# 2024. évi LXIX. törvény

# Magyarország kiberbiztonságáról[1]

[1] A nemzet érdekében kiemelten fontos napjaink információs társadalmát érő fenyegetések miatt az elektronikus információs rendszerek fenyegetéseinek mérséklése és a kulcsfontosságú ágazatokban a szolgáltatások folyamatosságának biztosítása.

[2] Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme, amely hozzájárul Magyarország és az Európai Unió biztonságához, ellenálló képességének és versenyképességének növeléséhez.

[3] A társadalom gyors digitális átalakulásával és összekapcsolódásával az elektronikus információs rendszerek, valamint a digitális eszközök a mindennapi élet központi elemévé váltak. A fejlődés a digitális fenyegetettségek körének bővüléséhez is vezetett, ami akadályozhatja a gazdasági tevékenységek folytatását, pénzügyi veszteséget okozhat és alááshatja a felhasználók bizalmát, ezzel jelentős károkat okozva a gazdasági és társadalmi életben. Ezen túlmenően a kiberbiztonság kulcsfontosságú tényező számos kritikus ágazat számára a digitális átalakulás sikeres felkarolásához és a digitalizáció gazdasági, társadalmi és fenntartható előnyeinek teljes körű kiaknázásához.

[4] Mindezekre, valamint az Európai Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvére figyelemmel az Országgyűlés a következő törvényt alkotja:

## *I. FEJEZET*

## *ÁLTALÁNOS RENDELKEZÉSEK*

### 1. A törvény hatálya

**1. §** (1) E törvénynek a szervezetek kötelezettségeire és a kiberbiztonsági hatósági felügyeletre vonatkozó rendelkezéseit kell alkalmazni

*a)* az 1. mellékletben felsorolt, a közigazgatási ágazathoz tartozó szervezetekre,

*b)* a többségi állami befolyás alatt álló azon gazdálkodó szervezetekre, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint meghaladják a középvállalkozásokra vonatkozó küszöbértékeket,

*c)* a 23. § (1) bekezdés *a)* pontja szerinti nemzeti kiberbiztonsági hatóság (a továbbiakban: nemzeti kiberbiztonsági hatóság), vagy a 23. § (2) bekezdése szerinti honvédelmi kiberbiztonsági hatóság (a továbbiakban: honvédelmi kiberbiztonsági hatóság) által a (6) bekezdés szerint alapvető vagy fontos szervezetként azonosított, az *a), b)* és *d)–f)* pont, valamint az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá nem tartozó szervezetekre,

*d)* a 2. és 3. melléklet szerinti szervezetekre, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint középvállalkozásoknak minősülnek vagy meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket,

*e)* méretüktől függetlenül a 2. és 3. melléklet szerinti szervezetekre, ha a szervezet

[1] Kihirdetve: 2024. XII. 20.

*ea)* elektronikus hírközlési szolgáltató,

*eb)* bizalmi szolgáltató,

*ec)* DNS-szolgáltató,

*ed)* legfelső szintű doménnév-nyilvántartó vagy

*ee)* doménnév-regisztrációt végző szolgáltató, valamint

*f)* a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságokra.

(2) A kritikus szervezetek ellenálló képességéről szóló törvény (a továbbiakban: Kszetv.) alapján kijelölt kritikus szervezetek és kritikus infrastruktúrák (a továbbiakban együtt: kritikus szervezet), valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény (a továbbiakban: Vbö.) alapján kijelölt, az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák (a továbbiakban együtt: az ország védelme és biztonsága szempontjából jelentős szervezet) vonatkozásában a szervezetnek az (1) bekezdés szerinti minősülése az irányadó e törvény rendelkezéseinek az alkalmazása során, kivéve, ha a kritikus szervezet vagy az ország védelme és biztonsága szempontjából jelentős szervezet az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozik.

(3) A szervezetek – az általuk nyújtott szolgáltatásnak az állam, a társadalom, a gazdaság működése szempontjából való kritikussága, valamint bizonyos esetekben a szervezet mérete alapján – alapvető vagy fontos szervezeteknek minősülnek.

(4) Az (1) bekezdés szerinti szervezetek közül alapvető szervezetnek minősülnek az alábbi szervezetek:

*a)* az 1. melléklet szerinti szervezetek, kivéve a 20 000 főt meg nem haladó lakosságszámú települések képviselő-testületének hivatalai,

*b)* a többségi állami befolyás alatt álló gazdálkodó szervezetek, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket,

*c)* azon szervezetek, amelyeket a nemzeti kiberbiztonsági hatóság vagy a honvédelmi kiberbiztonsági hatóság alapvető szervezetként azonosított,

*d)* a Kszetv. alapján kijelölt kritikus szervezetek,

*e)* a Vbö. alapján kijelölt, az ország védelme és biztonsága szempontjából jelentős szervezetek,

*f)* a 2. melléklet szerinti azon szervezetek, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint középvállalkozásnak minősülnek vagy meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket, valamint

*g)* a minősített bizalmi szolgáltatók és a legfelső szintű doménnév-nyilvántartók, valamint a DNS-szolgáltatók, méretüktől függetlenül.

(5) Az (1) bekezdés szerinti szervezetek közül fontos szervezetnek minősülnek és a szervezetekre vonatkozó rendelkezéseket az e törvényben foglalt eltérésekkel kell alkalmazni az alábbi szervezetekre:

*a)* a 20 000 főt meg nem haladó lakosságszámú települések képviselő-testületének hivatalai,

*b)* azon szervezetek, amelyeket a nemzeti kiberbiztonsági hatóság vagy a honvédelmi kiberbiztonsági hatóság fontos szervezetként azonosított,

*c)* a 2. melléklet szerinti szervezet, amely nem minősül alapvető szervezetnek, valamint

*d)* a 3. melléklet szerinti szervezet, amely a (4) bekezdés *b)–e)* pontja alapján nem minősül alapvető szervezetnek.

(6) Az (1) bekezdés *c)* pontja szerinti azonosítási eljárás feltétele, hogy a szervezet

1. Magyarországon egyedüli szolgáltatója egy olyan szolgáltatásnak, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához;

2. által nyújtott szolgáltatás zavara jelentős hatással lehet a közrendre, a közbiztonságra vagy a közegészségre;

3. által nyújtott szolgáltatás zavara jelentős hatást gyakorolhat kritikus fontosságú társadalmi vagy gazdasági tevékenységekre;

4. által nyújtott szolgáltatás zavara jelentős rendszerszintű kockázatot idézhet elő, különösen

azokban az ágazatokban, ahol az említett zavarnak határokon átnyúló hatása lehet;

5. nemzeti vagy regionális szinten különös fontossággal bír az adott ágazat vagy szolgáltatás típusa, vagy más, hazai kölcsönösen függő ágazatok szempontjából;

6. a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről szóló kormányhatározat alapján nemzetbiztonsági védelem alatt áll; vagy nemzetbiztonsági okból a nemzeti kiberbiztonsági hatóság, honvédelmi vagy katonai nemzetbiztonsági okból a honvédelmi kiberbiztonsági hatóság indokoltnak tartja az azonosítását;

7. legalább 20000 személynek nyújt a 2. és 3. mellékletben foglalt ágazatok szerinti, vagy az állam működéséhez szükséges szolgáltatásokat;

8. legalább öt, e törvény hatálya alá tartozó szervezetnek nyújt szolgáltatásokat;

9. többségi állami befolyás alatt áll;

10. jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozója;

11. az alapvető vagy fontos szervezet számára adatkezelést végez;

12. olyan köztulajdonban álló gazdasági társaságnak minősül, amely nem tartozik az (1) bekezdés *b)* pontjának hatálya alá vagy

13. költségvetési és európai uniós forrásból támogatott projektek keretében fejleszt elektronikus információs rendszert.

(7) E törvény kiberbiztonsági tanúsításra vonatkozó rendelkezéseit az információs és kommunikációs technológiai (a továbbiakban: IKT) termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsításával kapcsolatos tevékenységre kell alkalmazni.

(8) E törvény poszt-kvantumtitkosításra vonatkozó rendelkezéseit a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) elnökének rendeletében meghatározott, a következő szervezetekre (a továbbiakban: poszt-kvantumtitkosítás alkalmazására kötelezett szervezet) és hatósági felügyeletükre irányuló tevékenységre kell alkalmazni:

*a)* a kormányzati célú hálózatokról szóló kormányrendelet szerinti igénybevételre kötelezett szervezet, valamint

*b)* a következő törvények hatálya alá tartozó közműszolgáltató és a következő törvények felhatalmazása alapján kiadott jogszabályok hatálya alá tartozó, közszolgáltatást nyújtó szervezet:

*ba)* a földgázellátásról szóló törvény,

*bb)* a földgáz biztonsági készletezéséről szóló törvény,

*bc)* a villamos energiáról szóló törvény,

*bd)* a távhőszolgáltatásról szóló törvény,

*be)* a víziközmű-szolgáltatásról szóló törvény, valamint

*bf)* a hulladékról szóló törvény.

(9) E törvény sérülékenységvizsgálatra vonatkozó rendelkezéseit kell alkalmazni:

*a)* az (1) bekezdés *a)–c)* pontja szerinti szervezetek elektronikus információs rendszereit, valamint

*b)* a megállapodásban foglalt eltérésekkel a 61. § szerinti megállapodásban meghatározott elektronikus információs rendszereket
érintő sérülékenységvizsgálatokra.

(10) E törvény kiberbiztonsági incidenskezelésre vonatkozó rendelkezéseit kell alkalmazni:

*a)* az (1) bekezdés szerinti szervezetek, valamint

*b)* az e törvényben meghatározott eltérésekkel az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek
elektronikus információs rendszereit érintő kiberbiztonsági incidensek kezelésére.

(11) A (10) bekezdésben meghatározott szervezeteken kívüli szervezetek, illetve személyek által önkéntesen bejelentett kiberbiztonsági incidensek esetén a nemzeti kiberbiztonsági incidenskezelő központ az e törvényben meghatározottak szerint jár el.

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

*a)* a Magyarország területén letelepedett vagy letelepedett képviselővel rendelkező 1. § szerinti

szervezetekre,

*b)* a Magyarország területén szolgáltatást nyújtó elektronikus hírközlési szolgáltatókra,

*c)* azokra a DNS-szolgáltatókra, legfelső szintű doménnév-nyilvántartókra, doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetekre, felhőszolgáltatókra, adatközpont-szolgáltatókra, tartalomszolgáltató hálózati szolgáltatókra, irányított szolgáltatókra, irányított biztonsági szolgáltatókra, az online piacterek, online keresőprogramok és közösségimédia-szolgáltatási platformok szolgáltatóira, amelyek üzleti tevékenységének fő helye Magyarország területén található.

(2) Az (1) bekezdés *c)* pontja szerinti szervezet üzleti tevékenységének fő helye abban az esetben van Magyarországon, ha

*a)* a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket túlnyomórészt Magyarországon hozzák meg,

*b)* a szervezet elektronikus információs rendszereivel kapcsolatos kiberbiztonsági műveleteket Magyarországon végzik, vagy

*c)* a szervezetnek a legmagasabb munkavállalói létszámmal rendelkező telephelye Magyarországon van.

**3. §** (1) E törvény hatálya nem terjed ki

*a)* a minősített adatot kezelő elektronikus információs rendszerekre,

*b)* a műveleti célú elektronikus információs rendszerekre,

*c)* az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló kormányrendelet hatálya alá tartozó programozható rendszerekre, valamint

*d)* a Kormány rendeletében kijelölt szerv által nyújtott kiberbiztonsági szolgáltatásokra.

(2) A Kormány rendeletében határozza meg az (1) bekezdés *d)* pontja szerinti kiberbiztonsági szolgáltatások körét és az igénybevételére kötelezett, illetve jogosult szervezetek körét.

(3) E törvény rendelkezéseit a honvédelmi célú elektronikus információs rendszerek vonatkozásában az e törvényben meghatározott eltérésekkel kell alkalmazni.

## 2. Értelmező rendelkezések

**4. §** 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 információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

3. *adatfeldolgozó:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

4. *adatkezelés:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

5. *adatkezelő:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

6. *adatkicserélő szolgáltatás:* az elektronikus hírközlésről szóló törvény szerinti fogalom;

7. *adatközponti szolgáltatás:* olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is;

8. *adatosztályozás:* a szervezet által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából;

9. *ágazaton belüli kiberbiztonsági incidenskezelő központ:* olyan kiberbiztonsági incidenskezelő

központ, amelyet az e törvény hatálya alá tartozó egy vagy több, egy ágazathoz tartozó szervezet az ágazaton belül meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a központosított és egységes kezelése érdekében üzemeltet;

10. *auditor:* az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet;

11. *behatolásvizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az IKT-rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárására és kihasználhatóságának ellenőrzésére kerül sor a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával;

12. *belső informatikai biztonsági vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik, vagy a belső hálózatban használt eszköz, vagy rendszerelem vizsgálata kerül végrehajtásra;

13. *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;

14. *bizalmi szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

15. *bizalmi szolgáltató:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

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

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

18. *digitális szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

19. *DNS:* hierarchikusan felépülő elnevezési rendszer, más néven doménnévrendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

20. *DNS-szolgáltató:* olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja a szervezeten kívüli más szervezet vagy személy részére:

*a) autoritatív DNS-szolgáltatás:* a doménnév – doménnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű doménnév- nyilvántartó szolgáltatás része,

*b) rekurzív DNS-szolgáltatás:* olyan DNS-szolgáltatás, amely a felhasználók doménnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő doménnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,

*c) DNS-gyorsítótárazás:* a doménnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt doménnévadatok alapján történő kiszolgálása,

21. *doménnév:* az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

22. *doménnév-regisztrációt végző szolgáltató:* a legfelső szintű doménnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domén regisztrálására;

23. *elektronikus hírközlési szolgáltató:* az elektronikus hírközlésről szóló törvény szerinti fogalom;

24. *elektronikus információs rendszer:*

*a)* az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési 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, ideértve a kiber-fizikai rendszereket, vagy

*c)* az *a)* és *b)* alpontban szereplő elemek által működésük, használatuk, védelmük és

karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

25. *elektronikus információs rendszer biztonsága:* az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

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

27. *esemény:* az elektronikus információs rendszerben bekövetkezett állapotváltozás;

28. *európai kiberbiztonsági tanúsítási rendszer:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti fogalom;

29. *felhasználó szervezet:* központi rendszert vagy központi szolgáltatást igénybe vevő szervezet;

30. *felhőszolgáltatás:* olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez;

31. *felhőszolgáltató:* felhőalapú számítástechnikai szolgáltatást nyújtó szervezet;

32. *gyártó:* az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója;

33. *használatbavétel:* az elektronikus információs rendszer adatokkal való feltöltése és rendeltetésszerű használatának megkezdése;

34. *honvédelmi célú elektronikus információs rendszer:*

*a)* 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, valamint jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést,

*b)* az ország védelme és biztonsága szempontjából jelentős honvédelmi ágazaton belüli szervezet és infrastruktúra elektronikus információs rendszerei,

*c)* az ország védelme és biztonsága szempontjából jelentős kettős kijelöléssel nem érintett honvédelmi szervezet és honvédelmi infrastruktúra elektronikus információs rendszerei, valamint

*d)* a honvédelmi kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezet elektronikus információs rendszere;

35. *honvédelmi kiberbiztonsági incidenskezelő központ:* a 63. § (2) bekezdése szerint kijelölt szerv;

36. *ideiglenes hozzáférhetetlenné tétel:* az elektronikus adathoz való hozzáférés ideiglenes megakadályozása;

37. *IKT-folyamat:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 14. pontjában meghatározott fogalom;

38. *IKT-szolgáltatás:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 13. pontjában meghatározott fogalom;

39. *IKT-termék:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 12. pontjában meghatározott fogalom;

40. *jelentős kiberbiztonsági incidens:*

*a)* a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,

*b)* közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely

*ba)* a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;

*bb)* súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy

*bc)* jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;

41. *jelentős kiberfenyegetés:* olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

42. *képviselő:* Magyarországon letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, Magyarországon nem letelepedett szervezet nevében eljárjon, és akihez vagy amelyhez a kiberbiztonsági hatóság, vagy a kiberbiztonsági incidenskezelő központ az adott szervezet helyett fordulhat;

43. *kiberbiztonság:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott fogalom;

44. *kiberbiztonsági audit:* az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségének ellenőrzése;

45. *kiberbiztonsági hatóság:* a 23. § (1) bekezdés *a)* és *b)* pontja, valamint (2) bekezdése szerinti hatóság;

46. *kiberbiztonsági incidens:* olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

47. *kiberbiztonsági incidenskezelés:* minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;

48. *kiberbiztonsági incidenskezelő központ:* a 63. § (1) és (2) bekezdése szerinti szerv;

49. *kiberbiztonsági incidensközeli helyzet:* olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

50. *kiberfenyegetés:* az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalom;

51. *kiber-fizikai rendszer:* olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;

52. *kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató:* olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt;

53. *kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató:* olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról;

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

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

56. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére

irányuló intézkedésrendszer kidolgozása és az intézkedések végrehajtása;

57. *kockázatmenedzsment keretrendszer:* olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;

58. *közigazgatási szerv:* az 1. melléklet 1–13. pontja szerinti szervezet;

59. *közösségimédia-szolgáltatási platform:* olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással;

60. *központi rendszer:* egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek;

61. *központi szolgáltatás:* a központi szolgáltató által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;

62. *központi szolgáltató:* olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást;

63. *kutatóhely:* a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából;

64. *legfelső szintű doménnév-nyilvántartó:* olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű doménzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

65. *megfelelőségértékelés:* az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek;

66. *megfelelőségértékelő szervezet:* a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

67. *megfelelőségi nyilatkozat:* a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

68. *megfelelőségi önértékelés:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

69. *mérföldkő:* az európai uniós forrásból finanszírozott központi rendszer fejlesztése esetén a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról szóló, 2021. február 12-i (EU) 2021/241 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja és az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alap Pluszra, a Kohéziós Alapra, az Igazságos Átmenet Alapra és az Európai Tengerügyi, Halászati és Akvakultúra-alapra vonatkozó közös rendelkezések, valamint az előbbiekre és a Menekültügyi, Migrációs és Integrációs Alapra, a Belső Biztonsági Alapra és a határigazgatás és a vízumpolitika pénzügyi támogatására szolgáló eszközre vonatkozó pénzügyi

szabályok megállapításáról szóló, 2021. június 24-i (EU) 2021/1060 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja szerinti, valamint a fejlesztésekre irányuló egyéb projektek esetén a projektben meghatározott fogalom;

70. *minősített bizalmi szolgáltatás:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

71. *minősített bizalmi szolgáltató:* a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

72. *műszaki előírás:* az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/ EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 1025/2012/EU rendelet) 2. cikk 4. pontjában meghatározott fogalom;

73. *műveleti célú elektronikus információs rendszer:*

*a)* a rendvédelmi szervek és a nemzetbiztonsági szolgálatok számára törvényben meghatározott közbiztonsági, nemzetbiztonsági feladatok ellátása érdekében használt elektronikus információs rendszer és

*b)* a honvédségi szervezetek által, a törvényben meghatározott katonai műveleti feladatok – így különösen közvetlen művelettámogatás, -tervezés, -vezetés, helyzetkövetés – ellátása érdekében használt elektronikus információs rendszer;

74. *nagyszabású kiberbiztonsági incidens:* olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

75. *nem privát felhőszolgáltatás:* olyan szolgáltató által nyújtott felhőszolgáltatás, amelyet a szolgáltató bárki számára elérhető módon vagy kizárólag a szervezetek egy meghatározott köre számára nyújt;

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

77. *nemzeti kiberbiztonsági tanúsítási rendszer:* IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására, megfelelőségértékelésére Magyarországon alkalmazandó, az európai kiberbiztonsági rendszerek elvei alapján kidolgozott és a tanúsító hatóság által meghatározott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere;

78. *nemzeti kiberbiztonsági stratégia:* a kiberbiztonság területén követendő stratégiai célokat és prioritásokat, valamint a megvalósításukhoz szükséges irányítási intézkedéseket meghatározó dokumentum;

79. *nemzeti kiberbiztonsági tanúsítvány:* olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

80. *nemzeti válságkezelési terv:* az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv, amely meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait;

81. *online keresőprogram:* az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló, 2019. június 20-i (EU) 2019/1150 európai parlamenti és tanácsi rendelet 2. cikk 5. pontjában meghatározott fogalom;

82. *online piactér:* olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely

alkalmazást használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;

83. *regisztrált felhasználói jogosultság:* a biztonsági vizsgálatot végző személy számára a sérülékenységvizsgálat elvégzése érdekében célzottan létrehozott felhasználói jogosultság;

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

85. *sebezhetőség:* IKT-termék, -szolgáltatás, -folyamat gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti az IKT-termék, -szolgáltatás, -folyamat bizalmasságát, sértetlenségét vagy rendelkezésre állását;

86. *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, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

87. *sérülékenység:* az elektronikus információs rendszer gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti egy elektronikus információs rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását;

88. *sérülékenységkezelési terv:* a sérülékenységek megszüntetésére irányuló tervdokumentum;

89. *sérülékenységvizsgálat:* sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre;

90. *szabvány*: az 1025/2012/EU rendelet 2. cikk 1. pontjában meghatározott fogalom;

91. *szervezet:* állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet;

92. *támogató rendszer:* az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el;

93. *tanúsítás:* független harmadik fél által végzett megfelelőségértékelési tevékenység;

94. *tartalomszolgáltató hálózat szolgáltatója:* a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója;

95. *távoli sérülékenységvizsgálat:* olyan sérülékenységvizsgálat, amelynek során

*a)* az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

*b)* automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy

*c)* a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

96. *továbbfejlesztés:* az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van;

97. *üzemeltetési kiberbiztonsági incidens:* olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;

98. *üzemeltető:* az a természetes személy, jogi személy, jogi személyiség nélküli szervezet vagy

egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

99. *zárt, teljes körű, folytonos és a kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme,

*a)* amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul,

*b)* amely az elektronikus információs rendszer valamennyi elemére kiterjed,

*c)* amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi, valamint

*d)* amelynek költségei arányosak a fenyegetések által okozható károk értékével.

### 3. Általános alapelvek

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

*a)* az elektronikus információs rendszerben kezelt adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint

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

vonatkozásában a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet.

(2) Az elektronikus információs rendszer védelme keretében az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezet, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében

*a)* az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat

*b)* az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint

*c)* az *a)* és *b)* pontban foglaltakat kezelő személyek

együttesének védelmét is biztosítani szükséges.

(3) Megfelelő költségvetési forrást kell biztosítani

*a)* a nemzeti kiberbiztonsági hatóság és a honvédelmi kiberbiztonsági hatóság,

*b)* az 57. § (1) bekezdése szerinti sérülékenységvizsgálat végzésére jogosult állami szerv (a továbbiakban: sérülékenységvizsgálat végzésére jogosult állami szerv), valamint

*c)* a 63. § szerinti nemzeti kiberbiztonsági incidenskezelő központ és a honvédelmi kiberbiztonsági incidenskezelő központ

működésére.

## *II. FEJEZET*

## *ALAPVETŐ ÉS FONTOS SZERVEZETEK KÖTELEZETTSÉGEI*

### 4. Az alapvető és fontos szervezetek általános kötelezettségei

**6. §** (1) A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert.

(2) A szervezet vezetője az elektronikus információs rendszerek védelme érdekében kockázatmenedzsment keretrendszert hoz létre és működtet a közvetlenül alkalmazandó európai uniós jogi aktusban, ennek hiányában és a közvetlenül alkalmazandó európai uniós jogi aktus által nem szabályozott kérdésekben az informatikáért felelős miniszter rendeletében foglaltak szerint.

(3) A (2) bekezdésben meghatározott tevékenység keretében a szervezet vezetője

1. gondoskodik a szervezet által használt elektronikus információs rendszerek, központi szolgáltatások felméréséről és nyilvántartásba vételéről a következők szerinti bontásban:

*a)* a szervezet rendelkezésében lévő elektronikus információs rendszerek,

*b)* a szervezet által használt központi rendszerek,

*c)* a szervezet által igénybe vett, központi szolgáltató által biztosított szolgáltatások és támogató rendszerek,

*d)* a szervezet rendelkezésében lévő vagy a szervezet által használt egyéb támogató rendszerek;

2. meghatározza a szervezet rendelkezésében lévő, továbbá a szervezet használatában lévő elektronikus információs rendszerek védelmével kapcsolatos szerepköröket, felelősöket, feladatokat és az ehhez szükséges hatásköröket, kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt;

3. az 1. melléklet szerinti szervezet esetében gondoskodik az 1. pont *a)* alpontja szerinti elektronikus információs rendszerben kezelt adatok felméréséről és osztályozásáról;

4. az informatikáért felelős miniszter rendelete szerinti hatáselemzést és kockázatmenedzsment tevékenységet végez az 1. pont *a)* alpontja szerinti elektronikus információs rendszerekre és azok környezetére vonatkozóan;

5. a jogszabályban meghatározottak szerint biztonsági osztályba sorolja az 1. pont *a)* alpontja szerinti elektronikus információs rendszereket;

6. meghatározza az 1. pont *a)* alpontja szerinti elektronikus információs rendszerek vonatkozásában a kockázatokkal arányos védelmi intézkedéseket;

7. kiadja a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó információbiztonsági szabályzatot, valamint gondoskodik annak legalább kétévente vagy a jogszabályban meghatározott esetekben történő felülvizsgálatáról;

8. biztosítja az elektronikus információs rendszerek védelme vonatkozásában meghatározott védelmi intézkedések teljesülését;

9. gondoskodik – ha releváns – az európai uniós jogi aktusban foglaltak, valamint az informatikáért felelős miniszter rendelete szerint kiválasztott védelmi intézkedések megfelelőségének első biztonsági osztályba sorolás alkalmával történő értékeléséről,

10. rendszeresen gondoskodik a védelmi intézkedések időszakos értékeléséről, ennek keretében legalább kockázatelemzések, ellenőrzések, független és a kiberbiztonsági hatóság által kiadott ajánlás szerinti belső kiberbiztonsági értékelés lefolytatása révén meggyőződik arról, hogy a jogszabályoknak és a kockázatoknak megfelelően meghatározott védelmi intézkedések megfelelően biztosítják-e a szervezet és elektronikus információs rendszerei biztonságát;

11. gondoskodik a biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során feltárt hiányosságok orvoslásáról;

12. a szervezeten belül dönt az elektronikus információs rendszerek használatbavételéről vagy használatának folytatásáról és

13. gondoskodik a kiberbiztonsági hatósági kötelezések teljesítéséről.

