot regisztrált felhasználói jogosultság birtokában, illetve annak hiányában is, külön jogszabályban meghatározott feltételek szerint.

(3) A sérülékenységvizsgálatot, illetve a biztonsági esemény vizsgálatát - az (5) bekezdésben foglalt szervek és elektronikus információs rendszerek kivételével -

a) a Kormány rendeletében meghatározott állami szerv, vagy

b) telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges - jogszabályban meghatározott - szakértelemmel és infrastrukturális feltételekkel rendelkező gazdálkodó szervezet végezhet.

(4) A (3) bekezdés *b)* pontja szerinti gazdálkodó szervezet nevében és alkalmazásában kizárólag olyan személy végezheti a vizsgálatot, akinek a nemzetbiztonsági ellenőrzését elvégezték és a nemzetbiztonsági ellenőrzés során nemzetbiztonsági kockázatot nem állapítottak meg.

(5) A sérülékenységvizsgálatot, illetve a biztonsági esemény vizsgálatát

a) a zárt célú elektronikus információs rendszerek,

b) a 2. § (1) bekezdése szerinti állami és önkormányzati szervek európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemei elektronikus információs rendszerei, valamint

c) a 2. § (1) bekezdése szerinti, nemzetbiztonsági védelem alá eső állami és önkormányzati szervek

vonatkozásában - a (8) bekezdésben foglaltak kivételével - a Kormány rendeletében meghatározott állami szerv végzi el.

(6) Az (1) bekezdés szerinti vizsgálatok eredményét a vizsgálatot végző szerv vagy gazdálkodó szervezet a hatóság és az érintett szervezet részére a vizsgálatok befejezését követően haladéktalanul megküldi.

(7) Az érintett szervezet a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálatok lezárását követően tájékoztatja az érintett hatóságot.

(8) A 19. § (2) bekezdése szerinti eseménykezelő központ a honvédelmi célú elektronikus információs rendszerek vonatkozásában elvégzi a sérülékenységvizsgálatot, illetve a biztonsági esemény vizsgálatát.

(9) A sérülékenységvizsgálatot, illetve a biztonsági esemény vizsgálatát az (5) bekezdés szerinti állami szerv végzi el, ha az (5) bekezdés *b)* pontja szerinti elektronikus információs rendszereken kívüli, európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek elektronikus információs rendszerei tekintetében nincs a sérülékenységvizsgálat, illetve a biztonságiesemény-vizsgálat elvégzésére a jogszabályban meghatározott feltételeknek megfelelő gazdálkodó szervezet.

(10) Az (5) bekezdés szerinti állami szerv a sérülékenységvizsgálatot, illetve a biztonsági esemény vizsgálatát a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában - az azokon tárolt adatok megismerése nélkül - kormányrendeletben meghatározottak szerint látja el.

10. Eseménykezelő központok

19. § (1) A Kormány

a) az alapvető szolgáltatást nyújtó szolgáltatók, valamint a bejelentés-köteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereit - a (2) bekezdés szerinti elektronikus információs rendszerek kivételével - érintő,

b) az állami és önkormányzati elektronikus információs rendszerek működését biztosító infokommunikációs infrastruktúrát, illetve - a (2) bekezdés szerinti elektronikus információs rendszerek kivételével - a 2. §-ban meghatározott szervek nyílt elektronikus információs rendszereit érintő,

c) a 2. § (2) bekezdés *c)* pontjában meghatározott létfontosságú rendszerelemek elektronikus információs rendszereit érintő

biztonsági események és fenyegetések kezelése érdekében eseménykezelő központot működtet a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter irányítása alatt.

(2) A Kormány az (1) bekezdéstől eltérően, a honvédelmi célú elektronikus információs rendszereket érintő, e törvényben foglalt biztonsági események és fenyegetések kezelése érdekében eseménykezelő központot működtet a honvédelemért felelős miniszter irányítása alatt.

(3)

(4) A 2. §-ban meghatározott szervek a tudomásukra jutott biztonsági események adatait kötelesek haladéktalanul az (1) bekezdés szerinti eseménykezelő központ részére továbbítani.

(5) A (2) bekezdés szerinti eseménykezelő központ a biztonsági eseményekhez kapcsolódó és a (6) bekezdés szerinti együttműködés során tudomására jutott biztonsági események adatait köteles haladéktalanul az (1) bekezdés szerinti eseménykezelő központ részére továbbítani.

(6) A (2) bekezdés szerinti eseménykezelő központ részt vehet a szakterület szerinti nemzetközi együttműködésben és e célból akkreditálható.

