

ZMLUVA O ODBORNÝCH SLUŽBÁCH

Článok č. 1. Zmluvné strany

Klient: **Záchranná zdravotná služba Bratislava
štátna príspevková organizácia**
Antolská 110
850 07 Bratislava
Konajúci prostredníctvom: Ing. PhDr. Michal Kováčik, riaditeľ
IČO: 17 336 210
DIČ: 2020845827
IČ pre DPH: neplatca
Bankové spojenie: Štátna pokladnica
IBAN: SK85 8180 0000 0070 0028 7955
Zapísaná: v registri organizácii vedenej Štatistickým úradom
Zriadená: zriaďovacou listinou MZ SR č. 3724/1991 – A/XXI-3
s účinnosťou od 1.1.1992 v znení neskorších zmien

e-mail:
tel. sekretariát:
kontaktná osoba: Tomáš Semančík
e-mail:
tel.:

(ďalej len „Klient“, „Prevádzkovateľ základnej služby“ alebo „PZS“)

Dodávateľ: **Ratio Services s.r.o.**
Priehradná 59
821 07 Bratislava
Konajúci prostredníctvom: Mgr. Katarína Hettychová
IČO: 45 299 391
DIČ: 2022939435
IČ pre DPH: SK 2022939435
Bankové spojenie: Tatrabanka a.s.
IBAN: SK33 1100 0000 0029 2682 9022 Spoločnosť je zapísaná
Spoločnosť je zapísaná: v Obchodnom registri Okresného súdu Bratislava I, odd.
s.r.o. vl.č. 62039/B

(ďalej len „dodávateľ“)

Klient a dodávateľ sa ďalej označujú jednotlivo ako „**zmluvná strana**“ a spoločne ako „**zmluvné strany**“. Táto Zmluva o odborných službách sa ďalej označuje spoločne s jej prílohami ako „**zmluva**“. Zmluvné strany s úmyslom byť viazané podmienkami uvedenými nižšie uzatvárajú túto zmluvu o odborných službách podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodného zákonníka v platnom znení (ďalej len „**Obchodný zákonník**“).

Článok č. 2. Predmet zmluvy

- 2.1. Dodávateľ sa zaväzuje poskytnúť klientovi služby vymedzené v Článok č. 3. tejto zmluvy v súlade s podmienkami dohodnutými v tejto zmluve (ďalej len „**Služby**“) a klient sa zaväzuje uhradiť za poskytnuté služby dodávateľovi odmenu dohodnutú v Článok č. 5. Článok č. 4. tejto zmluvy.

Článok č. 3. Rozsah služieb – Audit kybernetickej bezpečnosti

- 3.1. Predmetom zmluvy je záväzok dodávateľa vykonať audit kybernetickej bezpečnosti klienta tak, ako je bližšie špecifikované v bode 3.5 nižšie, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení (ďalej len „**Zákon**“), príslušnej Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z. (ďalej len „**Vyhláška o bezpečnostných opatreniach**“) ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a Vyhlášky Národného bezpečnostného úradu č. 436/2019 Z.z. (ďalej len „**Vyhláška o audite**“) o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.
- 3.2. Dodávateľ sa v rámci auditu kybernetickej bezpečnosti zaväzuje zabezpečiť výkon auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti (ďalej len „**Audítor**“)

kybernetickej bezpečnosti") podľa Vyhlášky o audite, ktorý spĺňa všetky požiadavky na výkon auditu.

- 3.3. Dodávateľ je oprávnený použiť na splnenie predmetu tejto zmluvy subdodávateľov, za predpokladu, že s nimi uzatvoril písomnú zmluvu a o zapojení subdodávateľa vopred informoval klienta. Tým nie je dotknutá zodpovednosť za splnenie predmetu tejto zmluvy.
- 3.4. Zmluvné strany sa dohodli, že predmet zmluvy sa považuje za splnený riadne a včas dňom predloženia Záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa bodu 3.7 tejto zmluvy.
- 3.5. Audítor kybernetickej bezpečnosti sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť nasledovné služby:
- a) v súlade so Štandardom na výkon auditu kybernetickej bezpečnosti vydanom Kompetenčným centrom kybernetickej bezpečnosti (ďalej len „**Metodika auditu**“, uvedenom na URL: <https://cybercompetence.sk/wp-content/uploads/dokumenty/ine/metodika-audit.pdf>) a v súlade s požiadavkami Zákona a Vyhlášky o bezpečnostných opatreniach výkon auditu kybernetickej bezpečnosti, a teda auditu sietí a informačných systémov klienta ako prevádzkovateľa základnej služby, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek Zákona a Vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa základnej služby. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky:
- I. Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:
- Organizácia informačnej bezpečnosti,
 - Riadenie aktív, hrozieb a rizík,
 - Personálna bezpečnosť,
 - Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
 - Technických zraniteľností systémov a zariadení,
 - Riadenie bezpečnosti sietí a informačných systémov,
 - Riadenie prevádzky,
 - Riadenie prístupov,
 - Kryptografických opatrení,
 - Riešenia kybernetických bezpečnostných incidentov,
 - Monitorovania, testovania bezpečnosti a bezpečnostných auditov,
 - Fyzickej bezpečnosti a bezpečnosti prostredia,
 - Riadenia kontinuity procesov.
- 3.6. Klient je povinný poskytnúť dodávateľovi všetky informácie a súčinnosť potrebnú pre splnenie predmetu tejto zmluvy.
- 3.7. Výstupom auditu kybernetickej bezpečnosti je Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v slovenskom jazyku (ďalej aj ako „**Správa**“) vypracovaná v súlade s požiadavkami Vyhlášky o audite.

