Č. smlouvy Objednatele: 204/2020

SMLOUVA O DÍLO

uzavřená podle § 2586 a následujících zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, (dále jen „**občanský zákoník**")
(dále jen „**Smlouva**")

1. Smluvní strany

1.1 Objednatel

Česká republika – Ministerstvo vnitra

se sídlem:	Nad Štolou 936/3, 170 34 Praha 7
zastoupená:	Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru České republiky, plk. Ing. Radkem Jančíkem, ředitelem odboru Komunikačních a informačních systémů, generálního ředitele HZS ČR (dále jen MV-GŘ HZS ČR")
kontaktní adresa:	MV-GŘ HZS ČR, Kloknerova 26, 148 01 Praha 414
IČO:	00007064
bankovní spojení:	ČNB Praha 1
číslo účtu:	8908881/0710
ID schránky:	84taiur
kontaktní osoba ve věcech smluvních:	[redacted]
tel:	
kontaktní osoba ve věcech technických:	
tel:	
e-mail:	

(dále jen „**Objednatel**")

1.2 Zhotovitel

KPMG Česká republika, s.r.o.

společnost je zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 326

Sídlo:	Pobřežní 648/1a, Praha 8, 186 00
IČO:	00553115
bankovní spojení:	[redacted]
číslo účtu:	
ID schránky:	hbcgtsz
kontaktní osoba ve věcech smluvních:	[redacted]
tel:	
kontaktní osoba ve věcech technických:	
tel:	
e-mail:	

(dále jen „**Zhotovitel**")
(společně též jako „**Smluvní strany**")

2. Předmět smlouvy

Předmětem Smlouvy je zpracování Diferenční analýzy podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**"), a to v rozsahu podle přílohy č. 1 Smlouvy – Technická specifikace díla (dále jen „**Dílo**").

2.1 Metodika provedení díla

Zhotovení Díla (viz. čl. 2) bude probíhat ve 3 základních fázích:

- V první fázi Zhotovitel audituje prostředí Objednatele, cílem je získání potřebných informací pro zpracování diferenční analýzy v souladu s metodikou ČSN EN ISO 19011.
- Ve druhé fázi Zhotovitel navrhuje nápravná opatření s ohledem na stávající prostředí a požadavky Objednatele ve formě obecné definice (příklad „aplikační firewall").
- Ve třetí fázi Zhotovitel seznámí s návrhy Objednatele a Dílo předá na hmotném nosiči.

Metodika provedení diferenční analýzy

Metodika se zakládá na zjišťování stavu bezpečnostních opatření v kontextu požadavků jednotlivých ustanovení ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „**Vyhláška o kybernetické bezpečnosti**"), to vše v účinném znění, případně i ve znění doposud neúčinném avšak platném ke dni předání Díla. V rámci těchto tematických okruhů bude sledována sada dílčích hledisek pro plný soulad se zněním ZKB a Vyhláškou o kybernetické bezpečnosti. Popsání stávajícího stavu bude doplněno o nápravná opatření odsouhlasená Objednatelem bez podrobné specifikace a rozpočtových informací.

2.1.1 Výstupy

Podle jednotlivých fází budou podkladem k předání následující dokumenty:

- Auditní zpráva – hodnocení stávajícího prostředí Objednatele,
- Prezentace výsledků pro technické (odborné) součásti Objednatele,
- Prezentace výsledků pro management Objednatele.

Ve Výsledné zprávě Zhotovitel zdokumentuje stávající stav prostředí Objednatele, identifikuje a zhodnotí rozpory s požadavky ZKB a identifikuje nápravná opatření.

2.2 Předání Díla

Dílo bude předáno bez vad v listinné i elektronické podobě formou pořízení akceptačního protokolu mezi Smluvními stranami. Akceptační kritéria pro převzetí Díla jsou součástí přílohy č. 1 Smlouvy – Technická specifikace díla.

Po dohodě mezi Smluvními stranami je možné převzít Dílo i v případě, že bude mít nepodstatné vady.

3. Cena plnění

Cena za Dílo je stanovena fixní částkou ve výši 544 500,- Kč včetně DPH (slovy: pět set čtyřicet čtyři tisíc pět set korun českých včetně DPH), Cena bez DPH 450 000,- Kč, DPH 94 500,- Kč. Cena za Dílo je konečná a Zhotovitel nemá nárok na jakoukoliv dodatečnou, úhradu, odměnu, či poplatek.

4. Termíny předání Díla

Zhotovitel se zavazuje, že nejpozději do 60 kalendářních dnů od účinnosti smlouvy Dílo předá Objednateli. Zhotovitel není v prodlení v případě neposkytování součinnosti Objednatelem.

5. Platební a fakturační podmínky

5.1 Náležitosti faktur

Objednatel je povinen zaplatit dohodnutou cenu plnění dle čl. 3. Smlouvy.

Faktury musí obsahovat všechny náležitosti daňového dokladu uvedené v § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dalších dotčených právních předpisech. Faktura musí dále obsahovat:

- označení dokladu (faktura)
- číslo smlouvy
- den vystavení a lhůtu splatnosti
- IČO smluvních stran

Přílohou faktury bude akceptační protokol potvrzený Smluvními stranami.

5.2 Splatnost faktury

Lhůta splatnosti faktury je dohodnuta na 15 dnů ode dne doručení faktury Objednateli.

Zhotovitel se zavazuje vyhotovit a odeslat faktury do 15 dnů po vzniku práva fakturovat.

Fakturace po splnění požadovaných podmínek se uskuteční na adresu:

MV - GŘ HZS ČR pošt. přihr. 69
Kloknerova 26
148 01 Praha 414

na faktuře bude jako kupující uvedeno:

ČR - Ministerstvo vnitra
Nad Štolou 936/3
170 34 Praha 7

zastoupené – kontaktní adresa:

MV – GŘ HZS ČR
Kloknerova 26
pošt. přih. 69
148 01 Praha 414

Zhotovitel je povinen přiložit k faktuře originál předávacího protokolu (včetně dodaného příslušenství).

6. Vlastnické a užívací právo

Vlastnické a užívací právo ve smyslu § 2634 občanského zákoníku k Dílu resp. hmotným nosičům přechází na Objednatele dnem jeho předání. Zhotovitel není oprávněn Dílo sám užívat ani jej poskytnout třetí osobě.

7. Součinnost Objednatele

Objednatel se zavazuje poskytovat Zhotoviteli součinnost:

a) Poskytování požadovaných informací v obvyklých reakčních lhůtách bez zbytečných prodlev.
b) Poskytování přesných, úplných a správných informací, které budou vyžadovány.

8. Smluvní pokuty

V případě prodlení Zhotovitele s plněním této smlouvy, se smluvní strany dohodly na smluvní pokutě ve výši 0,05% z ceny Díla dle čl. 3 bez DPH za každý započatý den prodlení, nejvýše však 15 % z ceny Díla dle čl. 3 bez DPH.

V případě prodlení s úhradou splatné faktury dle čl. 5.2 Smlouvy uhradí Objednatel Zhotoviteli smluvní pokutu ve výši 0,05% z fakturované částky za každý započatý den prodlení.

V případě prodlení Objednatele s poskytnutím součinnosti ve smyslu čl. 7 Smlouvy, není Zhotovitel v prodlení a o tuto dobu prodlení se prodlužují všechny termíny plnění dle této Smlouvy.

9. Harmonogram

Podrobný časový harmonogram plnění Smlouvy bude sestaven v rámci úvodního jednání.

Předpokládaný harmonogram:

Pol.	Termín	Aktivita/Milník
0	T0	úvodní jednání provedené do 1 týdne od účinnosti Smlouvy
1	T0 + 30 kal. dnů	Vypracování návrhu analýzy stavu prostředí dle ZKB
2	T0 + 45 kal. dnů	Stanovení shody v hodnocení úrovně zabezpečení prostředí dle ZKB
3	T0 + 60 kal. dnů	KPMG připraví a předá finální závěrečnou zprávu (manažerské shrnutí)
4	T0 + 90 kal. dnů	KPMG vypracuje nabídku na zpracování penetračních testů

Výše uvedený harmonogram bude vycházet z množství osobních schůzek, nebo telefonických rozhovorů s odpovědnými osobami na základě dodaných odpovědných osob, dle předmětu hodnocených oblastí, které budou vycházet z požadavku, který je definován v příloze č.1 k č.j. MV-161289-1/PO-KIS-2020.

10. Zánik smlouvy

Smluvní strany se dohodly, že Smlouva zaniká:

- dohodou stran a způsoby uvedenými v občanském zákoníku.

11. Závěrečná ustanovení

Kontaktní osoby smluvních stran jsou oprávněny k poskytování součinnosti podle této Smlouvy.

Tato Smlouva nabývá platnosti dnem podpisu Smluvních stran a podle § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „zákon o registru smluv"), účinnosti dnem uveřejnění prostřednictvím registru smluv.

V souladu se zákonem o registru smluv, se Smluvní strany dohodly, že Objednatel zašle tuto Smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje Smluvních stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Tato Smlouva nesmí být bez předchozího písemného souhlasu druhé Smluvní strany postoupena třetí straně, nebo být součástí projektu přeměny podle zákona č. 125/2008 Sb., o přeměnách obchodních společností a družstev, ve znění pozdějších předpisů.

Smluvní strany se dohodly na uplatnění ustanovení § 576 občanského zákoníku, při posuzování vlivu nicotnosti (vady) této Smlouvy na ostatní ustanovení.

Smluvní strany se dohodly, že tato Smlouva se bude řídit právním řádem České republiky a zejména příslušnými ustanoveními občanského zákoníku.

Tuto Smlouvu lze měnit, doplňovat či zrušit pouze dohodou Smluvních stran, a to písemnými listinnými dodatky číslovanými vzestupnou řadou; jiná ujednání jsou neplatná a nebude k nim přihlíženo.

Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací této Smlouvy budou přednostně řešeny smírnou cestou. Nedojde-li k dohodě, budou spory řešeny před příslušnými obecnými soudy.

Veškerá korespondence mezi Smluvními stranami, včetně jejich prohlášení, je bez vlivu na sjednaný obsah práv a povinností Smluvních stran dle této Smlouvy, není-li ve Smlouvě stanoveno jinak.

Tato Smlouva je vyhotovena ve **čtyřech (4)** stejnopisech, z nichž **tři (3)** obdrží Objednatel a **jeden (1)** Zhotovitel.

Smluvní strany prohlašují, že předem souhlasí, v souladu se zněním zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, s možným zpřístupněním, či zveřejněním všech úkonů a okolností s touto Smlouvou souvisejících, ke kterému může kdykoliv v budoucnu dojít.

Každá ze Smluvních stran prohlašuje, že tuto Smlouvu uzavírá svobodně a vážně, že považuje obsah této Smlouvy za určitý a srozumitelný, a že jsou jí známy veškeré skutečnosti, jež jsou pro uzavření této Smlouvy rozhodující, na důkaz čehož připojují smluvní strany k této Smlouvě své podpisy.

Nedílnou součástí této Smlouvy jsou přílohy:

Příloha č. 1 – Zadávací dokumentace

V Praze dne: 5.11.2020

Za zhotovitele:

[redacted]

V PRAZE dne: 5.11.2020

Za Objednatele:

.....[redacted]

plk. Ing. Radek Jančík
ředitel odboru komunikačních
a informačních systémů

Ministerstvo vnitra
generální ředitelství
Hasičského záchranného sboru ČR
Kloknerova 26
148 01 Praha 414
-18-

Příloha č. 1: Zadávací dokumentace

1. SPECIFIKACE ZAKÁZKY

1. Předmět plnění díla

Předmětem plnění je přezkoumání informačního systému TCTV 112 (telefonní centrum tísňového volání 112) z hlediska implementace systému zajištění kybernetické bezpečnosti, bezpečnostních opatření (organizačních a technických opatření), dle zákona č. 181/2014 Sb (ZoKB) ve znění dalších změn zákona a souvisejících vyhlášek. TCTV 112 bude posouzena podle kritérií pro Kritickou informační infrastrukturu státu.

2. Popis TCTV 112

Viz příloha č. 1 - TCTV 112 – základní popis řešení

3. Detail předmětu plnění díla

3.1. Organizační část

Zhodnocení organizačních opatření implementovaných v IT prostředí TCTV 112 a HZS ČR.

- Bezpečnostní politika a bezpečnostní dokumentace
  - Identifikace a analýza bezpečnostní dokumentace a provozních směrnic a postupů
  - Zjednodušená definice primárních aktiv a hodnocení aktiv (CIA)
- Organizace bezpečnosti informací
  - Role a odpovědnosti
  - Oddělení odpovědností
  - Informační bezpečnost v projektech
  - Mobilní zařízení a práce na dálku
- Bezpečnost lidských zdrojů
  - Povědomí, vzdělávání a školení bezpečnosti informací
- Řízení aktiv
  - Management řízení aktiv a evidence aktiv
  - Vlastnictví aktiv
  - Odpovědnost za aktiva
  - Klasifikace aktiv a informací
  - Použití aktiv a životní cyklus aktiv
  - Řízení použití nosičů informací a médií
  - Manipulace s médii
- Řízení přístupu a přístupových práv
  - Požadavky organizace na řízení přístupu
  - Řízení přístupu uživatelů a jejich odpovědnost
  - Řízení přístupu k systémům a aplikacím
- Fyzická bezpečnost pracovišť a zařízení
  - Bezpečné oblasti
  - Fyzický perimetr
  - Fyzická bezpečnost a kontrola vstupu
  - Zařízení a fyzická bezpečnost
- Bezpečnost provozu
  - Provozní postupy a odpovědnosti
  - Dokumentace provozních postupů

    - Řízení změn
    - Řízení rizik / Plán zvládání rizik
    - Řízení kapacit
    - Princip oddělení prostředí vývoje, testování a provozu
    - Ochrana proti malwaru
    - Zálohování
    - Logování, zaznamenávání a monitorování událostí
    - Ochrana logů, logy o činnosti administrátorů a operátorů
    - Správa provozního softwaru
    - Opatření k auditu informačních systémů
- Bezpečnost komunikací a přenos dat
    - Přenos a ochrana informací
- Akvizice, vývoj a údržba informačních systémů
    - Bezpečnostní požadavky informačních systémů
    - Bezpečnost v procesech vývoje a podpory
    - Politika bezpečného vývoje
    - Postupy řízení změn systémů
    - Data pro testování
- Bezpečnost pro dodavatele a třetí strany
    - Bezpečnost informací v dodavatelských vztazích
    - Bezpečnostní požadavky v dohodách s dodavateli
    - Řízení dodávek služeb dodavatelů
- Řízení a zvládání bezpečnostních incidentů
    - Řízení incidentů bezpečnosti informací, sběr, vyhodnocování, reakce a zlepšování procesu
- Řízení kontinuity organizace
    - Plánování kontinuity bezpečnosti informací
    - Implementace kontinuity bezpečnosti informací
    - Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací
    - Dostupnost vybavení pro zpracování informací
    - Nástroj pro zajišťování úrovně dostupnosti informací
- Technologie kryptování
    - Politika pro použití kryptografických opatření
- Soulad s interními a externími právními požadavky
    - Identifikace odpovídající legislativy a smluvních požadavků
    - Ochrana záznamů
    - Soukromí a ochrana osobních údajů
    - Ochrana duševního vlastnictví
- Přezkoumání bezpečnosti informací
    - Nezávislá přezkoumání bezpečnosti informací
    - Shoda s bezpečnostními politikami a normami
    - Přezkoumání technické shody

3.2. Technická část

Zhodnocení technických opatření implementovaných v IT prostředí TCTV 112 a HZS ČR.

- Identifikace a kontrola implementace technických opatření
    - Fyzická bezpečnost

- Fyzický bezpečnostní perimetr
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
- Ochrana před škodlivým kódem
- Nástroj pro ochranu integrity komunikačních sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kóde
- Nástroj pro zaznamenávání činnosti informačních systémů, jejich uživatelů a administrátorů
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti informací
- Bezpečnost průmyslových, řídicích a obdobných specifických systémů

- Správa bezpečnosti sítě
  - Bezpečnost síťových služeb
  - Opatření a kontroly v sítích
  - Princip oddělení v sítích / segmentace komunikační sítě
- Řízení technických zranitelností
  - Implementace technických opatření pro řízení zranitelností a rizik
  - Vulnerability testování / Penetrační testy informačního a komunikačního systému

