2023. évi ……. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

A társadalom gyors digitális átalakulásával és összekapcsolódásával a hálózati és 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.
Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:

I. Fejezet

Általános rendelkezések

1. §

E törvény alkalmazásában:

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

2. *behatolásvizsgálat*: az információs és kommunikációs technológia (a továbbiakban: IKT) rendszer, valamint a hálózati és információs rendszer gyenge pontjainak feltárása és kihasználhatóságának ellenőrzése a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával,

3. *belső informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik,

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

5. *biztonsági incidens*: olyan esemény, amely sérti vagy veszélyezteti a tárolt, továbbított vagy feldolgozott adatok vagy a hálózati és információs rendszerek által nyújtott vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát,

6. *DNS-szolgáltató:* olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja*:*

a) *authoritatív DNS-szolgáltatás*: a legfelső szintű domain név regisztrátorok által kezelt domain név adatok lekérdezését közvetlenül elvégző szolgáltatás, amely a legfelső szintű domain név nyilvántartó szolgáltatás része,

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

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

7. *domain név*: az internetes kommunikációhoz használt IP cím alfanumerikus karakterekből álló megfelelője,

8. *domainnév regisztrációt végző szolgáltató:* a legfelső szintű domainnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domain regisztrálására,

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

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

11. *felhőszolgáltató:* felhőalapú számítástechnikai szolgáltatást nyújtó szervezet,

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

13. *hálózati és információs rendszer:* az elektronikus hírközlő hálózat, valamint minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi vagy a működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok,

14. *IKT-folyamat*: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

15. *IKT-szolgáltatás*: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

16. *IKT-termék*: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

17. *kiberbiztonsági audit*: a hálózati és információs rendszerek tekintetében a kiberbiztonsági követelmények teljesülésére vonatkozó vizsgálat, ellenőrzés,

18. *kiberfenyegetés:* az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

19. *közösségi média szolgáltatási platform*: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással,

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

21. *legfelső szintű domainnév-nyilvántartó:* olyan szervezet, amelyre egy meghatározott legfelső szintű domaint bíztak és amely felelős egyrészt a legfelső szintű domain kezeléséért – ideértve a legfelső szintű domain alatti domain nevek nyilvántartásba vételét –, másrészt a legfelső szintű domain technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű domain zónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű domainneveket a nyilvántartó kizárólag saját használatra veszi igénybe,

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

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

24. *megfelelőségi nyilatkozat*: a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték,

hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek,

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

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

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

28. *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, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal,

29. *rendelkezésre állás*: annak biztosítása, hogy a hálózati és információs rendszerek az arra jogosult személy számára elérhetőek és az azokban kezelt adatok felhasználhatóak legyenek,

30. *sértetlenség*: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik és a származás ellenőrizhetőségét, bizonyosságát is, valamint a hálózati és információs rendszer elemeinek azon tulajdonságát, amely biztosítja, hogy a hálózati és információs rendszer eleme rendeltetésének megfelelően használható,

31. *tanúsítás*: független harmadik fél által végzett megfelelőségértékelési tevékenység,

32. *tartalomszolgáltató hálózat szolgáltatója*: a digitális tartalmak és szolgáltatások széleskörű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója,

33. *távoli sérülékenységvizsgálat*: olyan informatikai biztonsági vizsgálat, amelynek során

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

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

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

2. §

Az e törvény hatálya alá tartozó hatósági eljárásokban az általános közigazgatási rendtartásról szóló törvény rendelkezéseit az e törvényben, a fogyasztóvédelemről szóló törvényben, a termékek piacfelügyeletéről szóló törvényben és a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló törvényben foglalt eltérésekkel és kiegészítésekkel, valamint a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló kormányrendeletben és a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) elnöke által kiadott rendeletben foglalt kiegészítésekkel kell alkalmazni.

II. Fejezet

Tanúsítási Rendszerek

1. A tanúsító hatóság feladatai

3. §

(1) Az e fejezetben foglaltakat IKT-termék, IKT-szolgáltatás vagy IKT-folyamat tanúsításával kapcsolatos hatósági tevékenységre kell alkalmazni.

(2) Az e fejezetben szabályozott kiberbiztonsági tanúsításra, valamint a tanúsító szervezet tevékenységére nem kell alkalmazni a megfelelőségértékelő szervezetek tevékenységéről szóló törvény rendelkezéseit.

4. §

(1) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet szerinti nemzeti kiberbiztonsági tanúsító hatóság (a továbbiakban: tanúsító hatóság) feladatait

a) – a *b)* pont kivételével – az SZTFH,
b) a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság

látja el.

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

5. §

(1) A tanúsító hatóság az európai kiberbiztonsági tanúsítási rendszerekkel kapcsolatosan

a) nyomon követi az európai kiberbiztonsági tanúsítási rendszerek fejlesztését és figyelemmel kíséri a kapcsolódó szabványosítási folyamatokat,
b) részt vesz az európai kiberbiztonsági tanúsítási csoport tevékenységében,
c) információkat gyűjt azokról az ágazatokról és szakterületekről, amelyek nem esnek európai kiberbiztonsági tanúsítási rendszer hatálya alá és amelyek esetében a kiberbiztonság növelése szükséges,
d) az érdekelt feleknek szükség esetén tájékoztatást, támogatást nyújt a tanúsítási rendszerekkel kapcsolatban,
e) elvégzi az (EU) 2019/881 európai parlamenti és tanácsi rendelet 57. cikk (4) bekezdése szerinti bejelentést.

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

a) legalább háromévente értékeli a hatályos nemzeti kiberbiztonsági tanúsítási rendszereket,
b) felülvizsgálatot megalapozó ok felmerülését követően haladéktalanul intézkedik a nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata érdekében,
c) európai kiberbiztonsági tanúsítási rendszer kiadása esetén haladéktalanul intézkedik az azonos tárgyú nemzeti kiberbiztonsági tanúsítási rendszer felülvizsgálata, hatályon kívül helyezése érdekében.

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

2. A nemzeti kiberbiztonsági tanúsítási rendszerek követelményei

6. §

A nemzeti kiberbiztonsági tanúsítási rendszernek a következő biztonsági célokat kell teljesítenie:

a) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan tárolással, kezeléssel, hozzáféréssel és közléssel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,
b) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan megsemmisítéssel, elvesztéssel, megváltoztatással vagy a hozzáférhetetlenséggel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,
c) a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá,
d) az ismert függőségek és sebezhetőségek azonosítása és dokumentálása,
e) annak rögzítése, hogy ki, mikor és mely védendő adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,
f) annak ellenőrizhetővé tétele, hogy ki, mikor és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,
g) annak ellenőrzése, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok nem tartalmaznak-e ismert sebezhetőségeket,
h) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állásának, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása,
i) az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok alapértelmezetten és tervezetten biztonságosak,
j) az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok szoftvere és hardvere naprakész, esetükben nem állnak fenn közismert sebezhetőségek és rendelkezésre állnak a biztonságos frissítésükre szolgáló mechanizmusok.

7. §

(1) A nemzeti kiberbiztonsági tanúsítási rendszernek tartalmaznia kell:

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

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

c) hivatkozást az értékelésben alkalmazott nemzetközi, európai vagy nemzeti szabványokra, vagy ha nem állnak rendelkezésre ilyen szabványok vagy azok nem megfelelőek, az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet II. mellékletében meghatározott követelményeket teljesítő műszaki előírásokra, vagy ha ilyen előírások nem állnak rendelkezésre, az európai kiberbiztonsági tanúsítási rendszerben meghatározott műszaki előírásra vagy egyéb kiberbiztonsági követelményekre való hivatkozást,

d) a megbízhatósági szintet vagy szinteket,

e) a megfelelőségi önértékelésre vonatkozó rendelkezést,

f) a megfelelőségértékelést végző személyekre, szervezetekre alkalmazandó konkrét vagy kiegészítő követelményeket,

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

h) a jelölések vagy címkék használati feltételeit,

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

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

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

(3) A nemzeti kiberbiztonsági tanúsítási rendszerben meg kell határozni

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

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

c) az értékelési eredmények dokumentálására vonatkozó követelményeket.

3. A nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjei

8. §

(1) A nemzeti kiberbiztonsági tanúsítási rendszerek az IKT-termékekre, az IKT-szolgáltatásokra és az IKT-folyamatokra az „alap”, a „jelentős” és a „magas” megbízhatósági szintek közül egy vagy több szintet határozhatnak meg.

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

a) alap megbízhatósági szinten a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok,
b) jelentős megbízhatósági szinten az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások kockázatának,
c) magas megbízhatósági szinten a jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások kockázatának

minimalizálására törekszik.

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

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

a) „alap” megbízhatósági szint esetén a műszaki dokumentáció áttekintését az adott tanúsítási rendszer elvárásainak teljesítése szempontjából,
b) „jelentős” megbízhatósági szint esetén
ba) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát és
bb) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően működteti-e a szükséges biztonsági funkciókat,
c) „magas” megbízhatósági szint esetén
ca) a közismert sebezhetőségek hiánya megállapításának felülvizsgálatát,
cb) az annak megállapítására szolgáló tesztelést, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat megfelelően, a legfejlettebb technika szerint működteti-e a szükséges biztonsági funkciókat, valamint
cc) behatolásvizsgálatok révén annak értékelését, hogy az mennyire ellenálló a jól képzett elkövetők által végrehajtott támadásokkal szemben.

4. A kiberbiztonsági tanúsítványokkal és a megfelelőségi nyilatkozatokkal kapcsolatos elvárások

9. §

(1) A nemzeti kiberbiztonsági tanúsítványban és a nemzeti megfelelőségi nyilatkozatban meg kell jelölni:

a) azt a nemzeti kiberbiztonsági tanúsítási rendszert, amely alapján a tanúsítvány vagy a nyilatkozat kiállításra került,
b) a megbízhatósági szintet és
c) a vonatkozó műszaki előírásokat, szabványokat, eljárásokat.

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

a) a kiállító szervezet nevét, címét,
b) a kiállítás dátumát,
c) az IKT-termék gyártója, az IKT-szolgáltatás nyújtója, az IKT-folyamat fejlesztője nevét és címét,
d) a megfelelőségértékelés megbízóját,
e) az alkalmazási területeket, vagy ha az adott alkalmazási területeken a megfelelőség feltételekkel érvényes, ezen feltételeket,
f) az érvényességi időt,
g) a tanúsítás tárgyát képező IKT-termék, IKT-szolgáltatás és IKT-folyamat azonosítását, ha van, verziószámát, valamint
h) a megfelelőségértékelő aláírását.

5. Megfelelőségi önértékelés, megfelelőségértékelés

10. §

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

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

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

11. §

Harmadik fél által végzett megfelelőségértékelési tevékenységet csak olyan szervezet végezhet, amelyet

a) a vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszerben meghatározott követelményekre figyelemmel a nemzeti akkreditálásról szóló törvény szerint kijelölt akkreditáló szerv akkreditált vagy külföldi akkreditált státusz esetén e státuszát elismerte és
b) a tanúsító hatóság nyilvántartásba vett.

6. A kiberbiztonsági tanúsítás felügyelete

12. §

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

(2) A tanúsító hatóság ügyintézési határideje 120 nap.

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

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

a) konkrét vagy kiegészítő követelményeket ír elő és ez alapján engedélyezési eljárás lefolytatása válik szükségessé, vagy
b) „magas” megbízhatósági szintet ír elő a rendszer keretében kiadandó kiberbiztonsági tanúsítványra és a tanúsító hatóság az ilyen tanúsítvány kiállításának feladatát egyes nemzeti vagy európai kiberbiztonsági tanúsítványok vonatkozásában vagy általános jelleggel átruházza a megfelelőségértékelő szervezetre.

(5) A (4) bekezdés *b)* pontja szerinti esetben az engedély megadásának feltétele, hogy a megfelelőségértékelő szervezet szerepeljen a védelmi és biztonsági célú beszerzésekről szóló törvényben meghatározott jegyzéken.

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

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

(8) Az egyes tanúsító hatósági eljárásokért igazgatási szolgáltatási díjat kell fizetni. Az igazgatási szolgáltatási díj mértékét és az annak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat

a) a 4. § (1) bekezdés *a)* pontja szerinti tanúsító hatóság által lefolytatott eljárások esetében az SZTFH elnökének a nemzeti kiberbiztonsági tanúsító hatóság eljárásával összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról szóló rendelete,
b) a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság által lefolytatott eljárások esetében az e törvény végrehajtására kiadott miniszteri rendelet

határozza meg.

13. §

(1) A tanúsító hatóság nyilvántartja és kezeli:

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

b) a megfelelőségi nyilatkozathoz benyújtott műszaki dokumentációt és az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok tanúsítási rendszernek való megfelelésével kapcsolatos összes egyéb lényeges információt,

c) a nemzeti akkreditáló szerv által akkreditált megfelelőségértékelő szervezet és annak kijelölt kapcsolattartója azonosításához szükséges adatokat, valamint ha a megfelelőségértékelő szervezet egyben az (EU) 2019/881 európai parlamenti és tanácsi rendelet 56. cikk (5) bekezdése szerinti közjogi szerv, ennek tényét,

d) az akkreditált státuszra vonatkozó határozatban foglalt, valamint az akkreditált státusz változására vonatkozó információkat,

e) ha a 12. § (4) bekezdése szerinti engedélyezési eljárás lefolytatása szükséges, akkor az azzal kapcsolatos kérelmet, adatokat, dokumentumokat,

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

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

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

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

j) a megfelelőségértékelő szervezet által kiadott tanúsítvány, valamint a tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat azonosításához szükséges adatokat,

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

l) a megfelelőségértékelő szervezet tájékoztatását a tanúsítvány kiállításának megtagadásáról, hatályának korlátozásáról vagy felfüggesztéséről és a tanúsítvány visszavonásáról,

m) a tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságát érintő, utólag észlelt sebezhetőséggel vagy rendellenességgel kapcsolatos információt,

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

o) a benyújtott panaszokkal kapcsolatos adatokat, dokumentumokat.

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

(3) Az (1) bekezdés szerinti adatok kezelésének célja a tanúsított IKT-termékkel, IKT-szolgáltatással vagy IKT-folyamattal kapcsolatos tanúsító hatósági tevékenység ellátása.

(4) Az (1) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – a következő szervezetek részére végezhető adattovábbítás:

a) a Bizottság részére a bejelentett megfelelőségértékelő szervezetek jegyzékének összeállítása, frissítése,

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

c) az állami és önkormányzat szervek elektronikus információbiztonságáról szóló törvény szerinti eseménykezelő központok részére a tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságát érintő, utólag észlelt sebezhetőséggel vagy rendellenességgel kapcsolatos tevékenység ellátása

érdekében.

(5) A megfelelőségértékelő szervezet és a gyártó az (1) bekezdés szerinti adatokat és azok változásait 8 napon belül megküldi a tanúsító hatóság részére a nyilvántartásba vétel érdekében.

14. §

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

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

15. §

(1) A tanúsító hatóság a feladatellátása során megismert minősített adatot, személyes adatot vagy különleges adatot, valamint az üzleti titoknak, banktitoknak, fizetési titoknak, biztosítási titoknak, értékpapírtitoknak, pénztártitoknak, orvosi titoknak és más hivatás gyakorlásához kötött titoknak minősülő és törvény által védett egyéb adatot kizárólag a feladat ellátásának időtartama alatt, a célhoz kötöttség elvének figyelembevételével kezeli. A tanúsító hatóság a hatósági ellenőrzés eredményeként tett megállapításokat alátámasztó adatokat rögzíti, és az így rögzített adatokat a megfelelőségértékelő szervezet akkreditált státuszának megszűnését követő 10. év utolsó napjáig, ennek hiányában a gyártó által kiadott uniós megfelelőségi nyilatkozat hatályosságának megszűnését követő 10. év utolsó napjáig kezeli. Ezt követően a tanúsító hatóság az adatokat a hálózati és információs rendszereiből és adathordozóiról törli.

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

(3) A tanúsító hatóság munkatársait az (1) bekezdés szerint megismert adatok tekintetében – a jogszabályban meghatározott kivételekkel – titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követő 5 évig, minősített adatok tekintetében azok érvényességi idejének végéig, személyes adatok tekintetében pedig időkorlát nélkül fennmarad.

(4) A tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárás, a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó

adattartamát az SZTFH elnöke – a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletben állapítja meg.

(5) A megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és tevékenységére vonatkozó részletes szabályokat az SZTFH elnöke – a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság tekintetében a Kormány – rendeletben állapítja meg.

III. Fejezet

Kiberbiztonsági felügyelet

7. A kiberbiztonsági felügyelettel érintettek köre

16. §

(1) Az e fejezetben foglaltakat

a) az *1. melléklet* szerinti magas kockázatú ágazatokban működő szolgáltatók és szervezetek, valamint
b) a *2. melléklet* szerinti jelentős kockázatú ágazatokban működő szolgáltatók és szervezetek

hálózati és információs rendszereire kell alkalmazni.

(2) Az e fejezetben foglalt szabályokat nem kell alkalmazni a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti mikro- és kisvállalkozásokra, kivéve, ha az (1) bekezdés *a)* és *b)* pontja szerinti szolgáltató vagy szervezet (a továbbiakban együtt: érintett szervezet)

a) elektronikus hírközlési szolgáltató,
b) bizalmi szolgáltató,
c) DNS-szolgáltatást nyújtó szolgáltató,
d) legfelső szintű domainnév-nyilvántartó,
e) domainnév regisztrációt végző szolgáltató.

(3) Az e fejezetben foglalt szabályokat nem kell alkalmazni az (1) bekezdés szerinti szervezeteknek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti honvédelmi célú elektronikus információs rendszereire és hálózataira.

17. §

Az e fejezetben foglalt szabályokat nem kell alkalmazni az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló törvény szerinti európai vagy nemzeti létfontosságú rendszerelemmé – a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján – kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő elektronikus információs rendszereinek, illetve az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló kormányrendelet hatálya alá tartozó programozható rendszerek védelmére.

8. Alapvető követelmények

18. §

(1) Az érintett szervezet a kiberfenyegetések által okozható károk mértékével arányos módon köteles gondoskodni a hálózati és információs rendszerei és azok fizikai környezetének a biztonságáról.

(2) Az (1) bekezdés szerinti biztonság magában foglalja a hálózati és információs rendszerek, valamint fizikai környezetük védelmét minden olyan eseménytől, amely veszélyeztetheti

a) a tárolt, továbbított vagy feldolgozott adatok, információk vagy
b) a hálózati és információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások

bizalmasságát, sértetlenségét és rendelkezésre állását.

(3) A (2) bekezdésben meghatározott védelemnek ki kell terjednie:

a) az információbiztonsági irányítás rendszerére,
b) a hálózati és információs rendszerek kockázatainak feltárására és kezelésére,
c) a kockázatok csökkentésére irányuló, a szervezet kockázatelemzésében rendszerenként meghatározandó biztonsági osztálynak megfelelő adminisztratív, logikai és fizikai intézkedések alkalmazására,
d) a biztonsági incidensek megelőzésére, felismerésére, kezelésére és hatásainak csökkentésére,
e) az üzletmenet folytonosság biztosítására és
f) a hálózati és információs rendszerek és az ezek által használt szoftver és hardver termékek beszerzésére, fejlesztésére, üzemeltetésére.

(4) Ha az érintett szervezet a hálózati és információs rendszer létrehozásában, üzemeltetésében, karbantartásában vagy javításában közreműködőt vesz igénybe, a (3) bekezdés szerinti követelményeknek a közreműködő esetében is teljesülniük kell.

(5) Az érintett szervezet vezetője köteles gondoskodni arról, hogy a (2) bekezdés szerinti követelményeket a (4) bekezdés szerinti közreműködő tekintetében szerződésbe foglalják.

(6) Az érintett szervezet vezetője

a) meghatározza a hálózati és információs rendszerek biztonságáért felelős személy feladatait és felelősségi körét,
b) meghatározza a hálózati és információs rendszerek felhasználóira vonatkozó szabályokat és
c) gondoskodik a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról.

19. §

(1) Az érintett szervezet köteles a hálózati és információs rendszereket, valamint az azon tárolt, továbbított vagy feldolgozott adatokat az SZTFH elnökének rendeletében meghatározott szempontrendszer alapján biztonsági osztályba sorolni.

(2) A biztonsági osztályba sorolás eredményeként a bizalmasság, a sértetlenség, a rendelkezésre állás sérülésének kockázata alapján „alap”, „jelentős” vagy „magas” biztonsági osztályt kell alkalmazni.

(3) Az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket az SZTFH elnöke rendeletben határozza meg.

(4) A 18. § (1)-(4) bekezdésében meghatározott egyes követelményeknek való megfelelés igazolására – ha rendelkezésre áll – európai vagy nemzeti tanúsítási rendszer alapján tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat alkalmazható.

(5) Az SZTFH elnökének rendeletében meghatározott érintett szervezetek kötelesek az európai vagy nemzeti tanúsítási rendszer alapján tanúsított, az SZTFH elnökének rendeletében meghatározott IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot használni.

20. §

(1) A legfelső szintű domain alatt bejegyzett domain nevekről a legfelső szintű domainnév-nyilvántartó központi nyilvántartást vezet.

(2) A központi domainnév nyilvántartás tartalmazza:

a) az érintett domain nevet,
b) a nyilvántartásba vétel dátumát,
c) a regisztráló nevét, kapcsolattartásra alkalmas elektronikus levelezési címét, telefonszámát és
d) a domain nevet kezelő személy, mint kapcsolattartó pont nevét, elektronikus levelezési címét és telefonszámát, ha eltér a regisztráló adataitól.

(3) A központi domainnév nyilvántartás adatai hitelességének ellenőrzése és integritásának biztosítása érdekében a legfelső szintű domainnév-nyilvántartó köteles eljárásrendet kidolgozni és azt – az SZTFH által előzetesen jóváhagyott – szabályzatban nyilvánosan közzétenni.

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

(5) A legfelső szintű domainnév-nyilvántartó a központi domainnév nyilvántartásban szereplő adatokhoz az ügyészség, a nemzetbiztonsági szolgálatok, a nyomozó hatóságok és az előkészítő eljárást folytató szervezetek részére közvetlen hozzáférést biztosít.

9. Kiberbiztonsági felügyeleti eszközök

21. §

(1) Az érintett szervezetek, valamint azok hálózati és információs rendszerei kiberbiztonsági felügyeletét az SZTFH látja el az SZTFH elnökének rendeletében foglaltak szerint. Az érintett szervezet e fejezetben meghatározott kötelezettségeinek teljesítését az SZTFH ellenőrzi az SZTFH elnökének rendeletében foglaltak szerint.

(2) Az SZTFH felügyeleti jogkörében az érintett szervezet tekintetében:

a) hatósági ellenőrzést végezhet,
b) súlyos biztonsági incidens bekövetkezése vagy a biztonsági követelményeknek való nem-megfelelés gyanúja esetén rendkívüli ellenőrzést hajthat végre vagy rendkívüli auditot rendelhet el vagy
c) az informatikai rendszer sérülékenységeit célszoftverek segítségével feltérképezheti.

(3) Az SZTFH a 18. §-ban és a 19. §-ban foglalt követelmények betartásának ellenőrzését

a) a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény alapján mikro- és kisvállalkozásnak minősülő
aa) elektronikus hírközlési szolgáltató,
ab) bizalmi szolgáltató,
ac) DNS-szolgáltatást nyújtó szolgáltató,
ad) legfelső szintű domainnév-nyilvántartó,
b) a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény alapján mikro- és kisvállalkozásnak nem minősülő, *1. melléklet* szerinti szervezet és
c) a domainnév regisztrációt végző szolgáltató

esetében kockázatértékelésen alapuló éves ellenőrzési terv alapján végzi.

(4) Az SZTFH eljárása során a sommás eljárás alkalmazása kizárt.

(5) Az SZTFH által lefolytatott hatósági ellenőrzés ügyintézési határideje 120 nap.

(6) Az SZTFH a cél megjelölésével jogosult az érintett szervezettől bekérni és megismerni:

a) a biztonsági osztályba sorolás, valamint a biztonsági intézkedések megfelelőségét alátámasztó dokumentumokat,
b) a belső informatikai biztonsági vizsgálat végrehajtásáról készült dokumentumot,
c) bármely egyéb adatot, információt, dokumentumot a felügyeleti feladatok elvégzése céljából.

22. §

(1) Az érintett szervezet az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles kétévente a tevékenység végzésére jogosult, független auditor (a továbbiakban: auditor) által kiberbiztonsági auditot végeztetni.

(2) Az auditor az audit végrehajtása során a tevékenység nyomon követésére alkalmas módon elvégzi a következőket:

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

b) kriptográfiai megfelelőségvizsgálatot, valamint
c) „jelentős” vagy „magas” biztonsági osztály esetén a kritikus biztonsági funkciókat végző egyedileg fejlesztett szoftverek biztonsági forráskód-vizsgálatát.

(3) Kiberbiztonsági auditot a feladat ellátásához szükséges szakértelemmel és infrastrukturális feltételekkel rendelkező, valamint a védelmi és biztonsági célú beszerzésekről szóló törvényben meghatározott jegyzéken szereplő auditor végezhet. Az auditorral szemben támasztott követelményeket, valamint a kiberbiztonsági audit lefolytatásának rendjét, és az audit – általános forgalmi adó nélkül számított – legmagasabb díját az SZTFH elnöke rendeletben határozza meg.

(4) Az audit végrehajtására jogosult gazdálkodó szervezetekről az SZTFH nyilvántartást vezet az SZTFH elnökének rendeletében foglaltak szerint.

(5) A nyilvántartás tartalmazza:

a) az auditor adatait és annak kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát, elektronikus levelezési címét,
b) az auditor nyilvántartásba vételekor adott azonosító számot,
c) az auditor által igénybe vett közreműködő adatait, valamint kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát, elektronikus levelezési címét,
d) az audit eredményét tartalmazó dokumentumot.

(6) Az (1) bekezdés szerinti audit eredményét az auditor az SZTFH és az érintett szervezet részére az audit befejezését követően haladéktalanul megküldi.

(7) Az auditor írásban haladéktalanul tájékoztatja az SZTFH-t, ha az érintett szervezet hálózati és információs rendszerével kapcsolatosan olyan tényt állapít meg, amely a szervezet folyamatos működését súlyosan veszélyezteti vagy bűncselekmény elkövetésére, jogszabály megsértésére vagy az érintett szervezet belső szabályzatának súlyos megsértésére vagy ezek veszélyére utaló körülményeket észlel.

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

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

(10) Az e fejezet szerinti kiberbiztonsági audit nem érinti a más jogszabály által előírt tanúsítási kötelezettséget.

23. §

(1) Ha az érintett szervezet a jogszabályokban foglalt kiberbiztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, az SZTFH jogosult

a) figyelmeztetni az érintett szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,
b) határidő tűzésével elrendelni az ellenőrzés vagy az audit során feltárt vagy tudomására jutott biztonsági hiányosságok elhárítását vagy a megfeleléshez szükséges intézkedések meghozatalát,
c) a szervezet tevékenységét engedélyező vagy felügyelő hatóság véleményét figyelembe véve eltiltani az érintett szervezetet a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységtől.

(2) Ha az (1) bekezdés szerinti intézkedések alkalmazása ellenére az érintett szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, a biztonsági hiányosságokat nem hárítja el vagy a tevékenységet nem hagyja abba, az SZTFH az eset összes körülményének mérlegelésével kormányrendeletben meghatározottak szerint bírságot szabhat ki, amely további nemteljesítés esetén megismételhető.

(3) A (2) bekezdés szerinti esetben a bírság kiszabásáról és a kiszabást megalapozó tényekről az SZTFH tájékoztatja a szervezet tevékenységét engedélyező vagy felügyelő hatóságot.

(4) Az SZTFH elrendelheti az érintett szervezet által nyújtott szolgáltatásokat igénybe vevők tájékoztatását az azokat potenciális érintő fenyegetésről vagy az ilyen fenyegetés elhárításához szükséges megelőző intézkedések várható hatásairól.

24. §

(1) Az SZTFH kiberbiztonsági felügyeleti tevékenységéért – a költségvetési szervek kivételével – az érintett szervezet az SZTFH elnökének rendeletében a (2) bekezdésben foglaltak alapján meghatározott mértékű kiberbiztonsági felügyeleti díj fizetésére köteles.

(2) A kiberbiztonsági felügyeleti díj mértéke az *1.* és a *2. mellékletben* felsorolt szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – legfeljebb 0,15 százaléka.

(3) A kiberbiztonsági felügyeleti díjat az érintett szervezet az SZTFH elnökének rendeletében meghatározott időpontban köteles megfizetni az SZTFH részére a felügyeleti díj megfizetéséről szóló nyilatkozat (a továbbiakban: nyilatkozat) egyidejű benyújtása mellett. A felügyeleti díj megfizetése a nyilatkozattételi kötelezettséget nem pótolja.

25. §

(1) Az SZTFH az SZTFH elnökének rendeletében foglaltak szerint az érintett szervezetekről nyilvántartást vezet, amely tartalmazza:

a) az érintett szervezet azonosításához szükséges adatokat,

b) ha az érintett 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,
c) a hálózati és információs rendszer biztonságáért felelős személy természetes személyazonosító adatait, telefonszámát, elektronikus levelezési címét,
d) az SZTFH elnökének rendeletében előírt további, személyes adatnak nem minősülő adatokat.

(2) Az érintett szervezet a működése megkezdését követő 30 napon belül az (1) bekezdésben meghatározott adatokat megküldi az SZTFH-nak a nyilvántartásba vétel érdekében.

(3) Az érintett szervezet az (1) bekezdés szerinti adatokban bekövetkező változást a változás bekövetkezésétől számított 15 napon belül megküldi a nyilvántartásba vétel érdekében.

(4) Az (1) bekezdés szerinti nyilvántartásból – ha jogszabály eltérően nem rendelkezik – adattovábbítás kizárólag az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott hatósági feladatokat ellátó szervezet, valamint eseménykezelő központok részére végezhető.

(5) Ha az érintett szervezet e törvény hatálya alá tartozó tevékenységet már nem végez, akkor az (1) bekezdés szerinti adatokat az SZTFH a tevékenység befejezésének bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(6) Ha az (1) bekezdés szerinti adatok változását az érintett szervezet bejelenti, akkor az eredeti adatokat az SZTFH az adat változása bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

10. Kiberbiztonsági incidensek jelentése

26. §

(1) Ha a hálózati és információs rendszerben olyan súlyos biztonsági incidens történt vagy annak közvetlen bekövetkezése fenyeget, amely

a) az érintett szervezet működésében vagy az általa végzett szolgáltatásnyújtásban súlyos zavart vagy vagyoni kárt okoz vagy
b) jelentős vagyoni vagy nem vagyoni kárt okoz más természetes vagy jogi személyek számára,

az érintett szervezet köteles haladéktalanul az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerinti eseménykezelő központ részére a Kormány rendeletében részletezettek szerint bejelentést tenni.

(2) A biztonsági incidensek kezelésének és műszaki vizsgálatának, valamint az eseménykezelő központ részére történő bejelentésének részletes szabályait a Kormány rendeletben határozza meg.

(3) Ha a szervezet a biztonsági incidensek kezeléséhez közreműködőt vesz igénybe, a közreműködőnek az SZTFH által – az SZTFH elnökének rendeletében foglaltak szerint –

kiállított tanúsítvánnyal kell rendelkeznie a (2) bekezdés szerinti, a biztonsági incidensek kezelésére vonatkozó szabályoknak történő megfelelésről, valamint a biztonsági incidensek kezeléséhez szükséges, az SZTFH elnökének rendeletében meghatározott feltételek teljesüléséről.

(4) Az (1) bekezdésben foglaltak nem érintik a más törvény alapján fennálló jelentési kötelezettségeket.

IV. Fejezet

Záró rendelkezések

11. Felhatalmazó rendelkezések

27. §

(1) Felhatalmazást kap a Kormány, hogy rendeletben meghatározza

a) a tanúsító hatóság által kiszabható bírság mértékét, megállapításának szempontrendszerét, valamint a bírság kiszabásának és befizetésének részletes eljárási szabályait,
b) 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság feladatának, a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárás, a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartamát,
c) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és tevékenységére vonatkozó részletes szabályokat,
d) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a nemzeti kiberbiztonsági tanúsítási rendszerekre figyelemmel a tanúsítási rendszereket,
e) a biztonsági incidensek kezelésére, műszaki vizsgálatára és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti eseménykezelő központ részére történő bejelentésére vonatkozó részletes szabályokat,
f) a kiberbiztonsági felügyeletet ellátó hatóság által kiszabható bírság mértékét, a bírság kiszabásának és befizetésének részletes eljárási szabályait.

(2) Felhatalmazást kap a Kormány, hogy rendeletben kijelölje a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóságot.

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

a) a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság kivételével a tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak és a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartamát,
b) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és azok tevékenységére vonatkozó részletes szabályokat,
c) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket,
d) a nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok alkalmazására kötelezett szervezeteket,

e) a kiberbiztonsági felügyelet és feladatellátás, továbbá a hatósági ellenőrzés lefolytatásának és az éves ellenőrzési terv elkészítésének részletes szabályait,

f) az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásba vételének rendjét, valamint a nyilvántartás személyes adatnak nem minősülő adattartalmára vonatkozó részletes szabályokat,

g) a biztonsági incidenskezelésben résztvevő közreműködők esetében a biztonsági incidensek kezeléséhez szükséges feltételeket, valamint a biztonsági incidenskezelésben résztvevő közreműködőknek a biztonsági incidensek kezelésére vonatkozó szabályoknak és a biztonsági incidensek kezeléséhez szükséges feltételeknek történő megfelelés tanúsítására vonatkozó részletes szabályokat,

h) a kiberbiztonsági audit lefolytatásának rendjét, az auditorok nyilvántartásba vételi eljárásának rendjét, az auditorral szemben támasztott szakmai követelményeket, valamint a kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját,

i) a biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket,

j) a kiberbiztonsági felügyeleti díj mértékét és megfizetésének időpontját.

(4) Felhatalmazást kap a honvédelemért felelős miniszter, hogy rendeletben meghatározza

a) az adópolitikáért felelős miniszterrel egyetértésben a 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatóság eljárásért fizetendő igazgatási szolgáltatási díj mértékét, a díjak beszedésével, megosztásával, kezelésével, nyilvántartásával és visszatérítésével kapcsolatos részletes szabályokat,

b) a hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében a megfelelőségértékelő szervezet által teljesítendő követelményeket.

12. Hatályba léptető rendelkezés

28. §

(1) Ez a törvény – a (2)-(4) bekezdésben foglalt kivétellel – 2023. április 1-jén lép hatályba.

(2) A 7. alcím, a 19. §, a 21. § (1) bekezdése, a 25. §, a 27. § (3) bekezdés *f)* pontja és a 29. § 2024. január 1-jén lép hatályba.

(3) A 18. §, a 21. § (2)-(4) bekezdése, a 22-24. §, a 24. § (2)-(8) bekezdése, a 10. alcím, a 27. § (1) bekezdés *e)* és *f)* pontja, a 27. § (3) bekezdés *d), e)* és *g)-j)* pontja, a 32-36. §, a 37. § *a)* és *c)* pontja, a 39. §, a 41. §, a 43. § és a 45. § 2024. július 1-jén lép hatályba.

(4) A 48. § 2024. október 18-án lép hatályba.

13. Átmeneti rendelkezések

29. §

(1) Az SZTFH felügyeleti jogkörében 2024. január 1-jétől az SZTFH elnökének rendeletében foglaltak szerint a 16. § (1) bekezdése szerinti érintett szervezetekről a 25. § (1) bekezdése alapján nyilvántartást vezet.

(2) A 16. § (1) bekezdésének hatályba lépésekor érintett szervezetnek minősülő szervezet a 25. § (1) bekezdésében meghatározott adatokat első alkalommal 2024. június 30-ig küldi meg a hatóságnak a nyilvántartásba vétel érdekében.

14. Az Alaptörvény sarkalatosságra vonatkozó követelményének való megfelelés

30. §

A 38-41. §, a 44. §, a 45. § és a 47. § az Alaptörvény 23. cikke alapján sarkalatosnak minősül.

15. Az Európai Unió jogának való megfelelés

31. §

(1) Ez a törvény az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet végrehajtásához szükséges rendelkezéseket állapít meg.

(2) Ez a törvény 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 szóló, 2022. december 14-i, (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

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

16. Módosító rendelkezések

32. §

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 15/B. § (4) bekezdése helyébe a következő rendelkezés lép:

„(4) A Kormány által rendeletben kijelölt hatóság kormányrendeletben meghatározott mértékű bírságot szabhat ki, ha a közvetítő szolgáltató nem teljesíti a (3) bekezdés szerinti feladatait.”

33. §

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 17. § (1a) bekezdés *g)* pontja helyébe a következő rendelkezés lép:

(Felhatalmazást kap a Kormány, hogy)

„*g)* rendeletben határozza meg a közvetítő szolgáltatónak a biztonsági események kezelésével és kivizsgálásával kapcsolatos feladatait, kijelölje a 15/B. § (4) bekezdése szerinti hatóságot, valamint a 15/B. § (4) bekezdése szerint kiszabható bírság mértékét, a bírság megállapításának szempontrendszerét és a bírság megfizetése módjának részletszabályait.”

34. §

Hatályát veszti az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény

a) 2. § *j)* pontja,
b) az „A bejelentés-köteles szolgáltatásokra vonatkozó különös szabályok” alcím címe,
c) 6/A-6/D. §-a,
d) 17. § (1a) bekezdés *a)-f)* pontja,
e) 18. § (1) bekezdés *e)* pontja.

35. §

Hatályát veszti a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

a) 1. § *b)-d)* pontja,
b) 2/A. alcíme,
c) 14. § *j), l)* és *m)* pontja,
d) 15/A. §-a.

36. §

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 19. § (1) bekezdés *a)* pontja helyébe a következő rendelkezés lép:

(A Kormány)

„*a)* a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi … törvény 16. § (1) bekezdése szerinti érintett szervezet hálózati és információs rendszerét érintő,”

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

37. §

Hatályát veszti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
a) 1. § (1) bekezdés 6a. és 7a. pontja,

b) 1. § (1) bekezdés 17a., 22a. és 24-24b. pontja,
c) 2. § (2) bekezdés *d)* pontja,
d) 2. § (6) és (8) bekezdése,
e) III/A. Fejezete,
f) 24. § (1) bekezdés *b)* pontjában a „ , valamint a tanúsító hatóság” szövegrész,
g) 24. § (1) bekezdés *o)* és *p)* pontja,
h) 24. § (1b) bekezdése,
i) 24. § (2) bekezdés *d)* és *e)* pontja,
j) 24. § (3) bekezdése,
k) 30. §-a.

38. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 1. § (1) bekezdése a következő *h)* ponttal egészül ki:

[A Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: Hatóság)]

„*h)* nemzeti kiberbiztonsági tanúsítással”

(kapcsolatos feladatokat ellátó, önálló szabályozó szerv, amely csak jogszabálynak van alárendelve.)

39. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 1. § (1) bekezdés *h)* pontja helyébe a következő rendelkezés lép:

[A Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: Hatóság)]

„*h)* nemzeti kiberbiztonsági tanúsítással, valamint a kiberbiztonsági felügyelettel”

(kapcsolatos feladatokat ellátó, önálló szabályozó szerv, amely csak jogszabálynak van alárendelve.)

40. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 3. § (6) bekezdése helyébe a következő rendelkezés lép:

„(6) A Hatóság látja el – a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok kivételével – a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi … törvény (a továbbiakban: Kibertan.tv.) szerinti nemzeti kiberbiztonsági tanúsító hatóság feladatait.”

41. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 3. § (6) bekezdése helyébe a következő rendelkezés lép:

„(6) A Hatóság látja el – a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok kivételével – a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi … törvény (a továbbiakban: Kibertan.tv.) szerinti nemzeti kiberbiztonsági tanúsító hatóság feladatait, továbbá a Kibertan.tv. hatálya alá tartozó érintett szervezetek, valamint azok hálózati és információs rendszerei kiberbiztonsági felügyeletét.”

42. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 5. § (2a) bekezdése helyébe a következő rendelkezés lép:

„(2a) A Hatóság a 3. § (6) bekezdése szerinti feladatkörében lefolytatott hatósági eljárásaiban az Ákr. rendelkezéseit az e törvényben, a fogyasztóvédelemről szóló törvényben, a termékek piacfelügyeletéről szóló törvényben és a Kibertan.tv.-ben foglalt eltérésekkel és kiegészítésekkel kell alkalmazni.”

43. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 5/A. §-a helyébe a következő rendelkezés lép:

„5/A. § A Hatóság a 3. § (6) bekezdése szerinti, nemzeti kiberbiztonsági tanúsító hatósági feladatkörében az ellenőrzés eredményeként a feltárt jogsértés súlyával arányosan, a jogsértésben rejlő kockázat mértékének és jellegének figyelembevételével – a termékek piacfelügyeletéről szóló törvényben és a Kibertan.tv.-ben foglaltakon túl – a következő jogkövetkezményeket is alkalmazhatja:

a) kötelezheti a gyártót az uniós megfelelőségi nyilatkozat módosítására vagy visszavonására,

b) a megfelelőségértékelő szervezet tanúsítványkibocsátási jogát részben vagy teljeskörűen felfüggesztheti vagy visszavonhatja,

c) a megfelelőségértékelő szervezetet törölheti a nyilvántartásból,

d) az engedélyköteles tevékenység végzésére vonatkozó engedélyt módosíthatja, visszavonhatja,

e) az érintett termék, szolgáltatás vagy folyamat vonatkozásában elrendelheti a tanúsításra utaló kifejezés, jelölés használatával történő forgalmazás, nyújtás, reklámozás korlátozását vagy megtiltását,

f) az érintett termék, szolgáltatás vagy folyamat vonatkozásában elrendelheti a megfelelőségi jelölés eltávolíttatását.”

44. §

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

(A Hatóság elnöke)

„*q)* megállapítja – a Kibertan.tv. 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatósági tevékenység kivételével – a Kibertan.tv. szerinti tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak és a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartamát, a hadiipari

kutatás, fejlesztés, gyártás és kereskedelem kivételével a megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és azok tevékenységére vonatkozó részletes szabályokat, továbbá meghatározza a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket,”

45. §

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

(A Hatóság elnöke)

„*q)* megállapítja – a Kibertan.tv. 4. § (1) bekezdés *b)* pontja szerinti tanúsító hatósági tevékenység kivételével – a Kibertan.tv. szerinti tanúsító hatósági tevékenység eljárásrendjének, az engedélyezési eljárásnak és a nyilvántartás vezetésének részletes szabályait, valamint a nyilvántartás személyes adatot nem tartalmazó adattartamát, a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a megfelelőségi önértékelésre, a tanúsítási eljárásra, valamint a megfelelőségértékelő szervezetek kötelezettségeire és azok tevékenységére vonatkozó részletes szabályokat, továbbá meghatározza a hadiipari kutatás, fejlesztés, gyártás és kereskedelem kivételével a nemzeti kiberbiztonsági tanúsítási rendszereket, a nemzeti vagy európai kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok alkalmazására kötelezett szervezeteket, a kiberbiztonsági felügyelet és feladatellátás, továbbá a hatósági ellenőrzés lefolytatásának és az éves ellenőrzési terv elkészítésének részletes szabályait, az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásba vételének rendjét, valamint a nyilvántartás személyes adatnak nem minősülő adattartalmára vonatkozó részletes szabályokat, a biztonsági incidenskezelésben résztvevő közreműködők esetében a biztonsági incidensek kezeléséhez szükséges feltételeket, valamint a biztonsági incidenskezelésben résztvevő közreműködőknek a biztonsági incidensek kezelésére vonatkozó szabályoknak és a biztonsági incidensek kezeléséhez szükséges feltételeknek történő megfelelés tanúsítására vonatkozó részletes szabályokat, a kiberbiztonsági audit lefolytatásának rendjét, az auditorok nyilvántartásba vételi eljárásának rendjét, az auditorral szemben támasztott szakmai követelményeket, valamint a kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját, a biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket, a kiberbiztonsági felügyeleti díj mértékét és megfizetésének időpontját,”

46. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 36/A. §-a helyébe a következő rendelkezés lép:

„36/A. § (1) Az 1. § (1) bekezdés *h)* pontja, a 3. § (6) bekezdése, az 5. § (2a) bekezdése, az 5/A. § és a 13. § *q)* pontja az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet végrehajtásához szükséges rendelkezéseket állapít meg.

(2) Ez a törvény 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 szóló, 2022. december 14-i, (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.”

47. §

A Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény

a) 1. § (1) bekezdés *f)* pontjában a „nyilvántartásba vételével, valamint,” szövegrész helyébe a „nyilvántartásba vételével,” szöveg,

b) 1. § (1) bekezdés *g)* pontjában az „és szabályozásával” szövegrész helyébe az „és szabályozásával, valamint” szöveg

lép.

48. §

Hatályát veszti a 31. § (3) bekezdése.

1. melléklet a 2023. évi …. törvényhez

Magas kockázatú ágazatokban működő szolgáltatók, valamint szervezetek

	A	B	C
1.	Ágazat	Alágazat	Szervezet
2.	Energia	Villamos energia	a villamos energiáról szóló törvény szerinti villamosenergia-ipari vállalkozás,
3.		Távfűtés és hűtés	a távhőszolgáltatásról szóló törvény szerinti engedélyes,
4.		Olaj	a bányászatról szóló törvény szerinti a) szénhidrogén szállítóvezetéket létesítő és üzemben tartó engedélyes, b) a kőolajfeldolgozásban, tárolásban használt létesítmény üzemeltetője,
5.			a behozott kőolaj és kőolajtermékek biztonsági készletezéséről szóló törvény szerinti központi készletező szervezet,
6.		Gáz	földgázipari vállalkozás,
7.		Hidrogén	a hidrogéntermelés, -tárolás és -szállítás üzemeltetője,
8.	Szállítmányozás	Légi szállítás	a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló kormányrendelet szerinti légiközlekedés védelmében közreműködő szervezet,
9.		Vasúti közlekedés	a vasúti közlekedésről szóló törvény szerinti vasúti pályahálózat működtetője – a saját célú vasúti pályahálózatok, iparvágányok kivételével –, a vállalkozó vasúti társaság, a vasúti pályakapacitás-elosztó szervezet,

10.		Közúti közlekedés	a közúti közlekedésről szóló törvény felhatalmazása alapján kiadott rendelet szerinti a) ITS-szolgáltató, b) forgalomirányítás végző,
11.		Vízi közlekedés	a víziközlekedésről szóló törvény szerinti hajózási tevékenység folytatásában részt vevő jogi személy, jogi személyiséggel nem rendelkező gazdálkodó szervezet,
12.	Egészségügy		az egészségügyről szóló törvény szerinti egészségügyi szolgáltató,
13.			magas biztonsági szintű biológiai laboratóriumok üzemeltetője, Egészségügyi Tartalékokat és vérkészleteket kezelő szervezet, gyógyszerek kutatásával és fejlesztésével foglalkozó szervezet, gyógyszeripari alaptermékeket és gyógyszerkészítményeket gyártó szervezet, gyógyszer-nagykereskedő, népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzékén szereplő kritikus fontosságú orvostechnikai eszközt gyártó szervezet,
14.	Ivóvíz, szennyvíz	Vízközmű szolgáltatás	a víziközmű-szolgáltatásról szóló törvény szerinti víziközmű-szolgáltató,
15.	Hírközlési szolgáltatás		az elektronikus hírközlésről szóló törvény szerinti a) elektronikus hírközlési szolgáltató, b) adatkicserélő szolgáltatást nyújtó szolgáltató,
16.			az elektronikus ügyintézés és a bizalmi szolgáltatások általános

			szabályairól szóló törvény szerinti bizalmi szolgáltató,
17.	Digitális infrastruktúra		a felhőszolgáltató,
18.			adatközponti szolgáltatást nyújtó szolgáltató,
19.			legfelső szintű domainnév-nyilvántartó,
20.			a DNS-szolgáltató,
21.			tartalomszolgáltató hálózat szolgáltatója,
22.	Kihelyezett IKT szolgáltatások		a) kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, b) kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató,
23.	Világűr		űralapú szolgáltatások nyújtását támogató földi infrastruktúra üzemeltető

2. melléklet a 2023. évi ….. törvényhez

Jelentős kockázatú ágazatokban működő szolgáltatók, valamint szervezetek

	A	B	C
1.	Ágazat	Alágazat	Entitás típusa
2.	Postai és futárszolgálatok		a postai szolgáltatásokról szóló törvény szerinti postai szolgáltató,
3.	Élelmiszer előállítása, feldolgozása és forgalmazása		az élelmiszerláncról és hatósági felügyeletéről szóló törvény szerint élelmiszer-vállalkozás,
4.	Hulladékgazdálkodás		a hulladékról szóló törvény szerinti tevékenységet végző,
5.	Vegyszerek előállítása és forgalmazása		a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről szóló 1907/2006/EK európai parlamenti és tanácsi rendelet 3. cikke szerinti gyártó, forgalmazó,
6.	Gyártás	Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása	az (EU) 2017/745 európai parlamenti és tanácsi rendelet (4) 2. cikkének 1. pontjában meghatározott orvostechnikai eszközöket, valamint az (EU) 2017/746 európai parlamenti és tanácsi rendelet (5) 2. cikkének 2. pontjában meghatározott in vitro diagnosztikai orvostechnikai eszközöket gyártó szervezet, kivéve az e rendelet 1. melléklete 5. pontjának ötödik franciabekezdésében említett orvostechnikai eszközöket gyártó szervezet,
		Számítógép, elektronikai, optikai termék gyártása	a gazdasági tevékenységek statisztikai osztályozása NACE

	Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló 1893/2006/EK rendelet 26. ágazata szerinti „Számítógép, elektronikai, optikai termék gyártása” tevékenységet végző gazdálkodó szervezet,
Villamos berendezések gyártása	a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló 1893/2006/EK rendelet 27. ágazata szerinti „Villamos berendezés gyártása” tevékenységet végző gazdálkodó szervezet,
Máshova nem sorolt gépek és berendezések gyártása	a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló 1893/2006/EK rendelet 28. ágazata szerinti „Gép, gépi berendezés gyártása” tevékenységet végző gazdálkodó szervezet,
Gépjárművek, pótkocsik és félpótkocsik gyártása	a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló 1893/2006/EK rendelet 29. ágazata szerinti „Közúti jármű gyártása” tevékenységet végző gazdálkodó szervezet,
Egyéb szállítóeszközök gyártása	a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló

			1893/2006/EK rendelet 30. ágazata szerinti „Egyéb jármű gyártása” tevékenységet végző gazdálkodó szervezet,
		Cement-, mész-, gipszgyártás	a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló 1893/2006/EK rendelet 23.5 alágazata szerinti „Cement-, mész-, gipszgyártás” tevékenységet végző gazdálkodó szervezet,
7.	Digitális szolgáltatók		a) az online-piactér szolgáltatója, b) a 2001. évi CVIII. törvény szerinti keresőszolgáltató, c) közösségi média szolgáltatási platform szolgáltatója, d) domainnév regisztrációt végző szolgáltató,
8.	Kutatás		kutatóhely