Správa bude mať nasledovnú štruktúru, pokiaľ z Vyhlášky o audite nevyplýva iná štruktúra a rozsah:

- Meno, priezvisko a číslo platného certifikátu audítora, dátum vyhotovenia a podpis audítora,
- Vymedzenie rozsahu vykonaného auditu kybernetickej bezpečnosti,
- Cieľ auditu kybernetickej bezpečnosti,
- Použité postupy a metodiky vykonaného auditu kybernetickej bezpečnosti,
- Zhrnutie zistení výsledkov auditu kybernetickej bezpečnosti a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,
- Odporúčané nápravné opatrenia audítora pri zistení nedostatkov,
- Dokumenty, ktorými sú najmä
 - Kópiu certifikátu audítora,
 - Kópiu žiadosti o výkon auditu podľa prílohy č. 1 Vyhlášky o audite,
 - Výpočet rozsahu trvania auditu a zdôvodnenie skrátenia alebo predĺženia,
 - Kontrolný záznam auditovaných bezpečnostných opatrení s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,
 - Harmonogram auditu,

6. Zoznam posúdenej dokumentácie,
7. Uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,
8. Zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vysovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov, a konkrétne uvedenie nedostatkov.

Správa bude podľa požiadavky klienta buď predložená v jednom elektronickom vyhotovení štatutárnemu orgánu klienta zabezpečeným kanálom a podpísaná kvalifikovaným elektronickým podpisom audítora kybernetickej bezpečnosti a správa bude predložená aj v tlačenej vyhotovení v dvoch vyhotoveniach štatutárnemu orgánu klienta spôsobom podľa bodu 6.3 tejto zmluvy.

Správa bude pripravená výlučne pre informovanie štatutárneho orgánu klienta a relevantných zainteresovaných strán klienta na účel špecifikovaný vyššie. Štatutárny orgán klienta je oprávnený Správu v podobe predloženej audítorom kybernetickej bezpečnosti predložiť Národnému bezpečnostnému úradu (ďalej len „NBÚ“), v súlade s účelom popísaným vyššie v tejto zmluve a ďalej sprístupniť nasledujúcemu audítorovi kybernetickej bezpečnosti vykonávajúcemu audit kybernetickej bezpečnosti u klienta pre informačné účely. Správa ani žiadna jej časť nesmie byť distribuovaná žiadnej tretej strane (s výnimkou výslovného predchádzajúceho písomného súhlasu dodávateľa udeleného vopred), ani použitá klientom na žiaden iný účel. Žiadna tretia strana nie je oprávnená použiť Správu alebo akékoľvek informácie v nich uvedené ani sa na ne spoliehať, pokiaľ osobitný právny predpis nestanovuje inak.

- 3.8. Audit kybernetickej bezpečnosti vykonáva Audítor kybernetickej bezpečnosti k stavu ku dňu výkonu auditu kybernetickej bezpečnosti, pričom Audítor kybernetickej bezpečnosti nie je povinný monitorovať a zohľadňovať siete a informačné systémy klienta ani udalosti, ktoré nastali po dátume vydania Správy a ani nie je povinný Správu aktualizovať.
- 3.9. Žiadne informácie, ktoré Audítor kybernetickej bezpečnosti predloží klientovi mimo Správy, nepredstavujú jeho konečné názory ani závery. Konečné názory alebo závery sa uvedú výlučne v Správe.
- 3.10. Pre vylúčenie akýchkoľvek pochybností platí, že akýkoľvek nesúhlas klienta so závermi Audítora kybernetickej bezpečnosti uvedenými v Správe sa nepovažuje za porušenie povinností dodávateľa ani audítora kybernetickej bezpečnosti vyplývajúcich zo zmluvy a nezakladá právo klienta na odstúpenie od zmluvy alebo iné s porušením povinnosti podľa tejto zmluvy inak súvisiace nároky.

