Útmutató

az elektronikus információs rendszerek fejlesztéséhez a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény és a 418/2024. (XII. 23.) Korm. rendelet alapján

Verzió: 1.0

A korábbi, *az állami és önkormányzati szervek információbiztonságáról szóló 2013. évi L. törvénynek* (a továbbiakban Ibtv.) és a kapcsolódó jogszabályoknak, az elektronikus információs rendszerek fejlesztésére vonatkozó keretei jelentős változáson mennek keresztül az új jogszabályi rendelkezések életbelépésével. Jelen útmutató célja, hogy az érintettek számára közérthető tájékoztatást adjon a változásokról, és főleg a fejlesztés során újként jelentkező feladatokról.

Az elektronikus információs rendszerek (a továbbiakban EIR) fejlesztéséhez kapcsolódó rendelkezések a *Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény* (a továbbiakban: Kibertv.) **II. fejezetének 9. alfejezete**, valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban Vhr.) **II. fejezetének 10. alfejezete** tartalmazza. Ezeket a szabályokat egyaránt alkalmazni kell új EIR-ek fejlesztése és a már meglévő (használatban lévő) EIR-ek továbbfejlesztése vonatkozásában is. A törvény továbbfejlesztésnek tekinti a már működő EIR olyan mértékű fejlesztését, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van (például kibővül a rendszerben kezelt adatok köre, vagy jelentősen megváltozik az adatkezelés technológiája – például valamilyen felhőbe kerül áthelyezésre az érintett rendszer.

A Kibertv. 13. §-a meghatározza, hogy a törvény mely címzettjeinek kell a fejlesztésre, tovább fejlesztésre vonatkozó szabályokat alkalmaznia:

- **a központi államigazgatási szervek, a Kormány kivételével,**
- **a Sándor-palota,**
- **az Alkotmánybíróság hivatala,**
- **az Országos Bírósági Hivatal és a bíróságok,**
- **az ügyészségek,**
- **az Alapvető Jogok Biztosának Hivatala,**
- **az Állami Számvevőszék,**
- **a Magyar Nemzeti Bank,**
- **a Magyar Honvédség,**
- **a fővárosi és vármegyei kormányhivatalok, a vármegyei közgyűlések hivatalai,**
- **a megyei jogú városok és a fővárosi kerületi önkormányzatok képviselő-testületének hivatalai,**

- **a 20 000 főt meghaladó lakosságszámú települések képviselő-testületének hivatalai,**
- **a központi szolgáltató (olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást),**
- **a központi rendszerek szolgáltatói (a központi rendszer felett rendelkezési jogosultsággal rendelkező szervezet, *központi rendszer*: egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett rendszer, amelyet egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek),**
- a Kibertv. 2. és 3. sz. melléklete szerinti szervezetnek nem minősülő többségi állami befolyás alatt álló gazdálkodó szervezetek, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket,
- *a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény* (a továbbiakban: Kszetv.) alapján kijelölt kritikus szervezetek,
- *a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021 évi XCIII. törvény* (a továbbiakban: Vbö.) alapján kijelölt, az ország védelme és biztonsága szempontjából jelentős szervezetek,
- a nemzeti kiberbiztonsági hatóság (a továbbiakban: Hatóság) által alapvető szervezetként azonosított, a fenti szervezetek körébe nem tartozó szervezet. (Az azonosítási eljárás feltételeit a Kibertv. 1. § (6) bekezdése sorolja fel.)

A fejlesztésben érintett szervezetek feladatai:

1. A tervezési ciklusban:

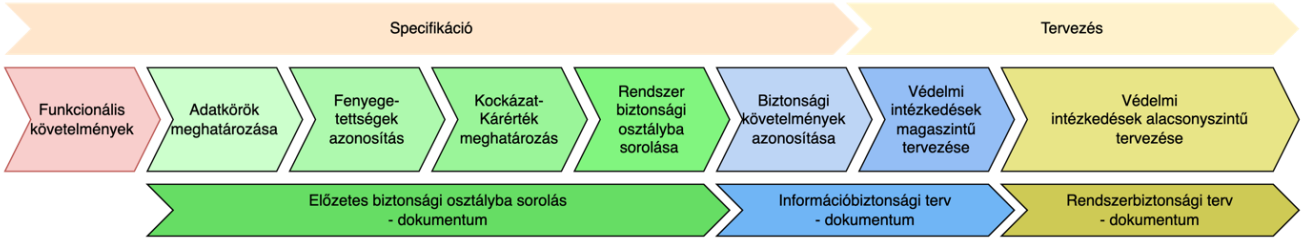
   - A Kibertv.-ben és a Vhr. 1. sz. mellékletében meghatározottak szerinti adatosztályozást kell végeznie a fenti felsorolásban vastagon jelzett alapvető szervezetek körébe tartozóknak, egyéb szervezetek esetében csak akkor, ha a fejlesztésben érintett rendszer esetében nem privát felhőszolgáltatás igénybevétele és külföldi adatkezelés megvalósítása történik.
   - A fejlesztésben érintett rendszer biztonsági osztályba sorolását el kell végezni annak érdekében, hogy a fejlesztendő rendszer biztonsági igényét megfelelően meg lehessen határozni.
   - A jogszabály arról is rendelkezik, hogy az adatosztályozást és a biztonsági osztályba sorolást a tervezési fázison belül
     - belső fejlesztés esetében az erőforrások allokációját megelőzően,
     - külső fejlesztés esetén a fejlesztésre irányuló szerződés megkötését megelőzően olyan módon, hogy **az információbiztonsági követelmények a fejlesztési szerződésben rögzítésre kerülhessenek**.
   - A fejlesztési projektek tervezése, ütemezése során figyelembe kell venni, hogy a Hatóságnak a Kibertv. 13. § (3) bekezdése alapján feladata az adatosztályozás és a biztonsági osztályba sorolás vizsgálata és **jóváhagyása**, ami hatósági eljárásban valósul meg. A hatósági eljárás indításaként az érintett szervezet az elvégzett adatosztályozás és biztonsági osztályba sorolás eredményét és indokolását a Hatóság által a honlapján közzétett nyomtatványon és mellékleteivel együtt nyújtja

be a Hatóság részre. Az eljárás során a Hatóságnak jogosultsága van az adatosztályozás és a biztonsági szintbe sorolás felülbírálatára, és indokolt esetben magasabb vagy alacsonyabb szintű besorolás megállapítására. Az adatosztályozás elvégzése minden olyan esetben kötelező, amennyiben a tervezet EIR működése során külföldi adatkezelésre vagy nem privát felhőszolgáltatás igénybevételére kerül sor. Ebben az esetben a Vhr. 3. § (2) bekezdésében megahatározott szervezetek a Kibertv. 1. sz. melléklete alapján költség-haszon elemzést és kilépési tervet, a legalább középvállalkozásnak minősülő többségi állami befolyás alatt álló, valamint a Kibertv. 2. és 3. sz. melléklet szerint nem minősülő gazdálkodó szervezetek pedig legalább kilépési tervet kell készíteni a Vhr.-ben meghatározottak szerint, és azt az adatosztályozás és a biztonsági osztályba sorolás eredményével együtt kell bejelenteni a Hatóság részére.

- A fejlesztésre, továbbfejlesztésre irányuló szerződésekben a szervezet köteles meghatározni a fejlesztő részére a Hatóság által jóváhagyott osztályba soroláshoz kapcsolódó követelményeket és a fejlesztés során intézkedik azok megvalósulása iránt a fejlesztést végző szervezet felé. Ennek módja lehet egy információbiztonsági terv elkészítése, ami a biztonsági osztályba sorolás eredményére tekintettel tartalmazza a rendszer kapcsán teljesítendő információbiztonsági kontrollokat. A teljeskörű tervből pedig ki kell szűrni azokat az elvárásokat, amiknek a megvalósítását a fejlesztő feladatként szükséges meghatározni. (Az információbiztonsági terv elkészítésében segítséget nyújthat a hatóság honlapján megtalálható „Információbiztonsági terv sablon” elnevezésű dokumentum.)

A tervezési fázishoz kapcsolódó feladatok és eredmények áttekintéséhez az alábbi két ábra további segítséget adhat:

Az alábbi két ábra és táblázat a fejlesztési fázisokhoz tartozó információbiztonsági dokumentumok előállításának folyamatlépéseit, bemeneti és kimeneti eredménytermékeinek összefüggéseit mutatja.



Sor.	Fázis	Dokumentum	Folyamatlépés	Bemenet	Feladat	Kimenet
1.	Specifikáció	Előzetes biztonsági osztályba sorolás	Adatkörök meghatározása	Funkcionális követelmények	Az egyes funkciókhoz tartozó adatörök meghatározása	Adatkörök
2.			Fenyegetettségek azonosítása	Adatkörök	Az adatkörökre vonatkozó fenyegetettségek azonosítása	Adatkör-fenyegetés összerendelés
3.			Kockázat – kártérték meghatározás	Adatkör-fenyegetés összerendelés	A bizalmassági, sértetlenségi és rendelkezésre állással kapcsolatos kártértékek azonosítása adatkörönként	BSR kárértékek adatkörönként
4.			Előzetes biztonsági osztályba sorolás	BSR kárértékek adatkörönként	A rendszer biztonsági osztályba sorolása az BSR értékek összesítésével	Előzetes biztonsági osztályba sorolás
5.		Információbiztonsági terv	Biztonsági követelmények azonosítása	Előzetes biztonsági osztályba sorolás	A biztonsági osztályhoz tartozó minimális követelmények azonosítása	Biztonsági követelmények
6.	Tervezés		Védelmi intézkedések magasszintű tervezése	Biztonsági követelmények	A biztonsági célokat és követelményeket kielégítő védelmi intézkedések magasszintű tervezése	Információbiztonsági terv
7.		Rendszerbiztonsági terv	Védelmi intézkedések alacsonyszintű tervezése	Információbiztonsági terv	A biztonsági célokat és követelményeket kielégítő védelmi intézkedések alacsonyszintű tervezése	Rendszerbiztonsági terv

2. A fejlesztés folyamatában elvégzendő feladatok:

   - A fejlesztést a Hatóság által jóváhagyott biztonsági osztályhoz *tartozó a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletben* (a továbbiakban: MK rendelet) meghatározott védelmi követelményeknek megfelelően kell végrehajtani.

   - A fejlesztés során a szervezet felülvizsgálja az
     - adatosztályozást, amennyiben az EIR-ben kezelendő adatok körében, valamint
     - a biztonsági osztályba sorolást, amennyiben az EIR kockázati környezetében változás következik be.

   - A felülvizsgálat eredményeként kapott besorolást a Hatóságnak jóváhagyásra be kell nyújtani.

   - A Kibertv. 13. § (7) bekezdése alapján a hatóság az eljárása során elrendelhet sérülékenységvizsgálatot, de a „jelentős" és „magas" biztonsági osztályba tartozó EIR esetében kötelező a teljeskörű sérülékenységvizsgálat kezdeményezése. Ez alól csak a sérülékenységvizsgálat végzésére jogosult állami szerv döntése alapján mentesülhet a szervezet. Fontos momentum, hogy a szervezet vezetőjének az EIR-ek használatbavételéről, vagy használatának folytatásáról szóló szervezeten belüli döntésének feltétele a feltárt sérülékenységek vonatkozásában készített sérülékenységkezelési terv Hatóság általi jóváhagyása.

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

   - A szervezet vezetőjének az elektronikus információs rendszer használatba vételére, további használatára irányuló, döntése abban az esetben hozható meg, ha a nemzeti kiberbiztonsági hatóság által jóváhagyott biztonsági osztályba sorolásból következő követelmények a fenti módon teljesültek.

   - A szervezet vezetőjének döntésével egyidejűleg gondoskodni kell az elektronikus információs rendszer kormányrendeletben meghatározott adatainak nemzeti kiberbiztonsági hatósághoz történő bejelentéséről.

Az eddig részletezettektől eltérően a Kibertv. 14. §-a szerint:

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

a) a 13. § (1) bekezdésében fel nem sorolt alapvető szervezet által történik, az alapvető szervezet köteles biztonsági osztályba sorolni az elektronikus információs rendszert és az annak megfelelő védelmi követelményeket kell teljesíteni,

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

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

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

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

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

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

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