



KÖZVETLEN BRÜSSZELI FORRÁS PÁLYÁZATI TÁJÉKOZTATÓ

Program	Horizon 2020
Pályázat megnevezése (magyar)	Digitális biztonság, a magánélet és a személyes adatok védelme, valamint felelősségrevonhatóság a kritikus ágazatokban
Pályázat megnevezése (angol)	Digital security, privacy, data protection and accountability in critical sectors
Pályázat kódja	SU-DS05-2018-2019

Általános információk

Célok

2019 során a következő két altéma egyikében nyújthatók be pályázatok

a) Digitális biztonság, a magánélet és a személyes adatok védelme a multimodális közlekedésben

A pályázatokban az alábbi területek közül legalább kettővel foglalkozni szükséges:

(1): Az állampolgárok valamennyi járműtípushoz való hozzáféréseinek biztonságos kezelése. Az egységes európai közlekedési piac egy páneurópai, akadálytalan, a magánélet védelmét tiszteletben tartó megoldást igényel a tömegközlekedéshez, a megosztott használaton alapuló közlekedéshez, valamint az egyéni mobilitáshoz való hozzáféréshez, amely hozzáadott értéket teremt a polgárok számára, miközben biztosítja az adatok és a magánélet védelmét. Az intelligensebb rendszerek megfelelő, fokozott összekapcsolása azonban növeli a sebezhetőség felületét, ezért új, személyre szabott megoldásokat szükséges kidolgozni. (2): Bizonyos kibertámadások elleni biztosítás és védelem a multimodális közlekedés területén az egymással összefüggő fenyegetések és a terjedő veszélyeztetettség kezelése érdekében. A gyakorlatban is megvalósítható megoldások létrehozására szükséges törekedni, amelyek olyan veszélyeztetettségekkel szemben nyújtanak védelmet, amelyek súlyos hatást és elterjedésükkel katasztrofális következményeket gyakorolnak a multimodális közlekedés üzemeltetésére. A pályázatokban integrált és holisztikus megközelítéseket és eszközöket szükséges javasolni a multimodális közlekedés szolgáltatási és üzemeltetési területén előforduló összetett biztonsági vagy adatvédelmi incidensek és a személyes adatokkal való visszaélés dinamikus és automatikus előrejelzésére és kezelésére.

(2): Bizonyos kibertámadások elleni biztosítás és védelem a multimodális közlekedés területén



az egymással összefüggő fenyegetések és a terjedő veszélyeztetettség kezelése érdekében. A gyakorlatban is megvalósítható megoldások létrehozására szükséges törekedni, amelyek olyan veszélyeztetettségekkel szemben nyújtanak védelmet, amelyek súlyos hatást és elterjedésükkel katasztrofális következményeket gyakorolnak a multimodális közlekedés üzemeltetésére. A pályázatokban integrált és holisztikus megközelítéseket és eszközöket szükséges javasolni a multimodális közlekedés szolgáltatási és üzemeltetési területén előforduló összetett biztonsági vagy adatvédelmi incidensek és a személyes adatokkal való visszaélés dinamikus és automatikus előrejelzésére és kezelésére.

(3): A kiberbiztonság legjobb gyakorlatainak gyors használatbavételét lehetővé tevő szabványosítás. A pályázatokban értékelni kell a közlekedésre alkalmazható biztonsági minősítés (security labelling) megvalósíthatóságát, továbbá vonatkozó ajánlásokat és lehetőségeket szükséges kidolgozni.

A megvalósítás eredményeképpen a fejlesztések a TRL7 technológiai készültségi szintet kell, hogy elérjék.

b) Digitális biztonság, a magánélet és a személyes adatok védelme az egészségügyben

A témakörben benyújtott pályázatoknak az összetett egészségügyi ökoszisztémára vonatkozó európai uniós jogszabályok (pl. NIS, eIDAS és GDPR) gyakorlati végrehajtásához kell hozzájárulniuk, az összes szervezet minden érintettjének bevonásával, figyelembe véve az összes kezelt adattípust, különös tekintettel az érzékeny adatokra, ahogyan a GDPR meghatározza.

A pályázatokban az alábbi területek közül legalább kettővel foglalkozni szükséges:

(1): Együttműködésben az egészségügyi ökoszisztémában résztvevő érdekelttekkel dinamikus veszélyeztetettségi adatbázis létrehozása az Információs és Kommunikációs Technológián alapuló egészségügyi rendszereket, technológiákat, alkalmazásokat és szolgáltatásokat fenyegető veszélyek összegyűjtésére, feltöltésére, karbantartására és terjesztésére. Az egészségügyet érintő támadásokra dinamikus rendszertan kidolgozása, amely az egészségügyi kiberbiztonsági incidenskezelő rendszerek kiépítéséhez szolgál alapul.

(2): Dinamikus, tényeken alapuló, kifinomult, a biztonsággal, valamint a magánélet és a személyes adatok védelmével kapcsolatos kockázatok értékelésére szolgáló keretrendszerek és eszközök létrehozása, amelyek képesek a fenyegetések dominóhatásának és a veszélyek tovaterjedésének a kezelésére az egymással összekapcsolt egészségügyi infrastruktúrákban, szervezetekben, rendszerekben, a szállítói láncot érintő szolgáltatásokban és alkalmazásokban.

(3): Olyan együttműködésen alapuló, a magánéletet tiszteletben tartó eszközök biztosítása, amelyek az egészségügyben érdekelttek számára lehetővé teszik az információkhoz való hozzáférést, valamint azok megosztását, továbbá tanácsot adnak és az incidenskezeléssel kapcsolatos legjobb vagy jó gyakorlatokat osztják meg.

A megvalósítás eredményeképpen a fejlesztések a TRL7 technológiai készültségi szintet kell,



MAGYAR FEJLESZTÉSI KÖZPONT

hogyan elérjék.

Kedvezményezett	• Kutatóközpont (kutatóhely, egyetemi kutatóközpont) • Nagyvállalat • Mikro-, kis- és középvállalkozás • Non-profit szervezet (civil szervezet) • Non-profit szervezet (állami fenntartású intézmény) • Egyházi jogi szervezet • Egyéb gazdasági társaság (pl. szociális szövetkezet)
Részvételi forma	Konzorciumban történő pályázás
Konzorcium	A konzorcium tagjai minimum három különböző EU tagországból vagy társult országból kell, hogy érkezzenek.
Támogatott projektek várható száma	2
Pénzügyi információk	
Teljes keret	10.000.000 EUR
EU hozzájárulás projektenként (max.)	5.000.000 EUR
Támogatási intenzitás	100%
Támogatási forma	Vissza nem térítendő
Előfinanszírozás	30-45% előleg kérhető.
Elszámolható közvetett költségek	A közvetlen költségeket kiegészíti a közvetett költségek átalány-alapú támogatása, melynek mértéke a közvetlen költségek 25%-ával egyezik meg. Az átalány alvállalkozói teljesítményre nem igényelhető.
Határidők	
Benyújtási határidő	2019.08.22.17:00
Benyújtás	Elektronikusan https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ds05-2018-2019;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502,31094503;programCode=H2020;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=H2020-SU-DS-2018-2019-2020;sortQuery=openingDate;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState