**Požadavky zadavatele v oblasti kybernetické bezpečnosti**

Zadavatel je v postavení provozovatele základní služby dle zákona č. 181/2014 Sb., resp. poskytovatele regulované služby v režimu vyšších povinností dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále oba zákony jen „**ZKB**“).

Účelem těchto podmínek je zajistit splnění povinností, které zadavateli ve vztahu k předmětu veřejné zakázky (technické a programové prostředky nabízené účastníkem zadávacího řízení za účelem splnění předmětu veřejné zakázky dále též jen „**nabízené řešení**“) vyplývají ze ZKB a jeho prováděcích předpisů.

* 1. Požadavky zadavatele ve vztahu k rizikovým technologiím

Zadavatel stanovil maximální přípustnou úroveň rizika spojeného s narušením důvěrnosti, integrity nebo dostupnosti, tj. kybernetické bezpečnosti, každé jednotlivé součásti nabízeného řešení **na úroveň nízká** ve smyslu přílohy č. 2 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**VKB**“), resp. přílohy č. 2 vyhlášky č. …/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „**maximální přípustná hodnota rizika**“ a „**VBOVR**“).

Nabízené řešení a osobní údaje v nabízeném řešení zpracovávané[[1]](#footnote-1) považuje zadavatel za aktiva ve smyslu § 2 VKB, resp. § 2 ZKB (tyto osobní údaje dále jen „**osobní údaje**“). Tato aktiva zadavatel dle ZKB ohodnotil na škálách uvedených v příloze č. 1 VKB, resp. v příloze č. 1 VBOVR, takto:

* důvěrnost: vysoká,
* integrita: kritická,
* dostupnost: střední.

Zadavatel je povinen v zadávacím řízení zohlednit následující akty Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“; technické a programové prostředky, ke kterým se tyto akty vztahují, resp. veškeré výrobky výrobců v těchto aktech stanovených, dále jen „**rizikové prostředky**“):

* varování NÚKIB ze dne 17. 12. 2018, sp. zn. 110-536/2018, č. j. 3012/2018-NÚKIB-E/110; a
* varování NÚKIB ze dne 10. 7. 2025, sp. zn. 350-544/2025-E, č. j. 4417/2025-NÚKIB-E/350 (veškeré tyto akty dále souhrnně jen „varování NÚKIB“).

Zadavatel je dále povinen stanovit rizika spojená s narušením kybernetické bezpečnosti osobních údajů, tj. rovněž údajů o zdravotním stavu pacientů zadavatele, a to zejména **pro případ, že nabízené řešení má vlastnost**, tj. nejedná se o vadu nabízeného řešení, a to bez ohledu na to, zda je taková vlastnost uvedena v dokumentaci nabízeného řešení, **která umožňuje osobám odlišným od zadavatele narušovat kybernetickou bezpečnost osobních údajů nebo spočívá v tom, že nabízené řešení narušuje kybernetickou bezpečnost osobních údajů automaticky nebo nabízené řešení umožňuje akceptovat povely osoby odlišné od zadavatele, které nejsou nezbytné pro plnění uzavřených smluv**, tj. např. provádění neoprávněného zpracování osobních údajů, neoprávněné odesílání i jen části osobních údajů mimo nabízené řešení, neoprávněné změny osobních údajů nebo neoprávněné omezování dostupnosti osobních údajů nebo nabízeného řešení (taková vlastnost dále jen „**backdoor**“).

Povinné hodnoty a podmínky povinně vstupující do hodnocení rizik jsou s ohledem na skutečnost, že zadavatel je mimo své postavení dle ZKB významným poskytovatelem zdravotních služeb:

* přítomnost každého rizikového prostředku v nabízeném řešení znamená hrozbu v úrovni: kritická;
* přítomnost backdoor v nabízeném řešení znamená hrozbu v úrovni: kritická a zranitelnost v úrovni: kritická.

Není-li některá hodnota vstupující do hodnocení rizik výše stanovena ani z výše uvedeného nevyplývá, resp. ji na pouze základě výše uvedeného nelze určit, zvolí ji účastník zadávacího řízení podle skutečnosti a tuto volbu uvede a řádně a přezkoumatelně odůvodní ve zprávě o hodnocení rizik.

**Tyto podmínky stanoví dvě možnosti, jak tyto požadavky zadavatele týkající se rizikových technologií splnit, a to buď provedením hodnocení rizik pro případ, že nabízené řešení obsahuje alespoň jeden rizikový prostředek, nebo čestným prohlášením pro případ, že nabízené řešení žádný rizikový prostředek neobsahuje.**

* 1. Hodnocení rizik

Zadavatel požaduje, aby účastník zadávacího řízení ve vztahu ke všem výskytům rizikových prostředků v nabízeném řešení a ve vztahu ke všem backdoor v nabízeném řešení **provedl hodnocení rizik** ve smyslu § 2 písm. d) VKB, resp. § 2 písm. e) VBOVR, a to postupy a s využitím škál dle příloh č. 1 a 2 VKB, resp. VBOVR, přičemž i to, co je v těchto přílohách VKB, resp. VBOVR uvedeno jako pouhý příklad, je pro účastníky tohoto zadávacího řízení povinné (toto hodnocení rizik dále jen „**hodnocení rizik**“).

Zadavatel proto požaduje, aby součástí nabídky byla podrobná a přezkoumatelná zpráva o provedení hodnocení rizik spojených s využitím rizikových prostředků v předmětu veřejné zakázky, která zadavateli umožní ve všech nezbytných detailech ověřit řádnosti provedení hodnocení rizik a která bude mít minimálně následující náležitosti (dále a výše jen „**zpráva o hodnocení rizik**“):

* + 1. podrobnou identifikaci všech rizikových prostředků zahrnutých v nabízeném řešení, a to včetně obchodního názvu, typu nebo verze, roku výroby, výrobce a sídla výrobce (postačuje stát),
		2. podrobnou identifikaci všech backdoor zahrnutých v nabízeném řešení, a to včetně obchodního názvu, typu nebo verze, roku výroby, výrobce a sídla výrobce (postačuje stát),
		3. hodnoty vstupních parametrů, které nejsou výslovně zadány touto zadávací dokumentací ani z ní nevyplývají,
		4. zdůvodnění volby hodnoty každého z těchto parametrů, které nejsou výslovně zadány touto zadávací dokumentací, a to mimo jiné s ohledem na roli rizikového prostředku a/nebo backdoor v nabízeném řešení,
		5. ve vztahu ke všem rizikovým prostředkům a backdoor určení výsledné hodnoty rizik spojených s užitím rizikových prostředků v nabízeném řešení, a
		6. technická **bezpečnostní opatření za účelem trvalého snížení hodnoty zjištěných rizik na úroveň maximální přípustné hodnoty rizika nebo na nižší úroveň (dále jen „bezpečnostní** opatření“), a to včetně řádného zdůvodnění účinnosti těchto bezpečnostních opatření, přičemž (zpráva o hodnocení rizik bude obsahovat výslovné prohlášení o splnění následujících odrážek):
			1. **veškeré náklady na pořízení a provoz těchto bezpečnostních opatření musí být součástí nabídkové ceny,**
			2. **tato bezpečnostní opatření nesmí vyžadovat vyšší složitost obsluhy nabízeného řešení, než jaká by byla v případě, kdyby nabízené řešení neobsahovalo žádný rizikový prostředek ani žádný backdoor,**
			3. **tato bezpečnostní opatření nesmí zvyšovat požadavky na personální zajištění obsluhy nabízeného řešení, a**
			4. **nabízené řešení včetně těchto bezpečnostních opatření musí jako celek splňovat veškeré požadavky zadavatel**e.

V případě, že bude dle zprávy o hodnocení rizik hodnota rizika ve vztahu ke kterémukoli rizikovému prostředku vyšší než maximální přípustná hodnota rizika, **požaduje zadavatel, aby součástí nabízeného řešení byla taková bezpečnostní opatření, která hodnotu rizik zjištěných při hodnocení rizik sníží** naúroveň maximální přípustné hodnoty rizika nebo na nižší úroveň.

Neúplnost, nesprávnost nebo nepřezkoumatelnost zprávy o hodnocení rizik ve vztahu ke všem rizikovým prostředkům, případně jiné její nedostatky, **může být důvodem pro vyloučení účastníka zadávacího řízení z další účasti v zadávacím řízení.**

Pokud bude dle zprávy o hodnocení rizik hodnota kteréhokoli rizika zjištěného při hodnocení rizik a po aplikaci bezpečnostních opatření vyšší než maximální přípustná hodnota rizika, nesplní nabídka účastníka zadávacího řízení zadávací podmínky. Zadavatel je v takovém případě **oprávněn účastníka zadávacího řízení vyloučit z další účasti v zadávacím řízení**.

* 1. Možnost čestného prohlášení

**V případě, že nabízené řešení neobsahuje žádný rizikový prostředek ani backdoor**, může účastník zadávacího řízení namísto provedení hodnocení rizik tuto skutečnost čestně prohlásit, tj. **doložit v nabídce čestné prohlášení**, že žádná položka nabízeného řešení neobsahuje žádné rizikové prostředky ani žádné backdoor, jak jsou tyto pojmy definovány v zadávací dokumentaci.

Zadavatel však upozorňuje, že v případě, že po uzavření smlouvy vyjde najevo, že toto čestné prohlášení neodpovídá skutečnosti, bude oprávněn odstoupit od smlouvy. Současně zadavatel v této souvislosti upozorňuje, že bude provádět testování (skenování) nabízeného řešení za účelem zjištění jeho kybernetických bezpečnostních zranitelností, které bude popisovat pomocí údajů z databáze CVE (Common Vulnerabilities and Exposures; dostupná z <https://cve.mitre.org/>), případně jiným vhodným způsobem.

* 1. Další požadavky zadavatele v oblasti kybernetické bezpečnosti

Za účelem trvalého udržování vysoké úrovně kybernetické bezpečnosti předmětu veřejné zakázky zadavatel požaduje, aby dodavatel:

* + 1. po celou dobu plnění smlouvy prováděl pravidelná technická a bezpečnostní školení osob na jeho straně přímo se podílejících na plnění smlouvy;
		2. po celou dobu plnění smlouvy dokumentoval změny přístupových oprávnění, které bude na své straně provádět;
		3. určil a průběžně aktualizoval havarijní kontaktní údaje pro zvládání kybernetických bezpečnostních událostí a incidentů, které bez zbytečného odkladu po nabytí účinnosti smlouvy poskytne zadavateli a oznámí zadavateli jakoukoliv jejich změnu bez zbytečného odkladu;
		4. poskytoval zadavateli součinnost při testování havarijního plánu vztahujícího se k předmětu veřejné zakázky, jakož i součinnost při provádění bezpečnostních, penetračních testů a testování zranitelností předmětu veřejné zakázky;
		5. při plnění předmětu veřejné zakázky využíval napojení na jednotnou adresářovou službu provozovanou na technologii Microsoft Active Directory zadavatele;
		6. využíval pro správu organizační struktury napojení na modul Identity Managementu informačního systému Enterprise Service Bus zadavatele;
		7. poskytovat součinnost při identifikaci a vyhodnocování potenciálních kybernetických bezpečnostních událostí v předmětu veřejné zakázky;
		8. zadavatel za účelem naplnění § 22 VKB, resp. § 23 VBOVR, provozuje systém log managementu systém TeskaLabs Logman.io; dodavatel poskytne veškerou nezbytnou součinnost pro napojení předmětu veřejné zakázky na tento systém log managementu tak, aby zadavatel rovněž ve vztahu k předmětu veřejné zakázky mohl plnit ustanovení § 22 VKB, resp. § 23 VBOVR;
		9. za účelem naplnění § 18 VKB, resp. § 19 VBOVR, poskytne dodavatel zadavateli kompletní komunikační schéma předmětu veřejné zakázky pro zajištění konfigurace bezpečnosti síťové infrastruktury a dále dodavatel poskytne veškerou nezbytnou součinnost pro správnou konfiguraci systému pokročilých síťových analýz Greycortex Mendel, aby zadavatel rovněž ve vztahu k předmětu veřejné zakázky mohl plnit ustanovení § 18 VKB, resp. § 19 VBOVR.
1. Pojmy „osobní údaje“ a „zpracování osobních údajů“ se vykládají podle nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). [↑](#footnote-ref-1)