2. AKCEPTAČNÍ KRITÉRIA

1. **V rámci plnění požaduje HZS ČR přezkoumat veškeré body v organizační i technické části, které jsou uvedené výše.**
   1.1. Pro každé opatření požadujeme popis aktuálního stavu
   1.2. Zhodnocení z pohledu požadavků prováděcí vyhlášky o KB (VoKB)
   1.3. Případné zhodnocení z pohledu „best practice“, pokud bude takovéto doporučení žádoucí.
   1.4. Obsahem zprávy jsou veškeré paragrafy obsažené v prováděcí vyhlášce ZoKB, tzn., že se organizace zkoumá z pohledu všech organizačních i technických opatření.
2. **Hodnocení stavu očekává HZS ČR v dvou variantách**
   2.1. Podrobná varianta pro technické (odborné) součásti HZS ČR
   2.2. Odděleně s menší mírou detailu pro vrcholný management HZS ČR
3. **Obecný návrh nápravných opatření**
   3.1. Cílem není hodnotit veškeré možné technické varianty nápravných opatření, ale určit jejich typ, který se aplikuje do plánu zvládání rizik a dalších strategických dokumentů HZS ČR
   3.2. Vydefinují se priority pro jednotlivá nápravná opatření, která vyplynou z výstupů analýzy.
4. **Prezentace výsledků pro technické (odborné) součásti HZS ČR**
5. **Prezentace výsledků pro vrcholný management**

3. KVALIFIKAČNÍ KRITÉRIA

Dodavatel doloží pro potřeby této zakázky zajištění následujících rolí v rámci řešitelského týmu

1. **Požadavky na vedoucího konzultačního týmu**

1.1. Řízení ISMS - Kompetence k řízení kybernetické bezpečnosti, - certifikace CISM nebo CISSP nebo obdobné

1.2. Řízení rizik – Kompetence k risk managementu – certifikace CRISC nebo obdobné

2. **Požadavky na roli specialista řešení kybernetických bezpečnostních incidentů, penetračního testování a bezpečnostní architektury**

2.1. Bezpečnostní testování

- Znalost metodiky kybernetických útoků – certifikace **EC-Council Certified Ethical Hacker (CEH)** nebo obdobné
- Vysoká kompetence v oblasti penetračního testování – certifikace **CompTIA Pentest+**
- Hluboká znalost metodik penetračního testování – **ECSA**
- Prokazatelná orientace v problematice penetračních testů – **eJPT**
- Vysoká kompetence v oblasti penetračního testování webových aplikací – certifikace **GWAPT**

2.2. Bezpečnostní architektura

- Znalost technických bezpečnostních opatření – certifikace CompTIA Security+ nebo obdobné
- Vysoká kompetence v oblasti enterprise security; řízení rizik; bezpečnostní architektury a kyber-bezpečnosti obecně – certifikace CompTIA Advanced Security Practitioner (CASP

2.3. Zvládání bezpečnostních incidentů

- Schopnost správy hrozeb a zranitelností – certifikace CompTIA Cybersecurity Analyst (CySA+)
- Schopnost rozpoznat a reagovat na hrozby kyberprostoru, cyber espionage, vnitřní hrozby a další požadavky týkající se kyber-bezpečnosti, kterým musí organizace
- čelit – certifikace CCNA Cyber Ops).
- Vysoké dovednosti potřebné k pomoci organizaci před, během a po narušení kybernetické bezpečnosti – certifikace Certified First Responder (CFR)

3. **Požadavky na organizaci**

3.1. Firemní zralost v oblasti zvládání kybernetických bezpečnostních incidentů potvrzená nezávislou nadnárodní autoritou a členstvím v celosvětové bezpečnostní komunitě TI

- Vysoká kompetence k zvládání kybernetických bezpečnostních incidentů – certifikace bezpečnostního týmu – zřízeného v České republice společností se sídlem v České republice – organizací Trusted Introducer minimálně na úrovni Accredited.

3.2. Firemní zralost v přístupu k bezpečnosti informací

- Zvládnuté řízení informační bezpečnosti v organizaci – norma ISO 27000 (ISO/IEC 27000)

4. **Požadavky na referenci**

4.1. Minimálně 4 referenční zakázky obdobného rozsahu u systému zařazeného do KII/VIS (z toho minimálně 1x KII) formou seznamu s referenčními kontakty

5. **Požadavky na bezpečnost**

5.1. Všichni členové týmu podepíší před uzavřením smlouvy NDA

Termín předání díla : nejpozději do 60 kalendářních dnů od účinnosti smlouvy

Zpracoval: