Rozšíření technologií pro komunikaci s občany

**1.1 Předmět zadání**

Dodavatel zajistí návrh, realizaci a nasazení systému automatizované informační podpory pro komunikaci s občany poskytované jako služba „Software as a Service“ (dále jen „SaaS“) včetně provedení analýz, vytvoření harmonogramu realizace, školení a projektového řízení.

**1.2 Výchozí stav**

Webová prezentace města Brna www.brno.cz poskytuje rozsáhlé množství informací určených pro občany, návštěvníky i podnikatele. Jednou z klíčových sekcí je „Potřebuji vyřídit“, která obsahuje informace k vyřizování životních situací na úřadě. Přestože je tato sekce pravidelně aktualizována a strukturována podle témat, někteří uživatelé mají potíže s orientací v jejím obsahu. Často se jim nedaří rychle a efektivně nalézt požadované informace, případně nejsou ochotni je samostatně vyhledávat.

Tato situace vede k tomu, že se občané obracejí na pracovníky úřadu telefonicky nebo e-mailem s dotazy, které by bylo možné zodpovědět prostřednictvím informací již dostupných na webu. To zatěžuje pracovníky úřadu a prodlužuje dobu vyřízení požadavků. Město Brno proto zvažuje zavedení automatizovaných řešení, která by uživatelům pomohla s vyhledáváním informací, zlepšila jejich orientaci na webu a snížila počet rutinních dotazů směřovaných na úřad.

**1.3 Základní popis a cíle**

Nabízená technologie musí poskytovat služby automatizovaného řešení na společném administračním rozhraní pro:

1. Chatbot
2. V budoucnu musí být řešení integrovatelné s Voicebotem (e-mail bot, aj. bot) nad stejným modelem pod stejným řízením a pravidly.

**1.4 Milníky a požadavky na harmonogram**

Je dodrženo rozdělení projektu na milníky a závislosti v rámci plnění, které jsou uvedené v následující tabulce.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Milník č. | Zahájení a závislosti | Popis Milníku | Lhůta splnění (ode dne účinnosti Smlouvy) | Platba % z ceny Díla |
| 1. | Účinností smlouvy | Projektový plán  Platforma pro automatizovanou komunikaci:   * Analýza a návrh technického řešení | do 30 dní |  |
| 2. | Zahájení podmíněno splněním a akceptací M1 | Platforma pro automatizovanou komunikaci:   * Implementace/nasazení do prostředí MMB.   Chatbot na brno.cz:   * Analýza a návrh technického řešení * Implementace Chatbota * Testovací prostředí * Produkční prostředí * Předání do Pilotního provozu | do 180 dní |  |
| 3. | Zahájení podmíněno splněním a akceptací M2 | Chatbota na brno.cz:   * Funkční testování se zapojením zaměstnanců MMB. * Bezpečnostní testování * Vyhodnocení Pilotního provozu a nastavení parametrů služeb * Školení | do 210 dní |  |
| 4. | Zahájení podmíněno splněním a akceptací M3 | Chatbot na brno.cz:   * Předání do Produkční provozu * Předání dokumentace. | do 224 dní |  |

**1.5 Technická specifikace platformy pro automatizovanou komunikaci a administrační rozhraní**

**1.5.1 Obecné a funkční požadavky**

Řešení bude sloužit jako obecný nástroj informační podpory veřejnosti, v souladu s platnou legislativou (zejm. zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů). Dále řešení musí být v souladu s platnou evropskou legislativou v oblasti umělé inteligence, zejména Nařízení Evropského Parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (dále jen “Akt AI”).

Jako takové proto musí splňovat následující požadavky:

1. Platforma pro správu botů musí být navržena jako otevřená a škálovatelná, umožňující budoucí rozšíření o další typy botů. Dodavatel je povinen při zpracování hlasového záznamu jakožto biometrického údaje zajistit odpovídající úroveň ochrany ve smyslu čl. 9 a čl. 32 GDPR, zejména s ohledem na možnost jeho zneužití.
2. Provozní prostředí musí být v souladu s požadavky „cloudových vyhlášek“ pro ISVS. Preferováno je řešení formou služby („SaaS“) provozované v cloudu dodavatele, který garantuje:
3. fyzické umístění dat v EU/EHP a že data nebudou přenášena mimo EU/EHP,
4. oddělený provoz modelů bez napojení na veřejné API (např. OpenAI).
5. Zvolený konkrétní jazykový model musí být vhodný pro využití ve veřejné správě.

1.5.2 Chatbot

1. Řešení musí být dostupné z webových stránek <https://www.brno.cz/> zadavatele bez sebemenších překážek a omezení v podobě nutnosti přihlášení nebo jakékoli identifikace uživatelů.
2. Řešení musí podporovat napojení na další komunikační kanály.
3. Umístění uživatelské části systému v cloudovém prostředí.
4. Řešení musí plně odpovídat pravidlům přístupnosti podle platných zákonů (zákona č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů) a obecně uznávaným standardům W3C, tj. WCAG (2.1).
5. Řešení musí u webových rozhraní sloužících interakci s uživatelem respektovat principy vstřícného UX/lll designu.
6. Řešení musí být provozováno jako plně automatizovaný robustní systém schopný uspokojit v režimu 24x7 (tj. při každodenním 24hodinovém provozu) jak předvídatelný, tak i mimořádný zájem uživatelů.
7. Řešení musí v maximální možné míře klást důraz na bezpečnost řešení včetně ochrany osobních údajů v intencích GDPR a souvisejících regulací, a tuto skutečnost doložit protokoly o realizaci příslušných testů, resp. uzavřením zpracovatelské smlouvy. Vývoj a nasazení řešení musí být v souladu se standardem OWASP Application Security Verification Standard verze minimálně 4.x, OWASP Top 10 a OWASP pro NLP/AI nástroje ([OWASP AI Security and Privacy Guide | OWASP Foundation](https://owasp.org/www-project-ai-security-and-privacy-guide/)).
8. Řešení netrpí základními zranitelnostmi, které je možné detekovat běžnými automatizovanými nástroji, zejména musí být odolné vůči známým prompt hacking a prompt injection útokům.
9. Řešení musí k samotnému provozu (SaaS) i zpracování dat využívat stabilní technologickou platformu nacházející se fyzicky na území Evropské unie (EU), resp. Evropského hospodářského prostoru (EHP). Osobní údaje, včetně metadat a síťových identifikátorů, nesmějí být přenášeny mimo EU/EHP a musí existovat záruky, že nebudou použity k jinému účelu.
10. Řešení musí být – v podobě výchozího komunikačního rozhraní – standardně integrovatelné do webového portálu zadavatele.
11. Řešení musí mít paralelní produkční a testovací prostředí (pro ad hoc i dávkové uživatelské testy), který umožní automatizovaný, auditovatelný a verzovaný přenos konfigurací z testovacího prostředí do produkčního prostředí bez nutnosti manuálních zásahů.
12. Řešení musí umožňovat do statických textových odpovědí Chatbota dynamicky načítat platnou hodnotu z externího zdroje (veřejně vystavených dat např. veřejné REST API ve formátu JSON).
13. Řešení musí poskytovat data pro provozní audit a reporting, a to jak prostřednictvím uživatelského rozhraní s možností zobrazení/vizualizace vč. generování škálovatelných sestav, tak pomocí exportu plných provozních logů pro příležitostné analýzy.
14. Řešení musí disponovat pro přípravu a aktualizaci dat znalostní báze takovým administračním rozhraním, které nevyžaduje zvláštní odborné znalosti nebo dovednosti (např. na úrovni programátora nebo počítačového lingvisty).
15. Řešení musí v případě nedostatečné jistoty při rozpoznávání významu dotazu (záměru) nabízet návrhy obsahově nejbližších témat/odpovědí do počtu 5 variant.
16. Řešení musí být pravidelně aktualizováno a chráněno proti známým zranitelnostem.
17. Chatbot bude provozován na webové stránce <https://www.brno.cz/>, případně dalších podstránkách, kde:
    1. Roční počet zobrazení: 5 426 416
    2. Roční návštěvnost: 2 032 446
    3. Nárazová denní návštěvnost: 8 706
18. Cílové skupiny uživatelů:
19. Občan – Poskytování informací o veřejných službách, administrativních procesech, úředních hodinách a dalších praktických záležitostech pro obyvatele města.
20. Podnikatel – Poskytování rychlých odpovědí na otázky týkající se podnikatelského prostředí, legislativy a dostupných dotačních programů.
21. Návštěvník města – Poskytování informací o turistických atrakcích, kulturních akcích, hromadné dopravě a dalších důležitých informacích pro pohodlný pobyt návštěvníků města Brna.
22. Chatbot musí disponovat:
    1. Vylepšenou schopností v oblasti pochopení přirozeného jazyka, aby mohl rozpoznávat a zpracovávat jazykové nuance, kontext a variace v dotazech uživatelů.
    2. Využitím pokročilých technik generování přirozeného jazyka pro tvorbu odpovědí nenalezených v předpřipravených konverzacích, které poskytují nejen relevantní informace, ale jsou také formulovány způsobem, který působí lidsky a přirozeně.
    3. Modely učení se s posilováním, které umožňují chatbotům učit se z interakcí s uživateli a neustále zlepšovat kvalitu a přesnost svých odpovědí s možností korekce administrátorem ze strany zadavatele pro zamezení nevhodných výstupů.
    4. Interaktivními a dynamickými odpověďmi – vytváření interaktivních odpovědí, které mohou zahrnovat průvodce krok za krokem, odkazy na další zdroje pro bohatší a užitečnější uživatelskou zkušenost.
    5. Kontextovým porozuměním – vývoj schopností Chatbota porozumět a zapamatovat si kontext konverzace, což umožňuje plynulý a koherentní dialog s uživatelem.
    6. Možností zapnutí a vypnutí režimu hodnocení konverzací, který zobrazí uživateli závěrečný formulář pro zpětnou vazbu (např. „Vyřešili jste svůj požadavek?“). Získaná data musí být využitelná pro vyhodnocení užitečnosti scénářů a zlepšování kvality odpovědí.
    7. Komunikační rozhraní chatbotů musí být vytvořeno s vizuálním vzhledem, který bude odpovídat vizuálnímu stylu webové nebo intranetové stránky, na kterou budou chatboty umístěny. GUI rozhraní musí zároveň umožňovat jednoduchou úpravu vzhledu. Chatbot bude mít podobu viditelného okna v pravém dolním rohu stránky.
23. Návrh, implementace a uvedení do provozu
    1. Služba Chatbot s umělou inteligencí tvořící odpovědi ze zadaných vstupních souborů a dat.
    2. Chatbot musí být schopen obsloužit minimálně 1000 dotazů denně a zároveň musí systém zvládnout obsluhu stovek uživatelů denně s možností více dotazů na jednoho uživatele.
    3. Systém musí být schopen dynamicky tvořit a načítat do textu odpovědí hodnoty ze zdrojových dat umístěných v prostředí webu <https://www.brno.cz/>, dále pak z adresářové struktury s uloženými strukturovanými i nestrukturovanými daty, taktéž s daty umístěnými v dané větvi stromu SharePoint a dalších externích zdrojích obdobného typu nevyžadujících autentizaci s možností definic podmínek hloubky stromu a to jak na webech, tak v adresářových strukturách, a to až na úroveň jednoho konkrétního odkazu (souboru).
    4. Součástí implementace je i migrace a adaptace znalostní báze otázek (životní situace) a odpovědí stávajícího systému chatbot, jakožto jednoho ze zdrojů dat.
    5. Návrh a vytvoření úvodního stromu komunikace s občany, podnikateli, návštěvníky.
    6. Komunikované informace budou podávány lidsky a přirozeně, využitím běžného konverzačního jazyka, tak aby jim rozuměl běžný občan. Informace, které bude chatbot poskytovat, se budou týkat pouze vybraných témat souvisejících s nabízenými službami města Brna.
    7. Součástí dodávky služby musí být i možnost monitoringu systémem vytvořených odpovědí a technologie musí umožnit jejich dočasnou či trvalou korekci.
    8. Nabízená technologie musí být schopna identifikovat změny obsahu zdrojových dat a s tím související úpravy generování odpovědí.
    9. Nabízená technologie musí blokovat vkládání a nesmí ukládat a ani zpracovávat osobní údaje občanů, podnikatelů, návštěvníků spadající pod GDPR.
24. Zajištění podpory provozu s definovaným objemem provozu, úrovní pokrytí služby a její garantovanou dostupností.
    1. Požadovaný objem provozu:
       * Prům. počet dotazů za měsíc: 30 000
       * Prům. počet dotazů za den: 1 000
    2. Garantovaná dostupnost služby: 99%
    3. Požadovaná technická podpora: 8H/5D

1.5.3 Administrační rozhraní

Uživatelsky přívětivé rozhraní pro různě zaměřené členy týmu zadavatele související s provozem systému, ideálně v podobě webové aplikace.

Tým zadavatele bude zajišťovat:

1. Příprava a aktualizace obsahu – požadujeme funkcionality formátování textu (zvýraznění, zalomení, jednoduchá tabulka), vkládání URL odkazů, editovatelnost/aktualizovatelnost všech údajů (s operativním promítnutím do produkce), ruční doplnění konkrétních klíčových slov či spojení a jejich validace.
2. Testování nových dat – využívající paralelní (testovací) instanci systému. Musí být zajištěna možnost testování obsahu před jeho zveřejněním v produkčním prostředí.
3. Nasazení na produkční prostředí – členové týmu zadavatele musí být schopni provést nasazení do produkce bez asistence dodavatele.
4. Sledování provozních metrik a vyhodnocování úspěšnosti odpovědí (stromová struktura i umělá inteligence) – umožňovat variabilní pohled na data (zobrazit, vizualizovat volitelné přehledy) s možností exportovat v editovatelném (např. CSV) i tiskovém formátu pravidelné reporty za zvolené období. Možné pohledy/exporty:
   1. Sumární statistiky za dané časové období.
   2. Historie uskutečněných konverzací.
   3. Nezodpovězené dotazy (očištěné od nerelevantních údajů – vulgarity, nesmysly, aj).
   4. Nejčastější témata, klíčová slova – možnost řazení.
   5. Procento zodpovězených dotazů.
   6. Srovnání v čase (prezentované grafem) – z důvodu sledování exponovaných období (volby, dotace, aj.).
5. Obdobné kroky v případě dalších technologií umožňující komunikaci s občany (voicebot, e-mailbot, …).

1.5.4.Požadavky na podporu NLP/NLU

1. Využití pokročilých nástrojů a technik z oblasti NLP/NLU se předpokládá v těchto třech oblastech:
2. Definování významu (automatické doplňování synonym, slovnědruhových variant a parafrází).
3. Rozpoznávání významu (s využitím vektorových prostorů / „embeddingů“, předtrénovaných jazykových modelů apod.).
4. Optimalizace znalostní báze (hlídání tematických překryvů při doplňování nových otázek a témat, správa ručně definovaných klíčových slov a spojení).
5. Integrace automatických a předpočítaných komponent či postupů nesmí znemožňovat uživatelské definování klíčových slov a frází (odborné terminologie) s vyšší váhou významnosti.
6. Zcela nezbytná je podpora češtiny, angličtiny, v případě mezijazykové homonymie mají prioritu nástroje s českou lokalizací (možnost psaní s diakritikou i bez ní, kontrola překlepů (pravopisu) / spellchecking, lemmatizace/generování apod.).
7. U integrace konkrétních jazykových modelů (natrénovaných tzv. hlubokým učením) jsou rozhodující výsledky, které dávají pro češtinu.
8. Svým designem je chatbot nástrojem pro automatické zodpovídání dotazů veřejnosti, nikoli skutečným konverzačním automatem, není proto cílem vytvářet a rozvíjet jeho identitu nebo schopnosti reagovat na obecná témata (mít své jméno, vědět, kolik je hodin atp.).

**1.5.5 Činnosti zajišťované dodavatelem**

1. Koordinace prací a projektové řízení pro včasné splnění všech lhůt a výstupů. Vedení schůzek a pořizování zápisů zajišťuje dodavatel.
2. Tvorbu a aktualizaci projektového plánu a harmonogramu projektu.
3. Technickou a funkční analýzu, návrh řešení, nasazení a testování.
4. Kompletaci, udržování a organizaci dokumentace. Veškerá dokumentace je v češtině nebo angličtině.
5. Zajištění infrastruktury a přípravu prostředí v infrastruktuře, správu a konfiguraci infrastruktury.
6. Školení a dokumentaci pro administrátory a správce obsahu (max 10 osob).

**1.5.6 Činnosti zajišťované zadavatelem**

1. Součinnost zaměstnanců při přípravě infrastruktury a při přípravě prostředí služby.
2. Projektové řízení a koordinaci osob na straně zadavatele, zajištění součinnosti při realizaci projektu.