

## VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 4

ve smyslu § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů  
(dále jen „ZZVZ“ či „zákon“)

### 1. Identifikační údaje o veřejné zakázce a o zadavateli

#### 1.1. Identifikační údaje o veřejné zakázce

Název veřejné zakázky	Zajištění kybernetické bezpečnosti Střední školy Edvarda Beneše Břeclav, příspěvková organizace
Režim veřejné zakázky	nadlimitní
Druh zadávacího řízení	otevřené řízení
Druh veřejné zakázky	dodávky

#### 1.2. Identifikační údaje zadavatele

Název	Střední škola Edvarda Beneše Břeclav, příspěvková organizace
Sídlo	nábř. Komenského 1126/1, 690 25, Břeclav
IČO	60680342
Zastoupené	Mgr. Jiřím Uherem, ředitelem
Právní forma	příspěvková organizace
Profil zadavatele	<a href="https://zakazky.krajbezkorupce.cz/profile_display_138.html">https://zakazky.krajbezkorupce.cz/profile_display_138.html</a>

#### 1.3. Identifikační údaje smluvního zástupce zadavatele ve smyslu § 43 zákona

Název	Advokátní kancelář Petráš Rezek s.r.o.
Sídlo	Opletalova 1525/39, Nové Město, 110 00 Praha 1
IČO	07417641
Zastoupený/á	Mgr. Filipem Petrášem, společníkem a jednatelem
Právní forma	společnost s ručením omezeným
Kontaktní osoba	Mgr. Michal Uherek <a href="mailto:Verejne.zakazky@petrasrezek.cz">Verejne.zakazky@petrasrezek.cz</a>
na základě pověření společnosti	
Název	Regionální rozvojová agentura Východní Moravy
Sídlo	třída Tomáše Bati 5146, 760 01 Zlín
IČO	45659176
Zastoupený/á	RNDr. Otakarem Prudilem, ředitelem

### 2. Předmět vysvětlení zadávací dokumentace

Zadavatel na základě žádostí dodavatelů ze dne 19.05.2025 a 21.05.2025 poskytuje následující vysvětlení zadávací dokumentace k výše uvedené veřejné zakázce.

#### Dotaz č. 1:

S ohledem na Vaši důkladnou argumentaci k požadavku provozu SaaS služeb výhradně v datových centrech v rámci EU na platformách AWS, Google Cloud nebo Microsoft Azure uvádíme následující:

V posledních letech významní výrobci cloudových řešení (např. Oracle, IBM, SAP, Cisco, Extreme Networks a další) investovali do vlastních cloudových infrastruktur a datových center v rámci EU, které splňují přísné požadavky na kybernetickou bezpečnost, GDPR, lokalizaci dat, dostupnost a certifikace. Tyto platformy často nabízejí:

- Pokročilé bezpečnostní mechanismy, monitoring a řízení rizik srovnatelné s AWS, Google Cloud a Microsoft Azure.

- Smluvně garantovanou dostupnost služeb (SLA) a geografickou redundanci v rámci EU.
- Transparentní compliance s GDPR a dalšími evropskými regulacemi

*Je proto přípustné, aby kromě tří jmenovaných veřejných platform byly akceptovány i cloudové služby výrobců.*

*Umožní zadavatel provoz SaaS služeb i v cloudové platformě výrobce?*

*Obdobně jako bylo upřesněno v dotazu a odpovědi č.3 z VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 2 ze dne 12.2.2025, kdy za nás se jedná o dvě naprosto srovnatelné oblasti co do využití cloudu výrobce.*

#### **Odpověď na dotaz č. 1:**

Zadavatel tímto upřesňuje podmínky zadávací dokumentace následovně:

Uvedením konkrétních cloudových platform (AWS, Google Cloud, Microsoft Azure) v zadávací dokumentaci měl zadavatel na zřeteli bezpečnostní standardy a osvědčenou praxi v evropském regulačním rámci. Zadavatel však **akceptuje také provoz SaaS služeb na cloudových platformách výrobce** (například Oracle Cloud, IBM Cloud, SAP Cloud, Cisco Cloud, Extreme Networks Cloud a další), **pokud nabídka jednoznačně a prokazatelně splní veškeré požadavky zadávací dokumentace.**

Tímto upřesněním zadavatel rozšiřuje možnosti použití i o cloudové služby výrobců, pokud budou splněny veškeré požadavky na bezpečnost, provozní stabilitu, umístění dat a právní soulad, jak je stanoveno zadávací dokumentací a příslušnými právními předpisy.

V souvislosti s touto úpravou zadavatel předkládá novou přílohu č. 01\_Technická specifikace\_oprava3.

#### **Dotaz č. 2:**

*Na základě Vaší požadavku na dodání minimálně 4 ks SFP transceiverů (1GbE) a 2 ks SFP+ transceiverů (10GbE) bychom si dovolili požádat o upřesnění tohoto požadavku s ohledem na reálné potřeby typického nasazení firewallu v síťové infrastruktuře.*

*V běžných topologiích podnikových sítí, kde je firewall nasazován jako centrální prvek pro oddělení a ochranu jednotlivých segmentů sítě, je standardní praxí využití dvou rozhraní pro tzv. „inside“ (LAN) a „outside“ (WAN) konektivitu. Většina moderních firewallů, včetně modelů s více SFP/SFP+ porty, běžně využívá pouze 1–2 optické porty pro každý typ konektivity (1GbE a 10GbE).*

*Většina moderních firewallů je navržena s důrazem na modularitu a flexibilitu, a proto umožňuje přizpůsobení počtu aktivních SFP/SFP+ portů konkrétní topologii. V typické síťové topologii (například star topology nebo redundantní páteřní propojení) je běžné osadit pouze 2 ks SFP transceiverů (1GbE) a 2 ks SFP+ transceiverů (10GbE), což plně pokrývá potřeby běžného provozu i základní redundance.*

*Z tohoto důvodu bychom rádi požádali o možnost dodat pouze 2 ks SFP (1GbE) a 2 ks SFP+ (10GbE) transceiverů, což odpovídá reálným potřebám pro typické nasazení firewallu dle běžných síťových topologií a zároveň umožňuje efektivnější využití prostředků. Požadavek na vyšší počet transceiverů vede ke zbytečnému navyšování nákladů bez přímého přínosu pro funkci sítě.*

***Můžete prosím potvrdit, zda je možné upravit požadavek na počet transceiverů v souladu s běžnou praxí a skutečnými potřebami nasazení firewallu?***

*Pokud by z Vaší strany trvala potřeba osazení vyššího počtu transceiverů, prosíme o doplnění podrobnějších informací o plánované topologii, počtu segmentů a očekávaném zatížení sítě. Tyto informace nám umožní lépe pochopit specifika řešení a navrhnout vhodné technické parametry s důrazem na efektivitu a bezpečnost.*

#### **Odpověď na dotaz č. 2:**

Na základě zaslaného dotazu uchazeče zadavatel provedl odbornou technickou analýzu skutečných potřeb střední školy a konzultoval aktuální stav síťové infrastruktury. S přihlédnutím k požadavku na efektivní provoz, kybernetickou bezpečnost, zajištění dostatečné konektivity i finanční odpovědnost rozhodl zadavatel následovně:

**Zadavatel potvrzuje, že v rámci nabídky plně postačuje dodat 2 ks SFP (1GbE) a 2 ks SFP+ (10GbE) transceiverů. Takto stanovený počet reflektuje potřeby školy i odpovídá relevantním technickým normám a legislativě.**

#### **Odůvodnění tohoto rozhodnutí:**

Na základě zpětné vazby, interní odborné analýzy a prověření technické části specifikace zadavatel potvrzuje, že požadavek uchazeče přijímá, takto:

- u technické specifikace v části FW 4ks, se mění počet kusů u položky „porty“: počet SFP (1GbE) transceiverů upraven ze 4 ks na 2 ks,
- u položky „transceivery“: počet SFP (1GbE) transceiverů upraven ze 4 ks na 2 ks.

Počet SFP+ (10GbE) transceiverů zůstává v původním rozsahu, tedy 2 ks, bez jakékoliv změny.

Tato úprava reflektuje skutečné potřeby střední školy a odpovídá optimálnímu řešení jak z hlediska technické funkčnosti, tak z pohledu hospodárného vynakládání veřejných prostředků. Výsledné řešení zároveň plně zachovává požadovanou úroveň zabezpečení i rozvojovou flexibilitu školní infrastruktury.

1. **Technická a provozní dostatečnost pro školní síť:** Po provedené analýze je zřejmé, že zvolený počet transceiverů zcela splňuje aktuální i předpokládané požadavky na připojení páteřních i koncových částí školní sítě, ať už jde o běžný provoz, přístupy z laboratorů, učeben, kanceláří nebo pro zajištění zabezpečeného připojení do internetu. Zvolená konfigurace rovněž umožňuje základní provozní redundanci pro případ výpadku spojení.
2. **Efektivní a hospodárné vynakládání prostředků školy:** Vyšší počet transceiverů by znamenal zvýšené náklady, avšak bez reálného přínosu pro bezpečnost nebo provoz sítě školy. V souladu s § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, je zadavatel povinen postupovat hospodárně, efektivně a transparentně. Z tohoto pohledu je požadovaný počet optimální.
3. **Legislativní a bezpečnostní legitimita řešení:** Dosavadní technická analýza prokázala, že snížený počet transceiverů nijak neohrožuje zabezpečení školní sítě, její oddělení vůči veřejnému internetu ani plnění požadavků na kybernetickou bezpečnost školních informačních systémů podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti.
4. **Možnost budoucího rozšíření:** V případě, že by v budoucnu došlo ke změnám ve školní síťové infrastruktuře nebo vzniku nových potřeb (například při zavádění nových systémů či projektů), je možné kapacitu snadno rozšířit doplněním dalších SFP/SFP+ modulů dle aktuální poptávky.

**Závěr:** Uvedené řešení nejlépe odpovídá skutečným potřebám střední školy, dodržuje právní i technické požadavky a zároveň zajišťuje hospodárné nakládání s finančními prostředky. Proto zadavatel akceptuje požadavek uchazeče a potvrzuje, že dodávka 2 ks SFP (1GbE) a 2 ks SFP+ (10GbE) transceiverů je plně dostačující.

V souvislosti s touto úpravou zadavatel předkládá novou přílohu č. 01\_Technická specifikace oprava3.

### **3. Další informace**

#### **Informace 1:**

Vysvětlení zadávací dokumentace je poskytováno v souladu s § 98 zákona ve lhůtě 3 pracovních dnů od doručení žádosti. Zadavatel s ohledem na obsah vysvětlení zadávací dokumentace přiměřeně prodlužuje lhůtu pro podání nabídek v souladu s § 99 zákona.

#### **Informace 2:**

Lhůta pro podání nabídek uvedená v Oznámení o zahájení zadávacího řízení se mění takto:

Lhůta pro podání nabídek – den: 13.06.2025

Lhůta pro podání nabídek – čas: 11:00

Oprava Oznámení o zahájení zadávacího řízení je zveřejněna ve Věstníku veřejných zakázek.  
Aktuální lhůta pro podání nabídek je uveřejněna na profilu zadavatele.

**Přílohy:**

01\_Technická specifikace\_oprava3

*Ve Zlíně (dle data elektronického podpisu)*

Mgr. Filip Petráš, advokát  
Advokátní kancelář Petráš Rezek s.r.o.  
smluvní zástupce zadavatele