Magyarország Kormánya
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE
SZÉCHENYI 2020

# Elektronikus információbiztonság megvalósítása a KÖFOP projektek során

## Tájékoztató hatósági eljárásról pályázók részére

2015. november 5.

## Bevezető

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 11. i) pontja a nemzeti kiberbiztonsági célok elérésének eszközeként jelölte meg a kiberbiztonsági szempontok érvényesítését az állami műszaki fejlesztési feladatok, valamint a kormányzati információs rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatok ellátása során.

Összhangban a Nemzeti Kiberbiztonsági Stratégiával, a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program (KÖFOP) keretében megvalósuló, e-közigazgatást támogató, illetve elektronikus információs rendszerek fejlesztésére irányuló projektek végrehajtásával összefüggésben kiemelt szempont az elektronikus információbiztonság feltételeinek megteremtése, a fejlesztések hatósági kontrolljának biztosítása.

A KÖFOP projektek ellenőrzése során, *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* (továbbiakban: Ibtv.) hatálya alá tartozó szervek vonatkozásában a Nemzeti Elektronikus Információbiztonsági Hatóság rendes hatósági ellenőrzési tevékenysége keretében, *az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet* (továbbiakban: Kr.) 8. §-ban megjelölt eljárásrend szerint jár el, azzal az eltéréssel, hogy tevékenységét összehangolja más, a KÖFOP projektek fölött kontrollt gyakorló szervek tevékenységével is.

A KÖFOP projektek végrehajtása során a Projektgazda köteles a rendszer biztonságára vonatkozó jogszabályi követelményeknek való megfelelést biztosítani, és ennek érdekében a Kr. 8. § szerint a Kormányzati Eseménykezelő Központ és Nemzeti Elektronikus Információbiztonsági Hatóság feladatait ellátó **Nemzeti Kibervédelmi Intézettel** (a továbbiakban: **NKI**), mint Hatósággal együttműködni. Az NKI a KÖFOP fejlesztések teljes életciklusát követi, a tervezés kezdetétől a végrehajtási/megvalósítási szakaszon át egészen a létrehozott megoldás üzembe állításáig.

# A KÖFOP hatósági ellenőrzési eljárása

## Projekt tervezési időszaka

A projekt tervezési időszakában a Projektgazda köteles az Ibtv. 7. § alapján, *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet* (továbbiakban: BMr.) 1. sz. mellékletében meghatározott kritériumrendszer mentén **meghatározni** a projekt keretében **fejlesztéssel érintett rendszer** – a projekt lezárását követően alkalmazandó – **biztonsági osztályát**, és ki kell töltenie az osztályba sorolás indoklására szolgáló nyilatkozatot.

A **megvalósíthatósági tanulmányban** a Projektgazda köteles megjelölni a fejlesztett rendszer esetében a fentiek alapján meghatározott biztonsági osztályt, valamint **bemutatni a meghatározott biztonsági osztályhoz kapcsolódó**, a BMr. 3. sz. mellékletében felsorolt **védelmi intézkedések megvalósításának módját**, és meghatározni a biztonsági intézkedésekre minimálisan fordítandó **költségkeretet**. Amennyiben a projekttel érintett rendszerre vonatkozó biztonsági követelmények egy részének – pl. központi üzemeltetés esetén a fizikai biztonsági követelmények – biztosítása nem a Projektgazda felelősségi körébe tartozik, úgy a Projektgazdának szükséges az adott biztonsági követelmények teljesüléséről a felelős szerv nyilatkozatát megkérnie (illetőleg a projekt során a felelősség megosztását szerződéses keretek között, az Ibtv. 11.§ (1) k, pontja szerint rendeznie).

Az NKI a biztonsági osztályba sorolás, valamint az adott biztonsági osztályhoz tartozó védelmi intézkedések tervezésének és megvalósításának nyomon követéséhez, támogatásához hatósági segédletet (és ahhoz kapcsolódó útmutatót) ad ki. **A Projektgazda a projekttel összefüggő adatszolgáltatási kötelezettségét a hatósági segédlet használatával köteles teljesíteni.**

**A KÖFOP pályázatok során alkalmazandó segédletet és útmutatót a hatóság elektronikus levélben küldi meg, amit a Projektgazdák a fejlesztes@govcert.hu címre írt levélben kezdeményezhetnek.**

A Projektgazda a biztonsági osztályba sorolást és indoklást, továbbá a biztonsági osztályhoz kapcsolódó védelmi intézkedések megvalósítási tervét és ütemezését is magában foglaló megvalósíthatósági tanulmányt, illetve az esetlegesen beszerzett nyilatkozatokat, egyéb kapcsolódó iratokat, valamint a kitöltött hatósági segédletet a központi kapcsolattartási címre (ekozig@bm.gov.hu) megküldi.

Az NKI a megvalósíthatósági tanulmány vonatkozó részében ellenőrzi a biztonsági osztályba sorolás megfelelőségét, vagy az Ibtv. 8. § (6) szerint felülbírálja. A biztonsági osztály sorolás megfelelősége esetén az NKI ellenőrzi a biztonsági osztályhoz kapcsolódó védelmi intézkedések megvalósítási- és költségterveit, megállapítja megfelelőségét, vagy hiánypótlást kezdeményez.

A részletes megvalósíthatósági tanulmányban foglalt fejlesztések információbiztonsági követelményeknek történő megfeleléséről az NKI hatósági állásfoglalást bocsát ki, melynek részeként – a projekt ütemezéséhez illeszkedően, a Kr. 8. § (2) bekezdés szerint – meghatározza, hogy a biztonsági intézkedések kialakításával összefüggő dokumentációkat véleményezés céljából az NKI részére milyen határidővel szükséges megküldeni. A Projektgazdának az NKI észrevételeit, kifogásait a dokumentációkban alkalmaznia kell, illetve a fejlesztés során meg kell valósítani.

## Korai jelzőrendszerhez való csatlakozás

Amennyiben az NKI kezdeményezi, a Projektgazda a fejlesztés részeként köteles vállalni, hogy az NKI által kialakításra kerülő, a közigazgatási rendszereket a kibertérből érő támadások azonosítását, ezáltal a szervezeti integritás erősítését támogató korai jelzőrendszerhez való csatlakozás alapvető műszaki feltételeit a fejlesztés keretében megteremti, és azt a rendszer teljes életciklusában fenntartja. A központi elemző alrendszerből és a Projektgazda védett rendszere meghatározott be és kimeneti hálózati csomópontjain elhelyezett szenzorokból álló jelzőrendszer a bemenő és kimenő forgalmat vizsgálja szignatúra és viselkedés alapú metódusokkal.

A Projektgazdának meg kell adnia a szenzor műszaki/technikai méretezéséhez szükséges adatokat (pl. átlagos és csúcs hálózati forgalom), és az NKI útmutatása alapján meg kell teremtenie a szenzor telepítésének infrastrukturális és egyéb feltételeit. Amennyiben a pályázó központosított szolgáltató szolgáltatását veszi igénybe, úgy az infrastrukturális feltételek megteremtését a Projektgazda és a központi szolgáltató között létrejött megállapodásban kell rendezni.

A Projektgazda tudomásul veszi, hogy a jelzőrendszer a központosított szolgáltató által nyújtott biztonsági szolgáltatásokat, rendszereket nem érinti, azokat nem váltja ki, és nem helyettesíti a Projektgazda által létesítendő rendszerelemeket sem, hanem azokat védelmi szempontból kiegészíti.

## Projekt végrehajtási szakasza

A projekt megvalósítása során – az előzetesen meghatározott ütemterv szerint – beérkezett dokumentációkat az NKI megvizsgálja, illetve összeveti a vonatkozó tervdokumentációkkal. Ha a vizsgálat a tervezett biztonsági intézkedések megvalósításának hiányát tárja fel, vagy lényeges kockázatot azonosít, akkor az NKI kezdeményezi a hiányosságok pótlását, illetve a kockázat kezelését. A Projektgazda a projekt fejlesztési fázisainak lezárását megelőzően a hiányosságokat pótolni, a lényeges kockázat tárgyában kockázatkezelési intézkedést köteles hozni.

## Projekt zárása

Az utolsó végrehajtási projektszakasz zárása előtt a projekt megvalósítása során beérkezett dokumentációk, valamint a projekt során tervezett biztonsági intézkedések megvalósítását érintő kockázatok függvényében az NKI az Ibtv. 14. § (2) bekezdés alapján részleges vagy teljes megfelelőségi vizsgálat (audit), illetve az Ibtv. 18. § (1) bekezdés alapján sérülékenységvizsgálat lefolytatását rendelheti el. A korábban felmerült, még nem pótolt hiányosságokat és nem kezelt kockázatokat, valamint az esetlegesen lefolytatott audit illetve sérülékenységvizsgálat során feltárt hiányosságokat és kockázatokat a projekt zárását megelőzően kezelni szükséges.

A projekt keretében létrehozott rendszer biztonsági megfelelősége, az NKI által megállapított hiányosságok pótlása, valamint a kockázatkezelési intézkedés meghozatala kapcsán készített **szakmai beszámoló NKI általi elfogadása a projekt fejlesztési fázisai lezárásának és az üzembe helyezésnek a feltétele.**

Amennyiben a projekt érintett, a támogatási szerződés alapján az elektronikus információbiztonsággal érintett **fejlesztések megvalósításra vonatkozó költségek elszámolhatóságának feltétele az információbiztonsági követelmények megfelelő teljesítésére vonatkozó, fentiek alapján kiadott hatósági állásfoglalás.** A végleges megvalósíthatóság tanulmányhoz kiadott hatósági állásfoglalás meglétét az e-közigazgatás szempontú véleményt tartalmazó dokumentum keretében szükséges támogató részére igazolni.

Az NKI eljárásának határidejére az egyéb jogszabályokban előírt határidők az irányadók. A vonatkozó jogszabályok a NEIH honlapján (neih.gov.hu) elérhetőek.