Článok č. 4. Miesto plnenia a harmonogram poskytovania služieb

- 4.1. Zmluvné strany sa dohodli, že preferovanou formou poskytovania Služieb je poskytnutie Služieb na mieste On-Site, a to v priestoroch Klienta, vzdialené poskytovanie Služieb On-Line uskutoční dodávateľ po dohode s Klientom.
- 4.2. Harmonogram poskytovania služieb je nasledovný, pričom lehoty začínajú plynúť 1. dňom nasledujúcim po dni účinnosti tejto zmluvy:

Fáza auditu	Termín
Nastavenie auditného programu najneskôr v termíne do:	3 dní
Výkon auditu kybernetickej bezpečnosti a Záverečná správa o výsledku auditu najneskôr v termíne do:	30 dní

Výsledkom akéhokoľvek oneskorenia zo strany klienta pri poskytnutí uvedených informácií, dokumentácie a všetkých údajov potrebných pre poskytnutie služieb podľa tejto zmluvy alebo akejkoľvek inej súčinnosti, ktorú je klient podľa tejto zmluvy povinný poskytnúť, bude oneskorenie uvedeného harmonogramu poskytovania Služieb zo strany Audítora kybernetickej bezpečnosti. Akékoľvek dodatočné informácie a/alebo úpravy vykonané klientom po tom, čo boli nevyhnutné informácie a dokumentácia predložená audítorovi kybernetickej bezpečnosti, môžu mať za následok oneskorenie a/alebo dodatočné poplatky podľa **Chyba! Nenašiel sa žiaden zdroj odkazov..** Audítor kybernetickej bezpečnosti sa zaväzuje informovať klienta o akýchkoľvek skutočnostiach vedúcich k oneskoreniu v dodržaní termínov alebo o iných okolnostiach, ktoré by mohli mať nepriaznivý vplyv na poskytovanie služieb podľa tejto zmluvy bezodkladne po tom, čo sa o nich audítor kybernetickej bezpečnosti dozvie.

- 4.3. Audítor kybernetickej bezpečnosti predloží návrh Správy klientovi na vyjadrenie pred vydaním finálnej verzie Správy. Klient je oprávnený predložiť svoje pripomienky k návrhu Správy najneskôr do 3 pracovných dní od predloženia príslušného návrhu Správy audítora. Audítor kybernetickej bezpečnosti následne, najneskôr do 3 pracovných dní od ukončenia výkonu auditu a po získaní pripomienok od klienta, vydá finálnu verziu Správy. V prípade, že sa klient nevyjadrí vo vyššie stanovenej lehote, považuje sa návrh Správy za akceptovaný zo strany klienta a Audítor kybernetickej bezpečnosti vydá finálnu verziu Správy.
- 4.4. Klient zabezpečí, že pravdivé, správne a úplné informácie a dokumenty potrebné na riadne a včasné splnenie predmetu zmluvy. Klient vyhlasuje, že pred dodávateľom alebo Audítorom kybernetickej bezpečnosti nebudú zamlčané žiadne informácie, ktoré dodávateľ alebo Audítor kybernetickej bezpečnosti potrebuje na účely plnenia predmetu zmluvy, bez ohľadu na to, či dodávateľ alebo audítor kybernetickej bezpečnosti takého informácie špecificky požadoval.
- 4.5. Klient je povinný určiť aspoň jedného pracovníka (ďalej „**Poverený pracovník**“), ktorý bude zodpovedný za plnenie administratívnych a iných požiadaviek na účely realizácie predmetu tejto zmluvy. Klient oznámi meno a kontaktné údaje (email, mobilné telefónne číslo) určeného pracovníka Audítorovi kybernetickej bezpečnosti pred začatím poskytovania služieb.
- 4.6. Audítor kybernetickej bezpečnosti predloží poverenému pracovníkovi detailnú požiadavku na informácie a dokumentáciu aspoň v rozsahu definovanom vo Vyhláske o audite. Tieto informácie a dokumentáciu Klient doručí Audítorovi kybernetickej bezpečnosti najneskôr 5 dní pred začatím poskytovania služieb, ak Audítor kybernetickej bezpečnosti neurčil neskoršiu lehotu. Audítor kybernetickej bezpečnosti nezačne poskytovať služby, kým od klienta neobdrží požadované úplné informácie a dokumentáciu. Ak informácie predložené Audítorovi kybernetickej bezpečnosti zo strany klienta nie sú doručené včas alebo nebudú dostatočné alebo primerané, za podmienok uvedených v zmluve si Audítor kybernetickej bezpečnosti vyhradzuje právo zmeniť harmonogram poskytovania služieb primerane podľa dostupnosti požadovaných informácií a jeho možností alebo odporučiť odklad výkonu auditu.

Článok č. 5. Odmena a platobné podmienky

- 5.1. Cena za služby uvedené v bode 3.1 vyššie bola dohodou zmluvných strán stanovená na **6 200,00 EUR** (slovom: Šesťtisícdivesto eur bez DPH, (**7 440 EUR** s DPH), (ďalej len „**Cena**“). Dodávateľ je platca DPH.
- 5.2. Cena sa bude fakturovať po ukončení poskytovania služby, ktorou sa rozumie predloženie finálnej Správy klientovi spôsobom podľa bodu 3.7 zmluvy. Faktúra bude vystavená do 5 dní odo dňa predloženia finálnej Správy klientovi, najneskôr však do piateho (5.) pracovného dňa mesiaca, nasledujúceho po mesiaci v ktorom boli Služby dodané. Faktúra je splatná do 30 dní odo dňa jej doručenia.
- 5.3. Cena je stanovená ako najvyššie prípustná, neprekročiteľná a platná za celú dobu trvania zmluvy. V dohodnutej Cene sú zahrnuté všetky náklady dodávateľa v súvislosti s poskytovaním plnenia podľa tejto zmluvy, vrátane prípadných cestovných nákladov a nákladov za stratu času počas tejto cesty. Okrem dohodnutej Ceny dodávateľ nemá nárok na žiadne ďalšie plnenia v zmysle tejto zmluvy.
- 5.4. Ceny boli stanovené dohodou zmluvných strán na základe platnej slovenskej legislatívy a na základe predpokladu poskytnutia úplných a pravdivých informácií a riadnej súčinnosti zo strany klienta.
- 5.5. Zmluvné strany sa dohodli, že faktúry budú vyhotovené v elektronickej podobe (tzv. elektronická faktúra) vo formáte PDF/A a Klientovi budú doručované emailom na emailovú adresu: **faktury@emergency-ba.sk**, pričom faktúry sa považujú za doručené Klientovi dňom ich odoslania.
- 5.6. Všetky peňažné plnenia podľa zmluvy sú splatné v EUR na bankový účet dodávateľa uvedený na faktúre.
- 5.7. V prípade omeškania Klienta s úhradou akéhokoľvek peňažného planenia alebo jeho časti podľa tejto zmluvy je dodávateľ oprávnený uplatniť si voči klientovi zmluvnú pokutu vo výške 0,5 % z dlžnej sumy za každý aj začatý deň omeškania v súlade s ustanovením § 369 Obchodného zákonníka. Klient sa zaväzuje zmluvnú pokutu podľa predchádzajúcej vety dodávateľovi uhradiť na základe faktúry dodávateľa.

- 5.8. V prípade omeškania dodávateľa s poskytnutím služieb – fáz auditu, podľa harmonogramu v zmysle bodu 4.2. je Klient oprávnený uplatniť si voči dodávateľovi zmluvnú pokutu vo výške 0,5 % z Ceny za každý aj začatý deň omeškania poskytnutia jednotlivých služieb – fáz auditu.
- 5.9. V prípade, ak sa preukáže po uzatvorení tejto zmluvy, že na relevantnom trhu existuje cena (ďalej aj „nižšia cena“) za rovnaké alebo porovnateľné služby, ako je uvedené v tejto zmluve a dodávateľ aj reálne za takúto nižšiu cenu služby už poskytol alebo stále poskytuje, ktorá je nižšia o viac ako 5 % ako cena dodávateľa podľa tejto zmluvy, zaväzuje sa dodávateľ poskytnúť Klientovi pre takúto službu po preukázaní tejto skutočnosti dodatočnú zľavu vo výške rozdielu medzi ním poskytovanou cenou podľa tejto zmluvy a nižšou cenou.
- 5.10. Dodávateľ sa zaväzuje, že pohľadávku voči Klientovi, ktorá mu, ako veriteľovi, vznikne z tohto zmluvného vzťahu, nepostúpi podľa § 524 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej len „Občiansky zákonník“) tretej osobe bez predchádzajúceho písomného súhlasu klienta, ako dlžníka. Postúpenie pohľadávky dodávateľom bez predchádzajúceho písomného súhlasu klienta je podľa § 39 a § 525 ods. 2 Občianskeho zákonníka absolútne neplatným právnym úkonom. Súhlas klienta je platný len za podmienky, že bol na takýto úkon udelený predchádzajúci písomný súhlas jeho zriaďovateľa (Ministerstvo zdravotníctva Slovenskej republiky).

Článok č. 6. Komunikácia

- 6.1. Adresy, telefónne čísla a e-mailové adresy zmluvných strán na účely ich oznámení týkajúcich sa tejto zmluvy sú:

Za dodávateľa: **RATIO SERVICES s.r.o.**
Do pozornosti: Ing. Tomáš Hettych
adresa uvedená v úvode zmluvy
Tel:
E-mail:

Klient: **Záchranná zdravotná služba Bratislava**
Do pozornosti: **Tomáš Semančík**, manažér kybernetickej bezpečnosti
adresa uvedená v úvode zmluvy
Tel:
E-mail:

- 6.2. O zmene kontaktných údajov alebo kontaktných osôb je dotknutá zmluvná strana povinná druhú zmluvnú stranu informovať bez zbytočného odkladu.
- 6.3. S výnimkou otázok týkajúcich sa zániku tejto zmluvy, nárokov na náhradu škody alebo iné peňažné plnenie podľa tejto zmluvy, ktorú musia byť uplatnené písomne, sú zmluvné strany oprávnené komunikovať aj formou emailu a táto emailová komunikácia bude považovaná za riadne oznámenie podľa tejto zmluvy. Písomnosť sa považuje za doručeníu za nasledovných podmienok:
- (a) v prípade osobného doručovania odovzdaním písomnosti oprávnenej osobe alebo inej osobe oprávnenej prijímať písomnosti za túto Zmluvnú stranu a podpisom takej osoby na doručenke a/alebo kópii doručovanej písomnosti, alebo odmietnutím prevzatia písomnosti takou osobou,
 - (b) v prípade poštového doručovania doručením na adresu Zmluvnej strany a v prípade doporučenej zásielky odovzdaním písomnosti osobe oprávnenej prijímať písomnosti za túto Zmluvnú stranu a podpisom takej osoby na doručenke, najneskôr však uplynutím siedmich dní odo dňa uvedeného na podacom lístku, a to bez ohľadu na úspešnosť doručenia,
 - (c) v prípade doručovania prostredníctvom elektronickej pošty dňom nasledujúcim po odoslaní elektronickej pošty, ak prijímajúca Zmluvná strana nepotvrdí prijatie elektronickej správy skôr, a to i v prípade, ak sa druhá Zmluvná strana o doručení elektronickej pošty nedozvedela alebo ak sa z dôvodov na prijímajúcej Zmluvnej strane s obsahom neoboznámila,
- 6.4. Klient si je vedomý, že v prípade emailovej komunikácie nemožno zaručiť úplnú bezpečnosť a bezchybnosť a že takéto informácie môžu byť zachytené, poškodené, môžu sa stratiť, zničiť, môžu byť doručené neskoro alebo neúplné, alebo môžu byť inak negatívne ovplyvnené.

Článok č. 7. Obmedzenie zodpovednosti

- 7.1. Dodávateľ zodpovedá len za skutočnú škodu spôsobenú porušením tejto zmluvy, najviac však do výšky sumy 50.000 EUR
- 7.2. Klient má zmluvný vzťah výlučne s dodávateľom. Klient nebude mať žiadne nároky voči iným osobám použitým pri plnení tejto zmluvy s výnimkou dodávateľa.

Článok č. 8. Autorské práva a duševné vlastníctvo

- 8.1. Dodávateľ je nositeľom všetkých práv duševného vlastníctva na všetko, čo vytvoril audítor kybernetickej bezpečnosti pred alebo počas poskytovania služieb, vrátane správ, písomného poradenstva, listov, odporúčaní alebo iných výstupov poskytovania služieb klientovi (ďalej ako „Výstupy“). Výstupy prechádzajú momentom ich odovzdania Klientovi do vlastníctva Klienta. Momentom vytvorenia Výstupov, predstavujúcich autorské dielo, udeľuje dodávateľ klientovi výhradnú licenciu na použitie týchto Výstupov na dosiahnutie účelu tejto zmluvy a v súlade s ostatnými ustanoveniami zmluvy. Licencia sa udeľuje na obdobie trvania majetkových práv k Výstupom. Spôsoby používania Výstupov ako aj vecný a územný rozsah licencie sú obmedzené účelom, na ktorý boli Výstupy vypracované.
- 8.2. Dodávateľ sa zaväzuje neposkytnúť alebo nesprístupniť Výstupy vrátane Záverečnej správy tretím stranám, s výnimkou prípadov uvedených v tejto zmluve (napr. bod. 3.7.) alebo ak tak ustanovuje všeobecne záväzný právny predpis alebo to nie je vyžadované orgánom verejnej moci pri výkone svojej pôsobnosti, súdom alebo iným oprávneným subjektom.

Článok č. 9. Mlčanlivosť

- 9.1. Audítor kybernetickej bezpečnosti je povinný vo vzťahu ku všetkým mu poskytnutým informáciám a údajom zachovávať mlčanlivosť podľa § 12 Zákona.

Článok č. 10. Ochrana osobných údajov

- 10.1. V súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie“) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov, v znení neskorších predpisov (ďalej len „Zákon OOÚ“) klient a dodávateľ sú v postavení samostatných prevádzkovateľov.
- 10.2. Klient aj dodávateľ sú povinní dôsledne chrániť všetky spracúvané osobné údaje, s ktorými prídu do styku pri plnení predmetu tejto zmluvy. Klient aj dodávateľ sú povinní prijať primerané technické a organizačné opatrenia tak, aby spracúvanie osobných údajov spĺňalo požiadavky Nariadenia resp. Zákona OOÚ a aby bola zabezpečená ochrana práv dotknutých osôb podľa Nariadenia a Zákona OOÚ. Zároveň sú povinní plniť ďalšie povinnosti uložené príslušnými právnymi predpismi v oblasti ochrany osobných údajov a ochrany informácií.
- 10.3. Klient potvrdzuje, že všetky osobné údaje poskytnuté dodávateľovi boli získané zákonným spôsobom, pri zachovaní všetkých základných zásad spracúvania osobných údajov.

Článok č. 11. Trvanie a ukončenie zmluvy

- 11.1. Platnosť zmluvy sa skončí podľa toho, ktorý prípad nastane skôr:
 - (a) riadnym splnením predmetu zmluvy; alebo
 - (b) zmluvné strany uzatvoria písomnú dohodu o ukončení platnosti zmluvy; alebo
 - (c) odstúpením od zmluvy po tom, ako jedna zmluvná strana prevezme písomné oznámenie druhej zmluvnej strany o odstúpení od zmluvy, v ktorom sa uvádza, že druhá zmluvná strana porušila povinnosti jej vyplývajúce zo zmluvy (ďalej len „porušujúca zmluvná strana“) za predpokladu, že porušujúca zmluvná strana bola na porušovanie povinností vopred písomne upozornená a napriek tomu nevykonala nápravu v primeranej lehote (ktorá nesmie byť kratšia ako 15 dní) od doručenia písomného upozornenia.
- 11.2. Dodávateľ je oprávnený od zmluvy odstúpiť na základe písomného oznámenia doručeného klientovi, ak zistí, že sa objavila závažná prekážka vo výkone auditu pred dňom alebo počas výkonu Auditu kybernetickej bezpečnosti (okrem iného vrátane zmeny v príslušnej legislatíve alebo v dôsledku rozhodnutia štátneho orgánu alebo inej príslušnej profesijnej organizácie alebo zmeny vo vlastníckej štruktúre klienta alebo jeho pridružených osôb, alebo náležitostiach žiadosti o Audit kybernetickej bezpečnosti), na základe ktorých by plnenie ktorejkoľvek časti zmluvy zo strany dodávateľa bolo

zmenené, sťažené, protiprávne alebo inak nezákonné alebo v rozpore s pravidlami nezávislosti alebo pravidlami profesijnej etiky.

- 11.3. Klient je oprávnený od zmluvy odstúpiť na základe písomného oznámenia doručeného dodávateľovi, ako dodávateľ porušuje akúkoľvek povinnosť stanovenú touto zmluvou alebo príslušnými právnymi predpismi a túto nesplní ani v dodatočnej primeranej lehote, ktorá mu na to bola Klientom v písomnom upozornení poskytnutá alebo ak dodávateľ (alebo audítor) stratí oprávnenie na poskytovanie Služieb podľa tejto zmluvy. Ustanovenia Obchodného zákonníka o dostúpení týmto nie sú dotknuté.
- 11.4. V prípade odstúpenia od zmluvy Klientom z dôvodu porušovania povinností dodávateľom, Klient nebude povinný uhradiť dodávateľovi Cenu podľa tejto zmluvy, ani žiadne náklady a výdavky, ktoré dodávateľ v súvislosti s plnením podľa tejto zmluvy mal.

