Dílčí smlouva č. 2024/11264 o poskytnutí služeb

k Rámcové dohodě o poskytování služeb - Audit kybernetické bezpečnosti IS ČP č. 2023/09505 ze dne 6.12.2023

Česká pošta, s.p.

se sídlem:	Politických vězňů 909/4, 225 99, Praha 1
IČO:	47114983
DIČ:	CZ47114983
zastoupen:	Ing. Martinem Götzem, ředitelem úseku ICT a eGovernment
zapsán v obchodním rejstříku u:	Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení:	[redacted]

dále jen „**Objednatel**“

a

KPMG Česká republika, s.r.o.

se sídlem:	Pobřežní 648/1a, 186 00 PRAHA 8
IČO:	00553115
DIČ:	CZ699001996
zastoupena:	Mgr. Evou Bláhovou, prokuristou se samostatnou prokurou
zapsána v obchodním rejstříku u:	Městského soudu v Praze, oddíl C, vložka 326
bankovní spojení:	[redacted]

dále jen „**Dodavatel**“

dále jednotlivě jako „**Smluvní strana**“, nebo společně jako „**Smluvní strany**“

uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), tuto Dílčí smlouvu o poskytnutí služeb (dále jen „**Smlouva**“) k **Rámcové dohodě o poskytování služeb - Audit kybernetické bezpečnosti IS ČP č. 2023/09505** ze dne 6.12.2023 (dále jen „**Rámcová dohoda**“).

Preambule

Objednatel provedl v souladu s Rámcovou dohodou soutěž o dílčí veřejnou zakázku „Penetrační testy interní aplikace Chatbot“ (dále jen „**minitendr**“). Tato Smlouva je uzavřena s Dodavatelem na základě výsledku minitendru.

1. Předmět Smlouvy a podmínky plnění

1.1. Předmětem této Smlouvy je závazek Dodavatele poskytnout Objednateli řádně a včas služby zahrnující penetrační testování aplikace Chatbot v rámci informačního systému ČP (dále jen „**Plnění**“). Bližší specifikace a požadavky na Plnění, které je Dodavatel Objednateli povinen poskytnout, je obsažena v příloze č. 1 této Smlouvy.

2. Cena

2.1. Maximální cena Plnění činí 96.600,- Kč (slovy: devadesát šest tisíc šest set korun českých) bez DPH. Rozklad ceny je uveden v příloze č. 1 Smlouvy.

2.2. Cena zahrnuje veškeré náklady Dodavatele spojené s plněním Dílčí smlouvy a poskytnutím plnění Objednateli. Tato cena je cenou konečnou, nejvýše přípustnou a nemůže být zvýšena bez předchozího písemného souhlasu Objednatele.

3. Práva a povinnosti Smluvních stran

3.1. Seznam osob, jejichž prostřednictvím bude Dodavatel zajišťovat plnění této Smlouvy, je uveden v Příloze č. 2 Smlouvy (dále jen „**realizační tým**“). Bude-li z důvodů vzniklých na straně Dodavatele nutné nahradit kteréhokoliv člena realizačního týmu, bude po předchozím odsouhlasení Objednatelem nahrazen novým členem týmu s odpovídající nebo vyšší kvalifikací, než která byla požadována v Zadáacím řízení, a to do 2 týdnů od oznámení důvodů pro nahrazení Objednateli.

4. Doba a místo plnění

4.1. Dodavatel se zavazuje poskytnout část Plnění dle kapitoly 6 Přílohy č. 1 Smlouvy – „Návrh penetračních testů“ do 30 dnů ode dne nabytí účinnosti Smlouvy a v tomto termínu rovněž zahájit část Plnění dle kapitoly 6 Přílohy č. 1 Smlouvy – „Provedení penetračních testů“. Poskytování Plnění dle této Smlouvy bude zahájeno bez zbytečného odkladu po nabytí její účinnosti.

4.2. Místem poskytování Plnění je Olšanská 9, Praha 3.

5. Bezpečnost ICT

5.1. Objednatel zastává pozici Povinné osoby ve smyslu zák. č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“) a je Provozovatelem kritické informační infrastruktury (dále jen „KII“), jejíž subsystém je předmětem auditu. Dodavatel bere na vědomí, že plnění Dodavatele dle Smlouvy se považuje za plnění významného dodavatele v souladu s § 2 písm. n) Vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB“), a že jej Objednatel eviduje jako významného

dodavatele v souladu s § 8 odst. 1 písm. b) VKB. Dodavatel prohlašuje, že byl seznámen s Pravidly pro Dodavatele v rozsahu a míře k předmětu plnění a bude dodržovat podmínky pro významné dodavatele, které jsou Přílohou č. 3 Smlouvy.

6. Závěrečná ustanovení

6.1. Tato Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv. Případné plnění předmětu této Smlouvy v době od okamžiku platnosti Smlouvy do okamžiku nabytí její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.

6.2. Smluvní strany jsou oprávněny od Smlouvy odstoupit ze stejných důvodů a za stejných podmínek, jaké platí pro odstoupení od Rámcové dohody.

6.3. V otázkách touto Smlouvou neupravených se použijí ustanovení Rámcové dohody.

6.4. Kontaktní osoby Smluvních stran pro účely plnění této jsou následující:

Kontaktní osoba Objednatele: [redacted]

Kontaktní osoba Dodavatele: [redacted]

6.5. Tato Smlouva je vyhotovena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál opatřený platnými elektronickými podpisy.

6.6. Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace Plnění a Cena

Příloha č. 2 – Složení poradenského týmu Dodavatele

Příloha č. 3 – Pravidla pro Dodavatele

6.7. Smluvní strany prohlašují, že tato Smlouva vyjadřuje jejich úplné a výlučné vzájemné ujednání týkající se daného předmětu této Smlouvy. Smluvní strany po přečtení této Smlouvy prohlašují, že byla uzavřena po vzájemném projednání, určitě a srozumitelně, na základě jejich pravé, vážně míněné a svobodné vůle. Na důkaz uvedených skutečností připojují podpisy svých oprávněných osob či zástupců.

V Praze	V Praze
Ing. Martin Götz ředitel úseku ICT a eGovernment **Česká pošta, s.p.**	Mgr. Eva Bláhová prokurista se samostatnou prokurou **KPMG Česká republika, s.r.o.**

Příloha č. 1 – Specifikace Plnění a Cena

[redacted]

1. Popis aplikace

[redacted]

[redacted]

[redacted]

[redacted]

2. Bezpečnostní opatření

[redacted]

3. Zranitelnosti a opravy

[redacted]

4. Přístupová práva a zabezpečení dat

[redacted]

[redacted]

5. Externí integrace a služby třetích stran

[redacted]

[redacted]

6. Výstupy

1) Návrh penetračních testů - libovolná struktura (včetně harmonogramu jejich realizace společně s ostatními výstupy)
2) Provedení penetračních testů
3) Detailní závěrečná zpráva s jednotlivými zjištěními či nálezy
4) Workshop pro prezentaci závěrečné zprávy, který zajistí:
    a. že zjištění budou správně pochopena dobře vyložena a vyargumentována,
    b. jejich příčiny budou podrobně vysvětleny
    c. konzultaci s vývojáři ČP v rozsahu 4 hod.
5) Retest penetračních testů –provedení jednoho retestu. Objednatel je oprávněn vyzvat Dodavatele k provedení dalšího retestu. Cena Plnění bude uhrazena dle skutečného počtu provedených retestů.

Cena:

Sazba (cena) za 1 člověkoden (MD)* v Kč bez DPH	13 800,00
Počet člověkodní za návrh a provedení penetračních testů	4
Počet člověkodní za provedení jednoho (1) retestu penetračních testů	1,5
Maximální celkový počet člověkodní alokovaných pro předmět plnění této Smlouvy**	7
Maximální celková cena za Plnění v Kč bez DPH	**96 600,00**

*Jedním člověkodnem (MD) se rozumí 8 hodin výkonu práce jednoho pracovníka Dodavatele pro Objednatele.

**Do maximálního počtu člověkodní alokovaných pro předmět plnění této Smlouvy je zahrnuto provedení dvou (2) retest penetračních testů. Cena bude hrazena dle skutečně provedených retestů

Příloha č. 2 – Složení poradenského týmu Dodavatele

Realizační tým Dodavatele bude složen z následujících členů:

role (pozice) v realizačním týmu	jméno a příjmení
Manager projektu	[redacted]
Konzultant	[redacted]
Auditor	[redacted]

Příloha č. 3: Pravidla pro dodavatele

1. Pravidla pro zabezpečení informací

1.1. Základní ustanovení

• Veškeré informace, které jsou v rámci smluvního vztahu Dodavateli poskytovány ze strany Objednatele nebo vzniknou během plnění smluvních činností, jsou informačním aktivem Objednatele (dále jen informace Objednatele), které je třeba chránit z pohledu bezpečnosti informací.

• Dodavatel se řídí obecně závaznými právními předpisy.

• Dodavatel musí informovat Objednatele o významných změnách týkajících se ovládání dodavatele podle zákona o obchodních korporacích, o změnách týkajících se vlastnictví či práva nakládání se zásadními aktivy Dodavatele, zejména pokud mohou mít dopad na plnění smluvních závazků vůči Objednateli.

1.2. Řízení rizika, změnové řízení.

• Dodavatel musí mít nastaven proces řízení rizik.

• Dodavatel je povinen informovat Objednatele o jakémkoli vzniklém riziku či hrozícím riziku, které by mohlo mít dopad na bezpečnost informací Objednatele. Dodavatel je dále povinen přijmout vhodná opatření k odstraňování takových rizik a informovat Objednatele o přijatých opatřeních a stavu jejich realizace.

1.3. Kontrola a audit Dodavatele

• Objednatel je oprávněn provést u Dodavatele a jeho případných poddodavatelů kontrolu plnění povinností týkajících se bezpečnosti informací. Dodavatel je povinen Objednateli takovou kontrolu umožnit do 10 dnů od nahlášení. Kontrola může zahrnovat přezkoumávání dokumentace, implementaci bezpečnostních opatření a kontrolu prostor, v kterých jsou prováděny činnosti, které mohou mít vliv na bezpečnost informací Objednatele. Dodavatel je povinen poskytnout součinnost pro provedení kontroly, zahrnující umožnění vstupu do požadovaných prostor (včetně prostor poddodavatelů), přístupu k příslušným dokumentům. Kontrola může být provedena zaměstnanci Objednatele nebo prostřednictvím další strany pověřené Objednatelem.

• Dodavatel je povinen udržovat aktuální dokumentaci všech opatření přijatých pro zajištění bezpečnosti informací Objednatele a poskytnout tuto dokumentaci osobám pověřeným Objednatelem v rámci kontroly plnění povinností Dodavatele.

1.4. Systém řízení bezpečnosti informací

• Dodavatel musí nakládat s informacemi Objednatele dle jejich klasifikace. Klasifikaci primárně určuje Objednatel. V případě, že data nejsou označena, má se za to, že se jedná o interní informace

Objednatele. Žádné informace, vyjma veřejných, není možné předávat třetím stranám bez vědomí a souhlasu Objednatele.

- Dodavatel musí zajistit, aby přístup k informacím Objednatele měly pouze osoby, které tyto informace potřebují pro výkon smluvních činností (dle zásad need to know – „potřeba vědět“) a že informace budou použity pouze pro účely plnění smlouvy.

- Dodavatel jmenuje zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této Přílohy a pro potřeby související komunikace mezi Smluvními stranami ohledně tohoto tématu (dále také jen „Kontaktní osoba“). Kontaktní osoba na straně dodavatele je:

[redacted]

- V případě, že Dodavatel pro plnění smluvních závazků vůči Objednateli využívá služeb třetí strany (poddodavatele), musí zajistit, aby se tito zavázali plnit všechny relevantní bezpečnostní požadavky ve stejném rozsahu jako jsou smluvně stanoveny mezi Dodavatelem a Objednatelem.

- Dodavatel musí zajistit, aby zaměstnancům, či zaměstnancům třetích stran, kteří mohou mít přístup k informacím Objednatele, byl tento umožněn s ohledem na rizika spojená s důvěrností informací (klasifikačním stupněm), byli náležitě proškoleni a poučeni a aby mezi nimi a Dodavatelem byla uzavřena dohoda o mlčenlivosti.

1.5. Řízení přístupu

- Systémy a prvky systémů musí být nakonfigurovány takovým způsobem, aby umožňovaly přístup pouze autorizovaným uživatelům.

- • Dodavatel musí zajistit používání dostatečně silných hesel, jejichž tvorba a užití bude v souladu s VKB. a Hesla (včetně dalších autentizačních prostředků, jako jsou prvky vícefaktorové autentizace) budou dostatečně chráněna před zneužitím.

- Pro autentizaci musí být používány unikátní účty pro každého uživatele, které nesmí být sdíleny.

- Jestliže jakékoliv oprávnění k přístupu do systémů a k informacím Objednatele již není platné (například při změně pracovní pozice nebo při ukončení práce zaměstnance, případně zaměstnance třetí strany), je Dodavatel povinen bezodkladně o této skutečnosti informovat Objednatele a zajistit zrušení přístupových oprávnění.

- Dodavatel musí zajistit logování všech úspěšných i neúspěšných přístupů k systémům a informacím Objednatele. Do logů musí být zaznamenány informace umožňující jednoznačnou informaci toho, kdo přistoupil nebo se pokusil přistoupit k těmto informacím. Záznamy musí být vyhodnocovány za účelem odhalení případného neoprávněného přístupu a musí být ukládány minimálně po dobu vyžadovanou VKB.

1.6. Bezpečnost informací a jejich předávání.

- Dodavatel musí zajistit, že informace Objednatele, jako jsou dokumenty a data nebudou předávány prostřednictvím nezabezpečených kanálů a ukládány na nezabezpečených úložištích. Informace nesmí být zejména: o ukládány na veřejných úložištích,
    - ukládány na soukromých zařízeních uživatelů (například princip BYOD),
    - ukládány na firemních zařízeních uživatelů, která nejsou zabezpečena šifrováním,
    - posílány prostřednictvím veřejné sítě bez zabezpečení (například bez pomoci VPN, TLS apod.),
    - posílány na emailové adresy uživatelů, které nejsou spravovány Dodavatelem anebo smluvní třetí stranou (např. freemailové služby, soukromý email zaměstnance apod.).

1.7. Fyzická bezpečnost a bezpečnost prostředí

- Dodavatel musí zajistit, aby do prostor, ve kterých jsou zpracovávány informace Objednatele, měly přístup pouze osoby, které jsou autorizovány k přístupu k těmto informacím.
- Prostředí, v kterém jsou umístěny informační systémy Objednatele, musí mít implementována opatření proti následkům vnějších vlivů, jako jsou například havárie, přírodní katastrofy nebo úmyslné poškození či zneužití.

1.8. Bezpečnost zařízení

- Dodavatel musí zajistit, aby na všech zařízeních byl používán pouze jím schválený legální software a přijmout opatření zamezující instalaci neschváleného softwaru uživateli.
- Dodavatel musí zajistit, aby na všech zařízeních, na kterých jsou zpracovávány informace Objednatele, probíhalo pravidelné přezkoumání zranitelností a včasná instalace oprav a bezpečnostních zásad.
- Na všech počítačích Dodavatele musí být provozována softwarová ochrana před škodlivým kódem, která je pravidelně aktualizována. Tato musí být nastavena tak, aby nemohla být vypnuta uživatelem.

1.9. Řízení bezpečnostních incidentů

- Dodavatel je povinen stanovit a dodržovat procesy pro řízení bezpečnostních událostí a incidentů a jmenovat role zodpovědné za tyto procesy.
- Dodavatel musí Objednateli bezodkladně po jejich detekci oznámit bezpečnostní události a incidenty, i ve stádiu podezření, prostřednictvím sjednaných ohlašovacích kanálů.
- Při řešení bezpečnostního incidentu je dodavatel povinen:
  - poskytnout veškerou potřebnou součinnost týmům Objednatele;
  - použít otestovaný postup zahrnující požadavky na zajištění důkazů;
  - navrhnout, implementovat a dokumentovat opatření, která zajistí minimalizaci dopadu incidentu na aktiva Objednatele;
  - provést analýzu příčin a navrhnout a implementovat opatření s cílem zamezit opakování incidentu.

1.10. Zálohování dat a jejich likvidace

- Dodavatel musí zajistit, aby na zálohované informace Objednatele byla aplikována minimálně stejná bezpečnostní opatření jako na data v provozním prostředí.
- V případě, že Dodavatel již nepotřebuje informace Objednatele k plnění smluvních závazků, anebo informace Objednatele nejsou součástí jejich plnění, je Dodavatel povinen zajistit bezpečnou likvidaci informací.