Mikrovállalkozások mentesülhetnek a kiberbiztonsági audit kötelezettség alól?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/5

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.14	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Ha a mikrovállalkozás a tevékenysége miatt a Kiberbiztonsági törvény hatálya alá esik (pl. bizalmi szolgáltató, internet szolgáltató), a védelmi intézkedéseket (pl. kockázatkezelés, incidenskezelés) is alkalmaznia kell, de nem kötelező kétévente kiberbiztonsági audit végzése.

2. A VIZSGÁLANDÓ KÉRDÉS

A mikrovállalkozások egyetemleges felmentést kapnak a kiberbiztonsági audit kötelezettsége alól tevékenységi körtől függetlenül?

3. VÁLASZ

A kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény 3. § (3) bekezdése alapján főszabályként mikrovállalkozásnak minősül az a vállalkozás, amelynek összes foglalkoztatotti létszáma 10 főnél kevesebb, és éves nettó árbevétele vagy mérlegfőösszege legfeljebb 2 millió eurónak megfelelő forintösszeg. (A törvény 3. § (4)-(5) bekezdései további szabályokat tartalmaznak a mikrovállalkozások körének meghatározásához.)

Bár bizonyos tevékenységet (elektronikus hírközlési szolgáltatás, bizalmi szolgáltatás, DNS-szolgáltatás, legfelső szintű doménnév-nyilvántartás vagy doménnév-regisztráció) esetén a mikrovállalkozások is a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) hatálya alá tartozhatnak, a jogszabály a költséges auditkötelezettség alól kifejezett kivételt fogalmaz meg számukra.

A kiberbiztonsági auditra vonatkozó kötelezettséget a Kiberbiztonsági tv. szabályozza. A gazdasági szereplőket illetően a törvény főszabály szerint méretkorlátot alkalmaz (közép- és nagyvállalatok), azonban vannak olyan szolgáltatások (az előző bekezdésben említett szolgáltatások), amelyek esetében a szervezet méretétől függetlenül alkalmazni kell a törvényt:

> *e) méretüktől függetlenül, az a) pont hatálya alá nem tartozó, a 2. és 3. melléklet szerinti szervezetekre, ha a szervezet*
> *ea) elektronikus hírközlési szolgáltató,*
> *eb) bizalmi szolgáltató,*
> *ec) DNS-szolgáltató,*
> *ed) legfelső szintű doménnév-nyilvántartó vagy*
> *ee) doménnév-regisztrációt végző szolgáltató, valamint*
> *f) a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságokra. [2024. évi LXIX. törvény 1. § (1) bekezdés e) pont].*

Ugyanakkor a Kiberbiztonsági tv. 16. §-a, amely a kiberbiztonsági audit elvégzését írja elő, kifejezetten nevesíti a mikrovállalkozásokat mint kivételt. Ez azt jelenti, hogy még ha egy mikrovállalkozás olyan speciális tevékenységet is végez, ami miatt a törvény hatálya alá tartozna

(pl. egy 3 fős, DNS-szolgáltatást nyújtó, alacsony árbevételű cég), az auditot nem kell elvégeztetnie.

A vonatkozó jogszabály pontos szövege:

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

Bár az audit alól mentesülnek, a törvény hatálya alá tartozó mikrovállalkozásoknak (tehát azoknak, akik az 1. § (1) bekezdés e) pontja szerinti speciális szolgáltatást nyújtanak) az egyéb kötelezettségeik fennmaradnak. Erre a Kiberbiztonsági tv. 1. § (1) bekezdésének felvezető szövege is utal.

> *(1) E törvénynek a szervezetek kötelezettségeire és a kiberbiztonsági hatósági felügyeletre vonatkozó rendelkezéseit kell alkalmazni […]*
>
> *[2024. évi LXIX. törvény 1. § (1) bekezdés]*

A mikrovállalkozásokat is terhelik tehát a Kiberbiztonsági tv-ből következő kötelezettségek:

- A védelmi intézkedéseket alkalmazni kell. A mentesítés kifejezetten a kétévente esedékes, külső auditor által végzett felülvizsgálatra vonatkozik. Ha a mikrovállalkozás a tevékenysége miatt a törvény hatálya alá esik (pl. bizalmi szolgáltató), a védelmi intézkedéseket (pl. kockázatelemzés, incidenskezelés) továbbra is alkalmaznia kellhet, csupán annak tanúsítása nem kötelező audit formájában.

  > *(1) A szervezet elektronikus információs rendszerei, valamint az azokban kezelt adatok, a nyújtott szolgáltatások kockázatokkal arányos védelmének biztosítása érdekében a szervezet az e törvény hatálya alá tartozó, a szervezet rendelkezésében lévő elektronikus információs rendszereit „alap”, „jelentős” vagy „magas” biztonsági osztályba sorolja […] [2024. évi LXIX. törvény 10. § (1) bekezdés]*

- Az auditmentesség nem jelent mentességet a nyilvántartásba vételi kötelezettség vagy a felügyeleti díj megfizetése alól, amennyiben a szervezet egyébként a törvény hatálya alá esik. A felügyeleti díj alól a törvény 7. §-a nem ad mentességet a mikrovállalkozásoknak, ha azok az 1. § (1) bekezdés e) pontja alá tartoznak.

  > *(1) A kiberbiztonsági felügyeleti tevékenységért […] valamint az 1. § (1) bekezdés d) és e) pontja szerinti szervezet […] az SZTFH elnökének rendeletében – a (2) bekezdésben foglaltak alapján – meghatározott mértékű kiberbiztonsági felügyeleti díj fizetésére köteles. [2024. évi LXIX. törvény 7. § (1) bekezdés]*

- Nyilvántartásba vételi kötelezettség: A mikrovállalkozásoknak is be kell jelentkezniük a hatósági nyilvántartásba, amennyiben az 1. § (1) bekezdés e) pontja alá tartoznak.

> *(5) [...] valamint az 1. § (1) bekezdés d) és e) pontja szerinti szervezet köteles a működése megkezdését követő vagy az e törvény hatálya alá kerülést követő 30 napon belül a 29. § (1) bekezdés a) pontjában meghatározott adatokat [...] megküldeni az SZTFH részére nyilvántartásba vétel érdekében. [2024. évi LXIX. törvény 8. § (5) bekezdés]*

- Incidensbejelentési kötelezettség: a Kiberbiztonsági tv. 1. § (1) bekezdés e) pontja alá eső mikrovállalkozásokat is terheli a súlyos kiberfenyegetések, kiberbiztonsági incidensközeli helyzetek és kiberbiztonsági incidensek bejelentésére vonatkozó kötelezettség.

> *(2) Az 1. § (1) bekezdés d) és e) pontja szerinti szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott olyan fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is –, amelyek a szervezet működésében vagy az általa végzett szolgáltatásnyújtásban súlyos zavart vagy vagyoni hátrányt okoz, illetve jelentős vagyoni vagy nem vagyoni kárt okoz más természetes vagy jogi személyek számára kötelesek a kormányrendeletben meghatározottak szerint bejelenteni a nemzeti kiberbiztonsági incidenskezelő központ részére. [2024. évi LXIX. törvény 66. § (2) bekezdés]*

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról