**Honvédelmi Kiberbiztonsági Hatóság / HKH**

**Tisztelt Látogató!**

Köszöntjük Önt a Honvédelmi Kiberbiztonsági Hatóság honlapján.

Kiemelten fontos napjaink információs társadalmát érő fenyegetések miatt az elektronikus információs rendszerek fenyegetéseinek mérséklése és a kulcsfontosságú ágazatokban a szolgáltatások folyamatosságának biztosítása.

Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme, amely hozzájárul Magyarország biztonságához, ellenálló képességének és versenyképességének növeléséhez.

A fentiek biztosítása érdekében hatósági tevékenység keretében a Honvédelmi Kiberbiztonsági Hatóság két nagy terület felügyeletét látja el.

A honvédelmi célú elektronikus információs rendszerek biztonságának hatósági felügyelete a rendszerek biztonsági követelményeinek teljesülésével összefüggő tevékenységet foglalja magában (kiberbiztonsági felügyelet).

A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok keretében az információs és kommunikációs technológiák biztonsági követelményeknek való megfelelőségével kapcsolatos hatósági tevékenység valósul meg (kiberbiztonsági tanúsítás).

1. **Kiberbiztonsági felügyelet**

A honvédelmi célú elektronikus információs rendszerekkel kapcsolatos a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 23. § (1) bekezdés b) pontja szerinti kiberbiztonsági felügyeleti feladatok ellátására a Kormány a honvédelemért felelős minisztert jelölte ki.

Egy elektronikus információs rendszer honvédelmi célúként történő azonosításának feltétele a jogszabályban meghatározott valamely szervezethez való tartozás és az ágazatspecifikus működés követelményének együttes fennállása (Kiberbiztonsági tv. 4. § 34. pont).

* 1. **Hatóság feladatai**

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: 418/2024 (XII. 23.) Korm. rendelet) 16. § (2) bekezdés szerint kijelölt, a honvédelmi célú elektronikus információs rendszerek kiberbiztonsági felügyeletét ellátó hatóság (Honvédelmi Kiberbiztonsági Hatóság / HKH) feladata (Kiberbiztonsági tv. 24. § (2) bekezdés):

1. vizsgálja az elektronikus információs rendszer biztonságáért felelős személy és helyettese jogszabályban foglalt követelményeknek való megfelelését, megfelelés esetén nyilvántartásba veszi azt,
2. vizsgálja a biztonsági osztályba sorolás megalapozottságát és a vizsgálat eredménye alapján dönt annak nyilvántartásba vételéről,
3. nyilvántartásba veszi és nyilvántartja a Kiberbiztonsági tv. 28. § (2) bekezdése szerinti adatokat,
4. az elektronikus információs rendszerek biztonságára vonatkozó irányelveket, ajánlásokat, követelményeket határoz meg,
5. iránymutatást adhat ki az európai uniós jogszabályban és az informatikáért felelős miniszter rendeletében meghatározott védelmi intézkedések egymásnak való megfeleltethetősége vonatkozásában,
6. az elektronikus információbiztonsági követelményeknek való megfelelés igazolása érdekében előírhatja - egy adott típusú technológia alkalmazásának előírása vagy előnyben részesítése nélkül - az elektronikus információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását,
7. ellenőrzi az elektronikus információs rendszerek osztályba sorolására vonatkozó, jogszabályban, vagy az általa meghatározott követelmények teljesülését,
8. elrendeli az ellenőrzése során feltárt vagy tudomására jutott biztonsági hiányosságok elhárítását, és az azok felszámolásához szükséges intézkedéseket, valamint ellenőrzi azok eredményességét,
9. megtehet, ellenőrizhet minden olyan, az elektronikus információs rendszerek védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek,
10. kiberbiztonsági incidens esetén hatósági eljárást indít, valamint a hozzá beérkező kiberbiztonsági incidensekről szóló bejelentésekről haladéktalanul tájékoztatja a nemzeti kiberbiztonsági incidenskezelő központot,
11. részt vehet információbiztonsági, kiberbiztonsági érintettségű gyakorlatokon, a nemzetközi információbiztonsági, kiberbiztonsági gyakorlatokon felkérésre képviseli Magyarországot,
12. közreműködik a magyar kibertér védelmét szolgáló tudatosító tevékenységekben,
13. ellenőrzi az elektronikus információs rendszerek fejlesztése során az információbiztonsági követelmények teljesülését,
14. kormányrendeletben foglaltak szerint jóváhagyja az elektronikus információs rendszerek használatba vételét, a megállapított hiányosságok pótlásáig megtilthatja vagy korlátozhatja az elektronikus információs rendszer használatát, a külföldön történő adatkezelést és a felhőszolgáltatás igénybevételét,
15. alapvető vagy fontos szervezetként azonosíthat valamely szervezetet a Kiberbiztonsági tv. végrehajtásáról szóló kormányrendeletben meghatározottak szerint,
16. javaslatot tehet a Kszetv. szerinti kijelölő hatóság részére kritikus szervezet és a Vbö. szerinti kijelölő hatóság részére az ország védelme és biztonsága szempontjából jelentős szervezet kijelölésére,
17. hazai információbiztonsági, kiberbiztonsági gyakorlatokat szervezhet, elrendelheti a szervezet gyakorlaton való részvételét, illetve a szervezet által szervezett gyakorlatok vonatkozásában iránymutatást adhat ki,
18. szakhatóságként jár el az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló kormányrendeletben meghatározott szakkérdésekben.

A HKH feladatai ellátása érdekében jogosult:

1. a biztonsági osztályba sorolást, a védelmi intézkedéseket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
2. a minimálisan elvárt védelmi intézkedéseket meghatározni,
3. a szervezet által meghatározott biztonsági osztályhoz tartozó védelmi intézkedéseken túl további biztonsági követelményeket meghatározni,
4. a szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések - többek között a dokumentált kiberbiztonsági szabályzatok - értékeléséhez, valamint az információk bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatást kérni,
5. a védelmi intézkedések és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
6. rendszeres, eseti és célzott biztonsági ellenőrzéseket végezni, ideértve a helyszíni ellenőrzéseket, a távoli felügyeleti intézkedéseket és a véletlenszerű ellenőrzéseket is,
7. a felügyeleti feladatai ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz hozzáférni és ezeket bekérni, illetve a megküldött dokumentumok felülvizsgálatát elrendelni,
8. eljárása során - a honvédelmi elektronikus információs rendszerek kivételével - független értékelőt igénybe venni, és az általa végzett ellenőrzés eredményét, továbbá a szervezet által megbízott független értékelő jelentésében vagy a kiberbiztonsági auditjelentésben foglaltakat figyelembe venni,
9. az elektronikus információs rendszerekre és eszközökre, a szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat figyelembe venni,
10. európai uniós jogi aktus által meghatározott kiberbiztonsági követelményeknek való megfelelést részben vagy egészben az informatikáért felelős miniszter rendeletében meghatározott védelmi követelményeknek való megfelelésnek tekinteni,
11. az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
12. a felügyeleti jogkörébe tartozó szervezetek vonatkozásában szabvány alkalmazására, európai vagy hazai kiberbiztonsági tanúsítási rendszerek által tanúsított IKT-termék használatára, illetve minősített bizalmi szolgáltatás igénybevételére iránymutatásokat kiadni,
13. az elektronikus információs rendszerek használatba vételének, meglévő elektronikus információs rendszer tovább használatának jóváhagyása során helyszíni ellenőrzést tartani és sérülékenységvizsgálatot elrendelni,
14. a Honvédelmi Kiberbiztonsági Incidenskezelő Központ megkeresése alapján a szervezet elektronikus információs rendszere kapcsán bejelentett sérülékenység felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni, illetve egyedi mérlegelés alapján sérülékenységvizsgálatot elrendelni.
    1. **Hatósági ellenőrzés**

Ellenőrzés során a HKH feladata a honvédelmi célú elektronikus információs rendszerekre vonatkozóan az osztályba sorolás megállapításának, a vonatkozó biztonsági követelmények (személyi, fizikai, logikai) teljesülésének ellenőrzése, valamint az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése.

A HKH az ellenőrzést a honvédelmi célú elektronikus információs rendszert működtető szervezet irányítását, vezetését vagy felügyeletét ellátó miniszter által jóváhagyott éves ellenőrzési terv vagy egyedi utasítás alapján végzi.

Ha a HKH azt állapítja meg, hogy a honvédelmi célú elektronikus információs rendszert működtető szervezet a biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, akkor az érintettet felszólítja a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére. (418/2024. (XII. 23.) Korm. rendelet 32-36. §)

* 1. **Kiberbiztonsági incidens kivizsgálás**

Kiberbiztonsági incidens kivizsgálás során a HKH feladata a bekövetkezett kiberbiztonsági incidens kivizsgálása, az incidenshez vezető körülmények feltárása, valamint a jövőbeli bekövetkezés megelőzése érdekében hatósági feladatszabás. (Kiberbiztonsági tv. 23. § (2) bekezdés)

* 1. **Nyilvántartás**

A HKH a honvédelmi célú elektronikus információs rendszerek vonatkozásában a Kiberbiztonsági tv. hatósági nyilvántartásra vonatkozó szabályai szerinti nyilvántartást vezet. Az adatok nyilvántartásba történő bejegyzését megelőzően vizsgálja a bejelentett adatok jogszabályban meghatározott követelményeknek való megfelelősségét.

Nyilvántartott adatok:

1. a szervezet azonosításához szükséges adatokat,
2. a szervezet elérhetőségei, ideértve elektronikus elérhetőségek, valamint a szervezet által használt nyilvános IP címek vagy IP-tartományok, valamint a szervezet székhelye, telephelye(i),
3. a szervezet alapvető vagy fontos szervezetnek minősülését,
4. ágazatba, alágazatba, szervezettípusba tartozását,
5. a szervezet elektronikus információs rendszereinek megnevezését, rövid leírását, biztonsági osztályának besorolását, a nyilvántartásba vétel, valamint a felülvizsgálat időpontjában elért biztonsági osztály meghatározását,
6. az elektronikus információs rendszerben kezelt adatok osztályozásához kapcsolódó adatokat, azok adatkezelésének helyszínét, ideértve az ország megnevezését vagy a felhő típusát,
7. az elektronikus információs rendszerhez kapcsolódóan igénybe vett felhőszolgáltatásokra vonatkozó adatokat,
8. az elektronikus információs rendszerhez kapcsolódó védelmi intézkedéseket és azok státuszát,
9. nem Magyarországon bejegyzett szervezet Magyarország területén működő képviselőjének nevét vagy cégnevét, levelezési címét, telefonszámát és elektronikus levelezési címét,
10. az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó személy, szervezet azonosítására alkalmas adatokat, valamint a feladatot ténylegesen ellátó természetes személy személyazonosító adatait, közvetlen elérhetőséget biztosító telefonszámát, elektronikus elérhetőségét, végzettségét, szakképzettségét, szakmai tapasztalatát,
11. a szervezet információbiztonsági szabályzatát,
12. a szervezet vezetője és az elektronikus információs rendszer biztonságáért felelős személy továbbképzésére vonatkozó adatokat,
13. a hatósági ellenőrzésekkel kapcsolatos információkat,
14. a sérülékenységvizsgálat eredményét, valamint a sérülékenységek megszüntetésére vonatkozó sérülékenységkezelési tervet.
15. Központi rendszerhez csatlakozott szervezet esetében:
16. a felhasználó szervezet által használt központi rendszer megnevezését, egyedi azonosító számát,
17. a központi rendszer szolgáltatójának nevét,
18. a központi rendszer egyedi azonosító számát,
19. a felhasználó szervezetek megnevezését,
20. a központi szolgáltató által nyújtott szolgáltatásban részt vevő elektronikus információs rendszer egyedi azonosító számát,
21. a központi szolgáltató által biztosított támogató rendszer azonosítására alkalmas adatokat,
22. a felhasználó szervezetek megnevezését,
23. a kiberbiztonsági incidensekkel kapcsolatos, a kiberbiztonsági incidenskezelő központtól kapott értesítéseket, az ezekben szereplő személyekre vonatkozó adatokat. (Kiberbiztonsági tv. 28. § (2) bekezdés)

A honvédelmi célú elektronikus információs rendszert működtető szervezet a Kiberbiztonsági tv. szerinti adatokat, valamint ezek változásait tizenöt napon belül megküldi a hatóságnak. (Kiberbiztonsági tv. 8. § (3) bekezdés a) pont)

* 1. **Az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák védelme**

A Magyarország területén székhellyel rendelkező az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák ellenállóképességének fokozását célzó keretrendszert a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény határozza meg.

Az ország védelme és biztonsága szempontjából jelentős szervezet és infrastruktúra kijelölésére, adatszolgáltatására, nyilvántartására, hatósági felügyeletére, támogatására, ellenálló képességének fejlesztésére vonatkozó kötelezettségeire, a rendkívüli események bejelentésére, az ország védelme és biztonsága szempontjából jelentős szervezetek és az eljáró hatóságok közötti együttműködésre, valamint az adatvédelemre – meghatározott eltérésekkel – a kritikus szervezetek ellenállóképességéről szóló 2024. évi LXXXIV. törvényben foglaltakat kell alkalmazni.

Az ország védelme és biztonsága szempontjából jelentős *honvédelmi kijelölésű* szervezetek és infrastruktúrák kijelölésével összefüggő hatósági eljárások lefolytatására kormányrendeletben kijelölt honvédelmi ágazati kijelölő hatóság rendelkezik hatáskörrel. A honvédelmi ágazati kijelölő hatóság látja el a honvédelmi ágazati nyilvántartó és ellenőrző hatósági feladatokat is.

Az ország védelme és biztonsága szempontjából jelentős *honvédelmi ágazaton belüli és kettős kijelöléssel nem érintett* szervezetek és infrastruktúrák elektronikus információs rendszerei tekintetében a Kiberbiztonsági tv. rendelkezései szerint a HKH látja el a kiberbiztonsági hatósági felügyeletet. (Vbö. 43/J. § (2) bekezdés)

* 1. **Fejlesztési projektek felügyelete**

A HKH a honvédelmi célú elektronikus információs rendszerek és az azokban kezelt adatok biztonsága érdekében egy fejlesztési projekt esetében a projekt teljes életciklusa alatt ellenőrzi az elektronikus információs rendszerek fejlesztése, továbbfejlesztése során az információbiztonsági követelmények teljesülését.

A szervezet elektronikus információs rendszer fejlesztése esetén a tervezési életciklusban elvégzett adatosztályozás és osztályba sorolás eredményét és indokolását jóváhagyásra benyújtja a nemzeti kiberbiztonsági hatóság részére:

*a)* belső fejlesztés esetén az erőforrások allokációját megelőzően,

*b)* külső fejlesztés esetén az arra irányuló szerződés megkötését megelőzően - a közbeszerzésekre vonatkozó jogszabályi rendelkezéseket is figyelembe véve - olyan módon, hogy az információbiztonsági követelmények az elektronikus információs rendszer fejlesztésére irányuló szerződésbe rögzítésre kerüljenek.

A fejlesztést a HKH által jóváhagyott, a biztonsági osztály vonatkozásában az informatikáért felelős miniszter rendeletében meghatározott védelmi követelményeknek megfelelően kell végrehajtani. A megállapított biztonsági osztályhoz tartozó követelményeket a rendszer használatbavételéig teljesíteni kell.

Az elektronikus információs rendszer használatbavételére, illetve meglévő elektronikus információs rendszer tovább használatára vonatkozó a szervezet vezetője által hozott döntésnek a HKH általi jóváhagyását a szervezet kérelmezi.

A HKH jóváhagyja az elektronikus információs rendszer használatba vételét, ha meggyőződött róla, hogy az érintett elektronikus információs rendszer valamennyi elvárt kiberbiztonsági kritériumot teljesíti. A megállapított hiányosságok pótlásáig megtilthatja vagy korlátozhatja az elektronikus információs rendszer használatát, a külföldön történő adatkezelést és a felhőszolgáltatás igénybevételét. (Kiberbiztonsági tv. 13-15. §; 418/2024. (XII. 23.) Korm. rendelet 13-15. §)

* 1. **Biztonságtudatosság**

Napjainkban nyilvánvalóvá vált, hogy egy számítógépet, okos eszközöket (IoT, telefon, tablet, szenzor, drón, robot, stb.) használó felhasználó biztonságtudatosságának hiánya vált a hálózatos környezet legnagyobb célpontjává. Mindennaposak az emberi hiszékenységet, tudatlanságot kihasználó rosszindulatú cselekmények. Ezeket az emberi gyengeségeket használja ki a legtöbb nagy kampány is, legyen az anyagi haszonszerzés érdekében indított támadás, vagy egy idegen állam által támogatott célzott támadás, amiben egy jól kiválasztott célszemély a szervezet számára is elviselhetetlenül nagy károkat képes okozni.

A HKH a biztonságtudatosság erősítése érdekében rendszeresen, heti kibervédelmi szemlén keresztül biztosítja a helyzetértékelést (situation awareness) – a szervezet elektronikus információs rendszer biztonságáért felelős személyének – a kibertérben történt eseményekről, fenyegetésekről, kártékony kódokról és egyéb kibertérrel összefüggő információkról. A felhasználóknak időszakonként, a fenyegetéseknek és célcsoportoknak megfelelően tematikus kiberbiztonsági szemlét készít a HKH.

* 1. **Elektronikus adat ideiglenes hozzáférhetetlenné tétele/eltávolítása**

A HKH azonnal végrehajthatónak nyilvánított határozatban rendeli el az ideiglenes hozzáférhetetlenné tételét annak az elektronikus hírközlő hálózat útján közzétett adatnak, amely honvédelmi érdeket sért vagy veszélyeztet, vagy honvédelmi célú elektronikus információs rendszer biztonságára fenyegetést jelent. Az ideiglenes (90+90 nap) hozzáférhetetlenné tétel az elektronikus adathoz való hozzáférés ideiglenes megakadályozása.

A határozat kötelezettje – annak határozatban történő megjelölése nélkül – valamennyi elektronikus hírközlési szolgáltató. Az elektronikus adat ideiglenes hozzáférhetetlenné tételét elrendelő határozatot a hatóság hirdetményi úton közli. A hirdetményt a hatóság honlapján kell közzétenni. A határozat közlésének napja a hirdetmény közzétételét követő nap.

A hatóság 1 millió forinttól 5 millió forintig terjedő bírsággal sújthatja azt az elektronikus hírközlési szolgáltatót, amely e kötelezettségének nem tesz eleget.

Az elektronikus adat ideiglenes eltávolítására az érintett elektronikus adatot kezelő, tárhelyszolgáltatót, illetve tárhelyszolgáltatást is végző közvetítő szolgáltatót kell kötelezni. Az eltávolításra kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására. (Kiberbiztonsági tv. 33-36. §)

* 1. **Azonosítási eljárás**

Az azonosítási eljárás során a HKH alapvető vagy fontos szervezetként azonosíthat egy szervezetet, ha az nem tartozik a Kiberbiztonsági tv. hatálya alá, illetve nem került az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölésére, de honvédelmi, katonai nemzetbiztonsági okból indokolt a kijelölése. A HKH az azonosítási eljárás során hivatalból jár el. (Kiberbiztonsági tv. 1. § (6) bekezdés, 26-27. §; 418/2024. (XII. 23.) Korm. rendelet 26-28. §)

1. **Kiberbiztonsági tanúsítás**

A Kiberbiztonsági tv. a kiberbiztonság egységes szintű emelése érdekében tartalmazza az információs és kommunikációs termékek, szolgáltatások és folyamatok kiberbiztonsági tanúsítására vonatkozó alapvető hazai szabályokat. (Kiberbiztonsági tv. 37-44. §; 418/2024. (XII. 23.) Korm. rendelet 45-46. §)

A kiberbiztonsági tanúsítás célja annak vizsgálata, hogy az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfelelnek-e az európai és nemzeti kiberbiztonsági tanúsítási rendszerekben foglalt biztonsági követelményeknek. A követelmények folyamatosan magas szinten tartása és megtartása képes lehet növelni a kiberfenyegetések elleni védelem szintjét.

