



KÖZVETLEN BRÜSSZELI FORRÁS PÁLYÁZATI TÁJÉKOZTATÓ

Program	Horizon 2020
Pályázat megnevezése (magyar)	Az okos- és biztonságos városok, valamint a közterületek biztonsága
Pályázat megnevezése (angol)	Security for smart and safe cities, including for public spaces
Pályázat kódja	SU-INFRA02-2019

Általános információk

Célok

Az okos- és biztonságos város biztonsága és megfelelő működése összekapcsolt, összetett és egymástól kölcsönösen függő hálózatokon és rendszereken alapul: tömegközlekedési hálózatok, energia-, kommunikációs és kereskedelmi infrastruktúra, polgári biztonsági és bűnüldöző szervek, közúti közlekedési, illetve közérdekű hálózatok és szolgáltatások.

Ezek a hálózatok hatékony infrastruktúrával felderítési forrásokat és "big data" adatgyűjtést látnak el. Az ilyen típusú szűrt adatokat a biztonsági szakemberek használják, hogy támogassák a képességeiket és teljesítményüket. Például a tömegek védelme, továbbá a köz- és kormányzati épületek biztonsága növelhető a fenyegetések vagy a bűncselekmények előkészítőinek azonosításával, valamint a veszélyes eszközök vagy termékek korai felismerése révén; az elsősegélynyújtók gyorsabban tudnak eljutni a katasztrófa helyszínére, ha valós idejű számításokkal kalkulálják ki a rövidebb, lehetséges útvonalat.

A tervezett megoldások esetében figyelembe kell venni, hogyan lehet összehangolni többek között a következőket:

- fegyverek, robbanóanyagok és mérgező anyagok felderítésére szolgáló módszerek;
- videokamerás felügyeleti rendszerek;
- a bűncselekmények előkészítőinek azonosítására és semlegesítésére szolgáló módszerek, amelyek a zsúfolt területekre való behatolást minimalizálják.

A platform kialakítása során a pályázatoknak biztosítani szükséges a következőket:

- a város területén a biztonsági szereplők aktív bevonása, koordinációjuk és irányításuk megvalósítása; az interoperabilitási problémák megoldása, ezen kívül a városi okos rendszereket és a biztonsági szakembereket helyi szinten támogató rendszerek összekapcsolása és integrációja, többek között a köztük fennálló egymásra utaltság



modellezése és szimulációja révén;

- a városi okos rendszerek biztonságának fokozása, különösen a beléptetés ellenőrzése, a biztonságos kommunikáció és adattárolás terén, továbbá a bűnözők lehetséges visszaéléseinek a kezelése;
- új üzemeltetési koncepciók vizsgálata, amelyek az új monitoringmódszerekből, az érzékelők széles körű hálózatai és a közösségi média által szolgáltatott adatokból származnak;
- kárenyhítési stratégiák vizsgálata különböző forgatókönyvek összefüggésében a rugalmasság növelése céljából;
- biztonsági események és következményeik szimulációjára szolgáló modulok integrációja;
- a platform biztonságra gyakorolt, mennyiségi és minőségi hatásainak mérésére alkalmas modulok integrációja;
- a többféle forrásból származó adatok megosztásának, konszolidációjának és elemzésének biztosítása.

A pályázatokban választ kell keresni az alábbi kulcskérdések közül legalább egyre:

- az okos rendszerek (például a Dolgok Internete), valamint az okos városban található okos infrastruktúrák (pl. okos (kormányzati) épületek, okos vasutak, okos kikötők, okos gyárak, okos hidak, okos kórházak) összekapcsolódásai révén kialakuló további biztonsági fenyegetések és kockázatok szimulációja, felderítése és elemzése;
- kiberbiztonsági keretrendszer létrehozása, hogy megkönnyítse az okos város összes érdekeltje közötti együttműködést, a várostervezőktől kezdve, az infrastruktúra-üzemeltetőkn, a biztonsági szakembereken, az informatikai terület felügyeletével foglalkozó szakértőkn és szolgáltatókon keresztül az okos szervezetekig;
- egy közös megközelítés támogatása és végrehajtása, amelynek célja, hogy biztosítsa és megbízható módon kezelje az okos infrastruktúrákból és az okos városok által befogadott rendszerekből származó adatokat, segítve a polgárokat, az állami hatóságokat, a biztonsági szakembereket és a városi gazdaságot átlátható, hatékony és elszámoltatható kiberbiztonsági adatkezelési folyamatokkal, az adatvédelmi irányelvekkel összhangban.

A technológia fejlesztés célja a TRL7 technológiai készültségi szint elérése.

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)
Résztvételi forma	Konzorciumban történő pályázás
Konzorcium	A konzorcium tagjai minimum három különböző EU tagországból vagy társult országból kell, hogy érkezzenek.



MAGYAR FEJLESZTÉSI KÖZPONT

Támogatott projektek várható száma	2
Pénzügyi információk	
Teljes keret	16.000.000 EUR
EU hozzájárulás projektenként (max.)	8.000.000 EUR
Támogatási intenzitás	Profitorientált társaságok részére 70%, non-profit szervezeteknek 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-infra02-2019;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502,31094503;programCode=H2020;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=H2020-SU-INFRA-2018-2019-2020;sortQuery=openingDate;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState