**TERVEZET!**

**A Kormány**

**...../2013. (..... ...) határozata**

**Magyarország Nemzeti Kiberbiztonsági Stratégiájáról**

1. A kormány elfogadja a határozat 1. mellékletében foglalt Magyarország Nemzeti Kiberbiztonsági Stratégiáját.

2. A kormány elrendeli a Nemzeti Kiberbiztonsági Koordinációs Tanács kialakításához szükséges intézkedések megtételét.

Felelős: Miniszterelnökség az érintett tárcák bevonásával
Határidő: 2013. június 30.

3. A kormány elrendeli a Nemzeti Kiberbiztonsági Stratégiában meghatározott feladatok ellátását szolgáló munka- és intézkedési terv elkészítését.

Felelős: Miniszterelnökség az érintett tárcák bevonásával
Határidő: 2013. június 30.

4. Ez a határozat a közzétételét követő napon lép hatályba.

Budapest, 2013. ....."

Orbán Viktor
miniszterelnök

*Melléklet az ...../2013. ( . .) Korm. határozathoz*

**Magyarország Nemzeti Kiberbiztonsági Stratégiája**

1. Jelen stratégia célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza a nemzeti jövőképet és azokat a nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben. Kiemelt cél, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel felvállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté alakítsa át. A megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése.

2. Jelen stratégia Magyarország Alaptörvényében megfogalmazott alapértékek – szabadság, biztonság, jogállamiság, nemzetközi és európai együttműködés – leképezése egy külön biztonság-, és gazdaságpolitikai területre, az Alaptörvény 38. cikkéből levezetett, a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma. A stratégia összhangban a 1035/2012. (II. 21.) Korm. határozattal elfogadott Magyarország Nemzeti Biztonsági Stratégiájával, kifejti annak a kiberbiztonságról szóló 31. pontjában meghatározott törekvéseket és megfogalmazott kormányzati felelősséget. A stratégia egyben igazodik az Európai Parlament által 2012. november 22-én elfogadott, „A kiberbiztonságról és védelemről szóló", 2012/2096(INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én "Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez.

I. Magyarország kiberbiztonsági környezete

3. A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak illetve Magyarország érintett benne.

4. A kibertérben megjelenő, különböző forrásból származó fenyegetések megnövekedett száma és ezek nagyságrendekkel megnövekedett következményei jelzik, hogy az elmúlt évtizedben nagy gyorsasággal nőtt azon felhasználók száma és hatékonysága, akik a kiberteret kritikus adatok, információk illegális megszerzésére, valamint a kommunikációs és informatikai rendszerekben történő károkozásra használják. A dinamikusan megjelenő új technológiák, mint például az informatikai felhő vagy a mobilinternet, újabb biztonsági kockázatok folyamatos kialakulásához vezetnek. Jelen Stratégia egyik fő célja annak a döntéshozó politikai és szakmai figyelemnek és képességnek a kiépítése, mely rugalmasan reagálva lehetővé teszi a belátható jövőben is a technológiai fejlődésből fakadó új

kiberbiztonsági problémák kezelését. A kibertérben fellépő veszélyek ugyanis egyben a Magyarországon található létfontosságú rendszerek és létesítmények biztonságát is érintik.

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

## II. Magyarország kiberbiztonsági értékrendje, jövőképe, céljai

6. Magyarország őrzi és védi szuverenitását a magyar kibertérben, melynek szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekinti. Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági, és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével valósul meg.

7. Magyarország a globális kibertér minden Magyarországgal hasonló értékrendet valló állami és nem állami tényezőjével jó viszony kialakítását és fenntartását célozza meg, továbbá nemzetközi szövetségi rendszerén, valamint EU, NATO, Európai Biztonsági és Együttműködési Szervezet (EBESZ) és más nemzetközi szervezeti tagságán keresztül törekszik a globális kibertér szabad használatának, békéjének és biztonságának szavatolására. Magyarország különös gonddal tekint a közép- és kelet európai régióra, melynek kiberbiztonságát regionális együttműködések keretében tovább erősíthetőnek látja.

8. Magyarország a jelen és a jövő kihívásaihoz igazodva követelményként rögzíti, hogy a magyar kibertér nyújtson biztonságos és megbízható környezetet:
a) az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,
b) a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,
c) a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,
d) az elektronikus közigazgatás számára, hozzájárulva az állami szolgáltatások innovatív és előremutató fejlesztéséhez.

9. Magyarország a szabad és biztonságos kibertér használat érdekében a nemzetbiztonság, a hatékony válságkezelés és a felhasználó-védelem szempontjainak összehangolásával megvalósítandó célként rögzíti, hogy:
a) rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő fenyegetések, támadások, illetve vészhelyzetek valamint a vétlen információszivárgások ellen,
b) nemzeti adatvagyona megfelelő szintű védelemben részesüljön, létfontosságú rendszereinek és létesítményeinek kibertérhez kapcsolódó működése üzembiztos legyen, valamint rendelkezésre álljon kompromittálás esetén a megfelelően gyors, hatékony és veszteséget minimalizáló, minősített helyzetben is alkalmazható helyreállítási képesség,
c) a magyar kibertér biztonságos működéséhez szükséges informatikai, hírközlési termékek és szolgáltatások színvonala elérje a legjobb nemzetközi gyakorlatokét, kiemelt hangsúlyt fektetve a nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre,

d) a kiberbiztonsági oktatás, képzés, valamint a kutatás és fejlesztés színvonala megfeleljen a legjobb nemzetközi gyakorlatoknak, hozzájárulva egy világszínvonalú hazai tudásbázis kialakításához,
e) a gyermekek számára a biztonságos kibertér kialakítása megfeleljen a legjobb nemzetközi gyakorlatoknak.

## III. A célok eléréséhez szükséges feladatok

10. Magyarország kiberbiztonsági helyzete alapvetően szilárd. A kibertér sajátos szerkezetéből eredően azonban számos olyan biztonsági kockázattal és fenyegetéssel kell számolni, amelyek nemzeti szempontból stratégiai kihívást jelentenek. A kiberbiztonság megfelelő szinten tartásához és folyamatos fejlesztéséhez, a kitűzött célok eléréséhez rendelkezésre álló eszközök és a feladatellátással érintett területek a következők:
a) Kormányzati koordináció. Kiemelt figyelmet kell fordítani a Miniszterelnökség keretében megvalósuló összkormányzati koordináció erősítésére, amely alapfeltétele a kormányzati és ágazati erőforrások koordinált és koncentrált alkalmazásának.
b) Együttműködés. Kiberbiztonsági érdekeink és céljaink eléréséhez szükséges az együttműködés javítása és a hatékony információcsere. Ennek érdekében olyan operatív együttműködési fórumok működtetése szükséges, amely a civil, a gazdasági és a tudományos területek képviselőinek részvételét biztosítja a kormányzati döntés-előkészítési folyamat során és lehetőséget nyújt arra, hogy ezen fórumok tagjai ajánlásokat fogalmazzanak meg a kiberbiztonsági tevékenység fejlesztésére, folyamatos újítására.
c) Szakosított intézmények. A kiberbiztonsággal összefüggő feladatok ellátását a specifikus szakértelemmel és hatáskörrel rendelkező szervezetekhez szükséges telepíteni. amely szervezetek nem csak egymással, hanem az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködnek. A feladatellátás érinti a nemzetbiztonsági, honvédelmi, bűnüldözési, katasztrófavédelmi és létfontosságú intézmények és létesítmények védelmével kapcsolatos feladatokat ellátó szervezeteket, valamint az elektronikus információbiztonság területén hatósági jogosítványokkal rendelkező intézményeket. A kiberbiztonsági eseményekkel kapcsolatos feladatok ellátását az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által akkreditált tagszervezetként működő kormányzati eseménykezelő központ, valamint az egyes szakágazatok területén működtetett ágazati eseménykezelő központok végzik.
d) Szabályozás. A többlépcsős jogalkotási tevékenység mellett szükséges a civil, a gazdasági és a tudományos terület szereplőivel együttműködési megállapodásokat kötni, amelyek megfelelő alapot és szabályozást biztosítanak a közös felelősségvállaláson alapuló kiberbiztonság hatékony működtetéséhez.
e) Nemzetközi együttműködések. Magyarország aktív szereplője kíván lenni különösen az EU, a NATO, valamint az ENSZ és az EBESZ kiberbiztonsági kezdeményezéseinek és együttműködésüknek, továbbá fenntartja élenjáró szerepét az operatív kormányzati együttműködések kialakításában és működtetésében az EU, a NATO és az EBESZ keretein belül, valamint a közép-és dél-kelet európai régióban. Magyarország fenntartja aktív szerepét a nemzeti/kormányzati és ágazati incidenskezelő központok európai és globális szervezeteiben.
f) Tudatosság. Magyarország fenntartja élen járó szerepét a kiberbiztonsággal összefüggő hazai és nemzetközi konferenciák szervezésében. Szakosított intézményein, a civil, a gazdasági és a tudományos terület szereplőivel kialakított együttműködéseken keresztül támogatja a kibertér biztonságos használatát célzó és figyelemfelhívó médiakampányokat, valamint a kiberbiztonsági gyakorlati tudást elősegítő kezdeményezéseket.

g) Oktatás, kutatás-fejlesztés. Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, a kormányzati tisztviselők képzésében és a szakmai továbbképzésekben a kiberbiztonság szakterülete integrálódjon az informatika oktatásába. Magyarország stratégiai partnerség kialakítására törekszik azon egyetemi és akadémiai kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.
h) Gyermekvédelem. Magyarország a kiberbiztonság lényegi elemének tekinti a gyermekek egészséges fejlődését lehetővé tevő környezet kialakítását és fenntartását, melyet minden érintett területen prioritásként kezel, megvalósítva egyben a Gyermekbarát Internet Európai Stratégiájának célkitűzéseit. Kifejezett hangsúlyt fektet a gyermekeknek és fiataloknak szóló minőségi online tartalmak előállításának ösztönzésére, a tudatosságnövelő és felkészítő intézkedések támogatására, a gyermekek zaklatása és kizsákmányolása elleni küzdelemre, s a biztonságos online környezet megteremtésére A gyermekvédelem területén kiemelt partnerének tekinti az online gyermekvédelem terén eredményeket elért magyar civil szervezeteket.
i) Gazdasági szereplők motivációja. Az informatikai és hírközlési közbeszerzések kiberbiztonsági követelményeinek meghatározása során Magyarország abban érdekelt, hogy azok a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönözzék a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat, kiemelt hangsúlyt fektetve a nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre. A magyar kormány törekszik egyben arra, hogy a gazdasági élet szereplőivel közösen dolgozzon ki olyan ösztönző intézkedéseket a gazdasági élet szereplői számára, amelyek a kiberbiztonság fokozását célozzák.

## IV. A Nemzeti Kiberbiztonsági Stratégia végrehajtásához rendelkezésre álló kormányzati eszközök

11. Magyarország a stratégia céljainak eléréséhez mind a kompetenciák, mind a potenciális erőforrások terén a szükséges eszközök jelentős részével már rendelkezik, ezek között szerepel:
a) a magyar kibertér biztonságáért felelős kormányzati szervezetek számbavétele és koordinációja, a hatékony együttműködés kialakítása;
b) a magyar kibertér biztonságáért felelős civil, gazdasági és tudományos szervezetek számbavétele és intézményes keretek között folyó együttműködés kialakítása;
c) a létfontosságú információs infrastruktúrák és vagyonelemek, illetve a nemzeti adatvagyon számbavétele és védelmének biztosítása;
d) a szakosított kormányzati intézmények működtetése;
e) a szabályozási környezet biztosítása;
f) a nemzetközi és regionális együttműködésekben történő részvétel, politikai, operatív és szabályozási szinten egyaránt;
g) a támogatási keretrendszer kialakítása a kutatás és fejlesztés, valamint az oktatás és tudatosítás terén;
h) gazdasági motivációs rendszerek megteremtése;
i) a kiberbiztonsági szempontok érvényesítése az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során.

12. A rendelkezésre álló eszközök megerősítéséhez, hatékonyabb felhasználásához és nemzeti biztonsági szempontok szerinti eredményesebb működtetéséhez szükséges egy

koherens kormányon belüli és kormányzati-nem kormányzati együttműködési rendszer kialakítása.

**2013. évi ..... törvény**

**az állami és önkormányzati szervek elektronikus információbiztonságáról**

A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.
Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.
Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:

## I. Fejezet
## Általános rendelkezések

*1. Értelmező rendelkezések*

**1. §**

(1) E törvény alkalmazásában

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

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

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

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

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

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

***7. auditálás:*** előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
***8. bizalmasság:*** az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik

meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

*9. **biztonsági esemény:*** nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és ezzel az informatikai biztonságpolitika vagy az informatikai biztonsági szabályzat megsértését vagy a biztonsági intézkedések kudarcát okozza;

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

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

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

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

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

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

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

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

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

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

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

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

*22. **fizikai védelem:*** a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai

jelzőrendszer, az élőerős védelem, a beléptető-rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

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

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

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

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

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

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

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

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

***31. kockázatkezelés:*** az elektronikus információs rendszerre a kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

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

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

***34. létfontosságú információs rendszerelem:*** az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése az európai létfontosságú rendszerelemmé

és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket, vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

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

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

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

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

*39. **sértetlenség:*** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

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

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

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

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

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

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

*46. **zárt célú elektronikus információs rendszer:*** törvényben vagy kormányrendeletben meghatározott elkülönült elektronikus információs, informatikai vagy hírközlési rendszer, hálózat;

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

(2) E törvény alkalmazásában elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók),

eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese:

a) a számítástechnikai rendszerek és hálózatok, ideértve az internet szolgáltatást is;
b) a vezetékes, a mobil, a rádiós és műholdas távközlés;
c) a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
d) a rádiós vagy műholdas navigáció;
e) az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek, stb.);
f) a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

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

*2. A törvény hatálya*

**2. §**

(1) E törvény rendelkezéseit kell alkalmazni

a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,
b) a Köztársasági Elnöki Hivatalra,
c) az Országgyűlés Hivatalára,
d) az Alkotmánybíróság Hivatalára,
e) az Országos Bírósági Hivatalra és a bíróságokra,
f) az ügyészségekre,
g) az Alapvető Jogok Biztosának Hivatalára,
h) az Állami Számvevőszékre,
i) a Magyar Nemzeti Bankra,
j) a fővárosi és megyei kormányhivatalokra,
k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,
l) a Magyar Honvédségre.

(2) E törvény rendelkezéseit kell alkalmazni:

a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők,
b) a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,
c) az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek

elektronikus információs rendszereinek védelmére.

(3) A minősített adatokat kezelő elektronikus információs rendszereket érintően

a) e törvény rendelkezéseit a minősített adat védelmére vonatkozó jogszabályokban meghatározott eltérésekkel kell alkalmazni,
b) a 14-18. §-ban meghatározott feladatok ellátásáról a minősített adatok védelmének szakmai felügyeletéért felelős miniszter gondoskodik.

(4) A 14-18. §-ban meghatározott feladatok ellátásáról:
a) a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat zárt célú elektronikus információs rendszerei, továbbá a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a honvédelemért felelős miniszter,
b) a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek zárt célú elektronikus információs rendszerei esetében a rendvédelmi szervet irányító miniszter,
c) a diplomáciai információs célokra használt zárt célú elektronikus információs rendszerei esetében a külpolitikáért felelős miniszter,
d) a Nemzeti Adó- és Vámhivatalnak az állami költségvetési bevételek biztosítását támogató elektronikus információs rendszerei esetében az adópolitikáért felelős miniszter,
e) az Információs Hivatal esetében a Kormány polgári hírszerzési tevékenység irányításáért felelős tagja
a jogszabályban meghatározottak szerint gondoskodik.

(5) A médiaszolgáltatási és az elektronikus hírközlési tevékenység esetén e törvény rendelkezéseit törvényben meghatározott eltérésekkel kell alkalmazni.

**3. §**

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

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

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

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

**4. §**

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

## II. Fejezet

## Elektronikus információbiztonsági követelmények

*3. Alapvető elektronikus információbiztonsági követelmények*

**5. §**

Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell
a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása
zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

**6. §**

Az elektronikus információs rendszernek az 5. §-ban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:
a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.

*4. Az elektronikus információs rendszerek biztonsági osztályba sorolása*

**7. §**

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

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

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

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

(5) A szervezet vezetője az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes

esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

**8. §**

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

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

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

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

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

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

*5. Az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintje*

**9. §**

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

(2) A szervezet biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább
a) a 2. § (1) bekezdés b)-d), g) és k) pontjába tartozó szervezetek esetén 2.,
b) a 2. § (1) bekezdés a), e), f), h)-j) pontjába tartozó szervezetek esetén 3.,
c) a 2. § (1) bekezdés l) pontjába tartozó szervezetek esetén 4.,
d) a 2. § (2) bekezdés b) és c) pontjába tartozó szervezetek esetén 5.
szintű.

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

(4) A hatóság a szervezet – kivéve a 2. § (3) és (4) bekezdésében meghatározott elektronikus információs rendszerek esetében – által megállapított biztonsági szintet felülbírálhatja és magasabb, kivételes esetben alacsonyabb szintű besorolást is megállapíthat.

**10. §**

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

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

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

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

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

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

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

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

*6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei*

**11. §**

(1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:
a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban

meghatározott követelmények teljesülését,
c) az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,
d) kiadja a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját,
e) meghatározza a szervezet elektronikus információs rendszereinek informatikai biztonsági stratégiáját,
f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, m) felelős azért, hogy az érintetteket a biztonsági követelményekről és a lehetséges fenyegetésekről haladéktalanul tájékoztassa,
n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

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

(3) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybe vétele esetén az (1) és (2) bekezdésben írt feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval és a szervezet vezetőjével.

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

**12. §**

A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:
a) a 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja
a hatóság részére.

**13. §**

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

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:
a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, irányítását, koordinálását és ellenőrzését,
c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) előkészíti a szervezet elektronikus információs rendszereire vonatkozó biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
f) kapcsolatot tart a hatósággal.

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

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

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését
a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők
b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők
e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

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

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

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

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

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

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

## III. Fejezet

## Az elektronikus információs rendszerek biztonsági felügyelete

*7. Az elektronikus információs rendszerek biztonságának felügyelete*

### 14. §

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

(2) A hatóság feladata:
a) az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,
b) az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,
c) az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,
d) a rendelkezésre álló információk alapján kockázatelemzés elvégzése,

e) a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása,
f) javaslattétel a kritikus infrastruktúra védelmi feladatok kormányzati koordinációjáért felelős miniszternek a nemzeti létfontosságú rendszerelem kijelölésére,
g) az információs társadalom biztonságtudatosságának elősegítése és támogatása,
h) együttműködés a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvényben meghatározott elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,
i) kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,
j) kapcsolattartás a Nemzeti Média- és Hírközlési Hatósággal, továbbá a kormányzati eseménykezelő központtal és az ágazati eseménykezelő központokkal, a kormányzati incidens-kezelés munkacsoport irányítása,
k) véleményezési jog gyakorlása a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,
l) együttműködés a kormányzati eseménykezelő központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal,
m) éves és egyedi jelentések készítése a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban.

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

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

**15. §**

(1) A hatóság nyilvántartja és kezeli
a) a szervezet azonosításához szükséges adatokat,
b) a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,
c) a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,
d) a szervezet informatikai biztonsági szabályzatát,
e) a biztonsági eseményekkel kapcsolatos bejelentéseket.

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

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

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

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

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

**16. §**

(1) A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:
a) az érintett szervezeteknél a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
b) a követelményeknek való megfelelőség alátámasztásához szükséges dokumentumokat bekérni, illetve a 12. § b) pontja alapján megküldött dokumentációt felülvizsgálni,
c) a biztonsági osztályba sorolást, a biztonsági szint megállapítását, vagy a védelmi intézkedéseket ellenőrizni, az ott feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
d) a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását,
e) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervezni,
f) a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviselni Magyarországot,
g) egyetértési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.

(2) A (3) bekezdésben meghatározott kivétellel, ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság
a) köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,
b) ha az a) pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető.

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

a) köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,
b) ha az a) pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti a szervezetet felügyelő szervhez – ha a szervezet azzal rendelkezik – fordulhat és kérheti a közreműködését,
c) ha az a) és b) pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti információbiztonsági gondnok kirendelését kezdeményezheti.

*8. Információbiztonsági felügyelő*

**17. §**

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

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

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

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

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

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

**18. §**

A Nemzeti Biztonsági Felügyelet
a) éves ellenőrzési terv alapján, és e törvény 14. § (2) bekezdés a), b) és e) pontjában foglaltakra tekintettel:
aa) szakhatóságként a Hatóság megkeresésére, továbbá
ab) egyedi esetekben a Hatóság felkérésére
az érintett szervezet vezetőjét előzetesen tájékoztatva sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,

b) a szervezetek elektronikus információs rendszerében a szervezet felkérésére sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,
c) a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálat lezárását követően haladéktalanul tájékoztatja a vizsgált szervezet vezetőjét,
d) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez,
e) a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot,
f) véleményezési jogot gyakorol a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,
g) az a)-c) pontban foglalt feladatok végrehajtásáról a hatóság részére tájékoztatást ad,
h) együttműködik a kormányzati eseménykezelő központtal.

*10. A kormányzati eseménykezelő központ*

**19. §**

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

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

(3) Az ágazati eseménykezelő központ a biztonsági eseményekhez kapcsolódó adatait köteles haladéktalanul a kormányzati eseménykezelő központ részére továbbítani.

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

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

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

**20. §**

(1) A kormányzati eseménykezelő központ ellátja a következő feladatokat:
a) az ágazati eseménykezelő központok szakmai támogatása,
b) a nemzetközi eseménykezelési együttműködésekben Magyarország képviselete és az ágazati eseménykezelő központok tájékoztatása a nemzetközi szervezetektől tudomására jutott információbiztonságot érintő eseményekről, fenyegetésekről,
c) a szervezetekkel való kapcsolattartás a bejelentett biztonsági események fogadására,

valamint az azok kezeléséhez szükséges operatív intézkedések megtétele és koordinálása,
d) napi rendszerességű hálózatbiztonsági helyzetértékelések elvégzése,
e) folyamatosan elérhető 24 órás ügyelet működtetése,
f) a biztonsági események kivizsgálása során a jogszabályban meghatározottak szerint a biztonsági események adatai műszaki vizsgálatának elvégzése,
g) a szervezeteknél előforduló biztonsági események adatainak gyűjtése, ezekről negyedévente jelentés készítése a 21. § szerinti Nemzeti Kiberbiztonsági Koordinációs Tanács részére,
h) elemzések, jelentések készítése a 21. § szerinti Nemzeti Kiberbiztonsági Koordinációs Tanács részére a hazai és nemzetközi információbiztonsági irányokról,
i) azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági eseményekről, ezek magyar nyelvű megjelenítése,
j) a nemzetközileg publikált sérülékenységek közzététele a honlapján,
k) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatok szervezése,
l) felkérésre részvétel a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon,
m) együttműködés a hatósággal és a Nemzeti Biztonsági Felügyelettel.

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

*11. A kormányzati koordináció biztosítása*

**21. §**

(1) A 2. § (1)-(4) bekezdéseiben említett szervezetek együttműködését a Miniszterelnökség által irányított Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) irányítja.

(2) A Tanács a Miniszterelnökséget vezető államtitkár irányításával és a Miniszterelnökség által delegált kiberkoordinátor támogatásával:
a) koordinálja a törvény hatálya alá tartozó szervezetek együttműködését a kiberbiztonsággal összefüggő feladatok ellátásában;
b) elősegíti a kiberbiztonság szabályozását, valamint a kiberbiztonság ágazati munkacsoportjainak munkáját;
c) támogatja a nem-kormányzati szereplőkkel való együttműködésnek keretet biztosító Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) munkáját;
d) támogatja a források hatékony felhasználását;
e) felügyeli Magyarország Nemzeti Kiberbiztonsági Stratégiájának végrehajtását es erről jelentest tesz a Nemzetbiztonsági Tanácsnak;
f) elősegíti a kiberbiztonságot érintő egységes magyar kormányzati álláspont kialakítását és hozzájárul Magyarország nemzetközi politikai képviseletéhez.

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

*12. Adatvédelmi rendelkezések*

**22. §**

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

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

## IV. Fejezet
## Oktatás-képzés, kutatás-fejlesztés

**23. §**

A Nemzeti Közszolgálati Egyetem a képzési tevékenységének ellátásával összefüggésben

a) a 11. § (1) bekezdés g) pontjában, a 13. § (8) bekezdésében meghatározott képzés érdekében kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját,
b) kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a 13. § (8) bekezdésében meghatározott képzettségi követelményeket,
c) gondoskodik a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek, és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről,
d) közreműködik az információbiztonsági, kibervédelmi, létfontosságú információs rendszer védelmi gyakorlatokon.

## V. Fejezet

## Záró rendelkezések

*13. Felhatalmazó rendelkezések*

**24. §**

(1) Felhatalmazást kap a Kormány, hogy rendeletben meghatározza
a) a hatóság feladatának részletes szabályait, a hatósági ellenőrzés lefolytatásának részletes eljárási szabályait,
b) a hatóság által kiszabható bírság mértékét, a bírság kiszabásának és befizetésének részletes

eljárási szabályait,
c) az információbiztonsági felügyelő kirendelésének szabályait, feladatkörét és eljárásának rendjét,
d) a Nemzeti Biztonsági Felügyelet szakhatósági feladat- és hatáskörét,
e) a kormányzati eseménykezelő központ és az ágazati eseménykezelő központok feladat- és hatáskörét, és
f) a 21. § szerinti Tanács, Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokat, feladat- és hatáskörüket.

(2) Felhatalmazást kap

a) az informatikáért felelős miniszter, hogy az e-közigazgatásért felelős miniszterrel és a minősített adatkezelésért felelős miniszterrel egyetértésben meghatározza a 6. és 7. §-okban előírt technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre vonatkozó követelményeket, továbbá a biztonsági osztályba sorolás és a szervezetek biztonsági szintbe sorolásának követelményeit,
b) a közigazgatás-fejlesztésért felelős miniszter, hogy az informatikáért felelős miniszterrel egyetértésben az e törvényben meghatározott vezetői, az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmát,
c) az informatikáért felelős miniszter, hogy a szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjét

rendeletben határozza meg.

(3) Felhatalmazást kap

a) a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat, továbbá a Honvédelmi Tanács és a Kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a honvédelemért felelős miniszter,
b) a rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek esetében a rendvédelmi szervet irányító miniszter,
c) a diplomáciai információs célokra használt rendszer esetében a külpolitikáért felelős miniszter,
d) a Nemzeti Adó- és Vámhivatal esetében az adópolitikáért felelős miniszter,
e) az Információs Hivatal esetében a Kormány polgári hírszerzési tevékenység irányításáért felelős tagja,

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

*14. Hatálybalépés*

**25. §**

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

*15. Átmeneti rendelkezések*

**26. §**

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

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

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

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

*16. Módosító rendelkezések*

**27. §**

(1) A minősített adat védelméről szóló 2009. évi CLV. törvény 10. § (4) bekezdése helyébe a következő rendelkezés lép:

„(4) Minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő

a) az e törvényben és a végrehajtására kiadott rendeletekben meghatározott személyi, fizikai és adminisztratív, valamint
b) ha a szerv a minősített adatot elektronikus információs rendszeren kezeli az e törvényben és az elektronikus információbiztonságról szóló törvényben és végrehajtásukra kiadott jogszabályokban meghatározott elektronikus

biztonsági feltételeket."

(2) A minősített adat védelméről szóló 2009. évi CLV. törvény 20. § (2) bekezdése a következő v) ponttal egészül ki:

*(A Nemzeti Biztonsági Felügyelet)*
„v) elvégzi az elektronikus információbiztonságról szóló jogszabályokban számára meghatározott feladatokat."

**28. §**

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 10. § (2) bekezdésének helyébe a következő rendelkezés lép:

„(2) Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót kizárólag az adatkezelő hozzájárulásával vehet igénybe. Az adatfeldolgozás jogszerűségéért és biztonságáért az adatkezelő felel."

**29. §**

Hatályát veszti a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 4. §-a.

*Melléklet az ...../2013. ( . .) Korm. határozathoz*

## ÁLTALÁNOS INDOKOLÁS

A stratégia célja, hogy a magyar kiberteret szabad, biztonságos és innovatív környezetté alakítsa át. A kormányzat e munkában a lehető legnagyobb mértékben számít elsősorban a kormányzaton belüli, a civil, a gazdasági (üzleti) és a tudományos szféra összehangolt tevékenységére, továbbá a nemzetközi együttműködésekre is. A közös erőfeszítések eredőjeként a magyar kibertér szabadságának megőrzése és biztonságának megteremtése a legjobb eszköz a világméretű kibertér szabadságának és biztonságának megerősítéséhez is.
Magyarország Nemzeti Kiberbiztonsági Stratégiája, valamint a most és a jövőben kapcsolódó törvények, határozatok, rendeletek, illetve ágazati intézkedési tervek által kifejezett nemzeti kormányzati törekvés egyben annak garantálására is hivatott, hogy Magyarországon a jövő generációi a XXI. század új kihívásaira biztonságban, hatékonyan, szabadon tudjanak válaszolni, valamint tudjanak élni a kibertér adta lehetőségekkel, ezzel is erősítve hazájuk felemelkedését és jólétét.
A stratégiához kapcsolódó első jogalkotási lépés az állami és önkormányzati szervek informatikai biztonságát kiemelő, jelen előterjesztés 2. mellékletét képező az állami és önkormányzati szervek elektronikus információbiztonságáról elektronikus információbiztonságáról szóló törvény.

## RÉSZLETES INDOKOLÁS

A társadalmi és gazdasági folyamatok egyre nagyobb hányada zajlik az Interneten, ez a „virtualizálódás" hozta létre a kibertér fogalmát. A kibertér létező valóság, ahol globálisan két milliárdnál több, Magyarországon mintegy három millió felhasználó jelenik meg, az egyének társadalmi életet élnek, csoportok és pártok szerveződnek, a gazdasági élet szereplői pedig szolgáltatásokat nyújtanak, pénzt és árukat mozgatnak. A kibertér egyben az a szféra, ahol az államok egyre gyakrabban érvényesítik nemzetbiztonsági, illetve nemzetgazdasági érdekeiket védekező vagy támadó jelleggel a kibertér nyújtotta lehetőségek felhasználásával. A kibertér nincs tekintettel az állami határokra, eszközeit és infrastruktúráját meghatározó mértékben az üzleti szektor szereplői tulajdonolják, működtetik és ellenőrzik. További jellegzetessége, hogy a kibertérnek nincs irányító központja, új elektronikus információs rendszerekkel (mint például a mobil internet vagy az informatikai felhő) naponta bővül és állami eszközökkel csekély mértékben szabályozható.

Fentiek figyelembevételével került meghatározása a kibertér fogalma, miszerint a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a Magyarországon található, a globális kibertér részét képező elektronikus információs rendszerekből és ezen elektronikus rendszereken keresztül adatok és információk formájában Magyarországra irányuló és hazánkban megjelenő társadalmi és gazdasági folyamatok összességéből áll.

A decentralizált, gyorsan növekvő, államilag nem szabályozott kibertér egyre nagyobb biztonsági problémákat vet fel, ebben a környezetben a névtelenség és a követhetetlenség mögé bújva a következmény-nélküliségben remélve lehet hírszerző tevékenységet folytatni, kormányzati és üzleti rendszereket kompromittálni, mások tulajdonát törvénytelen eszközökkel elvonni. A kibertérből jövő támadások eredetét igen nehéz egyértelműen megállapítani, leginkább a kibertámadások céljából, eszközrendszeréből és nagyságrendjéből

lehet következtetni arra, hogy hagyományos kiberbűnözés vagy államilag finanszírozott támadás ellen kell védekezni. Fentiek alapján a kibertérben megjelenő veszélyek forrásuk szerint az alábbi nagy csoportba oszthatók: állami vagy üzleti hírszerzés, bűnözés, terrorista csoportok, valamint aktivista egyének vagy csoportok.

A fenti veszélyek okán a közigazgatás és a társadalom működését lehetővé tevő informatikai infrastruktúrák, illetve a nemzeti adatvagyon védelme, a kiberbiztonság fenntartása kiemelt feladattá vált; alapvető kormányzati igénnyé és egyben feladattá emelve a kiberbiztonság biztosítását. Az állam kiberbiztonsága az információs társadalmak biztonságának szerves része lett: kiberbiztonság nélkül nem képzelhető el sem a nemzeti adatvagyon, sem az állami működés szempontból létfontosságú infrastruktúrák biztonságos működtetése.

Napjaink egyik meghatározó fejleményévé vált, hogy a nemzeti adatvagyon és a létfontosságú infrastruktúrák működésének kiber-kitettsége olyan szintre emelkedett, hogy egy infokommunikációs katasztrófa valószínűsíthetően ugyanakkora vagy akár nagyobb károkat képes okozni a nemzeti szuverenitás védelme, illetve a nemzetgazdaság működése számára, mint a hagyományos biztonságpolitikai kihívások, vagy egyes természeti katasztrófák.

A kibertérben megjelenő veszélyek és a lehetséges válaszlépések számbavételével határozható meg a kiberbiztonság jelentése, miszerint a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

A kibertérben fellépő veszélyek nem pusztán virtuális fenyegetések, kihatnak a fizikai világra is, mivel a kibertérhez kapcsolódó kommunikációs, irányító és ellenőrző rendszereiken keresztül a létfontosságú rendszerek és létesítmények folyamatos és biztonságos működése nagymértékben függ a kibertér még kialakítandó biztonsági normáktól. Biztonságpolitikai szempontból egyértelműen érzékelhető, hogy a biztonság- és védelempolitika szárazföldi, légi, tengeri és űr dimenziója mellett a kibertér, mint az ötödik biztonságpolitikai dimenzió jelent meg, ami rövid időn belül az egyik legfontosabb biztonságpolitikai dimenzióvá válhat.

A kibertérben való tevékenység elérkezett arra a gazdasági és politikai befolyásolási képességi fokra, s ennek következtében a kibertér biztonságának kérdése arra a nemzeti biztonságpolitikai szintre, hogy az a korábbi technikai részletszabályok helyett átfogó és összetett szabályozást igényel. A Magyarországgal szövetséges EU és NATO tagállamokban sorra kormányzati koordinációs szervezetek alakultak, együttműködési fórumokat alapítottak a közigazgatás, a gazdasági (üzleti), a tudományos (akadémiai) és civil szférák között, szakosított intézményeket működtetnek. Kiberbiztonsági stratégiákat alkotnak, kiberbiztonsági törvényeket fogadnak el, nemzeti és nemzetközi kiber válságkezelési mechanizmusokat és együttműködéseket alakítanak ki, tudatosító és képzési programokat indítanak be, valamint üzleti motivációs rendszereket állítanak fel a nemzeti kiberbiztonsági helyzet javítására.

Magyarország Nemzeti Kiberbiztonsági Stratégiája alapjaiban a 2001-ben elfogadott ún. „Budapest Konvenció"-ig nyúl vissza, amely egyrészt nemzetközi fontosságú konkrét magyar hozzájárulás a globális kiberbiztonság területén, másrészt napjainkig az egyetlen jogi kötőerővel bíró, referenciaként használt nemzetközi dokumentum. Az Egyezményben

megfogalmazott alapelvek mindmáig érvényesek, és nemzetközi szinten is széles körben elfogadottak.

A stratégia kapcsolódik:

- Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozathoz,
- Magyarország Nemzeti Katonai stratégiájának elfogadásáról szóló 1656/2012. (XII. 20.) Korm. határozathoz,
- a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényhez, azon belül a létfontosságú rendszerek és létesítmények hálózatbiztonsági környezetének kialakításához,
- a Magyary Zoltán Közigazgatás-fejlesztési Programhoz,
- a Digitális Megújulás Cselekvési Tervhez,
- az Európai Unió stratégiai törekvéseihez, úgymint a Digitális Menetrend, valamint az Elektronikus Kormányzati Cselekvési Tervhez,
- az Európai Parlament által 2012. november 22-én elfogadott, a kiberbiztonságról és védelemről szóló, 2012/2096(INI) számú állásfoglalásához,
- az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én "Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményhez.

A stratégia alapelve az átfogó és összehangolt megközelítés:

- melyben kormányzati és nem-kormányzati, katonai, rendvédelmi és civil, nemzeti és nemzetközi, gazdasági és politikai eszközök egyaránt megfelelő hangsúllyal szerepelnek,
- ahol a felelősségek letisztázva, összehangoltan fogalmazódnak meg,
- amely a kormányzati és a magánszféra önkéntes együttműködésére, önkéntes információ-megosztásra építve a kormányzat és az érintett szférák közös erőfeszítésével kerül megvalósításra.

A stratégia alapvető célja, hogy Magyarországon az informatikai eszközök, rendszerek és szolgáltatások, valamint az elektronikus hírközlési infrastruktúra és szolgáltatások üzembiztosak legyenek, továbbá megfelelő szintű felkészültséggel és védelemmel rendelkezzenek a kiberfenyegetések és kibertámadások ellen.

Jelen előterjesztés 2. mellékletét képező, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény a kormányzati koordináció céljából a Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) létrehozásáról rendelkezik, amelyre a Miniszterelnökség irányításával az érintett minisztériumok és hatóságok bevonásával kerül sor. A Tanács tevékenységén keresztül elősegíti a kiberbiztonság szabályozását, támogatja a források hatékony felhasználását, felügyeli a stratégia és akcióterv teljesülését, folyamatosan követve a kibertér változásait, szükség esetén javaslatot tesz ezek megújítására, a Miniszterelnökség által delegált kiberbiztonsági koordinátoron keresztül ellátja az egységes magyar álláspont kialakítását és képviseletét a nemzetközi politikai együttműködésekben.

Az együttműködés erősítése érdekében a Tanács létrehozása mellett olyan egyeztető fórum is kialakításra kerül, amelyben a kormányzat kijelölt képviselői és a civil, a gazdasági és a tudományos szektor meghatározó szereplői tudnak együttműködni a kiberbiztonság növelése

érdekében. A fórum működését középvezetői szintű munkacsoportok segítik. Az együttműködés kiterjed az 1249/2010. (XI. 19.) kormányhatározattal létrehozott Kritikus Infrastruktúra Védelmi Tárcaközi Szakmai Munkacsoporttal történő kapcsolattartásra is, amely az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi Irányelv végrehajtását segíti elő. Az együttműködési rendszer egyben kezeli a Kritikus Infrastruktúra Védelmi Konzultációs Fórummal és a Fórum munkáját segítő munkacsoportokkal történő kapcsolattartást is, melyek elsődleges feladata a kormányzati szereplők és a civil szféra kritikus infrastruktúra-védelemmel kapcsolatos együttműködésének megteremtése.

Háborús helyzetben a háborús vezetési rend egységességének elvéből kiindulva a Magyar Honvédség látja el a kiberműveleti tevékenységek országos koordinálását, ideértve úgy a katonai, mint a polgári célú kommunikációs és információs rendszerek védelmének irányítását.

A megelőzés, felkészülés és ellenőrzés minden esetben elsősorban az érintett szervezet saját felelőssége. Ezek megtámogatására és megerősítésére azonban ún. szakosított intézményeket szükséges működtetni. Ilyen speciális szakértelemmel és hatáskörrel rendelkező szakegység a rendőrség, valamint a Nemzeti Adó- és Vámhivatal szervezeti keretein belül is működik a számítógépes bűnözés elleni harcra szakosodott egységek formájában, valamint az Országos Katasztrófavédelmi Főigazgatóságon a kritikus infrastruktúrák informatikai védelméért felelős szervezeti egység keretében. Ilyen szervezet a Nemzeti Biztonsági Felügyelet is, amely sérülékenység vizsgálatot végez. Magyarország nemzetbiztonsági szolgálatai a kibertérben fellépő fenyegetések elhárítására és információszerzésre szakosodott szervezeti egységeket alakítottak ki. A Magyar Honvédség ellátja a katonai célú kommunikációs és információs rendszerek működtetését és védelmét, fokozatosan alakítja ki kibervédelmi képességeit, felhasználva az önkéntes tartalékos rendszerbe jelentkező szakértőket is. Mindezen szakosított intézmények munkáját a Nemzeti Média- és Hírközlési Hatóság, mint szakhatóság, kormányzati felkérésre segítheti. Az említett szervezeteken kívül további közigazgatási szervezetek és állami intézmények látnak el a hatásköri jogszabályokban lefektetett kiberbiztonsági feladatokat.