(4) A (3) bekezdés 10. pontjában meghatározott feladatokat a szervezet vezetője legalább kétévente, a biztonsági osztályba sorolás felülvizsgálatával egyidejűleg hajtja végre.

(5) A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében

*a)* gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak – az informatikáért felelős miniszter rendeletében meghatározott – kiberbiztonsági képzéséről, továbbképzéséről;

*b)* biztosítja a kötelezően előírt hazai kiberbiztonsági gyakorlatokon történő részvételt, illetve kiberbiztonsági gyakorlat önálló megtartását;

*c)* gondoskodik az elektronikus információs rendszer eseményeinek nyomonkövethetőségéről;

*d)* ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági

követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek;

*e)* az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról, az illetékes kiberbiztonsági incidenskezelő központnak való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról;

*f)* gondoskodik az érintetteknek a kiberbiztonsági incidensekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáról;

*g)* gondoskodik a kiberbiztonsági hatóság és az illetékes kiberbiztonsági incidenskezelő központ ajánlásainak, iránymutatásainak az elektronikus információs rendszer védelmének biztosítása érdekében történő figyelembevételéről;

*h)* köteles törekedni arra, hogy a jelen jogszabályban meghatározott feladatokat a lehető legrövidebb időn belül hajtsa végre;

*i)* az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek esetében gondoskodik arról, hogy a szervezet által az adott évben informatikai fejlesztésre fordított költségek legalább 5%-ának megfelelő összeget a szervezet a tárgyév során kiberbiztonsági fejlesztésekre fordítson és

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

(6) A (3)–(5) bekezdésben meghatározott feladatokért a szervezet vezetője az (5) bekezdés *d)* pontjában meghatározott esetben is felelős, kivéve – az igénybe vett szolgáltatások mértékéig – azokat az esetköröket, amikor központi szolgáltatót vagy központi rendszert kell a szervezetnek igénybe vennie.

(7) Az (5) bekezdés *e)* pontja szerinti jelentési kötelezettség teljesítése nem érinti a más törvény alapján fennálló jelentési kötelezettségeket.

(8) Az (1)–(5) bekezdés szerinti egyes követelményeknek való megfelelés igazolására – ha rendelkezésre áll – európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat alkalmazható.

(9) Az informatikáért felelős miniszter rendeletében – a honvédelmi célú elektronikus információs rendszerek tekintetében a honvédelmi miniszter rendeletében – meghatározott, 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek, valamint az SZTFH elnökének rendeletében meghatározott, 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek kötelesek az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított – az informatikáért felelős miniszter, a honvédelmi miniszter vagy az SZTFH elnöke rendeletében meghatározott – IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot használni.

(10) Az 1. § (1) bekezdés *a)* és *c)* pontja hatálya alá tartozó fontos szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet rendelkezésében lévő elektronikus információs rendszerek vonatkozásában

*a)* nem szükséges a (2) bekezdésben foglalt teljes körű kockázatmenedzsment keretrendszert működtetni,

*b)* nem kell teljesíteni a (3) bekezdés 4–5., 9. pontjában és a (4) bekezdésben foglaltakat, valamint

*c)* legalább az „alap” biztonsági osztályra irányadó követelményeket kell teljesíteni.

(11) A honvédelmi célú elektronikus információs rendszer felett rendelkezési jogosultsággal bíró szervezet a honvédelmi célú elektronikus információs rendszer vonatkozásában a hatósági eljárásban a honvédelmi kiberbiztonsági hatóságot keresi meg, az e törvény által előírt bejelentési és egyéb kötelezettségeket a honvédelmi kiberbiztonsági hatóság felé teljesíti.

(12) A hazai kiberbiztonsági gyakorlatok megtartásának részletszabályait, valamint az 1. § (1) bekezdés *a)–c)* pontja hatálya alá tartozó szervezetek kötelezettségeire vonatkozó részletes rendelkezéseket kormányrendelet határozza meg.

**7. §** (1) Az SZTFH kiberbiztonsági felügyeleti tevékenységéért az 1. § (1) bekezdés *b)* pontja szerinti azon szervezet, amely egyúttal a 2. és 3. melléklet szerinti szervezet is, valamint az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet – ha a szervezet a Polgári Törvénykönyvről szóló törvény

szerinti elismert vállalatcsoport (a továbbiakban: elismert vállalatcsoport) ellenőrzött tagja, helyette az uralkodó tag – az SZTFH elnökének rendeletében – a (2) bekezdésben foglaltak alapján – meghatározott mértékű kiberbiztonsági felügyeleti díj fizetésére köteles.

(2) Az éves kiberbiztonsági felügyeleti díj mértéke az (1) bekezdés szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – legfeljebb 0,015 százaléka, de legfeljebb 10 millió forint. Az ugyanazon elismert vállalatcsoportban vagy az ugyanazon, a Polgári Törvénykönyvről szóló törvény szerinti tényleges vállalatcsoportban, vagy a számvitelről szóló törvény szerinti anyavállalatot, leányvállalatokat és a konszolidálásba bevont közös vezetésű vállalkozásokat tartalmazó, egy konszolidációs körbe tartozó vállalkozáscsoportban részt vevő szervezetek tekintetében a fizetendő éves kiberbiztonsági felügyeleti díj együttes mértéke nem haladhatja meg az 50 millió forintot. A tényleges vállalatcsoportként vagy az egy konszolidációs körbe tartozó vállalkozáscsoportként való működés tényét az (1) bekezdés szerinti szervezet az SZTFH elnökének rendeletében foglaltak szerint igazolja.

(3) A kiberbiztonsági felügyeleti díjat az (1) bekezdés szerinti kötelezett az SZTFH elnökének rendeletében meghatározott módon és időpontban köteles megfizetni az SZTFH részére.

**8. §** (1) Az e törvény hatálya alá tartozó elektronikus információs rendszert működtető, nem Magyarországon bejegyzett szervezetnek Magyarország területén működő képviselőt kell írásban kijelölnie, aki az e törvényben foglaltak végrehajtásáért a szervezet vezetőjére vonatkozó szabályok szerint felel. A képviselő kijelölése nem érinti a szervezet, illetve a szervezet vezetőjének felelősségét.

(2) A szervezet vezetője köteles gondoskodni arról, hogy a szervezet együttműködjön a kiberbiztonsági hatósággal.

(3) Az együttműködés során a szervezet vezetője

*a)* gondoskodik a jogszabályban és a hatóság honlapján meghatározottak szerint az adatoknak, dokumentumoknak, valamint ezek változásainak, a változást követő tizenöt napon belül a kiberbiztonsági hatóság részére – nyilvántartásba vétel céljából – történő megküldéséről, valamint

*b)* biztosítja az ellenőrzés lefolytatásához szükséges feltételeket.

(4) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet – az 51. alcímben foglalt kivételekkel – az e törvény hatálya alá kerülését követő

*a)* 30 napon belül bejelenti a nemzeti kiberbiztonsági hatóság részére a 28. § (1) bekezdés 1. pont *a)–e)* és *j)* alpontjában meghatározott adatokat,

*b)* 30 napon belül bejelenti a nemzeti kiberbiztonsági hatóság részére az elektronikus információs rendszer biztonságáért felelős személy adatait,

*c)* 90 napon belül a 6. § (3) bekezdés 1. pontjában foglaltaknak megfelelően felméri a szervezet által használt elektronikus információs rendszereket,

*d)* 120 napon belül – ha releváns – elvégzi a 9. § szerinti adatosztályozást,

*e)* 180 napon belül megküldi a nemzeti kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát,

*f)* 180 napon belül – a 6. § szerinti kockázatmenedzsment keretrendszer létrehozatalával együttesen – elvégzi a már meglévő elektronikus információs rendszereinek biztonsági osztályba sorolását és megteszi a Kormány rendeletében meghatározott tartalmú bejelentést a nemzeti kiberbiztonsági hatóságnak.

(5) Az 1. § (1) bekezdés *b)* pontja hatálya alá tartozó, és egyidejűleg 2. és 3. melléklet szerinti szervezetnek minősülő szervezet, valamint az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet köteles a működése megkezdését követő vagy az e törvény hatálya alá kerülést követő 30 napon belül a 29. § (1) bekezdés *a)* pontjában meghatározott adatokat – a 29. § (1) bekezdés *a)* pont *ab)* alpontja szerinti adatok kivételével – megküldeni az SZTFH részére a nyilvántartásba vétel érdekében.

(6) A (4) és (5) bekezdés alkalmazása szempontjából az e törvény hatálya alá kerülés időpontja

*a)* új szervezet esetében a szervezet létesítésének,

*b)* a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvényben foglalt, a középvállalkozásokra vonatkozó méretkorlátok elérése esetében a bekövetkezést követő év első,

*c)* a hatály alá kerülést eredményező jogállást megalapozó jogi aktus hatálybalépésének napja.

(7) A szervezet a kiberbiztonsági információk megosztása érdekében az informatikáért felelős miniszter rendeletében meghatározott együttműködések megvalósítása céljából – a honvédelmi célú elektronikus információs rendszerekre vonatkozó információk kivételével – kiberbiztonsági információmegosztási megállapodásokat köthet. A szervezet kiberbiztonsági információmegosztási megállapodás megkötéséről, ilyen megállapodásban való részvételéről vagy annak felmondásáról tájékoztatja a kiberbiztonsági hatóságot.

## 5. Adatosztályozás

**9. §** (1) Annak érdekében, hogy a szervezet által kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az 1. § (1) bekezdés *a)* pontja szerinti szervezet köteles az általa az elektronikus információs rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szerinti osztályozására kormányrendeletben foglaltak szerint.

(2) Az 1. § (1) bekezdés *b)* és *c)* pontja szerinti szervezet az adatosztályozást nem privát felhőszolgáltatás igénybevétele és külföldi adatkezelés megvalósítása esetén köteles elvégezni, a külföldi vagy nem privát felhőszolgáltatás igénybevételével történő adatkezelés kockázatainak felmérése érdekében.

(3) Az adatosztályozás során figyelembe kell venni a logikailag együtt, egységben kezelt elektronikus adatok – ideértve az adatbázist, adattárat, egyedi dokumentumot és egyéb adatállományt – együttes biztonsági igényét.

(4) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet kizárólag az adatosztályozás alapján, annak eredményére figyelemmel vehet igénybe nem privát felhőszolgáltatást, vagy kezelhet külföldön adatot, amennyiben más jogszabály a felhőszolgáltatás igénybevételét, vagy a külföldi adatkezelést nem tiltja vagy korlátozza.

(5) A szervezet a biztonsági osztályba sorolás keretében, valamint abban az esetben vizsgálja felül az adatosztályozást, amennyiben az elektronikus információs rendszerben kezelendő adatok körében változás következik be.

## 6. A biztonsági osztályba sorolás

**10. §** (1) A szervezet elektronikus információs rendszerei, valamint az azokban kezelt adatok, a nyújtott szolgáltatások kockázatokkal arányos védelmének biztosítása érdekében a szervezet az e törvény hatálya alá tartozó, a szervezet rendelkezésében lévő elektronikus információs rendszereit „alap”, „jelentős” vagy „magas” biztonsági osztályba sorolja az érintett elektronikus információs rendszer sértetlensége és rendelkezésre állása, valamint az általa kezelt adat bizalmassága, sértetlensége és rendelkezésre állásának kockázata alapján, szigorodó védelmi előírásokkal.

(2) A biztonsági osztályba sorolásról a szervezet vezetője dönt, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolás eredményét a szervezet az elektronikus információs rendszerek nyilvántartásában vagy egyéb belső szabályzatban rögzíti.

(3) A biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket az informatikáért felelős miniszter rendeletben határozza meg.

(4) A szervezet az elektronikus információs rendszer biztonsági osztálya alapján meghatározza és megvalósítja az informatikáért felelős miniszter rendeletében előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

(5) Az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja szerinti szervezet elektronikus információs

rendszere vonatkozásában az e törvény hatálya alá kerüléskor teljesítenie kell legalább az informatikáért felelős miniszter rendeletében az „alap” biztonsági osztály vonatkozásában előírt védelmi intézkedéseket.

(6) Ha az (5) bekezdés szerinti elektronikus információs rendszer vonatkozásában a biztonsági osztályba sorolás alapján az „alap”-nál magasabb biztonsági osztály került meghatározásra, a védelem elvárt erősségének eléréséhez a szervezetnek a biztonsági osztályba sorolást követően legfeljebb két év áll rendelkezésére a biztonsági osztályhoz rendelt biztonsági intézkedések kivitelezésére.

(7) A biztonsági osztályba sorolást legalább kétévente, vagy az elektronikus rendszer biztonságát érintő, jogszabályban meghatározott változás esetén soron kívül, dokumentált módon felül kell vizsgálni.

## 7. Az elektronikus információs rendszer biztonságáért felelős személy

**11. §** (1) A szervezet vezetője az elektronikus információs rendszer védelméhez kapcsolódó feladatok ellátása, a kockázatmenedzsment keretrendszer működtetése, a kiberbiztonsági incidensek bejelentése és a kiberbiztonsági incidenskezelő központtal való kapcsolattartás érdekében a szervezeten belül kijelöli az elektronikus információs rendszer biztonságáért felelős személyt vagy a szervezeten kívüli személlyel megállapodást köt.

(2) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek esetében az (1) bekezdés szerinti megállapodás kötelező tartalmi elemeit kormányrendelet tartalmazza. Megállapodás megkötése esetén is meg kell jelölni azt a természetes személyt, aki az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátja.

(3) Az elektronikus információs rendszer biztonságáért felelős személy feladatait csak olyan személy végezheti, aki

*a)* cselekvőképes, büntetlen előéletű és

*b)* az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet esetében rendelkezik a feladatellátáshoz szükséges, az informatikáért felelős miniszter rendeletében előírt végzettséggel, szakképzettséggel, akkreditált nemzetközi képzettséggel vagy az informatikáért felelős miniszter rendeletében meghatározott szakterületen szerzett szakmai tapasztalattal.

(4) Elektronikus információs rendszer biztonságáért felelős személyként – az (5) bekezdésben foglalt kivétellel – nem jelölhető ki vagy bízható meg a szervezet gazdasági vezetői feladatait ellátó személy vagy az a személy, aki a szervezeten belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el, illetve ilyen személy közvetlen alárendeltségébe tartozik.

(5) A (4) bekezdést nem kell alkalmazni a következő szervezetek vonatkozásában:

*a)* az 1. § (1) bekezdés *a)–c)* pontja szerinti fontos szervezetek,

*b)* az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek.

(6) A szervezet vezetője biztosítja, hogy az elektronikus információs rendszer biztonságáért felelős személy

*a)* valamennyi, az elektronikus információs rendszerek védelmét érintő döntés előkészítésében részt vegyen;

*b)* rendelkezésére álljanak az elektronikus információs rendszer védelmének biztosításához szükséges feltételek, jogosultságok, információk, humán- és anyagi erőforrások;

*c)* hozzáférjen mindazon rendszerekhez, adatokhoz és információkhoz, amelyek az általa ellátandó feladatok végrehajtásához szükségesek és

*d)* ha a szervezeten belül került kijelölésre, a szakmai ismereteinek fenntartásához szükséges, az informatikáért felelős miniszter rendeletében meghatározott képzéseken, továbbképzéseken részt vegyen.

(7) Az elektronikus információs rendszer biztonságáért felelős személyt feladata ellátásával

kapcsolatosan tudomására jutott adatok és információk tekintetében titoktartási kötelezettség terheli. A titoktartási kötelezettség alól a szervezet vezetője adhat felmentést.

(8) Az elektronikus információs rendszer biztonságáért felelős személy részt vesz az informatikáért felelős miniszter rendeletében meghatározott szakmai képzésen, továbbképzésen.

(9) Az elektronikus információs rendszer biztonságáért felelős személy jogosult a szervezet elektronikus információbiztonsági kötelezettségeinek, feladatainak teljesítésében közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében jogosult megismerni a követelményeknek való megfelelőség alátámasztásához szükséges közreműködői tevékenységgel kapcsolatos adatot, valamint az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(10) Indokolt esetben a szervezet kijelölhet vagy megbízhat az elektronikus információs rendszer biztonságáért felelős személy helyettesítésére jogosult személyt, aki az elektronikus információs rendszer biztonságáért felelős személy tartós távolléte vagy akadályoztatása esetén ellátja az elektronikus információs rendszer biztonságáért felelős személy feladatait. Az elektronikus információs rendszer biztonságáért felelős személy és helyettese között a feladatok és felelősség megosztásáról a szervezet vezetője rendelkezik. A helyettesre az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó rendelkezéseket kell alkalmazni.

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

(12) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet esetében az elektronikus információs rendszer biztonságáért felelős személy feladat- és hatáskörére vonatkozó részletes szabályokat kormányrendelet határozza meg.

(13) A nemzeti kiberbiztonsági hatóság nyilvántartást vezet az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas személyekről.

(14) Az elektronikus információs rendszer biztonságáért felelős személyek nyilvántartásának célja, hogy a nyilvántartásban szereplő személyek közül a szervezetek a feladat ellátására alkalmas elektronikus információs rendszer biztonságáért felelős személyt választhassanak.

(15) Az elektronikus információs rendszer biztonságáért felelős személyek nyilvántartásába kerülés, illetve az onnan való törlés rendjét kormányrendelet határozza meg.

(16) A nemzeti kiberbiztonsági hatóság hatósági ellenőrzés keretében vizsgálja, hogy az elektronikus információs rendszer biztonságáért felelős személy megfelel-e a (3) bekezdés *a)* pontjában meghatározott büntetlen előéletre irányuló követelménynek. Ennek megállapítása érdekében adatot igényelhet a bűnügyi nyilvántartási rendszerből.

## 8. Az elektronikus információs rendszerek biztonságával kapcsolatos oktatás és képzés

**12. §** (1) A kiberbiztonsággal kapcsolatos képzést folytató felsőoktatási intézmény a képzési tevékenység ellátásával összefüggésben

*a)* gondoskodik az elektronikus információs rendszer biztonságáért felelős személyek képzéséről, továbbá

*b)* közreműködhet az információbiztonsági, kibervédelmi, valamint a kritikus szervezetek vonatkozásában a komplex ellenálló képességi gyakorlatokon.

(2) A kiberbiztonsággal kapcsolatos képzést folytató szervezet

*a)* az alapvető és fontos szervezetek vezetői, az elektronikus információs rendszer biztonságáért felelős személyek által irányított szervezeti egységek munkatársai részére képzést,

*b)* az alapvető és fontos szervezetek vezetői, az elektronikus információs rendszer biztonságáért felelős személyek, az elektronikus információs rendszer biztonságáért felelős személyek által irányított szervezeti egységek munkatársai részére továbbképzést

szervezhet.

## 9. Az elektronikus információs rendszer fejlesztése, továbbfejlesztése

**13. §** (1) Új elektronikus információs rendszerek fejlesztése, vagy már meglévő elektronikus információs rendszerek továbbfejlesztése (a továbbiakban együtt: fejlesztés) vonatkozásában jelen alcím rendelkezéseit kell alkalmazni az alábbi, alapvető szervezetnek minősülő szervezetek esetében

*a)* az 1. § (1) bekezdés *a)* és *c)* pontja szerinti szervezet, valamint

*b)* a 2. és 3. melléklet szerinti szervezetnek nem minősülő, az 1. § (1) bekezdés *b)* pontja szerinti szervezet.

(2) Elektronikus információs rendszer fejlesztése esetén a szervezet az információbiztonsági követelmények teljesülésének biztosítása és az elektronikus információs rendszer működésének nemzeti kiberbiztonsági hatóság általi jóváhagyása érdekében a kormányrendeletben meghatározottak szerint jár el.

(3) A fejlesztés során az elektronikus információs rendszer tervezési életciklusában végre kell hajtani – ahol az adatosztályozási kötelezettséget e törvény előírja – a rendszerben kezelni tervezett adatok osztályozását és az elektronikus információs rendszer biztonsági osztályba sorolását, amelyet a kormányrendeletben meghatározott módon a nemzeti kiberbiztonsági hatóságnak jóváhagyásra be kell nyújtani

*a)* belső fejlesztés esetén az erőforrások allokációját megelőzően,

*b)* külső fejlesztés esetén az arra irányuló szerződés megkötését megelőzően – a közbeszerzésekre vonatkozó jogszabályi rendelkezéseket is figyelembe véve – olyan módon, hogy az információbiztonsági követelmények az elektronikus információs rendszer fejlesztésére irányuló szerződésbe rögzítésre kerüljenek.

(4) A szervezet rögzíti a fejlesztésre irányuló szerződésben a nemzeti kiberbiztonsági hatóság által jóváhagyott osztályba soroláshoz kapcsolódó követelményeket és a fejlesztés során intézkedik azok megvalósulása iránt a fejlesztést végző szervezet felé.

(5) A fejlesztést a nemzeti kiberbiztonsági hatóság által jóváhagyott, a biztonsági osztály vonatkozásában az informatikáért felelős miniszter rendeletében meghatározott védelmi követelményeknek megfelelően kell végrehajtani.

(6) Ha a fejlesztés során olyan körülmény jut a szervezet tudomására, amely befolyásolja az érintett elektronikus információs rendszer biztonságát, akkor a (2)–(4) bekezdésben meghatározott feladatokat ismételten el kell végezni.

(7) A nemzeti kiberbiztonsági hatóság eljárása során elrendelhet sérülékenységvizsgálatot.

(8) Új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer továbbfejlesztése során a megállapított biztonsági osztályhoz tartozó követelményeket a rendszer használatbavételéig teljesíteni kell.

(9) A szervezet vezetőjének az elektronikus információs rendszer használatba vételére, további használatára irányuló, a 6. § (3) bekezdés 12. pontja szerinti döntése abban az esetben hozható meg, ha a nemzeti kiberbiztonsági hatóság által jóváhagyott biztonsági osztályba sorolásból következő követelmények a (8) bekezdés szerinti módon teljesültek.

(10) A 6. § (3) bekezdés 12. pontja szerinti döntéssel egyidejűleg gondoskodni kell az elektronikus információs rendszer kormányrendeletben meghatározott adatainak nemzeti kiberbiztonsági hatósághoz történő bejelentéséről.

(11) Központi rendszer fejlesztése esetén – az (1)–(10) bekezdésben foglaltakon túlmenően – az elektronikus információs rendszer felett rendelkezési jogosultsággal bíró szervezet köteles első alkalommal a tervezés fázisában és azt követően minden mérföldkő elérésekor tájékoztatni a nemzeti kiberbiztonsági hatóságot a központi rendszer biztonságát érintő kérdések vonatkozásában.

**14. §** (1) A 13. §-ban foglaltaktól eltérően, ha az elektronikus információs rendszer fejlesztése

*a)* az 1. § (1) bekezdés *b)* pontja szerinti és egyben a 2. vagy 3. melléklet szerinti szervezetnek

minősülő alapvető szervezet által történik, az alapvető szervezet köteles biztonsági osztályba sorolni az elektronikus információs rendszert és az annak megfelelő védelmi követelményeket kell teljesíteni,

*b)* fontos szervezet által történik, a fejlesztés során legalább az „alap” biztonsági osztálynak megfelelő védelmi követelményeket kell teljesíteni.

(2) Az (1) bekezdés szerinti szervezet intézkedik a védelmi követelmények megvalósulása iránt a fejlesztést végző szervezet felé.

(3) Az (1) bekezdés szerinti szervezet köteles a kiberbiztonsági hatóság részére bejelenteni

*a)* az elektronikus információs rendszert a tervezési életciklusban, a fejlesztés megkezdését megelőzően, valamint

*b)* a szervezet vezetőjének az elektronikus információs rendszer használatba vételére, további használatára irányuló, a 6. § (3) bekezdés 12. pontja szerinti döntését követően.

(4) Indokolt esetben a kiberbiztonsági hatóság sérülékenységvizsgálatot rendelhet el.

(5) A biztonsági osztályhoz tartozó követelményeket a rendszer használatbavételéig teljesíteni kell, a szervezet vezetőjének az elektronikus információs rendszer használatba vételére, további használatára irányuló, 6. § (3) bekezdés 12. pontja szerinti döntése ezek teljesülése esetében hozható meg.

**15. §** (1) Ha az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet elektronikus információs rendszerének sérülékenységvizsgálata jogszabály vagy a nemzeti kiberbiztonsági hatóság döntése alapján kötelező, akkor a 6. § (3) bekezdés 12. pontja szerinti döntés feltétele a feltárt sérülékenységek vonatkozásában készített sérülékenységkezelési terv nemzeti kiberbiztonsági hatóság általi jóváhagyása.

(2) Az (1) bekezdés szerinti, „jelentős” és „magas” biztonsági osztályba tartozó elektronikus információs rendszer esetében kötelező a kormányrendelet szerinti teljes körű sérülékenységvizsgálat kezdeményezése. Sérülékenységvizsgálat végzésének kötelezettsége alól kormányrendeletben meghatározott, sérülékenységvizsgálat végzésére jogosult állami szerv döntése alapján mentesülhet a szervezet.

(3) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet elektronikus információs rendszerei fejlesztése során irányadó részletes szabályokat kormányrendelet tartalmazza.

## 10. Kiberbiztonsági audit

**16. §** (1) Az 1. § (1) bekezdés *b)* pontja szerinti azon szervezet, amely egyúttal a 2. és 3. melléklet szerinti szervezet is, valamint az 1. § (1) bekezdés *d)* pontja és – a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti mikrovállalkozás kivételével – az 1. § (1) bekezdés *e)* pontja szerinti szervezet az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles kétévente, illetve a 23. § (1) bekezdése szerint illetékes kiberbiztonsági hatóság általi elrendelés esetén kiberbiztonsági auditot végeztetni.

(2) A szervezet köteles

*a)* a nyilvántartásba vételét követő 120 napon belül a kiberbiztonsági audit elvégzésére a 21. § (3) bekezdése szerinti nyilvántartásban szereplő auditorral megállapodást kötni, és

*b)* a kiberbiztonsági auditot első alkalommal a nyilvántartásba vételét követő két éven belül elvégeztetni.

(3) A honvédelmi célú elektronikus információs rendszerek tekintetében kiberbiztonsági audit nem végezhető.

(4) Ha az (1) bekezdés szerinti szervezet honvédelmi célú elektronikus információs rendszer felett is rendelkezési jogosultsággal bír, a szervezet vezetője felelős a (3) bekezdésben foglalt rendelkezések teljesüléséért.

(5) A honvédelmi kiberbiztonsági hatóság a jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok és az ország védelme és biztonsága szempontjából jelentős kettős kijelöléssel nem érintett honvédelmi szervezet és honvédelmi infrastruktúra

elektronikus információs rendszere esetében a honvédelmi célú elektronikus információs rendszerként történő nyilvántartásba vételről tájékoztatja az SZTFH-t.

## 11. A támogató rendszerekre vonatkozó speciális rendelkezések

**17. §** (1) A szervezetnek gondoskodnia kell arról, hogy a támogató rendszer is az általa támogatott elektronikus információs rendszernek megfelelő szintű védelemben részesüljön az informatikáért felelős miniszter rendeletében foglaltak alapján, ha az adott védelmi intézkedések kockázatarányosan alkalmazhatók az érintett támogató rendszer vonatkozásában. A szervezet köteles felmérni a támogató rendszerben használt védelmi intézkedéseket.

(2) Ha a szervezet a támogató rendszert szolgáltatásként nyújtja, tájékoztatja a támogató rendszert felhasználó szervezetet arról, hogy a támogató rendszer milyen biztonsági osztályhoz tartozó követelményeknek felel meg.

(3) Kizárólag olyan támogató rendszer vehető igénybe, amely megfelel az általa támogatott elektronikus információs rendszer védelmi igényeinek.

## 12. A központi rendszerekre vonatkozó speciális rendelkezések

**18. §** (1) A központi rendszer felett rendelkezési jogot gyakorló szervezet az általa a felhasználó szervezet részére biztosított központi rendszer vonatkozásában

*a)* ellátja 4. alcímben meghatározott feladatokat;

*b)* bejelenti a nemzeti kiberbiztonsági hatóság részére, hogy a rendelkezésében lévő központi rendszert mely szervezet részére szolgáltatja;

*c)* szerződéses követelményként meghatározza vagy szerződés hiányában honlapján elérhetővé teszi a felhasználó szervezet számára a központi rendszer védelme érdekében a felhasználó szervezet által a központi rendszer igénybevétele feltételeként betartandó elektronikus információbiztonsági követelményeket;

*d)* ellenőrizheti a *c)* pontban meghatározott feladatok végrehajtását;

*e)* a *d)* pont szerinti ellenőrzés során feltárt hiányosságok pótlására, hibák javítására határidő jelölésével felszólítja a felhasználó szervezetet, ennek eredménytelensége esetén további intézkedések megtétele érdekében tájékoztatja a nemzeti kiberbiztonsági hatóságot;

*f)* együttműködik a felhasználó szervezettel, ennek keretében

*fa)* a felhasználó szervezetet a központi rendszert érintő előre tervezett eseményekről legalább öt nappal az esemény előtt értesíti,

*fb)* soron kívül tájékoztatja a központi rendszert érintő kiberbiztonsági incidensekről,

*fc)* az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens esetén tájékoztatja a lehetséges megelőző, helyreállításhoz szükséges vagy egyéb intézkedésekről,

*fd)* ha a felhasználó szervezet elektronikus információs rendszere vonatkozásában végzett sérülékenységvizsgálat a központi rendszert érintő hibát, hiányosságot tár fel, intézkedik azok kijavítása érdekében,

*g)* bejelenti az illetékes kiberbiztonsági incidenskezelő központnak a központi rendszert érintő kiberfenyegetéseket, kiberbiztonsági incidensközeli helyzeteket, valamint

*h)* a központi rendszert érintő kiberfenyegetések, kiberbiztonsági incidensközeli helyzetek, kiberbiztonsági incidensek megelőzése, elhárítása, kezelése, illetve a következmények csökkentése érdekében megteszi az illetékes kiberbiztonsági incidenskezelő központ által előírt intézkedéseket, valamint az általa igénybe vett szolgáltatás érintettsége esetén intézkedik a szolgáltatás nyújtója felé a szükséges intézkedések megtétele érdekében.

(2) A felhasználó szervezet által igénybe vett központi rendszer vonatkozásában a felhasználó szervezet

*a)* az elektronikus információs rendszereinek a nemzeti kiberbiztonsági hatóság részére történő bejelentése során a központi rendszer használatát – a központi rendszer azonosítására alkalmas

adatok, valamint a központi rendszer felett rendelkezési jogot gyakorló szervezet megjelölésével – bejelenti,

*b)* a központi rendszer felett rendelkezési jogot gyakorló szervezet által meghatározott elektronikus információbiztonsági követelményeket teljesíti, ezeket rögzíti az információbiztonsági szabályzatában és

*c)* a központi rendszert érintő kiberbiztonsági incidenseket bejelenti az illetékes kiberbiztonsági incidenskezelő központ és a központi rendszer felett rendelkezési jogot gyakorló szervezet részére.

(3) Jogszabály alapján kötelezően igénybe vett felett rendelkezési jogot gyakorló szervezet esetén a központi rendszer szolgáltatója és a felhasználó szervezet közötti feladat- és felelősségmegosztást az adott központi rendszerre vonatkozó jogszabály rögzíti. Ennek hiányában, valamint önkéntesen igénybe vett központi rendszer esetében a központi rendszer felett rendelkezési jogot gyakorló szervezet és a felhasználó szervezet szolgáltatási szerződést köt.

(4) A központi rendszerekről a nemzeti kiberbiztonsági hatóság nyilvántartást vezet.

(5) A nemzeti kiberbiztonsági hatóság jogosult a központi rendszer vonatkozásában mind a központi rendszer szolgáltatójánál, mind a felhasználó szervezetnél az elektronikus információbiztonsági követelmények teljesülését ellenőrizni.

## 13. A központi szolgáltatók által nyújtott rendszerekre vonatkozó speciális rendelkezések

**19. §** (1) A központi szolgáltató tájékoztatja a felhasználó szervezetet arról, hogy az általa nyújtott szolgáltatás milyen biztonsági osztály követelményeinek megfelelő szolgáltatásokat tud nyújtani, vagy arról, hogy a központi szolgáltatásokat megvalósító rendszerek milyen biztonsági osztály követelményeinek felelnek meg. Amennyiben a központi szolgáltató által nyújtott szolgáltatással érintett elektronikus információs rendszer biztonsági osztályának megfelelnek a központi szolgáltató által biztosított védelmi intézkedések, a felhasználó szervezet igénybe veszi a szolgáltatást. Ellenkező esetben a felhasználó szervezet nem veszi igénybe a szolgáltatást, illetve kötelező igénybevétel esetén a felhasználó szervezet gondoskodik a felhasználó szervezet hatáskörében megvalósítható, kockázatarányos helyettesítő intézkedések alkalmazásáról.

(2) A központi szolgáltató

*a)* köteles folyamatosan kapcsolatot tartani a nemzeti kiberbiztonsági hatósággal,

*b)* bejelenti a nemzeti kiberbiztonsági hatóság részére, hogy a központi szolgáltatást vagy támogató rendszert mely szervezet részére nyújtja,

*c)* gondoskodik a központi szolgáltatás vagy a támogató rendszer kockázatarányos védelmi intézkedéseinek megvalósításáról,

*d)* meghatározza és elérhetővé teszi a felhasználó szervezet számára a központi szolgáltatás vagy támogató rendszer védelme érdekében a felhasználó szervezet által az igénybevétel feltételeként betartandó elektronikus információbiztonsági követelményeket,

*e)* együttműködik a felhasználó szervezettel, ennek keretében

*ea)* a központi szolgáltatást vagy a támogató rendszert érintő előre tervezett eseményekről legalább öt nappal az esemény előtt értesíti,

*eb)* soron kívül tájékoztatja a központi szolgáltatást vagy a támogató rendszert érintő kiberbiztonsági incidensekről,

*ec)* kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens esetén tájékoztatja a lehetséges megelőző, helyreállításhoz szükséges vagy egyéb intézkedésekről,

*ed)* ha a felhasználó szervezet elektronikus információs rendszere vonatkozásában végzett sérülékenységvizsgálat a központi szolgáltatást vagy a támogató rendszert érintő hibát, hiányosságot tár fel, intézkedik azok kijavítása érdekében,

*f)* bejelenti az illetékes kiberbiztonsági incidenskezelő központnak a központi szolgáltatást vagy a támogató rendszert érintő kiberfenyegetéseket, kiberbiztonsági incidensközeli helyzeteket, kiberbiztonsági incidenseket, valamint

*g)* a központi szolgáltatást vagy a támogató rendszert érintő kiberfenyegetések, kiberbiztonsági incidensközeli helyzetek, kiberbiztonsági incidensek megelőzése, elhárítása, kezelése, illetve a következmények csökkentése érdekében megteszi az illetékes kiberbiztonsági incidenskezelő központ által előírt intézkedéseket, valamint az általa igénybe vett szolgáltatás érintettsége esetén intézkedik a szolgáltatás nyújtója felé a szükséges intézkedések megtétele érdekében.

(3) A központi szolgáltató által a felhasználó szervezet részére biztosított központi szolgáltatás vagy támogató rendszer vonatkozásában a felhasználó szervezet

*a)* bejelenti a nemzeti kiberbiztonsági hatóság részére a központi szolgáltatás vagy a támogató rendszer használatát a központi szolgáltató megjelölésével,

*b)* a központi szolgáltató által meghatározott elektronikus információbiztonsági követelményeket teljesíti, ezeket rögzíti az információbiztonsági szabályzatában, valamint

*c)* a központi szolgáltatást vagy a támogató rendszert érintő kiberbiztonsági incidenseket bejelenti a kiberbiztonsági incidenskezelő központ és a központi szolgáltató részére.

(4) Jogszabály alapján kötelezően igénybe vett központi szolgáltatás vagy támogató rendszer esetén a központi szolgáltató és a felhasználó szervezet közötti feladat- és felelősségmegosztást az adott központi szolgáltatásra vagy támogató rendszerre vonatkozó jogszabály rögzíti. Ennek hiányában, valamint önkéntesen igénybe vett központi szolgáltatás vagy támogató rendszer esetében a központi szolgáltató és a felhasználó szervezet direktfinanszírozási szerződést köt.

(5) A központi szolgáltató által az állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújtott informatikai és elektronikus hírközlési szolgáltatási feladatokra vonatkozó részletes szabályokat kormányrendelet határozza meg.

(6) A központi szolgáltató által nyújtott központi szolgáltatásokról és támogató rendszerekről a nemzeti kiberbiztonsági hatóság nyilvántartást vezet.

(7) A nemzeti kiberbiztonsági hatóság jogosult az elektronikus információbiztonsági követelmények teljesülését mind a központi szolgáltatónál, mind a felhasználó szervezetnél ellenőrizni.

## 14. A legfelső szintű doménnév-nyilvántartás

**20. §** (1) A legfelső szintű domén alatt bejegyzett doménnevekről a legfelső szintű doménnév-nyilvántartó központi nyilvántartást vezet.

(2) A központi doménnév-nyilvántartás tartalmazza:

*a)* az érintett doménnevet,

*b)* a doménnév-regisztráció dátumát,

*c)* a doménnévhasználó nevét, kapcsolattartásra alkalmas elektronikus levelezési címét, telefonszámát, és

*d)* a doménnevet kezelő adminisztratív kapcsolattartó nevét, elektronikus levelezési címét és telefonszámát, ha azok eltérnek a *c)* pont szerinti adatoktól.

(3) A (2) bekezdés szerinti adatok kezelésének célja a doménnevet kezelő adminisztratív kapcsolattartó, valamint a doménnév-használó természetes vagy jogi személy azonosító és kapcsolattartási adatainak naprakészen tartása.

(4) A központi doménnév-nyilvántartás adatai hitelességének ellenőrzése és integritásának biztosítása érdekében a legfelső szintű doménnév-nyilvántartó köteles az ellenőrzésre vonatkozó – az SZTFH által előzetesen jóváhagyott – eljárásrendet nyilvánosan közzétenni.

(5) A legfelső szintű doménnév-nyilvántartó a központi doménnév-nyilvántartásban szereplő adatokat – a személyes adatok kivételével – nyilvánosan hozzáférhetővé teszi.

(6) A legfelső szintű doménnév-nyilvántartó a központi doménnév-nyilvántartásban szereplő adatokhoz az ügyészség, a nemzetbiztonsági szolgálatok, a nyomozó hatóságok és a büntetőeljárásról szóló törvény szerinti előkészítő eljárást folytató szervezetek, a kiberbiztonsági hatóság és a kiberbiztonsági incidenskezelő központ részére közvetlen hozzáférést biztosít.

# *III. FEJEZET*

# *A KIBERBIZTONSÁGI FELÜGYELET*

## 15. A kiberbiztonsági auditra vonatkozó rendelkezések

**21. §** (1) Az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségét az auditor ellenőrzi a kiberbiztonsági audit végrehajtása során.

(2) Kiberbiztonsági auditot az az auditor végezhet, amely a feladat ellátásához szükséges szakértelemmel és infrastrukturális feltételekkel rendelkezik, valamint az 57. § (1) bekezdés *c)* pontja szerinti gazdálkodó szervezetnek (a továbbiakban: sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet) minősül. Az auditorral szemben támasztott követelményeket az SZTFH elnöke rendeletben határozza meg.

(3) Az audit végrehajtására jogosult gazdálkodó szervezeteket a (2) bekezdés szerinti követelmények igazolt teljesítése esetén az SZTFH nyilvántartásba veszi az SZTFH elnökének rendeletében foglalt részletes szabályok szerint.

(4) A (3) bekezdés szerinti nyilvántartás tartalmazza:

*a)* az auditor adatait és annak kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát, valamint elektronikus levelezési címét,

*b)* az auditor – nyilvántartásba vételekor kapott – azonosító számát,

*c)* az auditor által igénybe vett közreműködő adatait, valamint kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát, elektronikus levelezési címét, és

*d)* az audit eredményét tartalmazó dokumentumot.

(5) A szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvénytől eltérően, ha a (3) bekezdés szerinti nyilvántartásba történő felvételről az SZTFH a rá irányadó ügyintézési határidőn belül nem döntött, a kérelmezőt nem illeti meg a kérelmében megjelölt tevékenység megkezdésének, illetve folytatásának joga, és az általános közigazgatási rendtartásról szóló törvénynek a hatóság mulasztására vonatkozó általános szabályait kell alkalmazni.

(6) Ha az auditor auditori tevékenységet már nem végez, akkor a (4) bekezdés szerinti adatokat az SZTFH a tevékenység befejezésének bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(7) Ha a (4) bekezdés szerinti adatok változását az auditor bejelenti, a nyilvántartásban a változás bejegyzését megelőzően szereplő adatot az SZTFH az adat változása bejegyzését követő öt év elteltével a nyilvántartásból törli.

(8) A (4) bekezdés szerinti adatok kezelésének célja az auditorokra vonatkozó információk naprakészen tartása, valamint az SZTFH ellenőrzési tevékenységének ellátása.

(9) A (4) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – adattovábbítás kizárólag a kiberbiztonsági hatóságok, valamint a kiberbiztonsági incidenskezelő központok részére végezhető.

**22. §** (1) A 21. § (1) bekezdése szerinti megfelelőség ellenőrzésére az auditor jogosult a tevékenység nyomon követésére alkalmas módon a következő vizsgálatokat elvégezni:

*a)* belső informatikai biztonsági és távoli sérülékenységvizsgálatot, valamint „jelentős” vagy „magas” biztonsági osztály esetén behatolásvizsgálatot,

*b)* kriptográfiai megfelelőségvizsgálatot, valamint

*c)* „jelentős” vagy „magas” biztonsági osztály esetén a kritikus biztonsági funkciókat végző egyedileg fejlesztett szoftverek biztonsági forráskódvizsgálatát.

(2) Az audit eredményét az auditor az SZTFH és a szervezet részére az audit befejezését követően

haladéktalanul megküldi.

(3) Az auditor írásban haladéktalanul tájékoztatja az SZTFH-t, ha a szervezet elektronikus információs rendszerével kapcsolatosan olyan tényt állapít meg, amely

*a)* a szervezet folyamatos működését súlyosan veszélyezteti, vagy

*b)* bűncselekmény elkövetésére, jogszabály megsértésére, a szervezet belső szabályzatának súlyos megsértésére vagy ezek veszélyére utaló körülményeket észlel.

(4) Az audit eredményét, valamint a (3) bekezdés szerinti tájékoztatást az SZTFH

*a)* az 1. § (1) bekezdés *b)* pontja szerinti szervezet esetében hivatalból megküldi,

*b)* az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet esetében a nemzeti kiberbiztonsági hatóság kérésére megküldi

a nemzeti kiberbiztonsági hatóság részére.

(5) Az auditor az ellenőrzött szervezet kezelésében lévő, az audit lefolytatásához szükséges, az ellenőrzött szervezettől megkapott dokumentumokat – ideértve a személyes adatokat és az üzleti titoknak minősülő adatokat is – az audit során ellenőrzött követelmények teljesülésének vizsgálata céljából, az audit lefolytatásához szükséges mértékben, annak befejezéséig kezeli, azokat harmadik személy részére nem továbbíthatja.

(6) Az auditor köteles szabályzatban rögzíteni azokat a munkaköröket, amelyeket betöltő személyek az audit során az üzleti titkokhoz hozzáférhetnek, annak tartalmát megismerhetik. Az auditban részt vevő személyeket az audit során tudomásukra jutott személyes adatok, valamint üzleti titok tekintetében titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követő 5 évig, személyes adatok tekintetében pedig időkorlát nélkül fennmarad.

(7) A jelen alcím szerinti kiberbiztonsági audit nem érinti a más jogszabály által előírt tanúsítási kötelezettséget.

(8) Az auditor kötelezettségeinek teljesítését az SZTFH ellenőrzi a 25. § (1) és (3) bekezdésének alkalmazásával.

(9) Az SZTFH elnöke rendeletben határozza meg az audit – általános forgalmi adó nélkül számított – legmagasabb díját, valamint a kiberbiztonsági audit lefolytatásának rendjét.

## 16. A kiberbiztonsági hatóságra vonatkozó általános rendelkezések

**23. §** (1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek kiberbiztonsági felügyeletét – a honvédelmi célú elektronikus információs rendszerek kivételével –

*a)* az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek elektronikus információs rendszerei esetében a Kormány rendeletében kijelölt nemzeti kiberbiztonsági hatóság,

*b)* az 1. § (1) bekezdés *d)* és *e)* pontja szerinti – az *a)* pont hatálya alá nem tartozó – szervezetek elektronikus információs rendszerei esetében az SZTFH

látja el.

(2) A honvédelmi célú elektronikus információs rendszerek esetében az e törvény szerinti kiberbiztonsági felügyeletet ellátó honvédelmi kiberbiztonsági hatóságot a honvédelmi ágazaton belül a Kormány rendeletben jelöli ki. A honvédelmi kiberbiztonsági hatóság tevékenységére a nemzeti kiberbiztonsági hatóságra vonatkozó rendelkezéseket kell alkalmazni.

(3) A nemzeti kiberbiztonsági hatóság önálló feladattal és hatósági jogkörrel rendelkező szerv, amely hatósági tevékenysége során kizárólag a jogszabályoknak van alávetve, minden más szervtől független és a feladatkörébe tartozó hatósági ügyek tekintetében – a feladat elvégzésére vagy a mulasztás pótlására irányuló utasítás kivételével – nem utasítható.

## 17. A kiberbiztonsági hatóság feladatai

**24. §** (1) A nemzeti kiberbiztonsági hatóság

1. vizsgálja az elektronikus információs rendszer biztonságáért felelős személy és helyettese jogszabályban foglalt követelményeknek való megfelelését, megfelelés esetén nyilvántartásba veszi

azt,

2. vizsgálja a biztonsági osztályba sorolás megalapozottságát és a vizsgálat eredménye alapján dönt annak nyilvántartásba vételéről,

3. nyilvántartásba veszi és nyilvántartja a 28. § (1) bekezdése szerinti adatokat,

4. az elektronikus információs rendszerek biztonságára vonatkozó irányelveket, ajánlásokat, követelményeket határoz meg,

5. iránymutatást adhat ki az európai uniós jogszabályban és az informatikáért felelős miniszter rendeletében meghatározott védelmi intézkedések egymásnak való megfeleltethetősége vonatkozásában,

6. az elektronikus információbiztonsági követelményeknek való megfelelés igazolása érdekében előírhatja – egy adott típusú technológia alkalmazásának előírása vagy előnyben részesítése nélkül – az elektronikus információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását,

7. ellenőrzi az elektronikus információs rendszerek osztályba sorolására vonatkozó, jogszabályban, vagy az általa meghatározott követelmények teljesülését,

8. elrendeli az ellenőrzése során feltárt vagy tudomására jutott biztonsági hiányosságok elhárítását, és az azok felszámolásához szükséges intézkedéseket, valamint ellenőrzi azok eredményességét,

9. megtehet, ellenőrizhet minden olyan, az elektronikus információs rendszerek védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek,

10. kiberbiztonsági incidens esetén – kormányrendeletben meghatározott esetben – hatósági eljárást indít, valamint a hozzá beérkező kiberbiztonsági incidensekről szóló bejelentésekről haladéktalanul tájékoztatja a nemzeti kiberbiztonsági incidenskezelő központot,

11. részt vehet információbiztonsági, kiberbiztonsági érintettségű gyakorlatokon, a nemzetközi információbiztonsági, kiberbiztonsági gyakorlatokon felkérésre képviseli Magyarországot,

12. hazai és nemzetközi információbiztonsági, kiberbiztonsági eseményeken képviseli Magyarországot,

13. részt vehet az (EU) 2022/2555 európai parlamenti és tanácsi irányelv 19. cikke szerinti szakértői értékelésben, illetve értékelést kezdeményezhet,

14. nyomon követi az (EU) 2022/2555 európai parlamenti és tanácsi irányelv hazai végrehajtását,

15. közreműködik a magyar kibertér védelmét szolgáló tudatosító tevékenységekben,

16. ellenőrzi az elektronikus információs rendszerek fejlesztése során az információbiztonsági követelmények teljesülését,

17. kormányrendeletben foglaltak szerint jóváhagyja az elektronikus információs rendszerek használatba vételét, a megállapított hiányosságok pótlásáig megtilthatja vagy korlátozhatja az elektronikus információs rendszer használatát, a külföldön történő adatkezelést és a felhőszolgáltatás igénybevételét,

18. alapvető vagy fontos szervezetként azonosíthat valamely szervezetet kormányrendeletben meghatározottak szerint,

19. javaslatot tehet a Kszetv. szerinti kijelölő hatóság részére kritikus szervezet, valamint a Vbö. szerinti kijelölő hatóság részére az ország védelme és biztonsága szempontjából jelentős szervezet kijelölésére,

20. hazai információbiztonsági, kiberbiztonsági gyakorlatokat szervezhet, elrendelheti a szervezet gyakorlaton való részvételét, illetve a szervezet által szervezett gyakorlatok vonatkozásában iránymutatást adhat ki,

21. szakhatóságként jár el az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló kormányrendeletben meghatározott szakkérdésekben,

22. az elektronikus információs rendszerek biztonságáért felelős európai uniós és nemzetközi szervezetekben, bizottságokban képviseli Magyarországot és

23. ellátja az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerinti egyedüli

kapcsolattartó pont feladatait.

(2) A nemzeti kiberbiztonsági hatóság az ellenőrzési feladatainak ellátása körében a Kszetv. és a Vbö. szerinti kijelölő hatóság javaslatainak előzetes kikérésével, kockázatelemzés alapján éves ellenőrzési tervet készít.

(3) A honvédelmi kiberbiztonsági hatóság ellátja az (1) bekezdés 1–11., 15–21. pontjában foglalt feladatokat, tevékenységére nem kell alkalmazni a 11. § (13) bekezdésének, valamint a 28. § (4) és (7) bekezdésének rendelkezéseit. A honvédelmi kiberbiztonsági hatóság az (1) bekezdés 10. pont esetén a honvédelmi kiberbiztonsági incidenskezelő központot tájékoztatja.

(4) A nemzeti kiberbiztonsági hatóság, valamint a honvédelmi kiberbiztonsági hatóság feladat- és hatáskörét, valamint az eljárására vonatkozó részletes szabályokat kormányrendelet tartalmazza.

(5) Az SZTFH

*a)* az (1) bekezdés 4., 5., 7., 8. és 11–15. pontjában, valamint a (3) és (4) bekezdésben, továbbá az SZTFH elnökének rendeletében foglaltak szerint jár el,

*b)* elrendelhet és ellenőrizhet minden olyan, az elektronikus információs rendszerek védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek,

*c)* nyilvántartja a 29. § (1) bekezdése szerinti adatokat,

*d)* jelentős biztonsági esemény bekövetkezése vagy a biztonsági követelményeknek való nem megfelelés gyanúja esetén rendkívüli ellenőrzést hajthat végre vagy rendkívüli auditot rendelhet el,

*e)* a cél megjelölésével jogosult a szervezettől bekérni és megismerni:

*ea)* a biztonsági osztályba sorolás, valamint a biztonsági intézkedések megfelelőségét alátámasztó dokumentumokat,

*eb)* a belső informatikai biztonsági vizsgálat végrehajtásáról készült dokumentumot, és

*ec)* egyéb, a jogszabályi megfelelést alátámasztó adatot, információt, dokumentumot a felügyeleti feladatok elvégzése céljából.

(6) Az SZTFH hatósági ellenőrzése lefolytatásának részletes szabályait az SZTFH elnökének rendelete határozza meg.

(7) A kiberbiztonsági hatóság jogosult felügyeleti intézkedések megtételére vagy jogkövetkezmények alkalmazására

*a)* azon szervezetek vonatkozásában, amelyek Magyarország területén szolgáltatásokat nyújtanak vagy amelyek hálózati és információs rendszere Magyarország területén található, és e célból valamely európai uniós tagállam kiberbiztonsági hatóságától kölcsönös segítségnyújtás iránti megkeresés érkezik, valamint

*b)* a kijelölt képviselővel egyik európai uniós tagállamban sem rendelkező, de Magyarországon szolgáltatást nyújtó szervezetek vonatkozásában.

(8) A kiberbiztonsági hatóság jogszabályban meghatározott feladatai ellátása érdekében jogosult kockázatelemzés alapján rangsorolni a felügyeleti feladatok végrehajtását.

(9) Az élelmiszerláncról és hatósági felügyeletéről szóló törvény szerinti élelmiszerlánc-felügyeleti szerv minden év február 1. napjáig tájékoztatja az SZTFH-t – a 23. § (1) bekezdés *b)* pontja szerinti kiberbiztonsági felügyelettel kapcsolatos feladatok ellátása céljából – a 3. mellékletben foglalt táblázat 3. sora szerinti szervezetek megnevezéséről és székhelyéről.

## 18. A hatósági eljárás általános szabályai

**25. §** (1) A kiberbiztonsági hatóság eljárása során a sommás eljárás alkalmazása kizárt.

(2) A nemzeti kiberbiztonsági hatóság által lefolytatott hatósági eljárás ügyintézési határideje a védelmi intézkedések teljesítésére irányuló ellenőrzés, valamint a kiberbiztonsági incidensek kivizsgálására irányuló hatósági eljárás esetén százhúsz nap.

(3) Az SZTFH által lefolytatott hatósági ellenőrzés ügyintézési határideje százhúsz nap, az auditorok, a sérülékenységvizsgálat végzésére, az incidens vizsgálatára jogosult gazdálkodó szervezet hatósági nyilvántartásával, valamint a poszt-kvantumtitkosítás alkalmazását tanúsító

szervezet, illetve a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezetek ellenőrzésével kapcsolatos eljárás esetén kilencven nap.

(4) A (3) bekezdés szerinti eljárás felfüggeszthető a cégellenőrzés befejezéséig terjedő időtartamra.

## 19. Azonosítási eljárás

**26. §** (1) A nemzeti kiberbiztonsági hatóság alapvető vagy fontos szervezetként azonosíthat (a továbbiakban: azonosítási eljárás) egy szervezetet, ha az nem tartozik az 1. § (1) bekezdésének hatálya alá, illetve nem került a Kszetv. alapján kritikus szervezetként vagy a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölésre és az 1. § (6) bekezdésében meghatározott feltételek közül legalább egy teljesül.

(2) Az 1. § (6) bekezdés 6–9. pontja szerinti feltételek együttes fennállása esetén a nemzeti kiberbiztonsági hatóság alapvető szervezetként azonosítja a szervezetet.

(3) A nemzeti kiberbiztonsági hatóság az azonosítási eljárás során a 2. §-ban foglalt rendelkezésekre figyelemmel jár el.

**27. §** (1) A nemzeti kiberbiztonsági hatóság az azonosítási eljárás során hivatalból jár el.

(2) A nemzeti kiberbiztonsági hatóság határozatban rendelkezik a szervezet alapvető vagy fontos szervezetek nyilvántartásába történő felvételéről, ennek keretében meghatározza a szervezetnek az e törvény alapján teljesítendő feladatait és erről tájékoztatja a szervezetet.

(3) Az azonosítási eljárás lefolytatása érdekében a nemzeti kiberbiztonsági hatóság – személyes adatok kivételével – jogosult

*a)* a szervezettől,

*b)* a szervezet felett hatósági, felügyeleti vagy ellenőrzési jogkört gyakorló szervezettől és

*c)* közhiteles nyilvántartásokból

adatot igényelni.

(4) Ha az alapvető vagy fontos szervezetként azonosított szervezet az azonosítással nem ért egyet, abban az esetben a szervezet köteles bizonyítani, hogy nem felel meg az alapvető vagy fontos szervezetként történő azonosításról szóló döntésben megállapított feltételeknek.

## 20. A hatósági nyilvántartás

**28. §** (1) A nemzeti kiberbiztonsági hatóság az e törvényben meghatározott feladatainak végrehajtása céljából nyilvántartja és kezeli

1. a szervezet vonatkozásában:

*a)* a szervezet azonosításához szükséges adatokat,

*b)* a szervezet elérhetőségeit, ideértve elektronikus elérhetőségeket, valamint a szervezet által használt nyilvános IP-címeket vagy IP-tartományokat, valamint az 1. melléklet szerinti szervezetek kivételével a szervezet székhelyét, telephelyét, fióktelepét,

*c)* a szervezet alapvető vagy fontos szervezetnek minősülését,

*d)* a 2. és 3. melléklet szerinti ágazatba, alágazatba, szervezettípusba tartozását,

*e)* ha releváns, azon európai uniós tagállamok listáját, amelyben a szervezet szolgáltatásokat nyújt,

*f)* a szervezet elektronikus információs rendszereinek megnevezését, rövid leírását, biztonsági osztályának besorolását, a nyilvántartásba vétel, valamint a felülvizsgálat időpontjában elért biztonsági osztály meghatározását,

*g)* az elektronikus információs rendszerben kezelt adatok osztályozásához kapcsolódó adatokat, azok adatkezelésének helyszínét, ideértve az ország megnevezését vagy a felhő típusát,

*h)* az elektronikus információs rendszerhez kapcsolódóan igénybe vett felhőszolgáltatásokra vonatkozó adatokat,

*i)* az elektronikus információs rendszerhez kapcsolódó védelmi intézkedéseket és azok státuszát,

*j)* nem Magyarországon bejegyzett szervezet Magyarország területén működő képviselőjének

nevét vagy cégnevét, levelezési címét, telefonszámát és elektronikus levelezési címét,

*k)* az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó személy, szervezet azonosítására alkalmas adatokat, valamint a feladatot ténylegesen ellátó természetes személy személyazonosító adatait, közvetlen elérhetőséget biztosító telefonszámát, elektronikus elérhetőségét, végzettségét, szakképzettségét, szakmai tapasztalatát,

*l)* a szervezet információbiztonsági szabályzatát,

*m)* a szervezet vezetője és az elektronikus információs rendszer biztonságáért felelős személy továbbképzésére vonatkozó adatokat,

*n)* a honvédelmi célú elektronikus információs rendszerek kivételével az audit eredményét,

*o)* a hatósági ellenőrzésekkel kapcsolatos információkat,

*p)* a sérülékenységvizsgálat eredményét, valamint a sérülékenységek megszüntetésére vonatkozó sérülékenységkezelési tervet;

2. központi rendszerhez csatlakozott szervezet esetében:

*a)* a felhasználó szervezet által használt központi rendszer megnevezését, egyedi azonosító számát,

*b)* a központi rendszer felett rendelkezési jogot gyakorló szervezet nevét;

3. központi rendszer esetében az 1. pontban foglaltakon túl:

*a)* a központi rendszer egyedi azonosító számát,

*b)* a felhasználó szervezetek megnevezését;

4. a központi szolgáltató esetében az 1. pontban foglaltakon túl:

*a)* a központi szolgáltató által nyújtott szolgáltatásban részt vevő elektronikus információs rendszer egyedi azonosító számát,

*b)* a központi szolgáltató által biztosított támogató rendszer azonosítására alkalmas adatokat,

*c)* a felhasználó szervezetek megnevezését;

5. a kiberbiztonsági incidensekkel kapcsolatos, a kiberbiztonsági incidenskezelő központtól kapott értesítéseket, az ezekben szereplő személyekre vonatkozó adatokat;

6. az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas természetes személyek személyazonosító adatait, elérhetőségeit, ideértve az elektronikus elérhetőségeket, valamint a szakértelmére vonatkozó adatokat;

7. a kormányrendeletben előírt további, személyes adatnak nem minősülő adatokat.

(2) A honvédelmi kiberbiztonsági hatóság az e törvényben meghatározott feladatainak végrehajtása céljából nyilvántartja az (1) bekezdés 1. pont *a)–m), o)* és *p)* alpontja szerinti, továbbá a 2.–5. és 7. pontja szerinti adatokat.

(3) A nemzeti kiberbiztonsági hatóság, valamint a nemzeti kiberbiztonsági incidenskezelő központ a honvédelmi kiberbiztonsági hatóság nyilvántartásából az (1) bekezdés 1. pont *a)–c), j)–k)* és *p)* alpontjai szerinti adatokat megismerheti.

(4) A nemzeti kiberbiztonsági hatóság – az SZTFH által nyújtott adatszolgáltatást is figyelembe véve – összeállítja az alapvető és fontos szervezetek jegyzékét, és azt kétévente felülvizsgálja.

(5) Az (1) és a (2) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – adattovábbítás kizárólag

*a)* az SZTFH,

*b)* a nemzeti kiberbiztonsági incidenskezelő központ,

*c)* az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerinti egyedüli kapcsolattartó pont,

*d)* a Nemzeti Adatvédelmi és Információszabadság Hatóság,

*e)* a Kszetv. szerinti kijelölő és nyilvántartó hatóság,

*f)* a Vbö. szerinti kijelölő és nyilvántartó hatóság,

*g)* az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság,

*h)* a honvédelmi kiberbiztonsági hatóság,

*i)* a Magyar Honvédség kibertér műveleti erői,

*j)* a honvédelmi kiberbiztonsági incidenskezelő központ és

*k)* a nemzeti kiberbiztonsági hatóság

részére végezhető.

(6) A nemzeti kiberbiztonsági hatóság a kritikus szervezet és az ország védelme és biztonsága szempontjából jelentős szervezet által megküldött információbiztonsági szabályzatot továbbítja a Kszetv. és a Vbö. szerinti nyilvántartó hatóságnak.

(7) A nemzeti kiberbiztonsági hatóság a honlapján közzéteszi az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas természetes személyek listáját.

**29. §** (1) Az SZTFH – az e törvényben meghatározott feladatainak végrehajtása céljából – az SZTFH elnökének rendeletében foglaltak szerint nyilvántartja és kezeli

*a)* az 1. § (1) bekezdés *b), d)* és *e)* pontja szerinti szervezet vonatkozásában:

*aa)* a szervezet azonosításához szükséges adatokat,

*ab)* a szervezet székhelyét, telephelyét, fióktelepét,

*ac)* ha a szervezet nem az Európai Unióban letelepedett szervezet, de Magyarországon belül kínál szolgáltatásokat és magyarországi letelepedett képviselőt jelöl ki, a képviselő nevét vagy cégnevét, levelezési címét, telefonszámát és elektronikus levelezési címét,

*ad)* az elektronikus információs rendszer biztonságáért felelős személy természetes személyazonosító adatait, telefonszámát és elektronikus levelezési címét,

*ae)* azon európai uniós tagállamok listáját, amelyben a szervezet szolgáltatásokat nyújt,

*af)* az SZTFH elnökének rendeletében előírt további, személyes adatnak nem minősülő adatokat;

*b)* a sérülékenységvizsgálat végzésére jogosult szervezet azonosításához szükséges adatokat, a szervezet elérhetőségeit, ideértve az elektronikus elérhetőségeket;

*c)* a sérülékenységvizsgálat végzésére jogosult természetes személy azonosításához szükséges természetes személyazonosító adatait, elérhetőségeit, ideértve az elektronikus elérhetőségeket, valamint a sérülékenységvizsgálat végzésére jogosult természetes személy szakértelmére vonatkozó adatokat; valamint

*d)* a kiberbiztonsági incidensek kezelésére jogosult gazdálkodó szervezetek azonosításához szükséges adatokat, a szervezet elérhetőségeit, ideértve az elektronikus elérhetőségeket.

(2) Az SZTFH összeállítja az 1. § (1) bekezdés *d)* és *e)* pontja hatálya alá tartozó alapvető és fontos szervezetek, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzékét, és azt kétévente felülvizsgálja. A jegyzék összeállítását és felülvizsgálatát követően az SZTFH tájékoztatja a nemzeti kiberbiztonsági hatóságot a kormányrendeletben meghatározott adatokról.

(3) Az (1) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – adattovábbítás kizárólag a kiberbiztonsági hatóságok, valamint a kiberbiztonsági incidenskezelő központok részére végezhető.

(4) Az SZTFH közvetlen hozzáférést biztosít a nemzeti kiberbiztonsági hatóság, valamint a nemzeti kiberbiztonsági incidenskezelő központ részére a szervezetnek az SZTFH által kezelt nyilvántartási adataihoz.

(5) Ha az (1) bekezdés *a)* pontja szerinti nyilvántartásban szereplő szervezet bejelenti, hogy már nem minősül az 1. § (1) bekezdés *b), d)* vagy *e)* pontja szerinti szervezetnek, akkor az (1) bekezdés *a)* pontja szerinti adatokat az SZTFH a bejelentést követő öt év elteltével köteles a nyilvántartásból törölni.

## 21. Jogkövetkezmények

**30. §** (1) Ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a biztonsági hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, a kiberbiztonsági hatóság

*a)* figyelmezteti a jogszabályokban foglalt biztonsági követelmények és az azokhoz kapcsolódó

eljárási szabályok betartására, valamint megfelelő határidő tűzésével felszólítja a követelmények, az ellenőrzés vagy az audit során feltárt vagy tudomására jutott biztonsági hiányosságok elhárítására vagy a megfeleléshez szükséges intézkedések meghozatalára, a jelentéstételi, az adatszolgáltatási kötelezettségek teljesítésére,

*b)* kötelezheti a jogsértő magatartás megszüntetésére, valamint arra, hogy tartózkodjon a jogsértő magatartás ismételt elkövetésétől,

*c)* – ha a szervezet azzal rendelkezik – a szervezetet felügyelő szervhez vagy a nemzeti vagyonról szóló törvény szerinti tulajdonosi joggyakorlóhoz fordulhat és kérheti a közreműködését, valamint

*d)* jogosult kormányrendeletben vagy – az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek esetében – az SZTFH elnöke által kiadott rendeletben meghatározottak szerint a szervezet költségére információbiztonsági felügyelőt kirendelni.

(2) Ha az (1) bekezdés szerinti intézkedések alkalmazása ellenére az érintett szervezet a jogszabályokban foglalt biztonsági követelményeket vagy az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a biztonsági hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, a kiberbiztonsági hatóság az eset összes körülményének mérlegelésével kormányrendeletben meghatározott mértékű bírságot szabhat ki.

(3) Ha a szervezet vezetője a jogszabályban előírt kötelezettségének nem tesz eleget, a nemzeti kiberbiztonsági hatóság az eset összes körülményének mérlegelésével kormányrendeletben meghatározott mértékű bírsággal sújthatja, ismételt jogsértés esetén sújtani köteles.

(4) A kiberbiztonsági hatóság által kiszabható bírság mértékét, megállapításának szempontrendszerét, valamint a bírság megfizetése módjának részletes eljárási szabályait kormányrendelet határozza meg.

(5) A kiberbiztonsági hatóság

*a)* kötelezheti a szervezetet arra, hogy a jogszabálysértés tényét és körülményeit a kiberbiztonsági hatóság által meghatározott módon, az adatvédelmi és az üzleti titokra vonatkozó szabályokat figyelembe véve hozza nyilvánosságra,

*b)* elrendelheti a szervezet által nyújtott szolgáltatásokat igénybe vevők tájékoztatását az azokat potenciális érintő fenyegetésről, valamint az ilyen fenyegetés elhárításához szükséges vagy lehetséges megelőző, védelmi vagy helyreállítási intézkedésekről, azok várható hatásairól,

*c)* kiberbiztonsági incidens bekövetkezése esetén honlapján tájékoztathatja a nyilvánosságot, illetve a szervezeteket határozatban kötelezheti tájékoztatásra, ha az egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő kiberbiztonsági incidens kezeléséhez szükséges és

*d)* kötelezheti a szervezetet arra, hogy válságkezelési vagy veszélyhelyzet-kezelési intézkedés megtételének szükségessége esetén a kiberbiztonsági hatóságot tájékoztassa.

(6) Ha a nem közigazgatási szervnek minősülő alapvető szervezet a kiberbiztonsági hatóság által szabott határidőn belül nem tesz eleget a hatósági kötelezésnek, a kiberbiztonsági hatóság

*a)* kezdeményezheti az illetékes hatóságnál az alapvető szervezet által nyújtott, a jogsértéssel érintett alapvető szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozó tanúsítás vagy engedély ideiglenes felfüggesztését és

*b)* kezdeményezheti a cégbíróságnál az alapvető szervezet vezetőjének az adott szervezetben betöltött vezető tisztségviselői feladatainak ellátásától való ideiglenes eltiltását.

(7) Az (1), (2), valamint a (5) és (6) bekezdésben foglalt jogkövetkezmények együttesen és ismételten is alkalmazhatóak.

(8) Ha a szervezet megteszi a szükséges intézkedéseket a hiányosságok orvoslása érdekében, illetve a hatósági kötelezést teljesíti, a kiberbiztonsági hatóság intézkedik a (6) bekezdés szerinti ideiglenes intézkedések megszüntetése iránt.

(9) A kiberbiztonsági hatóság a jogkövetkezmények alkalmazása során az arányosság és a fokozatosság szempontjait figyelembe véve jár el, szem előtt tartva a jogkövetkezmény hatékonyságát és visszatartó erejét.

(10) Ha a hatósági kötelezést az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet figyelmen kívül

hagyja, vagy a nemzeti kiberbiztonsági hatóság által javasolt védelmi intézkedéseket önhibájából nem teljesíti és ezzel kiberbiztonsági incidens vagy kiberbiztonsági incidensközeli helyzet áll elő, a nemzeti kiberbiztonsági hatóság a szervezetet a kiberbiztonsági incidens vagy kiberbiztonsági incidensközeli helyzet bekövetkezésének elhárítására fordított költségének megtérítésére kötelezheti.

(11) Ha az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet a jogszabályokban foglalt kiberbiztonsági követelményeket vagy az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az SZTFH az (1)–(5) bekezdésben foglaltakon túl

*a)* jogosult a szervezet tevékenységét engedélyező vagy felügyelő hatóság véleményének figyelembevételével eltiltani az érintett szervezetet a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységtől,

*b)* bírság kiszabása esetén tájékoztatja a szervezet tevékenységét engedélyező vagy felügyelő hatóságot a bírság kiszabásáról és a kiszabást megalapozó tényekről.

**31. §** (1) A kiberbiztonsági hatóság a 30. § (1) bekezdés *d)* pontja szerinti információbiztonsági felügyelőt határozott időtartamra vagy meghatározott feltétel bekövetkezéséig rendeli ki. Az információbiztonsági felügyelő felügyeli a szervezetnél a jogszabályokban foglalt biztonsági követelmények teljesítését és az ehhez kapcsolódó eljárási szabályok betartását. Az információbiztonsági felügyelő tevékenységének szakmai irányítását a kiberbiztonsági hatóság látja el.

(2) Az 1. § (1) bekezdés

*a) a)–c)* pontja szerinti szervezetek esetében az információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat kormányrendelet, a végzettségére, képzettségére, szakképzettségére vagy szakmai tapasztalatára vonatkozó követelményeket az informatikáért felelős miniszter rendelete,

*b) d)* és *e)* pontja szerinti szervezetek esetében az információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat az SZTFH elnöke rendeletben

határozza meg.

**32. §** (1) Ha az SZTFH azt észleli vagy – akár a nemzeti kiberbiztonsági hatóság jelzése alapján – tudomást szerez arról, hogy az auditor a jogszabályokban foglalt kiberbiztonsági követelményeket vagy az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az SZTFH jogosult

*a)* figyelmeztetni a jogszabályokban foglalt követelmények vagy az ehhez kapcsolódó eljárási szabályok teljesítésére,

*b)* határidő tűzésével elrendelni az azonosított hiányosságok elhárítását vagy a megfeleléshez szükséges intézkedések meghozatalát, vagy

*c)* az auditort az auditori tevékenységtől ideiglenesen eltiltani, amiről tájékoztatja a nemzeti kiberbiztonsági hatóságot.

(2) Ha az (1) bekezdés szerinti intézkedések alkalmazása ellenére az auditor a jogszabályokban foglalt követelményeket vagy az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az azonosított hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, az SZTFH az eset összes körülményének mérlegelésével kormányrendeletben meghatározottak szerint bírságot szabhat ki, amely további nemteljesítés esetén megismételhető.

(3) Ha az SZTFH az (1) bekezdés szerint olyan jogsértést tár fel, amely hatással van az auditor által ellenőrzött szervezetre, az SZTFH az adott auditor által ellenőrzött szervezetnél kijelölt elektronikus információs rendszer biztonságáért felelős személyt haladéktalanul értesíti, és tájékoztatást ad az esetleges kiberbiztonsági incidens vagy adatszivárgás körülményeiről.

## 22. Az ideiglenes hozzáférhetetlenné tétel

**33. §** (1) A kiberbiztonsági hatóság határozatban elrendelheti az ideiglenes hozzáférhetetlenné

tételét annak az elektronikus hírközlő hálózat útján közzétett adatnak, amely a magyar kibertér biztonságára fenyegetést jelent, és amellyel kapcsolatosan a nemzeti kiberbiztonsági incidenskezelő központ kiberbiztonsági incidenskezelést folytat.

(2) A honvédelmi kiberbiztonsági hatóság rendeli el az ideiglenes hozzáférhetetlenné tételét annak az elektronikus hírközlő hálózat útján közzétett adatnak, amely honvédelmi érdeket sért vagy veszélyeztet, vagy honvédelmi célú elektronikus információs rendszer biztonságára fenyegetést jelent.

(3) Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a kiberbiztonsági hatóság azonnal végrehajthatónak nyilvánított határozatában rendeli el. Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a kiberbiztonsági hatóság legfeljebb kilencven napra rendeli el, amely időtartam indokolt esetben további kilencven nappal meghosszabbítható.

(4) Az elektronikus adat ideiglenes hozzáférhetetlenné tételét elrendelő határozatot a kiberbiztonsági hatóság hirdetményi úton közli, valamint megküldi a Nemzeti Média- és Hírközlési Hatóságnak (a továbbiakban: NMHH).

(5) A hirdetményt 3 napig kell a kiberbiztonsági hatóság honlapján közzétenni. A határozat közlésének napja a hirdetmény közzétételét követő nap.

(6) Az NMHH a határozatot az elektronikus hírközlésről szóló törvény szerinti kézbesítési rendszeren keresztül küldi meg a határozat kötelezettje részére.

(7) A (3) bekezdés szerinti határozat kötelezettje – annak határozatban történő megjelölése nélkül – valamennyi elektronikus hírközlési szolgáltató.

(8) Az ideiglenes hozzáférhetetlenné tétel végrehajtását az NMHH az elektronikus hírközlésről szóló törvény alapján szervezi és ellenőrzi.

(9) Az ideiglenes hozzáférhetetlenné tételre vonatkozó kötelezettség a határozatban megjelölt határidő leteltével megszűnik.

(10) Az ideiglenes hozzáférhetetlenné tételt a kiberbiztonsági hatóság annak megszűnése előtt megszünteti, ha

*a)* az elrendelés oka megszűnt,

*b)* a büntetőügyben eljáró bíróság, ügyészség vagy nyomozó hatóság, illetve az NMHH tájékoztatása alapján az elektronikus adattal kapcsolatban elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedés, illetve elektronikus adat végleges hozzáférhetetlenné tétele intézkedés elrendelése vagy végrehajtása van folyamatban, vagy

*c)* a rendelkezés elektronikus hírközlési szolgáltatók általi végrehajtása a megadott adattartalommal kétséges lehet.

(11) Ha a kiberbiztonsági hatóság az (1) vagy (2) bekezdés alapján elektronikus adat hozzáférhetetlenné tételét rendelte el, és a határozat véglegessé válását követően megállapítja, hogy a határozatban foglalt elektronikus adat közzétételével megvalósult jogellenes tevékenység a jogellenesség megállapítása szempontjából azonos tartalommal más elektronikus adat – így különösen más IP-cím, domain-domain vagy domain-aldomain – hozzáférhetővé tételével vagy közzétételével is megvalósul, akkor ismételt hatósági eljárás és – a (3) bekezdés szerinti – döntéshozatal mellőzésével a hozzáférhetetlenné tételhez szükséges adatok megküldésével elektronikus úton, biztonságos kézbesítési szolgáltatás útján értesíti az NMHH-t (a továbbiakban: egyszerűsített utánkövetés), amely ezen adatokat kizárólag elektronikus úton közli a hozzáférést biztosító elektronikus hírközlési szolgáltatókkal. Az egyszerűsített utánkövetésre tekintettel megküldött, a hozzáférhetetlenné tételhez szükséges adatok szerinti elektronikus adat hozzáférhetetlenné tételét az elektronikus hírközlési szolgáltatók a kapcsolódó, (3) bekezdés szerint hozott határozat végrehajthatósága fennállásáig kötelesek biztosítani.

**34. §** (1) Jelentős kiberfenyegetés elhárítása vagy folyamatban lévő kiberbiztonsági incidenssorozat megszakítása érdekében a nemzeti kiberbiztonsági incidenskezelő központ vezetője azonnali hatállyal elrendelheti az ideiglenes hozzáférhetetlenné tételt a kiberbiztonsági hatóság döntéséig vagy legfeljebb hetvenkét óra időtartamban.

(2) Az azonnali hatályú ideiglenes hozzáférhetetlenné tételt a technika állása szerinti lehető

legrövidebb idő alatt végre kell hajtani.

**35. §** (1) A kiberbiztonsági hatóság 1 millió forinttól 5 millió forintig terjedő bírsággal sújthatja azt az elektronikus hírközlési szolgáltatót, amely az ezen alcím szerinti kötelezettségének nem tesz eleget. A bírság a kötelezettség teljesítésére megszabott határidő eredménytelen elteleltét követően – újabb határidő megjelölése mellett – ismételten is kiszabható.

(2) A kiberbiztonsági hatóságot, az NMHH-t és az elektronikus hírközlési szolgáltatót nem terheli felelősség azért a kárért, amely abból származik, hogy a hozzáférhetetlenné tett elektronikus adat a 33. § (1) és (2) bekezdésében foglaltak mellett olyan egyéb tartalmat is magában foglal, amelynek technikai elválasztására nincs lehetőség, vagy az nem várható el a hozzáférhetetlenné tétel végrehajtása során.

### 23. Az elektronikus adat ideiglenes eltávolítása

**36. §** (1) Az elektronikus adat ideiglenes eltávolítására az érintett elektronikus adatot kezelő, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben meghatározott tárhelyszolgáltatót, illetve tárhelyszolgáltatást is végző közvetítő szolgáltatót (a továbbiakban együtt: eltávolításra kötelezett) kell kötelezni. Az eltávolításra kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására.

(2) A (1) bekezdésben meghatározott határozatot az elektronikus adat felett rendelkezésre jogosultnak akkor kell kézbesíteni, ha az eljárás addigi adatai alapján személye és elérhetősége ismert.

(3) Az ideiglenes eltávolításra a 33. § (1)–(5) és (9)–(11) bekezdése, valamint a 34–35. § megfelelően alkalmazandó.

## *IV. FEJEZET*

## *A KIBERBIZTONSÁGI TANÚSÍTÁSRA VONATKOZÓ RENDELKEZÉSEK*

**37. §** Az e fejezetben szabályozott kiberbiztonsági tanúsításra, valamint az (EU) 2019/881 európai parlamenti és tanácsi rendelet szerinti nemzeti kiberbiztonsági tanúsító hatóság (a továbbiakban: tanúsító hatóság) tevékenységére nem kell alkalmazni a megfelelőségértékelő szervezetek tevékenységéről szóló törvény rendelkezéseit.

### 24. A nemzeti kiberbiztonsági tanúsítási rendszerek követelményei

**38. §** A nemzeti kiberbiztonsági tanúsítási rendszernek a következő biztonsági célokat kell teljesítenie:

*a)* a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan tárolással, kezeléssel, hozzáféréssel és közléssel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,

*b)* a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan megsemmisítéssel, elvesztéssel, megváltoztatással vagy a hozzáférhetetlenséggel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,

*c)* annak biztosítása, hogy a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá,

*d)* az ismert függőségek és sebezhetőségek azonosítása és dokumentálása,

*e)* annak rögzítése, hogy a feljogosított személy, program vagy gép mely időpontban és mely védendő adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,

*f)* annak ellenőrizhetővé tétele, hogy a feljogosított személy, program vagy gép mely időpontban

és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,

*g)* annak ellenőrzése, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok nem tartalmaznak-e ismert sebezhetőségeket,

*h)* fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állásának, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása,

*i)* annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kockázatarányosan, alapértelmezetten és tervezetten biztonságosak legyenek,

*j)* annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok szoftvere és hardvere naprakész legyen, és

*k)* annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok vonatkozásában nem állnak fenn közismert sebezhetőségek, továbbá rendelkezésre állnak a biztonságos frissítésükre szolgáló mechanizmusok.

**39. §** (1) A nemzeti kiberbiztonsági tanúsítási rendszernek tartalmaznia kell:

*a)* a tanúsítási rendszer tárgyát és hatályát, az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok típusát vagy kategóriáit,

*b)* a tanúsítási rendszer céljának és annak az egyértelmű meghatározását, hogy a kiválasztott szabványok, értékelési módszerek és megbízhatósági szintek milyen módon felelnek meg a rendszer célfelhasználói igényeinek,

*c)* hivatkozást az értékelésben alkalmazott nemzetközi, európai vagy nemzeti szabványokra, vagy ha nem állnak rendelkezésre ilyen szabványok vagy azok nem megfelelőek, az 1025/2012/EU rendelet II. mellékletében meghatározott követelményeket teljesítő műszaki előírásokra, vagy ha ilyen előírások nem állnak rendelkezésre, az európai kiberbiztonsági tanúsítási rendszerben meghatározott műszaki előírásra vagy egyéb kiberbiztonsági követelményekre való hivatkozást,

*d)* a megbízhatósági szintet vagy szinteket,

*e)* a megfelelőségi önértékelésre vonatkozó kizáró vagy megengedő rendelkezést,

*f)* a megfelelőségértékelést végző személyekre, szervezetekre alkalmazandó kiegészítő követelményeket,

*g)* az alkalmazandó konkrét értékelési kritériumokat és módszereket, ideértve az értékelés típusait is,

*h)* a jelölések vagy címkék használati feltételeit,

*i)* a kiadandó nemzeti kiberbiztonsági tanúsítvány vagy megfelelőségi nyilatkozat tartalmát és formátumát, és

*j)* a rendszer alapján kibocsátott nemzeti kiberbiztonsági tanúsítványok kibocsátására, érvényességi idejére, fenntartására, meghosszabbítására, megújítására, valamint a hatályának bővítésére vagy szűkítésére vonatkozó feltételeket.

(2) Ha a nemzeti kiberbiztonsági tanúsítási rendszer több megbízhatósági szintre is érvényes, akkor a követelményeknek tartalmazniuk kell a különböző megbízhatósági szintekre vonatkozó elvárások pontos megkülönböztetését.

(3) A nemzeti kiberbiztonsági tanúsítási rendszerben meg kell határozni

*a)* az egyes követelményekhez vagy követelmény csoportokhoz tartozó értékelési eljárásokat,

*b)* azokat a kritikus védelmi funkciókat, amelyek esetében végre kell hajtani a tevékenység utólagos nyomon követésére is alkalmas belső informatikai biztonsági vagy távoli sérülékenységvizsgálatot vagy behatolásvizsgálatot, kriptográfiai értékeléseket, biztonsági forráskódelemzéseket, valamint

*c)* az értékelési eredmények dokumentálására vonatkozó követelményeket.

## 25. A nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjei

**40. §** (1) A nemzeti kiberbiztonsági tanúsítási rendszerek az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra az „alap”, a „jelentős” és a „magas” megbízhatósági

szintek közül egy vagy több szintet határozhatnak meg.

(2) A megbízhatósági szint arra vonatkozóan szolgál biztosítékkal, hogy az adott IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljesítik a vonatkozó biztonsági követelményeket, biztonsági funkciókat és olyan szintű értékelésen estek át, amely

*a)* „alap” megbízhatósági szinten a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok,

*b)* „jelentős” megbízhatósági szinten az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások kockázatának,

*c)* „magas” megbízhatósági szinten a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások kockázatának
minimalizálására törekszik.

(3) A megbízhatósági szintnek a biztonsági események valószínűsége és hatása szempontjából arányban kell állnia az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat rendeltetés szerinti használatához kapcsolódó kockázat szintjével.

(4) Az elvégzendő értékelési tevékenységeknek legalább a következőket kell magukban foglalniuk:

*a)* „alap” megbízhatósági szint esetén a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

*b)* „jelentős” megbízhatósági szint esetén

*ba)* a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

*bb)* a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát, és

*bc)* az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően működteti-e a szükséges biztonsági funkciókat,

*c)* „magas” megbízhatósági szint esetén

*ca)* a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,

*cb)* a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát,

*cc)* az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően, a legfejlettebb technika szerint működteti-e a szükséges biztonsági funkciókat, valamint

*cd)* behatolásvizsgálatok révén annak értékelését, hogy az mennyire ellenálló a jól képzett elkövetők által végrehajtott támadásokkal szemben.

## 26. A kiberbiztonsági tanúsítványokkal és a megfelelőségi nyilatkozatokkal kapcsolatos elvárások

**41. §** (1) A nemzeti kiberbiztonsági tanúsítványban és a nemzeti megfelelőségi nyilatkozatban meg kell jelölni:

*a)* azt a nemzeti kiberbiztonsági tanúsítási rendszert, amely alapján a tanúsítvány vagy a nyilatkozat kiállításra került,

*b)* a megbízhatósági szintet, valamint

*c)* a vonatkozó műszaki előírásokat, szabványokat és eljárásokat.

(2) A nemzeti kiberbiztonsági tanúsítványban és a nemzeti megfelelőségi nyilatkozatban fel kell tüntetni:

*a)* a kiállító szervezet nevét, címét,

*b)* a kiállítás dátumát,

*c)* a gyártó nevét és címét,

*d)* a megfelelőségértékelés megbízóját,

*e)* az alkalmazási területeket, vagy ha az adott alkalmazási területeken a megfelelőség feltételekkel érvényes, ezen feltételeket,

*f)* az érvényességi időt,

*g)* a tanúsítás tárgyát képező IKT-termék, IKT-szolgáltatás és IKT-folyamat azonosítását, ha van, annak verziószámát, valamint

*h)* a kiállító aláírását.

(3) A tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója vagy az olyan IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója, amelynek tekintetében megfelelőségi nyilatkozatot állítottak ki, köteles az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságát érintő sebezhetőségről vagy rendellenességről haladéktalanul tájékoztatni a tanúsító hatóságot.

**42. §** (1) Azon az IKT-terméken, IKT-szolgáltatáson vagy IKT-folyamatban, amely tanúsított, vagy amelynek tekintetében megfelelőségi nyilatkozatot állítottak ki, – az SZTFH elnökének vagy a 45. § (1) bekezdés *b)* pontja szerinti esetben a Kormány rendeletében meghatározott módon és formában – megfelelőségi jelölést kell elhelyezni.

(2) Tilos az (1) bekezdés szerinti megfelelőségi jelölés jogosulatlan elhelyezése, valamint olyan jelölés elhelyezése, amely hasonlít a megfelelőségi jelölés formájára, vagy azt a látszatot kelti, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat tanúsított, vagy annak vonatkozásában megfelelőségi nyilatkozatot állítottak ki, és így harmadik felet megtéveszthet.

## 27. Megfelelőségi önértékelés, megfelelőségértékelés

**43. §** (1) Megfelelőségi önértékelésre abban az esetben kerülhet sor, ha azt a nemzeti kiberbiztonsági tanúsítási rendszer az „alap” megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások és IKT-folyamatok esetében lehetővé teszi.

(2) A gyártó nemzeti megfelelőségi nyilatkozatot állít ki arról, hogy megtörtént annak vizsgálata, hogy a nemzeti kiberbiztonsági tanúsítási rendszer követelményei teljesülnek. A vizsgálatnak tartalmaznia kell a nemzeti kiberbiztonsági tanúsítási rendszer követelményei teljesülésének a tanúsítási rendszerben meghatározott módszertan szerinti értékelését.

(3) A megfelelőségi önértékelést végző gyártó a (2) bekezdés szerinti megfelelőségi nyilatkozat kiállítását követő 15 napon belül, nyilvántartásba vétel céljából – elektronikusan kereshető formában is – megküldi a tanúsító hatóság részére a megfelelőségi nyilatkozat másolati példányát, a műszaki dokumentációt, a nemzeti kiberbiztonsági tanúsítási rendszerben meghatározott értékelési módszer alapján elkészített értékelési jelentést, valamint a megjelölt tanúsítási rendszernek való megfeleléssel kapcsolatos összes egyéb lényeges értékelési információt.

**44. §** (1) Harmadik fél által végzett megfelelőségértékelési tevékenységet csak olyan szervezet végezhet,

*a)* amelyet a vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszerben meghatározott követelményekre figyelemmel a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló szerv akkreditált vagy külföldi akkreditált státusz esetén e státuszát elismerte,

*b)* amely az SZTFH elnökének – a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletében az egyes megbízhatósági szintekre vonatkozóan meghatározott követelményeknek megfelel, és

*c)* amelyet a tanúsító hatóság nyilvántartásba vett.

(2) A megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és tevékenységére vonatkozó részletes szabályokat

*a)* a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével az SZTFH elnöke

*b)* a hadiipari kutatás, fejlesztés, gyártás és kereskedelem vonatkozásban a Kormány

rendeletben határozza meg.

(3) A szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvénytől eltérően, ha az (1) bekezdés *c)* pontja szerinti nyilvántartásba történő felvételről a tanúsító hatóság a rá irányadó ügyintézési határidőn belül nem döntött, a kérelmezőt nem illeti meg

a kérelmében megjelölt tevékenység megkezdésének, illetve folytatásának joga, és az általános közigazgatási rendtartásról szóló törvénynek a hatóság mulasztására vonatkozó általános szabályait kell alkalmazni.

## 28. A kiberbiztonsági tanúsítás felügyelete

**45. §** (1) A tanúsító hatóság feladatait

*a)* az SZTFH,

*b)* az *a)* ponttól eltérően a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság látja el.

(2) A hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket az SZTFH elnöke rendeletben határozza meg. A hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a nemzeti kiberbiztonsági tanúsítási rendszerekre figyelemmel a tanúsítási rendszereket a Kormány rendeletben határozza meg.

**46. §** (1) A tanúsító hatóság az európai kiberbiztonsági tanúsítási rendszerekkel kapcsolatosan

*a)* nyomon követi az európai kiberbiztonsági tanúsítási rendszerek fejlesztését és figyelemmel kíséri a kapcsolódó szabványosítási folyamatokat,

*b)* részt vesz az európai kiberbiztonsági tanúsítási csoport tevékenységében,

*c)* információkat gyűjt azokról az ágazatokról és szakterületekről, amelyek nem esnek európai kiberbiztonsági tanúsítási rendszer hatálya alá és amelyek esetében a kiberbiztonság növelése szükséges,

*d)* az érdekelt feleknek szükség esetén tájékoztatást, támogatást nyújt,

*e)* elvégzi az (EU) 2019/881 európai parlamenti és tanácsi rendelet 57. cikk (4) bekezdése szerinti tájékoztatást.

(2) A tanúsító hatóság a nemzeti kiberbiztonsági tanúsítási rendszerek fenntartásával kapcsolatosan

*a)* legalább háromévente, az aktuális biztonsági kockázatokra figyelemmel értékeli a hatályos nemzeti kiberbiztonsági tanúsítási rendszereket,

*b)* felülvizsgálatot megalapozó ok felmerülését követően haladéktalanul intézkedik a nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata érdekében,

*c)* európai kiberbiztonsági tanúsítási rendszer kiadása esetén haladéktalanul intézkedik az azonos tárgyú nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata, továbbá hatályon kívül helyezése érdekében.

(3) Az (1) bekezdés *b)* és *e)* pontja szerinti feladatok tekintetében tanúsító hatóságként az SZTFH jár el.

**47. §** (1) A tanúsító hatóság eljárása során a sommás eljárás kizárt.

(2) A tanúsító hatóság ügyintézési határideje 120 nap.

(3) Európai kiberbiztonsági tanúsítási rendszer esetében a tanúsító hatóság a nemzeti akkreditáló szerv által akkreditált megfelelőségértékelő szervezetet a hatósági nyilvántartásba vételről szóló határozat véglegessé válásától számított 15 napon belül bejelenti az Európai Bizottság részére. A kérelmező szervezet az akkreditált státuszát a nemzeti akkreditáló szerv határozatának csatolásával igazolja.

(4) A tanúsító hatóság a megfelelőségértékelő szervezet vonatkozásában engedélyezési eljárást folytat le, ha az IKT-termékre, IKT-szolgáltatásra vagy IKT-folyamatra vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer

*a)* kiegészítő követelményeket ír elő és ez alapján engedélyezési eljárás lefolytatása válik szükségessé, vagy

*b)* „magas” megbízhatósági szintet ír elő a rendszer keretében kiadandó kiberbiztonsági tanúsítványra és a tanúsító hatóság az ilyen tanúsítvány kiállításának feladatát egyes nemzeti vagy európai kiberbiztonsági tanúsítványok vonatkozásában vagy általános jelleggel átruházza a

megfelelőségértékelő szervezetre.

(5) A (4) bekezdés *b)* pontja szerinti esetben az engedély megadásának feltétele, hogy a megfelelőségértékelő szervezet az 57. § (1) bekezdés *c)* pontja szerinti gazdálkodó szervezetnek minősüljön.

(6) A (4) bekezdés szerinti engedélyezési eljárásban kiadott engedély hatálya legfeljebb az akkreditált státusz lejártáig terjedhet.

(7) Európai kiberbiztonsági tanúsítási rendszer esetében a tanúsító hatóság a (4) bekezdés szerinti engedélyezési eljárás lefolytatása esetén a megfelelőségértékelő szervezetet az engedély megadásáról szóló határozat véglegessé válását követő 15 napon belül bejelenti az Európai Bizottságnak.

(8) A tanúsító hatóság kiberbiztonsági tanúsítási felügyeleti feladatai keretében jogosult

*a)* felszólítani a megfelelőségértékelő szervezeteket és a megfelelőségi nyilatkozatok kibocsátóit a hatósági feladatellátáshoz szükséges információk, adatok rendelkezésre bocsátására, valamint

*b)* a megfelelőségértékelő szervezeteknél és a megfelelőségi nyilatkozatok kibocsátóinál hatósági ellenőrzést végezni.

(9) A tanúsító hatóság eljár azzal – a 44. § szerinti követelményeknek nem megfelelő – szervezettel szemben, amely jogosulatlanul végez megfelelőségértékelési tevékenységet.

(10) A 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság által lefolytatott eljárásokért igazgatási szolgáltatási díjat kell fizetni. Az igazgatási szolgáltatási díj mértékét és az annak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat az e törvény végrehajtására a honvédelemért felelős miniszter által kiadott rendelet határozza meg.

**48. §** (1) A tanúsító hatóság nyilvántartja és kezeli:

*a)* az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártója által rendelkezésre bocsátott megfelelőségi nyilatkozat adatait,

*b)* a megfelelőségi nyilatkozathoz benyújtott műszaki dokumentációt és az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsítási rendszernek való megfelelésével kapcsolatos információkat,

*c)* a megfelelőségértékelő szervezet és annak kijelölt kapcsolattartója azonosításához szükséges adatokat, ha a megfelelőségértékelő szervezet egyben az (EU) 2019/881 európai parlamenti és tanácsi rendelet 56. cikk (5) bekezdése szerinti közjogi szerv, ennek tényét, valamint az SZTFH elnökének rendeletében meghatározott követelmények teljesülését alátámasztó dokumentumokat,

*d)* a nemzeti akkreditáló szerv által akkreditált megfelelőségértékelő szervezet akkreditált státuszára vonatkozó határozatban foglalt, valamint az akkreditált státusz változására vonatkozó információkat,

*e)* ha a 47. § (4) bekezdése szerinti engedélyezési eljárás lefolytatása szükséges, akkor az azzal kapcsolatos kérelmet, adatokat és dokumentumokat,

*f)* az engedélyezési eljárás során kiadott engedélyre, annak felfüggesztésére, részben vagy egészben történő visszavonására vonatkozó adatokat, valamint annak tényét, hogy az engedély hatályát vesztette,

*g)* ha a tanúsító hatóság a „magas” megbízhatósági szintű kiberbiztonsági tanúsítvány kiállításának jogát megfelelőségértékelő szervezetre átruházta, a delegált jogkör azonosításához szükséges adatokat,

*h)* az Európai Bizottság által a megfelelőségértékelő szervezet nyilvántartásba vételekor adott azonosító számot,

*i)* a megfelelőségértékelő szervezet által igénybe vett közreműködő, valamint kijelölt kapcsolattartója azonosításához szükséges adatokat,

*j)* a megfelelőségértékelő szervezet által kiadott tanúsítvány adatait,

*k)* a gyártó, valamint kijelölt kapcsolattartója azonosításához szükséges adatokat,

*l)* a tanúsítványok kiállításának megtagadásával, hatályának korlátozásával, felfüggesztésével és a visszavonásával kapcsolatos információkat,

*m)* a 41. § (3) bekezdése szerinti sebezhetőséggel vagy rendellenességgel kapcsolatos információt,

*n)* a felügyeleti tevékenység ellátása során tudomására jutott adatokat, dokumentumokat, valamint

*o)* a benyújtott panaszokkal kapcsolatos adatokat, dokumentumokat.

(2) Az (1) bekezdés szerinti nyilvántartás az (1) bekezdés *f)* és *g)* pontja szerinti adatok tekintetében közhiteles nyilvántartásnak minősül.

(3) Az (1) bekezdés szerinti adatok kezelésének célja az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságával összefüggő információk naprakészen tartása, valamint az azokat érintő sebezhetőséggel vagy rendellenességgel kapcsolatos feladatok, továbbá a tanúsító hatóság ellenőrzési és felügyeleti hatósági tevékenységének ellátása.

(4) Az (1) bekezdés szerinti nyilvántartásban szereplő bármely adatot érintően – ha jogszabály eltérően nem rendelkezik – a következő szervezetek részére végezhető adattovábbítás:

*a)* az Európai Bizottság részére a bejelentett megfelelőségértékelő szervezetek jegyzékének összeállítása és frissítése,

*b)* a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló szerv részére a megfelelőségértékelő szervezetek tevékenységének akkreditációjával és felügyeletével kapcsolatos feladatok ellátása, valamint

*c)* a 63. § szerinti kiberbiztonsági incidenskezelő központok részére a 41. § (3) bekezdése szerinti sebezhetőséggel vagy rendellenességgel kapcsolatos tevékenység ellátása

érdekében.

(5) A megfelelőségértékelő szervezet és a gyártó az (1) bekezdés szerinti adatokat az adatok rendelkezésre állásától, valamint az adatok változását a változás bekövetkezésétől számított 8 napon belül megküldi a tanúsító hatóság részére a nyilvántartásba vétel érdekében.

**49. §** (1) Ha a tanúsító hatóság tudomására jut vagy az ellenőrzése során megállapítja, hogy a megfelelőségértékelő szervezet vagy a gyártó a vonatkozó európai uniós vagy magyar jogszabályokban foglalt biztonsági követelményeket és a kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, – a figyelmeztetést tartalmazó döntésében határidő tűzésével – felszólítja a megfelelőségértékelő szervezetet vagy a gyártót a vonatkozó európai uniós és magyar jogszabályokban foglalt biztonsági követelmények és a kapcsolódó eljárási szabályok teljesítésére.

(2) Ha az (1) bekezdésben meghatározottak ellenére a megfelelőségértékelő szervezet vagy a gyártó a jogszabályban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a tanúsító hatóság – az eset összes körülményének mérlegelésével a kormányrendeletben meghatározott mértékű – bírságot szabhat ki, amely további nemteljesítés esetén megismételhető.

(3) A tanúsító hatóság a jogosulatlan megfelelőségértékelési tevékenységet végző személlyel szemben a Kormány rendeletében meghatározott mértékű közigazgatási bírságot szabhat ki. A Hatóság a bírság összegének megállapításakor a közigazgatási szabályszegések szankcióiról szóló törvényben foglalt szempontokat mérlegeli. Figyelmeztetés közigazgatási szankció alkalmazásának nincs helye.

**50. §** (1) A tanúsító hatóság a feladatellátása során megismert minősített adatot, személyes adatot vagy különleges adatot, valamint az üzleti titoknak, banktitoknak, fizetési titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak, orvosi titoknak és más hivatás gyakorlásához kötött titoknak minősülő és törvény által védett egyéb adatot kizárólag a feladat ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével kezeli. A tanúsító hatóság a hatósági ellenőrzés eredményeként tett megállapításokat alátámasztó adatokat rögzíti, és az így rögzített adatokat a megfelelőségértékelő szervezet akkreditált státuszának megszűnését követő 10. év utolsó napjáig, vagy a gyártó által kiadott megfelelőségi nyilatkozat hatályosságának megszűnését követő 10. év utolsó napjáig kezeli azzal, hogy ha az ellenőrzéssel érintett IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében megfelelőségértékelő szervezet által kiadott tanúsítvány és megfelelőségi önértékelés is rendelkezésre áll, az akkreditált státusz megszűnésének és a megfelelőségi nyilatkozat hatályossága megszűnésének időpontja közül a későbbi időpontot kell

figyelembe venni. Ezt követően a tanúsító hatóság az adatokat az elektronikus információs rendszereiből és adathordozóiról törli.

(2) A tanúsító hatóság eljárása során keletkezett adatok – ha törvény eltérően nem rendelkezik – nem nyilvánosak.

(3) A tanúsító hatóság munkatársait az (1) bekezdés szerint megismert adatok tekintetében – a jogszabályban meghatározott kivételekkel – 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 tanúsító hatóság a tanúsító hatósági tevékenységét, a hatósági ellenőrzést, valamint a nyilvántartás vezetésével kapcsolatos feladatainak ellátását az SZTFH elnöke – a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletében foglaltak szerint végzi.

(5) A gyártó a megfelelőségi önértékelés során, valamint a megfelelőségértékelő szervezet a tanúsítási eljárás során az SZTFH elnöke – a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletében foglaltak szerint jár el.

# *V. FEJEZET*

# *A POSZT-KVANTUMTITKOSÍTÁS*

## 29. A poszt-kvantumtitkosítás alkalmazásának általános szabályai

**51. §** A poszt-kvantumtitkosítás alkalmazására kötelezett szervezet elektronikus információs rendszere 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, a poszt-kvantumtitkosítás alkalmazására kötelezett szervezetek fizikailag elkülönített helyszíneik közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy információs társadalommal összefüggő szolgáltatásaik igénybevétele során a hagyományos kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantumtitkosítási alkalmazással történő
zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét.

## 30. A poszt-kvantumtitkosítás alkalmazására kötelezett szervezet védelme

**52. §** A poszt-kvantumtitkosítás alkalmazására kötelezett szervezet a jogszabályban meghatározott feladatainak ellátása körében köteles a fizikailag elkülönített helyszínei közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatás igénybevétele esetén poszt-kvantumtitkosítás alkalmazást annak kiépítéséhez az alkalmazás nyújtására jogosult, nyilvántartásba vett szervezettől beszerezni, és a kezelésében álló hálózatain a védelmet kialakítani, annak érdekében, hogy az elektronikus úton történő információáramlás a kvantumszámítógép okozta kibertámadás ellen biztosított legyen.

## 31. A poszt-kvantumtitkosítás alkalmazást nyújtó szervezetre vonatkozó feltételek

**53. §** (1) Kizárólag olyan szervezet nyújthat poszt-kvantumtitkosítás alkalmazást (a továbbiakban: poszt-kvantumtitkosítás alkalmazást nyújtó szervezet) a poszt-kvantumtitkosítás alkalmazására kötelezett szervezet számára, amely

*a)* nemzetbiztonsági kockázatot nem jelent és

*b)* a (3) bekezdés szerinti követelményeknek megfelel.

(2) Az (1) bekezdésben foglaltak alapján poszt-kvantumtitkosítás alkalmazás nyújtására vonatkozó tevékenységet kizárólag olyan szervezet végezhet,

*a)* amely a minősített adat védelméről szóló törvényben meghatározott telephely biztonsági tanúsítvánnyal rendelkezik, valamint

*b)* amelynek munkavállalója, alvállalkozója a minősített adat védelméről szóló törvényben meghatározott személyi biztonsági tanúsítvánnyal rendelkezik.

(3) A poszt-kvantumtitkosítás alkalmazás nyújtására vonatkozó tevékenységet csak olyan szervezet végezhet, amely által használt elektronikus információs rendszer biztosítja a rendszerelemek zártságát, és megakadályozza az informatikai rendszerhez történő jogosulatlan hozzáférést, valamint annak észrevétlen módosítását. A poszt-kvantumtitkosítás alkalmazást nyújtó szervezet elektronikus információs rendszerének meg kell felelnie az e törvény szerinti követelményeknek.

## 32. A poszt-kvantumtitkosítás követelményeinek való megfelelés tanúsítása

**54. §** (1) Az 53. § (3) bekezdésében meghatározott követelményeknek való megfelelést a poszt-kvantumtitkosítás alkalmazást nyújtani kívánó szervezetnek az 56. § (3) bekezdés *b)* pontja szerinti nyilvántartásban szereplő tanúsító szervezet (a továbbiakban: tanúsító szervezet) által kiadott, az informatikai rendszerre vonatkozó zártsági tanúsítással kell igazolnia.

(2) A tanúsító szervezet szakvéleményt bocsát ki a poszt-kvantumtitkosítás alkalmazást nyújtani kívánó szervezetnek arra vonatkozóan, hogy a végpontok közötti alkalmazása kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantumtitkosításra alkalmas.

(3) Ha tanúsító szervezet a tanúsított szervezet informatikai rendszerével kapcsolatosan olyan tényt állapít meg, amely a szervezet folyamatos működését kedvezőtlenül érinti vagy bűncselekmény elkövetésére, jogszabály megsértésére vagy ezek veszélyére utaló körülményeket észlel, haladéktalanul értesíti az SZTFH-t.

## 33. A tanúsító szervezetre vonatkozó rendelkezések

**55. §** (1) Tanúsító szervezet kizárólag olyan szervezet lehet, amely nemzetbiztonsági kockázatot nem jelent, és megfelel az 53. § (2) bekezdése szerinti követelményeknek.

(2) A tanúsító szervezet a poszt-kvantumtitkosítás alkalmazást nyújtani kívánó szervezet, vagy a tanúsított szervezet kezelésében lévő, a tanúsítás lefolytatásához szükséges adatokat – ideértve a megismert minősített adatot, személyes adatot vagy különleges adatot, üzleti titkot, banktitkot, fizetési titkot, biztosítási titkot, értékpapírtitkot, pénztártitkot, más hivatás gyakorlásához kötött titkot – kizárólag a tanúsítással igazolandó követelmények teljesülésének vizsgálata céljából, a tanúsítási eljárás lefolytatásához szükséges mértékben, a tanúsítási eljárás befejezéséig jogosult kezelni, azokat harmadik személy részére nem továbbíthatja.

(3) A tanúsító szervezet köteles szabályzatban rögzíteni azon munkaköröket, amelyeket betöltő személyek a tanúsítási eljárás során az üzleti titokhoz hozzáférhetnek, annak tartalmát megismerhetik. Az eljárásban részt vevő munkatársakat a tanúsítási eljárás során tudomásukra jutott üzleti titok tekintetében titoktartási kötelezettség terheli a poszt-kvantumtitkosítás alkalmazást tanúsító szervezetnél fennálló jogviszonyuk megszűnését követően is.

## 34. A poszt-kvantumtitkosítás felügyelete

**56. §** (1) Az SZTFH a felügyeleti jogkörében a tanúsító szervezet, illetve a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezetek tekintetében

*a)* hatósági ellenőrzést végezhet,

*b)* a jelen fejezetben meghatározott követelményeknek való nem megfelelés gyanúja esetén

rendkívüli ellenőrzést hajthat végre.

(2) A tanúsító szervezet, illetve a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezet kötelezettségeinek teljesítését az SZTFH ellenőrzi a 25. § (1) és (3) bekezdésének alkalmazásával az SZTFH elnökének rendeletében meghatározott részletes szabályok szerint.

(3) Az SZTFH – az e törvény szerinti ellenőrzési feladatainak végrehajtása céljából – nyilvántartást vezet

*a)* a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezetekről, valamint

*b)* az 54. § szerinti tanúsítást végző tanúsító szervezetről.

(4) A (3) bekezdés szerinti nyilvántartás tartalmazza:

*a)* a szervezet megnevezését és székhelyét, valamint annak kijelölt kapcsolattartója természetes személyazonosító adatait, telefonszámát, és elektronikus levelezési címét,

*b)* a szervezet – nyilvántartásba vételekor kapott – azonosító számát,

*c)* az SZTFH elnökének rendeletében előírt további, személyes adatnak nem minősülő adatokat.

(5) Ha a (3) bekezdés szerinti nyilvántartásban szereplő szervezet poszt-kvantumtitkosítás alkalmazás nyújtására vonatkozó tevékenységet vagy tanúsító tevékenységet már nem végez, akkor a (3) bekezdés szerinti adatokat az SZTFH a tevékenység befejezésének bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(6) Ha a (3) bekezdés szerinti adatok változását a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezet vagy a tanúsító szervezet bejelenti, a nyilvántartásban a változás bejegyzését megelőzően szereplő adatot az SZTFH az adat változása bejegyzését követő öt év elteltével a nyilvántartásból törli.

(7) A (3) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – adattovábbítás kizárólag a kiberbiztonsági hatóságok, valamint a kiberbiztonsági incidenskezelő központok részére végezhető.

# *VI. FEJEZET*

# *SÉRÜLÉKENYSÉGVIZSGÁLAT*

## 35. Sérülékenységvizsgálat végzésére jogosultak

**57. §** (1) Sérülékenységvizsgálat végzésére jogosult

*a)* a honvédelmi célú elektronikus információs rendszerek kivételével a Kormány rendeletében kijelölt állami szerv,

*b)* a honvédelmi célú elektronikus információs rendszerek vonatkozásában a honvédelmi kiberbiztonsági incidenskezelő központ, valamint

*c)* a telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges infrastrukturális feltételekkel és szakértelemmel rendelkező gazdálkodó szervezet, amely szerepel a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek SZTFH által vezetett nyilvántartásában.

(2) A sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet részéről kizárólag olyan személy végezheti a vizsgálatot,

*a)* akinek a nemzetbiztonsági ellenőrzését elvégezték és a nemzetbiztonsági ellenőrzés során nemzetbiztonsági kockázatot nem állapítottak meg,

*b)* aki rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges szakértelemmel,

*c)* aki a sérülékenységvizsgálati szakterületen legalább kétéves szakmai tapasztalattal rendelkezik, és

*d)* aki szerepel a sérülékenységvizsgálat lefolytatására jogosult személyek SZTFH által vezetett nyilvántartásában.

(3) Az (1) bekezdés *c)* pontja szerinti nyilvántartásba vétel feltétele, hogy a

sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet legalább két fő, (2) bekezdés szerinti szakértőt foglalkoztasson. Az (1) bekezdés *c)* pontja és a (2) bekezdés *d)* pontja szerinti nyilvántartásba vétel részletes szabályait, a tevékenység végzéséhez szükséges infrastrukturális feltételeket és szakértelmet az SZTFH elnöke által – az informatikáért felelős miniszter véleményének kikérésével – kiadott rendelet határozza meg.

(4) Az (1) és (2) bekezdés szerinti nyilvántartásba történő felvételi eljárás során az SZTFH a feladat ellátásához szükséges szakértelem és infrastrukturális feltételek teljesülésének megállapítása érdekében bevonja a sérülékenységvizsgálat végzésére jogosult állami szervet.

(5) A sérülékenységvizsgálatot – a honvédelmi célú elektronikus információs rendszerek kivételével – a sérülékenységvizsgálat végzésére jogosult állami szerv végzi

*a)* az 1. melléklet 1–9., 11., 14. és 15.pontja szerinti szervezetek,

*b)* a nemzeti kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezetnek a nemzeti kiberbiztonsági hatóság által meghatározott
elektronikus információs rendszere vonatkozásában.

(6) Ha a sérülékenységvizsgálat végzésére jogosult állami szervnek nem áll rendelkezésére elegendő humánerőforrás a sérülékenységvizsgálat elvégzésére, hozzájárulhat ahhoz, hogy az (5) bekezdésben meghatározott szervezet – a szervezet választása szerinti – sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezettel végeztesse el a sérülékenységvizsgálatot.

(7) Az állam, a gazdaság és a társadalom működése, biztonsága szempontjából kiemelkedő jelentőséggel bíró elektronikus információs rendszer sérülékenységvizsgálatát a sérülékenységvizsgálat végzésére jogosult állami szerv magához vonhatja vagy vizsgálatát támogathatja.

(8) A sérülékenységvizsgálatot a sérülékenységvizsgálat végzésére jogosult állami szerv végzi el, ha az (5) bekezdés *a)* pontja szerinti elektronikus információs rendszereken kívüli, a Kszetv. szerinti kritikus szervezet elektronikus információs rendszere tekintetében nincs a sérülékenységvizsgálat elvégzésére e törvényben meghatározott feltételeknek megfelelő, sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet.

(9) Az az (1) bekezdés szerinti szerv, amelynél a sérülékenységvizsgálatot kezdeményezték köteles vizsgálni a sérülékenységvizsgálat elvégzésére való jogosultságát, és ha más, az (1) bekezdés szerinti szerv kizárólagos jogosultságát állapítja meg, köteles a megkeresést az illetékes szervhez haladéktalanul továbbítani.

## 36. Sérülékenységvizsgálat megindítása

**58. §** (1) A nemzeti kiberbiztonsági hatóság a szervezetet kötelezheti arra, hogy sérülékenységvizsgálatot végeztessen. Ha a hatósági kötelezésnek a szervezet nem tesz eleget, a nemzeti kiberbiztonsági hatóság bírságot szabhat ki.

(2) Az (1) bekezdés szerinti hatósági kötelezés esetén a nemzeti kiberbiztonsági hatóság figyelembe veszi az elektronikus információs rendszernek az állam működése szempontjából való jelentőségét.

(3) A nemzeti kiberbiztonsági hatóság az (1) bekezdés szerinti kötelezésében meghatározza, hogy mely elektronikus információs rendszerre terjedjen ki a sérülékenységvizsgálat, valamint meghatározhatja az alkalmazandó sérülékenységvizsgálati eszközt vagy módszert is.

**59. §** A sérülékenységvizsgálat végzésére jogosult állami szerv saját kezdeményezésre is indíthat és lefolytathat sérülékenységvizsgálatot regisztrált felhasználói jogosultság birtokában, illetve annak hiányában is az 57. § (5) bekezdése szerinti szervezetek elektronikus információs rendszere vonatkozásában.

**60. §** (1) Az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek kivételével a törvény hatálya alá tartozó szervezet vezetője sérülékenységvizsgálatot hatósági kötelezés nélkül is kezdeményezhet, kizárólag a biztonsági osztályba sorolt és a kiberbiztonsági hatóság által nyilvántartásba vett elektronikus információs rendszer vonatkozásában.

(2) A szervezet vezetője az (1) bekezdés szerinti sérülékenységvizsgálatot – annak tervezése és előkészítése érdekében – annak tervezett kezdetét megelőzően legalább hatvan nappal köteles kezdeményezni. A sérülékenységvizsgálat tervezett kezdeti időpontjának meghatározása során a szervezet – az elektronikus információs rendszer használatba vételének tervezett időpontját is szem előtt tartva – a sérülékenységvizsgálati módszer kormányrendeletben meghatározott időigényét is figyelembe veszi.

(3) A sérülékenységvizsgálat végzésére jogosult állami szerv a hozzá beérkezett igények közötti mérlegelést követően fontossági sorrendet állíthat fel, amely fontossági sorrendre figyelemmel a vizsgálat már korábban kijelölt kezdő időpontját legfeljebb tizenöt nappal későbbi időpontban is meghatározhatja.

(4) A sérülékenységvizsgálat végzésére jogosult állami szerv előnyben részesíti a szervezet általi kezdeményezésekkel szemben a kiberbiztonsági hatóság által elrendelt vagy a hivatalból indított sérülékenységvizsgálat lefolytatását. A sorrend felállítása során a rendelkezésre álló erőforrások, valamint az elektronikus információs rendszernek kockázatalapú megközelítés alapján, az állam működése szempontjából való jelentőségének mérlegelésével jár el. Ha a szervezet által kezdeményezett igény teljesítése nem akadályozza kötelező feladatainak ellátását, a sérülékenységvizsgálat végzésére jogosult állami szerv szabad kapacitásai függvényében elvégzi a sérülékenységvizsgálatot.

**61. §** E törvény hatálya alá nem tartozó elektronikus információs rendszerek vonatkozásában a sérülékenységvizsgálat végzésére jogosult állami szerv az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezettel kötött megállapodás alapján végezhet sérülékenységvizsgálatot.

### 37. A sérülékenységvizsgálatra vonatkozó általános rendelkezések

**62. §** (1) A sérülékenységvizsgálat az elektronikus információs rendszer egy meghatározott részére is irányulhat.

(2) A sérülékenységvizsgálat a tevékenység jellegénél fogva szolgáltatáskiesést vagy -csökkenést eredményezhet, amelyből eredő károkért a sérülékenységvizsgálatot végző szervet – a szándékos károkozás kivételével – felelősség nem terheli.

(3) A sérülékenységvizsgálati módszereket és a sérülékenységvizsgálat végrehajtására vonatkozó részletszabályokat kormányrendelet határozza meg.

(4) A sérülékenységvizsgálat eredményéről a vizsgálatot végző szervezet állásfoglalást állít ki, amely tartalmazza a feltárt sérülékenységek besorolását is. Az állásfoglalás részletes tartalmi elemeit kormányrendelet határozza meg.

## *VII. FEJEZET*

## *A KIBERBIZTONSÁGI INCIDENSEKKEL KAPCSOLATOS RENDELKEZÉSEK*

### 38. A kiberbiztonsági incidenskezelő központok

**63. §** (1) A Kormány – a honvédelmi célú elektronikus információs rendszerek kivételével – az 1. § (10) bekezdésében meghatározott szervezetek nyílt elektronikus információs rendszereit érintő fenyegetések, kiberbiztonsági incidensek és válságok kezelése érdekében nemzeti kiberbiztonsági incidenskezelő központot működtet az általa rendeletben kijelölt szerv útján.

(2) A Kormány a honvédelmi célú elektronikus információs rendszereket érintő fenyegetések, kiberbiztonsági incidensek és válságok kezelése érdekében kiberbiztonsági incidenskezelő központot működtet az általa rendeletben kijelölt szerv útján.

(3) A nemzeti kiberbiztonsági incidenskezelő központ jóváhagyásával – a honvédelmi ágazat kivételével – ágazaton belüli kiberbiztonsági incidenskezelő központ (a továbbiakban: ágazaton belüli kiberbiztonsági incidenskezelő központ) is létrehozható a kormányrendeletben meghatározottak szerint. A nemzeti kiberbiztonsági incidenskezelő központ elvégzi vagy elvégezteti az ágazaton belüli kiberbiztonsági incidenskezelő központ képességeinek felmérését és vizsgálatát, amely alapján együttműködési megállapodást kötnek. A vizsgálat során az SZTFH elnökének a 70. § (3) bekezdés *b)* pontja szerinti rendeletében meghatározott feltételeket is figyelembe kell venni.

**64. §** (1) A nemzeti kiberbiztonsági incidenskezelő központ ellátja:

*a)* a kiberteret érintő fenyegetésekkel, a korai figyelmeztetéssel és a kiberbiztonsági incidensek megelőzésével,

*b)* a kiberbiztonsági incidensek kezelésével,

*c)* a kiberbiztonsági válsághelyzetek kezelésével,

*d)* a sérülékenységekkel,

*e)* a kiberbiztonsággal kapcsolatos tájékoztatási, tudatosító tevékenységgel és

*f)* az európai uniós és a nemzetközi együttműködésben Magyarország képviseletével

kapcsolatos, kormányrendeletben részletezett feladatokat.

(2) A nemzeti kiberbiztonsági incidenskezelő központ – a honvédelmi érdeket veszélyeztető kibertevékenységekkel és szervezetekkel kapcsolatos tevékenységek és a katonai kibertér műveletek kivételével –

*a)* ellátja az e törvény hatálya alá tartozó szervezetek tekintetében az ott meghatározott hatásköri szabályok szerint a kibertérből érkező fenyegetésekkel és támadásokkal szembeni feladatokat,

*b)* a honvédelmi ágazat kivételével irányítja a kibertérből érkező fenyegetésekre történő felkészülést és a kapcsolódó biztonsági feladatokat,

*c)* elemzi – az azon folytatott kommunikáció megismerése nélkül – az elektronikus hírközlési hálózatok forgalmát, észleli a kibertérből érkező fenyegetéseket és támadásokat,

*d)* végrehajtja vagy kezdeményezi a kibertérből érkező támadás megszakításához, valamint a bekövetkezés okainak és felelőseinek megállapítása érdekében szükséges intézkedéseket.

(3) A nemzeti kiberbiztonsági incidenskezelő központ az 1. § (10) bekezdésében meghatározott szervezetek elektronikus információs rendszere, vagy az e törvény hatálya alá tartozó IKT-termék vagy IKT-szolgáltatás vonatkozásában bármely természetes vagy jogi személy által bejelentett sebezhetőség, sérülékenység kapcsán ellátja a kormányrendelet által meghatározott koordinációs és egyéb feladatokat. A sebezhetőségek, sérülékenységek felderítésének, bejelentésének részletes szabályait a Kormány rendeletben szabályozza. Az 1. § (10) bekezdésében fel nem sorolt szervezetek elektronikus információs rendszere, vagy az e törvény hatálya alá nem tartozó IKT-termék vagy IKT-szolgáltatás vonatkozásában bejelentett sebezhetőség, sérülékenység esetén a nemzeti kiberbiztonsági incidenskezelő központ a rendelkezésére álló erőforrások függvényében és a veszélyeztetettség mértékének mérlegelésével látja el a kormányrendeletben meghatározott feladatokat. Ez utóbbi bejelentések tekintetében a nemzeti kiberbiztonsági incidenskezelő központ csak akkor köteles eljárni, ha az nem jelent aránytalan vagy indokolatlan terhet a nemzeti kiberbiztonsági incidenskezelő központ számára vagy a bejelentés az e törvény hatálya alá tartozó szervezet elektronikus információs rendszerét érinti.

(4) A magyar kiberteret súlyosan veszélyeztető kiberbiztonsági incidensek kezelését és vizsgálatát a nemzeti kiberbiztonsági incidenskezelő központ magához vonhatja vagy azok kezelését és vizsgálatát támogathatja.

(5) A honvédelmi kiberbiztonsági incidenskezelő központ a honvédelmi ágazat tekintetében ellátja az (1) bekezdés szerinti feladatokat.

(6) Az ágazaton belüli kiberbiztonsági incidenskezelő központ a nemzeti kiberbiztonsági incidenskezelő központtal kötött együttműködési megállapodásban meghatározott feladatokat látja el.

(7) A nemzeti kiberbiztonsági incidenskezelő központ, valamint a honvédelmi kiberbiztonsági

incidenskezelő központ feladat- és hatáskörét, feladatai ellátásának részletes szabályait, valamint a korai figyelmeztetés részletes szabályait, annak rendszerét, a rendszer üzemeltetőjének kijelölésére vonatkozó előírásokat, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét kormányrendelet határozza meg.

## 39. A kiberbiztonsági incidensek megelőzése

**65. §** (1) A nemzeti kiberbiztonsági incidenskezelő központ a kibertérből érkező fenyegetettségek felderítésére irányuló, védelmi, prevenciós célú eszközöket alkalmazhat és ez irányú szolgáltatásokat (a továbbiakban együtt: prevenciós eszközök) nyújthat az 1. § (1) bekezdése szerinti szervezeteknek.

(2) A prevenciós eszközök alkalmazását az 1. § (1) bekezdése szerinti szervezet – saját költségére – kezdeményezheti a nemzeti kiberbiztonsági incidenskezelő központnál, amely a rendelkezésére álló erőforrások függvényében és a veszélyeztetettség mértékének mérlegelésével dönt a prevenciós eszközök alkalmazásáról.

(3) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetet a nemzeti kiberbiztonsági incidenskezelő központ javaslata alapján a nemzeti kiberbiztonsági hatóság is kötelezheti prevenciós eszközök alkalmazására, valamint a nemzeti kiberbiztonsági incidenskezelő központ – kockázatelemzés alapján – saját maga is dönthet prevenciós eszközök alkalmazásáról az érintett szervezet előzetes tájékoztatását követően.

(4) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet a nemzeti kiberbiztonsági incidenskezelő központ megkeresése esetén köteles a prevenciós eszközök igénybevételére.

(5) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet a nemzeti kiberbiztonsági incidenskezelő központ megkeresése esetén köteles csatlakozni a nemzeti kiberbiztonsági incidenskezelő központ által működtetett, a fenyegetettségi információkat megosztó rendszerhez, valamint maga is kezdeményezheti az ezen rendszerhez történő csatlakozást. A nemzeti kiberbiztonsági incidenskezelő központ a veszélyeztetettség mértékének mérlegelésével és a rendelkezésére álló erőforrások figyelembevételével írja elő az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet csatlakozását vagy járul hozzá a csatlakozáshoz.

(6) A nemzeti kiberbiztonsági incidenskezelő központ jogosult valamennyi magyar felhasználású, geolokációjú internetes cím és rajta elhelyezett szolgáltatások vonatkozásában olyan kizárólag általános kiberbiztonsági célú információkat gyűjteni, amelyekből egyértelműen azonosíthat fenyegetéseket és kiberbiztonsági incidenseket.

(7) A (6) bekezdés szerinti tevékenység nem okozhat aránytalan sérelmet a szolgáltatás üzemeltetője számára és nem eredményezheti a szolgáltatás elérhetetlenségét.

(8) A sérülékenységvizsgálat során megállapított adatokat a nemzeti kiberbiztonsági incidenskezelő központ a kibertér állapotának értékelése céljából, kizárólag anonim módon hasznosíthatja és használhatja fel.

## 40. A kiberbiztonsági incidensek bejelentése és kezelése

**66. §** (1) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is – a nemzeti kiberbiztonsági incidenskezelő központ részére kötelesek haladéktalanul, a kormányrendeletben meghatározottak szerint bejelenteni.

(2) Az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is –, amelyek a szervezet működésében vagy az általa végzett szolgáltatásnyújtásban súlyos zavart vagy vagyoni hátrányt okoz, illetve jelentős vagyoni vagy nem vagyoni kárt okoz más természetes vagy jogi személyek számára kötelesek a kormányrendeletben

meghatározottak szerint bejelenteni a nemzeti kiberbiztonsági incidenskezelő központ részére.

(3) Az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek a (2) bekezdés szerinti kiberbiztonsági incidensnek nem minősülő kiberbiztonsági incidenseket is bejelenthetik a nemzeti kiberbiztonsági incidenskezelő központ részére.

(4) A honvédelmi célú elektronikus információs rendszert érintő fenyegetést, kiberbiztonsági incidensközeli helyzetet és kiberbiztonsági incidenst a szervezet a Kormány rendeletében meghatározott honvédelmi kiberbiztonsági incidenskezelő központnak jelenti be.

(5) A honvédelmi kiberbiztonsági incidenskezelő központ és az ágazaton belüli kiberbiztonsági incidenskezelő központ a tudomására jutott fenyegetések, kiberbiztonsági incidensközeli helyzetek és kiberbiztonsági incidensek adatait köteles haladéktalanul a nemzeti kiberbiztonsági incidenskezelő központ részére továbbítani.

(6) Ha a nemzeti kiberbiztonsági incidenskezelő központ, a honvédelmi kiberbiztonsági incidenskezelő központ, valamint az ágazaton belüli kiberbiztonsági incidenskezelő központ illetékességének hiányát észleli, a bejelentést haladéktalanul megküldi az illetékes kiberbiztonsági incidenskezelő központnak.

**67. §** (1) Azok a szervezetek vagy személyek, amelyek nem tartoznak az 1. § (10) bekezdésének hatálya alá, önkéntes alapon bejelenthetik a nemzeti kiberbiztonsági incidenskezelő központnak az olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket, illetve kiberbiztonsági incidenseket, amelyek jelentős hatást gyakorolnak vagy gyakorolhatnak a magyar kibertér biztonságára.

(2) A nemzeti kiberbiztonsági incidenskezelő központ az e törvény hatálya alá tartozó szervezetek bejelentését előnyben részesítheti az önkéntes bejelentésekkel szemben. A nemzeti kiberbiztonsági incidenskezelő központ az önkéntes bejelentéseket a rendelkezésére álló erőforrások függvényében kezeli és a veszélyeztetettség mértékének mérlegelésével jár el.

(3) Az önkéntes bejelentésekkel összefüggésben a nemzeti kiberbiztonsági incidenskezelő központ csak akkor köteles eljárni, ha az nem jelent aránytalan vagy indokolatlan terhet a nemzeti kiberbiztonsági incidenskezelő központ számára vagy az önkéntes bejelentés az e törvény hatály alá tartozó szervezet elektronikus információs rendszerét érinti.

(4) Az önkéntes bejelentés eredményeként a bejelentő számára nem írható elő olyan kötelezettség, amely ne vonatkozott volna rá a bejelentés megtétele nélkül is.

**68. §** (1) Ha az elektronikus információs rendszert olyan jelentős kiberbiztonsági incidens éri vagy annak közvetlen bekövetkezése fenyegeti, amely a rendszer felett rendelkezési jogosultsággal rendelkező szervezet vagy a felhasználó szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, a nemzeti kiberbiztonsági incidenskezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a rendszer felett rendelkezési jogosultsággal rendelkező szervezetet, hogy a jelentős kiberbiztonsági incidens megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg.

(2) Ha a szervezethez információbiztonsági felügyelő került kirendelésre, az (1) bekezdés szerinti körülmények felmerüléséről a nemzeti kiberbiztonsági incidenskezelő központot haladéktalanul tájékoztatja. Azonnali beavatkozást igénylő esetben a nemzeti kiberbiztonsági incidenskezelő központ – az információbiztonsági felügyelő útján – az információk sérülésének elkerüléséhez szükséges mértékben ideiglenes intézkedést alkalmazhat.

## 41. A kibertérből érkező támadás megszakításához szükséges intézkedések

**69. §** (1) A 64. § (2) bekezdés *d)* pontja szerinti, a kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtására a Kormány által kijelölt személy erre vonatkozó döntése alapján van lehetőség. A támadás megszakítását követően meg kell vizsgálni a védelem fokozásához szükséges további intézkedések lehetséges körét, illetve az ország védelmével összefüggő további döntések szükségességét.

(2) A 64. § (2) bekezdés *d)* pontja szerinti intézkedésnek

*a)* az okozott sérelemmel vagy közvetlen fenyegetéssel arányosnak és szükséges mértékűnek kell lennie, és törekedni kell arra, hogy a támadás megszakításán túli eredményre vagy sérelemre ne vezessen,

*b)* biztosítani kell az összhangot a nemzetbiztonsági, honvédelmi, bűnüldözési és külpolitikai érdekekkel és törekvésekkel.

(3) Külföldről érkező jelentős kibertámadás esetén a foganatosított intézkedésekről és azok okairól tájékoztatni kell a külpolitikáért felelős minisztert a további intézkedések megtétele céljából.

## 42. Kiberbiztonsági incidensek kezelése

**70. §** (1) Kiberbiztonsági incidens bekövetkezése esetén a szervezet intézkedik az érintett kiberbiztonsági incidens kezelése érdekében.

(2) A kiberbiztonsági hatóság kötelezheti a szervezetet arra, hogy az érintett kiberbiztonsági incidenst kezelje. Ha a hatósági kötelezésnek a szervezet nem tesz eleget, a kiberbiztonsági hatóság bírságot szabhat ki.

(3) Az érintett kiberbiztonsági incidens kezelését

*a)* megfelelő szaktudással rendelkező foglalkoztatott alkalmazása esetén a szervezet önmaga,

*b)* a szervezet által megbízott, telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges – az SZTFH elnökének rendeletében meghatározott – szakértelemmel és infrastrukturális feltételekkel rendelkező és az SZTFH által vezetett (4) bekezdés szerinti nyilvántartásban szereplő gazdálkodó szervezet,

*c)* az ágazaton belüli kiberbiztonsági incidenskezelő központ,

*d)* a nemzeti kiberbiztonsági incidenskezelő központ, vagy

*e)* honvédelmi kiberbiztonsági incidenskezelő központ

végzi.

(4) Az SZTFH nyilvántartást vezet a kiberbiztonsági incidens kezelésére jogosult gazdálkodó szervezetekről az SZTFH elnökének rendeletében foglalt részletes szabályok szerint.

(5) A (4) bekezdés szerinti nyilvántartás tartalmazza:

*a)* a gazdálkodó szervezet megnevezését és székhelyét, valamint annak kijelölt kapcsolattartója természetes személyazonosító adatait, telefonszámát, és elektronikus levelezési címét,

*b)* a gazdálkodó szervezet – nyilvántartásba vételekor kapott – azonosító számát,

*c)* az SZTFH elnökének rendeletében előírt további, személyes adatnak nem minősülő adatokat.

(6) A (4) bekezdés szerinti nyilvántartásba történő felvételi eljárás során az SZTFH a feladat ellátásához szükséges – az SZTFH elnökének rendeletében meghatározott – szakértelem és infrastrukturális feltételek teljesülésének megállapítása érdekében bevonja a nemzeti kiberbiztonsági incidenskezelő központot.

(7) Ha az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet a kiberbiztonsági incidens kezelését nem maga végzi, a (4) bekezdés szerinti nyilvántartásban szereplő gazdálkodó szervezetek közül választ. Ha a kiberbiztonsági incidens kezelése meghaladja a gazdálkodó szervezet kapacitásait, a szervezet megkeresheti az ágazaton belüli kiberbiztonsági incidenskezelő központot vagy a nemzeti kiberbiztonsági incidenskezelő központot az érintett kiberbiztonsági incidens kezelése érdekében.

(8) Ha az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet a kiberbiztonsági incidens kezelését nem maga végzi, a (4) bekezdés szerinti nyilvántartásban szereplő gazdálkodó szervezetek közül választ vagy megkeresi az ágazaton belüli kiberbiztonsági incidenskezelő központot vagy a nemzeti kiberbiztonsági incidenskezelő központot a kiberbiztonsági incidens kezelése érdekében.

(9) Az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet esetében a (3) bekezdés *b)* pontja szerinti gazdálkodó szervezet nevében és alkalmazásában kizárólag olyan személy végezheti az incidenskezelést, akinek a nemzetbiztonsági ellenőrzését elvégezték és a nemzetbiztonsági ellenőrzés során nemzetbiztonsági kockázatot nem állapítottak meg.

(10) A nemzeti kiberbiztonsági incidenskezelő központ az érintett kiberbiztonsági incidens kezelését a rendelkezésére álló erőforrások függvényében, a veszélyeztetettség mértékének mérlegelésével látja el.

(11) Az érintett kiberbiztonsági incidens kezelését a nemzeti kiberbiztonsági incidenskezelő központ végzi el, ha a Kszetv. szerinti kritikus szervezet elektronikus információs rendszere, vagy a Vbö. alapján kijelölt, az ország védelme és biztonsága szempontjából jelentős szervezetek tekintetében nincs a kiberbiztonsági incidenskezelés elvégzésére a jogszabályban meghatározott feltételeknek megfelelő gazdálkodó szervezet vagy nem rendelkezik elegendő kapacitással.

(12) A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában a kiberbiztonsági incidens kezelését kizárólag a nemzeti kiberbiztonsági incidenskezelő központ olyan munkatársa végezheti, akinek a nemzetbiztonsági ellenőrzését elvégezték és a nemzetbiztonsági ellenőrzés során nemzetbiztonsági kockázatot nem állapítottak meg.

(13) A nemzeti kiberbiztonsági incidenskezelő központ a tudomására jutott kiberbiztonsági incidensekről tájékoztathatja a 73. § (3) bekezdés szerinti Operatív Törzs vezetőjét, ha a kiberbiztonsági incidens az Operatív Törzs más tagja által képviselt szervezetet is érinti.

(14) Az érintett kiberbiztonsági incidensek kezelésére vonatkozó részletszabályokat kormányrendelet állapítja meg.

(15) Jelen § rendelkezéseit a kiberbiztonsági incidensközeli helyzetek kezelése vonatkozásában is alkalmazni kell.

### 43. Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek kiberbiztonsági incidenseinek kezelésére irányadó rendelkezések

**71. §** (1) Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek kiberbiztonsági incidenseinek kezelése során a 63–64. §, a 67. §, a 68. § (1) bekezdése, a 69. §, valamint a 70. § (10), (13) és (14) bekezdése szerinti rendelkezések alkalmazandóak.

(2) Ha a kiberbiztonsági incidens kezelése meghaladja a (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezet vagy az általa igénybe vett közreműködő kapacitásait, a szervezet megkeresheti az ágazaton belüli kiberbiztonsági incidenskezelő központot vagy a nemzeti kiberbiztonsági incidenskezelő központot a kiberbiztonsági incidens kezelése érdekében.

## *VIII. FEJEZET*

## *A KIBERBIZTONSÁGGAL KAPCSOLATOS FELADATOK KOORDINÁCIÓJÁNAK SZERVEZETRENDSZERE*

### 44. A kiberbiztonságért felelős biztos

**72. §** (1) A kiberbiztonságért felelős biztost az informatikáért felelős miniszter jelöli ki.

(2) A kiberbiztonságért felelős biztos felel az Európai Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelv szerinti

*a)* nemzeti kiberbiztonsági stratégia, valamint

*b)* nemzeti válságkezelési terv

összeállításáért és az érintett szervezetekkel való koordinációjáért.

(3) A kiberbiztonságért felelős biztos vezeti a Nemzeti Kiberbiztonsági Munkacsoportot.

### 45. A Nemzeti Kiberbiztonsági Munkacsoport

**73. §** (1) A Kormány kiberbiztonsági kérdésekben javaslattevő, véleményező szerve a Nemzeti Kiberbiztonsági Munkacsoport.

(2) A Nemzeti Kiberbiztonsági Munkacsoport gondoskodik az e törvényben és végrehajtási rendeleteiben meghatározott tevékenységek összehangolásáról.

(3) A Nemzeti Kiberbiztonsági Munkacsoport tevékenységét Operatív Törzs, valamint a kiberbiztonsági almunkacsoportok és a nem kormányzati szereplőkkel való együttműködés kereteit biztosító Nemzeti Kiberbiztonsági Fórum támogatja.

(4) Az Operatív Törzs tevékenységét a kiberbiztonságért felelős biztos irányítja. Az Operatív Törzs – a védelmi és biztonsági igazgatás központi szerve bevonásával – minősíti a jelentős vagy nagyszabású kiberbiztonsági incidens miatt bekövetkezett védelmi és biztonsági eseményt, valamint kezdeményezi a válságkezelési vagy veszélyhelyzet-kezelési intézkedések megtételét.

(5) A Nemzeti Kiberbiztonsági Munkacsoport és annak működését támogató testületek létrehozásával, működtetésével kapcsolatos szabályokat, feladat- és hatásköröket kormányrendelet szabályozza.

## 46. A kiberbiztonsági válsághelyzet-kezelés szervezetrendszere

**74. §** (1) Jelentős vagy nagyszabású kiberbiztonsági incidens esetén a nemzeti kiberbiztonsági incidenskezelő központ kezdeményezése alapján a Nemzeti Kiberbiztonsági Munkacsoport Operatív Törzse javaslatot tehet a kiberbiztonsági incidens kiberbiztonsági válsághelyzetté történő minősítésére.

(2) A kiberbiztonsági válsághelyzet olyan védelmi és biztonsági esemény, amely esetén a Kormány az informatikáért felelős miniszter előterjesztése alapján összehangolt védelmi tevékenységet rendelhet el.

(3) Kiberbiztonsági válsághelyzet esetén – ha e törvény vagy a végrehajtására kiadott kormányrendelet eltérően nem rendelkezik – a Vbö. rendelkezéseit kell alkalmazni.

(4) Kiberbiztonsági válsághelyzet és az az alapján elrendelt összehangolt védelmi tevékenység esetén a Kormány intézkedésként bevezetheti

1. a kiberbiztonsági válsághelyzet-kezelésben érintett szerv vagy szervezet készenlétének fokozását, prevenciós tevékenységét;

2. az 1. pont szerinti szervek vagy szervezetek műveleti vagy élőerős védelmét, valamint annak fokozását;

3. a honvédelmi szervezetek, a rendvédelmi szervek és a nemzetbiztonsági szolgálatok felderítő, elhárító, valamint kibertér műveleti erői tevékenységének fokozását a fenyegetettség Magyarországra történő átterjedésének, illetve a támadás elhárításának, valamint következményeinek megakadályozása érdekében;

4. a 3. pont szerinti szervek vagy szervezetek összehangolt védelmi tevékenység keretében végzett összehangolt vagy együttes fellépését;

5. a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatás, valamint az azt egyedül biztosító alapvető vagy fontos szervezetként még be nem azonosított szolgáltató haladéktalan azonosításának elrendelését;

6. elektronikus hírközlési szolgáltatások szüneteltetését, korlátozását és ellenőrzését, azokhoz való hozzáférés lehetetlenné tételét, továbbá az elektronikus informatikai hálózatok és eszközök, valamint az elektronikus hírközlő berendezések térítésmentes igénybevételét, használatra való átengedését, használatának mellőzését, valamint hozzáférhetetlenné tételét;

7. a kiberbiztonsági válsághelyzet-kezeléséhez szükséges szolgáltató működési helyiségeinek, technikai eszközparkjának, elektronikus információs rendszerének és létesítményeinek térítésmentes igénybevételét, használatra való átengedését;

8. az állami, valamint a kiberbiztonsági válsághelyzet-kezelésben érintett szerv vagy szervezet információs és kommunikációs rendszerei folyamatos üzemeltetésének biztosítása érdekében a javítókapacitások és alkatrészkészletek térítésmentes igénybevételét, vagy használatuk korlátozását,

valamint a javítókapacitásokkal rendelkező társaságok tulajdonosait és munkavállalóit terhelő javítási, üzemeltetési szolgáltatások teljesítését;

9. a kiberbiztonság szavatolása szempontjából fontos termékek, eszközök készletezését, tartalékolását;

10. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (a továbbiakban: EU-CyCLONE), valamint az Európai Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) kötelező tájékoztatását és dönt annak tartalmáról,

11. a kötelező hivatalos kormányzati tájékoztatás nyújtását az érintettek részére, valamint

12. az Európai Unió tagállamainak, valamint az Észak-atlanti Szerződés Szervezetén belüli szövetséges országok tájékoztatását a kiberbiztonsági válsághelyzet kapcsán a Kormány által megtett intézkedésekről a diplomáciai csatornák igénybevételével.

(5) A (4) bekezdés 10–12. pontja szerinti tájékoztatás nyújtása során a minősített adatok védelmére vonatkozó uniós és nemzeti szabályokban és az általános adatvédelmi jogszabályokban foglalt rendelkezésekre tekintettel kell eljárni.

(6) A kiberbiztonsági válsághelyzet ideje alatt a kiberbiztonsági válsághelyzet megelőzése, megismerése, felderítése és továbbterjedésének megakadályozása, valamint az állami szervek összehangolt feladatellátásának megszervezése céljából az Operatív Törzs – a kiberbiztonsági válsághelyzettel összefüggően –

*a)* adatszolgáltatást kérhet bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől, amely ezen adatszolgáltatásnak köteles haladéktalanul, térítésmentesen eleget tenni,

*b)* kezeli a kiberbiztonsági incidens kezelése során megismert személyes adatokat.

(7) Az Operatív Törzs a (6) bekezdés alapján kezelt adatokat a nemzetbiztonsági tevékenységre vonatkozó információk kivételével köteles átadni a nemzeti eseménykezelő központnak.

(8) Az Operatív Törzs a (6) bekezdés alapján kezelt adatokat – a kiberbiztonsági válsághelyzetre okot adó körülmények vizsgálata céljából – a nemzeti kiberbiztonsági incidenskezelő központnak átadhatja.

(9) Az Operatív Törzs vezetője a kiberbiztonsági válsághelyzeten a kiberbiztonsági válsághelyzetet kiváltó esemény kezelése érdekében jogosult

*a)* az Operatív Törzs tagjának az általa képviselt szervezet vonatkozásában azonnali intézkedéstételi kötelezettséget előírni,

*b)* dönteni a nemzeti kiberbiztonsági incidenskezelő központnak vagy a honvédelmi incidenskezelő központnak a kiberbiztonsági incidens kezelésébe történő bevonásáról.

(10) Az 1. § (10) bekezdése hatálya alá tartozó szervezet – az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezet kivételével – a kiberbiztonsági válsághelyzetre való felkészülés és annak kezelése érdekében kiberbiztonsági tervet készít, amelyben felméri a kibertérből érkező lehetséges kockázatokat és ezek alapján kidolgozza a működési területén foganatosítandó válságkezelési eljárási elemeket.

(11) A kiberbiztonsági válsághelyzettel érintett szervezet – a (12) bekezdésben foglalt kivétellel – a nemzeti kiberbiztonsági incidenskezelő központ, valamint a védelmi és biztonsági igazgatás központi szervének kérésére köteles a (10) bekezdésben meghatározott tervvel, valamint a kiberbiztonsági válsághelyzet kezelése érdekében bevezetett intézkedésekkel kapcsolatos adatokat, információkat összegyűjteni, és elektronikus formában átadni vagy egyéb módon hozzáférhetővé tenni.

(12) A honvédelmi célú elektronikus információs rendszerek tekintetében a (11) bekezdésben meghatározott adatokat a honvédelmi kiberbiztonsági incidenskezelő központ, valamint a védelmi és biztonsági igazgatás központi szerve számára kell – kérésük esetén – hozzáférhetővé tenni.

(13) A kiberbiztonsági válsághelyzetkezelésben részt vevő szervek vagy szervezetek kijelölését, feladat- és hatáskörét, a követendő eljárásrendet, az EU-CyCLONE-ban Magyarország képviseletét ellátó szerveket a Kormány rendeletben határozza meg.

## 47. A nemzeti koordinációs központ

**75. §** Az (EU) 2021/887 európai parlamenti és tanácsi rendelet szerinti, a kiberbiztonsági kompetenciaközösség számára kapcsolattartási pontként szolgáló nemzeti koordinációs központ feladatait a Kormány rendeletében kijelölt szerv az abban foglaltak szerint látja el.

## 48. Együttműködés és jelentéstétel

**76. §** (1) A kiberbiztonsági hatóságok, a tanúsító hatóság, a poszt-kvantumtitkosítást felügyelő hatóság, a Kszetv. szerinti kijelölő hatóság, a Vbö. szerinti kijelölő hatóság, az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság, a sérülékenységvizsgálat végzésére jogosult állami szerv, a kiberbiztonsági incidenskezelő központok, a nemzeti koordinációs központ, valamint az egyedüli kapcsolattartó pont kölcsönösen együttműködnek és tájékoztatják egymást az elektronikus információbiztonságot érintő megállapításaikról.

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

(3) Az (1) bekezdés szerinti szervezetek közötti együttműködés, az EU-CyCLONe-nal, a CSIRT-hálózattal, más európai uniós tagállamok és harmadik országok CSIRT-jeivel, hatóságaival, egyedüli kapcsolattartó pontjaival való együttműködés, valamint az Európai Bizottság és az ENISA részére történő tájékoztatás és adatszolgáltatás rendjére vonatkozó részletes szabályokat a Kormány rendeletben határozza meg.

# *IX. FEJEZET*

# *ADATKEZELÉSI ÉS ADATVÉDELMI RENDELKEZÉSEK*

**77. §** (1) A kiberbiztonsági hatóság, a sérülékenységvizsgálat végzésére jogosult szerv vagy gazdálkodó szervezet, a kiberbiztonsági incidenskezelő központ, az egyedüli kapcsolattartó pont, valamint nemzeti koordinációs központ az e törvényben meghatározott elektronikus információs rendszerek védelmével összefüggő feladatai ellátása során megismert minősített adatot, személyes adatot vagy védett adatot, üzleti titkot, banktitkot, fizetési titkot, biztosítási titkot, értékpapírtitkot, pénztártitkot, orvosi titkot és más hivatás gyakorlásához kötött titkot, illetve a feladatellátás során megismert egyéb adatot kizárólag a jogszabályban meghatározott feladatai ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével, az adatkezelésre vonatkozó jogszabályokban foglaltakkal összhangban jogosult kezelni.

(2) Az (1) bekezdés szerinti szervek a feladatellátás befejezését követően a feladatellátáshoz kapcsolódóan rögzített adatokat – a (3)–(6) bekezdésben meghatározott kivétellel – kötelesek az elektronikus információs rendszereikből és adathordozóikról törölni.

(3) A (1) bekezdés szerinti szerv az (1) bekezdésben meghatározott adatokat a hatósági döntés véglegessé válását, a sérülékenységvizsgálat lezárását, valamint a kiberbiztonsági incidens vagy kiberbiztonsági válsághelyzet vizsgálatának lefolytatását követő öt évig jogosult kezelni, és az öt év elteltével köteles az elektronikus információs rendszereiből és adathordozóiról törölni.

(4) Ha a szervezet e törvény hatálya alá tartozó tevékenységet már nem végez, akkor a kiberbiztonsági hatóság a szervezet vonatkozásában nyilvántartott adatokat a tevékenység befejezése bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(5) Ha az adatok változását a szervezet bejelenti, akkor az eredeti adatokat a kiberbiztonsági hatóság az adat változásának bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(6) A kiberbiztonsági incidenskezelő központ a prevenciós eszközök, szolgáltatások alkalmazása során keletkezett adatokat, továbbá a kiberbiztonsági incidenskezelő központ és az egyedüli

kapcsolattartó pont a hozzá érkezett bejelentések adatait az adatok keletkezésétől, illetve a bejelentés beérkezésétől számított öt évig jogosult kezelni és megőrzi; ezt követően köteles az elektronikus információs rendszereiből és adathordozóiról törölni.

**78. §** (1) A kiberbiztonsági hatóság, a sérülékenységvizsgálat végzésére jogosult szerv vagy gazdálkodó szervezet, valamint a kiberbiztonsági incidenskezelő központ munkatársait a megismert adatok tekintetében írásba foglalt titoktartási kötelezettség terheli, amely

*a)* a foglalkoztatásra irányuló jogviszony megszűnését követő öt évig,

*b)* minősített adatok tekintetében azok érvényességi idejének végéig,

*c)* személyes adatok tekintetében pedig időkorlát nélkül

áll fenn.

(2) A kiberbiztonsági hatóság, a sérülékenységvizsgálat végzésére jogosult szerv vagy gazdálkodó szervezet, valamint a kiberbiztonsági incidenskezelő központ eljárása során keletkezett adatok – a 79. §-ban foglaltak kivételével – nem nyilvánosak.

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

**79. §** (1) A sérülékenységvizsgálat végzésére jogosult állami szerv jogosult a sérülékenységvizsgálatok eredményéről anonimizált, a rendszerek sérülékenységére utalást nem tartalmazó statisztikákat közzétenni.

(2) A nemzeti kiberbiztonsági incidenskezelő központ jogosult a feladatellátása során keletkező adatokról, információkról, trendekről, levont következtetésekről statisztikákat, incidensek technikai leírásait anonimizált módon közzétenni.

**80. §** (1) A 77. § (1) bekezdése szerinti szervek tájékoztatási, adatszolgáltatási kötelezettségük teljesítése során a minősített adatok védelmére vonatkozó és az általános adatvédelmi jogszabályokban foglalt rendelkezésekre figyelemmel járnak el. A tájékoztatás és az adatszolgáltatás nem vonatkozhat olyan információk szolgáltatására, amelyek közzététele ellentétes lenne Magyarország nemzetbiztonsági, közbiztonsági vagy alapvető védelmi érdekeivel.

(2) Bizalmas információkat – beleértve az üzleti titoktartási szabályokat – kizárólag akkor lehet megosztani az Európai Bizottsággal és más érintett hatóságokkal, ha az információcsere az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alkalmazásához szükséges. A megosztott információnak az információcsere célja szempontjából lényeges és arányos mértékre kell korlátozódnia. Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell a szervezetek biztonsági és kereskedelmi érdekeit.

# *X. FEJEZET*

# *ZÁRÓ RENDELKEZÉSEK*

## 49. Felhatalmazó rendelkezések

**81. §** (1) Felhatalmazást kap a Kormány, hogy rendeletben kijelölje

*a)* a kiberbiztonsági szolgáltatások nyújtására jogosult szervet,

*b)* a nemzeti kiberbiztonsági hatóságot,[2]

*c)* a honvédelmi célú elektronikus információs rendszerek tekintetében a kiberbiztonsági felügyeletet ellátó hatóságot,[3]

[2] Lásd: 418/2024. (XII. 23.) Korm. rendelet.

[3] Lásd: 418/2024. (XII. 23.) Korm. rendelet.

*d)* a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóságot,[4]

*e)* a sérülékenységvizsgálat végzésére jogosult állami szervet,[5]

*f)* a nemzeti kiberbiztonsági incidenskezelő központ működtetését végző szervet,[6]

*g)* a honvédelmi kiberbiztonsági incidenskezelő központ működtetését végző szervet,[7]

*h)* a kiberbiztonsági válsághelyzet kezelésében részt vevő szerveket és szervezeteket, az EU-CyCLONE-ban Magyarország képviseletét ellátó szerveket, valamint[8]

*i)* a nemzeti koordinációs központot.[9]

(2) Felhatalmazást kap a Kormány, hogy rendeletben megállapítsa

1. a kiberbiztonsági szolgáltatások részletes szabályait, a kiberbiztonsági szolgáltatások körét, az igénybevételére kötelezett, illetve jogosult szervezeteket, valamint a szolgáltatások igénybevételének rendjét,

2. az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek kötelezettségeire vonatkozó részletes rendelkezéseket;[10]

3. az elektronikus információs rendszerekben kezelt adatok osztályozására vonatkozó részletes szabályokat;[11]

4. a 11. § (1) bekezdése szerinti megállapodás minimális tartalmi elemeit;[12]

5. az elektronikus információs rendszer biztonságáért felelős személy részletes feladat- és hatáskörét, az elektronikus információs rendszer biztonságáért felelős személyek nyilvántartásába kerülés, illetve az onnan való törlés rendjét;[13]

6. az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezet elektronikus információs rendszerei fejlesztése során alkalmazandó részletes szabályokat;[14]

7. a központi szolgáltató által az állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújtott informatikai és elektronikus hírközlési szolgáltatási feladatokra vonatkozó részletes szabályokat;

8. a nemzeti kiberbiztonsági hatóság, valamint a honvédelmi célú elektronikus információs rendszerek tekintetében a kiberbiztonsági felügyeletet ellátó hatóság feladat- és hatáskörét, valamint az eljárására és a nyilvántartásra vonatkozó részletes szabályokat;[15]

9. az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek esetében az információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat;[16]

10. a kiberbiztonsági hatóság által kiszabható bírság mértékét, megállapításának szempontrendszerét, valamint a bírság megfizetése módjának részletes eljárási szabályait;[17]

11. a tanúsító hatóság által kiszabható bírság mértékét, megállapításának szempontrendszerét, valamint a bírság megfizetése módjának részletes eljárási szabályait;[18]

12. a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság feladatának, a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak, a hatósági ellenőrzésnek, a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartalmát, valamint a megfelelőségi jelölés elhelyezésére vonatkozó szabályokat;

---

[4] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[5] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[6] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[7] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[8] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[9] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[10] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[11] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[12] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[13] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[14] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[15] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[16] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[17] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[18] Lásd: 418/2024. (XII. 23.) Korm. rendelet.

13. a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségi önértékelésre, a tanúsítási eljárásra, a megfelelőségértékelő szervezetekkel szemben támasztott követelményekre, valamint a megfelelőségértékelő szervezetek kötelezettségeire és tevékenységére vonatkozó részletes szabályokat;

14. a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a nemzeti kiberbiztonsági tanúsítási rendszerekre figyelemmel a tanúsítási rendszereket;

15. a sérülékenységvizsgálat végrehajtására vonatkozó részletszabályokat, az egyes sérülékenységvizsgálati módszereket, az állásfoglalás tartalmi elemeit;[19]

16. a nemzeti kiberbiztonsági incidenskezelő központ, valamint a honvédelmi kiberbiztonsági incidenskezelő központ feladat- és hatáskörét, feladatai ellátásának részletes szabályait;[20]

17. az ágazaton belüli kiberbiztonsági incidenskezelő központ létrehozatalára vonatkozó részletes szabályokat;[21]

18. a sebezhetőségek, sérülékenységek felderítésének, bejelentésének részletes szabályait, a nemzeti kiberbiztonsági incidenskezelő központ által a bejelentett sebezhetőség, sérülékenységgel összefüggő koordinációs és egyéb feladatait;[22]

19. a korai figyelmeztetés részletes szabályait, annak rendszerét, a rendszer üzemeltetőjének kijelölésére vonatkozó előírásokat, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét;

20. a honvédelmi célú elektronikus információs rendszerekre vonatkozó korai figyelmeztetés részletes szabályait, annak rendszerét, a rendszer üzemeltetőjének kijelölésére vonatkozó előírásokat, valamint a kapcsolódó korai figyelmeztető szolgáltatás igénybevételének rendjét;

21. a fenyegetések, kiberbiztonsági incidensközeli helyzetek és kiberbiztonsági incidensek bejelentésének rendjét, a kiberbiztonsági incidensek és kiberbiztonsági incidensközeli helyzetek kezelésére és vizsgálatára vonatkozó részletszabályokat;[23]

22. a hazai kiberbiztonsági gyakorlatok megtartásának részletszabályait;[24]

23. a kiberbiztonsági válsághelyzet kezelésében érintett szervek és szervezetek feladat- és hatáskörét, a követendő eljárásrendet;[25]

24. a Nemzeti Kiberbiztonsági Munkacsoport és annak működését támogató testületek létrehozásával, működtetésével kapcsolatos szabályokat, feladat- és hatásköröket, valamint[26]

25. a 76. § (1) bekezdése szerinti szervek közötti és a 76. § (3) bekezdése szerinti szervezetekkel való együttműködés, valamint az Európai Bizottság és az ENISA részére történő tájékoztatás és adatszolgáltatás rendjére vonatkozó részletes szabályokat,[27]

(3) Felhatalmazást kap az informatikáért felelős miniszter, hogy rendeletben meghatározza

*a)* a biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket,

*b)* a szervezet vezetőjének, munkatársainak, valamint az elektronikus információs rendszer biztonságáért felelős személynek a szakmai képzésére és továbbképzésére vonatkozó rendelkezéseket,

*c)* a – 11. § (3) bekezdés *b)* pontjában megjelölt szervezetek vonatkozásában az elektronikus információs rendszer biztonságáért felelős személy, valamint – az 1. § (1) bekezdés *a)–c)* pontja szerinti szervezetek vonatkozásában – az információbiztonsági felügyelő feladatellátásához szükséges végzettséget, szakképzettséget, képzettséget vagy szakmai tapasztalatot,

*d)* a kötelezően alkalmazandó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján

[19] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[20] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[21] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[22] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[23] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[24] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[25] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[26] Lásd: 418/2024. (XII. 23.) Korm. rendelet.
[27] Lásd: 418/2024. (XII. 23.) Korm. rendelet.

tanúsított IKT-termékeket, IKT-szolgáltatásokat vagy IKT-folyamatokat, valamint az ezek alkalmazására kötelezett, 1. § (1) bekezdés *a)–c)* pontja szerinti szervezeteket.

(4) Az informatikáért felelős miniszter a (3) bekezdés *a)* pontja szerinti rendeletet az SZTFH elnöke véleményének kikérését követően adja ki.

(5) Felhatalmazást kap a honvédelemért felelős miniszter, hogy rendeletben meghatározza az adópolitikáért felelős miniszterrel egyetértésben a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság eljárásáért fizetendő igazgatási szolgáltatási díj mértékét, a díjak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat.

