Az Országgyűlés
Törvényalkotási Bizottsága

Hivatkozási szám a TAB ülésén:
1. (T/9716.)

A bizottság
kormánypárti
tagjainak javaslata.

Javaslat módosítási szándék megfogalmazásához a Törvényalkotási Bizottság számára a **Magyarország kiberbiztonságáról** szóló **T/9716. számú** törvényjavaslathoz

Módosítópont sorszáma: **1.**

Törvényjavaslat érintett rendelkezése: **preambulum**

Módosítás jellege: **módosítás**

[1] A nemzet érdekében kiemelten fontos **[–]**napjaink információs társadalmát érő fenyegetések miatt **[– a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint]**az **[ezt kezelő információs rendszerek, illetve a kulcsfontosságú ágazatokban az alapvető szolgáltatások nyújtására használt]**elektronikus információs rendszerek fenyegetéseinek mérséklése és **[az említett]**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, **[mely]**amely hozzájárul Magyarország és az Európai Unió biztonságához, **[ellenállóképességének]**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:

Módosítópont sorszáma: **2.**

Törvényjavaslat érintett rendelkezése: **1. § (1) bekezdés c) pont**
Módosítás jellege: **módosítás**

1. §

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

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

Módosítópont sorszáma: **3.**
Törvényjavaslat érintett rendelkezése: **1. § (8) bekezdés nyitó szövegrész**
Módosítás jellege: **módosítás**

(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 **[alkalmazásra]**alkalmazására kötelezett szervezet) és hatósági felügyeletükre irányuló tevékenységre kell alkalmazni:

Módosítópont sorszáma: **4.**
Törvényjavaslat érintett rendelkezése: **4. § 10. pont**
Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

10. auditor: az e törvény szerinti kiberbiztonsági **[audit-tevékenység]**auditтevékenység végzésére jogosult, független gazdálkodó szervezet;

Módosítópont sorszáma: **5.**
Törvényjavaslat érintett rendelkezése: **4. § 24. pont c) alpont**
Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

24. elektronikus információs rendszer:

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

Módosítópont sorszáma: **6.**

Törvényjavaslat érintett rendelkezése: **4. § 35. pont**

Módosítás jellege: **elhagyás**

4. §

E törvény alkalmazásában

[35. honvédelmi kiberbiztonsági hatóság: a 23. § (2) bekezdése alapján kijelölt kiberbiztonsági hatóság;]

Módosítópont sorszáma: **7.**

Törvényjavaslat érintett rendelkezése: **4. § 45. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

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

Módosítópont sorszáma: **8.**

Törvényjavaslat érintett rendelkezése: **4. § 61. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

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

Módosítópont sorszáma: **9.**

Törvényjavaslat érintett rendelkezése: **4. § 62. pont**

Módosítás jellege: **elhagyás**

4. §

E törvény alkalmazásában

[62. központi rendszer szolgáltatója: a központi rendszer felett rendelkezési jogosultsággal rendelkező szervezet;]

Módosítópont sorszáma: **10.**

Törvényjavaslat érintett rendelkezése: **4. § 63. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

63. központi szolgáltatás: a **[központosított informatikai és elektronikus hírközlési]**központi szolgáltató **[információbiztonsággal kapcsolatos feladatköréről szóló kormányrendelet szerinti szolgáltatások fogalomba tartozó]**által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;

Módosítópont sorszáma: **11.**

Törvényjavaslat érintett rendelkezése: **4. § 75. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

75. műveleti célú elektronikus információs rendszer: **[a rendvédelmi szervek és a nemzetbiztonsági szolgálatok számára törvényben meghatározott közbiztonsági, nemzetbiztonsági feladatok ellátása érdekében használt 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;

Módosítópont sorszáma: **12.**

Törvényjavaslat érintett rendelkezése: **4. § 78. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

78. 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)];

Módosítópont sorszáma: **13.**

Törvényjavaslat érintett rendelkezése: **4. § 82. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

82. 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;

Módosítópont sorszáma: **14.**

Törvényjavaslat érintett rendelkezése: **4. § 84. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

84. online piactér: olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást **[alkalmaz]**használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;

Módosítópont sorszáma: **15.**

Törvényjavaslat érintett rendelkezése: **4. § 94. pont**

Módosítás jellege: **módosítás**

4. §

E törvény alkalmazásában

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

Módosítópont sorszáma: **16.**

Törvényjavaslat érintett rendelkezése: **5. § (2) bekezdés c) pont**

Módosítás jellege: **módosítás**

(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

c) az **[ezeket]**a) és b) pontban foglaltakat kezelő személyek

együttesének védelmét is biztosítani szükséges.

Módosítópont sorszáma: **17.**

Törvényjavaslat érintett rendelkezése: **6. § (4) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **18.**

Törvényjavaslat érintett rendelkezése: **6. § (5) bekezdés c) és d) pont**

Módosítás jellege: **módosítás**

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

c) gondoskodik az elektronikus információs rendszer eseményeinek **[nyomon követhetőségéről]**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 **[foglaltak]**foglaltaknak megfelelően szerződéses kötelemként teljesüljenek;

Módosítópont sorszáma: **19.**

Törvényjavaslat érintett rendelkezése: **6. § (10) bekezdés a) pont**

Módosítás jellege: **módosítás**

(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 **[teljeskörű]**teljes körű kockázatmenedzsment **[keretrendszer]**keretrendszert működtetni,

Módosítópont sorszáma: **20.**

Törvényjavaslat érintett rendelkezése: **8. § (3) bekezdés a) pont**

Módosítás jellege: **módosítás**

(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

Módosítópont sorszáma: **21.**

Törvényjavaslat érintett rendelkezése: **8. § (5) bekezdés**

Módosítás jellege: **módosítás**

(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.

Módosítópont sorszáma: **22.**

Törvényjavaslat érintett rendelkezése: **9. § (1) bekezdés**

Módosítás jellege: **módosítás**

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 **[a]**kormányrendeletben foglaltak szerint.

Módosítópont sorszáma: **23.**

Törvényjavaslat érintett rendelkezése: **10. § (1) bekezdés**

Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **24.**

Törvényjavaslat érintett rendelkezése: **10. § (7) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **25.**

Törvényjavaslat érintett rendelkezése: **11. § (4) bekezdés**

Módosítás jellege: **módosítás**

(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 **[vagy pénzügyi döntéshozatallal]**kapcsolatos munkakört lát el, illetve ilyen személy közvetlen alárendeltségébe tartozik.

Módosítópont sorszáma: **26.**

Törvényjavaslat érintett rendelkezése: **11. § (9) bekezdés**

Módosítás jellege: **módosítás**

(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 **[bekérni a]**szükséges közreműködői tevékenységgel kapcsolatos adatot, valamint az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

Módosítópont sorszáma: **27.**

Törvényjavaslat érintett rendelkezése: **11. § (10) bekezdés**

Módosítás jellege: **módosítás**

(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 **[helyettes]**helyettese között a feladatok és felelősség megosztásáról a szervezet vezetője rendelkezik. A helyettesre az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó rendelkezéseket kell alkalmazni.

Módosítópont sorszáma: **28.**

Törvényjavaslat érintett rendelkezése: **11. § új (16) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **29.**

Törvényjavaslat érintett rendelkezése: **12. § (2) bekezdés**

Módosítás jellege: **módosítás**

(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.]**

szervezhet.

Módosítópont sorszáma: **30.**

Törvényjavaslat érintett rendelkezése: **14. § (1) bekezdés a) pont**

Módosítás jellege: **módosítás**

14. §

(1) A 13. §-ban foglaltaktól eltérően, ha az elektronikus információs rendszer fejlesztése
a) **[a 13]**az 1. § (1) **[bekezdésében fel nem sorolt]**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,

Módosítópont sorszáma: **31.**
Törvényjavaslat érintett rendelkezése: **15. §**
Módosítás jellege: **módosítás**

15. §

(1) Ha az 1. § (1) bekezdés a)–c) pontja szerinti szervezet elektronikus információs **[rendszer]**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 **[teljeskörű]**teljes körű sérülékenységvizsgálat kezdeményezése. Sérülékenységvizsgálat végzésének kötelezettsége alól **[a]**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**[, továbbfejlesztése]** során irányadó részletes szabályokat kormányrendelet tartalmazza.

Módosítópont sorszáma: **32.**
Törvényjavaslat érintett rendelkezése: **16. § (1) bekezdés**
Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **33.**
Törvényjavaslat érintett rendelkezése: **16. § (4) bekezdés**
Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **34.**

Törvényjavaslat érintett rendelkezése: **16. § új (5) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **35.**

Törvényjavaslat érintett rendelkezése: **18. § (1)-(4) bekezdés**

Módosítás jellege: **módosítás**

18. §

[(1) A központi rendszer a központi rendszer szolgáltatója rendelkezésében lévő elektronikus információs rendszer.]

(2) A központi rendszer **[szolgáltatója által]**felett rendelkezési jogot gyakorló szervezet az általa a felhasználó szervezet részére biztosított központi rendszer vonatkozásában**[a központi rendszer szolgáltatója]**

a) ellátja **[a központi rendszer vonatkozásában a]**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 **[az elektronikus információs]**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 **[az elektronikus információs]**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 **[és]**az általa igénybe vett szolgáltatás érintettsége esetén intézkedik a szolgáltatás nyújtója felé a szükséges intézkedések megtétele érdekében.

(3) A **[központi rendszer szolgáltatója által a]**felhasználó szervezet **[részére biztosított]**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 **[szolgáltatójának]**felett rendelkezési jogot gyakorló szervezet megjelölésével – bejelenti,

b) a központi rendszer **[szolgáltatója által a központi rendszer vonatkozásában]**felett rendelkezési jogot gyakorló szervezet által meghatározott elektronikus információbiztonsági **[feladatokat,]**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 **[szolgáltatója]**felett rendelkezési jogot gyakorló szervezet részére.

(4) Jogszabály alapján kötelezően igénybe vett **[központi rendszer]**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 **[szolgáltatója]**felett rendelkezési jogot gyakorló szervezet és a felhasználó szervezet szolgáltatási szerződést köt.

Módosítópont sorszáma: **36.**

Törvényjavaslat érintett rendelkezése: **19. § (1) bekezdés**

Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **37.**

Törvényjavaslat érintett rendelkezése: **19. § (2) bekezdés b) pont**

Módosítás jellege: **módosítás**

(2) A központi szolgáltató

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

Módosítópont sorszáma: **38.**

Törvényjavaslat érintett rendelkezése: **19. § (2) bekezdés d) pont**

Módosítás jellege: **módosítás**

(2) A központi szolgáltató

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,

Módosítópont sorszáma: **39.**

Törvényjavaslat érintett rendelkezése: **19. § (3) bekezdés b) pont**

Módosítás jellege: **módosítás**

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

b) a központi szolgáltató által **[a központi szolgáltatás vagy a támogató rendszer vonatkozásában]**meghatározott elektronikus információbiztonsági követelményeket teljesíti, ezeket rögzíti az információbiztonsági szabályzatában, valamint

Módosítópont sorszáma: **40.**

Törvényjavaslat érintett rendelkezése: **19. § (4) bekezdés**

Módosítás jellege: **módosítás**

(4) Jogszabály alapján kötelezően igénybe vett központi szolgáltatás vagy támogató rendszer esetén a központi szolgáltató és a felhasználó szervezet közötti feladat- és **[felelősség-megosztást]**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.

Módosítópont sorszáma: **41.**

Törvényjavaslat érintett rendelkezése: **20. § (2) bekezdés c) pont**

Módosítás jellege: **módosítás**

(2) A központi doménnév-nyilvántartás tartalmazza:

c) a **[doménnév-használó]**doménnévhasználó nevét, kapcsolattartásra alkalmas

elektronikus levelezési címét, telefonszámát, és

Módosítópont sorszáma: **42.**

Törvényjavaslat érintett rendelkezése: **21. § (1) bekezdés**

Módosítás jellege: **módosítás**

21. §

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

Módosítópont sorszáma: **43.**

Törvényjavaslat érintett rendelkezése: **22. § (4) bekezdés a) pont**

Módosítás jellege: **módosítás**

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

a) az 1. § (1) bekezdés **[a)–c]**b) pontja szerinti szervezet esetében hivatalból megküldi, a nemzeti kiberbiztonsági hatóság részére.

Módosítópont sorszáma: **44.**

Törvényjavaslat érintett rendelkezése: **23. § (1) bekezdés a) és b) pont**

Módosítás jellege: **módosítás**

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 **[rendszerek]**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 **[rendszerek]**rendszerei esetében az SZTFH

látja el.

Módosítópont sorszáma: **45.**

Törvényjavaslat érintett rendelkezése: **24. § (1) bekezdés 13. pont**

Módosítás jellege: **módosítás**

24. §

(1) A nemzeti kiberbiztonsági hatóság

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

Módosítópont sorszáma: **46.**

Törvényjavaslat érintett rendelkezése: **24. § (1) bekezdés 16. pont**

Módosítás jellege: **módosítás**

24. §

(1) A nemzeti kiberbiztonsági hatóság

16. ellenőrzi az elektronikus információs rendszerek fejlesztése**[, továbbfejlesztése]** során az információbiztonsági követelmények teljesülését,

Módosítópont sorszáma: **47.**

Törvényjavaslat érintett rendelkezése: **24. § (3) bekezdés**

Módosítás jellege: **módosítás**

(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. § (3) és (6) bekezdésének rendelkezéseit. A honvédelmi kiberbiztonsági hatóság az (1) bekezdés 10. pont esetén a honvédelmi kiberbiztonsági incidenskezelő központot tájékoztatja.

Módosítópont sorszáma: **48.**

Törvényjavaslat érintett rendelkezése: **24. § (5) bekezdés**

Módosítás jellege: **módosítás**

(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]**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.

[f) egyéb, a jogszabályi megfelelést alátámasztó adatot, információt, dokumentumot a felügyeleti feladatok elvégzése céljából.]

Módosítópont sorszáma: **49.**

Törvényjavaslat érintett rendelkezése: **24. § új (9) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **50.**

Törvényjavaslat érintett rendelkezése: **25. § (3) bekezdés**

Módosítás jellege: **módosítás**

(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 **[alkalmazást]**alkalmazását tanúsító szervezet, illetve a poszt-kvantumtitkosítás alkalmazás nyújtására jogosult szervezetek ellenőrzésével kapcsolatos eljárás esetén kilencven nap.

Módosítópont sorszáma: **51.**

Törvényjavaslat érintett rendelkezése: **26. § (1) bekezdés**

Módosítás jellege: **módosítás**

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 **[kijelölésére]**kijelölésre és az 1. § (6) **[bekezdésben]**bekezdésében meghatározott feltételek közül legalább egy teljesül.

Módosítópont sorszáma: **52.**

Törvényjavaslat érintett rendelkezése: **28. § (1) bekezdés 1. pont b) alpont**

Módosítás jellege: **módosítás**

28. §

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

1. a szervezet vonatkozásában:

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

Módosítópont sorszáma: **53.**

Törvényjavaslat érintett rendelkezése: **28. § (1) bekezdés 2. pont b) alpont**

Módosítás jellege: **módosítás**

28. §

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

2. központi rendszerhez csatlakozott szervezet esetében:

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

Módosítópont sorszáma: **54.**

Törvényjavaslat érintett rendelkezése: **28. § (2) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **55.**

Törvényjavaslat érintett rendelkezése: **28. § új (3) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **56.**

Törvényjavaslat érintett rendelkezése: **28. § (3) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **57.**

Törvényjavaslat érintett rendelkezése: **28. § (4) bekezdés**

Módosítás jellege: **módosítás**

(4) 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,**[és]**

i) a Magyar Honvédség kibertér műveleti erői,

j) a honvédelmi kiberbiztonsági incidenskezelő központ és

k) a nemzeti kiberbiztonsági hatóság
részére végezhető.

Módosítópont sorszáma: **58.**

Törvényjavaslat érintett rendelkezése: **29. § (1) bekezdés**

Módosítás jellege: **módosítás**

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,

ab) 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,

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

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

ad) 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;**[valamint]**

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.

Módosítópont sorszáma: **59.**

Törvényjavaslat érintett rendelkezése: **29. § (2) bekezdés**

Módosítás jellege: **módosítás**

(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.

Módosítópont sorszáma: **60.**

Törvényjavaslat érintett rendelkezése: **30. § (1) bekezdés a) pont**

Módosítás jellege: **módosítás**

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,

Módosítópont sorszáma: **61.**

Törvényjavaslat érintett rendelkezése: **30. § új (3) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **62.**

Törvényjavaslat érintett rendelkezése: **31. § (2) bekezdés**

Módosítás jellege: **módosítás**

(2) Az **[információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat az]**1. § (1) bekezdés**[a)–c) pontja szerinti szervezetek esetében kormányrendelet, az 1. § (1) bekezdés d) és e) pontja szerinti szervezetek esetében az SZTFH elnöke rendeletben határozza meg.]**

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.

Módosítópont sorszáma: **63.**

Törvényjavaslat érintett rendelkezése: **33. § (11) bekezdés**

Módosítás jellege: **módosítás**

(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.

Módosítópont sorszáma: **64.**

Törvényjavaslat érintett rendelkezése: **39. § (3) bekezdés b) pont**

Módosítás jellege: **módosítás**

(3) A nemzeti kiberbiztonsági tanúsítási rendszerben meg kell határozni

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 **[forráskód-elemzéseket]**forráskódelemzéseket, valamint

Módosítópont sorszáma: **65.**

Törvényjavaslat érintett rendelkezése: **42. § (1) bekezdés**

Módosítás jellege: **módosítás**

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 **[44]**45. § (1) bekezdés b) pontja szerinti esetben a Kormány rendeletében meghatározott módon és formában – megfelelőségi jelölést kell elhelyezni.

Módosítópont sorszáma: **66.**

Törvényjavaslat érintett rendelkezése: **44. § (1) bekezdés b) pont**

Módosítás jellege: **módosítás**

44. §

(1) Harmadik fél által végzett megfelelőségértékelési tevékenységet csak olyan szervezet végezhet,

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

Módosítópont sorszáma: **67.**

Törvényjavaslat érintett rendelkezése: **45. § (1) bekezdés**

Módosítás jellege: **módosítás**

45. §

(1) A tanúsító hatóság feladatait

a) **[– a b) pont kivételével –]**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.

Módosítópont sorszáma: **68.**

Törvényjavaslat érintett rendelkezése: **47. § (6) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **69.**

Törvényjavaslat érintett rendelkezése: **49. § (3) bekezdés**

Módosítás jellege: **módosítás**

(3) A tanúsító hatóság a jogosulatlan megfelelőségértéklési tevékenységet végző személlyel szemben a Kormány rendeletében meghatározott mértékű közigazgatási bírságot szabhat ki. A Hatóság a bírság összegének megállapításakor a közigazgatási szabályszegések szankcióiról szóló **[2017. évi CXXV.]**törvényben foglalt szempontokat mérlegeli. Figyelmeztetés közigazgatási szankció alkalmazásának nincs helye.

Módosítópont sorszáma: **70.**

Törvényjavaslat érintett rendelkezése: **51. § nyitó szövegrész**

Módosítás jellege: **módosítás**

51. §

A poszt-kvantumtitkosítás **[alkalmazásra]**alkalmazására kötelezett szervezet elektronikus információs rendszere teljes életciklusában meg kell valósítani és biztosítani kell

Módosítópont sorszáma: **71.**

Törvényjavaslat érintett rendelkezése: **51. § b) pont**

Módosítás jellege: **módosítás**

51. §

A poszt-kvantumtitkosítás alkalmazásra kötelezett szervezet elektronikus információs rendszere teljes életciklusában meg kell valósítani és biztosítani kell

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása, a poszt-kvantumtitkosítás **[alkalmazásra]**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-kvantum titkosítási]**poszt-kvantumtitkosítási alkalmazással történő
zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét.

Módosítópont sorszáma: **72.**
Törvényjavaslat érintett rendelkezése: **30. alcím cím**
Módosítás jellege: **módosítás**

30. A poszt-kvantumtitkosítás **[alkalmazásra]**alkalmazására kötelezett szervezet védelme

Módosítópont sorszáma: **73.**
Törvényjavaslat érintett rendelkezése: **52. §**
Módosítás jellege: **módosítás**

52. §

A poszt-kvantumtitkosítás **[alkalmazásra]**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.

Módosítópont sorszáma: **74.**
Törvényjavaslat érintett rendelkezése: **53. § (1) bekezdés nyitó szövegrész**
Módosítás jellege: **módosítás**

53. §

(1) Kizárólag olyan szervezet nyújthat poszt-kvantumtitkosítás alkalmazást (a továbbiakban: poszt-kvantumtitkosítás alkalmazást nyújtó szervezet) a poszt-kvantumtitkosítás **[alkalmazásra]**alkalmazására kötelezett szervezet számára, amely

Módosítópont sorszáma: **75.**
Törvényjavaslat érintett rendelkezése: **56. § (1) bekezdés b) pont**
Módosítás jellege: **módosítás**

56. §

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

b) a jelen fejezetben meghatározott követelményeknek való **[nem-megfelelés]**nem megfelelés gyanúja esetén rendkívüli ellenőrzést hajthat végre.

Módosítópont sorszáma: **76.**

Törvényjavaslat érintett rendelkezése: **56. § (3) bekezdés nyitó szövegrész**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **77.**

Törvényjavaslat érintett rendelkezése: **57. § (5) bekezdés a) pont**

Módosítás jellege: **módosítás**

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

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

elektronikus információs rendszere vonatkozásában.

Módosítópont sorszáma: **78.**

Törvényjavaslat érintett rendelkezése: **62. § (2) bekezdés**

Módosítás jellege: **módosítás**

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

Módosítópont sorszáma: **79.**

Törvényjavaslat érintett rendelkezése: **63. §**

Módosítás jellege: **módosítás**

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 **[a Kormány által]**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 **[a Kormány által]**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. § (**[5) bekezdése szerinti SZTFH rendeletben]**3) bekezdés b) pontja szerinti rendeletében meghatározott feltételeket is figyelembe **[veszi]**kell venni.

Módosítópont sorszáma: **80.**

Törvényjavaslat érintett rendelkezése: **65. § (1) és (2) bekezdése**

Módosítás jellege: **módosítás**

65. §

(1) A nemzeti kiberbiztonsági incidenskezelő központ a kibertérből érkező fenyegetettségek felderítésére irányuló, védelmi, prevenciós célú eszközöket alkalmazhat és **[ezirányú]**ez irányú szolgáltatásokat (a továbbiakban együtt: prevenciós eszközök) nyújthat az 1. § (**[10]**1) bekezdése **[a) pontja]**szerinti szervezeteknek.

(2) A prevenciós eszközök alkalmazását az 1. § (1) **[bekezdés]**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.

Módosítópont sorszáma: **81.**

Törvényjavaslat érintett rendelkezése: **65. § (5) bekezdés**

Módosítás jellege: **módosítás**

(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) **[bekezdésben megjelölt]**bekezdés a)–c) pontja szerinti szervezet csatlakozását vagy járul hozzá a csatlakozáshoz.

Módosítópont sorszáma: **82.**

Törvényjavaslat érintett rendelkezése: **70. § (3) bekezdés új b) pont**

Módosítás jellege: **kiegészítés**

(3) Az érintett kiberbiztonsági incidens kezelését

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,

végzi.

Módosítópont sorszáma: **83.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

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

Módosítópont sorszáma: **84.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

(4) 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.

Módosítópont sorszáma: **85.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

(4) 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.

Módosítópont sorszáma: **86.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

(4) 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.

Módosítópont sorszáma: **87.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

(4) 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.

Módosítópont sorszáma: **88.**

Törvényjavaslat érintett rendelkezése: **70. § új (4) bekezdés**

Módosítás jellege: **kiegészítés**

(4) 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.

Módosítópont sorszáma: **89.**

Törvényjavaslat érintett rendelkezése: **70. § új (7) bekezdés**

Módosítás jellege: **kiegészítés**

(7) 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.

Módosítópont sorszáma: **90.**

Törvényjavaslat érintett rendelkezése: **71. § (1) bekezdés**

Módosítás jellege: **módosítás**

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. § (**[4)]**10), (13) és (**[7)–(8) bekezdései]**14) bekezdése szerinti rendelkezések alkalmazandóak.

Módosítópont sorszáma: **91.**

Törvényjavaslat érintett rendelkezése: **73. § (4) bekezdés**

Módosítás jellege: **módosítás**

(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.

Módosítópont sorszáma: **92.**

Törvényjavaslat érintett rendelkezése: **46. alcím cím**
Módosítás jellege: **módosítás**

46. A kiberbiztonsági **[válsághelyzetkezelés]**válsághelyzet-kezelés szervezetrendszere

Módosítópont sorszáma: **93.**
Törvényjavaslat érintett rendelkezése: **74. § (4) bekezdés**
Módosítás jellege: **módosítás**

(4) Kiberbiztonsági válsághelyzet és az az alapján elrendelt összehangolt védelmi tevékenység esetén a Kormány intézkedésként bevezetheti

1. a kiberbiztonsági **[válsághelyzetkezelésben]**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 **[válsághelyzetkezeléséhez]**válsághelyzet-kezeléséhez szükséges szolgáltató működési helyiségeinek, technikai eszközparkjának, elektronikus információs rendszerének és létesítményeinek térítésmentes igénybevételét, használatra való átengedését;
8. az állami, valamint a kiberbiztonsági **[válsághelyzetkezelésben]**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.

Módosítópont sorszáma: **94.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **95.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) Az Operatív Törzs a (6) bekezdés alapján kezelt adatokat a nemzetbiztonsági tevékenységre vonatkozó információk kivételével köteles átadni a nemzeti eseménykezelő központnak.

Módosítópont sorszáma: **96.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) Az Operatív Törzs a (6) bekezdés alapján kezelt adatokat – a kiberbiztonsági válsághelyzetre okot adó körülmények vizsgálata céljából – a nemzeti kiberbiztonsági incidenskezelő központnak átadhatja.

Módosítópont sorszáma: **97.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) 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.

Módosítópont sorszáma: **98.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) 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.

Módosítópont sorszáma: **99.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) 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.

Módosítópont sorszáma: **100.**

Törvényjavaslat érintett rendelkezése: **74. § új (6) bekezdés**

Módosítás jellege: **kiegészítés**

(6) 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.

Módosítópont sorszáma: **101.**

Törvényjavaslat érintett rendelkezése: **76. § (1) bekezdés**

Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **102.**

Törvényjavaslat érintett rendelkezése: **77. § (3) bekezdés**

Módosítás jellege: **módosítás**

(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 **[kötelesek]**köteles az elektronikus információs rendszereiből és adathordozóiról törölni.

Módosítópont sorszáma: **103.**

Törvényjavaslat érintett rendelkezése: **77. § (5) bekezdés**

Módosítás jellege: **módosítás**

(5) Ha az adatok változását a szervezet bejelenti, akkor az eredeti adatokat a kiberbiztonsági **[hatóságaz]**hatóság az adat változásának bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

Módosítópont sorszáma: **104.**

Törvényjavaslat érintett rendelkezése: **78. § (2) és (3) bekezdés**

Módosítás jellege: **módosítás**

(2) A kiberbiztonsági hatóság, a sérülékenységvizsgálat végzésére jogosult szerv vagy gazdálkodó szervezet, valamint a kiberbiztonsági incidenskezelő központ eljárása során keletkezett adatok – a **[78]**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 **[határozatát]**határozata az ügyfélen, valamint az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény 33. § (3) bekezdése alapján iratbetekintésre jogosult személyen kívül **[a kiberbiztonsági hatóság mással]**más által nem **[közölheti]**ismerhető meg.

Módosítópont sorszáma: **105.**

Törvényjavaslat érintett rendelkezése: **80. § (1) bekezdés**

Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **106.**

Törvényjavaslat érintett rendelkezése: **81. § (1) bekezdés c) pont**

Módosítás jellege: **módosítás**

81. §

(1) Felhatalmazást kap a Kormány, hogy rendeletben kijelölje

c) a honvédelmi célú elektronikus információs rendszerek tekintetében a **[hatósági feladatokat]**kiberbiztonsági felügyeletet ellátó **[szervet]**hatóságot,

Módosítópont sorszáma: **107.**

Törvényjavaslat érintett rendelkezése: **81. § (2) bekezdés 6. pont**
Módosítás jellege: **módosítás**

(2) Felhatalmazást kap a Kormány, hogy rendeletben megállapítsa
6. az 1. § (1) bekezdés a)–c) pontja szerinti szervezet elektronikus információs rendszerei fejlesztése**[, továbbfejlesztése]** során **[irányadó]**alkalmazandó részletes szabályokat;

Módosítópont sorszáma: **108.**
Törvényjavaslat érintett rendelkezése: **81. § (2) bekezdés 8. pont**
Módosítás jellege: **módosítás**

(2) Felhatalmazást kap a Kormány, hogy rendeletben megállapítsa
8. a nemzeti kiberbiztonsági hatóság, valamint a honvédelmi célú elektronikus információs rendszerek tekintetében a **[hatósági feladatokat]**kiberbiztonsági felügyeletet ellátó **[szerv]**hatóság feladat- és hatáskörét, valamint az eljárására és a nyilvántartásra vonatkozó részletes szabályokat;

Módosítópont sorszáma: **109.**
Törvényjavaslat érintett rendelkezése: **81. § (2) bekezdés 13. pont**
Módosítás jellege: **módosítás**

(2) Felhatalmazást kap a Kormány, hogy rendeletben megállapítsa
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;

Módosítópont sorszáma: **110.**
Törvényjavaslat érintett rendelkezése: **81. § (2) bekezdés 25. pont**
Módosítás jellege: **módosítás**

(2) Felhatalmazást kap a Kormány, hogy rendeletben megállapítsa
25. a **[77]**76. § (1) bekezdése szerinti szervek közötti és a **[77]**76. § (3) bekezdése szerinti szervezetekkel való együttműködés, valamint az Európai Bizottság és az ENISA részére történő tájékoztatás és adatszolgáltatás rendjére vonatkozó részletes szabályokat,

Módosítópont sorszáma: **111.**
Törvényjavaslat érintett rendelkezése: **81. § (3) bekezdés c) pont**
Módosítás jellege: **módosítás**

(3) Felhatalmazást kap az informatikáért felelős miniszter, hogy rendeletben meghatározza
c) a – 11. § (3) bekezdés b) pontjában megjelölt szervezetek vonatkozásában az elektronikus információs rendszer biztonságáért felelős személy, **[feladatellátáshoz]**valamint – az 1. § (1) bekezdés a)-c) pontja szerinti szervezetek vonatkozásában – az információbiztonsági felügyelő feladatellátásához szükséges végzettséget, szakképzettséget, képzettséget vagy szakmai tapasztalatot,

Módosítópont sorszáma: **112.**

Törvényjavaslat érintett rendelkezése: **81. § (5) bekezdés**

Módosítás jellege: **módosítás**

(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.

[a) 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, valamint

b) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségértékelő szervezetekkel szemben támasztott követelményeket.]

Módosítópont sorszáma: **113.**

Törvényjavaslat érintett rendelkezése: **81. § (6) bekezdés e) pont**

Módosítás jellege: **módosítás**

(6) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza

e) az 1. § (1) bekezdés b), d) és e) pontja szerinti szervezeteknek a 29. § (1) bekezdés **[1.]**a) pontja szerinti kiberbiztonsági felügyeleti hatósági nyilvántartásba vételének rendjét, valamint a nyilvántartás személyes adatnak nem minősülő adattartalmára vonatkozó részletes szabályokat,

Módosítópont sorszáma: **114.**

Törvényjavaslat érintett rendelkezése: **81. § (6) bekezdés g) pont**

Módosítás jellege: **módosítás**

(6) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza

g) a poszt-kvantumtitkosítás **[alkalmazásra]**alkalmazására kötelezett szervezeteket,

Módosítópont sorszáma: **115.**

Törvényjavaslat érintett rendelkezése: **81. § (7) bekezdés**

Módosítás jellege: **módosítás**

(7) Felhatalmazást kap az SZTFH elnöke, hogy rendeletben meghatározza**[a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és személyek nyilvántartásba vételének részletes szabályait, a tevékenység végzéséhez szükséges infrastrukturális feltételeket és szakértelmet.]**

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.

Módosítópont sorszáma: **116.**
Törvényjavaslat érintett rendelkezése: **82. § (2) bekezdés**
Módosítás jellege: **módosítás**

82. §

(1) Ez a törvény – a (2) bekezdésben foglalt kivétellel – 2025. január 1-jén lép hatályba.

(2) A **[121]**120. § (1) bekezdése 2025. **[június 1-jén]**január 2-án lép hatályba.

Módosítópont sorszáma: **117.**
Törvényjavaslat érintett rendelkezése: **83. §**
Módosítás jellege: **módosítás**

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 **[alábbi]**szervezet a 8. § (4) bekezdés szerinti határidőn belül teljesíti a nemzeti kiberbiztonsági hatóság részére, ha

a) e törvény **[hatályba lépését]**hatálybalépését megelőzően az Ibtv. hatálya alá tartozott és még nem teljesítette a 8. § (4) bekezdés szerinti kötelezettséget, valamint
b) e törvény **[hatályba lépését]**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 **[hatályba lépésekor]**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 **[hatályba lépéséig]**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 **[hatályba lépését]**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 **[hatályba lépéséig]**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.

Módosítópont sorszáma: **118.**

Törvényjavaslat érintett rendelkezése: **85. §**

Módosítás jellege: **módosítás**

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 **[hatályba lépését]**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 **[hatályba lépésétől]**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 **[hatályba lépését]**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.

Módosítópont sorszáma: **119.**

Törvényjavaslat érintett rendelkezése: **86. §**

Módosítás jellege: **módosítás**

86. §

(1) **[Ha az]**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**[, vagy meglévő rendszer továbbfejlesztésére]** vonatkozó előírásait kell alkalmazni az e törvény **[hatályba lépésekor]**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. § (**[5]**6) bekezdése szerinti fokozatos kivitelezésre, azzal, hogy a vonatkozó **[határidők]**határidő számításának alapját e törvény **[hatályba lépésének]**hatálybalépésének napja képezi.

Módosítópont sorszáma: **120.**

Törvényjavaslat érintett rendelkezése: **87. §**

Módosítás jellege: **módosítás**

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 **[hatályba lépését]**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 **[41/2015. (VII. 15.) BM]**rendeletben foglaltaknak való megfelelést vizsgálja, kivéve, ha a szervezet az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések teljesítéséről nyilatkozott.