A kiberbiztonsági események operatív kezeléséhez kapcsolódó alapfeladatot lát el az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által akkreditált tagszervezeteként működő kormányzati eseménykezelő központ, valamint ágazati esemény- illetve incidenskezelő központok (CERT-ek). Kiemelendő, hogy a szakosított intézmények kiberbiztonsági tevékenységük során együttműködnek a személyes adatvédelem és a titokvédelem kapcsán hatósági feladatokat ellátó hatóságokkal, valamint a Kormányzati Kiberbiztonsági Koordinációs Tanáccsal.

A magyar kibertér biztonságának szabályozása több lépésben történik meg. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvénnyel Magyarország gondoskodott a kritikus infrastruktúrák védelméről, érintve azok hálózatbiztonsági követelményeit. A jelen előterjesztés 2. mellékletében szereplő törvényjavaslat útján az állami és önkormányzati szervek elektronikus információbiztonsága kerül szabályozásra, amely felhatalmazást ad a kapcsolódó végrehajtási szabályok kormányrendeletek és/vagy miniszteri rendeletek megalkotására. Ezen jogszabályokat egészítik ki azok az operatív együttműködési megállapodások, melyek egyrészről a

kormányzati szervek közötti munkafolyamatokat rendezik, másrészt a magyar kibertér nem kormányzati tényezői és a kormányzati szervek közötti kapcsolatok jogalapját teremtik meg.

A nemzetközi együttműködés területén igen sikeres és elismert Magyarország eddigi részvétele a különböző nemzetközi együttműködési struktúrákban, többek között:

- az Európai Unió tagországai által önkéntes alapon szerveződött Európai Kiber Válság Együttműködési Keret (European Cyber Crisis Cooperation Framework) munkacsoportjában,
- az Európai Hálózati és Információbiztonsági Ügynökség, az ENISA által kialakított képességfejlesztő együttműködésekben,
- az International Watch and Warning Network tagállamok „kibervihar" (Cyberstorm) típusú nemzetközi együttműködései keretében lezajlott nemzetközi gyakorlatokon,
- a Meridian konferenciasorozathoz hasonló kormányzati együttműködésekben.

A jövőben még hangsúlyosabban és koordináltabban szükséges részt venni a szabad és biztonságos globális kibertér kialakításáért felelős nemzetközi együttműködésekben, ezért kiemelt figyelmet kell fordítani a 2012-es „Bizalommal és biztonsággal a szabadságért és fejlődésért" mottójú Budapesti Kibertér Konferencia utókezelésére és a magyar kormány aktív szerepet kíván vállalni a 2013-as szöuli konferencia előkészítésében.

A tudatosság növelése és a megfelelő szakemberek biztosítása érdekében kiemelt figyelmet kell fordítani arra, hogy az oktatás minden területén megjelenjen a kiberbiztonsági képzés. Speciális képzési formát igényel a kormányzati tisztviselők alap-, illetve továbbképzése, annak érdekében, hogy az informatika szakterületen dolgozó kormányzati tisztviselők megfelelő tudás birtokában képesek legyenek az e-közigazgatást egyre szélesebb körben alkalmazó magyar közigazgatás elektronikus információs rendszereinek biztonságos működtetésére. A Gyermekbarát Internet Európai Stratégiájának célkitűzéseivel összhangban kiemelten fontos területként szükséges kezelni a gyermekvédelmet.

A Nemzeti Kiberbiztonsági Stratégiában meghatározott feladatok ellátására munka- és intézkedési terv elkészítése szükséges, amelynek végrehajtását a Miniszterelnökség irányítása alatt álló Tanács irányítja és ellenőrzi. A munka- és intézkedési tervben meghatározott feladatok és mutatószámok követik az Európai Hálózati és Információ Biztonsági Ügynökségnek a nemzeti kiberbiztonsági akciótervekre vonatkozó ajánlását.

A magyar kormány kormányzati felelőssége tudatában azért készítette el a jelen Stratégiát, hogy mind a ma generációja, mind a jövő generációi a magyar kiberteret szabad, biztonságos és innovatív környezetként használva tudjanak a XXI. század kihívásaira válaszolni, ezzel is erősítve saját boldogulásukat és hazájuk jólétét.

*Melléklet a ..... törvényhez*

## ÁLTALÁNOS INDOKOLÁS

A modern állam, és annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Az elektronikus információs rendszerek nélkülözhetetlenné váltak a társadalom egésze számára, mert az állam működése, a különböző szolgáltatások megvalósítása és igénybevétele elképzelhetetlen ezen rendszerek nélkül. Már önmagukban ezeknek az információs rendszereknek a kiesése is katasztrófahelyzetet idézhet elő. Információs rendszereink és hálózataink – azok közül is elsősorban azok, amelyek működése elengedhetetlen a társadalom és a gazdaság zavartalan működéséhez – egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel. A szándékos károkozások olyan formái, mint a különböző hackercsoportok számítógépvírusokkal történő vagy az információs rendszer leállására vezető ún. szolgáltatás megtagadást eredményező támadásai egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Folyamatosan növekvő fenyegetést jelent sérülékeny információs rendszereinkre a hadviselés egy új formája, amelyet kiberműveleteknek (angolul: cyber operations) neveznek, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus. A különböző információs infrastruktúrák, eszközök, és szolgáltatások bármelyikének megsemmisülése vagy sérülése a társadalom széles rétegeit érintheti. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell.

A törvénytervezet az állam kiberbiztonságot érintő szerepét és feladatait meghatározó Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat figyelembevételével készült.

Bizonyos közigazgatási informatikai rendszerek biztonságát korábban az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet szabályozta, amely 2012 áprilisában hatályon kívül helyezésre került, így jelenleg nincsen olyan jogszabály, amely egységes biztonsági követelményeket szabna az elektronikus információk védelmével kapcsolatban.

A minősített adatok és az ezeket kezelő elektronikus információs rendszerek védelme a minősített adatok védelméről szóló 2009. évi CLV. törvényben és a végrehajtására kiadott rendeletekben szabályozásra került.

A nemzet szempontjából fontos, a minősített adatok körébe nem tartozó, de a kezelt adatok jellegére és a nyilvántartások alapján végzett állami feladatok fontosságára tekintettel kiemelt jelentőségű állami nyilvántartások védelmének biztosítását a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény szolgálja.

Jelen törvény hatálya kiterjed a létfontosságú infrastruktúrákra is, melynek alapvető rendelkezéseit – a Kormány 2012. szeptembert 12-ei ülésén megvitatott és elfogadott – a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényjavaslat tartalmazza.

A törvényjavaslat tudatosan használja az információbiztonság, információs rendszer kifejezések előtt az „elektronikus" jelzőt. Az információbiztonság ugyanis a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben az elektronikus információs rendszerek biztonsága csak az elektronikus információs rendszerekben szereplő adatok, és az azokat kezelő rendszer védelmét jelenti. A törvényjavaslat pedig az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza az azokat kezelő szervezetek tudatos biztonságának növelésén keresztül.

Az elektronikus információs rendszerek védelme egy igen széles körű információvédelem része, amely önállóan is működtethető. A NATO *Security within the North Atlantic Treaty Organisation* direktívája szerinti elektronikus információvédelmen (INFOSEC) kívül az információvédelem többi részét (személyi védelem, dokumentumvédelem, fizikai védelem, elhárítás/hírszerzés) is magába foglalja, de csak az elektronikus információs rendszer vonatkozásában.

Az elektronikus információs rendszerek értelmezése az informatikai, a kommunikációs, és az egyéb elektronikus rendszerek konvergenciájára épül. Az információs társadalomhoz és a médiához kötődő iparágak konvergenciáról az Európai Bizottság *i2010: európai információs társadalom a növekedésért és a foglalkoztatásért című* (COM(2003) 784) közleménye az európai audiovizuális politika szabályozásának jövőjére vonatkozóan megállapítja, hogy „Az információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája végre mindennapjaink valóságává válik ...".

A törvényjavaslat egy preventív szabályozási környezetnek az alapjait kívánja megteremteni, amely ténylegesen a megelőzést helyezi előtérbe és ezen keresztül a biztonsági problémák kialakulásának mérséklését és az előforduló biztonsági események számának csökkentését, illetve tudatos kezelését célozza.

## RÉSZLETES INDOKOLÁS

### Az 1. §-hoz

Az 1. § a törvényjavaslat értelmező rendelkezéseit tartalmazza.

Az értelmező rendelkezések az elfogadott és általánosan alkalmazott hazai szakkifejezésekre épülnek. Ezek jelentős része a Kormány 3296/1991. (VII. 5.) határozata alapján 1991.november 27-én létrehozott Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlásaként 1996. április 2-án elfogadott Informatikai Rendszerek Biztonsági Követelményei című dokumentumban rögzítésre került. Az itt leírt fogalmak és definíciók az Informatikai Biztonság Kézikönyve (Verlag Dashöfer, Budapest, 2000-2005), illetve a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásaiban is megjelentek, a nemzetközi szakirodalmat, szabványokat figyelembe véve újra feldolgozva korábbi definíciókat. Az információ- és kommunikációtechnológiák konvergenciája miatt magyarul az informatikai és kommunikációs technológia, néha az informatikai és kommunikációs rendszerek kifejezéseket, gyakran az angol information and communication technology kifejezés rövidítését az ICT-t vagy ennek rossz magyarsággal való átírását az IKT-t használják. Emellett az informatikai, infokommunikációs technológia, vagy az infokommunikációs rendszerek kifejezéseket is alkalmazzák. Az eltérő fogalomhasználat

egységesítése érdekében a törvényjavaslat az elektronikus információs rendszerek kifejezést használja.

A 2. §-hoz

A törvényjavaslat 2. §-a a szabályozás személyi és tárgyi hatályát határozza meg.

A személyi hatály az alkotmányos rend fenntartása szempontjából kiemelt fontosságú közszolgálati szervek adatait kezelő szervezetek és a nemzeti adatvagyont kezelő szervezetek mellett az európai és nemzeti létfontosságú információs rendszerek, rendszerelemek közé tartozó szervezetekre terjed ki. Az érintett szervek felsorolásának alapját a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény, a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény, az ügyészségről szóló 2011. évi CLXIII. törvény és a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény képezi. A Kormány és a kormánybizottságok nem kerülnek a törvényjavaslat személyi hatálya alá, mivel önálló szervezetrendszerrel nem rendelkező testületként gyakorolják feladataikat és önálló elektronikus információs rendszerekkel nem rendelkeznek.

A tárgyi hatály a kiemelt fontosságú közszolgálati szervek adatait és a nemzeti adatvagyont kezelő szervezetek, valamint az európai és nemzeti létfontosságú információs infrastruktúrák elektronikus információs rendszereinek védelmére vonatkozik.

Ez a személyi és tárgyi hatály kellően széles körű ahhoz, hogy Magyarország kibervédelme szempontjából minden, az állam működése szempontjából lényeges elektronikus információs rendszer védelmére kitérjen.

A törvényjavaslat az egységes szabályozási környezet kialakítása érdekében rendelkezik a más törvényekkel való összhangról. Ennek értelmében a minősített adatok vonatkozásában e törvény rendelkezéseit a minősített adat védelméről szóló 2009. évi CLV. törvényben foglalt eltérésekkel kell alkalmazni.

A törvényjavaslat kifejezetten elkülöníti rendvédelmi szervek és a rendvédelmi szervet irányító miniszter által irányított szervek, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség zárt célú elektronikus információs rendszerei, a külpolitikáért felelős miniszter diplomáciai információs célokra használt zárt célú elektronikus információs rendszerei, a Miniszterelnök irányítása alá tartozó Információs Hivatal, valamint a Nemzeti Adó- és Vámhivatal állami költségvetési bevételek biztosítását támogató elektronikus információs rendszereit. Ezeknek az esetében is kötelező a megfelelő biztonság kialakítása és fenntartása, de a rendszerek fokozott védelme érdekében a hatósági és eseménykezelési feladatok az irányítást ellátó miniszter felelősségi körén belül maradnak, így nem nő azok köre, akik ezen érzékeny rendszereket, azok védelmi megoldásait megismerhetik, vagy akár annak védelmét felülbírálhatnák.

A 3. §-hoz

A törvényjavaslat arra való tekintettel, hogy napjainkban fontos kérdés az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése általánosan elfogadott gyakorlattá vált (ezzel a nemzeti adatvagyon törvény is foglalkozik

már), korlátozza az adatvagyon Magyarország területén kívüli kezelését. Ez a tilalom nem terjedhet ki azonban a Magyar Honvédségre és a külképviseletekre, mert ezek feladatukból adódóan külföldön is kell, hogy dolgozhassanak adataikkal, elektronikus információs rendszereikkel. A létfontosságú információs infrastruktúrákhoz olyan intézmények tartozhatnak (pénzintézetek, távközlési szolgáltatók, stb.), amelyek esetében a csak Magyarország területén belül engedélyezett adatkezelés súlyos költségkihatásokkal járhat. Itt az adatok Európai Unión belüli kezelésének kényszere elégséges korlátozás, mert az uniós és az uniós országok nemzeti szabályozása megfelelő védelmet és ellenőrizhetőséget biztosít.

Mivel a nemzeti adatvagyon eleme része lehet a létfontosságú információs infrastruktúráknak, de kötelezően nem az, ezért a törvényjavaslat szerinti szigorító kivétel a csak hazai kezelésre. Az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése miatt került a törvényjavaslatba az a kényszer, hogy amennyiben nem Magyarországon bejegyzett cég végzi az adatok kezelését, akkor legyen elérhető kapcsolattartó személy, illetve ez a személy folyamatosan (24/7) legyen felkérhető, utasítható a törvény végrehajtásával kapcsolatban, és akár a felelősségre vonásra is sor kerülhessen.

A 4. §-hoz

A nemzeti adatvagyont kezelő szervezetek, illetve a létfontosságú rendszerelemként számításba vehető szervezetek egy része komoly munkával és jelentős költségekkel auditáltatta szervezetét az informatikai biztonságirányítási rendszerről szóló nemzetközi ISO/IEC 27001 szabvány szerint, illetve a nemzetközi egyezménnyel elfogadott Common Criteria, vagy a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma szerint minősített informatikai eszközöket, vagy más szabványok vagy ajánlások alapján tanúsított rendszerelemeket használ. Ezek a minősítések garanciát szolgáltatnak a tudatos eljárásokra, így – és a jogbiztonság megőrzését is szem előtt tartva – ezen tanúsítványokat a hatóság az eljárása során figyelembe veszi.

Az 5-6. §-hoz

A törvényjavaslat egyik legfontosabb eleme az alapvető elektronikus információbiztonsági követelmények meghatározása. Az ebben a körben használt fogalmakat az informatika szakma már régóta használja ugyan, de azok törvényi szinten, általános követelményként történő megfogalmazása olyan előrelépést jelent az elektronikus információs rendszerek biztonsága területén, ami önmagában mérföldköve lehetne az elmúlt időszak ez irányú szabályozási törekvéseinek.

A törvényjavaslat az elektronikus információs rendszerek biztonságának általános követelményeit az elektronikus információs rendszerek biztonságának definíciójából levezetve, úgy határozza meg, hogy a védelem minden lehetséges módja (logikai, fizikai és adminisztratív védelem) a tervezéstől a megvalósításig felhasználásra kerüljön. A védelem olyan legyen, hogy lehetőleg kerülje el a fenyegetések bekövetkezését, de ha ez nem lehetséges, akkor erről annak bekövetkezése előtt az érintettek szerezzenek tudomást. Az elektronikus információs rendszerek esetében különösen fontos a biztonsági események bekövetkeztének azonnali észlelése, hogy arra mielőbb reagálhasson a szervezet vezetése. A biztonsági esemény bekövetkezése után kiemelt szerepet kap a gyakran incidenskezelésnek is nevezett biztonsági események kezelése. Ennek során a bekövetkezett biztonsági események hiteles dokumentálása, a bekövetkezett károk következményeinek a kezelése, a biztonsági eseményeket kiváltó okok kivizsgálása és felelősségek megállapítása és a szükséges

felelősségre vonás után a szabályozás javításával, a védelmi intézkedések kiegészítésével vagy megerősítésével és az érintettek oktatásával, tudatosság képzésével gondoskodni kell arról, hogy az adott biztonsági események bekövetkezésének esélye kisebb legyen és az ezáltal okozott kár is csökkenjen.

Az információ biztonságának érdekében a megelőzés-észlelés-reagálás-eseménykezelés, az ún. PreDeCo elvek felhasználásával a törvényjavaslat előírja a lehetséges biztonsági események megelőzését, a bekövetkezett biztonsági események kezelését.

A törvényjavaslat elfogadja azt a nézetet, hogy a védelem tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. A biztonság a védett rendszer olyan állapota, amelyben annak védelme az összes számításba vehető fenyegetést figyelembe veszi, a rendszer valamennyi elemére kiterjed, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul és annak költségei hosszútávon arányosak a fenyegetések által okozható károkkal.

A biztonság nagyon sok részletet jelent, ugyanakkor egy és oszthatatlan. Ezt az egy és oszthatatlan biztonságot a védelmi tevékenységek (folyamatok) részterületein keresztül lehet megvalósítani. Az információbiztonság alapvető feladatai a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás és a biztonsági események kezelése. A korai figyelmeztetés előírásként történő meghatározása nem figyelmeztető rendszer kiépítésére, hanem a szervezet aktív cselekvési képességére vonatkozik, az észlelés folyamatának azon része, amely más szervezettől érkező figyelmeztetések azonosítására és feldolgozására utal.

A biztonság tervezése, kialakítása során e feladatok mindegyikére kellő hangsúlyt kell fektetni ahhoz, hogy a védelem elérje célját.

A 7-8. §-hoz

A védelemnek költséghatékonynak kell lennie, azaz csak a lehetséges veszteségek és károk nagyságrendjével arányosan indokolt a védelemre költeni. Ennek érdekében meg kell állapítani, hogy az adott elektronikus információs rendszer, illetve az abban kezelt adatok a bizalmasságának, a sértetlenségének vagy a rendelkezésre állásának elvesztése külön-külön milyen nagyságrendű károkat okoz. A nagyságrend megállapítása elégséges, mert egyrészt a pontos értéket nehéz, hosszadalmas és költséges meghatározni, másrészt a nagyságrend ismerete már elég ahhoz, hogy a védelemre történő ráfordítások értéke meghatározható legyen. Mivel az osztályba sorolást külön el kell végezni a bizalmassági, sértetlenségi és rendelkezésre állási szempontok szerint is, így minden egyes elektronikus információs rendszerre számos kombinációban állíthatók be a műszaki védelmi intézkedések. Ez biztosítja a kockázatarányos és költséghatékony műszaki védelmet. A biztonsági osztályozás részletszabályainak meghatározására a törvény végrehajtási rendeletében kerül sor.

Ilyen biztonsági osztályozás és a hozzátartozó követelmények már megtalálhatók az *Informatikai Biztonsági Irányítási Követelmények* című Közigazgatási Informatikai Bizottsági ajánlásban (KIB 25. sz. ajánlás 1-2. kötet), valamint hasonló követelménylistát tartalmaz a KIB 28. ajánlás is. A törvényjavaslat ezen technológiai követelményeknek felülvizsgálatát és miniszteri rendeletben történő megjelenítését szorgalmazza.

A szervezet vezetőjének a felelőssége, hogy az elektronikus információs rendszerek osztályba sorolását elvégezzék. Mivel a kockázatok folyamatosan változnak, ezért az osztályba sorolást

rendszeresen frissíteni kell. Ez az elvárás biztosítja azt, hogy a biztonság ne egy statikus, egyszer kialakított állapot legyen, hanem a szervezetnek folyamatosan figyelemmel kelljen kísérnie a rá vonatkozó kockázatokat, azaz legyen egy kockázatkezelési folyamata. A mérvadó információbiztonsági szabványok és ajánlások kivétel nélkül ezt a lépést tekintik a legalapvetőbb elvárásnak a biztonság megteremtéséhez.

