PROVÁDĚCÍ SMLOUVA
OUTSOURCING PROFESIONÁLNÍCH ODBORNÝCH SLUŽEB ICT (OPOS)
ČÁST BEZPEČNOST INFORMACÍ

Smluvní strany:

Česká republika – Ministerstvo zemědělství

se sídlem: Těšnov 65/17, 110 000 Praha 1 – Nové Město

IČ: 00020478

bankovní spojení: Česká národní banka, číslo účtu: 6015-1226001/0710

zastoupená: David Šetina,

ředitel Odboru správy centrálních informačních systémů a kybernetické bezpečnosti

(dále jen „**Objednatel**")

číslo smlouvy DMS: ~~*165-2015-133310*~~ 734-2015-13310, *číslo smlouvy Objednatele:* ~~S2015-0021~~ S2015-0092

opraveno dne: 6.11. 2015

a

BDO IT, a.s.

se sídlem: Olbrachtova 1980/5, 140 00 Praha 4

IČ: 25056646, DIČ: CZ25056646

společnost zapsaná v obchodním rejstříku vedeném u Městského obchodního soudu v Praze,

oddíl B, vložka 4080

bank. spojení: Raiffeisenbank, a.s., č. účtu: 465434001/5500

zastoupená: Ing. Miloslav Rut, místopředseda představenstva

(dále jen „**Poskytovatel**")

číslo smlouvy Poskytovatele:

dnešního dne uzavřely tuto smlouvu v souladu s ustanoveními § 1746 odst. 2, § 2358 a násl. a § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „**občanský zákoník**") a § 92 odst. 1 písm. a) dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**ZVZ**")

(dále jen „**Prováděcí smlouva**").

1. ÚVODNÍ USTANOVENÍ

1.1 Tato Prováděcí smlouva se uzavírá jako prováděcí smlouva k rámcové smlouvě OUTSOURCING PROFESIONÁLNÍCH ODBORNÝCH SLUŽEB ICT uzavřené Objednatelem a Poskytovatelem dne 10. 6. 2015, číslo smlouvy Objednatele: S2015-0021, číslo sml. DMS 165-2015-13310 (dále jen "**Rámcová smlouva**").

1.2 Práva a povinnosti stran při poskytování plnění dle této Prováděcí smlouvy se řídí ustanoveními této Prováděcí smlouvy a ustanoveními Rámcové smlouvy.

1.3 Ustanovení Rámcové smlouvy mají v případě rozporu přednost před ustanoveními této Prováděcí smlouvy, ledaže by se jednalo o nepodstatnou změnu v podmínkách Rámcové smlouvy ve smyslu § 92 odst. 5 ZVZ.

2. PŘEDMĚT SMLOUVY

2.1 Poskytovatel se na základě této Prováděcí smlouvy zavazuje poskytnout Objednateli Služby uvedené v příloze č. 1 této Prováděcí smlouvy.

2.2 Objednatel se zavazuje zaplatit za řádně poskytnuté Služby cenu v souladu s podmínkami Rámcové smlouvy.

2.3 Celkový rozsah Služeb poskytovaných na základě této Prováděcí smlouvy nepřekročí 25 člověkodnů.

2.4 Poskytovateli uzavřením této Prováděcí smlouvy nevzniká právo na čerpání plnění v předpokládaném rozsahu stanoveném v příloze č. 1 Rámcové smlouvy.

3. DOBA A MÍSTO PLNĚNÍ

3.1 Místem plnění této Prováděcí smlouvy se sjednává: Těšnov 65/17, 110 000 Praha 1 – Nové Město, datová centra - Nagano: K Červenému dvoru 25/3156, 130 00 Praha 3 a Chodov: V lomech 2339/1, 149 00 Praha 4. Službu je též možné poskytovat v těchto lokalitách prostřednictvím vzdálené správy (např. pomocí VPN ze sídla poskytovatele).

3.2 Služby budou poskytovány v době stanovené v harmonogramu uvedeném v příloze č. 2 této Prováděcí smlouvy.

4. OSTATNÍ UJEDNÁNÍ

4.1 Objednatel je oprávněn pozastavit poskytování plnění dle této Prováděcí smlouvy svým jednostranným písemným oznámením doručeným Poskytovateli, a to bez jakýchkoliv sankcí. Pozastavení plnění se stává účinným sedmým dnem následujícím po doručení oznámení o pozastavení

plnění Poskytovateli. Právo Poskytovatele na úhradu ceny řádně poskytnutého plnění do doby pozastavení plnění tím není dotčeno.

5. TRVÁNÍ SMLOUVY

5.1 Tato Prováděcí smlouva nabývá účinnosti dnem doručení přijetí návrhu na její uzavření smluvní straně, která návrh na uzavření Prováděcí smlouvy učinila.

5.2 Tato Prováděcí smlouva se uzavírá na dobu určitou, a to do na dobu 3 měsíců ode dne nabytí její účinnosti.

5.3 Objednatel je oprávněn odstoupit od této Prováděcí smlouvy za podmínek uvedených v odst. 16.2 a 16.3 Rámcové smlouvy.

5.4 Poskytovatel je dále oprávněn od této Prováděcí smlouvy odstoupit za podmínek stanovených příslušnými právními předpisy.

5.5 Objednatel je oprávněn bez jakýchkoliv sankcí tuto Prováděcí smlouvu vypovědět bez udání důvodů, a to s měsíční výpovědní lhůtou, která začne běžet následujícím dnem po dni, kdy byla písemná výpověď doručena Poskytovateli.

6. ZÁVĚREČNÁ USTANOVENÍ

6.1 Poskytovatel je srozuměn s tím, že Objednatel je oprávněn zveřejnit Smlouvu na svých webových stránkách a dále je povinen uveřejnit dle § 147a odst. 1 písm. a) ZVZ na svém profilu, který se nachází na internetové adrese https://zakazky.eagri.cz/profile_display_2.html (dále jen „Profil"), tuto Smlouvu včetně všech jejích změn a dodatků. Dále je Poskytovatel srozuměn s tím, že dle § 147a odst. 1 písm. b) ZVZ je Objednatel povinen uveřejnit na Profilu výši skutečné uhrazené Ceny za plnění Veřejné zakázky a dle § 147a odst. 1 písm. c) ZVZ též seznam subdodavatelů Poskytovatele. Poskytovatel tímto uděluje souhlas Objednateli k uveřejnění všech podkladů, údajů a informací uvedených v tomto odstavci a těch, k jejichž uveřejnění vyplývá pro Objednatele povinnost dle právních předpisů.

6.2 Nedílnou součást této Prováděcí smlouvy tvoří tyto přílohy:

Příloha č. 1: Popis poskytovaných Služeb
Příloha č. 2: Harmonogram plnění

6.3 Tato Prováděcí smlouva je uzavřena ve čtyřech stejnopisech, z nichž každá strana obdrží po dvou stejnopisech.

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Objednatel	Poskytovatel
V Praze dne 05 -11- 2015	V Praze dne 2/11/2015
.....	.....
Česká republika – Ministerstvo zemědělství David Šetina, ředitel Odboru správy centrálních informačních systémů a kybernetické bezpečnosti	**BDO IT, a.s.** Ing. Miloslav Rut, místopředseda představenstva

Příloha č. 1

Popis poskytovaných Služeb

1. Služba č. 2 dle přílohy č.1 Rámcové smlouvy Outsorcing profesionálních služeb ICT (OPOS) část bezpečnost informací – vymezení předmětu plnění: Analytik bezpečnosti informací

Primárním předmětem této služby je zajištění odborných profesních služeb ICT dle konkrétních potřeb Objednatele v oblasti problematiky bezpečnosti informací IT pro Objednatele, příp. celý rezort Objednatele v souladu se závaznými standardy a principy Objednatele. Zejména se jedná o:

a) spolupráce na činnostech modelu PDCA při zavádění ISMS pro Objednatele i rezort Objednatele;

b) monitoring aktuálních standardů a technických a technologických řešení v oblasti předmětné činnosti a návrhy jejich aplikace do prostředí Objednatele;

c) návrhy testování bezpečnosti aplikací a systémů;

d) provádění kontrolní činnosti v oblasti bezpečnosti informací, identifikace rizik;

e) provádění analýz v oblasti bezpečnosti ICT a včetně návrhů nápravných opatření;

f) příprava technických podkladů pro provozní požadavky na bezpečnost informací;

g) pravidelné kontroly zavedených bezpečnostních opatření u poskytovaných služeb jednotlivými dodavateli;

h) pravidelné kontroly, zda nastavení bezpečnostních parametrů informačních systémů odpovídají předepsaným hodnotám;

i) provádění bezpečnostních a penetračních testů ICT;

j) provádění auditů IS z hlediska bezpečnosti informací;

k) bezpečnostní dohled provozu infrastruktury, sledování a vyhodnocování logů v systémech a dohledových nástrojích, vytváření reportů, monitoring, řešení a vyhodnocování bezpečnostních incidentů, následné návrhy nápravných opatření;

l) dohled nad bezpečným přístupem k IS a aplikacím;

m) tvorba a revize dokumentace bezpečnosti informací;

n) posuzování a připomínkování přípravné a realizační dokumentace projektů a provozní dokumentace z pohledu předmětné služby;

o) poskytování součinnosti v souladu s předmětnou službou při plánování, navrhování a řešení vývoje a změn agendových systémů a technologických řešení v souladu s předmětnou službou;

p) poskytování součinnosti, konzultací a informací dodavatelům ICT řešení v souladu s předmětnou službou v průběhu analýzy, návrhu řešení, realizace, akceptace a předávání do provozu;

q) poskytování vstupů do dokumentace veřejných zakázek, zejména požadavků vycházejících z předmětné služby a jejich souladu s platnou legislativou;

r) ukládání a správa dokumentace spojené s předmětnou činností v příslušné elektronické knihovně Objednatele;

s) řídit se platnou legislativou a vnitřními předpisy Objednatele a plnit odborné úkoly v oblasti předmětné služby Objednatelem.

Náplň Služby 2. Analytik bezpečnosti informací dle bodu i) provádění bezpečnostních a penetračních testů ICT:

Penetrační testy

Budou provedeny penetrační testy webu/portálu MZe „Jentodobré" po jeho migraci na technologii Liferay s cílem ověřit technologickou a konfigurační bezpečnost daného portálu a to s ohledem na:

- možné dlouhodobé nedostatky přetrvávající již z období před migrací na technologii Liferay
- možné nedostatky způsobené migrací na technologii Liferay.

Předmětem testů je ověření webu MZe „Jentodobré" a identifikace jeho případných závažných zranitelností, které by mohli vést k ohrožení požadovaných parametrů jeho provozu nebo k jeho neoprávněnému způsobu použití/zneužití. Spolu s identifikací zranitelností bude ověřena též jejich reálná zneužitelnost či možnost výskytu/uplatnění a vymezena hlavní účinná opatření k jejich eliminaci.

Penetrační testy budou typově primárně zaměřeny na techlogickou a systémově–aplikační infrastrukturu portálu a to jak z hlediska přístupu z vnějšího tak z interního prostředí MZe.

Penetrační testy budou zahrnovat:

- Provedení penetračních testů v rozsahu:
  - Externí penetrační test prostředí portálu „Jentodobré"
  - Interní penetrační test backend aplikací (portálu „Jentodobré")
  - Testy konfigurace serverů portálu „Jentodobré" v rozsahu 4 + 4 virtuání servery
  - Skenování známých zranitelností systému jako celku
- Provedení penetračních testů bude doplněno orientačním testem zdrojových kódů se zaměřením na formulář pro evidenci uživatelů
- Zpracování zprávy z penetračních testů
- Případný retest po odstranění identifikovaných slabin a nedostatků.

Výstup penetračních testů

- Výstupem penetračních testů bude zpráva z penetračních testů zahrnující:
- Manažerský souhrn hlavních zjištění a doporučení
- Základní informace o provedeném bezpečnostním testu (časový rámec, cíl a rozsah, použité postupy a techniky)
- Souhrnné informace k průběhu provedených testů s důrazem na faktory ovlivňující jejich průběh a výsledek
- Popis bezpečnostních slabin a specifikace doporučených protiopatření s důrazem na úroveň rizik jednotlivých slabin a prioritu doporučovaných opatření.

Dle výsledku testu a náročnosti mohou být penetrační testy v omezeném rozsahu doplněny přetestováním portálu „Jentodobré" po implementaci doporučených opatření.

Ochrana informací MZe a požadavky na součinnost

Potřebné informace budou zjišťovány formou konzultací s určenými pracovníky zadavatele a dodavatele s tím, že v případě potřeby budou též zpřístupněny vybrané nutné informace a dokumenty (např. uživatelská dokumentace, popisy architektury řešení, konfigurací a

nastavení použitých komponent, popisy komunikačních protokolů, apod.). Maximální zatížení zaměstnanců zadavatele nepřekročí 4 člověkodny.

Po dobu provádění penetračních testů budou zajištěny:

- Stabilita testovaných prostředí portálu „Jentodobré" (zejména z hlediska konfigurace, prvků a verzí systémového a aplikačního vybavení)
- Dostatečná exkluzivita k provedení testů v tom smyslu, že nebudou prováděny jiné aktivity, které by s testováním byly kolizní (např. zátěžové testy, rekonfigurace apod.).
- Případné potřebné přístupy, role a účty nutné k testování portálu „Jentodobré".

Testy budou prováděny takovým způsobem, aby byla minimalizována rizika jejich negativního dopadu na infrastrukturu a aplikace zadavatele, zejména:

- testy budou prováděny ve stanovených prostředích a ve stanoveném rozsahu
- testy budou probíhat v předem stanovených termínech
- automatizované nástroje (např. skenery zranitelností) budou nastaveny po dohodě s akceptovatelnou mírou intenzity skenování. Nebudou prováděny činnosti, které by mohly závažným způsobem negativně ovlivnit provozovanou internetovou/intranetovou infrastrukturu bez předešlého souhlasu pověřených pracovníků MZe ČR.

V případě zjištění závažné chyby může být prověření , po dohodě s MZe, provedeno do větší hloubky.

2. Způsob zadávání požadavků na služby

Výše uvedené činnosti bodu zadávány vždy prostřednictvím oprávněné osoby dle článku 11 rámcové smlouvy a to buď přímo, nebo potvrzením požadavku jiné osoby s odkazem na plnění dle této smlouvy.

Předmětem plnění pro výše uvedené služby může být:

i. požadavek v HelpDesk systému MZe
ii. Písemný úkol
iii. E-mailový úkol
iv. Úkol ze zápisu

V urgentních případech mohou být požadavky předány i telefonicky ovšem následně musí dojít k potvrzení těchto úkolů jednou z výše uvedených forem

Pro vyloučení pochybností smluvní strany uvádí, že v souladu s článkem 7 rámcové smlouvy výše uvedené služby jsou služby, které nepodléhají akceptaci dle článku 7.2 rámcové smlouvy a budou v souladu s článkem 7.4 rámcové smlouvy evidovány ve Výkazech práce předložených Poskytovatelem Objednateli po ukončení měsíce, ve kterém byly Služby poskytovány.

Objednatel	Poskytovatel
V Praze dne 05 -11- 2015	V Praze dne 2/11/2015
Nepodepsáno	Nepodepsáno
Česká republika – Ministerstvo zemědělství David Šetina, ředitel Odboru správy centrálních informačních systémů a kybernetické bezpečnosti	**BDO IT, a.s.** Ing. Miloslav Rut, místopředseda představenstva

MINISTERSTVO ZEMĚDĚLSTVÍ
Těšnov 65/17
110 00 Praha 1 - Nové Město
-22-

Příloha č. 2

Harmonogram plnění

Služby profesionálních odborných služeb ICT budou čerpány dle konkrétních potřeb Objednatele.

Obecné ujednání:

Akceptace a dílčí akceptace a následná fakturace bude probíhat s odkazem na čl. 7.3 Rámcové smlouvy Outsorcing profesionálních odborných služeb ICT (OPOS), část bezpečnost informací.

Návrh harmonogramu a potřebných zdrojů

Penetrační testy budou probíhat v předem stanovených termínech po dohodě s klíčovými uživateli, využívány budou doby mimo provozní špičky. K ukončení služby dojde tři kalendářní měsíce po podpisu smlouvy.

Fáze	Název modulu	Zdroje (ČLD)	Trvání
1	Provedení penetračních testů	15	2 týdny
2	Zpracování zprávy z penetračních testů	5	1 týden
3	Rámcový retest odstranění identifikovaných slabin a nedostatků (provedení po odstranění identifikovaných slabin a nedostatků)	5	1 týden
	CELKEM	25	4 týdny

V rámci harmonogramu je proveden i návrh zdrojů a to v celkové výši maximálně 25 člověkodní. Dle uzavřené smlouvy se jedná o pozici analytika bezpečnosti informací.

Objednatel

V Praze dne 05 -11- 2015

.....

Česká republika – Ministerstvo zemědělství
David Šetina,
ředitel Odboru správy centrálních informačních systémů a kybernetické bezpečnosti

Poskytovatel

V Praze dne 2/11/2015

.....

BDO IT, a.s.
Ing. Miloslav Rut, místopředseda představenstva