Módosítópont sorszáma: **121.**

Törvényjavaslat érintett rendelkezése: **88. §**

Módosítás jellege: **módosítás**

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.

Módosítópont sorszáma: **122.**

Törvényjavaslat érintett rendelkezése: **89. § (1) bekezdés**

Módosítás jellege: **módosítás**

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 **[1.]**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.

Módosítópont sorszáma: **123.**

Törvényjavaslat érintett rendelkezése: **89. § új (2) bekezdés**

Módosítás jellege: **kiegészítés**

(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.

Módosítópont sorszáma: **124.**

Törvényjavaslat érintett rendelkezése: **89. § új (2) bekezdés**

Módosítás jellege: **kiegészítés**

(2) 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.

Módosítópont sorszáma: **125.**

Törvényjavaslat érintett rendelkezése: **89. § (6) bekezdés**

Módosítás jellege: **módosítás**

(6) Az a szervezet, amely 2024. december 31. napján a sérülékenységvizsgálat lefolytatásának szabályairól szóló **[271/2018. (XII. 20.) Korm. rendelet 22. § (5) bekezdése]**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.

Módosítópont sorszáma: **126.**

Törvényjavaslat érintett rendelkezése: **90. § (3) bekezdés**

Módosítás jellege: **módosítás**

90. §

(1) A 92. § az Alaptörvény 46. cikk (6) bekezdése alapján sarkalatosnak minősül.

(2) A 96. § az Alaptörvény IX. cikk (6) bekezdése alapján sarkalatosnak minősül.

(3) A **[109–111]**118–121. § és a **[113]**123. § az Alaptörvény 23. **[cikke]**cikk (4) bekezdése alapján sarkalatosnak minősül.

Módosítópont sorszáma: **127.**

Törvényjavaslat érintett rendelkezése: **91. § (1) bekezdés**

Módosítás jellege: **módosítás**

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,**[valamint]**

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.

Módosítópont sorszáma: **128.**

Törvényjavaslat érintett rendelkezése: **Új 92. §**

Módosítás jellege: **kiegészítés**

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.

Módosítópont sorszáma: **129.**

Törvényjavaslat érintett rendelkezése: **Új 97. §**

Módosítás jellege: **kiegészítés**

97. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény 49. § (7) bekezdés i) pontja helyébe a következő rendelkezés lép és a bekezdés a következő j) ponttal egészül ki:

(A Hatóság)

„i) elrendeli az állagmegóvásra, átalakításra, helyreállításra vonatkozó kötelezettség teljesítését, illetve az elektronikus hírközlési építmény bontását, ha annak állapota az állékonyságot, az életet, testi épséget és az egészséget, a köz- és vagyonbiztonságot veszélyezteti, vagy az elektronikus hírközlési építmény használatra alkalmatlan, vagy a használatával véglegesen felhagytak;

j) egyéb, törvényben meghatározott szankciót alkalmazhat.”

Módosítópont sorszáma: **130.**

Törvényjavaslat érintett rendelkezése: **Új 98. §**

Módosítás jellege: **kiegészítés**

98. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény 86/B. §-a helyébe a következő rendelkezés lép:

„86/B. §

(1) Az elektronikus hírközlő hálózat üzemeltetője a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) elnöke által kiadott rendeletben meghatározott kiberbiztonsági követelmények betartásával és alkalmazásával köteles végezni az üzemeltetési tevékenységet.

(2) Az elektronikus hírközlési szolgáltató által az elektronikus hírközlési szolgáltatáshoz használt rendszernek rendelkeznie kell a Magyarország kiberbiztonságáról szóló törvény alapján kiállított nemzeti vagy európai kiberbiztonsági tanúsítvánnyal, ha az adott, hírközlési szolgáltatáshoz használt rendszerre vonatkozóan nemzeti vagy európai kiberbiztonsági tanúsítási rendszer meghatározásra került.”

Módosítópont sorszáma: **131.**

Törvényjavaslat érintett rendelkezése: **Új 99. §**

Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény a következő 97/A. §-sal egészül ki:

„97/A. §

(1) Az elektronikus hírközlési építmény üzemeltetője, ennek hiányában a tulajdonosa a használat során köteles az építmény állagát megóvni, az élet, a testi épség és az egészség, a köz- és vagyonbiztonság védelme érdekében az építmény műszaki állapotának rendszeres felülvizsgálatát és a szükséges átalakítási, felújítási, helyreállítási munkálatokat elvégezni, továbbá az üzemen vagy használaton kívüli hálózatokat elbontani.

(2) Az elektronikus hírközlési építmény üzemeltetője, ennek hiányában tulajdonosa az építményt elbontja, ha annak használatával véglegesen felhagy, vagy az építmény további használatra alkalmatlan. Az üzemeltető, ennek hiányában a tulajdonos az elektronikus

hírközlési építmény elbontását követően az eredeti állapot helyreállítására köteles, kivéve, ha az érintett ingatlan tulajdonosával vagy a tulajdonosi jog gyakorlójával eltérően állapodnak meg.

(3) Azt az elektronikus hírközlési építményt, amelynek használatával véglegesen felhagytak, vagy használatra alkalmatlan, és tulajdonosa nem ismert vagy nem elérhető, az ingatlan tulajdonosa – a tulajdonát képező ingatlant érintő építményrész erejéig – az elektronikus hírközlési építmények elhelyezéséről és az elektronikus hírközlési építményekkel kapcsolatos hatósági eljárásokról szóló NMHH rendelet szerinti engedély alapján elbontathatja. A bontással okozott kárért a bontási engedélyt kérő felel.

(4) Az elektronikus hírközlési építmény rongálódott, használaton kívüli, vagy használatra alkalmatlan állapotát a Hatóság ügyfélszolgálatán bárki bejelentheti.”

Módosítópont sorszáma: **132.**

Törvényjavaslat érintett rendelkezése: **Új 99. §**

Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény „Ingatlanhasználat, közös építményhasználat” alcíme a következő 98/B. §-sal egészül ki:

„98/B. §

(1) 2027. január 1-jétől belterületen a helyi építési szabályzatokban meghatározott területeken nyomvonalas elektronikus hírközlési építmény csak földfelszín alatti elhelyezéssel létesíthető.

(2) Az (1) bekezdés nem vonatkozik

a) a földfelszín feletti elektronikus hírközlő hálózat

aa) egyes szakaszainak más nyomvonalra történő áthelyezésére (kiváltás),

ab) korszerűsítésére (ideértve a meglévő hálózat modernizálását, új technológiájú hálózattal történő kiváltását is),

ac) felújítására, vagy

b) a meglévő, földfelszín feletti elektronikus hírközlő hálózatról előfizetői leágazással történő bekötésre.”

Módosítópont sorszáma: **133.**

Törvényjavaslat érintett rendelkezése: **Új 99. §**

Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény „Ingatlanhasználat, közös építményhasználat” alcíme a következő 98/C. §-sal egészül ki:

„98/C. §

(1) A helyi önkormányzat a működési területéhez tartozó, a helyi építési szabályzatában

megjelölt belterületen – kormányrendeletben meghatározott feltételek szerint – jogosult a földfelszín felett 5 évnél régebben létesített nyomvonalas elektronikus hírközlő hálózat földfelszín alatti elhelyezésre történő cseréjét kezdeményezni, amennyiben az érintett előfizetők, illetve ingatlantulajdonosok az ingatlanukat érintő munkavégzéshez előzetesen hozzájárulnak, és annak költségeit vállalják.

(2) A jogszerűen létesített elektronikus hírközlő hálózat üzemeltetője a kezdeményezés alapján 6 hónapon belül kiváltási-ütemezési tervet készít annak figyelembevételével, hogy az a szolgáltatásnyújtás folytonosságát ne veszélyeztesse.

(3) Ha a kezdeményezés szerinti területen több elektronikus hírközlési szolgáltató, illetve hálózatüzemeltető is rendelkezik hálózattal, akkor a kiváltási-ütemezési tervet e törvénynek a tervezett építési munkák összehangolására vonatkozó szabályai szerint kell elkészíteni.

(4) Az (1)-(3) bekezdés alkalmazandó a villamos energiáról szóló 2007. évi LXXXVI. törvény 33/F. §-ában foglalt, használaton kívüli hálózati infrastruktúra elbontásának esetében is.

(5) Az (1)-(4) bekezdés alapján kialakított kiváltási-ütemezési tervet az érintett üzemeltetők és az önkormányzat közös megállapodásban véglegesítik. A megállapodás tartalmazza az elvégzendő munkákat és azoknak az egyes feleket terhelő költségeit.”

Módosítópont sorszáma: **134.**
Törvényjavaslat érintett rendelkezése: **Új 99. §**
Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény a következő 163/F. §-sal egészül ki:

„163/F. §

E törvénynek a Magyarország kiberbiztonságáról szóló 2024. évi … törvénnyel megállapított 98/B. §-át a 2027. január 1-ét követően indult építésügyi hatósági engedélyezési eljárásokban kell alkalmazni.”

Módosítópont sorszáma: **135.**
Törvényjavaslat érintett rendelkezése: **Új 99. §**
Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény 163/P. §-a helyébe a következő rendelkezés lép:

„163/P. §

(1) E törvénynek a Magyarország kiberbiztonságáról szóló 2024. évi … törvénnyel megállapított 86/B. § (1) bekezdését e rendelkezés hatálybalépését követően az SZTFH elnökének az elektronikus hírközlő hálózat üzemeltetője által teljesítendő kiberbiztonsági

követelményekre vonatkozó részletes szabályokat tartalmazó rendelete hatálybalépését követő 30. naptól kell alkalmazni.

(2) E törvénynek a Magyarország kiberbiztonságáról szóló 2024. évi … törvénnyel megállapított 86/B. § (2) bekezdését e rendelkezés hatálybalépését követően az SZTFH elnökének az elektronikus hírközlési szolgáltatáshoz használt rendszerek nemzeti kiberbiztonsági tanúsítási rendszeréről szóló rendelete hatálybalépését követő 180. naptól kell alkalmazni.”

Módosítópont sorszáma: **136.**

Törvényjavaslat érintett rendelkezése: **Új 99. §**

Módosítás jellege: **kiegészítés**

99. §

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. §-a a következő (6) bekezdéssel egészül ki:

„(6) Felhatalmazást kap az SZTFH elnöke, hogy – az Elnök véleményének kikérésével – rendeletben határozza meg az elektronikus hírközlési szolgáltatáshoz használt rendszerek vonatkozásában alkalmazandó európai vagy nemzeti kiberbiztonsági tanúsítási rendszert.”

Módosítópont sorszáma: **137.**

Törvényjavaslat érintett rendelkezése: **111. §**

Módosítás jellege: **módosítás**

111. §

(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) A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § q) pontja helyébe a következő rendelkezés lép:

(A Hatóság elnöke)

„q) megállapítja a kiberbiztonsági felügyeleti díj mértékét és a megfizetésére vonatkozó rendelkezéseket, az auditorok nyilvántartásba vételi eljárásának rendjét, és az auditorral szemben támasztott követelményeket, a kiberbiztonsági audit lefolytatásának rendjét, valamint a kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját, a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezetek vonatkozásában a kiberbiztonsági felügyelet és feladatellátás, továbbá a hatósági ellenőrzés lefolytatásának részletes szabályait, a Kiberbiztonsági tv. 1. § (1) bekezdés b), d) és e) pontja szerinti szervezeteknek a Kiberbiztonsági tv. 29. § (1) bekezdés **[1.]**a) pontja szerinti kiberbiztonsági felügyeleti hatósági nyilvántartásba vételének rendjét, valamint a nyilvántartás személyes adatnak nem minősülő adattartalmára vonatkozó részletes szabályokat, a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezetek esetében az információbiztonsági felügyelő személyével szembeni követelményeket, a kirendelésére, jogosítványaira, feladataira vonatkozó részletes szabályokat, a poszt-kvantumtitkosítás **[alkalmazásra]**alkalmazására kötelezett szervezeteket, 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, a poszt-kvantumtitkosítás alkalmazást nyújtó szervezet informatikai rendszerelemei zártsága tanúsítására vonatkozó részletes szabályokat, a Kiberbiztonsági tv. 54. § (1) bekezdése szerinti tanúsító szervezet nyilvántartásba vételére, a nyilvántartás személyes adatot nem tartalmazó adattartalmára, valamint a tanúsító szervezet ellenőrzésére vonatkozó részletes szabályokat, a Kiberbiztonsági tv. 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, – 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, – a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével – a nemzeti kiberbiztonsági tanúsítási rendszereket, a kötelezően alkalmazandó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termékeket, IKT-szolgáltatásokat vagy IKT-folyamatokat, valamint az ezek alkalmazására kötelezett, a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezeteket, a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és személyek nyilvántartásba vételének részletes szabályait, a tevékenység végzéséhez szükséges infrastrukturális feltételeket és szakértelmet, továbbá 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,”

Módosítópont sorszáma: **138.**

Törvényjavaslat érintett rendelkezése: **Új 112. §**

Módosítás jellege: **kiegészítés**

112. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13/A. §-a a következő 3. ponttal egészül ki:

„3. meghatározza az elektronikus hírközlési szolgáltatáshoz használt rendszerek vonatkozásában alkalmazandó európai vagy nemzeti kiberbiztonsági tanúsítási rendszert.”

Módosítópont sorszáma: **139.**

Törvényjavaslat érintett rendelkezése: **117. §**

Módosítás jellege: **módosítás**

117. §

[A honvédelmi adatkezelésekről]Hatályát veszti a védelmi és biztonsági tevékenységek összehangolásáról szóló **[2022]**2021. évi **[XXI]**XCIII. törvény **[99. §-ában a „biztonságának felügyeletét” szövegrész helyébe a „kiberbiztonsági felügyeletét” szöveg, az „az állami és önkormányzati szervek elektronikus információbiztonságáról” szövegrészek helyébe az „a Magyarország kiberbiztonságáról” szöveg és a „biztonsági események” szövegrész helyébe a „kiberbiztonsági incidensek” szöveg lép]**85. § (1) bekezdés f) és h)-j) pontja, valamint (2) bekezdése.

Módosítópont sorszáma: **140.**

Törvényjavaslat érintett rendelkezése: **121. §**

Módosítás jellege: **elhagyás**

[121. §

A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 81. § (1) bekezdés d) pont da) alpontja a „kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről” szövegrész helyett a „Magyarország kiberbiztonságáról” szöveggel lép hatályba.]

Módosítópont sorszáma: **141.**

Törvényjavaslat érintett rendelkezése: **1. melléklet 15. pont**

Módosítás jellege: **módosítás**

E törvény értelmében közigazgatási ágazathoz tartozó szervezetnek a következő szervezeteket kell tekinteni:

15. a központi **[rendszerek szolgáltatói]**rendszer felett rendelkezési jogot gyakorló szervezet.

Módosítópont sorszáma: **142.**

Törvényjavaslat érintett rendelkezése: **2. melléklet cím**

Módosítás jellege: **módosítás**

[.]2. Kiemelten kockázatos ágazatokban működő szolgáltatók és szervezetek

Módosítópont sorszáma: **143.**
Törvényjavaslat érintett rendelkezése: **2. mellékletben foglalt táblázat 9. sor**
Módosítás jellege: **módosítás**

	A	B	C
...			
9	Közlekedés	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,

Módosítópont sorszáma: **144.**
Törvényjavaslat érintett rendelkezése: **3. mellékletben foglalt táblázat 3. és 4. sor**
Módosítás jellege: **módosítás**

	A	B	C
...			
3	Élelmiszer a) előállítása, 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 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

	A	B	C
			1. melléklete szerinti gazdasági társaságok kivételével,

Indokolás

1. Pontosító módosítás.

2. Pontosító rendelkezés, mert a A DORA rendelet ágazatspecifikus jogszabály a NIS 2 irányelvhez képest, amelyre tekintettel a hatálya alá tartozó szervezetek nem azonosíthatóak a törvény keretében. A DORA rendelet hatálya alá tartozó szervezetek felett a hatósági felügyeletet a Magyar Nemzeti Bank gyakorolja.

3. Nyelvhelyességi és szerkesztési módosítás.

4. Nyelvhelyességi és szerkesztési módosítás.

5. Nyelvhelyességi és szerkesztési módosítás.

6. A 4. § 35. pont törölve arra figyelemmel, hogy az 1. § (1) bekezdés c) pontjában a fogalom már bevezetésre került.

7. Pontosító módosítás.

8. Pontosító módosítás.

9. Pontosító módosítás.

10. Pontosító módosítás.

11. A 4. § 75. pont kiegészítésével jelenik meg a tervezetben a NIS2 irányelv 2. cikk (7) bekezdése szerinti rendelkezés, miszerint az irányelv nem alkalmazandó azokra a közigazgatási szervekre, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés - többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása - területén végzik tevékenységeiket.

12. Nyelvhelyességi és szerkesztési módosítás.

13. Pontosító módosítás.

14. Pontosító módosítás.

15. Nyelvhelyességi és szerkesztési módosítás.

16. Pontosító rendelkezés.

17. Nyelvhelyességi és szerkesztési módosítás.

18. Technikai pontosítás.

19. Nyelvhelyességi és szerkesztési módosítás.

20. Nyelvhelyességi és szerkesztési módosítás.

21. Pontosító rendelkezés.

22. Technikai pontosítás.

23. Pontosító rendelkezés, a 6. § (3) bekezdés 5. pontjában a biztonsági osztályba sorolás vonatkozásában előírt kötelezettséggel összhangban.

24. Nyelvhelyességi és szerkesztési módosítás.

25. Az elektronikus információs rendszer biztonságáért felelős személy összeférhetetlenségével kapcsolatos rendelkezések pontosításra kerülnek.

26. Technikai pontosítás.

27. Technikai pontosítás.

28. A szakasz az elektronikus információs rendszer biztonságáért felelős személy büntetlen előéletére irányuló követelmény ellenőrzésére vonatkozó rendelkezésekkel kerül kiegészítésre.

29. Technikai pontosítás.

30. A bekezdésben a 13. §-ra történő visszahivatkozás pontosításra került.

31. Pontosító rendelkezés.

32. A kiberbiztonsági auditra kötelezett szervezetek köre pontosításra került.

33. Technikai pontosítás, valamint a tervezet egészével, különösen a 6. § (1) és (11) bekezdés szófordulatával való összhang megteremtése.

34. A honvédelmi kiberbiztonsági hatóság és a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) közötti együttműködésre vonatkozó rendelkezésekkel kerül kiegészítésre a szakasz.

35. A központi rendszer szolgáltatója terminológiát érintő módosítás.

36. Pontosító rendelkezések.

37. Pontosító rendelkezések.

38. Pontosító rendelkezések.

39. Pontosító rendelkezések.

40. Nyelvhelyességi és szerkesztési módosítás.

41. Nyelvhelyességi és szerkesztési módosítás.

42. Pontosító rendelkezések.

43. Pontosító rendelkezések.

44. Pontosító rendelkezések.

45. Pontosító rendelkezések.

46. Pontosító rendelkezések.

47. A rendelkezés 11. § (13) bekezdéssel történő kiegészítése összhangban van a 28. § (6) bekezdésének nem alkalmazásával. Erre tekintettel szükséges a 28. § (2) bekezdés felsorolásából a 6. pont elhagyása. Valamennyi rendelkezés az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas személyek nyilvántartására vonatkozik.

48. Technikai pontosítások.

49. A módosító javaslat kiegészítése szükséges annak rögzítésével, hogy az élelmiszerláncról és hatósági felügyeletéről szóló törvény szerinti élelmiszerlánc-felügyeleti szerv minden év február 1. napjáig tájékoztatja az Szabályozott Tevékenységek Felügyeleti Hatóságát a 3. mellékletben foglalt táblázat 3. sora szerinti szervezetek megnevezéséről és székhelyéről.

50. Nyelvhelyességi és szerkesztési módosítás.

51. Technikai pontosítások.

52. Pontosító rendelkezések.

53. A központi rendszer szolgáltatója terminológiát érintő módosítás.

54. A rendelkezés 11. § (13) bekezdéssel történő kiegészítése összhangban van a 28. § (6) bekezdésének nem alkalmazásával. Erre tekintettel szükséges a 28. § (2) bekezdés felsorolásából a 6. pont elhagyása. Valamennyi rendelkezés az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas személyek nyilvántartására vonatkozik.

55. A nemzeti kiberbiztonsági hatóság, valamint a nemzeti kiberbiztonsági incidenskezelő központ által a honvédelmi kiberbiztonsági hatóság nyilvántartásából megismerhető adatok körének a megjelenítésével egészül ki.

56. Nyelvhelyességi és szerkesztési módosítás.

57. Az adattovábbításra jogosult szervezetek köre kerül kiegészítésre.

58. A kiberbiztonsági incidensek kezelése vonatkozásában – a hatályos szabályozáshoz hasonlóan – megteremtésre kerül annak a lehetősége, hogy gazdálkodó szervezet is bevonásra kerülhessen a kiberbiztonsági incidensek kezelésébe. Az incidenskezelést elsősorban a szervezet maga végzi. Ha a szervezet nem maga kezeli az incidenst, az SZTFH felügyeleti tevékenységi körébe tartozó szervezetek gazdálkodó szervezetet vonnak be. A Nemzetbiztonsági Szakszolgálat által felügyelt szervezetek vagy gazdálkodó szervezetet vonnak be vagy az incidenskezelő központhoz fordulhatnak. Az SZTFH felügyeleti tevékenységi körébe tartozó szervezetek akkor fordulhatnak az incidenskezelő központhoz, ha a kiberbiztonsági incidens kezelése meghaladja a gazdálkodó szervezet kapacitásait. Kiemelendő ugyanakkor, hogy a nemzeti kiberbiztonsági incidenskezelő központ megkeresés

esetén is csak a rendelkezésére álló erőforrások függvényében, a veszélyeztetettség mértékének mérlegelésével látja el a kiberbiztonsági incidens kezelését. A kiberbiztonsági incidens kezelésére jogosult gazdálkodó szervezetek nyilvántartását a jövőben az SZTFH vezeti.

59. Nyelvhelyességi és szerkesztési módosítás.

60. Pontosító rendelkezés.

61. A § kiegészül a szervezet vezetőjével szemben alkalmazható szankcionálással.

62. A 31. § (2) bekezdése kiegészül az információbiztonsági felügyelő végzettségére, képzettségére, szakképzettségére vagy szakmai tapasztalatára vonatkozó követelményeknek az informatikáért felelős miniszter rendeletében történő meghatározásával.

63. Nyelvhelyességi és szerkesztési módosítás.

64. Nyelvhelyességi és szerkesztési módosítás.

65. Pontosító rendelkezések.

66. Pontosító rendelkezés.

67. Pontosító rendelkezések.

68. Pontosító rendelkezések.

69. Pontosító rendelkezések.

70. Nyelvhelyességi és szerkesztési módosítás.

71. Nyelvhelyességi és szerkesztési módosítás.

72. Nyelvhelyességi és szerkesztési módosítás.

73. Nyelvhelyességi és szerkesztési módosítás.

74. Nyelvhelyességi és szerkesztési módosítás.

75. Nyelvhelyességi és szerkesztési módosítás.

76. Nyelvhelyességi és szerkesztési módosítás.

77. Nyelvhelyességi és szerkesztési módosítás.

78. Nyelvhelyességi és szerkesztési módosítás.

79. Pontosító rendelkezések.

80. Pontosító rendelkezések.

81. Pontosító rendelkezések.

82. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

83. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

84. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

85. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

86. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

87. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

88. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

89. A kiberbiztonsági incidensek kezeléséhez kapcsolódó rendelkezés.

90. Pontosító rendelkezések.

91. Nyelvhelyességi és szerkesztési módosítás.

92. Nyelvhelyességi és szerkesztési módosítás.

93. Nyelvhelyességi és szerkesztési módosítás.

94. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

95. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

96. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

97. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

98. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

99. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

100. Mivel az alapjogok csak a szükséges és arányos mértékben korlátozhatók, ezért a korlátozásokat törvényi szinten kell szabályozni.

101. Az együttműködéssel érintett szervezetek körét pontosító rendelkezés.

102. Nyelvhelyességi és szerkesztési módosítás.

103. Nyelvhelyességi és szerkesztési módosítás.

104. A 78. § (2) bekezdésben technikai pontosítás. Továbbá a 78. § (3) bekezdés az Ákr. 33. § (5) bekezdése vonatkozásában kívánja meghatározni az iratbetekintésre jogosultak körét azzal, hogy kizárja a hatósági döntés bárki által történő megismerését és a döntés megismerésének lehetőségét az ügyfélen, a tanún és a szemletárgy birtokosán kívül azon személyekre korlátozza, akiknek az irat megismerése joga érvényesítéséhez, illetve jogszabályon, bírósági vagy hatósági határozaton alapuló kötelezettsége teljesítéséhez szükséges. A hatóság a határozatot közli az ügyféllel, azzal, akire nézve az rendelkezést tartalmaz és az ügyben eljárt szakhatósággal. A tervezet 73. § (3) bekezdése az Ákr. közlésre vonatkozó szabályainak módosításával a

szakhatóságot zárja ki a határozat közléséből, de továbbra is megmarad a döntés bárki általi megismerésének lehetősége ezzel veszélyeztetve védett adatok biztonságát. A pont a 31. § (2) bekezdésének módosításához kapcsolódó felhatalmazó rendelkezéssel egészül ki, valamint a „feladatellátáshoz” kifejezés pontosításra kerül.

105. Pontosító rendelkezések.

106. Pontosító rendelkezések.

107. Pontosító rendelkezések.

108. A kiegészítés a 19. § (5) bekezdéséhez fűzött kiegészítéshez kapcsolódó felhatalmazó rendelkezés.

109. A megfelelősségértékelő szervezetekre vonatkozó szabályozás egy normában való összefoglalása.

110. Pontosító rendelkezések.

111. Pontosító rendelkezések.

112. A megfelelősségértékelő szervezetekre vonatkozó szabályozás egy normában való összefoglalása.

113. Technikai pontosítás.

114. Nyelvhelyességi és szerkesztési módosítás.

115. A kiegészítés a 70. §-t érintő módosításokhoz kapcsolódó felhatalmazó rendelkezés.

116. A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § m) pontjának módosításának hatálybalépése napjaként 2025. január 2. napját szükséges rögzíteni.

117. Technikai és nyelvhelyességi pontosítás.

118. Nyelvhelyességi és szerkesztési módosítás.

119. Pontosító rendelkezések.

120. Pontosító rendelkezések.

121. Az átmeneti rendelkezéseket tartalmazó kiegészítés.

122. Az átmeneti rendelkezéseket tartalmazó kiegészítés.

123. Az átmeneti rendelkezéseket tartalmazó kiegészítés.

124. Az átmeneti rendelkezéseket tartalmazó kiegészítés.

125. Technikai pontosítás.

126. Technikai pontosítás.

127. A törvényjavaslat 70. §-a alapján a kiberbiztonsági incidens kezelését az SZTFH által

vezetett nyilvántartásban szereplő gazdálkodó szervezet végezheti. Az incidenskezelési tevékenység a szolgáltatási irányelv hatálya alá tartozó tevékenységnek minősül, amennyiben a tevékenységet díjazás (gazdasági ellenérték) ellenében látják el (szolgáltatási irányelv 4. cikk 1. pont). A szolgáltatási irányelv 15. cikk (2) bekezdés d) pontja szerint a szolgáltatási tevékenység meghatározott szolgáltatók számára való fenntartása korlátozó tevékenységnek minősül, kivéve, ha e korlátozásra más uniós jogi aktus ad lehetőséget. A szolgáltató kijelölése csak akkor áll összhangban a szolgáltatási irányelvvel, ha az irányelv 15. cikk (3) bekezdésében írt együttes feltételek – diszkriminációmentesség, közérdekűség és arányosság – maradéktalanul teljesülnek. A fentiekre figyelemmel a törvényjavaslatot a szolgáltatási irányelvre utaló jogharmonizációs és bejelentési záradékkal el kell látni.

128. A törvényjavaslatot a szolgáltatási irányelvre utaló bejelentési záradékkal el kell látni.

129. A hírközlési törvény javasolt módosítása az szabályozza elektronikus hírközlési építményekkel kapcsolatos hatósági hatásköröket.

130. Az elektronikus hírközlésről szóló 2003. évi C. törvény új 86/B. § (2) bekezdéséhez kapcsolódó kodifikációs pontosítás.

131. A javasolt módosítás a hírközlési hálózatokkal összefüggésben részletes állagmegóvási kötelezettséget ír elő, amely alapján a hálózat üzemeltetője, ennek hiányában a tulajdonosa köteles az építmény állagát megóvni, az élet, a testi épség és az egészség, a köz- és vagyonbiztonság védelme érdekében az építmény műszaki állapotának rendszeres felülvizsgálatát és a szükséges átalakítási, felújítási, helyreállítási munkálatokat elvégezni, továbbá az üzemen vagy használaton kívüli hálózatokat elbontani. Szintén el kell bontani a használaton kívüli vagy a használatra alkalmatlan hálózatokat, amelynek részletes szabályait is tartalmazza a módosítási javaslat. Mindezen kötelezettségeket a hírközlési hatóság felügyeli és e körben hatékony felügyeleti intézkedést, jogkövetkezményt alkalmazhat. Jogsértés esetén ugyanis a hatóság elrendeli az állagmegóvásra, átalakításra, helyreállításra vonatkozó kötelezettség teljesítését, illetve az elektronikus hírközlési építmény bontását, ha annak állapota az állékonyságot, az életet, testi épséget és az egészséget, a köz- és vagyonbiztonságot veszélyezteti, vagy az elektronikus hírközlési építmény használatra alkalmatlan, vagy a használatával véglegesen felhagytak.

132. A javaslat rögzíti azt a főszabályt, hogy 2027. január 1-től belterületen a helyi építési szabályzatokban meghatározott területeken új nyomvonalas elektronikus hírközlési építmény csak földfelszín alatti elhelyezéssel létesíthető.

133. A javaslat rendezi, hogy a helyi önkormányzat az 5 évnél régebben létesített nyomvonalas elektronikus hírközlő hálózat földfelszín alatti elhelyezését, cseréjét kezdeményezheti a helyi építési szabályzatában megjelölt belterületen, ha az érintett előfizetők, az ingatlan tulajdonosok az ingatlanukban szükséges munkavégzéshez előzetesen hozzájárulnak, és annak költségeit vállalják. Mindez természetesen nem zárja ki annak a lehetőségét, hogy a szolgáltatók vagy az önkormányzat az indokolt költségek viselését átvállalják részben vagy egészben. A tervezet a költséghatékonyság érdekében ezért együttműködési megállapodás megkötését írja elő az

érintett szolgáltatók, valamint a szolgáltatók és az önkormányzat tekintetében, amely megállapodás rendezi a költségviselés szabályait. Az önkormányzat kezdeményezése alapján az elektronikus hírközlő hálózat üzemeltetője kiváltási-ütemezési tervet készít annak figyelembevételével, hogy az a szolgáltatásnyújtás folytonosságát ne veszélyeztesse.

A tervezet egyértelműsíti, hogy a villamos hálózat földkábelesítése esetében a hírközlési hálózatra is megfelelően alkalmazandók a villamos energiáról szóló törvény szabályai. E szabály egyúttal a költséghatékony földkábelesítést is biztosítja azáltal, hogy a villamoshálózattal párhuzamosan futó hírközlési hálózatok cseréjére egyidejűleg kerüljön sor, illetve a villamoshálózaton lévő hírközlési légkábeles hálózatok ne akadályozzák a villamoshálózat tényleges elbontását.

134. A javaslat átmeneti rendelkezéseket állapít meg.

135. A javaslat előírja, hogy az elektronikus hírközlési szolgáltatáshoz használt rendszernek rendelkeznie kell a Magyarország kiberbiztonságáról szóló törvény alapján kiállított nemzeti vagy európai kiberbiztonsági tanúsítvánnyal, ha az adott, hírközlési szolgáltatáshoz használt rendszerre vonatkozóan nemzeti vagy európai kiberbiztonsági tanúsítási rendszer meghatározásra került.

A javaslat ehhez kapcsolódóan szabályozza azt, hogy ha a tanúsítási rendszer meghatározásra kerül, annak az elektronikus hírközlési szolgáltatóknak mennyi időn belül kell megfelelniük.

136. A javaslat előírja, hogy az elektronikus hírközlési szolgáltatáshoz használt rendszernek rendelkeznie kell a Magyarország kiberbiztonságáról szóló törvény alapján kiállított nemzeti vagy európai kiberbiztonsági tanúsítvánnyal, ha az adott, hírközlési szolgáltatáshoz használt rendszerre vonatkozóan nemzeti vagy európai kiberbiztonsági tanúsítási rendszer meghatározásra került.

A javaslat ehhez kapcsolódóan szabályozza azt, hogy ha a tanúsítási rendszer meghatározásra kerül, annak az elektronikus hírközlési szolgáltatóknak mennyi időn belül kell megfelelniük.

137. A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § m) pontjának módosítása az egyes házszabályi rendelkezésekről szóló 10/2014. (II. 24.) OGY határozat (a továbbiakban: HHSZ) 42. § b) pontjának felel meg, elfogadása a HHSZ 44. § (1) bekezdés b) pontjában meghatározottak szerint a jogrendszer koherenciájának biztosítását célozza.

138. A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény felhatalmazó rendelkezéseinek kiegészítése indokolt az elektronikus hírközlési szolgáltatáshoz használt rendszerek vonatkozásában alkalmazandó európai vagy nemzeti kiberbiztonsági tanúsítási rendszer meghatározásával.

139. A honvédelmi adatkezelésekről szóló 2022. évi XXI. törvény változásokkal érintett rendelkezésének módosítása más előterjesztés keretében folyamatban van, és ott a módosítási igények lekezelésre kerülnek. Erre figyelemmel a módosító rendelkezés jelen előterjesztésben történő feltüntetése okafogyottá vált.

140. A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény érintett rendelkezésének módosítása más előterjesztés keretében folyamatban van, és ott a módosítási igények lekezelésre kerülnek. Erre figyelemmel a módosító rendelkezés jelen előterjesztésben történő feltüntetése okafogyottá vált.

141. A törvényjavaslat 1. mellékletének pontosítása.

142. A törvényjavaslat 2. mellékletének pontosítása.

143. A törvényjavaslat 2. mellékletének pontosítása.

144. A törvényjavaslat 3. mellékletének pontosítása.