20. § (1) A 19. § (1) bekezdés szerinti eseménykezelő központ ellátja a következő feladatokat:

a) a 19. § (6) bekezdése szerinti kivétellel nemzetközi eseménykezelési együttműködésben Magyarország képviselete, a magyar kiberteret érintő nemzetközi bejelentések fogadása és kezelése,

b) a szervezetekkel, szolgáltatókkal való kapcsolattartás a bejelentett biztonsági események fogadására, valamint azok kezeléséhez szükséges intézkedések megtétele és koordinációja,

c) a magyar kibertér rendszeres biztonsági helyzetértékelésének elvégzése,

d) folyamatosan elérhető 24 órás ügyelet működtetése,

e) a biztonsági események kivizsgálásának támogatása, amely során elvégezheti a biztonsági események adatainak műszaki vizsgálatát, amelyhez adatokat és az adatokhoz elektronikus hozzáférést kérhet,

f) azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági fenyegetettségekről, ezek magyar nyelvű megjelenítése,

g) a nemzetközileg publikált sérülékenységek hozzáférhetővé tétele a honlapján,

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

i) hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt,

j) együttműködik a hatósággal, továbbá szükség szerint a biztonsági esemény kezelése tekintetében érintett szervezetekkel,

k) a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgozhat ki és tréningeket tarthat, felvilágosító, szemléletformáló kampányokat szervezhet.

(2) A 19. § (2) bekezdése szerinti eseménykezelő központ az általa támogatott ágazatok tekintetében ellátja az (1) bekezdés *b), c), d), e), f), i), j)* és *k)* pontja szerinti feladatokat.

(3) A 19. § (1) bekezdése szerinti eseménykezelő központ az (1) bekezdés szerinti feladatait a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában - az azokon tárolt adatok megismerése nélkül - kormányrendeletben meghatározottak szerint látja el.

11. A kormányzati koordináció biztosítása

21. § (1) Az e-közigazgatásért felelős miniszter által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) a Kormány javaslattevő, véleményező szerveként gondoskodik a 2. § (1), (2) és (5) bekezdésében, valamint a 14. § (1) bekezdésében meghatározott szervezetek e törvényben és végrehajtási rendeleteiben meghatározott tevékenységeinek összehangolásáról.

(2) A Tanács tevékenységét az e-közigazgatásért felelős miniszter által delegált kiberkoordinátor, valamint a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító kiberbiztonsági munkacsoportok és a Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) támogatja.

(3)-(4)

12. Adatvédelmi rendelkezések

22. § (1) A 2. § (5) bekezdése, valamint a 18. § (3) bekezdése szerinti szerv vagy gazdálkodó szervezet, 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 - a (2) bekezdésben meghatározott kivétellel - kötelesek az elektronikus információs rendszereikből és adathordozóikról törölni.

(2) A hatóság, a 18. § (5) bekezdése szerinti szerv, valamint a 19. § (1) és (2) bekezdése szerinti eseménykezelő központ az (1) bekezdésben meghatározott adatokat a hatósági döntés véglegessé válását, a sérülékenységvizsgálat lezárását, valamint a biztonsági esemény vizsgálatának lefolytatását követő öt évig jogosultak kezelni, és az öt év elteltével kötelesek az elektronikus információs rendszereikből és adathordozóikról törölni.

(3) A hatóság, a 2. § (5) bekezdése szerinti szerv, a 18. § (3) bekezdése szerinti szerv vagy gazdálkodó szervezet, a 18. § (5) bekezdése szerinti szerv, valamint a 19. § (1) és (2) bekezdése szerinti eseménykezelő központ munkatársait az (1) bekezdés szerint megismert adatok tekintetében írásba foglalt titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követő 5 évig, minősített adatok tekintetében azok érvényességi idejének végéig, személyes adatok tekintetében pedig időkorlát nélkül fennmarad.

(4) A hatóság eljárása során keletkezett adatok nem nyilvánosak.

(5) A zárt célú és honvédelmi célú elektronikus információs rendszerek - e törvényben meghatározott - hatósági feladatainak ellátására Kormány által kijelölt szervnek a véglegessé vált határozata az ügyfélen és az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény 33. § (3) bekezdése alapján iratbetekintésre jogosult személyen kívül más által nem ismerhető meg.

12/A. Elektronikus kapcsolattartás

22/A. § (1) Az e törvény hatálya alá tartozó szervezetek és elektronikus információs rendszerek tekintetében

a) a 7. § szerinti biztonsági osztályba sorolás eredményének bejelentése, a 8. § (5) bekezdése szerinti cselekvési terv, a 15. § (1) bekezdés *a)-c)* pontja szerinti adatok és a 15. § (1) bekezdés *d)* pontja szerinti szabályzat megküldése a hatóság felé,

b) a 13. § (3) bekezdése szerinti biztonsági esemény bejelentése az eseménykezelő központ felé

a hatóság és az eseménykezelő központ által működtetett elektronikus rendszerben, elektronikus úton történik.

(2) Biztonsági esemény bejelentése bármely csatornán megvalósítható, ha a szervezet

elektronikus információs rendszere oly mértékben sérül, hogy az elektronikus kapcsolattartás lehetetlenné válik.

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, együttműködik az eseménykezelő központ szakembereivel,

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

V. FEJEZET

ZÁRÓ RENDELKEZÉSEK

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,

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

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

d) a korai figyelmeztetés részletes szabályait, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét,

e) az eseménykezelő központot, feladat- és hatáskörét, a biztonságiesemény-kezelési eljárás részletes szabályait,

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

g) a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató e törvény alapján ellátandó feladataira vonatkozó részletes szabályokat,

h) a 2. § (3) bekezdése szerinti elektronikus információs rendszereket, valamint e rendszerek tekintetében a hatósági feladatokat ellátó szerveket és a feladatellátás részletes szabályait,

i) a 2. § (5) bekezdése szerinti hatóságot és a feladatellátás részletes szabályait,

j) a sérülékenységvizsgálatra, biztonsági esemény kivizsgálására feljogosított állami szerveket, a 18. § (3) bekezdés *b)* pontja szerinti gazdálkodó szervezettel szemben támasztott szakmai követelményeket, a sérülékenységvizsgálatra, biztonsági esemény kivizsgálására vonatkozó eljárási szabályokat, és

k) a 19. § (2)-(4) bekezdése szerinti eseménykezelő központot, feladat- és hatáskörét,

l) a 16. § (1) bekezdése szerinti független, képesített ellenőr igénybevételével kapcsolatos eljárásrendet,

m) a honvédelmi célú elektronikus információs rendszerre vonatkozóan a korai figyelmeztetés részletes szabályait, így különösen annak rendszerét, a rendszer üzemeltetőjének kijelölését, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét,

n) a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában a hatóság 14. § (2) bekezdése, valamint a 20. § (1) bekezdése szerinti feladatait, továbbá a sérülékenység vizsgálat, illetve a biztonsági esemény vizsgálat részletes szabályait.

(1a) Felhatalmazást kap a Kormány, hogy rendeletben kijelölje a hatóságot.

(2) Felhatalmazást kap

a) az e-közigazgatásért felelős miniszter, hogy az informatikáért 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,

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

c) az e-közigazgatásért felelős miniszter, hogy a szervezetek hatósági nyilvántartásba vételének rendjét

rendeletben határozza meg.

(3)

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.

(5) A 2. § (1) bekezdése alá tartozó, 2014. július 1-jét követően jogelőd nélkül létrejött szervezet esetében

a) a 9. § szerinti biztonsági szintbe sorolást a létesítést megalapozó döntés hatálybalépésétől számított egy éven belül kell elvégezni;

b) a (3) bekezdés szerinti adatközlésre megállapított határidőket a létesítést megalapozó döntés hatálybalépésétől kell alkalmazni.

(6) A 2. § (2) bekezdése alapján a törvény hatálya alá 2014. július 1-jét követően kerülő szervezetek tekintetében

a) a 2. § (2) bekezdés *a)* pontja szerinti adatkezelési tevékenység feltétele, hogy az adatkezelést végző az adatkezelési tevékenység megkezdése előtt a törvény 7. § szerinti biztonsági osztályba sorolási, továbbá a (3) bekezdés szerinti bejelentési kötelezettségének eleget tegyen;

b) a 2. § (2) bekezdés *b)* pontja esetében a (3) bekezdés szerinti határidőket az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől kell számítani, a 7. § szerinti biztonsági osztályba sorolást az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépését követő három hónapon belül kell elvégezni;

c) a 2. § (2) bekezdés *c)* pontja esetében a (3) bekezdés szerinti határidőket a létfontosságú információs rendszerelemmé kijelölő határozat véglegessé válásától kell számítani, a 7. § szerinti biztonsági osztályba sorolást a kijelölő határozat véglegessé válásától számított egy éven belül kell elvégezni.

(7) A (4) bekezdés szerinti kötelezettség teljesítésére megállapított határidőt a 2014. július 1-jét követően a törvény hatálya alá kerülő szervezetek esetében

a) a 2. § (1) bekezdés tekintetében a szervezet létesítését megalapozó döntés hatálybalépésétől;

b) a 2. § (2) bekezdés *a)* pont tekintetében az adatkezelés megkezdésétől;

c) a 2. § (2) bekezdés *b)* pont tekintetében az adatfeldolgozói tevékenységet megalapozó jogszabály hatálybalépésétől;

d) a 2. § (2) bekezdés *c)* pont tekintetében a létfontosságú információs rendszerelemmé kijelölő határozat véglegessé válásától

kell számítani.

16. Az Európai Unió jogának való megfelelés

27. § Ez a törvény a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

28. § E törvény tervezetének a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelv 15. cikk (7) bekezdése szerinti előzetes bejelentése megtörtént.

29. § Ez a törvény a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i, (EU) 2016/1148 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.