(6) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza

*a)* a kiberbiztonsági felügyeleti díj mértékét, megfizetésére vonatkozó rendelkezéseket,

*b)* az auditorok nyilvántartásba vételi eljárásának rendjét, és az auditorral szemben támasztott követelményeket,

*c)* a kiberbiztonsági audit lefolytatásának rendjét, valamint a kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját,

*d)* az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek vonatkozásában a kiberbiztonsági felügyelet és feladatellátás, továbbá a hatósági ellenőrzés lefolytatásának részletes szabályait,

*e)* az 1. § (1) bekezdés *b), d)* és *e)* pontja szerinti szervezeteknek a 29. § (1) bekezdés *a)* pontja szerinti kiberbiztonsági felügyeleti hatósági nyilvántartásba vételének rendjét, valamint a nyilvántartás személyes adatnak nem minősülő adattartalmára vonatkozó részletes szabályokat,

*f)* az 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezetek esetében az információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat,

*g)* a poszt-kvantumtitkosítás alkalmazására kötelezett szervezeteket,

*h)* a poszt-kvantumtitkosítás alkalmazást nyújtó szervezet nyilvántartásba vételére, a nyilvántartás személyes adatot nem tartalmazó adattartalmára, valamint a poszt-kvantumtitkosítás alkalmazást nyújtó szervezet ellenőrzésére vonatkozó részletes szabályokat,

*i)* a poszt-kvantumtitkosítás alkalmazást nyújtó szervezet informatikai rendszerelemei zártsága tanúsítására vonatkozó részletes szabályokat,

*j)* a tanúsító szervezet nyilvántartásba vételére, a nyilvántartás személyes adatot nem tartalmazó adattartalmára, valamint a tanúsító szervezet ellenőrzésére vonatkozó részletes szabályokat,

*k)* a 45. § (1) bekezdés *b)* pontja szerinti tanúsító hatósági tevékenység kivételével a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak, a hatósági ellenőrzésnek, a nyilvántartás vezetésének részletes szabályait és a nyilvántartás személyes adatot nem tartalmazó adattartalmát, valamint a megfelelőségi jelölés elhelyezésére vonatkozó szabályokat,

*l)* a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a megfelelőségi önértékelésre, a tanúsítási eljárásra, a megfelelőségértékelő szervezetekkel szemben támasztott követelményekre, valamint a megfelelőségértékelő szervezetek kötelezettségeire és azok tevékenységére vonatkozó részletes szabályokat,

*m)* a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket,

*n)* a kötelezően alkalmazandó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termékeket, IKT-szolgáltatásokat vagy IKT-folyamatokat, valamint az ezek alkalmazására kötelezett, 1. § (1) bekezdés *d)* és *e)* pontja szerinti szervezeteket.

(7) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza

*a)* a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és személyek nyilvántartásba vételének részletes szabályait, a tevékenység végzéséhez szükséges infrastrukturális feltételeket és szakértelmet, valamint

*b)* a kiberbiztonsági incidensek kezelésére jogosult gazdálkodó szervezetek nyilvántartásba vételének részletes szabályait, a nyilvántartás személyes adatot nem tartalmazó adattartalmát, valamint a tevékenység végzéséhez szükséges infrastrukturális feltételeket és szakértelmet.

(8) Az SZTFH elnöke a (7) bekezdés szerinti rendeletet az informatikáért felelős miniszter

véleményének kikérését követően adja ki.

## 50. Hatályba léptető rendelkezések

**82. §** (1) Ez a törvény – a (2) bekezdésben foglalt kivétellel – 2025. január 1-jén lép hatályba.
(2) A 120. § (1) bekezdése 2025. január 2-án lép hatályba.

## 51. Átmeneti rendelkezések

**83. §** (1) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerinti nyilvántartásban 2024. december 31. napján szereplő – 8. § (4) bekezdés szerinti adatok körébe tartozó – adatokat nem kell ismételten bejelenteni, azokat a nemzeti kiberbiztonsági hatóság a 28. § (1) bekezdése szerinti nyilvántartás részeként kezeli.
(2) A 8. § (4) bekezdés szerinti adatszolgáltatási kötelezettséget az 1. § (1) bekezdés *a)* és *b)* pontja szerinti szervezet a 8. § (4) bekezdés szerinti határidőn belül teljesíti a nemzeti kiberbiztonsági hatóság részére, ha
*a)* e törvény hatálybalépését megelőzően az Ibtv. hatálya alá tartozott és még nem teljesítette a 8. § (4) bekezdés szerinti kötelezettséget, valamint
*b)* e törvény hatálybalépését megelőzően nem tartozott az Ibtv. hatálya alá.
(3) Ha az 1. § (1) bekezdés *a)* és *b)* pontja szerinti szervezet az elektronikus információs rendszer biztonságáért felelős személy adatait az Ibtv. alapján már bejelentette a nemzeti kiberbiztonsági hatóság részére, úgy annak ismételt bejelentésére nem köteles.
(4) Ha az 1. § (1) bekezdés *a)* és *b)* pontja szerinti szervezetnek az elektronikus információs rendszer biztonságáért felelős személye a törvény hatálybalépésekor nem felel meg a 11. § (4) bekezdése szerinti követelményeknek, az összeférhetetlenségi ok megszüntetésére 2 év áll rendelkezésére.
(5) Ha az 1. § (1) bekezdés *a)* és *b)* pontja szerinti szervezetnek a már működő elektronikus információs rendszerei első alkalommal történő biztonsági osztályba sorolását az Ibtv. alapján e törvény hatálybalépéséig már el kellett volna végeznie, úgy az első alkalommal történő biztonsági osztályba sorolást e törvény hatálybalépését követő 120 napon belül – a 6. § szerinti kockázatmenedzsment keretrendszer létrehozatalával együttesen – kell elvégeznie.
(6) Ha az 1. § (1) bekezdés *a)* és *b)* pontja szerinti szervezet elektronikus információs rendszerei biztonsági osztályba sorolásáról a kiberbiztonsági hatóság e törvény hatálybalépését megelőzően, az Ibtv. alapján hatósági döntést hozott, úgy a biztonsági osztályba sorolás felülvizsgálatát az e törvényben foglaltak szerint, a biztonsági osztályba sorolásról hozott hatósági döntés véglegessé válását követő két éven belül kell elvégezni. Ha ez alapján a felülvizsgálat esedékessége e törvény hatálybalépéséig már eltelt vagy e törvény hatálybalépésétől számított 180 napon belül van, a biztonsági osztályba sorolás felülvizsgálatára vonatkozó határidő meghosszabbodik olyan módon, hogy a rendelkezésre álló idő 180 nap legyen.
**84. §** Az Ibtv. szerinti 1. és 2. biztonsági osztály az „alap”, a 3. és 4. biztonsági osztály a „jelentős”, az 5. biztonsági osztály a „magas” biztonsági osztálynak felel meg.
**85. §** (1) Ha az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet e törvény hatálybalépését megelőzően az Ibtv. hatálya alá tartozott, és már teljesítette az elektronikus információs rendszerei biztonsági osztályához ott előírt követelményeket, az informatikáért felelős miniszter rendeletében előírt új védelmi intézkedések kivitelezésére e törvény hatálybalépésétől számított 1 év áll rendelkezésére.
(2) Ha az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet e törvény hatálybalépését megelőzően az Ibtv. hatálya alá tartozott, és még nem kellett teljesítenie az elektronikus információs rendszerei biztonsági osztályához ott előírt követelményeket, az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések bevezetésénél

alkalmazhatja a 10. § (6) bekezdése szerinti fokozatos kivitelezés lehetőségét. A fokozatosságot figyelembe vevő határidő számítás alapját a 84. § szerint meghatározott biztonsági osztály képezi, amelyhez tartozó követelményeket már teljesíteni kellett. A védelmi intézkedések kivitelezésére rendelkezésre álló idő nem lehet kevesebb, mint 1 év.

**86. §** (1) Az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet esetében e törvény új rendszer fejlesztésére vonatkozó előírásait kell alkalmazni az e törvény hatálybalépésekor még használatba nem vett,

*a)* saját fejlesztésű fejlesztés alatt álló rendszer esetében, amennyiben az erőforrásigényeket még nem fogadták el,

*b)* külső fejlesztés alatt álló rendszer esetében, amennyiben a fejlesztésre irányuló beszerzési eljárást még nem írták ki, vagy a fejlesztésre irányuló szerződést még nem kötötték meg.

(2) Ha az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet fejlesztett rendszere e törvény hatályba lépésekor túljutott az elektronikus információs rendszer fejlesztésének (1) bekezdésben meghatározott lépésein,

*a)* a szervezet – ha még nem végezte el, – 180 napon belül elvégzi az elektronikus információs rendszer biztonsági osztályba sorolását,

*b)* az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések teljesítésénél lehetősége van a 10. § (6) bekezdése szerinti fokozatos kivitelezésre, azzal, hogy a vonatkozó határidő számításának alapját e törvény hatálybalépésének napja képezi.

**87. §** Ha az 1. § (1) bekezdés *a)* pontja szerinti szervezet, valamint a 2. és 3. melléklet szerinti szervezetnek nem minősülő, 1. § (1) bekezdés *b)* pontja hatálya alá tartozó szervezet e törvény hatálybalépését megelőzően az Ibtv. hatálya alá tartozott, az elektronikus információbiztonsági követelményeknek való megfelelés ellenőrzése során az e törvényben meghatározott határidők elteltéig a kiberbiztonsági hatóság az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló rendeletben foglaltaknak való megfelelést vizsgálja, kivéve, ha a szervezet az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések teljesítéséről nyilatkozott.

**88. §** (1) Az Ibtv. rendelkezései alapján folyamatban lévő hatósági ügyeket a kiberbiztonsági hatóság az Ibtv. szerint zárja le.

(2) A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján kijelölt létfontosságú rendszerelem üzemeltetője a Kszetv.-ben, illetve a Vbö.-ben meghatározott kijelölési eljárásban hozott döntés véglegessé válásáig e törvény alkalmazásában kritikus szervezetnek minősül.

**89. §** (1) Az az 1. § (1) bekezdés *b), d)* vagy *e)* pontja szerinti szervezet, amely 2024. december 31. napján az SZTFH által a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 26. § (1) bekezdése szerint vezetett nyilvántartásban érintett szervezetként szerepel, nem köteles a 8. § (5) bekezdése szerinti bejelentés megtételére, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 26. § (1) bekezdése szerinti nyilvántartásban szereplő adatait az SZTFH a 29. § (1) bekezdés *a)* pontja szerinti nyilvántartás részeként kezeli. A 29. § (1) bekezdés *a)* pont *ae)* alpontja szerinti adatokat 2025. február 15. napjáig kell bejelenteni az SZTFH részére.

(2) Az az 1. § (1) bekezdés *b), d)* és *e)* pontja szerinti szervezet, amely 2025. január 1-je előtt megkezdte működését, a 16. § (1) bekezdése szerinti első kiberbiztonsági auditot 2025. december 31-ig köteles elvégeztetni.

(3) Az a gazdálkodó szervezet, amely a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 26. § (1) bekezdése szerint vezetett nyilvántartásban érintett szervezetként szerepel, és 2024. december 31. napjáig a kiberbiztonsági tanúsításról és a

kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 20. § (1) bekezdése szerint az elektronikus információs rendszereinek, valamint az azon tárolt, továbbított vagy feldolgozott adatoknak a biztonsági osztályba sorolását elvégezte, nem köteles a 10. § (1) bekezdése alapján ismételten elvégezni a biztonsági osztályba sorolást.

(4) Az a gazdálkodó szervezet, amely 2024. december 31. napján a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 23. § (6) bekezdése szerinti nyilvántartásban auditorként szerepel, nem köteles ismételten kérni nyilvántartásba vételét, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 23. § (6) bekezdése szerinti nyilvántartásban szereplő adatait az SZTFH a 21. § (3) bekezdése szerinti nyilvántartás részeként kezeli.

(5) Az a szervezet, amely 2024. december 31. napján a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 14. § (1) bekezdése szerinti nyilvántartásban megfelelőségértékelő szervezetként szerepel, nem köteles ismételten kérni nyilvántartásba vételét, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 14. § (1) bekezdés *c)–e), g)–j)* és *l)* pontja szerinti adatait az SZTFH a 48. § (1) bekezdése szerinti nyilvántartás részeként kezeli.

(6) A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 14. § (1) bekezdése szerinti nyilvántartásban 2024. december 31. napján szereplő – (7) bekezdés szerinti adatok körébe nem tartozó – adatokat nem kell ismételten bejelenteni, azokat az SZTFH a 48. § (1) bekezdése szerinti nyilvántartás részeként kezeli.

(7) Az e törvény hatálybalépésekor a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény alapján folyamatban lévő hatósági eljárásokat az SZTFH a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény rendelkezéseinek alkalmazásával folytatja le azzal, hogy az e törvény hatálybalépésétől számított 30 napon belül az SZTFH jogosult hiánypótlást kibocsátani. Az eljárás eredményeként e törvény szerint nyilvántartandó adatokat az SZTFH az e törvény szerinti nyilvántartásokba jegyzi be.

(8) Az a szervezet, amely 2024. december 31. napján a sérülékenységvizsgálat lefolytatásának szabályairól szóló kormányrendelet szerinti, a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetekről vezetett nyilvántartásban szerepel, nem köteles ismételten kérni nyilvántartásba vételét, a nyilvántartásban szereplő adatait az SZTFH – az Alkotmányvédelmi Hivatal adatszolgáltatása alapján – az 57. § (1) bekezdés *c)* pontja szerinti nyilvántartás részeként kezeli.

(9) Az 57. § (1) bekezdés *c)* pontja szerinti nyilvántartásba a (8) bekezdés alapján bejegyzett szervezet az e törvényben és az e törvény végrehajtására kiadott jogszabályban a nyilvántartásba vétel feltételeként meghatározott követelmények teljesítését 2025. július 31. napjáig igazolja az SZTFH részére. Az igazolás elmulasztása esetén az SZTFH törli a szervezetet a nyilvántartásából.

## 52. Az Alaptörvény sarkalatosságra vonatkozó követelményének való megfelelés

**90. §** (1) A 93. § az Alaptörvény 46. cikk (6) bekezdése alapján sarkalatosnak minősül.

(2) A 97. § az Alaptörvény IX. cikk (6) bekezdése alapján sarkalatosnak minősül.

(3) A 118–121. § és a 123. § az Alaptörvény 23. cikk (4) bekezdése alapján sarkalatosnak minősül.

## 53. Az Európai Unió jogának való megfelelés

**91. §** (1) Ez a törvény

*a)* az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek,

*b)* a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről szóló, 2022. december 14-i (EU) 2022/2557 európai parlamenti és tanácsi irányelvnek, valamint

*c)* a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.
való megfelelést szolgálja.

(2) Ez a törvény

*a)* az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletnek,

*b)* az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról szóló, 2021. május 20-i (EU) 2021/887 európai parlamenti és tanácsi rendeletnek, valamint

*c)* a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek
a végrehajtásához szükséges rendelkezéseket állapít meg.

**92. §** A 70. § 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.

## 54. Módosító és hatályon kívül helyező rendelkezések

**93–119. §**[28]

**120. §** (1) A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § *m)* pontja helyébe a következő rendelkezés lép:

*(A Hatóság elnöke)*

„*m)* megállapítja a Pmt. 1. § (1) bekezdés *i)* pontjában meghatározott szolgáltatók (a továbbiakban: szolgáltatók) számára kiadandó, a Pvkit. szerinti szűrőrendszer kidolgozására és működtetésének minimumkövetelményeire vonatkozó részletszabályokat, a szolgáltatók tekintetében a belső kockázatértékelés elkészítésének szabályrendszerére, a belső ellenőrző és információs rendszer működtetésére, az egyszerűsített és a fokozott ügyfél-átvilágítás esetköreire és azok felügyeleti jóváhagyásának szabályaira, az auditált elektronikus hírközlő eszköz és működtetésének minimum követelményeire, auditálásának módjára, valamint az ilyen eszköz útján végzett ügyfélátvilágítás végrehajtására, a megerősített eljárás esetköreire és feltételrendszerére, a kijelölt felelős vezető és a megfelelési vezető kijelölésére és helyettesítésére, valamint a kockázatérzékenységi megközelítés alapján üzleti kapcsolat létesítéséhez vagy ügyleti megbízás teljesítéséhez a kijelölt felelős vezető döntését igénylő esetek meghatározására és e döntések meghozatalára, a képzési programra, az ügylet felfüggesztésére, az ügyfél és a tényleges tulajdonos vonatkozásában kiemelt közszereplői minőség megállapításával kapcsolatos kockázatkezelési rendszer kialakítására vonatkozó részletszabályokat,”

(2)[29]

**121–131. §**[30]

## *1. melléklet a 2024. évi LXIX. törvényhez*

[28] Hatályon kívül helyezve: 2010. évi CXXX. törvény 12–12/B. § alapján. Hatálytalan: 2025. I. 2-től.
[29] Hatályon kívül helyezve: 2010. évi CXXX. törvény 12–12/B. § alapján. Hatálytalan: 2025. I. 2-től.
[30] Hatályon kívül helyezve: 2010. évi CXXX. törvény 12–12/B. § alapján. Hatálytalan: 2025. I. 2-től.

## *Közigazgatási ágazathoz tartozó szervezetek*

E törvény értelmében közigazgatási ágazathoz tartozó szervezetnek a következő szervezeteket kell tekinteni:

1. a központi államigazgatási szerv, a Kormány kivételével,
2. a Sándor-palota,
3. az Országgyűlés Hivatala,
4. az Alkotmánybíróság Hivatala,
5. az Országos Bírósági Hivatal és a bíróságok,
6. az ügyészségek,
7. az Alapvető Jogok Biztosának Hivatala,
8. az Állami Számvevőszék,
9. a Magyar Nemzeti Bank,
10. a Magyar Honvédség,
11. a fővárosi és vármegyei kormányhivatalok, a vármegyei közgyűlések hivatalai,
12. a megyei jogú városok és a fővárosi kerületi önkormányzatok képviselő-testületének hivatalai,
13. a települések képviselő-testületének hivatalai,
14. a központi szolgáltató,
15. a központi rendszer felett rendelkezési jogot gyakorló szervezet.

*2. melléklet a 2024. évi LXIX. törvényhez*

## *2. Kiemelten kockázatos ágazatokban működő szolgáltatók és szervezetek*

| | A | B | C |
|---|---|---|---|
| 1 | Ágazat | Alágazat | Szervezet típusa |
| 2 | Energetika | Villamos energia | a villamos energiáról szóló törvény szerinti villamosenergia-ipari vállalkozás a közvilágítási üzemeltetési engedélyes kivételével, |
| 3 | | Távfűtés és hűtés | a távhőszolgáltatásról szóló törvény szerinti engedélyes, |
| 4 | | Kőolaj | a bányászatról szóló törvény szerinti<br>a) szénhidrogén szállítóvezetéket létesítő és üzemben tartó engedélyes,<br>b) a kőolajfeldolgozásban, tárolásban használt létesítmény üzemeltetője, |
| 5 | | | a behozott kőolaj és kőolajtermékek biztonsági készletezéséről szóló törvény szerinti központi készletező szervezet, |
| 6 | | Földgáz | – az egyablakos kapacitásértékesítő, a szervezett földgázpiaci engedélyes és a vezetékes PB-gáz szolgáltató kivételével<br>– a földgázellátásról szóló törvény szerinti engedélyes tevékenységet folytató földgázipari vállalkozás, |
| 7 | | Hidrogén | a hidrogéntermelés, -tárolás és -szállítás üzemeltetője, |
| 8 | Közlekedés | Légi közlekedés | a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló kormányrendelet szerinti légiközlekedés védelmében közreműködő szervezet, |
| 9 | | Vasúti közlekedés | az erdőről, az erdő védelméről és az erdőgazdálkodásról szóló 2009. évi XXXVII. törvény 1. melléklete szerinti gazdasági társaságok kivételével a vasúti közlekedésről szóló törvény szerinti vasúti pályahálózat működtetője – a saját célú vasúti pályahálózatok, iparvágányok kivételével –, a vállalkozó vasúti társaság, a vasúti pályakapacitás-elosztó szervezet, |
| 10 | | Közúti közlekedés | a közúti közlekedésről szóló törvény felhatalmazása alapján kiadott rendelet szerinti *a)* intelligens közúti közlekedési rendszerek üzemeltetését végző szolgáltató,<br>b) forgalomirányítást végző szervezet, |

| | | | |
|---|---|---|---|
| 11 | | Vízi közlekedés | a víziközlekedésről szóló törvény szerinti hajózási tevékenység folytatásában részt vevő jogi személy, jogi személyiséggel nem rendelkező gazdálkodó szervezet, |
| 12 | | Tömegközlekedés | a vasúti és közúti személyszállítási közszolgáltatásról, valamint az 1191/69/EGK és az 1107/70/EGK tanácsi rendelet hatályon kívül helyezéséről szóló, 2007. október 23-i 1370/2007/EK európai parlamenti és tanácsi rendelet 2. cikk *d)* pontja szerinti közszolgáltató szervezet, |
| 13 | Egészségügy | | az egészségügyről szóló törvény szerinti egészségügyi szolgáltató,<br>magas biztonsági szintű biológiai laboratóriumok üzemeltetője,<br>egészségügyi tartalékokat és vérkészleteket kezelő szervezet,<br>gyógyszerek kutatásával és fejlesztésével foglalkozó szervezet,<br>gyógyszeripari alaptermékeket és gyógyszerkészítményeket gyártó szervezet, gyógyszer-nagykereskedő, népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzékén szereplő kritikus fontosságú orvostechnikai eszközt gyártó szervezet, |
| 14 | Ivóvíz, szennyvíz | Víziközmű szolgáltatás | a víziközmű-szolgáltatásról szóló törvény szerinti víziközmű-szolgáltató, |
| 15 | Hírközlési szolgáltatás | | az elektronikus hírközlésről szóló törvény szerinti *a)* elektronikus hírközlési szolgáltató, *b)* adatkicserélő szolgáltatást nyújtó szolgáltató, |
| 16 | | | a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti bizalmi szolgáltató, |
| 17 | Digitális infrastruktúra | | a felhőszolgáltató, |
| 18 | | | adatközponti szolgáltatást nyújtó szolgáltató, |
| 19 | | | legfelső szintű doménnév-nyilvántartó, |
| 20 | | | a DNS-szolgáltató, |
| 21 | | | tartalomszolgáltató hálózat szolgáltatója, |
| 22 | Kihelyezett IKT szolgáltatások | | *a)* kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató,<br>b) kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató, |
| 23 | Űralapú szolgáltatás | | űralapú szolgáltatások nyújtását támogató földi infrastruktúra üzemeltető |

## *3. melléklet a 2024. évi LXIX. törvényhez*

## *3. Kockázatos ágazatokban működő szolgáltatók és szervezetek*

| | A | B | C |
|---|---|---|---|
| 1 | Ágazat | Alágazat | Szervezet típusa |
| 2 | Postai és futárszolgálatok | | a postai szolgáltatásokról szóló törvény szerinti postai szolgáltató, |
| 3 | Élelmiszer<br>a) előállítása,<br>b) az élelmiszer-higiéniáról szóló, 2004. április 29-i 852/2004/EK európai parlamenti és tanácsi rendelet 2. cikk (1) bekezdés *m)* pontja szerinti feldolgozása és<br>c) forgalmazása | | az élelmiszerláncról és hatósági felügyeletéről szóló törvény szerinti élelmiszer-vállalkozás, amely a kereskedelemről szóló 2005. évi CLXIV. törvény 2. § 18. pontja szerinti nagykereskedelemi tevékenységgel, ipari termeléssel és feldolgozással foglalkozik, |
| 4 | Hulladékgazdálkodás | | a hulladékról szóló törvény szerinti tevékenységet végző gazdálkodó szervezet, az erdőről, az erdő |

| | | | |
|---|---|---|---|
| | | | védelméről és az erdőgazdálkodásról szóló 2009. évi XXXVII. törvény 1. melléklete szerinti gazdasági társaságok kivételével, |
| 5 | Vegyszerek előállítása és forgalmazása | | a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről szóló, 2006. december 18-i 1907/2006/EK európai parlamenti és tanácsi rendelet 3. cikke szerinti gyártó, forgalmazó, |
| 6 | Gyártás | Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása | az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről szóló, 2017. április 5-i (EU) 2017/745 európai parlamenti és tanácsi rendelet 2. cikke 1. pontjában meghatározott orvostechnikai eszközöket, valamint az in vitro diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről szóló, 2017 április 5-i (EU) 2017/746 európai parlamenti és tanácsi rendelet 2. cikke 2. pontjában meghatározott in vitro diagnosztikai orvostechnikai eszközöket gyártó szervezet, kivéve a népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzékén szereplő kritikus fontosságú orvostechnikai eszközöket gyártó szervezet, |
| 7 | | Számítógép, elektronikai, optikai termék gyártása | gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 26. ágazata szerinti „Számítógép, elektronikai, optikai termék gyártása” tevékenységet végző gazdálkodó szervezet, |
| 8 | | Villamos berendezések gyártása | a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 27. ágazata szerinti „Villamos berendezés gyártása” tevékenységet végző gazdálkodó szervezet, |
| 9 | | Máshova nem sorolt gépek és berendezések gyártása | a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 28. ágazata szerinti „Gép, gépi berendezés gyártása” tevékenységet végző gazdálkodó szervezet, |
| 10 | | Gépjárművek, pótkocsik és félpótkocsik gyártása | a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 29. ágazata szerinti „Közúti jármű gyártása” tevékenységet végző gazdálkodó szervezet, |

| | | | |
|---|---|---|---|
| 11 | | Egyéb szállítóeszközök gyártása | a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 30. ágazata szerinti „Egyéb jármű gyártása” tevékenységet végző gazdálkodó szervezet, |
| 12 | | Cement-, mész-, gipszgyártás | a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról szóló 1893/2006/EK európai parlamenti és tanácsi rendelet módosításáról szóló, 2022. október 10-i (EU) 2023/137 felhatalmazáson alapuló bizottsági rendelet 23.5 alágazata szerinti „Cement-, mész-, gipszgyártás” tevékenységet végző gazdálkodó szervezet, |
| 13 | Digitális szolgáltatók | | *a)* az online-piactér szolgáltatója,<br>b) az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény szerinti keresőszolgáltató,<br>c) közösségi média szolgáltatási platform szolgáltatója,<br>d) doménnév regisztrációt végző szolgáltató, |
| 14 | Kutatás | | kutatóhely |

# TARTALOMJEGYZÉK

A tartalomjegyzék megjelenítéséhez kattintson a szürke hátterű szövegrészen jobb egér gombbal és válassza ki a Mező frissítése menüpontot.