

VEC: ODPOVEĎ (02) NA ŽIADOSŤ O VYSVETLENIE PODĽA § 48 ZÁKONA Č. 343/2015 Z. Z. O VEREJNOM OBSTARÁVANÍ A O ZMENE A DOPLNENÍ NIEKTORÝCH ZÁKONOV V ZNENÍ NESKORŠÍCH PREDPISOV

IDENTIFIKAČNÉ ÚDAJE VEREJNÉHO OBSTARAVATEĽA

Názov: **Mesto Košice**
Sídlo: Trieda SNP 48/A, 040 11 Košice
IČO: 00691135
DIČ: 2021186904
IČ DPH: SK2021186904

OZNAČENIE VEREJNÉHO OBSTARÁVANIA

Názov zákazky: **Malé zlepšenia eGov služieb mesta Košice**
Typ zákazky: Nadlimitná zákazka zadávaná postupom verejnej súťaže podľa § 66 a nasl. zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“), zabezpečované elektronickou formou predkladania ponúk
Číslo vestníka: 162/2021 - 16.07.2021
Značka: 33575 - MSS
Číslo ozn. v Ú. v. EÚ: 2021/S 137-365135 zo dňa 19.07.2021

Verejný obstarávateľ **Mesto Košice** so sídlom Trieda SNP 48/A, 040 11 Košice (ďalej len „verejný obstarávateľ“) uverejnil vo Vestníku verejného obstarávania č. 162/2021 zo dňa 16.07.2021 pod značkou 33575 - MSS a v Úradnom vestníku EÚ č. S137 zo dňa 19.07.2021 pod značkou 2021/S 137-365135 oznámenie o vyhlásení verejného obstarávania (ďalej len „Oznámenie“) na predmet zákazky „**Malé zlepšenia eGov služieb mesta Košice**“.

V súlade s §48 zákona č. 343/2015 o verejnom obstarávaní (ďalej len „ZVO“) Vám poskytujeme **vysvetlenie informácií** potrebných na vypracovanie ponuky:

Otázka č. 4:

Špecialista pre bezpečnosť IT:

- 1 osoba zodpovedná za činnosti zabezpečujúce ochranu IS a jeho zložiek proti bezpečnostným hrozbám
- a nepriateľským aktivitám, ktorých cieľom je krádež informácií, financií, zničenie dát, znefunkčnenie činnosti IS, prípadne iné činnosti s negatívnym dopadom, realizované prostredníctvom IS alebo na IS,
- minimálne 5 rokov odbornej praxe ochrany bezpečnosti informačných systémov,
- získaný a platný certifikát CISSP alebo ekvivalent daného certifikátu vydávaný medzinárodne uznávanou

Bude verejný obstarávateľ pre splnenie uvedenej podmienky akceptovať špecialistu, ktorý má certifikát Audítora Kybernetickej bezpečnosti vydaný Kompetenčným centrom kybernetickej bezpečnosti SR v zmysle zákona o kybernetickej bezpečnosti?

Pre odôvodnenie primeranosti uvádzame, že pre jeho získanie je potrebné okrem iných aj detailná znalosť procesov kybernetickej bezpečnosti, bezpečnostných technológií a IT architektúry, riadenie rizík, auditné procesy, riadenie kontinuity, riadenie incidentov a pod. (CISA, CISM, CRISC). Podľa dostupnej dokumentácie v podkladoch VO nie je žiadna iná potreba špecialistu v projekte mimo vyššie uvedených, kde v podmienkach SR uvedené audítorské oprávnenie nepostačuje na splnenie činností na ochranu IS.

Odpoveď č. 4:

Certifikát CISSP a certifikát audítora kybernetickej bezpečnosti nie je možné považovať za ekvivalentné. Audit kybernetickej bezpečnosti nie je projektová technická činnosť, riadenie projektov, ani riadenie informačnej bezpečnosti organizácie, ale činnosť súvisiaca výhradne s posudzovaním zhody. Okrem toho pre audítora kybernetickej bezpečnosti platia prísne požiadavky na objektivnosť a nestrannosť. Profesná prax držiteľa certifikátu CISSP je smerovaná na výkon riadenia informačnej bezpečnosti organizácie, vrátane projektovej technickej činnosti, riadenia projektov a bezpečnostnej architektúry. Pre držiteľa certifikátu CISSP nie sú explicitne definované požiadavky na nestrannosť.

Verejný obstarávateľ nebude akceptovať predloženie certifikátu Audítora kybernetickej bezpečnosti vydaný Kompetenčným centrom kybernetickej bezpečnosti SR. Bude akceptovať certifikát CISSP, CISM, CISA alebo ekvivalent daného certifikátu vydávaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.