

Úrad verejného zdravotníctva Slovenskej republiky
Trnavská cesta 52
826 45 Bratislava

Váš list číslo/zo dňa
29.02.2024

Naše číslo
01032024

Kontaktná osoba
Monika Sládečková/
BID Procurement Manager

Dátum, miesto
01.03.2024, Bratislava

VEC: Žiadosť o vysvetlenie - odpoveď

Na základe žiadosti verejného obstarávateľa vo veci vysvetlenia podmienok účasti, zo dňa 29.02.2024 doručenej prostredníctvom portálu JOSEPHINE k zákazke „Služby podpory, prevádzky, údržby a rozvoja Integrovaného systému úradov verejného zdravotníctva“ (ďalej aj „zákazka“) realizovanej postupom verejnej súťaže podľa § 66 prostredníctvom informačného systému JOSEPHINE. Oznámenie o vyhlásení verejného obstarávania bolo zverejnené v Úradnom vestníku EÚ č. 2023/S 165-520208 z 29.08.2023 a vo Vestníku verejného obstarávania č. 170/2023 z 30.08.2023 ozn. 29469 – MSS Oznámenie o vyhlásení verejného obstarávania (ďalej len „Oznámenie“) Vám odpovedáme nasledovne :

OTÁZKA:

1.

Verejný obstarávateľ požadoval nasledovnú podmienku účasti:

Kľúčový expert č. 4 - Špecialista pre oblasť verejného zdravotníctva (IT analytik - business)

- minimálne dve profesionálne praktické skúsenosti v oblasti tvorby analýz pre verejné zdravotníctvo.

V rámci predloženého životopisu Mgr. Petra Labaša sú uvedené praktické skúsenosti:

Obdobie: 11/2022-10/2023

Pozícia: softvérový architekt, systémový analytik

Odberateľ/ Zamestnávateľ: Implementácia systému telemedicíny pre sieť kardiologických ambulancií

Názov projektu: Univerzálny telemedicínsky systém pre kardiologické ambulancie

Popis projektu: príprava ponuky, analýza, návrhy riešenia, modelovanie procesov, koordinácia projektových aktivít

Obdobie: 02/2021-09/2023

Pozícia: softvérový architekt, systémový analytik

Odberateľ/ Zamestnávateľ: Výskumný projekt v spolupráci s Jesseniova lekárska fakulta UK a STU Bratislava

Názov projektu: Systém telemedicíny (komplexný inteligentný kognitívny systém pre monitorovanie zdravotného stavu pacientov na báze telemedicíny)

Popis projektu: analýza, návrh riešenia, modelovanie procesov, koordinácia projektových aktivít

Obdobie: 07-11/2020

Pozícia: IT programátor/ vývojár

Odberateľ/ Zamestnávateľ: Úrad verejného zdravotníctva SR

Názov projektu: Integrovaný systém úradov verejného zdravotníctva

Popis projektu: analýza a programovanie, testovanie, spustenie unit testov, odstraňovanie chýb

Obdobie: 03/2012-11/2015

Pozícia: IT analytik, IT programátor/ vývojár

Odberateľ/ Zamestnávateľ: Prvá stavebná sporiteľňa

Názov projektu: EPI – register pohľadávok - konkurzy

Popis projektu: Integrácia do bankového systému, príprava testovanie, konzultácia s EPI, prevádzka systému evidencie a výmeny informácií o vyhlásených konkurzoch a pohľadávky klientov v bankovom sektore. Komplexné softvérové riešenia v oblasti preverovania bonity klienta, kontroly jeho pohľadávok, upomínania, odstupovania, exekúcií, vymáhania

Verejný obstarávateľ Vás na základe vyššie uvedeného, žiada o bližšie vysvetlenie praktických skúseností uvedených v zozname praktických skúseností tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti:

- minimálne dve profesionálne praktické skúsenosti **v oblasti tvorby analýz pre verejné zdravotníctvo.**

Verejný obstarávateľ Vás súčasne žiada o doplnenie konkrétnych odberateľov/ zamestnávateľov do praktických skúseností s názvom:

Univerzálny telemedicínsky systém pre kardiologické ambulancie

Systém telemedicíny (komplexný inteligentný kognitívny systém pre monitorovanie zdravotného stavu pacientov na báze telemedicíny

Odpoveď 1. :

Vo svojej pozícii IT analytik – business pracoval **pán Peter Labaš na projektoch venovaných inovatívnym službám verejného zdravotníctva – konkrétne pripravoval / tvoril analýzy riešení pre Telemedicínu (Telemedicina je diaľkový prenos lekárskeho informácií (tlak, pulz atď.) od pacienta k lekárovi prostredníctvom telekomunikácií a informačných technológií: obojsmerné video, e-mail, smartfóny, bezdrôtové prístroje a ďalšie. Tieto technológie sa používajú na určenie stavu pacienta, na poskytovanie lekárskeho služieb na diaľku a na poskytovanie konzultácií na diaľku. Telemedicina je súčasťou elektronického zdravotníctva. Elektronické zdravotníctvo je efektívny a bezpečný spôsob využitia informačných a komunikačných technológií pri podpore zdravia a aktivít súvisiacich so zdravím; zahŕňa poskytovanie zdravotnej starostlivosti, monitoring verejného zdravia, ale aj zdravotnícku literatúru a vzdelávanie, vedomostnú bázu a vedecký výskum.).** V spolupráci s lekármi Jesseniovej lekárskej fakulty UK a Fakultnej nemocnice v Martine **analyzoval, navrhol a verifikoval model a funkčný prototyp flexibilného a robustného systému telemedicíny** pre využitie v nemocniciach, zdravotných strediskách, domovoch sociálnych služieb a v neposlednom rade pre bežných obyvateľov, ktorým má systém slúžiť s celospoločenským dopadom. Veľký význam má v prípade starších ľudí či chronicky chorých pacientov, pričom riešenie pozostáva z novo navrhnutých a vyvinutých prvkov lekárskej monitorovacej elektroniky i dostupných prvkov, ktoré poskytujú možnosť merať parametre napomáhajúce k analýze klinického stavu pacientov so spojením

s novými modulmi prepojenia nemocničných systémov, či Národné centrum zdravotníckych informácií - NCZI s koncovými bodmi. Vzhľadom na veľmi nízky stupeň rozvoja telemedicíny na Slovensku a jej význam pre všetkých obyvateľov v prípade pandemických hrozieb i nad ich rámec a vzhľadom na perspektívu témy, ktorá bude v blízkej dobe neustále rozvíjaná, možno projektu prisúdiť veľký význam a výsledok bude dosahovať ihneď i dlhodobu významnú pridanú hodnotu. Inovatívnosť riešenia spočíva vo využití najmodernejších nástrojov IKT, teda ako nových miniatúrnych meracích zariadení, tak i metód kognitívneho spracovania dát pomocou neurónových sietí, schopných vo veľkej miere vyhodnocovať dáta s veľkou presnosťou a zároveň sa dlhodobo automatizovane učiť novým možnostiam pre zabezpečenie pomocných podkladov pre rozhodovanie lekárov vo veci zdravotného stavu pacienta. Telemedicina eliminuje i potrebu kontaktu lekár – pacient, čo priamo zamedzuje šíreniu potencionalneho prenosu na zdravotnícky personál a tiež sa pomocou telemedicínskeho systému umožní vykonávanie častejších meraní a šetrenie kapacity zdravotného personálu. Inovácia a vysoká pridaná hodnota riešenia, ktoré predstavuje výsledok projektu spočíva aj vo včasnej identifikácii zmien zdravotného stavu, teda včasnej prevencie, čo je v medicíne najlacnejšie i najmenej náročné riešenie.

Verejný obstarávateľ Vás súčasne žiada o doplnenie konkrétnych odberateľov/ zamestnávateľov do praktických skúseností s názvom:

Univerzálny telemedicínsky systém pre kardiologické ambulancie - **pre zamestnávateľa Asseco Central Europe - pre odberateľa FEI STU v rámci výskumného programu pre Telemedicínu**

Systém telemedicíny (komplexný inteligentný kognitívny systém pre monitorovanie zdravotného stavu pacientov na báze telemedicíny) - **pre zamestnávateľa Asseco Central Europe - pre odberateľa Výskumná agentúra - v rámci projektu 313011ASY8 - Výskum a rozvoj telemedicínskych riešení na podporu boja proti pandémie vyvolanej ochorením COVID-19 a znižovaní jej negatívnych následkov monitorovaním zdravotného stavu ľudí za účelom eliminácie rizika nákazy u rizikových skupín obyvateľstva.**

OTÁZKA

2.

Verejný obstarávateľ požadoval nasledovnú podmienku účasti:

Kľúčový expert č. 10 Konzultant pre oblasť bezpečnosti (Špecialista pre bezpečnosť IT)

- minimálne 2 profesionálne praktické skúsenosti v oblasti bezpečnosti informačných systémov v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov.

V rámci predloženého životopisu p. Vladimíra Sekerku sú uvedené praktické skúsenosti, z ktorých nevyplýva, že sa týkali oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov.**

Verejný obstarávateľ Vás na základe vyššie uvedeného, žiada o bližšie vysvetlenie praktických skúseností uvedených v zozname praktických skúseností tak, aby bolo možné vyhodnotiť stanovenú podmienku účasti:

- minimálne 2 profesionálne praktické skúsenosti v oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov, **zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov.

Verejný obstarávateľ Vás súčasne žiada o informáciu, či sa praktická skúsenosť s názvom Zabezpečenie Aplikačnej bezpečnosti v súlade s požiadavkami zákona o kybernetickej bezpečnosti (odberateľ: Letisko Košice – Airport Košice, a.s.), týkala oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** alebo len oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti**

Odpoveď 2. :

Verejný obstarávateľ požadoval nasledovnú podmienku účasti:

Kľúčový expert č. 10 Konzultant pre oblasť bezpečnosti (Špecialista pre bezpečnosť IT)

- minimálne 2 profesionálne praktické skúsenosti v oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov, **zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov.

V rámci predloženého životopisu pána Vladimíra Sekerku bola uvedená, okrem iného, praktická skúsenosť **pre verejného obstarávateľa „Ministerstvo vnútra Česká republika“** , v rámci ktorej, pán Vladimír Sekerka zastával pozíciu „**Expert pre oblasť bezpečnosti**“ v rámci realizácie projektov : **Projekt e-Sbirka** a **Projekt e-Legislativa** . Jedná sa o **dva samostatne** realizované projekty, ktoré sú síce na seba naviazané, ale je nutné podotknúť, že každý systém si vyžadoval samostatné komplexné riešenie kybernetickej bezpečnosti:

- **Portál e-Sbírký** : Kompletní garantovaný právni rád dostupný každému bez omezení , Úplně, přehledně, jednoduše a jednom místě stát zpřístupňuje každému úplná znění právních aktů
- **Veřejný portál e-Legislativy** : zlepšuje proces tvorby a projednání právních předpisů, zvyšuje transparentnost a kvalitu legislativního procesu a zvyšuje orientaci v častých změnách právního řádu.“

Systém e-Sbirka slúži na digitalizáciu právnych predpisov v právne záväznom či overenom úplnom (konsolidovanom) znení vo forme právnych aktov zaradených v Zbierke v elektronickej podobe, ako aj v informatívnej štruktúrovanej podobe, ktorá umožní modernú dynamickú prácu s právnymi predpismi, ako vyhľadávanie v texte, zobrazenie úplných znení v rôznych časových okamžikoch, naviazanie základných predpisov s ich novelami, využívanie odkazov do súvisiacich predpisov a právnych slovníkov Českej republiky i Európskej únii.

Systém e-Legislativa slúži ako editor právnych predpisov, tzv. „e-Šablona“, ktorý bude umožňovať tvorbu a novelizáciu predpisov podľa všetkých legislatívnych pravidiel.

Predmetom bola kompletná implementácia a akceptácia týchto významných informačných systémov : **systému e-Sbírka a systému e-Legislativa a súčasťou predmetu zákazky boli tvorby bezpečnostnej dokumentácie** ako sú bezpečnostné stratégie, bezpečnostné politiky, bezpečnostná dokumentácia na úrovni interných riadiacich aktov (Smernica Riadenie rizík a aktív, Smernica riadenie dodávateľov, Smernica riadenie prevádzky a komunikácii, Smernica riadenie prístupu, Smernica zálohovanie a obnova a dlhodobé uchovávanie, Smernica bezpečnosť komunikačnej siete, Smernica bezpečné používanie kryptografickej ochrany, Smernica Ochrana pred škodlivým kódom, smernica Zvládanie kybernetických bezpečnostných incidentov, Smernica Riadenie zmien, Plány kontinuity činnosti a obnovy, Bezpečnostná politika a pod.) **Smernice upravovali všetky** oblasti v súlade so **zákonom č. 181/2014 Sb. o kybernetickej bezpečnosti** a o zmene súvisiacich zákonov (zákon o kybernetickej bezpečnosti), ve znění pozdějších předpisů a **vyhlášky č. 316/2014 Sb., o kybernetickej bezpečnosti**, ve znění pozdějších předpisů a **zákona č. 365/2000 Sb., o informačních systémech veřejné správy** a o zmene některých dalších zákonů, ve znění pozdějších předpisů, ktoré sú **priamym ekvivalentom slovenských zákonov** č. 69/2018 Z .z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Berúc do úvahy vyššie uvedené, máme za to, že p. Vladimír Sekerka, ako **Expert v oblasti bezpečnosti spĺňa podmienku** aplikácie relevantnej ekvivalentnej legislatívy, ktorá bola definovaná v súťažných podkladoch.

Praktická skúsenosť preukazovaná prostredníctvom projektu „Elektronické služby zdravotníctva- ESO1“ **pre odberateľa Ministerstvo zdravotníctva Slovenskej republiky spĺňa** podmienku praktickej skúsenosti v oblasti bezpečnosti informačných systémov v **súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, resp. **jeho ekvivalentom**, vzhľadom na fakt, že zabezpečenie bezpečnosti spomínaného systému bolo realizované v roku 2015 v súlade s vtedy platným **zákonom č. 275/2006 Z. z. o informačných systémoch vo verejnej správe** a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcimi právnymi predpismi, ktorý je priamym predchodcom a bol zrušený súčasne platným **zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi. Vzhľadom na fakt, že zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti bol prijatý až tri roky po ukončení tohto projektu, môžeme konštatovať, že bezpečnosť systému realizovaného v rámci projektu bola zabezpečená v súlade so všetkými vtedy platnými právnymi normami a štandardmi.

Aby verejný obstarávateľ, **nemal akékoľvek pochybnosti** o odbornosti p. Vladimíra Sekerku v oblasti bezpečnosti informačných systémov, **dopĺňame** ďalšiu odbornú praktickú **skúsenosť v oblasti bezpečnosti informačných systémov**, kde p. Vladimír Sekerka zastával pozíciu „**Expert pre bezpečnosť informácií**“ v rámci projektu „**Projekt Kybernetická bezpečnosť**“, ktorý pozostával s Vypracovaním analýzy rizík a stratégie za rezort zdravotníctva a vypracovanie analýzy rizík, stratégie, riadiacej dokumentácie a smerníc **v súlade s požiadavkami zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov a **v súlade s požiadavkami zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov **pre odberateľa Ministerstvo zdravotníctva Slovenskej republiky**.

Verejný obstarávateľ požadoval preukázať u kľúčového experta č. 10 Konzultant pre oblasť bezpečnosti (Špecialista pre bezpečnosť IT) **minimálne 2 profesionálne praktické skúsenosti v oblasti bezpečnosti informačných systémov v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v oblasti zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov. Máme za to, že požiadavka verejného obstarávateľa nebola stanovená tak, že profesionálna praktická skúsenosť musí byť realizovaná súčasne v oblasti bezpečnosti informačných systémov v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a zároveň v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi, alebo ekvivalenty uvedených zákonov.** Na základe vyššie uvedeného, máme za to, že Projekt „Zabezpečenie aplikačnej bezpečnosti v súlade s požiadavkami zákona o kybernetickej bezpečnosti pre odberateľa Letisko Košice – Airport Košice, a.s. „ spĺňa verejným obstarávateľom stanovenú podmienku na praktickú skúsenosť v oblasti bezpečnosti informačných systémov **v súlade so zákonom č. 69/2018 Z .z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov.

Veríme, že týmto vysvetlením došlo k riadnemu a uspokojivému zodpovedaniu otázok Verejného obstarávateľa, ako aj k náprave akýchkoľvek pochybností a nejasností. Zároveň vyhlasujeme, že týmto vysvetlením nedochádza k zmene ponuky.

Príloha :

- Kľúčový expert č. 4 - Špecialista pre oblasť verejného zdravotníctva (IT analytik - business) : Životopis Peter Labaš
- Kľúčový expert č. 10 Konzultant pre oblasť bezpečnosti (Špecialista pre bezpečnosť IT) : Životopis Vladimír Sekerka

V Bratislave, dňa 01.02.2024

Profesijný životopis

Kľúčový expert č. 4 – Špecialista pre oblasť verejného zdravotníctva (IT analytik – business)

Titul, Meno a priezvisko: Mgr. Peter Labaš

Vzdelanie / odborná kvalifikácia :

Inštitúcia (Od dátumu - do dátumu)	Diplom:
2010-2016	Paneurópska vysoká škola, fakulta Informatiky, odbor Aplikovaná informatika (I. a II. Stupeň vysokoškolského vzdelania)

Pracovná pozícia:

Opis pracovnej náplne:	
Analytik systémov IT	Návrh, analýza a príprava nových riešení pre HealthCare projekty Analýza a príprava zadání a úloh pre tím vývojárov/testerov/integrátorov Komunikácia a kooperácia s business analytikmi Implementácia projektov a všetkých potrebných častí IKT systémov a riešení Príprava softvérovej architektúry, modelovanie procesov Participácia na NCZI, UVZ riešeniach Automatizácia skladu liekov CPL – nemocnica SZ Trebišov Projekt telemetrie
Softvérový analytik	Analýza a vývoj softvéru (SAAS) v oblasti poisťovníctva (poisťovne DE, AT, CH) Definovanie a popis business pravidiel a nastavení produktov podľa potrieb konkrétnej poisťovne
Senior analytik	Implementácie a integrácie bankových systémov Vývoj DMS, ECM a FrontOffice systému Spracovanie Externých exekúcií, odstúpení, konkurzov, vymáhanie pohľadávok, upomienok na nesplácanie.

	Hromadné spracovania marketingových akcií, distribučné cesty komunikácie s klientami, výpisy z účtov, zmluvy a záložné zmluvy, generovanie zmluv PO
--	---

Profesijné skúsenosti

Zamestnávateľ / pracovnoprávny vzťah	Miesto	Mesiac a rok plnenia / zamestania	Funkcia	Popis
Asseco Central Europe, a.s.	Bratislava	03/2020 - trvá	Analytik systémov IT	návrhy informačných systémov v oblasti zdravotných služieb, konzultačné činnosti v oblasti verejného zdravotníctva
Msg Life Slovakia s.r.o.	Bratislava	03/2016 - 02/2020	Softvérový analytik	Návrhy a správa informačných systémov v oblasti poistenia, konzultačné činnosti v oblasti verejného zdravotníctva
Prvá stavebná sporiteľňa, a.s.	Bratislava	01/96 – 01/2015	Senior analytik – vývoj softvéru Develop TeamLead	Návrhy a správa informačných systémov v oblasti bankovníctva

Prehľad profesnej praxe vzťahujúcej sa k predmetu verejnej zákazky

Čas plnenia zmluvy / projektu t.j. od – do (mesiac / rok)	Názov a sídlo odberateľa resp. zamestnávateľa	Pozícia na projekte	Názov referencie / projektu	Stručný opis projektu, popis a rozsah činností, ktorý expert zabezpečoval	Meno, priezvisko, funkcia, tel.číslo, e-mail na pracovníka odberateľa/zamestnávateľa, ktorého si
---	---	---------------------	-----------------------------	---	--

					možno tieto údaje overiť
11.2022-10.2023	<u>pre zamestnávateľa Asseco Central Europe - pre odberateľa FEI STU</u> v rámci výskumného programu pre Telemedicínu	Softverový architekt, systémový analytik	Univerzálny telemedicínsky systém pre kardiologické ambulancie	Príprava ponuky, príprava / tvorba Analýzy pre telemedicínu (projekt z oblasti verejného zdravotníctva) , návrhy riešenia, modelovanie procesov, koordinácia projektových aktivít Implementácia systému telemedicíny pre sieť kardiologických ambulancií	
02.2021-09.2023	<u>pre zamestnávateľa Asseco Central Europe - pre odberateľa Výskumná agentúra</u> - v rámci projektu 313011ASY8 - Výskum a rozvoj telemedicínskych riešení na podporu boja proti pandémie vyvolanej ochorením COVID-19 a znižovaní jej negatívnych následkov monitorovaním zdravotného stavu ľudí za účelom eliminácie	Softverový architekt, systémový analytik	Systém telemedicíny (komplexný inteligentný kognitívny systém pre monitorovanie zdravotného stavu pacientov na báze telemedicíny)	Tvorba Analýz pre systém Telemedicínu (projekt z oblasti verejného zdravotníctva), návrh riešenia, modelovanie procesov, koordinácia projektových aktivít Výskumný projekt v spolupráci s Jesséniova lekárska fakulta UK a STU Bratislava	

	rizika nákazy u rizikových skupín obyvateľstva.				
07-11.2020 (ITMS: 311071T621)	<u>pre</u> zamestnávateľa Asseco Central Europe - Pre odberateľa Úrad verejného zdravotníctva Slovenskej republiky	IT programátor /vývojár	Integrovaný systém úradov verejného zdravotníctva – IS UVZ	Tvorba Analýz pri návrhu Integrovaného systému úradov verejného zdravotníctva, programovanie, testovanie, spustenie unit testov, odstraňovanie chýb - revízia a interná akceptácia analytických výstupov	
03.2012- 11.2015	Prvá stavebná sporiteľňa a.s.	IT analytik IT programátor /vývojár	EPI – register pohľadávok - konkurzy	Integrácia do bankového systému, príprava testovanie, konzultácia s EPI, prevádzka systému evidencie a výmeny informácii o vyhlásených konkurzoch na pohľadávky klientov v bankovom sektore. Komplexné softvérove riešenia v oblasti preverovania bonity klienta, kontroly jeho pohľadávok, upomínania,	

				odstupovania, exekúcií, vymáhania	
--	--	--	--	---	--

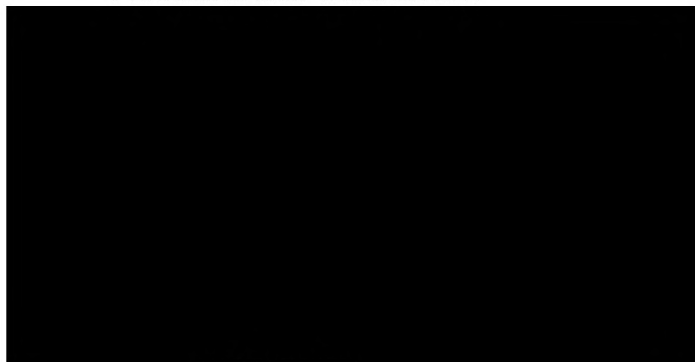
Certifikáty:

Rok	Certifikáty:
2016	Windows Server , PowerShell (GOPAS)
2015	Togaf (certifikačná skúška PEVŠ)
2014	Prince 2 (certifikačná skúška PEVŠ)
2011	Cisco (základná úroveň)
2010	Web Service Development (IBM)
2007	Vývoj Microsoft .NET aplikácií – C# (GOPAS)
2000	LN Domino a vývoj pre Internet (Ability)
2000	LN Application Development (Ability)
1999	SAP garant modulu FI (Slovakodata, Interdata Slovensko)

Týmto vyjadrujem svoj súhlas so správou, spracovaním a uchovaním osobných údajov v súlade s nariadením č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a zákonom č.18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov na účely podania ponuky na predmet zákazky: „Služby podpory, prevádzky, údržby a rozvoja Integrovaného systému úradov verejného zdravotníctva.“, verejného obstarávateľa: Úrad verejného zdravotníctva Slovenskej republiky, (ďalej len „zákazka“).

Vyhlasujem, že všetky uvedené informácie sú pravdivé a v prípade realizácie zákazky budem k dispozícii pri plnení zákazky.

V Bratislave dňa: 4. marca 2024



Profesijný životopis

Kľúčový expert č. 10 – Konzultant úre oblasti bezpečnosti (Špecialista pre bezpečnosť IT)

Meno a priezvisko: Vladimír Sekerka

Vzdelanie / odborná kvalifikácia :

Inštitúcia (Od dátumu - do dátumu)	Diplom:
Fakulta Matematiky, Fyziky a Informatiky, Univerzity Komenského v Bratislave. Špecializácia: Teoretická informatika 09/1992-05/1997	Vysokoškolské vzdelanie druhého stupňa/Magisterský titul

Pracovná pozícia:

Opis pracovnej náplne:	
Konzultant informačnej bezpečnosti	<ul style="list-style-type: none">- riešenie bezpečnosti vo vývojových projektoch- plány kontinuity činnosti a havarijné plány- realizácia analýzy rizík- užívateľské politiky riadenia prístupu k informačným systémom (definícia procesov a prístupových práv na základe business rolí)- kontrola riadenia prístupov k informačným systémom- príprava pobočky spoločnosti pre získanie certifikátu ISO/IEC 27001 o riadení informačnej bezpečnosti

Profesijné skúsenosti

Zamestnávateľ / pracovnoprávny vzťah	Miesto	Mesiac a rok plnenia / zamestania	Funkcia	Popis
ISTROBANKA, a.s. Laurinská 1 811 01 Bratislava	Bratislava	08/1997 – 08/2004	Vedúci oddelenia informačnej bezpečnosti	<ul style="list-style-type: none">- riadenie informačnej bezpečnosti a analýzy rizík- návrh bezpečnostných opatrení- vzdelávanie zamestnancov v oblasti informačnej bezpečnosti
Všeobecná úverová banka, a.s. Mlynské nivy 1 829 90 Bratislava	Bratislava	10/2005 – 02/2007	Vedúci oddelenia informačnej bezpečnosti	<ul style="list-style-type: none">- riadenie informačnej bezpečnosti a analýzy rizík- návrh bezpečnostných opatrení- vzdelávanie zamestnancov v oblasti informačnej bezpečnosti

ICZ a.s. Na hřebenech II 1718/10 140 00 Praha 4	Praha	02/2007 – 07/2009	Konzultant informačnej bezpečnosti	<ul style="list-style-type: none"> - návrh systému riadenia bezpečnosti vo veľkých organizáciách (klienti so 4000+ zamestnancami a 600+ aplikáciami) - návrh metodiky a realizácia Analýzy rizík - analýza rizík nástrojom RA2 - tvorba vlastného nástroja pre analýzu rizík - implementácia klasifikácie aktív - návrh systému riadenia bezpečnosti v súlade so štandardom ISO/IEC 27001
Asseco Central Europe, a.s. Budějovická 778/3a 140 00 Praha 4	Praha	02/2010 – 02/2012	Špecialista informačnej bezpečnosti	<ul style="list-style-type: none"> - riešenie bezpečnosti vo vývojových projektoch - plány kontinuity činnosti a havarijné plány - realizácia analýzy rizík - užívateľské politiky riadenia prístupu k informačným systémom (definícia procesov a prístupových práv na základe business rolí) - kontrola riadenia prístupov k informačným systémom - príprava pobočky spoločnosti pre získanie certifikátu ISO/IEC 27001 o riadení informačnej bezpečnosti
TEMPEST a.s. Krasovského 14 851 01 Bratislava	Bratislava	07/2012 – 09/2014	Špecialista informačnej bezpečnosti	<ul style="list-style-type: none"> - analýza rizík informačného systému, návrh opatrení na znižovanie rizík - návrhy smerníc súvisiacich s informačnou bezpečnosťou - audit informaçnej bezpečnosti v súlade s platnými smernicami a zmluvami - havarijné plány v nástroji LDRPS - analýza dostupných nástrojov pre analýzu rizík pre potrebu klientov - bezpečnostné IT projekty na ochranu osobných údajov
ASTIR, s.r.o.	Bratislava	02/2019 – 09/2021	Bezpečnostný špecialista	- Príprava spoločností na certifikáciu v súlade so štandardmi ISO27001, ISO9001 a ISO22301.
LYNX - spoločnosť s ručením obmedzeným Košice Gavlovičova 9 040 17 Košice Kontakt: Ing. Zoltán Kollár Tel.: +421 55 727 17 17	Bratislava	05/2015 - 09/2021	Bezpečnostný špecialista	<ul style="list-style-type: none"> - implementácia a realizácia požiadaviek kybernetickej bezpečnosti podľa zákona o kybernetickej bezpečnosti 69/2018 - realizácia bezpečnosti informačných systémov - implementácia bezpečnosti aplikačnej infraštruktúry v súlade so zákonom o kybernetickej bezpečnosti - analýza rizík a procesy riadenia rizík - bezpečnostné IT projekty na ochranu osobných údajov - zabezpečenie kontinuity činnosti - BIA, stratégia, plány, testovanie - vypracovanie, realizácia a implementácia dokumentácie, procesov a auditov podľa požiadaviek normy ISO / IEC 27001 - príprava spoločností na certifikáciu ISO / IEC 27001 a ISO 9001

Asseco Central Europe, a.s. Galvaniho 19045/19, 821 04 Bratislava	Bratislava	10/2021 - trvá	Bezpečnostný špecialista	<ul style="list-style-type: none"> - riešenie bezpečnosti vo vývojových projektoch - plány kontinuity činnosti a havarijné plány - realizácia analýzy rizík - užívateľské politiky riadenia prístupu k informačným systémom (definícia procesov a prístupových práv na základe business rolí) - kontrola riadenia prístupov k informačným systémom - príprava pobočky spoločnosti pre získanie certifikátu ISO/IEC 27001 o riadení informačnej bezpečnosti
---	------------	-------------------	-----------------------------	--

Prehľad profesnej praxe vzťahujúcej sa k predmetu verejnej zákazky

Čas plnenia zmluvy / projektu t.j. od – do (mesiac / rok)	Obdobie , počas ktorého sa expert zúčastni l na realizáci í projektu	Názov a sídlo odberateľa resp. zamestnávateľa	Pozícia na projekte	Názov referencie / projektu	Stručný opis projektu, popis a rozsah činností, ktorý expert zabezpečoval	Meno, priezvisko, funkcia, tel.číslo, e- mail na pracovníka odberateľa/ zamestnávateľa , ktorého si možno tieto údaje overiť
09/2018 - súčasnosc ť	01/2022 - súčasnosc ť	Česká republika – Ministerstvo vnitro Praha 7, Nad Štolou 936/3, 170 00, IČ: 00007064	Expert pre oblast' bezpečnosti	Projekt e- Sbírka a Projekt e- Legislative	Implementátor technického riešenia projektu „Projekt e- Sbírka a e-Legislative (Projekt elektronické Sbírky zákonů a mezinárodních smluv a elektronické tvorby právních předpisů : Portál e-Sbírky : Kompletní garantovaný právní řád dostupný každému bez omezení Úplně, přehledně, jednoduše a jednom místě stát zpřístupňuje každému úplná znění právních aktů a Veřejný portál e-Legislative : Systém e-Legislative zlepšuje proces tvorby a projednání právních předpisů, zvyšuje transparentnost a kvalitu legislativního procesu a zvyšuje orientaci v častých změnách právního řádu.)“	

					<p>Predmetom bola kompletná implementácia a akceptácia významného informačného systému e-Sbírka a systému e-Legiskativa slúžiaceho k modelovaniu enterprise architektúry, vrátane dodávky a implementácie integračnej platformy a vrátane služieb analýzy a návrhu/modelovaniu enterprise architektúry.</p> <p>Súčasťou predmetu zakázky boli tvorby bezpečnostnej dokumentácie ako sú bezpečnostné stratégie, bezpečnostné politiky, bezpečnostná dokumentácia na úrovni interných riadiacich aktov (Smernica Riadenie rizík a aktív, Smernica riadenie dodávateľov, Smernica riadenie prevádzky a komunikácii, Smernica riadenie prístupu, Smernica zálohovanie a obnova a dlhodobé uchovávanie, Smernica bezpečnosť komunikačnej siete, Smernica bezpečné používanie kryptografickej ochrany, Smernica Ochrana pred škodlivým kódom, smernica Zvládanie kybernetických bezpečnostných incidentov, Smernica Riadenie zmien, Plány kontinuity činnosti a obnovy, Bezpečnosť politika apod.) Smernice upravovali všetky oblasti v súlade so zákonom č. 181/2014 Sb. o kybernetické bezpečnosti v ČR a v súlade so zákonom 365/2000 Sb.o informačních systémech veřejné správy v ČR .</p>	
05/2019 – 09/2021	05/2019 – 09/2021	Letisko Košice - Airport Košice, a.s. Letisko Košice, 041 75 Košice	Špecialista informačnej bezpečnosti	Zabezpečeni e aplikačnej bezpečnosti v súlade s požiadavka mi zákona o kybernetick ej bezpečnosti	<p>Predmetom zákazky bolo zabezpečiť implementáciu bezpečnostných opatrení a súlad infraštruktúry IS letiska Košice s požiadavkami zákona o kybernetickej bezpečnosti a súvisiacej legislatívy (bezpečnosť informačných systémov v súlade so zákonom č. 69/2018 Z .z. o kybernetickej</p>	<p>N n e</p> <p>sis</p>

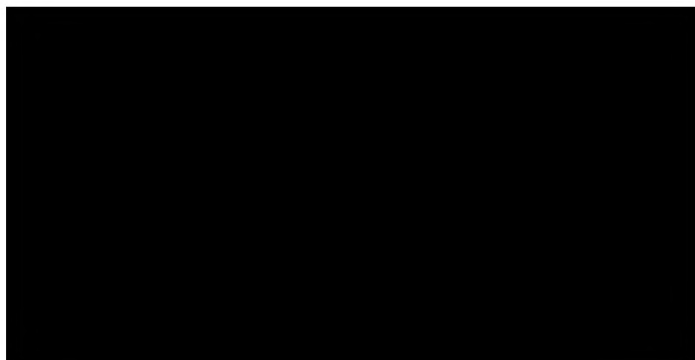
					<p>bezpečnosti a o zmene a doplnení niektorých zákonov a s nimi súvisiacimi vykonávajúcim právnymi predpismi,) a zabezpečiť procesy implementácie aplikačnej bezpečnosti a monitorovania závažných kybernetických bezpečnostných incidentov. Súčasťou predmetu zakázky boli tvorby bezpečnostnej dokumentácie ako sú bezpečnostné stratégie, bezpečnostné politiky, bezpečnostná dokumentácia na úrovni interných riadiacich aktov (Smernica o bezpečnej prevádzke IS a sietí, Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov, Politika BCM vrátane stratégie obnovy a BCP a DRP plány,) metodiky pre bezpečnostné činnosti. Smernice upravovali všetky oblasti v súlade so zákonom o kybernetickej bezpečnosti.</p>	
09 2017- /2022	09/ 2017-/ 2022	OKTE, a.s. Mlynské nivy 48 821 09 Bratislava.	Špecialista informačnej bezpečnosti	Vytvorenie integrované ho systému riadenia informačnej kvality a bezpečnosti	<p>Príprava spoločnosti na certifikáciu v súlade s požiadavkami ISO27001 a ISO9001. Súčasťou predmetu zakázky boli tvorby bezpečnostnej dokumentácie ako sú bezpečnostné stratégie, bezpečnostné politiky, bezpečnostná dokumentácia na úrovni interných riadiacich aktov (Smernica o bezpečnej prevádzke IS a sietí, Smernica o informačnej bezpečnosti, Politika BCM vrátane stratégie obnovy Plány BCP a DRP. Smernice upravovali všetky oblasti v súlade s požiadavkami ISO27001)</p>	
10/2020 - súčasnosť	10/2020 - 09/2021	Slovenská elektrizačná prenosová sústava, a.s.	Expert pre bezpečnosť informácií	Implementácia SW nástroja na riadenie procesov	<p>Predmetom zákazky je zabezpečenie efektívnej správy dokumentácie BCM (Business Continuity Plan – plán kontinuity činnosti) vrátane BIA (Business</p>	

		Mlynské nivy 59/A 824 84 Bratislava		plánovania kontinuity činností (BCM)	Impact Analysis – analýza dopadov), DRP (Disaster Recovery Plan – havarijný plán) na všetky procesy spoločnosti Slovenská elektrizačná prenosová sústava, a.s., kde ako expert zabezpečujem práce implementácie SW nástroja pre riadenie kontinuity činností, plánovania a riadenia kontinuity činností (pre tvorbu analýz dopadov, disaster recovery; vývoj stratégií kontinuity; vypracovanie a implementácia plánov kontinuity; udržiavanie a vykonávanie plánov kontinuity) a zabezpečujem implementačné a konzultačné práce v oblasti riadenia bezpečnosti v súlade s normou STN ISO/IEC 27001.	
06/2015 – 12/2015	06/2015 – 12/2015	Ministerstvom zdravotníctva Slovenskej republiky Limbová 2 837 52 Bratislava	Expert pre bezpečnosť informácií	Elektronické služby zdravotníctva- ESO1	Predmetom zákazky bolo zrealizovať Národný zdravotný portál, ktorý zabezpečil centrálne poskytovanie informácií pre pacientov, zdravotníckych pracovníkov a ďalšie subjekty a posluží ako vstupná brána pre národné eHealth aplikácie. V rámci zákazky bol vytvorený systém elektronického objednávanie k lekárom, elektronickej preskripcie a elektronickej zdravotnej knihy, kde ako expert som zabezpečoval práce v oblasti riadenia bezpečnosti pri vývoji a nasadení komplexného informačného systému so zameraním na ochranu osobných údajov s implementáciou systému riadenia informačnej bezpečnosti v súlade s normou STN ISO/IEC 27001 a implementáciou bezpečnostných opatrení v oblasti infraštruktúry informačného systému. Projekt bol v súlade s požiadavkami zákonom č. 275/2006 Z. z. o informačných systémoch vo verejnej správe a o zmene a doplnení niektorých zákonov a s	

					nimi súvisiacimi vykonávajúcim právnymi predpismi,)	
08/2023 – 12/2023	08/2023 – 12/2023	Ministerstvom zdravotníctva Slovenskej republiky Limbová 2 837 52 Bratislava	Expert pre bezpečnosť informácií	Projekt Kybernetická bezpečnosť	Vypracovanie analýzy rizík a stratégie za rezort zdravotníctva a vypracovanie analýzy rizík, stratégie, riadiacej dokumentácie a smerníc v súlade s požiadavkami zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a v súlade s požiadavkami zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov	<div></div>

Certifikáty:

Rok	Certifikáty:
2007	Certifikát CISSP - Certified Information Systems Security Professional
2008	Certifikát CISA - Certified Information Systems Auditor
2008	Certifikát CISM - Certified Information Security Manager
2017	Interný audítor ISMS podľa ISO/IEC 27001:2013 a ISO 19011:2011
2017	Manažér systému informačnej bezpečnosti podľa ISO/IEC 27001:2013
2018	Interný audítor pre interné audity systému manažérstva služieb podľa normy STN/IEC 20000-1:2014
2018	Certifikát CBCP – Certified Business Continuity Professional



Týmto vyjadrujem svoj súhlas so správou, spracovaním a uchovaním osobných údajov v súlade s nariadením č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a zákonom č.18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov na účely podania ponuky na predmet zákazky: „Služby podpory, prevádzky, údržby a rozvoja Integrovaného systému úradov verejného zdravotníctva.“, verejného obstarávateľa: Úrad verejného zdravotníctva Slovenskej republiky, (ďalej len „zákazka“).

Vyhlasujem, že všetky uvedené informácie sú pravdivé a v prípade realizácie zákazky budem k dispozícii pri plnení zákazky.

V Bratislave dňa: 4. marca 2024