Článok č. 12. Záverečné ustanovenia

- 12.1. Zmluvné strany vyhlasujú, že Klient za účelom naplnenia požiadavky v zmysle § 1 ods. 7 písm. a) Vyhlášky o audite predložil dodávateľovi pred podpisom tejto zmluvy dotazník (v rámci opisu predmetu zákazky) obsahujúci informácie predpokladané prílohou č. 2 Vyhlášky o audite. Zmluvné strany súhlasia, že predmetný prieskum, ktorý tvorí Prílohu č. 1 tejto zmluvy, sa považuje za žiadosť o výkon auditu v zmysle Vyhlášky o audite a v tomto rozsahu bude v zmysle § 2 od. 2 písm. g) bod 2 Vyhlášky o audite, súčasťou Správy.
- 12.2. Zmluvné strany vyhlasujú, že získali všetky potrebné povolenia a oprávnenia na uzavretie tejto zmluvy a na jej plnenie.
- 12.3. Táto zmluva sa vyhotovuje v troch vyhotoveniach v slovenskom jazyku. Klient dostane dve vyhotovenia a dodávateľ jedno vyhotovenie v slovenskom jazyku.
- 12.4. Akékoľvek zmeny a/alebo doplnenia Zmluvy sa môžu vykonať iba na základe dohody obidvoch Zmluvných strán, a to vo forme písomných a očíslovaných dodatkov k Zmluve podpísaných oprávnenými zástupcami oboch Zmluvných strán.
- 12.5. Klient súhlasí s tým, aby bol uvedený v referenčných listinách Dodávateľa v súvislosti s poskytovaním služieb podľa Zmluvy.
- 12.6. V prípade, že akékoľvek ustanovenie Zmluvy je alebo sa stane neplatným, neúčinným alebo vykonateľným, nie je tým dotknutá platnosť, účinnosť, alebo vykonateľnosť ostatných ustanovení Zmluvy, pokiaľ to nevylučuje v zmysle všeobecne záväzných právnych predpisov samotná povaha takého ustanovenia. Zmluvné strany sa zaväzujú bez zbytočného odkladu po tom, ako zistia, že niektoré z ustanovení Zmluvy je neplatné, neúčinné alebo nevykonateľné, nahradiť dotknuté ustanovenie ustanovením novým, ktorého obsah bude v čo najväčšej miere zodpovedať vôli Zmluvných strán v čase uzatvorenia Zmluvy.
- 12.7. Táto zmluva nadobúda platnosť dňom podpísania zmluvnými stranami a účinnosť deň po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.
- 12.8. Zmluvné strany vyhlasujú, že túto zmluvu uzatvorili slobodne, vážne a bez omylu, nebola uzatvorená v tiesni ani za nápadne nevýhodných podmienok, že si zmluvu prečítali a jej obsahu porozumeli, a na znak súhlasu s jej obsahom ju podpisujú.
- 12.9. Zoznam príloh – neoddeliteľnou súčasťou tejto zmluvy je:
Príloha č. 1 – Opis predmetu zákazky zahrňujúci Kópiu prieskumu – žiadosti o výkon auditu

V Bratislave, dňa _____

V Bratislave, dňa _____

Ratio Services, s.r.o.
Mgr. Katarína Hettychová
konateľ

Záchranná zdravotná služba Bratislava
Ing. PhDr. Michal Kováčik
riaditeľ

Príloha č. 1. ku Zmluve o odborných službách

Opis predmetu zákazky

Predmet zákazky: Audit kybernetickej bezpečnosti podľa zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Predmetom tejto zákazky je vykonanie auditu kybernetickej bezpečnosti (ďalej len „audit“) podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) v súlade s vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „vyhláška o audite“) u prevádzkovateľa základnej služby **Záchraná zdravotná služba Bratislava so sídlom Antolská 11, 850 07 Bratislava (ďalej len „ZZS BA“)** s cieľom overiť plnenie povinností podľa zákona a posúdiť zhodu prijatých bezpečnostných opatrení s požiadavkami podľa zákona a vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška“) prevádzkovateľa základnej služby. Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu.

Opis predmetu zákazky

- a) Posúdenie kompletnosti údajov potrebných na vykonanie auditu v rozsahu minimálnych náležitostí uvedených v prílohe č.2 vyhlášky NBÚ č.436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- b) Určenie rozsahu auditu spôsobom podľa prílohy č.3 vyhlášky NBÚ č.436/2019Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- c) Určenie metódy auditu podľa prílohy č.4 vyhlášky NBÚ č.436/2019Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- d) Pripravenie podkladov a pracovných dokumentov potrebných na výkon auditu,
- e) Preskúmanie bezpečnostnej dokumentácie a vyhodnotenie bezpečnostných opatrení v oblastiach:
 1. organizácie informačnej bezpečnosti,
 2. riadenia aktív, hrozieb a rizík,
 3. personálnej bezpečnosti,
 4. riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
 5. technických zraniteľností systémov a zariadení,
 6. riadenia bezpečnosti sietí a informačných systémov,
 7. riadenia prevádzky,
 8. riadenia prístupov,
 9. kryptografických opatrení,
 10. riešenia kybernetických bezpečnostných incidentov,
 11. monitorovania, testovania bezpečnosti a bezpečnostných auditov,
 12. fyzickej bezpečnosti a bezpečnosti prostredia,
 13. riadenia kontinuity procesov;
- f) vypracovanie kontrolného záznamu auditovaných bezpečnostných opatrení podľa prílohy č.4 vyhlášky NBÚ č.436/2019Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
- g) vyhodnotenie auditných zistení, oboznámenie prevádzkovateľa základnej služby so zistenými nedostatkami a zostavenie odporúčaných opatrení na ich odstránenie v písomnej forme,
- h) vypracovanie a predloženie záverečnej správy o výsledkoch auditu v rozsahu podľa § 2 vyhlášky NBÚ č.436/2019Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora, ktorá obsahuje najmä:
 - a) meno, priezvisko, číslo platného certifikátu audítora, dátum vyhotovenia a jeho podpis,
 - b) vymedzenie rozsahu vykonaného auditu,

- c) cieľ auditu,
- d) metódy vykonaného auditu,
- e) zhrnutie zistení výsledkov auditu a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,
- f) odporúčané nápravné opatrenia audítora pri zistení nedostatkov,
- g) dokumenty, najmä:
 - 1. kópia certifikátu audítora,
 - 2. kópia žiadosti o vykonanie auditu,
 - 3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,
 - 4. kontrolný záznam s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,
 - 5. harmonogram auditu,
 - 6. zoznam posúdenej dokumentácie,
 - 7. uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,
 - 8. zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov.

Obstarávateľ požaduje vykonanie auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti podľa vyhlášky NBÚ č.436/2019Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Minimálne náležitosti k vykonaniu auditu kybernetickej bezpečnosti podľa prílohy číslo 2. vyhlášky NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Minimálne technické a funkčné parametre prevádzky základných služieb:

1. Počet služieb verejného obstarávateľa zaradených do zoznamu základných služieb: 1
2. Počet informačných systémov s väzbou na základné služby: 2
3. Počet zamestnancov (používateľov základných služieb): 700
4. Počet pracovníkov zúčastňujúcich na prevádzke IS (interní a externí): 1+1
5. Počet lokalít v Bratislave – 2, počet staníc ZZS BA v rámci SR: 56
6. Počet tretích strán zúčastňujúcich na prevádzke IS: 0
7. Verejný obstarávateľ je zapojený do siete Sanet, SWAN
8. Verejný obstarávateľ nevlastní platný certifikát ISMS (ISO27001:2013).
9. Odhadovaný počet externých zaregistrovaných používateľov základných služieb: 0
10. Verejný obstarávateľ má zaregistrovaný informačný systém kategórie III.
11. V ZZS BA sa za posledné 2 roky nevyskytol závažný kybernetický bezpečnostný incident.
12. V ZZS BA nebol vykonaný audit kybernetickej bezpečnosti ani nebola uložená pokuta za porušenie povinnosti podľa zákona č. 69/2018 Z. z.

Obsah a náležitosti ponuky

Ponuka uchádzača bude obsahovať:

- Uchádzač, ktorý predkladá svoju ponuku v prípade, že ponuku nevypracoval sám, uvedie vo svojej ponuke osobu, ktorej služby využil alebo podklady pri jej vypracovávaní využil. Údaje uvedie v rozsahu meno a priezvisko, obchodné meno alebo názov, adresa pobytu, sídlo alebo miesto podnikania a identifikačné číslo, ak bolo pridelené,
- Doklady preukazujúce splnenie podmienok účasti – kópia certifikátu audítora
- Návrh na plnenie kritéria - cenovú ponuku (príloha č.2)
- Čestné vyhlásenie uchádzača, že nekoná v rozpore s vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Úspešný uchádzač bude vyzvaný na predloženie návrhu zmluvy, ktorý musí byť v súlade s Výzvou na predloženie ponuky (vrátane príloh) a s jeho ponukou.

Úspešný uchádzač je povinný do tretieho pracovného dňa nasledujúceho po dni nadobudnutia účinnosti Zmluvy predložiť Objednávateľovi na schválenie vypracovaný organizačný a časový harmonogram výkonu auditu, ktorého súčasťou bude identifikácia organizačných útvarov, procesov, auditovaných sietí a informačných systémov a fyzických lokalít Prevádzkovateľa základnej služby s uvedením jednotlivých časových úsekov auditu.

Termín realizácie predmetu zákazky: Úspešný uchádzač je povinný začať s vykonávaním auditu kybernetickej bezpečnosti podľa dohody zmluvných strán. Úspešný uchádzač je povinný vykonať audit a predložiť záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti **do konca októbra 2021**. Predpokladaný termín vykonania certifikačného auditu je **september – október 2021**