Řízení letového provozu České republiky

SRPI R/11178/2024

Odpovědi na dotazy č.1 obdržené v rámci lhůty pro podání nabídek – VZMR „Analýza kybernetických rizik ERP systému v prostředí Dynamics 365 - II“

Přesné znění dotazu č.1:

„Ve vztahu k realizaci předmětu plnění zakázky týkající se provedení Analýzy kybernetických rizik ERP systému v prostředí Dynamics 365 je po zájemci požadováno, aby byl certifikován dle ISO 27001, a to i když se předmět zakázky týká kybernetické bezpečnosti dle platné národní legislativy (především ***zákon č. 181/2014 Sb.****, o kybernetické bezpečnosti /ZoKB/ a jeho prováděcí* ***vyhlášky č. 82/2018 Sb.*** */VoKB/, v platných zněních) a dle plánované* ***novely národní legislativy ve spojení s transponovanou evropskou bezpečnostní směrnicí NIS2****?* V souladu s § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, kdy Zadavatel při postupu podle tohoto zákona musí dodržovat zásady transparentnosti a přiměřenosti a ve vztahu k dodavatelům musí dodržovat zásadu rovného zacházení a zákazu diskriminace.
Trvá Zadavatel na této certifikaci?“

Odpověď na dotaz č.1:

Důvodem tohoto požadavku je zajistit ochranu všech informací vyplývajících z analýzy rizik prostředí ERP v cloudu. Analýza rizik zahrnuje citlivé informace týkající se obchodních tajemství, osobních údajů a dalších kritických dat. ISO 27001 poskytuje nezbytný rámec pro řízení informační bezpečnosti, který zahrnuje opatření na ochranu těchto citlivých informací před únikem, neoprávněným přístupem a jinými bezpečnostními hrozbami.

Certifikace podle ISO 27001 je důkazem toho, že Dodavatel má zavedeny a efektivně implementuje odpovídající bezpečnostní politiky a postupy. To nám dává jistotu, že citlivé informace budou náležitě chráněny a že Dodavatel splňuje mezinárodní standardy v oblasti informační bezpečnosti.

Ano, Zadavatel trvá na certifikaci 27001, která je nezbytná k zajištění nejvyšší úrovně ochrany dat Zadavatele a informací během a po provedení analýzy rizik.

Přesné znění dotazu č.2:

„V souladu s § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, kdy Zadavatel při postupu podle tohoto zákona musí dodržovat zásady transparentnosti a přiměřenosti a ve vztahu k dodavatelům musí dodržovat zásadu rovného zacházení a zákazu diskriminace.
a. Zadavatel požaduje kvalifikaci prokázat pouze prostřednictvím Certified Information Systems Security Professional (CISSP) nebo certifikaci Certified Information Security Manager (CISM) a není možné prokázat kvalifikaci ekvivalentními certifikáty od jiných certifikujících organizací? V případě že ano, jaké bude Zadavatel uznávat ekvivalentní certifikáty?
b. Zadavatel požaduje kvalifikaci prokázat pouze prostřednictvím Certifikace Microsoft Certified: Cybersecurity Architect Expert a není možné prokázat kvalifikaci ekvivalentními certifikáty od jiných certifikujících organizací? V případě že ano, jaké bude Zadavatel uznávat ekvivalentní certifikáty?“

Odpověď na dotaz č.2:

Zadavatel považuje za nezbytně nutný předpoklad pro plnění předmětu prokázání požadovaných certifikací ad a) CISSP nebo CISM, ad b) Certifikace Microsoft Certified: Cybersecurity Architect Expert.
Zadavatel nepřipouští jiné certifikace.

Přesné znění dotazu č.3:

„Jaký je výčet možných zjištěných vad díla dle čl. 8 dokumentu Smlouva – Záruka a odpovědnost za vady, na které se záruka a odpovědnost vztahuje?“

Odpověď na dotaz č.3:

V možnostech Zadavatele není uvést taxativní výčet možných vad, které by mohly v budoucnu na díle nastat, a na které se tedy záruka vztahuje. Záruka a odpovědnost za vady je tedy ve smlouvě formulována obecně s tím, že není-li ve smlouvě uvedeno jinak, řídí se odpovědnost za vady ust. § 2615 ve spojení s ust. § 2099 a násl. občanského zákoníku.

Přesné znění dotazu č.4:

„Zadavatel (Řízení letového provozu České republiky, s.p.) bude pravděpodobně zařazen jako „poskytovatel regulované služby v režimu vyšších povinností“) a bude muset splnit požadavky na dodržení souladu s platnými standardy a legislativou ČR.
ZoKB není obecným doporučením, ale závazným předpisem, který organizaci zajišťující životně důležité služby pro chod státu ukládá, jak mají příslušná aktiva chránit (tj. jaká má být jejich minimální ochrana) a tím zajistit základní funkce státu jak v oblasti kritické infrastruktury, tak i v případě významných systémů a poskytovaných významných služeb. Pokud se Zadavatel musí řídit ZoKB, má zákon přednost před uvedenými ISO normami a struktura dokumentace se musí přizpůsobit zákonnému předpisu. Normy v našem právním systému jsou nezávazné a závaznými se stávají až požadavkem uvedeným v zákonné, případně podzákonné normě.
Zadavatel požaduje provedení důkladné kybernetické analýzy rizik v prostředí Dynamics 365 v souladu s požadavky technických norem ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017 a ISO/IEC 270018 a nepožaduje dodržení souladu s platnou národní legislativou ke kybernetické bezpečnosti (ZoKB a VoKB) a dodržení souladu s plánovanou novelou národní legislativy ve spojení s transponovanou evropskou bezpečnostní směrnicí NIS2, které jsou pro systémy KII a VIS v současnosti povinné.
Trvá Zadavatel na daných požadavcích, případně je upraví?“

Odpověď na dotaz č.4:

Zadavatel trvá na stanovených požadavcích (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017, ISO/IEC 27018). Cílem Zadavatele je zajištění komplexního přístupu k analýze rizik, který bude plně v souladu jak s ISO normami, tak s národními právními předpisy. Díky požadavku Zadavatele bude zajištěno, že všechna rizika budou řádně identifikována a řízena v souladu s mezinárodně uznávanými postupy a zároveň Dodavatel bude plně dodržovat legislativní požadavky České republiky. Ve smlouvě tedy výslovně není uveden požadavek na dodržení souladu s platnou národní legislativou, nicméně s ohledem na její závaznost, je Zadavatelem tento soulad předpokládán.

Přesné znění dotazu č.5:

„Zadavatel ve výčtu Požadovaných služeb a dokumentů uvedených v Příloze č. 1 Smlouvy nemá uveden jeden ze základních dokumentů kybernetické bezpečnosti Analýza dopadů BIA (Business Impact Analysis), jehož cílem je identifikovat klíčové business systémy, služby, procesy a aktiva a následně zhodnotit jejich dopad na business Zadavatel.
Trvá Zadavatel na tom, že dané dokument nebude požadovat?“

Odpověď na dotaz č.5:

Dle požadavku Zadavatele na soulad s mezinárodními standardy a národní legislativou se předpokládá, že BIA je klíčovou součástí komplexního procesu analýzy rizik, který je Zadavatelem požadován. Bez BIA není možné hodnotit dopady, prioritizovat rizika, rozhodovat a mitigaci rizik, a navrhovat strategii BCP (Business Continuity Planning). Zadavatel požaduje zpracování dokumentu BIA v rámci zpracování Risk Analýzy.

Přesné znění dotazu č.6:

„Zadavatel v požadavcích na dodržení souladu s platnými standardy a legislativou ČR se odkazuje na neplatná legislativu (zákon č. 101/2000 Sb., o ochraně osobních údajů, zákon č. 227/2000 Sb., o elektronickém podpisu).“

Odpověď na dotaz č.6:

Zadavatel následujícím upravuje formální nedostatek. Tímto Zadavatel upravuje přílohu č. 1 Smlouvy, konkrétně začátek kapitoly „Další požadavky na dodržení souladu s platnými standardy a legislativou ČR“.

Původní znění:

- *Obecné nařízení o ochraně osobních údajů (GDPR):*

GDPR stanovuje přísné požadavky na ochranu osobních údajů občanů EU, včetně jejich sběru, zpracování a uchování. To zahrnuje i služby SaaS, které zpracovávají osobní údaje.
Zákon o ochraně osobních údajů (Zákon č. 101/2000 Sb.): Český zákon o ochraně osobních údajů dodržuje principy GDPR a poskytuje dodatečné ustanovení pro ochranu osobních údajů v České republice.

- *Zákon o elektronickém podpisu (Zákon č. 297/2016 Sb.):*

Poskytuje rámec pro používání elektronických podpisů a elektronické identifikace, což může být důležité pro zajištění autenticity a integrity dat v prostředí SaaS.

- *Zákon o kybernetické bezpečnosti (Zákon č. 181/2014 Sb.):*

Zákon stanovuje povinnosti pro poskytovatele služeb a organizace v oblasti kybernetické bezpečnosti, což může zahrnovat i ochranu dat a služeb poskytovaných prostřednictvím SaaS.

Nové znění:

- Obecné nařízení o ochraně osobních údajů (GDPR):

GDPR stanovuje přísné požadavky na ochranu osobních údajů občanů EU, včetně jejich sběru, zpracování a uchování. To zahrnuje i služby SaaS, které zpracovávají osobní údaje.

- Zákon č. 110/2019 Sb., o zpracování osobních údajů:

V České republice upravuje konkrétní aspekty ochrany osobních údajů, které nejsou přímo řešeny Obecným nařízením o ochraně osobních údajů (GDPR), nebo které GDPR přenechává na národní legislativě.

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce:

V České republice upravuje právní rámec pro poskytování služeb vytvářejících důvěru v oblasti elektronických transakcí.

- Zákon o kybernetické bezpečnosti (Zákon č. 181/2014 Sb.):

Zákon stanovuje povinnosti pro poskytovatele služeb a organizace v oblasti kybernetické bezpečnosti, což může zahrnovat i ochranu dat a služeb poskytovaných prostřednictvím SaaS.

Následující části kapitoly se nemění. Aktuální znění přílohy č.1 smlouvy viz dokument označený Příloha č 1 smlouvy V2.

Přesné znění dotazu č.7:

„Zadavatel požaduje, aby byl kladen důraz na soulad s platnou legislativou a standardy v České republice týkající se ochrany dat, např. obchodní tajemství, osobních údajů a zákonů vztahujících se k ERP podniku, avšak nepožaduje prokázání znalosti/dovednosti v oblasti ochrany osobních údajů ani právní vzdělání.
Trvá Zadavatel na tom, že dané znalosti/dovednosti nebude požadovat?“

Odpověď na dotaz č.7:

Standardy ISO 27000 a legislativa v podobě ZoKB a VoKB poskytují robustní rámec pro ochranu citlivých informací, včetně obchodních tajemství, osobních údajů a dat obsažených v ERP systémech. Tyto standardy a předpisy se vzájemně doplňují a poskytují komplexní přístup k ochraně dat v souladu s nejlepšími mezinárodními a národními praktikami.
Zadavatel stanovil veškeré předpoklady/ požadavky v souladu s požadovaným předmětem plnění.

V rámci nabídky bude součástí smlouvy Příloha č 1 smlouvy V2.

Jan Prokopec
Digitálně podepsal Jan Prokopec
Datum: 2024.08.29 09:03:52 +02'00'

Ing. Jan Prokopec

vedoucí oddělení přípravy a realizace investic

Řízení letového provozu
České republiky, státní podnik
Navigační 787, 252 61 Jeneč
Česká republika
E info@rlp.cz / www.rlp.cz

IČO: 49710371, DIČ: CZ699004742
Registrováno Městským soudem v Praze
oddíl A, vložka 10771
Bankovní spojení: ČSOB Praha 5, č.ú. 88153/0300
Držitel certifikátu kvality ISO 9001, ISO 14001