Az elektronikus információs rendszerek biztonsági osztályának és a szervezetek biztonsági szintjének elérési követelményei a fokozatosság elvére épülnek. Az adott osztály és szint elérése a szervezet feladat- és hatáskörének függvénye, amelyek biztosítják, hogy a szervezet a feladatellátásával, a közigazgatási szervezetrendszerben elfoglalt helyével, piaci szerepével, valamint elektronikus információs rendszereinek jelentőségével, állapotával arányosan kerüljön kialakításra.

A 9-10. §-hoz

A megelőzés alapját képező, kockázatokkal arányos, költséghatékony védelem kialakításának egyik nemzetközileg elfogadott eszköze az információbiztonsági irányítási rendszer kialakítása a szervezetnél. Ez biztosítja, hogy az alapvető biztonsági követelmények meghatározása egy magas absztrakciós szinten is megtörténjen. A szervezeti biztonság megteremtése azért is fontos, mert bevezetésének költsége elenyésző (elsősorban szabályozási feladatokat határoz meg), mégis jelentősen növeli az információbiztonság szintjét. Eszerint minden érintett szervezetnek kötelessége rendszerszinten kezelnie az információbiztonságot.

A törvényjavaslat egyik fontos követelménye az, hogy a szervezetnek azt a biztonsági szintet kell elérnie az információbiztonsági irányítási rendszerében, amely megegyezik az általa kezelt elektronikus információs rendszerek közül a legmagasabb biztonsági osztállyal. Azaz, ha pl. nemzeti adatvagyon-elemet kezelő rendszere van a szervezetnek, a legmagasabb érettségi szintet kell elérnie, vagy ha pl. egy központi államigazgatási szerv olyan elektronikus információs rendszert kezel, melyben az információk bizalmassági besorolása 2., sértetlenségi besorolása 3., rendelkezésre állási besorolása pedig 1., akkor a szervezeti biztonsági szintjét 3. szintre kell hoznia. Ha ennél a szervezetnél minden érték 2., a szervezeti biztonsági szintje akkor is 3., hiszen a törvényjavaslat 9. § (2) bekezdés b) pontja eszerint rendelkezik.

A 7-9. és a 10-11. §-ok együttes alkalmazása költséghatékony megoldás, mert nem a szervezet egészénél egységesen, azonos biztonsági osztályba sorolva kell az elektronikus információs rendszerek védelmét megvalósítani, hanem ez rendszerenként eltérő lehet. A szervezet biztonsági szintjének elérése viszont garantálja, hogy az információbiztonsági irányítási rendszer a legmagasabb kockázatok által elvárt legyen.

A szervezeti biztonsági szintet ugyan az általa kezelt elektronikus információs rendszer besorolása határozza meg, de ennek a biztonsági szintnek az elérése jól tervezhető módon, kellő időráfordítással valósítandó meg. A szervezet vezetője kezdetben besorolja a szervezetet az aktuális érettségi szintre, majd kétévente köteles egy szintet lépni a skálán mindaddig, amíg eléri az elvárt szintet. Pl. egy olyan központi államigazgatási szervnél, ahol nincsen jelen az információbiztonsági szabályozás, akár 4 év is rendelkezésre áll a követelmények teljesítéséhez.

A 11-12. §-hoz

A törvényjavaslat ezen szakaszai az érintett szervezetek vezetőinek legfontosabb, a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától független feladatait és felelősségeit határozzák meg. Ezek a feladatok elsősorban adminisztratív feladatok, amelyek arra vonatkoznak, hogy a szükséges szinten és a szükséges mélységben legyen szabályozva az elektronikus információs rendszerek biztonsága, és annak nevesített felelőse legyen a szervezetnél. A szervezet köteles biztonsági stratégiát és informatikai biztonsági szabályzatot készíteni, utóbbiak része lehet a biztonságpolitika is. A szakmai irányítást ellátó miniszter által meghatározott ágazati informatikai biztonságpolitika és ágazati informatikai biztonsági stratégia keretében szabályzat minták és iránymutatások kiadására is sor kerülhet.

A szervezet vezetőjének felelősségét nem csökkenti, ha az elektronikus információs rendszer kiszervezésre kerül, függetlenül attól, hogy a közreműködőkkel kötött szerződésben köteles a törvényi rendelkezések kötelező alkalmazását előírni.

Az előírások között a folyamatos oktatás, képzés kötelezettségének rögzítése egy, a technikai fejlődés következtében gyorsan változó területnek való megfelelés miatt szükséges.

A szervezet vezetője köteles együttműködni a hatósággal, így lehetőség nyílik arra, hogy a védelmi tevékenységben szükséges kapcsolattartás és információcsere megvalósulhasson. Ezen információcsere egyik legfontosabb esete a törvényjavaslatban külön nevesítésre került: a szervezet vezetője köteles a bekövetkezett biztonsági eseményeket a hatóság, a Nemzeti Biztonsági Felügyelet és a biztonsági események kezelésére vonatkozó feladatokat ellátó kormányzati eseménykezelő központ tudomására hozni. Ez is hozzájárul az országos szintű kibervédelmi rendszer kialakításához; mely összhangban van az Európai Unió tervezett kibervédelmi intézkedéseivel.

A 13. §-hoz

A törvényjavaslat előírja, hogy a szervezeteknek legyen olyan munkatársa az elektronikus információs rendszer biztonságáért felelős személyében, aki képes az elektronikus információs rendszerek védelmének feladatait összefogni, koordinálni. Hatásköre mindenre ki kell, hogy terjedjen az elektronikus információs rendszerek védelme kapcsán, ugyanakkor felelőssége oszthatatlan. Az információs rendszer biztonságáért felelős személy alapfeladatainak meghatározására a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától függetlenül, általánosságban került sor.

A törvényjavaslat nagy hangsúlyt helyez a felhasználói tudatosság növelésére, melynek révén elérhető, hogy maguk az érintettek is körültekintően védjék adataik biztonságát, megértve a kérdés jelentőségét. Ennek érdekében a törvény hatálya alá tartozó szervezetek munkatársainak, kiemelten az elektronikus információs rendszer biztonságáért felelős személyeknek a törvény kötelező képzésen való részvételt ír elő.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 77. § (1) bekezdés a) pontjában foglaltakra figyelemmel a Kormány rendeletben állapítja meg azokat a munkaköröket, amelyek – a 2. számú melléklet 18. pontja alapján – fontos és bizalmas munkakörnek minősülnek, illetve e munkakörök tekintetében meghatározza a biztonsági ellenőrzések szintjét. Azon kormányzati szándékhoz igazodva, amely szerint a jövőben kiemelt figyelmet kell fordítani arra, hogy az állami szereplők számára informatikai

szolgáltatást nyújtó személyek vagy szervezetek esetén az informatikai felelősök nemzetbiztonsági ellenőrzése megtörténjen, a jövőben az elektronikus információs rendszer biztonságáért felelős személy esetében is felmerülhet ilyen irányú igény.

A 14-16. §-hoz

A törvényjavaslat szerint létrejön az informatikáért felelős miniszter irányítása alatt, a minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező szervezeti egység (a továbbiakban: hatóság), amely az információbiztonsággal kapcsolatos nyilvántartásokat vezeti, illetve ellenőrzi a törvény betartását.

Létrehozásának indoka, hogy kell egy olyan hatóság, amely képes ellenőrizni az e törvényben foglalt és az ahhoz kapcsolódó követelmény megvalósulását. Ennek keretében jogosult szankcionálni azokban az esetekben, amikor a szervezetnél az elektronikus információs rendszert veszélyeztető informatikai állapot alakul ki. Nem közigazgatási szervek esetében bírságolási joga van.

A 17 §-hoz

A hatóság közigazgatási szervek esetében információbiztonsági felügyelőt nevezhet ki. Az információbiztonsági felügyelő jogosult a szervezet által meghozott védelmi intézkedéseket véleményezni, adott esetben az intézkedéssel szemben kifogással élhet. A fenyegetés elhárítása érdekében intézkedéseket, eljárásokat javasolhat. Ezzel a jogkörrel a törvényjavaslatban foglaltak megvalósítása jelentősen hatékonyabban történhet meg.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 77. § (1) bekezdés a) pontjában foglaltakra figyelemmel a Kormány rendeletben állapítja meg azokat a munkaköröket, amelyek – a 2. számú melléklet 18. pontja alapján – fontos és bizalmas munkakörnek minősülnek, illetve e munkakörök tekintetében meghatározza a biztonsági ellenőrzések szintjét. Az információbiztonsági felügyelő esetében ezért indokolt a munkakörnek az e felhatalmazás szerinti kormányrendeletben történő megjelenítése.

A 18. §-hoz

A Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) feladatai komplex rendszerbe foglalhatóak:

- egyrészről a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény szerinti szakhatóságként igazgatási szolgáltatási díj ellenében közreműködik az osztályba sorolás és a biztonsági szint meghatározására, a hatósághoz érkező bejelentések kivizsgálására vonatkozó, a hatóság által lefolytatott eljárásban, valamint a hatóság éves ellenőrzési terv alapján végzett ellenőrző tevékenységében,
- másrészről a szervezet felkérésére az ellenőrzési tervtől függetlenül is végezhet sérülékenységvizsgálatot, feltárva ez által a biztonsági esemény bekövetkezését megelőzően az esetleges sérülékenységeket, hiányosságokat, költséghatékonnyá téve ez által a megelőzést,
- harmadrészről hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez, valamint a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi

gyakorlatokon felkérésre képviseli Magyarországot, koordinálja, irányítja a magyarországi felek részvételét.

A hatóság és az NBF közötti feladatmegosztás leképezi a kormányzaton belüli feladat meghatározást, melynek értelmében az informatikai terület ellenőrzése az informatikáért felelős miniszter feladat- és hatáskörébe, míg a szélesebb értelemben vett információbiztonság az e-közigazgatásért és a minősített adatok védelmének szakmai felügyeletéért felelős miniszter feladatkörébe tartozik.

A 19-20. §-hoz

A törvényjavaslat a biztonsági események kezelése, a károk mérséklése érdekében megfogalmazza azokat a biztonsági eseményeket kezelő funkciókat, melyek értelmében hálózatbiztonsági helyzetértékeléseket, folyamatos 24 órás ügyeletet kell működtetni.

A törvényjavaslat szerinti kormányzati eseménykezelő központ és annak feladatai korábban is léteztek, az időközben hatályon kívül helyezett, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendeletben. Ágazati eseménykezelő központból (Számítógépes Vészhelyzeti Reagáló Egység – Computer Emergency Response Team, CERT) több is létrehozható – a zárt célú hálózatok esetében ez egyébként is indokolt –, figyelemmel kell lenni azonban arra, hogy a nemzetközi CERT közösség elsősorban bizalmi elven működik, ezért indokolt, hogy Magyarországot egy nemzetközileg elismert CERT, a kormányzati eseménykezelő központ képviselje. A kormányzati eseménykezelő központ az ágazati eseménykezelő központok operatív tevékenységét koordinálja, így részt vesz az információk megosztásában. A kormányzati eseménykezelő központ támogatja a CERT-eket a nemzetközileg elfogadott működési rend kialakításában.

A 21. §-hoz

A törvényjavaslat értelmében Nemzeti Kiberbiztonsági Koordinációs Tanács jön létre és működik

- a törvény hatálya alá tartozó szervezetek együttműködésének irányítása,
- a kiberbiztonsággal összefüggő feladatok ellátásának és a nemzetközi politikai együttműködés koordinálása,
- a kiberbiztonság szabályozásának elősegítése,
- a források hatékony felhasználásának támogatása érdekében,
- felügyeli a Nemzeti Kiberbiztonsági Stratégia végrehajtását.

A Tanács munkáját az általa felkért képviselőkből álló Nemzeti Kiberbiztonsági Fórum és ún. ágazati kiberbiztonsági munkacsoportok segítik. A Tanács jellegéből adódóan sok szempontból képes áttekinteni az elektronikus információs rendszerek biztonságával, a létfontosságú információs infrastruktúrák védelmével, és a kibervédelemmel kapcsolatos feladatokat, javaslataiban képes megjeleníteni az abban résztvevők szakmai álláspontját.

Működése ez által hozzájárul az elektronikus információs rendszerek gyors fejlődéséhez, a fenyegetések változásához igazodó követelmények kialakításához.

A 22. §-hoz

Az elektronikus információs rendszerek összetettsége és működésének sajátossága miatt a gyakorlatban gyakran nem valósul meg a törvényes adatkezelés elvének betartása. A törvényjavaslat külön kiemeli a biztonságos és törvényes adatkezelés követelményeinek kölcsönös figyelembevételét.

A 23. §-hoz

A törvényjavaslat alapvető célja az az elektronikus információs rendszer biztonságáért felelős személy kötelező információbiztonsági képzésének előírása. A hazai felsőoktatási környezetben az információbiztonság területén jelenleg ilyen kötelező jellegű, intézményesített vezetőképzés nincs. A mérnök, a programozó és a gazdasági informatikus alapszakokon és mesterszakokon különböző műszaki jellegű oktatások vannak, amelyek között a Budapesti Műszaki Egyetemen és az Óbudai Egyetemen informatikai biztonsági szakirányú képzést is tartanak. A Nemzeti Közszolgálati Egyetemen a nemzetbiztonsági képzés keretén belül oktatnak informatikai védelmet. Akkreditált felnőttképzés e téren a Nemzetközi Technológiai Közhasznú Kft. (Puskás Alapítvány) informatikai biztonsági felelős képzése, amely alapvetően az időközben hatályon kívül helyezett, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet követelményeihez igazodik. A törvényjavaslatban előírt követelményeknek megfelelő képzés és a vezetőképzés erősítése érdekében mindezekre figyelemmel szükséges egy új átfogó képzési struktúra kialakítása.

Az információbiztonsági tudatosság növelése érdekében a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara javaslatot tesz a képzési követelményekre, és részt vesz a törvény hatálya alá tartozó személyek kötelező oktatásában. Ez biztosítja, hogy az érintettek magas színvonalú képzésben részesüljenek.

A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara az elektronikus információs rendszerek biztonsága, a létfontosságú információs infrastruktúrák védelme, a kibervédelem tekintetében a jövőben nemzeti és esetleges nemzetközi kutatóhelyként is részt vehet a szakterület kutatásában, fejlesztésében. E feladatokban való részvétellel az egyetemi oktatók-kutatók folyamatos gyakorlati ismereteket szereznek, illetve azokat karbantartják. Az oktatói-kutatói kapacitást a szükséges szakmai kidolgozó munkában költséghatékonyabban lehet felhasználni, mint külső cégeket igénybe venni erre a feladatra.

A törvényjavaslat az oktatás, fejlesztés és a gyakorlat kombinációjával egy magas szintű oktatási, kutatás-fejlesztési centrumot hoz létre az elektronikus információs rendszerek biztonságának területén.

A nemzetközi oktatási környezetben már számos akkreditált képzés elfogadott. Ezek közül a legelismertebbek közé tartozik:

- Az Information Systems Audit and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzése, amelyet az USA Védelmi Minisztériuma is szakirányú képzésként ismer el és vezetői szintű ismereteket nyújt. A képzést Magyarországon felsőfokú oktatási intézményekben – külön megállapodás alapján –, az ISACA magyarországi szervezetének felügyeletével, hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.
- Az International Information Systems Security Certification Consortium, Inc. Certified Information Systems Security Professional (CISSP) képzése az informatikai rendszerek

technikai kérdéseinek biztonsági vonatkozásairól szól. A képzést Magyarországon a Budapesti Műszaki Egyetemen hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.

Mindkét (CISM, CISSP) végzettség megszerzéséhez gyakorlati tapasztalatokat is igazolni kell, a képzések időtartama eltérő, a minősítések megtartásához éves szinten meghatározott kreditpontot kell elérni.

Nemzetközileg ismert és elfogadott még az EC-Council Certified Ethical Hacker és Certified Penetration Tester képzés, amely Magyarországon a NetAcadémia Oktatóközpontnál végezhető el.
A képzések üzleti alapon, a hazai viszonylatokhoz képest nagyon drágán működnek, ezért célszerű a költséghatékonyabb és a nemzetközi oktatási környezettel összhangban álló – adott esetben a későbbiekben mesterképzés útján elismertethető – hazai képzést előnyben részesíteni, ami egyúttal a kutatási kapacitás fejlesztését is lehetővé teszi.

A 24. §-hoz

A törvényjavaslat végrehajtásához a tervezetben megfogalmazott végrehajtási rendeletek kiadása szükséges.

A közigazgatási informatikai feladatok kormányzati koordinációjáról szóló 1026/2007. (IV. 11.) Korm. határozat 3. pontja alapján létrehozott Közigazgatási Informatikai Bizottság által 2008 júniusában kiadott, az információbiztonsági követelményekhez kapcsolódóan a meglévő és a terület részletes szabályozását szolgáló 25. ajánlásnak a Magyar Informatikai Biztonsági Irányítási Keretrendszer és Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma részeit és a 28. ajánlás IT biztonsági követelményrendszer – biztonsági szintek követelményeit rendeli felülvizsgálni és azt követően felhasználni. Ezek az ajánlások a szakterület legfontosabb szabványaira, az ISO/IEC 27000-es sorozatra és a Common Criteriára épülnek, de nem teljesen azonosak azokkal. Ezeket a szabványokat már sok helyen használják hazánkban is, általánosan elfogadottak az Európai Unióban és a NATO-ban is. Miniszteri rendeletben történő kiadásukkal elérjük, hogy a hazai követelmények igazodjanak a nemzetközi szabványokhoz, de ennek ellenére Magyarország kormányzata saját hatáskörében képes azt szigorítani, vagy enyhíteni, igazítani a nemzeti igényekhez. A törvényjavaslatban foglalt követelményekhez kapcsolódóan a meglévő és a terület részletes szabályozását szolgáló Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásait célszerű már a törvény elfogadásával egy időben egységes követelményrendszerként kiadni. Ez egyértelművé teszi a részletes szabályozás szakmai tartalmát, és biztos alapot teremt a későbbi szabályozáshoz. A Közigazgatási Informatikai Bizottság 28. ajánlásának elkészítése Európai Uniós forrásból finanszírozott, így megtérülési szempontból is indokolt a további felhasználása.

A 25. §-hoz

A törvényjavaslat hatályba léptető rendelkezést tartalmaz.

A 26. §-hoz

A törvényjavaslat alapján a törvény rendelkezései 2013. július 1–jén lépnek hatályba. Az

átmeneti rendelkezések megfelelő türelmi időt határoznak meg annak érdekében, hogy a törvényjavaslat hatálya alá tartozó alanyok felkészülhessenek a törvényjavaslatban megfogalmazott követelmények betartására és betartatására.

A törvényjavaslatban megállapított határidők összhangban állnak a minősített adat védelméről szóló 2009. évi CLV. törvény 40. §-ában meghatározott 2014. december 31-ei határidővel, mivel a tervezet a szervezetnek a nem minősített adatot kezelő elektronikus információs rendszereit érintően a törvényjavaslatban előírt követelményeknek történő megfelelésre hosszabb időt biztosít.

A 27-28. §-hoz

A törvényjavaslat elfogadásával három törvény módosítása válik szükségessé.
- A minősített adatok védelméről szóló 2009. évi CLV. törvény kiegészítésével egyértelművé válik, hogy a minősített adatokat elektronikusan kezelő rendszerek tekintetében az elektronikus biztonság kialakítása során nem csak a minősített adatokra vonatkozó, hanem az e törvényben meghatározott követelményekre is figyelemmel kell lenni. Ha az egyes elektronikus információs rendszerek összekapcsolásra kerülnek, akkor a minősítésnek ki kell terjednie a minősített adatot kezelő más, nem minősített rendszerekre is. Ha az egyes elektronikus információs rendszerek nem kerülnek összekapcsolásra, akkor a törvényjavaslat rendelkezéseivel összhangban a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet rendelkezéseit is figyelembe kell venni a követelmények meghatározása során.
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény módosítása megszünteti az adatfeldolgozás kiszervezésének tilalmát, amely korszerűtlen szabályozás módosításának szükségességére az Országgyűlés elé 2012 márciusában beterjesztett Nemzeti Adatvédelmi és Információszabadság Hivatal beszámolója is kitért.
- A nemzeti adatvagyonról szóló 2010. évi CLVII. törvény rendelkezéseinek hatályon kívül helyezését a differenciált, ezáltal költséghatékony információbiztonsági védelmi intézkedések iránti igény indokolja.