Nemzeti kiberbiztonsági tanúsító hatóságként a tanúsítási rendszerek szabályainak nyomon követésére, felügyeletére és betartatására a Szabályozott Tevékenységek Felügyeleti Hatósága került kijelölésre.

A honvédelemért felelős miniszter látja el a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő európai vagy nemzeti kiberbiztonsági tanúsítási rendszer hatálya alá tartozó IKT-termék, IKT-szolgáltatás vagy IKT-folyamat vonatkozásában a kiberbiztonsági tanúsító hatósági feladatokat.

* 1. **Engedélyezési eljárás lefolytatása**

A tanúsító hatóság a megfelelőségértékelő szervezet vonatkozásában engedélyezési eljárást folytat le, ha az IKT-termékre, IKT-szolgáltatásra vagy IKT-folyamatra vonatkozó nemzeti vagy európai kiberbiztonsági tanúsítási rendszer kiegészítő követelményeket ír elő és ez alapján engedélyezési eljárás lefolytatása válik szükségessé, vagy „magas” megbízhatósági szintet ír elő a rendszer keretében kiadandó kiberbiztonsági tanúsítványra és a tanúsító hatóság az ilyen tanúsítvány kiállításának feladatát egyes nemzeti vagy európai kiberbiztonsági tanúsítványok vonatkozásában vagy általános jelleggel átruházza a megfelelőségértékelő szervezetre. (Kiberbiztonsági tv. 47. § (4) bekezdés; a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet (a továbbiakban: 608/2023. (XII. 22.) Korm. rendelet) 12-16. §)

* 1. **Hatósági nyilvántartás**

A Hatóság a Kiberbiztonsági tv. 48. § (1) bekezdése szerinti adatokat kezeli, amelynek célja az IKT-termék, IKT-szolgáltatás vagy IKT-folyamat biztonságával összefüggő információk naprakészen tartása, valamint az azokat érintő sebezhetőséggel vagy rendellenességgel kapcsolatos feladatok, továbbá a tanúsító hatóság ellenőrzési és felügyeleti hatósági tevékenységének ellátása. (Kiberbiztonsági tv. 48. §; 608/2023. (XII. 22.) Korm. rendelet 17-23. §)

* 1. **Hatósági ellenőrzés**

A tanúsító hatóság kiberbiztonsági tanúsítási felügyeleti feladatai keretében jogosult felszólítani a megfelelőségértékelő szervezeteket és a megfelelőségi nyilatkozatok kibocsátóit a hatósági feladatellátáshoz szükséges információk, adatok rendelkezésre bocsátására, valamint a megfelelőségértékelő szervezeteknél és a megfelelőségi nyilatkozatok kibocsátóinál hatósági ellenőrzést végezni.

Ha a tanúsító hatóság tudomására jut vagy az ellenőrzése során megállapítja, hogy a megfelelőségértékelő szervezet vagy a gyártó a vonatkozó európai uniós vagy magyar jogszabályokban foglalt biztonsági követelményeket és a kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, felszólítja a megfelelőségértékelő szervezetet vagy a gyártót a vonatkozó európai uniós és magyar jogszabályokban foglalt biztonsági követelmények és a kapcsolódó eljárási szabályok teljesítésére.

Ha a megfelelőségértékelő szervezet vagy a gyártó a jogszabályban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a tanúsító hatóság bírságot szabhat ki, amely további nemteljesítés esetén megismételhető. (Kiberbiztonsági tv. 47. § (8) bekezdés b) pont; 608/2023. (XII. 22.) Korm. rendelet 24-26. §)

* 1. **Tanúsítási rendszerek nyomon követése**

A Hatóság folyamatosan figyelemmel kíséri az európai kiberbiztonsági tanúsítási rendszerek fejlesztését, a kapcsolódó szabványosítási folyamatokat, azokat a kapcsolódó szakterületeket, ahol szükséges lehet a kiberbiztonság növelése. A nemzeti tanúsítási rendszerek fenntartásával kapcsolatosan értékeli a tanúsítási rendszereket és szükség esetén intézkedik a felülvizsgálatukra.

* 1. **Megfelelőségértékelés**

A Kormány által meghatározott egyes tanúsítási rendszerek esetében a megfelelőségértékelést a tanúsító hatóság végzi. Ehhez a hatóság akkreditált vizsgáló laboratóriumot igénybe vehet.

* 1. **Megfelelőségértékelő szervezetek**

A Hatóság által nyilvántartásba vett megfelelőségértékelő szervezetek:

A megfelelőségértékelő szervezet megnevezése, székhelyének címe, elektronikus levelezési címe és telefonszáma, a nyilvántartásba vételi okirat száma, a nyilvántartásba vétel időpontja, lejárata, a bejegyzett megbízhatósági szint és tanúsítási rendszer.

*(Szerkesztői megjegyzés: egyenlőre nincs nyt-ba vett szervezet. Kérjük az adatkörök megjelenítését.)*

* 1. **Tanúsítási rendszerek – hadiipari kutatás, fejlesztés, gyártás és kereskedelem tekintetében**
  2. **Panaszkezelési szabályzat**

Panaszkezelési eljárásrend

A panaszokról, a közérdekű bejelentésekről, valamint a visszaélések bejelentésével összefüggő szabályokról szóló 2023. évi XXV. törvény (a továbbiakban: Panasztörvény) alapján a **panasz** olyan kérelem, amely egyéni jog- vagy érdeksérelem megszüntetésére irányul, és elintézése nem tartozik más – így különösen bírósági, közigazgatási – eljárás hatálya alá. A panasz javaslatot is tartalmazhat. Panasszal bárki fordulhat a panasszal összefüggő tárgykörben az eljárásra jogosult szervhez.

**A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság** (a továbbiakban: Hatóság) a kiberbiztonsági tanúsítási tárgykörben benyújtott panaszok elintézése során a következők szerint jár el.

**Ki és hogyan tehet panaszt?**

Kiberbiztonsági tanúsítás tárgykörben panasszal bárki fordulhat a Hatósághoz a következő módon:

* e-mailben: [hatosag@hkh.gov.hu](mailto:hatosag@hkh.gov.hu);
* Hivatali Kapun: Honvédelmi Kiberbiztonsági Hatóság (HAEIBH) (KRID: 463531787)
* postai úton a Hatóság levelezési címén (1525 Budapest, Pf. 74.);
* a Hatóság telefonos elérhetőségén: 06 (1) 372-1832. A telefonon tett panaszt a Hatóság írásba foglalja és a panaszos részére nyolc napon belül másodpéldányban megküldi.

Az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló 2019/881 európai parlamenti és tanácsi rendelet szerint a természetes és jogi személyek panaszt nyújthatnak be a Hatósághoz

* a Hatóság által kiadott európai kiberbiztonsági tanúsítvánnyal összefüggő tárgykörben;
* a megfelelőségértékelő szervezetek által kiadott európai kiberbiztonsági tanúsítványokkal kapcsolatos tárgykörben, amennyiben ezek a tanúsítványok „magas” megbízhatósági szintre vonatkoznak;
* uniós megfelelőségi nyilatkozatokkal kapcsolatos tárgykörben.

A **bejelentésnek tartalmaznia kell** a bejelentő természetes személyazonosító adatait (bejelentő családi és utóneve, születési hely, születési idő), állandó lakcímét és levelezési címét. Jogi személy bejelentő esetén pedig a jogi személy nevét és székhelyét meg kell jelölni.

Kérjük, hogy a hatékonyabb elintézés érdekében az ügyben rendelkezésre álló iratok másolatát csatolja a panasz előterjesztéséhez.

**A panasz vagy közérdekű bejelentés elbírálásának a menete**

Ha a panasz elintézésére nem a Hatóság az eljárásra jogosult szerv, a Hatóság a panaszt a beérkezéstől számított nyolc napon belül az eljárásra jogosult szervhez átteszi, erről egyidejűleg a panaszost értesíti.

A panaszt – ha a törvény eltérően nem rendelkezik – a beérkezéstől számított harminc napon belül kell elintézni. Ha a vizsgálat előreláthatólag ennél hosszabb ideig tart, a Hatóság a panaszost a hosszabbítás indokainak megjelölésével erről tájékoztatja, azonban az elintézési határidő ebben az esetben sem haladhatja meg a hat hónapot.

A Hatóság a panaszost a panasz kiegészítésére, pontosítására, a tényállás tisztázására, valamint további információk rendelkezésre bocsátására hívhatja fel, továbbá a panaszost szükség esetén meghallgatja.

A Hatóság **mellőzheti** a panasz vizsgálatát, amennyiben

* nyilvánvalóvá válik, hogy a panaszos rosszhiszeműen, valótlan adatot vagy információt közölt;
* ugyanazon panaszos a korábbival azonos tartalmú, ismételt panaszt terjesztett elő;
* a panaszt a sérelmezett tevékenységről vagy mulasztásról való tudomásszerzéstől számított hat hónap után terjesztették elő.

A Hatóság **mellőzi**

* a sérelmezett tevékenységről vagy mulasztásról való tudomásszerzéstől számított

egy éven túl előterjesztett;

* azonosíthatatlan személy által tett panasz vizsgálatát.

A Hatóság az azonosíthatatlan személy által tett panaszt megvizsgálja, ha annak alapjául súlyos jog- vagy érdeksérelem szolgál.

A panaszost, amennyiben jóhiszeműen járt el, nem érheti hátrány a panasz megtétele miatt.

A Hatóság a panasz elintézése során a személyes adatok, illetve más adatok – különösen a minősített adat, illetve a törvény által védett titok – védelmére vonatkozó szabályok szerint jár el. A panaszos személyes adatai csak a kezdeményezett eljárás lefolytatására hatáskörrel rendelkező szerv részére adhatók át, ha e szerv annak kezelésére a törvény alapján jogosult, vagy adatai kezeléséhez a panaszos hozzájárult. A panaszos személyes adatai hozzájárulása nélkül nem hozhatók nyilvánosságra.

Ha nyilvánvalóvá vált, hogy a panaszos rosszhiszeműen, valótlan adatot vagy információt közölt és

* ezzel bűncselekmény vagy szabálysértés elkövetésére utaló körülmény merült fel, személyes adatait az eljárás lefolytatására jogosult szerv vagy személy részére;
* alappal valószínűsíthető, hogy másnak jogellenes kárt vagy egyéb jogsérelmet okozott, személyes adatait az eljárás kezdeményezésére, illetve lefolytatására jogosult szervnek vagy személynek kérelmére

át kell adni.

1. **Jogforrások**

* Magyarország kiberbiztonságáról szóló LXIX. törvény;
* Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet;
* A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet;
* A honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságok meghatározásáról szóló 6/2020. (IV. 16.) HM rendelet;
* Az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet;
* A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet;
* A kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól szóló 305/2023. (VII. 11.) Korm. rendelet; (hatályon kívül)
* A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsítás keretében fizetendő igazgatási szolgáltatási díjról szóló 1/2023. (I.12.) HM. rendelet;
* A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelem területén megfelelőségértékelő szervezetek által teljesítendő követelményekről szóló 2/2023. (I.12.) HM. rendelet;
* A haditechnikai termékek gyártásának és a haditechnikai szolgáltatások nyújtásának engedélyezéséről szóló 2005. évi CIX. törvény.

1. **Ügyintézés**

* Általános tájékoztató
* Kiberbiztonsági tv. 4. § 34. pont szerinti szervezetek adatszolgáltatási kötelezettségének teljesítésére irányuló kérelem
* Adatosztályozás és az elektronikus információs rendszer biztonsági osztályba sorolásának jóváhagyására irányuló kérelem
* Elektronikus információs rendszer használatba vételének jóváhagyására irányuló kérelem
* Megfelelőségértékelő szervezet nyilvántartásba vételére, adatváltozásának bejelentésére, engedélyezésére irányuló kérelem
* Sebezhetőség bejelentése

1. **Hirdetmények**

Feltöltött dokumentumok szerinti döntések.

1. **Kapcsolat**

* Székhely cím: 1021, Budapest Budakeszi út 99-101.
* Levelezési cím: 1525, Budapest Pf. 74.
* Telefonszám: 06 (1) 372-1832
* e-mail: hatosag@hkh.gov.hu
* hivatali kapu név: Honvédelmi Kiberbiztonsági Hatóság
* rövidített hivatali kapu név: HAEIBH
* KRID: 46353