

SMLOUVA O DODÁVCE MODULU PŘEDMĚTY A STUDIJNÍ PLÁNY STUDIJNÍHO INFORMAČNÍHO SYSTÉMU A SOUVISEJÍCÍCH SLUŽBÁCH

č. UKRUK/574155/2023-24

(dále jen „*Smlouva*“)

Smluvní strany:

Univerzita Karlova

se sídlem: Ovocný trh 560/5, 116 36 Praha 1

zastoupená: Mgr. Martinem Maňáskem, kvestorem

IČO: 00216208, DIČ: CZ00216208

bank. spojení: Česká spořitelna, a.s., pobočka v Praze 1, č. účtu: 909909339/0800

ID datové schránky: piyj9b4

(dále jen „*Objednatel*“)

a

Aricoma Digital s.r.o.

se sídlem: Vinohradská 1511/230, 100 00 Praha 10

registrovaný: u Městského soudu v Praze, oddíl C, vložka 12440

zastoupený: Ing. Tomáš Rutrle, MBA, jednatel

IČO: 47117087, DIČ: CZ47117087

tel.: +420 910 972 106 / +420 601 576 247

bank. spojení: Československá obchodní banka, a. s., č. účtu: 217570063/0300

ID datové schránky: 8sqaah

(dále jen „*Dodavatel*“)

(dále společně Objednatel a Dodavatel jako „*smluvní strany*“)

uzavřely v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“), a podle ust. § 61 an. zákona č. 121/2000 Sb., autorský zákon, v platném znění (dále jen „**autorský zákon**“), tuto Smlouvu takto:

1. Úvodní prohlášení

- 1.1. Univerzita Karlova (dále též „**UK**“), v souladu se zákonem č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, v platném znění (zákon o vysokých školách), jako Objednatel prohlašuje, že je oprávněna uzavřít a řádně plnit tuto Smlouvu a závazky v ní obsažené.
- 1.2. Společnost Aricoma Digital s.r.o. jako Dodavatel prohlašuje, že je právnickou osobou řádně založenou a zapsanou podle českého právního řádu v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 12440, a že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.
- 1.3. Dodavatel prohlašuje, že ve smyslu § 4b) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**zákon o střetu zájmů**“), není a ani jeho poddodavatelé nejsou obchodní společnostmi, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona o střetu zájmů nebo jím ovládaná osoba, vlastní podíl představující alespoň 25% účasti společníka v obchodní společnosti.
- 1.4. Dodavatel prohlašuje, že se na něj, jeho poddodavatele a ani na jím nabízené plnění nevztahují mezinárodní sankce ve smyslu § 2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů.

2. Východiska a účel Smlouvy

- 2.1. Tato Smlouva je uzavřena na základě výsledku veřejné zakázky nazvané „**RUK – ÚVT – Dodávka modulu Předměty a studijní plány Studijního informačního systému na Univerzitě Karlově**“ (dále jen „**Veřejná zakázka**“) zadávané v dynamickém nákupním systému s názvem „**RUK – ÚVT – Dynamický nákupní systém na rozvoj studijního informačního systému Univerzity Karlovy**“ (dále jen „**Dynamický nákupní systém**“ nebo „**DNS**“) zavedeném v souladu s § 139 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“).
- 2.2. Veřejná zakázka souvisí s realizací projektu zadavatele Transformace pro VŠ na UK (reg. číslo NPO_UK_MŠMT-16602/2022) financovaného prostřednictvím Národního plánu obnovy pro oblast vysokých škol pro roky 2022-2024 (dále jen „**Projekt**“).
- 2.3. Záměrem Objednatele je dodávka modulu Předměty a studijní plány (dále jen „**Software**“ nebo též „**Předmět plnění**“) Studijního informačního systému UK (dále též „**SIS**“ nebo též „**SIS UK**“), včetně získání potřebných licencí k jeho užití, jeho uvedení do provozu na UK, a dodání dokumentace, jak je uvedeno dále v této Smlouvě.
- 2.4. Dodavatel je podnikatelem v oblasti poskytování IT služeb a prohlašuje, že je schopen Objednateli dodat plnění blíže specifikované v této Smlouvě.
- 2.5. Objednatel prohlašuje, že Software je součástí SIS UK a představuje tedy významný informační systém dle § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZoKB**“), a tímto musí splňovat všechny nároky kladené na informační systém této kategorie.

- 2.6. Účelem této Smlouvy je určit podmínky vytvoření díla a rozsah služeb, které Dodavatel dodá Objednateli a které Dodavatel bude poskytovat Objednateli v souvislosti s převzetím a nasazením Software u Objednatele.
- 2.7. Smluvní strany se zavazují poskytovat si navzájem součinnost vyplývající z této Smlouvy, nezbytnou pro řádné plnění povinností vyplývajících z této Smlouvy. Smluvní strany se zejména zavazují informovat se bez zbytečného odkladu o všech skutečnostech a okolnostech, které mají nebo mohou mít vliv na řádné plnění povinností Smluvních stran dle této Smlouvy.

3. Předmět smlouvy

- 3.1. Předmětem této Smlouvy je vytvoření a dodávka modulu Předměty a studijní plány pro Studijní informační systém Univerzity Karlovy (dále jen „**SIS UK**“) a zajištění podpory provozu v parametrech stanovených Zadávací dokumentací, touto Smlouvou a dle požadavků Objednatele.
- 3.2. Předmětem smlouvy je provedení komplexního plnění sestávajícího z následujících dílčích plnění:
 - 3.2.1. **Poskytnutí licence Software** a zajištění poskytnutí příslušných software třetích stran nutných pro správnou funkčnost dodávaného řešení, za podmínek:
 - a) časově, množstevně a místně neomezené licence,
 - b) výhradní licence k Software,
 - 3.2.2. **Dodávka Předmětu plnění a poskytnutí implementačních služeb** pro vytvoření testovacího a produkčního prostředí, a to způsobem potřebným pro řádné nasazení a provoz Software minimálně v rozsahu stanoveném touto Smlouvou). Plnění bude zahrnovat zejména:
 - a) dodávku licencí Software a dalšího SW (podpůrný SW třetích stran),
 - b) dodávku Software splňujícího požadavky Objednatele specifikované v Příloze č. 1a, č. 1b a č. 3 této Smlouvy, včetně dodání, instalace a konfigurace programového vybavení třetích stran, které je nezbytné pro provoz Software u Objednatele,
 - c) instalaci iniciační verze Software či jejích dílčích částí a konfiguraci na hardwarovém vybavení Objednatele,
 - d) příprava a provedení unit a integračních testů, systémových testů a výkonnostních testů dle kap. 5.3.1. Přílohy č. 1b této Smlouvy,
 - e) propojení dodaného řešení do celkového funkčního celku s ostatním HW a/nebo SW a aplikačním vybavením Objednatele,
 - f) součinnost s Objednatel a třetími stranami při vytváření rozhraní Software na informační systémy Objednatele,
 - g) technickou pomoc a konzultace poskytované Objednateli při testování Software a jeho rozhraní,
 - h) zaškolování administrátorů Software v souladu s kap. 6.1.3. Přílohy č. 1b této Smlouvy,
 - i) implementaci Software do produkčního prostředí, akceptace produkčního provozu,
 - j) dodání kompletní dokumentace k Software v rozsahu uvedeném v kap. 5.2. a 6.3. Přílohy č. 1b této Smlouvy,
 - k) udělení příslušných uživatelských a souvisejících oprávnění dle článku 14 této Smlouvy,
 - l) předání zdrojových kódů k Software dle čl. 14.3. Smlouvy,
 - m) případné další služby, které byly součástí nabídky Dodavatele,

n) záruku na Software dle technických požadavků
(dále souhrnně jen „*Implementace*“).

3.2.3. **Poskytování servisních činností a technické podpory k Předmětu plnění** (dále jen „*Správa a podpora*“) zahrnující:

- a) správu Software, zejména běžnou údržbu Software, řešení závad, poruch a nestandardních stavů,
- b) poskytování technické podpory klíčovým uživatelům Objednatele při obsluze a užívání Software, zejména zodpovídání telefonických a písemných dotazů, podávání technických informací o Software a poskytování asistence klíčovým uživatelům prostřednictvím vzdáleného přístupu. Klíčoví uživatelé budou ze strany Objednatele určeni nejpozději před zahájením testovacího provozu,
- c) implementace opravených verzí Software a dodávka upravené související dokumentace,

a to způsobem popsaným v článku 5 této Smlouvy, přičemž Dodavatel bere na vědomí, že součástí Správy a podpory je řádné poskytování součinnosti Dodavatele při integraci všech systémů Objednatele.

(dále jen souhrnně „*Předmět plnění*“)

- 3.3. Detailní popis Předmětu plnění a popis způsobu naplnění požadavků Objednatele je uveden v Přílohách č. 1a, č. 1b a č. 3 této Smlouvy. Předmět plnění rovněž zahrnuje plnění, která nejsou výslovně uvedena v této Smlouvě či jejích přílohách, ale jejichž realizace je nezbytná pro provedení Předmětu plnění tak, aby byl naplněn účel Smlouvy.
- 3.4. Předmětem této Smlouvy je taktéž doprava do místa plnění dle čl. 4.3. Smlouvy a veškeré další činnosti podmiňující uvedení Předmětu plnění do provozu a jeho řádnou funkčnost.
- 3.5. Dodavatel prohlašuje, že se seznámil s rozsahem a povahou Předmětu plnění. Jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k řádnému užívání předmětu Smlouvy.
- 3.6. Dodavatel se zavazuje, že Předmět plnění je v souladu s právními předpisy, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že materiály, výrobky, postupy a poskytované služby vyhovují požadavkům na Předmět plnění a veškerým podmínkám a požadavkům uvedeným v zadávacích podmínkách k Veřejné zakázce.
- 3.7. Dodavatel prohlašuje, že Předmět plnění není plněním nemožným a pečlivě zvážil všechny možné důsledky uzavření této Smlouvy.
- 3.8. Dodavatel je povinen realizovat Předmět plnění dle této Smlouvy za podmínek uvedených v kapitolách a přílohách Zadávací dokumentace k Veřejné zakázce, v této Smlouvě, jejích přílohách a dodatcích uzavřených postupem dle této Smlouvy.
- 3.9. Nestanoví-li tato Smlouva jinak, stanovují Smluvní strany aplikační přednost smluvních dokumentů v následujícím pořadí: přílohy Smlouvy, samotný text Smlouvy.
- 3.10. Dodavatel se zavazuje, že odevzdá Předmět plnění (či jeho dílčí části), jakož i dokumenty, které se k nim vztahují, řádně a včas Objednateli v ujednaném množství, jakosti a provedení.
- 3.11. Dodavatel se zavazuje postupovat při dodávce Předmětu plnění s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s Předmětem plnění, které Objednatel Dodavateli poskytne nebo s pokyny jím pověřených osob.

- 3.12. Dodavatel se dále zavazuje přijmout potřebná opatření tak, aby byla zajištěna integrita, důvěrnost a dostupnost dat uložených v Software v souladu s účelem této Smlouvy a aktuální dokumentací Software. Dodavatel neodpovídá za data chybně zadaná Objednatelem a ani za zpracování těchto dat Objednatelem v systémech třetích stran.
- 3.13. Dodavatel se zavazuje poskytovat plnění tak, aby byly dodrženy požadované lhůty plnění dle článků 4 a 5 této Smlouvy.
- 3.14. Objednatel je oprávněn průběžně kontrolovat provádění Předmětu plnění (či jeho dílčích částí) prostřednictvím svého Vedoucího týmu. Úkolem a oprávněním Vedoucího týmu je zejména komunikace s Dodavatelem a dohlížení na plnění Předmětu plnění tak, aby byly zabezpečeny požadavky Objednatele na kvalitu plnění dle Smlouvy. K řádnému výkonu role Vedoucího týmu se Dodavatel zavazuje poskytnout veškerou součinnost. Vedoucí týmu obou smluvních stran jsou specifikovány v Příloze č. 4 této Smlouvy.
- 3.15. Nedohodnou-li se Smluvní strany jinak, je Vedoucí týmu Objednatele oprávněn účastnit se veškerých činností realizačního týmu Dodavatele a kontrolovat veškeré plnění spočívající v Implementaci a Správě a podpoře. Dodavatel vyhradí na své straně Vedoucího týmu dle Přílohy č. 4 Smlouvy, která bude s Vedoucím týmu Objednatele komunikovat a poskytovat veškeré informace nezbytné pro výkon oprávnění Vedoucího týmu Objednatele. Kontrola plnění Smlouvy však nesmí vést k nadměrnému zatížení Dodavatele a ohrožovat možnost řádného plnění Smlouvy Dodavatelem.

4. Doba a místo dodání

- 4.1. Dodavatel se zavazuje provést dodávku Předmětu plnění dle čl. 3.2.1 a čl. 3.2.2. Smlouvy v následujících dílčích termínech plnění:

Dílčí plnění	Mezní termín plnění
a) Zahájení projektu, kickoff	do 14 dnů od nabytí účinnosti Smlouvy
b) Vývoj, implementace a integrace iniciační verze modulu Předměty a studijní plány SIS UK <ul style="list-style-type: none"> - poskytnutí licence Software a zajištění poskytnutí příslušných software třetích stran nutných pro správnou funkčnost Software, - dodávka a kompletní implementace Software do testovacího prostředí (dle čl. 3.2.1.,3.2.2. písm. a) až i) Smlouvy)	nejpozději do 30. 5. 2024
c) Převedení Software do produkčního provozu, akceptace produkčního provozu (dle čl. 3.2.2. písm. j) až m) Smlouvy)	nejpozději do 30. 6. 2024

- 4.2. Dodavatel se zavazuje poskytovat službu Správy a podpory dle čl. 3.2.3. Smlouvy po dobu 24 měsíců od akceptace produkčního provozu Software.
- 4.3. Místem plnění je sídlo Objednatele.
- 4.4. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Dodavatel oprávněn poskytovat službu Správa a podpora (nebo její dílčí části) také vzdáleným přístupem, a to takovým způsobem, kterým nedojde k narušení systému řízení bezpečnosti Objednatele.

- 4.5. Školení obsluhy Software, která jsou součástí Předmětu plnění, budou prováděna prezenční formou nebo distanční formou v závislosti na roli osoby, která se školení účastní.
- 4.6. Povinnost Dodavatele odevzdat Předmět smlouvy je splněna jeho včasným a řádným předáním Objednateli, a současně akceptací Předmětu plnění.
- 4.7. Převzetím se pro účely této Smlouvy rozumí okamžik podpisu akceptačního protokolu bez výhrad oprávněnými zástupci obou Smluvních stran, uvedenými v čl. 22.6. této Smlouvy.
- 4.8. Objednatel je oprávněn nepřevzít Předmět plnění, pokud neodpovídá požadavkům uvedeným v zadávacích podmínkách Veřejné zakázky, Přílohách č. 1a, č. 1b a č. 3 Smlouvy, či vykazuje jakékoliv jiné právní či faktické vady.
- 4.9. Zdržení dodávky Předmětu plnění (či jeho dílčí části) zapříčiněné vyšší mocí, mezi což se počítá např. porucha strojů, nezaviněný výpadek dodávek energie a surovin nebo zdržení na straně výrobců a dodavatelů Dodavatele, a vlivy, které Dodavatel nemohl ovlivnit bez neúměrného finančního zatížení, nejsou pro Objednatele důvodem k odstoupení od této Smlouvy.

5. Správa a podpora Předmětu plnění

- 5.1. Účelem tohoto článku Smlouvy je stanovení rozsahu podmínek provádění servisní činnosti a poskytování provozní podpory Dodavatelem, a to na celém Předmětu plnění dle článku 3 této Smlouvy a v místě provedení instalace dle článku 4 (tzv. servis on-site) nebo distanční formou (není-li nutný zásah v místě provedení instalace).
- 5.2. Správu a podporu provádí Dodavatel na základě povinností popsanych v tomto článku 5 Smlouvy.
- 5.3. Dodavatel se zavazuje zahájit poskytování hrazené Správy a podpory ke dni akceptace produkčního provozu. Správa a podpora bude poskytována po dobu 24 měsíců od akceptace produkčního provozu Software.
- 5.4. Dodavatel se zavazuje:
 - 5.7.1. poskytovat Správu a podporu s péčí řádného hospodáře odpovídající podmínkám sjednaným v této Smlouvě;
 - 5.7.2. poskytovat Správu a podporu v rozsahu a v kvalitě definované v tomto článku 5 Smlouvy.
- 5.5. Dodavatel se zavazuje využívat k řádnému poskytování Správy a podpory evidenční systém požadavků vlastněný a provozovaný Objednatelem (dále jen „ServiceDesk“), v němž bude probíhat zejména hlášení vad a požadavků ze strany Objednatele, vyřizování těchto požadavků a další komunikace Smluvních stran. Dodavatel je povinen evidovat a vyřizovat veškeré požadavky související s poskytováním Správy a podpory v ServiceDesku.
- 5.6. Současně je Dodavatel povinen zřídit Hot-line technické podpory, s níž bude moci Objednatel telefonicky komunikovat za v místě a čase běžné hovorné a jemuž bude moci písemně zasílat své požadavky. Hot-line bude poskytována na telefonním čísle +420 603 378 294. Komunikační platforma pro písemnou komunikaci bude dohodnuta mezi smluvními stranami na kickoff projektu.
- 5.7. Pro hlášení poruch prostřednictvím Hot-line technické podpory dle čl. 5.6. Smlouvy musí být Dodavatel dostupný v režimu 5x8 v pracovních dnech v době od 8:00 hod do 16:00 hod. Objednatel je povinen při nahlášení incidentu/vady uvést také telefonické spojení na oprávněného zástupce pro možnost vyžádání doplňujících informací ze strany Dodavatele.

- 5.8. Objednateli vzniká nárok na odstranění nestandardního nebo poruchového stavu/incidentu či požadavku Objednatele (dále jen „Poruchy“) okamžikem ohlášení jeho výskytu. Poruchou se rozumí jakákoliv technická změna vůči akceptovanému provoznímu stavu na plnění dodaném Dodavatelem dle článku 3 této Smlouvy.
- 5.9. Servisní činnost popsanou v tomto článku provádí Dodavatel vždy na základě hlášení poruchy Objednatelem. Není-li mezi Smluvními stranami sjednáno jinak, je Dodavatel povinen jakékoliv vady na Předmětu plnění odstranit v následujících lhůtách:

Kategorie vady	Definice vady	Reakční doba	Lhůta pro odstranění vady
A	Vážné vady s nejvyšší prioritou, které mají kritický dopad na funkčnost či užití Předmětu plnění dle této Smlouvy nebo jeho části a dále vady, které znemožňují užívání Předmětu plnění dle této Smlouvy nebo jeho části Objednatelem nebo způsobují vážné provozní problémy.	2 hod	8 hodin
B	Vada, která svým charakterem nespadá do kategorie A. Vážné vady způsobující zhoršení výkonnosti a funkčnosti či užití předmětu plnění dle této Smlouvy nebo jeho části. Předmět plnění dle této Smlouvy nebo jeho část má omezení nebo je částečně nefunkční. Jedná se o odstranitelné vady, které způsobují problémy při užívání či provozování plnění předmětu dle této Smlouvy nebo jeho části Objednatelem, ale umožňují provoz či částečné využití.	6 hod	4 prac. dny
C	Vada, která svým charakterem nespadá do kategorie A nebo kategorie B. Vady snadno odstranitelné s minimálním dopadem na funkcionality, funkčnost či užití předmětu plnění dle této Smlouvy nebo jeho části.	12 hod	8 prac. dnů

- 5.10. Kategorii incidentů dle čl. 5.9. této Smlouvy stanovuje Objednatel. Dodavatel určuje a plně odpovídá za stanovení způsobu odstranění Poruchy, za analýzu příčiny Poruchy, za stanovení posloupnosti jednotlivých činností a za stanovení doby, kdy tyto činnosti budou prováděny. K tomu je Objednatel povinen poskytnout nezbytnou potřebnou součinnost, tedy takovou, kterou si Dodavatel nemůže jakkoliv zajistit sám. V případě, kdy Objednatel Dodavateli požadovanou součinnost neposkytne, se pozastavuje čas plnění SLA v neprospěch Objednatele.
- 5.11. Lhůty pro provedení servisní činnosti uvedené v čl. 5.9. této Smlouvy začínají běžet od okamžiku potvrzení přijetí požadavku na provedení servisní činnosti Dodavatelem. Do požadovaných časových limitů se nezapočítává doba mimo nastavenou pracovní dobu uvedenou v čl. 5.7. této Smlouvy.
- 5.12. Dodavatel bez zbytečného odkladu informuje Objednatele o odstranění Poruchy prostřednictvím ServiceDesku. Po provedení servisní činnosti bude Dodavatelem sepsán zápis do ServiceDesku k příslušnému ticketu, ticket bude uzavřen. Pokud Objednatel nesouhlasí, reaguje nejdéle do 2 kalendářních dnů změnou stavu ticketu s odůvodněním v ServiceDesku. Ticket se tak vrací do otevřeného stavu.

- 5.13. Dodavatel je oprávněn Objednateli vyúčtovat náklady spojené s odstraňováním Poruchy podle tohoto článku v případě, že bude prokazatelně zjištěno, že Porucha nastala v důsledku porušení povinností podle této Smlouvy Objednatelem.
- 5.14. V případě, že Správa a podpora nebude poskytována řádně z důvodů zásahu Vyšší moci, nezohledňuje se tato doba do lhůt pro odstranění Poruch stanovených čl. 5.9. Smlouvy.
- 5.15. Dodavatel se zavazuje zajistit nejpozději do 10 pracovních dnů od uskutečnění jakékoli změny Software provedené Dodavatelem po dokončení Předmětu plnění na základě této Smlouvy, která uvedla Software do nesouladu s dokumentací k Software, aktualizaci této dokumentace.
- 5.16. Dodavatel je povinen pravidelně a neprodleně informovat Objednatele o dostupnosti všech aktualizací Software, a to včetně aktualizací vzniklých v důsledku řešení incidentů. Objednatel není povinen souhlasit s provedením implementace žádné aktualizace nabídnuté Dodavatelem. V případě, že Objednatel takovou aktualizaci odmítne, bude o této skutečnosti sepsán písemný protokol. V případě, že se u Objednatele vyskytne incident v přímém důsledku chyby, na kterou Dodavatel Objednatele upozornil dle první věty tohoto ustanovení a odmítl-li Objednatel implementaci aktualizace, jejíž implementace prokazatelně chybu odstraňovala, není Dodavatel v prodlení s odstraněním touto chybou způsobeného incidentu.
- 5.17. Pokud dojde k poruše Software v důsledku vnějších událostí, které nezpůsobil Dodavatel (např. vandalství, terorismus, válka, občanské nepokoje, požáry, povodně a jiné živelné události, výbuchy, úniky chemických a radioaktivních materiálů a podobně), je Objednatel povinen uhradit Dodavateli náklady na práci servisního technika, jakož i všechny ostatní účelně vynaložené náklady spojené s provedením servisní činnosti, a to podle aktuálního ceníku Dodavatele ke dni vyúčtování.
- 5.18. Smluvní pokuty za nedodržení lhůt a požadavků definovaných v tomto článku jsou uvedeny v článku 18 této Smlouvy.

6. Realizační tým, poddodavatelé

- 6.1. Dodavatel se zavazuje využít při plnění této Smlouvy v daných pozicích pouze členy realizačního týmu uvedené v Příloze č. 4 této Smlouvy. Jakákoliv změna členů realizačního týmu uvedených v Příloze č. 4 této Smlouvy musí být předem písemně schválena Objednatelem. Dodavatel se v takovém případě zavazuje nahradit člena realizačního týmu takovou osobou, která disponuje potřebnou odborností na výkon dané role a současně splňuje kvalifikační požadavky Objednatele dle Zadávací dokumentace či jejích příloh k Dynamickému nákupnímu systému (byly-li pro danou roli stanoveny). Pro vyloučení jakýchkoliv pochybností Objednatel uvádí, že jedna fyzická osoba nesmí zastávat více pozic v realizačním týmu.
- 6.2. Objednatel je oprávněn písemně požadovat v nezbytně nutných a opodstatněných případech změnu člena realizačního týmu, respektive členů realizačního týmu. V takovém případě je Dodavatel povinen ve lhůtě do 30 kalendářních dnů od písemného požadavku Objednatele nahlásit Objednateli změnu původního člena realizačního týmu novým členem, který splňuje požadavky Objednatele dané Zadávací dokumentací či jejími přílohami k DNS (byla-li pro danou roli v realizačním týmu stanovena kvalifikační kritéria).
- 6.3. V případě postupu dle čl. 6.1. nebo čl. 6.2. této Smlouvy je Dodavatel povinen neprodleně doložit Objednateli veškeré doklady, ze kterých vyplyne splnění uvedených kvalifikačních požadavků Objednatele. Objednatel po posouzení předložených dokladů písemně

odsouhlasí nebo neodsouhlasí navrženou změnu člena realizačního týmu, příp. požádá o doplnění dalších informací či dokladů, a to do 5 kalendářních dnů od doručení nahlášení změny. Objednatel je povinen požadavek na změnu člena realizačního týmu Dodavatele řádně odůvodnit.

- 6.4. Dodavatel je povinen dále specifikovat rozsah částí Předmětu plnění a poskytovaných služeb, které budou prováděny prostřednictvím třetí osoby – poddodavatele (dále jen „Poddodavatel“). Dodavatel musí v souladu se ZZVZ Poddodavatele identifikovat. Dále se Dodavatel zavazuje, že plnění dodané prostřednictvím Poddodavatele budou v souladu se všemi podmínkami této Smlouvy. Tímto není dotčena výlučná odpovědnost Dodavatele za poskytování řádného plnění dle této Smlouvy.
- 6.5. Dodavatel se zavazuje plnění dle této Smlouvy dodávat sám nebo s využitím Poddodavatelů uvedených v Příloze č. 5 této Smlouvy. Jakákoliv dodatečná změna osoby Poddodavatele nebo rozsahu plnění svěřeného Poddodavateli dle vymezení v Příloze č. 5 Smlouvy musí být předem písemně schválena Objednatel. Pokud se má změna týkat Poddodavatele, prostřednictvím kterého Dodavatel v DNS prokazoval splnění kvalifikace, musí nový Poddodavatel splňovat tutéž minimální kvalifikaci jako Poddodavatel původní a uvedené musí být Objednateli bez jakýchkoli pochybností doloženo. Povinnost Dodavatele dle předchozí věty se uplatní i pro případy, kdy by plnění původně svěřené Poddodavateli realizoval Dodavatel sám. Objednatel svůj souhlas s případnou změnou Poddodavatele neodepře bezdůvodně.
- 6.6. Dodavatel je povinen ve všech smlouvách uzavřených s Poddodavatelem zajistit závazek poskytnout subjektům provádějícím audit a kontrolu nezbytné informace týkající se poddodavatelských činností. V případě porušení tohoto ustanovení není Objednatel povinen uhradit práce zhotovené Poddodavatelem.
- 6.7. Všechny osoby, které Dodavatel při plnění Smlouvy použije, musí splňovat veškeré předpoklady vyžadované pro tuto činnost Smlouvou a účinnými právními předpisy, musí být bezúhonné a musí být plně seznámeny s důsledky možné trestní odpovědnosti právnických osob. Provedení činnosti dle Smlouvy Poddodavatelem nezavazuje Dodavatele jeho odpovědnosti vůči Objednateli. Dodavatel odpovídá Objednateli za činnost dle Smlouvy, kterou svěřil Poddodavateli, ve stejném rozsahu, jako by ji poskytoval sám.

7. Spolupráce Objednatele a Dodavatele

- 7.1. Každá ze smluvních stran jmenuje svého zplnomocněného zástupce, Vedoucího týmu, který ji bude výlučně zastupovat v realizačních záležitostech souvisejících s plněním této Smlouvy. Jména a kontakty Vedoucího týmu za Objednatele a Dodavatele, složení týmu Dodavatele jsou uvedeny v Příloze č. 4 Smlouvy.
- 7.2. Vedoucí týmu na straně Dodavatele odpovídá za řízení činnosti případných poddodavatelů.
- 7.3. Vedoucí týmu na straně Objednatele odpovídá za řízení činnosti případných třetích stran, jejichž součinnost je nezbytná pro úspěšné plnění závazků Objednatele dle této Smlouvy.
- 7.4. Smluvní strany zajistí svým zplnomocněným zástupcům dle čl. 7.1. této Smlouvy dostatečné pravomoci pro výkon jejich činností.
- 7.5. Objednatel je oprávněn jmenování svého zplnomocněného zástupce dle čl. 7.1. této Smlouvy změnit, je však povinen o takové změně předem písemně informovat Dodavatele.
- 7.6. Změnu ve jmenování svého zplnomocněného zástupce dle čl. 7.1. této Smlouvy a náhradu dalších členů realizačního týmu Dodavatele identifikovaných v Příloze č. 4 Smlouvy je Dodavatel oprávněn provést pouze po vzájemné písemné dohodě smluvních stran a po

předložení dokladů k jeho kvalifikaci (v souladu s čl. 6.3. Smlouvy).

- 7.7. Objednatel si vyhrazuje právo zřizovat po dobu platnosti této Smlouvy podle potřeby organizační struktury projektu a v případech, kdy to bude nezbytné pro plnění závazků Dodavatele vyplývajících z této Smlouvy, požadovat zastoupení Dodavatele v těchto strukturách.
- 7.8. Způsob řízení prací, které jsou předmětem této Smlouvy, je rámcově popsán v kap. 6.1.1. Přílohy č. 1b této Smlouvy.

8. Komunikace mezi smluvními stranami

- 8.1. Nebude-li smluvními stranami dohodnuto jinak, budou spolu smluvní strany komunikovat:
 - a) písemně poštou na adresy uvedené v záhlaví této Smlouvy,
 - b) prostřednictvím datových schránek,
 - c) elektronickou poštou mezi zplnomocněnými zástupci,
 - d) osobně prostřednictvím zplnomocněných zástupců,
 - e) prostřednictvím ServiceDesk, nebo
 - f) způsoby uvedenými v kap. 6.1.2. Přílohy č. 1b této Smlouvy.
- 8.2. Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé straně doručena buď osobně, nebo doporučeným dopisem či jinou formou doporučeného poštovního styku, nebo prostřednictvím informačního systému datových schránek není-li dohodnuto mezi smluvními stranami jinak.
- 8.3. Písemnost, která má být dle této smlouvy doručena druhé straně (oznámení, výpověď, odstoupení od smlouvy, reklamace vad apod.), je doručena dnem jejího převzetí Vedoucím týmu druhé smluvní strany nebo dnem, kdy byla doručena osobně nebo prostřednictvím držitele poštovní licence do sídla této smluvní strany, nebo doručením do datové schránky.
- 8.4. Komunikace elektronickou poštou je považována za doručenu okamžikem potvrzení převzetí přijímající stranou, resp. okamžikem odpovědi přijímající strany.
- 8.5. Komunikace mezi smluvními stranami bude probíhat v českém jazyce.

9. Změny smlouvy

- 9.1. Kterákoliv ze Smluvních stran je oprávněna písemně navrhnout změny Smlouvy, jejích příloh, vč. změny specifikace Předmětu plnění, služby Správy a podpory Software. Objednatel není povinen navrhovanou změnu akceptovat. Dodavatel se zavazuje vynaložit veškeré úsilí, které po něm lze rozumně požadovat, aby změnu požadovanou Objednatelem akceptoval. Dodavatel se zavazuje provést hodnocení dopadů kteroukoliv Smluvní stranou navrhovaných změn na termíny plnění, celkovou cenu, funkcionalitu Software a požadavků na součinnost Objednatele. Dodavatel je povinen toto písemné hodnocení a návrh řešení provést bez zbytečného odkladu, nejpozději do 14 kalendářních dnů ode dne doručení návrhu kterékoliv Smluvní strany druhé Smluvní straně.
- 9.2. Jakékoliv změny závazku ze Smlouvy, které nejsou vyhrazenou změnou ve smyslu článku 20 této Smlouvy, budou řešeny výhradně postupem a v souladu s § 222 ZZVZ.

10. Cena za plnění

- 10.1. Objednatel je povinen uhradit Dodavateli cenu za Předmět plnění, a to ve výši a postupem určenými dle této Smlouvy. Celková cena v sobě zahrnuje veškeré vynaložené náklady Dodavatele související s poskytnutím plnění.
- 10.2. Objednatel se zavazuje zaplatit Dodavateli za **dodávku Předmětu plnění** dle čl. 3.5.1. a 3.5.2. této Smlouvy celkovou cenu uvedenou v Příloze č. 2 Smlouvy, položka A. Licence a implementace (celkem A1 až A5).
- 10.3. Objednatel se zavazuje hradit Dodavateli za **poskytování Správy a podpory** dle článku 5 této Smlouvy měsíční odměnu uvedenou v Příloze č. 2 Smlouvy, položka B. Zajištění provozní a technické podpory.
- 10.4. Dodavatel nese odpovědnost za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.
- 10.5. Ceny uvedené v tomto článku Smlouvy jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady Dodavatele nutné k řádnému a včasnému dodání Předmětu plnění (např. správní a místní poplatky, vedlejší náklady, náklady spojené s dopravou do místa plnění, náklady související s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů Předmětu plnění, zajištění veškerých legislativních povinností apod.). Součástí ceny je i cena za služby a dodávky, které nejsou výslovně uvedeny, ale Dodavatel jakožto odborník o nich ví nebo má vědět, že jsou nezbytné pro řádné a včasné plnění. Dodavatel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazku ze Smlouvy včetně správních poplatků.

11. Platební podmínky

- 11.1. Dodavatel je oprávněn fakturovat dodávku Předmětu plnění dle čl. 3.5.1. a 3.5.2. této Smlouvy odpovídající položkám A1 až A5 v příloze č. 2 Smlouvy (odpovídající licenci a implementaci Software) po akceptaci produkčního provozu bez výhrad ze strany Objednatele a ve lhůtě dle čl. 4.1. písm. c) Smlouvy, a to na základě akceptačního protokolu, v souladu s akceptační procedurou uvedenou v čl. 13 této Smlouvy.
- 11.2. Cena za poskytování služeb Správy a podpory dle článku 10.3. této Smlouvy bude fakturována za každý kalendářní měsíc, v němž byly služby poskytovány. Daňový doklad bude Dodavatelem vystaven nejpozději do 10 kalendářních dnů od ukončení daného kalendářního měsíce. V případě, že služby nebudou poskytovány po celou dobu kalendářního měsíce, sníží se fakturovaná částka poměrným způsobem s ohledem na dobu, po kterou byly služby skutečně poskytovány.
- 11.3. Vyúčtování ceny za plnění dle této Smlouvy provede Dodavatel na základě daňového dokladu – faktury splňující veškeré podstatné náležitosti dle zvláštních právních předpisů, zejména náležitosti uvedené v § 28 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a náležitosti obchodní listiny ve smyslu ustanovení § 435 Občanského zákoníku, zejména:
 - a) evidenční číslo daňového dokladu,
 - b) název a sídlo Objednatele a Dodavatele,
 - c) číslo Smlouvy a den jejího uzavření,
 - d) název projektu: Transformace pro VŠ na UK, registrační číslo: NPO_UK_MSMT16602/2022, SC A1,
 - e) datum vystavení daňového dokladu a datum uskutečnění zdanitelného plnění,

- f) označení banky a číslo účtu, na který má být zaplacen a který je registrován u příslušného správce daně a je zveřejněn způsobem umožňujícím dálkový přístup ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění,
 - g) cenu za plnění (základ daně), sazbu daně a její výši, pokud nejde o plnění dle ust. § 92e zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění,
 - h) číselný kód klasifikace CZ – CPA, a v případě plnění dle ust. § 92e zákona o DPH poznámku „daň odvede zákazník“,
 - i) IČO a DIČ Dodavatele a Objednatele.
- 11.4. Pro vyloučení pochybností se uvádí, že Dodavatel není oprávněn vystavit fakturu dle čl. 11.1. této Smlouvy dříve, než po provedení všech příslušných akceptačních procedur dle článku 13 této Smlouvy.
- 11.5. Přílohou faktury dle čl. 11.1. této Smlouvy bude kopie akceptačního protokolu podepsaného pověřenými zástupci obou Smluvních stran v souladu s čl. 22.6. této Smlouvy.
- 11.6. Faktury jsou splatné do třiceti (30) kalendářních dnů od prokazatelného doručení faktury Objednateli.
- 11.7. Objednatel je oprávněn do data splatnosti vrátit fakturu, která neobsahuje požadované náležitosti, a která obsahuje jiné cenové údaje nebo jiný druh plnění než dohodnuté ve Smlouvě s tím, že doba splatnosti nové (opravené) faktury začíná znovu běžet ode dne jejího doručení Objednateli.
- 11.8. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu Objednatele ve prospěch účtu Dodavatele.
- 11.9. Objednatel neposkytuje zálohové platby.
- 11.10. V případě, že se Dodavatel stane nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, je povinen o tom neprodleně písemně informovat Objednatele. Bude-li Dodavatel ke dni uskutečnění zdanitelného plnění veden jako nespolehlivý plátcem, bude část ceny za služby dle této Smlouvy odpovídající dani z přidané hodnoty uhrazena přímo na účet správce daně v souladu s ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. O tuto částku bude ponížena celková cena a Dodavatel obdrží cenu dle této Smlouvy bez DPH. V případě, že se Dodavatel stane nespolehlivým plátcem ve smyslu tohoto bodu, má Objednatel současně právo od této Smlouvy odstoupit.

12. Práva a povinnosti smluvních stran

- 12.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.
- 12.2. Objednatel se zavazuje k poskytnutí součinnosti podle zdůvodněných požadavků Dodavatele, zahrnující zejména (nikoliv však výlučně):
- a) zpřístupnění a zajištění provozu hardwarového vybavení pro instalaci a provoz Software u Objednatele, a to minimálně v testovací instanci, a to včetně poskytnutí licencí Operačních systémů a virtualizační platformy v případě využití technologií podporovaných ze strany Objednatele, které jsou definovány v Příloze č. 1b Smlouvy.
 - b) spolupráci na řízení prací, blíže specifikovanou v článku 7 této Smlouvy,

- c) spolupráci při přípravě, provádění a vyhodnocení testů Software,
 - d) další součinnosti, na kterých se Objednatel a Dodavatel písemně dohodnou.
- 12.3. Objednatel bude udržovat testovací prostředí Software, do něhož bude instalován opravený Software dodaný Dodavatelem pro účely akceptačních testů.
 - 12.4. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy takovým způsobem, aby nedocházelo k prodlení s plněním jednotlivých termínů a k prodlení splatnosti jednotlivých peněžních závazků.
 - 12.5. Objednatel poskytne Dodavateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy.
 - 12.6. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob, nebo jimi pověřených osob, nebo statutárního orgánu Smluvních stran.
 - 12.7. Smluvní strany se zavazují, že v případě změny svého sídla, pracoviště a svých zástupců budou o této změně druhou Smluvní stranu informovat nejpozději do 15 kalendářních dnů.
 - 12.8. Objednatel se zavazuje, že bude na žádost Dodavatele spolupracovat či poskytne součinnost případným dalším dodavatelům Dodavatele.
 - 12.9. Objednatel je povinen zaplatit Dodavateli odměnu za Předmět plnění v souladu s ustanovením článků 10 a 11 této Smlouvy.
 - 12.10. Dodavatel je povinen upozorňovat Objednatele včas na všechny hrozící vady svého plnění či potenciální výpadky v rámci plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění Smlouvy potřebné, a o nichž Dodavatel ví, nebo vědět má a může.
 - 12.11. Dodavatel je povinen bezodkladně a s vyvinutím přiměřeného úsilí řešit ve spolupráci s Objednatelem veškeré překážky v plnění předmětu této Smlouvy.
 - 12.12. Dodavatel je povinen upozornit Objednatele bez zbytečného odkladu na chybnost nebo nevhodnost jím udělených pokynů nebo poskytnutých informací, jestliže tuto chybnost nebo nevhodnost mohl zjistit při vynaložení odborné péče. Trvá-li Objednatel na provedení pokynů nebo použití informací, na jejichž nevhodnost byl upozorněn ze strany Dodavatele, neodpovídá Dodavatel za jakoukoli újmu vzniklou v důsledku provedení pokynů, na jejichž nevhodnost Objednatele prokazatelně předem upozornil. Objednateli nevzniká nárok na smluvní pokutu za porušení povinnosti, které bylo způsobeno v přímém důsledku chybného či nevhodného pokynu Objednatele nebo informace jím poskytnuté Dodavateli, na které Dodavatel prokazatelně předem Objednatele upozornil a Objednatel na jejich provedení nebo použití prokazatelně trval.
 - 12.13. Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při provádění bezpečnostního auditu u Objednatele. Objednatel je dále oprávněn vyvolat bezpečnostní audit u Dodavatele dle své potřeby.
 - 12.14. Dodavatel je povinen k náhradě škody bez ohledu na to, zda je škoda kryta pojištěním. Škoda může být, byť částečně, uhrazena pojišťovnou dle sjednaného pojištění odpovědnosti za škodu.
 - 12.15. Objednatel uděluje Dodavateli souhlas s použitím základních informací o této Smlouvě (název společnosti, předmět a místo realizace plnění a cena) pro účely doložení referencí Dodavatele.
 - 12.16. Dodavatel se v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů ve znění pozdějších právních předpisů stane osobou povinnou spolupůsobit při výkonu finanční kontroly a plnit veškeré povinnosti, které mu jsou tímto zákonem uloženy. Tímto nejsou dotčeny ostatní povinnosti Dodavatele

vyplývající ze Smlouvy.

- 12.17. Ve smyslu čl. 140 Nařízení Evropského parlamentu a rady č. 1303/2013 ze dne 17. prosince 2013 o společných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti, Evropském zemědělském fondu pro rozvoj venkova a Evropském námořním a rybářském fondu, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti a Evropském námořním a rybářském fondu a o zrušení nařízení Rady (ES) č. 1083/2006, ve znění pozdějších předpisů je Dodavatel povinen uchovávat veškerou dokumentaci související s realizací předmětu této Smlouvy, a to minimálně po dobu 10 let od roku následujícího po roce, v němž došlo k vypořádání příspěvku Objednatel ze strany poskytovatele dotace.
- 12.18. Dodavatel je povinen dodržovat pravidla publicity Národního plánu obnovy pro oblast vysokých škol.
- 12.19. Dodavatel včetně svých Poddodavatelů se zavazuje splnit podmínku, že všichni jeho skuteční vlastníci s podílem přesahujícím alespoň 25 % a zaměstnanci, kteří se podíleli na přípravě nabídky k Veřejné zakázce nejsou ve střetu zájmů z důvodu veřejné funkce dle § 2 odst. 1 písm. c) zákona č. 159/2006, o střetu zájmů, v platném znění nebo z důvodu střetu zájmů zaměstnanců ve smyslu rodinných, osobních či citových vazeb, politické nebo národnosti spřízněnosti, hospodářských důvodů, finančního nebo jiného přímého nebo nepřímého osobního zájmu s Objednatelem či jeho zaměstnanci. Nesplnění povinností Dodavatele dle tohoto ustanovení Smlouvy se považuje za podstatné porušení Smlouvy.
- 12.20. Dodavatel prohlašuje, že on sám i jeho případný Poddodavatel (Poddodavatelé) není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 sb., o střetu zájmů nebo, jím ovládaná osoba, vlastní podíl představující alespoň 25% účasti společníka v obchodní společnosti. Dodavatel prohlašuje, že se na nabízené plnění nevztahují sankce EU a že on ani jeho Poddodavatel (Poddodavatelé) není osobou, subjektem či orgánem uvedeným na sankčním seznamu EU, nebo osobou, subjektem či orgánem, na které se vztahuje zákaz zadat nebo dále plnit veřejnou zakázku (čl. 5k Nařízení Rady (EU) č. 2022/576 ze dne 8.4.2022, kterým se mění Nařízení (EU) č. 833/2014, o omezujících opatřeních vzhledem k činností Ruska, destabilizujícím situaci na Ukrajině).

13. Předání a akceptace předmětu plnění

- 13.1. Po dokončení implementace Předmětu plnění dle čl. 3.2.1. – čl. 3.2.2. této Smlouvy bude Předmět plnění Dodavatelem předán do testovacího provozu, a to na základě oboustranně potvrzeného Předávacího protokolu. Objednatel bude provádět po dobu 30 kalendářních dní od podpisu Předávacího protokolu testování Předmětu plnění a Dodavatel se zavazuje poskytnout Objednateli po tuto dobu nezbytnou součinnost při odstraňování vad a nedostatků. Předmětem testování v rámci testovacího provozu je ověření souladu dodaného Předmětu plnění se specifikací plnění uvedenou v přílohách č. 1a, č. 1b a č. 3 této Smlouvy.
- 13.2. Po uplynutí lhůty uvedené v čl. 13.1. této Smlouvy bude Dodavatelem vyhotoven Akceptační protokol, který bude v závislosti na úspěšnosti provedeného testování/ověřování obsahovat jeden z následujících závěrů:
- a) Předmět plnění je akceptován bez výhrad – V rámci testovacího provozu bylo ověřeno, že dodané plnění zcela odpovídá specifikaci plnění uvedené v přílohách č. 1a, č. 1b a č. 3 této Smlouvy. Ve vztahu k akceptaci dodávky bude plnění akceptováno bez výhrad, pokud nebyly identifikovány žádné podstatné vady, přičemž za

podstatnou vadu je považována vada, kdy poskytnuté plnění neumožňuje dosažení účelu sjednaného touto Smlouvou pro každou, byť jen dílčí část plnění. Odstranění podstatných vad bude vždy předloženo v písemné formě pro jednotlivou konkrétní vadu samostatně.

- b) Předmět plnění je akceptován s výhradami – V rámci testovacího provozu bylo ověřeno, že dodané plnění je funkční a nebrání zamýšlenému užití, avšak neodpovídá zcela specifikaci plnění uvedené v přílohách č. 1a, č. 1b a č. 3 této Smlouvy. Nesplněné požadavky či nalezené vady budou uvedeny v akceptačním protokolu. Dodavatel se zavazuje odstranit vady plnění uvedené v akceptačním protokolu nejpozději do termínu dohodnutého s Objednatelem. V případě nedodržení termínu pro odstranění vad, na kterém se Dodavatel dohodl s Objednatelem, se uplatní sankční podmínky pro prodloužení s termínem odstranění vad.
 - c) Předmět plnění je neakceptován a vrácen k přepracování – V rámci testovacího provozu bylo zjištěno, že dodané plnění není funkční, nebo jeho vady brání zamýšlenému užití. Nesplněné požadavky či vady plnění bránící jeho využití budou uvedeny v akceptačním protokolu. Dodavatel se zavazuje odstranit vady plnění uvedené v akceptačním protokolu v termínu dohodnutém s Objednatelem, nejpozději do 14 kalendářních dnů. V případě nedodržení termínu pro odstranění vad, na kterém se Dodavatel dohodl s Objednatelem, se uplatní sankční podmínky pro prodloužení s termínem odstranění vad. Nedodržení termínu pro odstranění vad bude navíc považováno za podstatné porušení této Smlouvy.
- 13.3. Po dokončení akceptačního řízení k testovacímu provozu dle čl. 13.2. této Smlouvy podepíše smluvní strany akceptační protokol.
 - 13.4. Po úspěšném akceptačním řízení dle čl. 13.2. této Smlouvy dojde k převedení Předmětu plnění do produkčního provozu, tj. Dodavatel zajistí nejpozději do 5 pracovních dnů od podpisu akceptačního protokolu dle čl. 13.3. této Smlouvy spuštění konečné a ostré verze Předmětu plnění. Uvedení Předmětu plnění do ostrého provozu bude potvrzeno oboustranným podpisem akceptačního protokolu o spuštění Předmětu plnění do produkčního provozu.
 - 13.5. Smluvní strany jsou oprávněny dohodnout se písemně na odlišných akceptačních procedurách.
 - 13.6. Akceptační a předávací protokol zpracovává vždy Dodavatel s platností originálu ve dvou vyhotoveních s tím, že po jejich podpisu osobami oprávněnými obdrží každá ze smluvních stran jedno vyhotovení.

14. Duševní vlastnictví, práva třetích osob

- 14.1. Objednatel nabývá dnem uhrazení ceny za příslušné plnění časově, množstevně a teritoriálně neomezené právo (licenci) užit Software či jeho dílčí části ke všem způsobům užití. Tato licence je výhradní a Dodavatel není oprávněn poskytnout licenci k Předmětu plnění třetí osobě, ani s Předmětem plnění v rozsahu udělené licence jakkoliv nakládat.
- 14.2. Objednatel je oprávněn udělit třetí osobě podlicenci k Software či Software dále upravovat dle svých potřeb. Práva Objednatele vyplývající z udělené licence trvají i po ukončení účinnosti této Smlouvy.
- 14.3. Dodavatel se zavazuje předávat Objednateli na základě vyžádání Objednatele zdrojovou formu Software a aktualizovanou dokumentaci k Software, a to na oboustranně dohodnutém médiu či oboustranně dohodnutým postupem. Dokumentací k Software dle

tohoto bodu se rozumí dokumentace dle čl. 3.2.2. písm. j) této Smlouvy.

- 14.4. Dodavatel se zavazuje odškodnit Objednatele za všechny důvodné a přiměřené nároky třetích osob z titulu porušení jejich chráněných práv souvisejících s plněním Dodavatele podle této Smlouvy, pokud Objednatel:
- oznámi Dodavateli bez zbytečného odkladu písemně a uceleně uplatnění jakéhokoliv podobného nároku třetích osob,
 - neuzná sám předmětný nárok,
 - zplnomocní Dodavatele k vypořádání takového nároku soudní nebo mimosoudní cestou,
 - neučiní bez předchozí konzultace s Dodavatelem jakékoliv právní úkony ve věci předmětných nároků.
- 14.5. Cena za udělení licence je již zahrnuta v ceně uvedené v čl. 10.2. této Smlouvy.

15. Kybernetická bezpečnost

- 15.1. Dodavatel tímto bere na vědomí, že Objednatel je osobou povinnou dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „**ZoKB**“) a plní povinnosti vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „**VyKB**“).
- 15.2. Dodavatel tímto bere na vědomí, že je pro Objednatele při zajišťování smluvního vztahu založeného touto Smlouvou v pozici významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VyKB a v pozici možného budoucího provozovatele ve smyslu § 2 písm. g) VyKB. V případě, že se Dodavatel stane provozovatelem ve smyslu shora uvedeného, bude o tomto informován Objednatelem.
- 15.3. Objednatel je v souladu s ustanovením § 4 odst. 4 ZoKB a ve spojení s přílohou č. 7 VyKB povinen stanovit závazná bezpečnostní opatření, která se vztahují na Dodavatele při plnění předmětu této smlouvy (dále jen „**Bezpečnostní opatření**“).
- 15.4. Dodavatel je povinen v rozsahu plnění této Smlouvy naplnit všechna Bezpečnostní opatření uvedená v Příloze č. 6 této smlouvy – Bezpečnostní požadavky.
- 15.5. Dodavatel se dále zavazuje:
- poskytnout na vyžádání Objednateli dokumenty, zprávy, a obdobné vstupy, které budou prokazovat naplnění Bezpečnostních požadavků;
 - na požádání s Objednatelem konzultovat kdykoli v průběhu účinnosti této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Bezpečnostních požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;
 - neprodleně informovat Objednatele o všech významných změnách v naplnění Bezpečnostních požadavků, které nastanou kdykoli v průběhu účinnosti této Smlouvy;
 - bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Bezpečnostních požadavků, pokud stávající řešení přestalo být funkční a efektivní;
 - bezodkladně a prokazatelně informovat Objednatele o kybernetických bezpečnostních událostech a incidentech, které mohou ovlivnit poskytování služeb dle této Smlouvy;
 - při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k Bezpečnostním opatřením a jejichž následkem může vzniknout újma nebo nesoulad s platnými a účinnými právními předpisy či jinými předpisy vztahujícími se k poskytování služeb dle této

Smlouvy.

- 15.6. Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění.

16. Ochrana a utajení informací

- 16.1. Za důvěrné informace se bez ohledu na formu jejich zachycení považují informace tvořící obchodní tajemství podle jiných právních předpisů a dále informace, které Objednatel za důvěrné označí.
- 16.2. Pro nakládání s osobními údaji, s nimiž Dodavatel může přijít do styku v průběhu plnění, a pro ochranu těchto údajů při jejich zpracování platí v plném rozsahu ustanovení zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.
- 16.3. Bude-li to nezbytné k plnění předmětu Smlouvy, poskytne Objednatel Dodavateli pro plnění předmětu Smlouvy zabezpečený vzdálený přístup do databáze SIS UK, která je umístěna u Objednatele. V této databázi jsou zpracovávány osobní údaje osob, studenty či zaměstnanci Objednatele, a dále ostatní uživatelé SIS UK. Dodavateli bude do této databáze poskytnut přístup nezbytný k plnění předmětu Smlouvy, a to po dobu platnosti a účinnosti Smlouvy. Pracovníci Dodavatele nejsou oprávněni nahlížet na data ve zpřístupněné databázi bez vědomí a bez výslovného souhlasu Objednatele. Dodavatel je povinen zajistit, že vzdálený přístup do databáze budou mít pouze osoby, které jsou v době trvání této Smlouvy v pracovněprávním nebo obdobném smluvním vztahu s Dodavatelem, podílejí se na plnění předmětu Smlouvy a jsou písemně zavázány vůči Objednateli povinností mlčenlivosti. Zabezpečený vzdálený přístup Dodavatele do databáze bude omezen na vyjmenované pracovníky Dodavatele, kterým bude Objednatelem přiděleno přístupové jméno a heslo. Zabezpečený vzdálený přístup bude možný pouze z předem dohodnutých síťových adres a omezen na přístupové protokoly dohodnuté mezi zplnomocněnými zástupci Objednatele a Dodavatele.
- 16.4. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li dále v tomto článku výslovně sjednáno jinak. Zavazují se tímto, že podniknou všechny kroky k zabezpečení těchto informací.
- 16.5. Povinnost oboustranného utajení důvěrných informací platí bez ohledu na ukončení účinnosti této Smlouvy.
- 16.6. Smluvní strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací.
- 16.7. Smluvní strany jsou povinny respektovat veškerá práva a oprávněné zájmy druhé smluvní strany a její obchodní značky, loga a ochranné známky v souladu s právními předpisy a vnitřními předpisy Objednatele.
- 16.8. Dodavatel se zavazuje, že každou tiskovou zprávu nebo jinou informaci určenou ke zveřejnění a týkající se uzavření této Smlouvy a průběhu jejího plnění předloží ke schválení a korektuře Objednateli a nebude ji publikovat bez předchozího písemného schválení Objednatelem.
- 16.9. Objednatel se zavazuje, že návrhy na zveřejnění, které mu Dodavatel předloží v souladu s ustanovením čl. 16.8. této Smlouvy, posoudí bez zbytečného odkladu a nebude Dodavateli bezdůvodně bránit v tom, aby využil skutečnost uzavření této Smlouvy a významné události v průběhu jejího plnění k propagačním účelům.
- 16.10. Žádné ustanovení této Smlouvy nebrání žádné ze stran v poskytnutí informací třetí straně

či ve zveřejnění informací, pokud povinnost poskytnutí těchto informací vyplývá z platných právních předpisů.

- 16.11. Veškerá data Objednatele, k nimž Dodavatel získá v průběhu platnosti této Smlouvy přístup, jsou považována za důvěrné informace ve smyslu čl. 16.1. této Smlouvy a Dodavatel je nesmí použít k jiným účelům než k plnění předmětu Smlouvy.

17. Odpovědnost za vady, záruka, záruční doba

- 17.1. Dodavatel odpovídá za to, že každá část výsledku Implementace Software má ke dni její akceptace vlastnosti stanovené touto Smlouvou či jejími přílohami, a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.
- 17.2. Dodavatel poskytuje záruku za jakost Software po dobu 24 měsíců od okamžiku podpisu akceptačního protokolu k produkčnímu provozu Software.
- 17.3. Po dobu poskytování Správy a podpory budou veškeré záruční a mimozáruční vady Software řešeny plněním Dodavatele poskytovaným v rámci těchto služeb. Toto ustanovení se dále žádným způsobem nedotýká práv Objednatele z vadného plnění.
- 17.4. Cestovní náklady, náklady na materiál a jiné náklady, které Dodavateli vzniknou v souvislosti s odstraněním vad předmětu plnění dle tohoto článku, nese v plné výši Dodavatel.
- 17.5. Dodavatel je povinen odstranit vady Předmětu plnění ve lhůtách stanovených čl. 5.9. této Smlouvy.
- 17.6. Při vadě způsobené neodborným zásahem je Dodavatel oprávněn účtovat Objednateli servisní zásah dle platného ceníku Dodavatele.

18. Sankční ujednání

- 18.1. Nedodrží-li Dodavatel lhůtu stanovenou v čl. 4.1. písm. c) Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 500.000, – Kč (bez DPH).
- 18.2. Nedodrží-li Dodavatel lhůty pro odstranění vad dle čl. 5.9. této Smlouvy, je povinen uhradit Objednateli následující smluvní pokuty:

Kategorie vady	Výše smluvní pokuty
A	15.000, – Kč za každých i započatých 8 hodin (pracovní den 8-16 hod) prodlení a jednotlivou vadu
B	5.000, – Kč za každých i započatých 8 hodin (pracovní den 8-16 hod) prodlení a jednotlivou vadu
C	1.000, – Kč za každých i započatých 8 hodin (pracovní den 8-16 hod) prodlení a jednotlivou vadu

- 18.3. Nedodrží-li Objednatel lhůtu splatnosti faktury uvedenou v čl. 11.6. této Smlouvy, je povinen uhradit Dodavateli smluvní pokutu ve výši 0,05 % fakturované částky za každý započatý kalendářní den prodlení.
- 18.4. Poruší-li Dodavatel povinnosti vyplývající z čl. 16 této Smlouvy, je povinen zaplatit Objednateli smluvní pokutu ve výši 500.000, – Kč (bez DPH) za každé porušení takové povinnosti.
- 18.5. V případě porušení povinnosti poskytovat plnění dle této Smlouvy v daných pozicích

prostřednictvím členů realizačního týmu uvedených v Příloze č. 4 této Smlouvy a provádět jejich změny pouze se souhlasem Objednatele dle čl. 6.1. této Smlouvy, má Objednatel nárok na smluvní pokutu ve výši 1.000, – Kč (bez DPH) za každý započatý den poskytování plnění dle této Smlouvy na příslušné pozici osobou neuvedenou v Příloze č. 4 této Smlouvy.

- 18.6. V případě porušení povinnosti Dodavatele plnit tuto Smlouvu prostřednictvím Poddodavatelů uvedených v Příloze č. 5 této Smlouvy v rozsahu uvedeném v Příloze č. 5 této Smlouvy nebo povinnosti provádět jejich změny v souladu s čl. 6.5. této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 5.000,– Kč (bez DPH) za každý započatý den poskytování plnění dle této Smlouvy prostřednictvím Poddodavatelů neuvedených v Příloze č. 5 této Smlouvy, v rozporu se zněním Přílohy č. 5 této Smlouvy nebo Dodavatelem, pokud neprokázal kvalifikaci v souladu s čl. 6.5. této Smlouvy.
- 18.7. Smluvní strany sjednávají, že výši smluvních pokut uvedených v této Smlouvě považují za přiměřenou.
- 18.8. Výše uvedené smluvní pokuty je možné v případě závažného porušení povinností Dodavatele sčítat.
- 18.9. Splatnost smluvních pokut činí 30 kalendářních dnů od doručení nároku na její uhrazení druhé Smluvní straně.

19. Náhrada újmy

- 19.1. Zaplacením smluvní pokuty není dotčeno právo Smluvních stran na úhradu způsobené újmy vzniklé v souvislosti s plněním předmětu Smlouvy v plné výši.
- 19.2. Každá ze Smluvních stran je povinna nahradit způsobenou škodu druhé Smluvní straně, a to v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
- 19.3. Dodavatel odpovídá za způsobenou újmu porušením povinnosti dle této Smlouvy, opomenutím nebo zásadně nekvalitním dodáním Předmětu plnění v plné výši. Dodavatel se zároveň zavazuje Objednatele odškodnit za jakékoliv škody, které mu v důsledku porušení povinností Dodavatele vzniknou na základě pravomocného rozhodnutí soudu či jiného státního orgánu.
- 19.4. Dodavatel odpovídá Objednateli za škodu v plné výši, která mu vznikne z důvodu vrácení jakékoliv dotace na Projekt či příspěvku, který obdržel nebo měl obdržet na krytí nákladů plnění dle této Smlouvy, a které mu byly odňaty nebo neposkytnuty z důvodů stojících na straně Dodavatele.
- 19.5. Dodavatel nese odpovědnost za ztrátu, poškození či únik dat v důsledku vadného poskytnutí služeb ze strany Dodavatele.
- 19.6. Žádná ze Smluvních stran není povinna nahradit škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytnout službu nebo Licence nebo jejich části s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.
- 19.7. Žádná ze Smluvních stran nemá povinnost nahradit škodu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě škody ve smyslu § 2913 čl. 2 občanského zákoníku.

- 19.8. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě škody bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě škody.
- 19.9. Každá ze Smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta.
- 19.10. Náhrada újmy se řídí platnými ustanoveními vztahujícími se k náhradě majetkové a nemajetkové újmy stanovené zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- 19.11. Jakákoliv ustanovení týkající se omezení výše či druhu škody se nepřipouští.

20. Výhrada změny dodavatele

- 20.1. Objednatel si ve smyslu § 100 odst. 2 ZZVZ vyhrazuje právo realizovat změnu v osobě Dodavatele v průběhu plnění dle této Smlouvy, budou-li splněny následující podmínky:
- a) nastanou důvody umožňující Objednateli ukončit tento smluvní vztah výpovědí nebo odstoupením od této Smlouvy pro důvody na straně Dodavatele nebo bude-li tato Smlouva ukončena ze strany Dodavatele před uplynutím doby jejího trvání,
 - b) Dodavatel bude nahrazen dodavatelem, jehož nabídka se umístila jako další v pořadí při hodnocení nabídek ve Veřejné zakázce (dále jen „Nahrazující dodavatel“),
 - c) Nahrazující dodavatel prokáže Objednateli splnění všech podmínek účasti ve smyslu § 36 ZZVZ, které byly ve Veřejné zakázce stanoveny,
 - d) Nahrazující dodavatel splní veškeré další podmínky pro uzavření této Smlouvy ve smyslu § 104 ZZVZ, pokud byly ve Veřejné zakázce tyto další podmínky stanoveny,
 - e) Nahrazující dodavatel předloží Objednateli originály dokladů o své kvalifikaci, pokud je Objednatel již nemá k dispozici,
 - f) Objednatel u Nahrazujícího dodavatele zjistí údaje o jeho skutečném majiteli, a to postupem dle § 122 odst. 5 nebo 6 ZZVZ,
 - g) Nahrazující dodavatel nebo jeho případní poddodavatelé nejsou obchodními společnostmi, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 sb., o střetu zájmů, ve znění pozdějších předpisů, nebo, jím ovládaná osoba, vlastní podíl představující alespoň 25% účasti společníka v obchodní společnosti a
 - h) na Nahrazujícího dodavatele, na jeho případné poddodavatele ani na jím nabízené plnění se nevztahují mezinárodní sankce ve smyslu § 2 zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů.
- 20.2. Pokud se postupem dle čl. 20.1. této Smlouvy nepodaří uzavřít smlouvu s Nahrazujícím dodavatelem, může Objednatel nahradit Dodavatele dodavatelem, jehož nabídka se umístila jako další v pořadí za Nahrazujícím dodavatelem při hodnocení nabídek ve Veřejné zakázce. Při tom musí být rovnocenným způsobem splněny podmínky uvedené v čl. 20.1. této Smlouvy.
- 20.3. Dodavatel, který nahradí Dodavatele postupem dle čl. 20.1. nebo 20.2. této Smlouvy, bude pokračovat v plnění dle této Smlouvy za podmínek odpovídajících jeho nabídce předložené ve Veřejné zakázce.
- 20.4. Realizace změny v osobě Dodavatele proběhne buď cestou ukončení této Smlouvy a uzavřením smlouvy nové, nebo cestou postoupení pohledávky z této Smlouvy ve smyslu § 1879 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

21. Ukončení smlouvy

- 21.1. Smlouva je uzavřena na dobu určitou, a to na dobu 24 měsíců od akceptace Produkčního provozu Software.
- 21.2. Smlouva může být ukončena:
- splněním,
 - vzájemnou dohodou Smluvních stran,
 - výpovědí jednou ze Smluvních stran,
 - odstoupením od Smlouvy,
 - ze zákona.
- 21.3. Ve všech případech zániku Smlouvy je Dodavatel povinen zařídit ještě vše, co nesnese odkladu, dokud Dodavatel nebo jeho právní nástupce neprojeví jinou vůli.
- 21.4. Smluvní strany mohou ukončit platnost Smlouvy písemnou dohodou nebo výpovědí, a to i bez udání důvodů. Výpovědní lhůta činí 3 měsíce a počíná běžet začátkem kalendářního měsíce následujícího po měsíci, ve kterém byla písemná výpověď doručena druhé Smluvní straně na adresu uvedenou v záhlaví této Smlouvy.
- 21.5. Smluvní strany se dohodly, že odstoupit od této Smlouvy je možné pouze v případech stanovených právními předpisy České republiky či touto Smlouvou. Za porušení smluvních povinností Dodavatele podstatným způsobem, které opravňují Objednatele k odstoupení od této Smlouvy, se považuje:
- 21.5.1. prodlení Dodavatele s dodáním Předmětu plnění v mezních termínech uvedených v čl. 4.1. písm. b) nebo c) Smlouvy, nebo
- 21.5.2. prodlení Dodavatele s odstraňováním vad či nedodělků předaného (akceptovaného) Předmětu plnění ve lhůtách stanovených v příslušném akceptačním protokolu nebo ve Smlouvě delší než 30 kalendářních dnů, pokud Dodavatel nezjedná nápravu ani v dodatečně přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 kalendářních dnů od doručení takovéto výzvy, nebo
- 21.5.3. prodlení Objednatele s úhradou faktury za Předmět plnění delší než 60 kalendářních dnů, pokud Objednatel nezjedná nápravu ani do 10 kalendářních dnů od doručení písemného oznámení Dodavatele o takovém prodlení se žádostí o jeho nápravu, nebo
- 21.5.4. opakované porušení SLA dle čl. 5.9. této Smlouvy ve třech po sobě jdoucích měsících,
- 21.5.5. porušení povinnosti ochrany a utajení informací dle článku 16 této Smlouvy ze strany Dodavatele.
- 21.6. Objednatel je dále oprávněn bez jakýchkoliv sankcí odstoupit od této Smlouvy, pokud:
- 21.6.1. na majetek Dodavatele je prohlášen úpadek nebo Dodavatel sám podá dlužnický návrh na zahájení insolvenčního řízení, nebo
- 21.6.2. Dodavatel vstoupí do likvidace, nebo
- 21.6.3. Dodavatel je uznán, byť nepravomocně, vinným ze spáchání trestného činu podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů, nebo

- 21.6.4. Objednatel zjistí, že je Dodavatel Osobou vedenou na sankčních seznamech, tj. fyzickou nebo právnickou osobou uvedenou v příloze I Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisech k tomuto Nařízení č. 269/2014 (tzv. sankční seznamy), nebo
- 21.6.5. Objednatel zjistí, že je Dodavatel obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, tj. člen vlády nebo vedoucí jiného ústřední orgánu státní správy, v jehož čele není člen vlády, nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.
- 21.7. Pokud jedna Smluvní strana odstupuje od Smlouvy, potom je dle této Smlouvy povinna tuto skutečnost sdělit druhé Smluvní straně písemně. Toto sdělení musí označovat okolnost, resp. důvod, pro nějž Smluvní strana odstupuje od Smlouvy a přesná citace ustanovení Smlouvy nebo právního předpisu, který ji k odstoupení opravňuje. Bez těchto náležitostí je odstoupení neplatné mimo případů, kdy právo odstoupit od Smlouvy vyplývá přímo ze zákona. Sdělení o odstoupení od Smlouvy musí obsahovat prohlášení, že smluvní strana odstupuje od Smlouvy až okamžikem marného uplynutí dodatečně přiměřené lhůty stanovené k odstranění porušení, které je důvodem odstoupení, je-li to vzhledem k povaze porušené povinnosti možné. Za řádné doručení oznámení o odstoupení od Smlouvy se považuje jeho doručení prostřednictvím poskytovatele poštovních služeb, kurýra, nebo její doručení do datové schránky druhé Smluvní strany.
- 21.8. Smluvní strany se dohodly, že v případě odstoupení od Smlouvy se nevrací Dodavatelem již provedené a Objednatelem akceptované plnění dle Smlouvy.
- 21.9. V případě odstoupení či výpovědi Smlouvy jsou Smluvní strany povinny ve lhůtě 15 kalendářních dnů od řádného odstoupení od Smlouvy či uplynutí výpovědní lhůty vypořádat vzájemně své závazky a pohledávky vyplývající z této Smlouvy. Dodavateli přísluší poměrná výše odměny dle článku 10 Smlouvy odpovídající dosud dodané části Předmětu plnění.
- 21.10. Ukončením účinnosti Smlouvy nejsou dotčena práva a povinnosti založená Smlouvou, která mají podle zákona, Smlouvy nebo na základě své povahy trvat i po jejím skončení, zejména ustanovení o odpovědnosti za škodu (škoda může spočívat i v nákladech vynaložených Objednatelem na realizaci nového zadávacího řízení), o sankcích včetně smluvních pokut ve smyslu čl. 19 této Smlouvy a o ochraně a utajení informací ve smyslu čl. 17 Smlouvy.

22. Ostatní ujednání a kontaktní údaje

- 22.1. Právní vztahy touto Smlouvou výslovně neupravené se budou řídit českými, obecně závaznými právními předpisy, zejména zákonem č. 89/2012 Sb., občanský zákoník, v platném znění.
- 22.2. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů, vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, a k jejich vyřešení zejména prostřednictvím jednání odpovědných osob nebo pověřených zástupců.
- 22.3. Smluvní strany mají zájem především na smírném řešení sporu. Nebude-li možné vyřešit spor smírnou cestou, je dána příslušnost věcně a místně příslušného soudu v České republice dle zákona č. 99/1963 Sb., občanský soudní řád, v platném znění, a to dle sídla Objednatele.

- 22.4. Dodavatel souhlasí se zveřejněním všech náležitostí tohoto smluvního vztahu, souhlasí i s uveřejněním této Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
- 22.5. Dodavatel odpovídá za dodržování předpisů BOZP vyplývajících z povahy jeho prací.
- 22.6. Odpovědnými osobami k podpisu předávacího a akceptačního protokolu jsou Vedoucí týmu obou smluvních stran, uvedení v Příloze č. 4 této Smlouvy.
- 22.7. Odpovědné osoby k podpisu předávacího a akceptačního protokolu jsou oprávněny předávat a přebírat předmět Smlouvy a podepisovat za tím účelem předávací a akceptační protokoly. Odpovědné osoby nejsou oprávněny měnit či rušit smluvní vztahy vyplývající z této Smlouvy.
- 22.8. Dodavatel je oprávněn uveřejnit na svém profilu zadavatele celý text Smlouvy (§ 219 ZZVZ) za předpokladu, že uveřejnění nebrání zvláštní právní předpis.

23. Dodržování důstojných pracovních podmínek

- 23.1. Dodavatel prohlašuje, že si je vědom skutečnosti, že Objednatel má zájem na realizaci Veřejné zakázky v souladu se zásadami společensky odpovědného zadávání veřejných zakázek.
- 23.2. Dodavatel se zavazuje po celou dobu trvání Smlouvy zajistit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a Zákoníku práce, a to vůči všem osobám, které se na plnění zakázky podílejí a bez ohledu na to, zda bude dle této smlouvy plněno Dodavatel či jeho Poddodavatelem.
- 23.3. Dodavatel se dále zavazuje po celou dobu trvání smlouvy zajistit u sebe a svých Poddodavatelů dodržování zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon).
- 23.4. Dodavatel je povinen před zahájením plnění a po jeho ukončení předložit čestné prohlášení, v němž uvede, že všechny osoby podílející se na předmětu smlouvy jsou či byly vedeny v příslušných registrech, zejména živnostenském rejstříku, registru pojištěnců ČSSZ a mají příslušná povolení k pobytu v ČR a k výkonu pracovní činnosti. Dále zde bude uvedeno, že byly proškoleny z problematiky BOZP a že jsou vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy (je-li relevantní). Dodavatel bere na vědomí, že tato prohlášení je Objednatel oprávněn poskytnout příslušným orgánům veřejné moci ČR. Tato povinnost platí bez ohledu na to, zda bude plnění dle této Smlouvy prováděno Dodavatel či jeho Poddodavatelem.
- 23.5. Objednatel je oprávněn průběžně kontrolovat dodržování povinností Dodavatele dle čl. 23.1. a 23.2. Smlouvy, a to i přímo u pracovníků vykonávajících Předmět plnění, přičemž Dodavatel je povinen tuto kontrolu umožnit, strpět a poskytnout Objednateli veškerou nezbytnou součinnost k jejímu provedení.

24. Závěrečná ustanovení

- 24.1. Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě nebo která

mají být učiněna na základě této Smlouvy, musí být učiněna v písemné formě a opačné straně doručena buď osobně, nebo doporučeným dopisem, či jinou formou registrovaného poštovního styku, na adresu uvedenou na titulní stránce této Smlouvy, nebude-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak. Oznámení se považují za doručena uplynutím desátého (10.) dne po jejich prokazatelném odeslání.

- 24.2. Změny a doplňky této Smlouvy musí mít písemnou formu, přičemž každá ze Stran se zavazuje spravedlivě zvážit návrhy Strany druhé.
- 24.3. Smlouva je uzavírána elektronicky, a to tak, že je opatřena elektronickými podpisy (zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo kvalifikovaným elektronickým podpisem) oprávněných zástupců smluvních stran.
- 24.4. Smlouva nabývá platnosti dnem podpisu oprávněnými zástupci smluvních stran a nabývá účinnosti dnem zveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Smluvní strany dohodly, že text smlouvy zveřejňuje Objednatel. Před zveřejněním Objednatel odstraní z textu Smlouvy všechny osobní a kontaktní údaje, případně další části Smlouvy, označené Dodavatelem jako obchodní tajemství.
- 24.5. Stane-li se některé ustanovení této Smlouvy neplatné, nebo neúčinné, nedotýká se to ostatních ustanovení této Smlouvy, která zůstávají v platnosti a účinnosti. Smluvní strany se v tomto případě zavazují dohodou nahradit ustanovení neplatné (neúčinné) novým ustanovením platným (účinným), které nejlépe odpovídá původně zamýšlenému ekonomickému účelu ustanovení neplatného (neúčinného). Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.
- 24.6. Uvedené Smluvní strany prohlašují, že se samy přesvědčily o identitě druhé Smluvní strany, taktéž že její označení uvedené v záhlaví této Smlouvy odpovídá aktuálnímu stavu, že je jim známa nesporná totožnost a řádné oprávnění osob jednajících za druhou Smluvní stranu k tomuto jednání a zároveň si vzájemně prohlásily, že tyto údaje nejsou dotčeny změnami již uskutečněnými, avšak ještě nezapsanými v obchodním rejstříku. Zároveň prohlašují, že uzavření této Smlouvy je v souladu se zákonem předepsanými či interně stanovenými pravidly, jakož i v plném zájmu jimi zastupovaných Smluvních stran.
- 24.7. Smluvní strany, vědomy svých závazků vyplývajících z této Smlouvy a v úmyslu být touto Smlouvou plně vázány, potvrzují tímto její pravost podpisy osob řádně oprávněných jednat za příslušnou Stranu a současně prohlašují, že tato Smlouva byla sepsána po vzájemné shodě o jejich náležitostech.
- 24.8. Nedílnou součástí této Smlouvy jsou následující přílohy:
 - a) Příloha č. 1a – Specifikace a popis předmětu plnění
 - b) Příloha č. 1b – Obecná technická specifikace
 - c) Příloha č. 2 – Položkový rozpočet
 - d) Příloha č. 3 – Koncepce nabízeného řešení
 - e) Příloha č. 4 – Složení týmu za Objednatele a Poskytovatele
 - f) Příloha č. 5 – Seznam poddodavatelů
 - g) Příloha č. 6 – Bezpečnostní požadavky
- 24.9. Smluvní strany potvrzují, že si tuto Smlouvu přečetly, rozumí jejímu obsahu, souhlasí s ní a nemají proti ní výhrad. Svými podpisy potvrzují, že Smlouva je jejich projevem pravé, svobodné a vážné vůle a že ji neuzavřely v omylu ani pod pohrůžkou násilí. Na důkaz pravosti Smluvní strany opatřují tuto Smlouvu podpisy oprávněných osob, které garantují, že jsou plně oprávněny tuto Smlouvu za Smluvní strany platně uzavřít.

Za Aricoma Digital s.r.o.

V Praze dne

Za Univerzitu Karlovu

V Praze dne

.....
Ing. Tomáš Rutrle, jednatel

.....
Mgr. Martin Maňásek, kvestor

Příloha č. 1a – Specifikace a popis předmětu plnění

Obsah

1	Úvod	3
1.1	Předmět plnění.....	3
1.2	Oblasti plánovaného rozvoje (není předmětem této VZ).....	3
2	Byznys analýza	3
2.1	Popis modulu.....	3
3	Uživatelské rozhraní	3
3.1	Flow chart diagramy.....	3
3.2	Přístupy k návrhům UI v prostředí Figma.....	4
3.2.1	Komponenty:.....	4
3.2.2	Katalog předmětů.....	4
3.2.3	Studijní programy	4
4	Popis vnějších rozhraní a vazeb na jiné moduly.....	4
4.1	Veřejné REST rozhraní implementované dodavatelem	4
4.2	Veřejná REST rozhraní používaná dodavatelem.....	4
4.3	Veřejné microfrontend rozhraní implementované dodavatelem	5
4.4	Datový interface pro integraci se stávajícím SIS.....	5
4.4.1	Datový interface pro stávající databázi SISu	5
4.4.2	Popis modulem používaných tabulek.....	5
4.4.3	Zápisové operace.....	5
5	Požadavky na výkon a dostupnost pro modul Předměty a studijní plány	5
5.1	Frontendový modul	5
5.2	Backendový modul	5
5.3	Vysoká dostupnost (HA)	5
6	Požadavky na audit a observability	5
6.1	Struktura požadovaných auditních událostí.....	6
6.2	Metriky	6
6.2.1	Seznam poskytovaných speciálních metrik.....	6
6.3	Tracing	6
6.3.1	Seznam poskytovaných traců backendového modulu	6
6.3.2	Seznam poskytovaných traců frontendového modulu	6
7	Zajištění jakosti (QA) a dokumentace pro modul Předměty a studijní plány.....	6
7.1	Pokrytí kódu unit testy	6
7.2	Seznam požadovaných systémových (end-to-end) testů.....	6
7.3	Seznam požadovaných výkonnostních testů.....	6
7.4	Seznam požadovaných testovacích nástrojů (mock, generátory, simulátory).....	6

1 Úvod

1.1 Předmět plnění

Předmětem plnění je dodávka software a jeho podpora během provozu. Plnění proběhne ve dvou fázích. V první fázi bude dodána iniciální verze software. Ve druhé fázi bude zajišťována průběžná podpora. Tento dokument dále detailně specifikuje základní funkcionality k realizaci v rámci první fáze s výjimkou kapitoly 1.2 která nastiňuje oblasti budoucího rozvoje aplikace.

Aplikace slouží uživatelům bez přihlášení do systému (anonym) k zobrazení informací o předmětech, studijních programech a studijních plánech, které jsou evidovány na Univerzitě Karlově.

Součástí dodávky je implementace řešení, které splňuje požadavky specifikované dokumentací, realizace potřebných testů řešení a jeho nasazení v prostředí UK.

Dle obecných technických požadavků na moduly se implementací rozumí implementace (i) jednoho, nebo více frontendových modulů pro zobrazování předmětů, studijních programů a plánů a (ii) implementace jednoho backendového modulu, jež bude řídit přístup k datům pro zobrazování informací o předmětech a (iii) jednoho backendového modulu, jež bude řídit přístup k datům o studijních programech.

Součástí tohoto zadání jmenovitě není implementace backend modulů pro přístup k datům o studijních plánech a přístup k rozvrhům předmětů. Potřebná data z těchto modulů budou přístupná v rámci veřejného API.

1.2 Oblasti plánovaného rozvoje (není předmětem této VZ)

- Funkce pro přihlášeného uživatele, např.:
 - o Označení předmětu záložkou (připojení poznámky, seskupování do různých seznamů...)
 - o Napojení na prostor dané třídy v rámci e-learningové platformy (Teams, Moodle...)

2 Byznys analýza

2.1 Popis modulu

Modul Předměty a studijní plány je referenčním zdrojem základních informací o všech předmětech, které jsou ve studijním informačním systému evidovány. Studijní programy vyjadřují zaměření studia a jsou realizovány prostřednictvím studijních plánů, které tvoří soubor povinných, povinně volitelných a volitelných předmětů a jejich uspořádání z hlediska vzájemných vztahů a časové posloupnosti. Hlavním účelem modulu je zobrazit uživatelům všechny detailní informace k předmětům a zobrazit postavení předmětu ve Studijním plánu s návazností na Studijní program.

Předměty je možné vyhledat na základě různých kritérií, včetně jejich zařazení do konkrétního studijního programu i studijního plánu. Modul se skládá z vlastní databáze, uživatelského rozhraní a z aplikačních rozhraní, která slouží ostatním modulům i vlastnímu uživatelskému rozhraní.

Důležité entity včetně předmětů, studijních programů a studijních plánů, jejich atributy a vztahy jsou popsány v konceptuálním datovém modelu. Rozsah a popis funkcionalit je vyjádřen use case diagramy s příslušnými scénáři. Konceptuální datový model a use case diagram jsou součástí příloh tohoto dokumentu.

3 Uživatelské rozhraní

3.1 Flow chart diagramy

Katalog předmětů:

<https://www.figma.com/file/zLQzkLO2SAhlzBc0tdqpAg/P%C5%99edm%C4%9Bty-v.1---Flow-chart?type=whiteboard&t=U8mAAcw5HU0n9Elv-1>

Studijní plány:

<https://www.figma.com/file/Nj61LeHD3cqNr6yI020w2z/Studijn%C3%AD-programy?type=design&mode=design&t=RNskV2rGZMDUsBR8-1>

3.2 Přístupy k návrhům UI v prostředí Figma

Soubory UI návrhů ve Figmě jsou přístupné pro prohlížení na těchto adresách.

3.2.1 Komponenty:

Design systém:

<https://www.figma.com/file/Ye5Fy9jLvd4o0eG3TA9jnb/SoSIS-Design-system?type=design&node-id=5%3A2&mode=design&t=3dl0KbgEDq6guevD-1>

Komponenty Katalogu předmětů:

https://www.figma.com/file/S3EkJvjuTg8KTx27WXbqD9/komponenty_predmetu?type=design&mode=design&t=RNskV2rGZMDUsBR8-1

Komponenty Studijních plánů:

https://www.figma.com/file/3GDVgiDoBQZG3sj8m2lks/komponenty_stud_programy?type=design&mode=design&t=RNskV2rGZMDUsBR8-1

3.2.2 Katalog předmětů

Návrhy obrazovek: <https://www.figma.com/file/cWOru7xmDepGGu8ullCTP4/Katalog-p%C5%99edm%C4%9Bt%C5%AF?type=design&mode=design&t=RNskV2rGZMDUsBR8-1>

Prototyp: <https://www.figma.com/proto/cWOru7xmDepGGu8ullCTP4/Katalog-p%C5%99edm%C4%9Bt%C5%AF?page-id=775%3A7775&type=design&node-id=957-25161&viewport=-609%2C-87%2C0.12&t=v5bk9GkDaUHeXnDc-1&scaling=scale-down&starting-point-node-id=775%3A8100&mode=design>

3.2.3 Studijní programy

Návrhy obrazovek: <https://www.figma.com/file/Nj61LeHD3cqNr6yl020w2z/Studijn%C3%AD-programy?type=design&mode=design&t=U8mAAcw5HU0n9Elv-1>

Prototyp: <https://www.figma.com/proto/Nj61LeHD3cqNr6yl020w2z/Studijn%C3%AD-programy?page-id=802%3A1834&type=design&node-id=804-9489&viewport=58%2C502%2C0.13&t=JX0M0hZd1FtSSyid-1&scaling=contain&starting-point-node-id=802%3A1835&mode=design>

Flowchart a exporty obrazovek UI jsou součástí přílohy.

4 Popis vnějších rozhraní a vazeb na jiné moduly

4.1 Veřejné REST rozhraní implementované dodavatelem

Detailní specifikace veřejného REST API backendového modulu pro předměty je popsána v příloženém souboru `subjects_basic_v1.0.0.yaml`. Pro studijní programy v souboru `study-programmes_basic_v1.0.0.yaml`. Veškeré operace popsané v souborech jsou čtecí a nevyžadují kontext uživatele. Obecné specifikace jsou pak popsány v sekci Obecné požadavky na strojová rozhraní modulů v obecné části dokumentu. Preferujeme použití veřejného API dodavatelem pro implementaci frontendových modulů nicméně primárním cílem je poskytnout stabilní API pro ostatní moduly. V případě potřeby může být specifikace veřejného API rozšířena/upravena po konzultaci se zadavatelem.

4.2 Veřejná REST rozhraní používaná dodavatelem

Moduly budou mít dále přístup k následujícím operacím:

- Operace z modulu Studijní plány dle příloženého souboru `curricula_basic_v1.0.0.yaml`. (detail studijního plánu)
- Operace z modulu Rozvrhy dle příloženého souboru `schedule_basic_v1.0.0.yaml`. (Zobrazení vyučujících daného předmětu pomocí `/subjects/{subjectCode}`)

4.3 Veřejné microfrontend rozhraní implementované dodavatelem

Frontend modul bude poskytovat následující microfrontend rozhraní pro ostatní moduly:

- Zobrazení detailních informací o předmětu (všechny parametry včetně dlouhých textových polí)

Frontend moduly budou moci využívat následujících microfrontend rozhraní ostatních modulů:

- Zobrazení rozvrhu předmětu.

4.4 Datový interface pro integraci se stávajícím SIS

4.4.1 Datový interface pro stávající databázi SISu

Pro modul Předměty bude vytvořen db uživatel sosis_subjects. Ve schématu tohoto uživatele bude možné vytvářet další tabulky pro uložení vlastních dat modulu.

4.4.2 Popis modulem používaných tabulek

Struktura zveřejněných tabulek vyplývá z konceptuálního modelu, ale ne vždy mu přesně odpovídá. Detailní seznam tabulek (sloupců a jejich datových typů) a vazeb mezi nimi je uveden v příloze.

4.4.3 Zápisové operace

Modul slouží jen pro náhled, nepožaduje žádná data.

5 Požadavky na výkon a dostupnost pro modul Předměty a studijní plány

5.1 Frontendový modul

Odhadovaný běžný provoz modulu je zpracování cca 1000 požadavků za minutu vygenerovaných cca 1000 současně pracujících uživatelů, špičkovou zátěž modulu lze očekávat cca 10x vyšší co do počtu aktivních uživatelů i co do počtu požadavků. Pro plynulou práci s aplikací je nutné očekávat základní response systému cca do 200ms (max 1s). Doba response musí být garantována pro 98% požadavků při špičkové zátěži.

Do základní response je potřeba zahrnout většinu základních operací typu zobrazení detailu předmětu, vyhledání předmětů na základě filtrovacích kritérií apod.

Pro vyhledávací operace na základě pokročilých fulltextových kritérií může být doba k zobrazení výsledků mírně prodloužena až na nižší jednotky sekund. Základní response modulu však musí být shodná, kdy modul poskytuje uživateli zpětnou vazbu během provádění déle trvajících akce. Do této kategorie déle trvajících akcí lze zahrnout např. pokročilé vyhledávání předmětu s použitím dalších informací zjišťovaných z jiných modulů prostřednictvím API.

5.2 Backendový modul

Odhadovaná zátěž backendového modulu je cca 1000 požadavků za minutu, špičkovou zátěž modulu lze očekávat cca 20x vyšší. Požadovaná základní response backendového modulu pro poskytnutí dat je do 200ms. Pro fulltextové vyhledávací operace je požadovaná response v nižších jednotkách sekund.

5.3 Vysoká dostupnost (HA)

Všechny funkce frontendového i backendového modulu mají podporovat plnohodnotnou vysokou dostupnost (tzv. režim hot-hot).

6 Požadavky na audit a observability

V první fázi implementace (vyhledání a zobrazení předmětů a studijních plánů) není požadováno uchovávání žádných auditních událostí.

Při dalším rozvoji mohou být identifikovány další požadavky na auditování událostí (např. Zobrazení detailu předmětu přihlášeným uživatelem).

6.1 Struktura požadovaných auditních událostí

[V první fázi implementace nejsou žádné požadované auditní události.]

6.2 Metriky

6.2.1 Seznam poskytovaných speciálních metrik

Oproti obecné části ZD nejsou požadovány žádné speciální metriky pro frontendové ani backendové moduly.

6.3 Tracing

6.3.1 Seznam poskytovaných traců backendového modulu

Modul bude poskytovat trace spany zejména pro celou dobu vyhodnocování příchozích požadavků (pomocí API), a také podřízený span pro interakci s databází.

6.3.2 Seznam poskytovaných traců frontendového modulu

Modul bude poskytovat trace spany zejména pro celou dobu vyhodnocování příchozích požadavků (pomocí UI), a také podřízený span pro interakci s backendovým modulem a jinými moduly prostředí.

7 Zajištění jakosti (QA) a dokumentace pro modul Předměty a studijní plány

7.1 Pokrytí kódu unit testy

Zadavatel požaduje pokrytí kódu unit testy v míře uvedené v příloze č. 1b výzvy.

7.2 Seznam požadovaných systémových (end-to-end) testů

100 % uživatelských cest musí být pokryto systémovými testy.

Oproti popisu uvedenému v příloze č. 1b výzvy nemá zadavatel žádné specifické požadavky na end-to-end testy.

7.3 Seznam požadovaných výkonnostních testů

Dodavatel připraví sadu výkonnostních testů pro všechny běžné operace vyplývající z business analýzy včetně kombinovaných testů pro současný běh uživatelských scénářů vyplývajících z typických uživatelských cest tak, jak je popsáno v příloze č. 1b výzvy.

Oproti příloze č. 1b výzvy nemá zadavatel pro výkonnostní testy žádná další upřesnění.

7.4 Seznam požadovaných testovacích nástrojů (mock, generátory, simulátory)

Kromě nástrojů uvedených v příloze č. 1b výzvy nepožaduje zadavatel žádné další speciální testovací nástroje.

Příloha č. 1b – Obecná technická specifikace

Obsah

1	Úvod a obecná architektura	4
1.1	Popis problému a motivace	4
1.2	Obecné infrastrukturní požadavky	4
1.2.1	Koncept nové architektury	4
1.2.2	Prostředí, kontejnerizace	5
1.2.3	Git repositář kódu, CI/CD	7
1.2.4	Správa hesel a přístupových údajů (Secrets).....	8
1.2.5	Principy komunikace mezi službami/moduly	8
1.2.6	Webhooks.....	9
1.2.7	Síťový provoz a napojení, reverzní proxy, API brána.....	9
1.2.8	Autentizace a autorizace	10
1.2.9	Perzistentní datová úložiště	10
1.2.10	Audit	12
1.2.11	Logování	13
1.2.12	Tracing	16
1.2.13	Metriky a monitoring.....	17
1.2.14	Diagramy primárních interakcí modulu.....	18
1.2.15	Reporting.....	20
1.2.16	Dostupnost a spolehlivost (High Availability).....	20
1.3	Obecné technické požadavky na moduly	21
1.3.1	Technické požadavky na backendové moduly	21
1.3.2	Technické požadavky na frontendové moduly.....	21
1.3.3	Interakce mezi moduly	23
2	Obecné požadavky na uživatelská rozhraní	23
2.1	Obecné principy uživatelského rozhraní	23
2.2	Předání grafických podkladů pro UI	24
2.3	Uživatelské rozhraní - popis základního layoutu	24
2.3.1	Základní prvky uživatelského prostředí.....	25
2.3.2	Responzivita a breakpoints.....	25
2.3.3	Dimenze základních sekcí layoutu	26
2.3.4	Grafické náhledy.....	27
2.4	Požadavky na optimalizaci.....	31
2.5	Požadavky na přístupnost a použitelnost.....	31
3	Obecné požadavky na strojová rozhraní modulů.....	32
3.1	Obecná pravidla.....	33

3.1.1	Jmenné konvence	33
3.1.2	Chování klientů rozhraní	33
3.2	Obecné požadavky na veřejná API	33
3.2.1	Zdroje a jejich typy	33
3.2.2	Pravidla pro určování zdrojů a tvorbu jejich URL	34
3.2.3	Pravidla pro návrh operací pro manipulaci se zdroji	37
3.2.4	Pravidla pro stránkování a filtrování kolekcí pomocí parametrů v URL	37
3.2.5	Pravidla pro definici zdrojů a operací pro manipulaci se zdroji	38
3.2.6	Pravidla pro návrh a popis JSON datových struktur	38
3.3	Obecné požadavky na privátní API	39
4	Datový interface pro integraci se stávající databází SISu	39
4.1	Konfigurační parametry	39
4.2	Langy	40
5	Zajištění jakosti (QA) a dokumentace	40
5.1	Obecné požadavky na kvalitu kódu a bezpečnost	40
5.1.1	Kvalita kódu	40
5.1.2	Bezpečnost	40
5.2	Obecné požadavky na dokumentaci	41
5.3	Obecné požadavky na QA	42
5.3.1	Obecné požadavky na testování	42
5.3.2	Mock, simulační nástroje a nástroje na generování dat	43
5.3.3	Doporučená systémová konfigurace	44
6	Způsob řízení projektu a administrace	44
6.1	Požadavky na způsob řízení, komunikaci a podporu	44
6.1.1	Způsob řízení	44
6.1.2	Způsob komunikace	44
6.1.3	Školení administrátorů	44
6.2	Časový harmonogram	44
6.3	Dokumentace a požadavky na dodávku	45

1 Úvod a obecná architektura

1.1 Popis problému a motivace

Univerzita Karlova využívá studijní informační systém (dále jen „SIS“) vyvinutý firmou ERUDIO s.r.o. Jádro tohoto systému pochází z 90. let 20. století a je již technologicky zastaralé. Systém má velké množství modulů, které však od sebe nejsou odděleny, což (mimo jiné) významně ztěžuje možnost škálovat výkon systému a také realizovat rozvoj systému více dodavateli. Výkonové problémy se pak projevují zejména při hromadných elektronických zápisech do předmětů a přihlašování studentů na zkoušky. Část modulů má podobu tzv. těžkých klientů, většina z nich má podobu webových aplikací. Jednou z velkých nevýhod stávajících webových modulů SISu je však jejich velmi problematické až nemožné využívání z mobilních zařízení.

V roce 2021 uzavřela UK dodatky smluv s firmou ERUDIO s.r.o., které umožňují SIS dále rozvíjet vlastními silami nebo s využitím třetích stran. To otevřelo univerzitě cestu k tomu, aby se vyvázala ze stávající vendor lock-in pozice a otevřela vývoj SISu směrem k většímu počtu dodavatelů, mezi nimiž by plnila úlohu integrátora.

Záměrem je převést SIS do podoby moderního informačního systému, který má modulární a servisně orientovanou architekturu, kde jednotlivé moduly spolu komunikují formou volání služeb, a ne sdílením dat ve společné databázi. Tento architektonický model umožňuje lépe škálovat výkon systému a usnadňuje jeho vývoj více různými dodavateli, kteří realizují jednotlivé moduly nebo jejich části, které spolu komunikují prostřednictvím těchto webových služeb.

Současně je cílem formálně popsat procesy (provést tzv. byznys analýzu), pro které SIS poskytuje podporu, a funkcionality obsažené v systému tak, aby tento (průběžně aktualizovaný) popis mohl sloužit jako podklad pro další rozvoj systému – pro komunikaci mezi univerzitou a jednotlivými dodavateli a také mezi dodavateli navzájem.

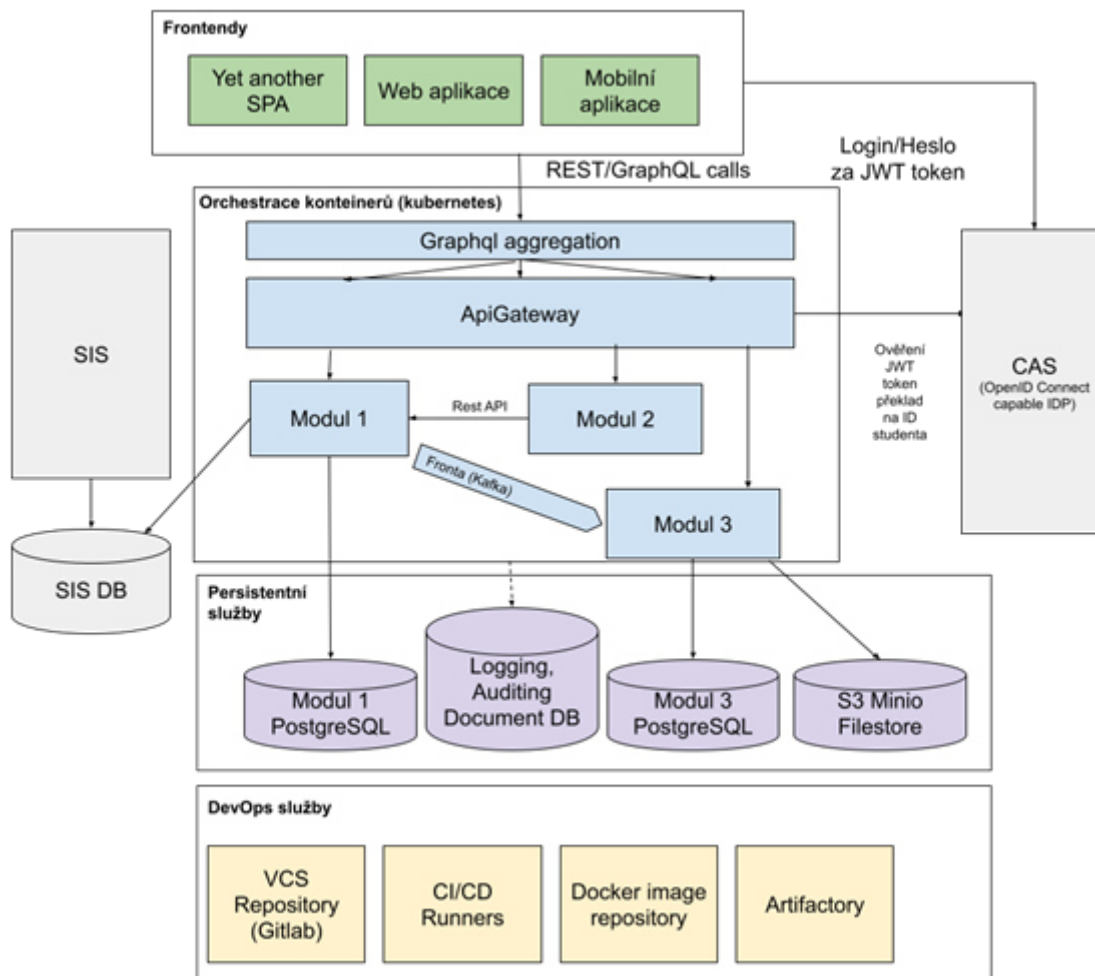
1.2 Obecné infrastrukturní požadavky

1.2.1 Koncept nové architektury

Nová architektura se vyznačuje svojí modulárností. Infrastruktura poskytuje sdílené služby aplikačním modulům, jako je autentizace, persistence, logování, monitorování, audit atd.

Cílem této architektury je umožnit zejména:

- Paralelní vývoj několika dodavateli
- Postupnou reimplementaci Studijního Informačního Systému (SIS)
- Škálování výkonu při zátěži
- Continuous deployment
- Rozsáhlé možnosti QA na různých úrovních systému
- V případě zastarání jednoho modulu není třeba přepisovat celý systém



1.2.2 Prostředí, kontejnerizace

Veškeré aplikace budou nasazovány pomocí kontejnerů. Zvolenou technologií pro orchestraci je Kubernetes. Správa Kubernetes probíhá pomocí platformy Rancher. Kubernetes je napojený na Centrální Autentizační Službu (CAS) UK.

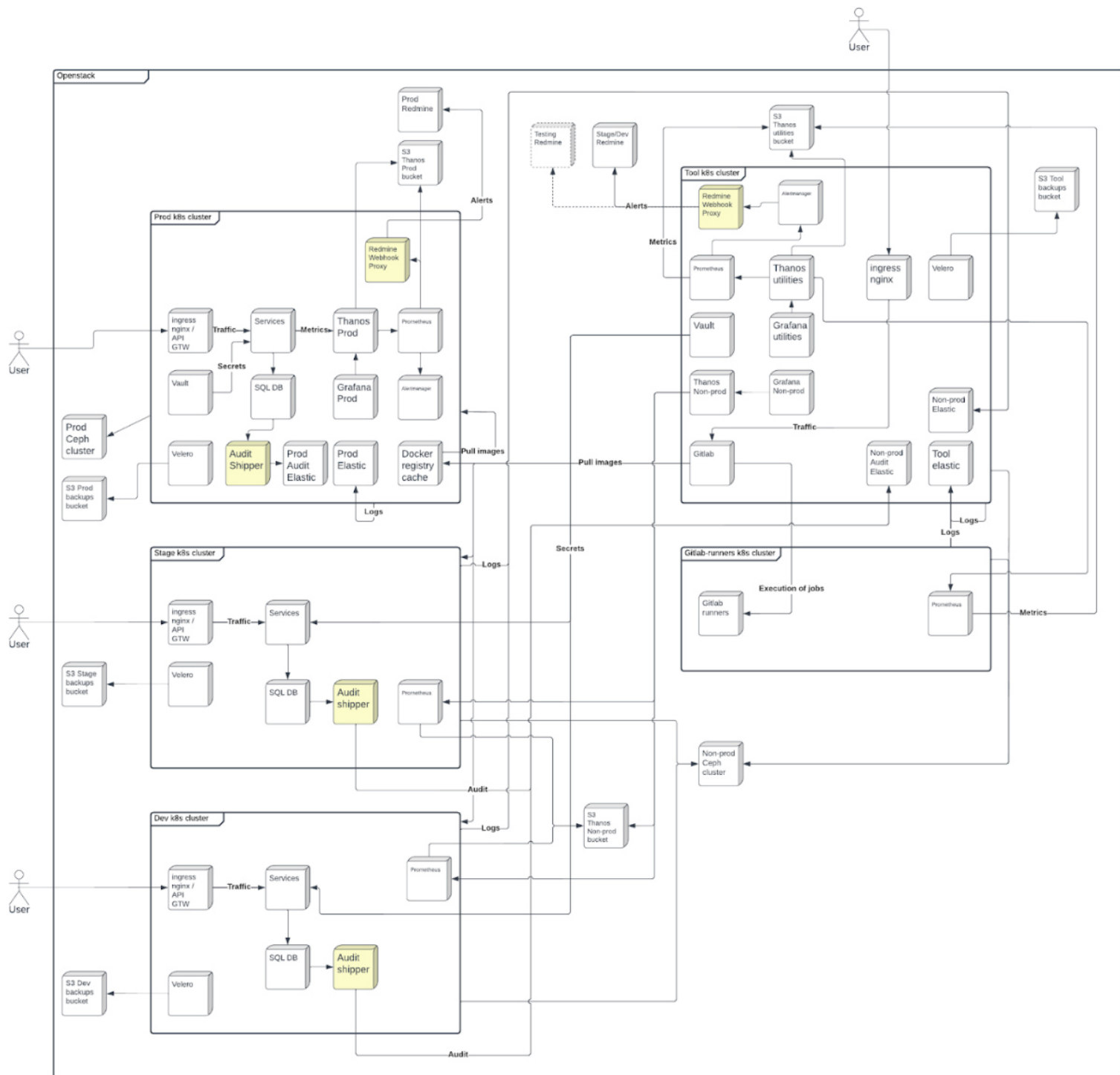
Jsou připravená tři prostředí:

1. **DEV (Development)**
 - Vývojářské prostředí
 - Toto prostředí bude dostupné dodavatelům, vývojáři zde mohou nasazovat své moduly bez asistence pomocí předpřipravených CI/CD pipelines
 - Možnost testovat integraci s ostatními moduly při vývoji
2. **STAGE (Staging)**
 - Testovací prostředí pro UK
 - Možnost spouštět zátěžové testy
 - Nasazování modulů je spravováno UK
3. **PROD (Production)**
 - Prostředí dostupné cílovým uživatelům

Každé z výše uvedených prostředí má vlastní Kubernetes cluster. Pro zjednodušení správy prostředí STAGE a DEV používají tato prostředí také sdílený TOOLS cluster, který obsahuje zejména sdílený Ceph cluster a sdílené nástroje pro monitoring a logování. Mezi další neprodukční systémové cluster patří také GitLab Runners cluster a Rancher management cluster.

Jedním z cílů vytvořeného prostředí je nasazení modulů v režimu vysoké dostupnosti (high availability) společně s automatickým škálováním dle aktuální zátěže.

Následující diagram znázorňuje přiřazení jednotlivých systémových komponent do zmiňovaných clusterů. Vlastní komponenty (vytvářeny interně na UK) jsou zvýrazněny žlutě. Moduly vyvíjené dodavateli jsou shrnuty pod komponentu "Services".



Legenda

- Kubernetes – nástroj pro orchestraci kontejnerů nad clusterem serverů
- NGINX Ingress – obecná reverzní proxy
- Kong API Gateway – specializovaná rozšiřitelná reverzní proxy s pokročilými funkcemi
- PostgreSQL – relační databáze
- Kafka – asynchronní fronta pro komunikaci mezi moduly
- Ceph – platforma spravující datová úložiště
- S3 – běžné rozhraní pro úložiště souborů/objektů
- GitLab – nástroj pro správu zdrojových kódů a automatizaci
- GitLab Runner – komponenta GitLabu, která zprostředkovává automatizaci
- Docker Registry – úložiště obrazů kontejnerů
- ArgoCD – nástroj pro synchronizaci nasazování aplikací a infrastruktury
- Velero – zálohovací nástroj pro Kubernetes
- Prometheus – nástroj pro sběr a krátkodobé úložiště metrik
- Alertmanager – nástroj pro správu automatizovaných upozornění
- Thanos – nástroj pro dlouhodobé ukládání metrik
- Grafana – nástroj pro zobrazování metrik a grafů
- Redmine – wiki a správa incidentů
- Redmine Webhook Proxy – vlastní komponenta pro napojení Alertmanageru a Redmine
- Elasticsearch – úložiště logů a audit záznamů
- Logstash – nástroj pro transformaci logů a audit záznamů
- Filebeat – nástroj pro sběr logů z jednotlivých komponent
- Audit Shipper – vlastní komponenta pro přesun audit záznamů z modulových DB schémat do centrálního úložiště auditních záznamů, napr. Elasticsearch
- Kibana – nástroj pro zobrazení a vyhledávání logů a audit záznamů
- Gatekeeper – nástroj pro vynucování pravidel pro všechny součásti Kubernetes

1.2.3 Git repositář kódu, CI/CD

Pro správu zdrojového kódu jednotlivých modulů je používána platforma GitLab, provozována v rámci výše popsaného kontejnerového prostředí. GitLab je sdílený pro všechna tři běhová prostředí. Slouží také zároveň jako Container Repository (nicméně produkční prostředí má vlastní Docker Registry Cache).

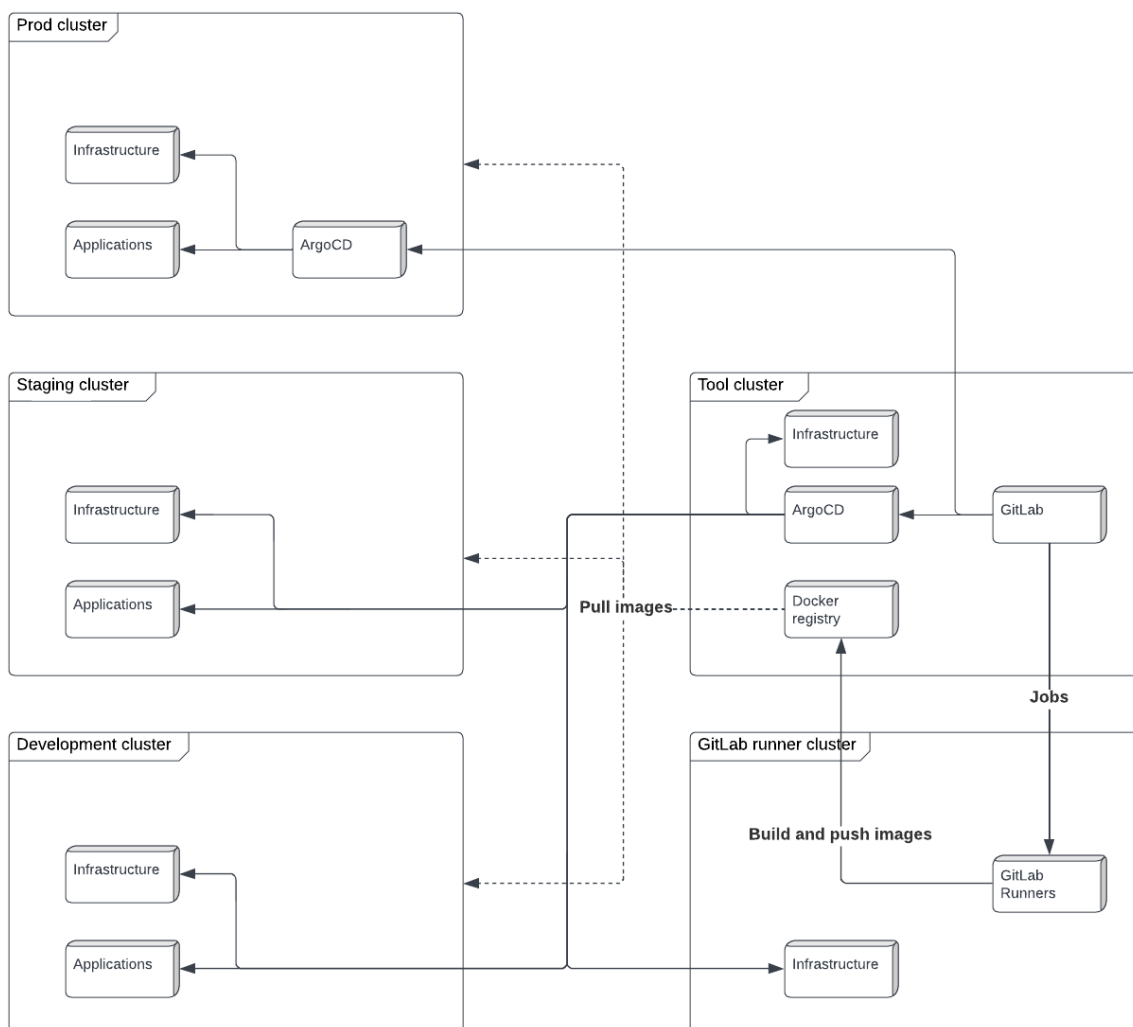
Pro každý modul bude v rámci prostředí GitLab připraven separátní projekt (skupina projektů), ke kterému obdrží dodavatel daného modulu přístup. Zadavatel také vytvoří základní CI/CD pipelines pomocí nástrojů GitLab, ArgoCD a Helm Charts pro automatizované nasazování modulu v prostředí DEV. Správa a následný vývoj těchto CI/CD pipelines bude následně probíhat ve spolupráci s dodavatelem. Finální CI/CD pipelines budou zadavatelem aplikovány také do STAGE a PROD prostředí.

Každý modul musí být reprezentovaný kontejnerem s následujícími požadavky:

- Kód musí být kompatibilní s rootless Docker image
- Každý modul používá standardní šablony pro GitLab CI a standardní Helm chart
- Base images kontejnerů: poslední stable Alpine, Debian nebo Ubuntu

Kromě samotného vyvíjeného modulu budou dodavateli zpřístupněné v rámci prostředí GitLab i vzorové moduly.

Následující CI/CD diagram znázorňuje 2 ArgoCD instance, které obsluhují všechny clustery a nasazení infrastruktury a modulů. Produkční instance je kompletně oddělená od neprodukční. ArgoCD je napojené na GitLab a synchronizuje stav několika repositářů s nastavením aplikací do jednotlivých clusterů.



1.2.4 Správa hesel a přístupových údajů (Secrets)

Veškeré přístupové údaje (URL služeb, hesla, tokeny atd.) budou každému modulu poskytnuty pomocí GitLab proměnných v odpovídajícím GitLab projektu a poté pomocí CI/CD pipelines dostupná jako proměnné běhového prostředí (OS environment variables). Každý modul tedy musí tyto informace načítat při startu z proměnných prostředí. **Je explicitně zakázáno ukládat podobné informace, zejména hesla a podobné přístupové údaje v jakýchkoliv konfiguračních souborech modulu.**

1.2.5 Principy komunikace mezi službami/moduly

Pro komunikaci mezi jednotlivými moduly budou použité následující technologie

- REST(-like) HTTP API
- GraphQL
- RPC
- Fronta
- Webhooks

1.2.5.1 Synchronní komunikace

Jako primární technologie určená pro synchronní komunikaci mezi moduly bude použito REST-like HTTP API. V některých případech v budoucnu může být také předepsána implementace GraphQL nebo RPC rozhraní. Konkrétní specifikace typu API (REST vs. GraphQL vs. RPC), včetně specifikace požadovaných operací, datových formátů, vstupních a výstupních dat bude detailně určena v zadávací dokumentaci každého modulu.

Kromě předpisu API rozhraní, které má modul vystavit pro ostatní moduly bude součástí zadávací dokumentace každého modulu také seznam a popis API rozhraní jiných modulů, které bude požadovaný modul potřebovat pro implementaci svých funkcionalit.

Pro zamezení snižování výsledné spolehlivosti modulů by moduly mezi sebou neměly v rámci zpracovávání jednoho požadavku od uživatele provést víc než dvě synchronní volání. Moduly by navíc neměly mezi sebou mít cyklickou závislost synchronních volání.

1.2.5.2 Asynchronní komunikace

Jako primární technologie určenou pro asynchronní komunikaci mezi moduly bude použita fronta, implementována pomocí platformy Apache Kafka. V rámci jednoho prostředí bude poskytnuta jedna sdílená instance Kafky. Přístupové informace modul obdrží v rámci sady odevzdávaných přístupových údajů pomocí CI/CD, jak bylo popsáno výše.

1.2.6 Webhooks

Další z dostupných alternativ pro komunikaci mezi moduly je také využití Webhooks u případů, kde charakter komunikace implementovaný touto technologií bude výhodnější než použití standardního REST API rozhraní. Požadavek na použití Webhooks bude pro daný modul specifikován v rámci zadávací dokumentace modulu.

1.2.7 Síťový provoz a napojení, reverzní proxy, API brána

Veškerý síťový provoz bude směřován na vstupní komunikační body (endpointy) modulu pomocí reverzní proxy a API brány. Tyto prvky budou poskytovat terminaci příchozího TLS spojení, load-balancing, základní autorizaci a směřování datového provozu na odpovídající moduly. Pro propagaci zdrojových IP adres klientů příchozích HTTP spojení budou přidávány hlavičky **X-Forwarded-For**.

Použité technologie pro reverzní proxy i API bránu jsou zároveň kompatibilní s logovacím, monitorovacím a tracing řešením, takže transparentně probíhá např. zaznamenávání požadavků do logu včetně cesty volání, status kódu a doby trvání, korelace logů, latence a statistických indikátorů s ostatními moduly.

Korelace jednotlivých auditních a logovacích zpráv je zajištěna pomocí přidávání identifikátoru požadavku Correlation-ID do všech logovacích a auditních zpráv. Tento identifikátor je automaticky vytvořen pro každý nový požadavek vstupující do systému přes API bránu, a to pomocí přidání HTTP hlavičky **X-Correlation-Id** s hodnotou vygenerovaného identifikátoru.

1.2.8 Autentizace a autorizace

Architektura počítá jednak s přístupem anonymních uživatelů, jednak s přístupem uživatelů autentizovaných a autorizovaných pomocí odpovídajícího flow OpenID Connect/OAuth, s využitím stávající Centrální Autentizační Služby (CAS) UK.

Pro přístup autentizovaných uživatelů počítá architektura systému se dvěma hlavními případy užití:

- Uživatel přistupující k systému pomocí prohlížeče skrze webový Portál
- Jiný systém/uživatel přistupující přímo k veřejnému API systému

V případě uživatele přistupujícího pomocí webového prohlížeče proběhne autentizace a autorizace ve webovém prostředí Portálu s využitím stávající Centrální Autentizační Služby (CAS) UK. Z pohledu aplikačních modulů bude výsledkem přihlášení access token, který obdrží Portál jakožto vstupní uživatelská webová brána do SIS.

Na základě přijatého access tokenu a z něj odvozených informací o přihlášeném uživateli může Portál rozhodnout, ke kterým portálovým aplikacím bude uživateli poskytnutý přístup. Pro vstup do specifické portálové aplikace musí Portál následně požádat o poskytnutí odpovídajícího HTML UI specifický modul. V rámci tohoto volání Portál poskytne modulu také access token kontextu transakce, případně další odvozené informace o přihlášeném uživateli. Jestliže volaný modul potřebuje navíc kontaktovat další modul, musí mu v rámci odpovídajícího API volání tato data také přeposlat.

Podobně v případě přístupu přes veřejné API systému obdrží modul v rámci přijatého požadavku také odpovídající access token a z něj odvozené informace. Tato data bude v případě volání dalších modulů těmto modulům také přeposílat. Viz též níže sekci Technické požadavky na frontendové moduly.

Jednotlivé moduly můžou na základě obdrženého access tokenu a dalších odvozených informací dále přesněji vyhodnocovat interní autorizační pravidla v závislosti na specifikách své aplikační logiky. Detaily autorizační logiky specifické pro daný modul budou upřesněné v zadávací dokumentaci.

1.2.9 Perzistentní datová úložiště

Pro perzistentní ukládání dat má každý modul k dispozici následující tři druhy úložišť:

- RDBMS – Relační databáze podporující transakce
- File/blob úložiště – S3
- Fulltext indexovaná dokumentová databáze (Document Store)

Pro všechny výše uvedené nástroje pro perzistenci dat zabezpečí zadavatel zároveň odpovídající řešení pro zálohu dat.

Všechny tyto nástroje jsou zároveň spravovány centrálně a přístupové údaje k nim jsou jednotlivým modulům poskytovány dle výše popsaného mechanismu sdílení přístupových údajů.

Veškeré změny nutné pro instalaci nebo upgrade se provádí automatizovanými migračními skripty poskytnutými dodavatelem. Úkolem těchto skriptů je zabezpečit reprodukovatelnost instalace na dalších prostředích.

Z důvodu použití kontejnerizace a automatického horizontálního škálování nesmí moduly ukládat žádná persistentní data na lokální disk. Jakákoliv potřeba ukládat data na disk dočasně musí být předem konzultována a odsouhlasena zadavatelem. Detaily takové případné implementaci pak musí být popsány v dodavatelem doložené technické dokumentaci.

1.2.9.1 *Relační databáze*

Standardní relační databáze bude v drtivé většině případů použita jako primární nástroj pro perzistentní uložení dat. Jedním z hlavních důvodů je nutnost integrace nově vyvíjených modulů s původním Studijním informačním systémem na datové úrovni, protože integrace na úrovni databáze je jediný původním systémem podporovaný způsob napojení. Původní systém využívá databázi Oracle.

Pro každý modul tedy bude vytvořeno nové databázové schéma, v rámci kterého budou vytvořeny pohledy (views) pro čtení dat sdílených s původním systémem, a také uložené databázové procedury (stored procedures) pro vykonávání zápisových transakcí. Detailní popis dostupných databázových prostředků je dodán jako součást zadávací dokumentace daného modulu.

Kromě práce se sdílenými (starými) daty budou některé moduly potřebovat také ukládat data odpovídající novým, doposud nevidovaným byznys objektům. Pro tyto datové entity bude zadavatelem předepsána datová struktura databázových tabulek, které modul v rámci jemu dostupného databázového schématu bude využívat pro perzistenci datových entit odpovídajícího typu.

Vedle specifikací předepsaných datových objektů budou moduly typicky potřebovat i další pomocné databázové tabulky pro ukládání implementačně specifických perzistentních dat. Strukturu potřebných tabulek sdělí dodavatel zadavateli v průběhu implementace, a to v podobě automaticky spustitelných SQL skriptů. Vytvoření potřebných databázových struktur poté zabezpečí zadavatel.

Každý modul pracující s relační databází musí tento zdroj využívat optimalizovaným způsobem, dle dobrých zvyklostí. Nutností je používání kvalitního Database Connection Pool nástroje (pro Javu např. c3p0) umožňujícího vysokou míru nastavitelnosti a sdílení databázových spojení. Nastavení Database Connection Poolu pak musí být dostupné v rámci konfigurace modulu, který ho využívá. Samozřejmostí je pak používání prepared statements a dalších standardních doporučení při práci s relační DB.

1.2.9.2 *File/blob úložiště – S3*

Pro potřeby ukládání souborů nebo blobů je pro každý modul k dispozici objektové úložiště dostupné pomocí S3 API, poskytované systémem Ceph. V případě potřeby je možné vytvořit pro daný modul i vícero S3 bucketů.

Vytváření S3 bucketů je možné na základě konzultace a schválení zadavatelem. Dodavatel musí kromě účelu a typu užití poskytnout také očekávaný objem ukládaných dat, včetně odhadované četnosti čtecích a zápisových operací.

1.2.9.3 Fulltext indexovaná dokumentová databáze

V odůvodněných případech je možné pro modul vytvořit separátní index v rámci dokumentové databáze Elasticsearch. Tento typ perzistence je vhodný zejména v případech, kdy je potřebná fulltextová indexace dokumentově orientovaných dat.

Vytváření indexů je možné na základě konzultace a schválení zadavatelem. Dodavatel musí kromě účelu a typu užití poskytnout také očekávaný objem ukládaných dat, včetně odhadované četnosti čtecích a zápisových operací.

1.2.10 Audit

Nedílnou součástí procesování většiny příchozích požadavků daným modulem je synchronní, transakčně korektní a dostatečně průkazné vytváření odpovídajících auditovacích záznamů popisujících důležité kontextuální podrobnosti procesovaných požadavků. Vytvářené auditní záznamy jsou pak neměnné a slouží primárně jako zdroj dat pro naplnění legislativních požadavků, nebo také pro účely reportingu.

Součástí zadávací dokumentace pro každý modul je také seznam auditních událostí, které nastávají v rámci daného modulu po dobu jeho aplikačního běhu. Příkladem takových událostí může být například již zmiňovaná obsluha příchozích požadavků, generování odchozích požadavků, ale také například start/stop modulu, runtime změna konfigurace, přihlášení uživatele, import dat, zpuštění důležitých automatizovaných procesů na pozadí, detekce alertu nebo chyby systému, zaslání e-mailu, atd.

Každý záznam o auditní události musí obsahovat:

- Časovou značku (timestamp) události
- Typ události
- ID služby (modulu)
- ID instance
- ID uživatele
- ID požadavku
- Correlation ID (viz sekce Logování)
- Session ID (ID sezení přihlášeného uživatele, viz níže sekce Technické požadavky na frontendové moduly)
- ID nebo jméno vykonávané akce
- Další položky specifické pro daný typ události specifikované v zadávací dokumentaci modulu (typicky vyžadované legislativou a platnými směrnici)

Přesný seznam všech pro modul předepsaných auditních událostí, které modul musí implementovat, včetně požadované struktury dat, je součástí zadávací dokumentace daného modulu.

Auditní záznam pro předepsanou událost musí být uložen perzistentním a transakčně korektním způsobem jako nedílná součást odpovídajícího výpočetního procesu. Například, nemělo by být možné vrátit data v rámci obsluhy požadavku ale přitom nevytvořit odpovídající auditní záznam, nebo naopak, neobsloužit požadavek ale přitom vytvořit auditní záznam o jeho obsluze. Tato vlastnost se typicky dosahuje pomocí vytváření auditních záznamů v rámci stejné databázové transakce, uvnitř které probíhá i obsluha procesovaného požadavku a zápis aplikačních dat. Jinými slovy, pro vytváření auditních záznamů bude použit tzv. Outbox Pattern, s outbox tabulkou v databázi modulu.

Kromě samotného sémantického významu jednotlivých auditních událostí je tyto možné dělit do dvou hlavních kategorií na a) párové, a b) nepárové. Příkladem nepárových událostí je např. start

systému nebo pokus o přihlášení uživatele do systému. Párové události typicky popisují začátek a konec odpovídajícího procesu nebo transakce, přičemž pro daný proces platí, že buď má delší trvání, nebo v jeho průběhu je zvýšená pravděpodobnost možného pádu nebo zaseknutí systému (např. z důvodu nedostatku systémových procesů, čekání na externí zdroje atd.). Párové události jsou tedy typicky používané pro zaznamenání procesování uživatelských požadavků, přičemž jeden auditní záznam je vytvořen při přijetí požadavku (včetně detailů popisujících „kdo se ptá na co“), a druhý auditní záznam je vytvořen při zaslání odpovědi na daný požadavek (detaily zde zachycují „co bylo poskytnuto“, případně úspěšnost (status) dané transakce, dobu trvání, a podobně.

Auditní záznamy vytvářené všemi aplikačními moduly v rámci jejich transakčních databázových schémat jsou kontinuálně přesouvány a agregovány do dlouhodobého centrálního perzistentního úložiště auditních záznamů pomocí interně vyvíjené komponenty Audit Shipper.

1.2.11 Logování

Všechny moduly zapisují logovací záznamy do standardních výstupů, tj. do **stdout** a **stderr**, přičemž do **stderr** by měly být zapisovány pouze chybové zprávy (zprávy úrovně ERROR).

Logy jsou agregovány, zpracovány a uchovávány pomocí platformy Elastic Stack (Filebeat, Logstash, Elasticsearch, Kibana) za účelem možnosti vzájemné korelace událostí ze všech modulů a pro zajištění dostupnosti logů i po kritickém selhání a odstranění kontejneru. Webové rozhraní aplikace Kibana v DEV prostředí bude dodavateli zpřístupněno pro umožnění vyhledávání událostí týkajících se konkrétního modulu, kontejneru, časového rozmezí, ID požadavku či úrovně atd. Do budoucna se plánuje vytvoření vlastní aplikace pro prohlížení logovacích záznamů, který by poskytoval ještě větší pohodlí a přehled pro náhled do logů objemných víceúrovňových transakcí.

Z výše uvedených důvodů musí moduly vytvářet logovací záznamy ve strojově čitelné strukturované formě. Jako výchozí formát bylo zvoleno Elastic Common Schema (ECS) ve formátu JSON (<https://www.elastic.co/guide/en/ecs-logging/overview/current/intro.html>). Tento formát byl dále rozšířen o několik přídatných atributů. Následující tabulka uvádí přehled povinných atributů (ECS fields), které musí obsahovat každý logovací záznam. Samozřejmě, je možné logovat i další metadata dle ECS standardu, nicméně níže uvedené položky jsou povinné.

Název atributu	Popis	Příklad
@timestamp	Časová značka logovacího záznamu	2022-10-11T20:48:18.054Z
custom.nano	Počet nanosekund v rámci aktuální sekundy z časové značky logovací události. Slouží pro rozlišení pořadí událostí/zpráv vytvořených v rámci stejné milisekundy.	54230932
log.level	Log level logovací zprávy. Možné hodnoty jsou ERROR, WARN, INFO, DEBUG, TRACE. Tabulka uvedená níže obsahuje popis logovacích zpráv, které má modul vytvářet pro jednotlivé logovací levely.	INFO
service.name	Jméno nebo identifikátor modulu, stanovený na základě domluvy se zadavatelem	portal

Název atributu	Popis	Příklad
message	Obsah textu logovací zprávy	Received request: /portal/
error.stack_trace	Stacktrace logovací zprávy (je-li dostupný), určený zejména pro chybové zprávy	java.lang. NullPointerException at java.base/ java.util.Objects. requireNonNull (Objects.java:208) at ...
custom.correlation.id	Unikátní ID zpracovávaného požadavku, které bylo přiřazeno pomocí platformy API Gateway při vstupu do systému. Všechny moduly v rámci architektury si při následných voláních tento identifikátor odevzdávají v HTTP hlavičkách.	2b7e26cc-fcdb-429f- b685- f5150c2bb95a#1765
custom.uuid	ID logovacího záznamu ve tvaru UUID, vygenerováno modulem při vzniku záznamu	cb9321ba-b30f-47ad- 90b9-781fb310576a
custom.has_children	Boolean příznak indikující, zda-li daná logovací událost je počátkem logicky podřazeného výpočetního podstromu obsahujícího podřazené logovací záznamy (které mohou být vytvořené jiným modulem nebo volanou komponentou modulu). Při stromovém zobrazení logovacích záznamů si je možné logovací záznamy s hodnotou tohoto příznaku nastavenou na „true“ možné představit jako rozkliknutelný podstrom podřazených logovacích událostí.	false
custom.parent	ID přímo nadřazeného rodičovské logovací zprávy. Jestliže je aktuální požadavek vykonáván jako podřazená operace nějaké nadřazené části aplikační logiky, pošle nadřazený modul nebo komponenta modulu identifikátor rodičovské logovací zprávy (kořen logovacího podstromu) pomocí HTTP hlavičky X-Parent-Id , nebo pomocí interních komunikačních cest mezi interními komponenty moduly. Od podřazené aplikační logiky se pak očekává vyplňování tohoto identifikátoru do všech vytvářených zpráv až do momentu, kdy nevznikne nový logovací podstrom. Způsob vytváření a užití parent id je také demonstrován pomocí zdrojového kódu vzorových modulů, které budou dodavateli zpřístupněny v rámci přístupu do GitLab.	b0da9c30-b7f4-4210- 8605-0b7d797bcf20

Následující tabulka popisuje, jaký typ logovacích zpráv je vyžadováno vytvářet v rámci jednotlivých logovacích levelů.

Log level	Typ požadovaných logovacích zpráv
ERROR	<ul style="list-style-type: none"> Zalogování chybových stavů, z nichž se modul (proces zpracování požadavku) nezotavil, včetně stacktrace
WARN	<ul style="list-style-type: none"> Zalogování chybových a "deprecated" stavů, z nichž se modul (proces zpracování požadavku) zotavil
INFO	<ul style="list-style-type: none"> Zalogování zahájení a ukončení každé transakce/requestu včetně ID uživatele a status kódu (transakcí se rozumí každá naplánovaná aktivita - job, aktivita iniciovaná uživatelem i aktivita iniciovaná jinou komponentou systému) Zalogování zahájení a ukončení komunikace s ostatními moduly a systémy třetích stran Modul zajistí dostupnost informací o činnosti modulu pro potřeby zpětné diagnostiky neočekávaných a náhodných stavů
DEBUG	<ul style="list-style-type: none"> Zalogování interních kroků aplikační logiky z pohledu procesního flow takovým způsobem, aby bylo možné ověřit korektnost procesního algoritmu Zalogování všech ostatních zpráv, které pomohou případné diagnostice neočekávaných stavů
TRACE	<ul style="list-style-type: none"> Zalogování podrobností o průběhu vykonávání aplikační logiky, obsahujících zejména objemný obsah, např. payload transakcí, TLS handshake, velmi jemné krokování složitějších algoritmů apod.

Následující ukázka kódu v jazyce Java demonstruje jeden z možných způsobů vytváření logovacího záznamu ve formátu JSON na základě dodaných strukturovaných hodnot jednotlivých atributů (fieldů).

Ukázka Java kódu – příklad serializace logovacího záznamu
<pre> public String toJson() { JSONObject jsonLog = new JSONObject(); jsonLog.put("@timestamp", DateTimeFormatter.ISO_INSTANT.withZone(ZoneOffset.UTC).format(instant)); jsonLog.put("custom.nano", Integer.toString(instant.getNano())); jsonLog.put("custom.correlation.id", correlationId); if (uuid != null) jsonLog.put("custom.uuid", uuid); if (parent != null) jsonLog.put("custom.parent", parent); if (stackTrace != null) jsonLog.put("error.stack_trace", stackTrace); jsonLog.put("log.level", level.name()); jsonLog.put("message", message); jsonLog.put("custom.has_children", hasChildren ? "true" : "false"); jsonLog.put("service.name", serviceName); </pre>

```
return jsonLog.toString();  
}
```

V některých případech bude nutné citlivé údaje vkládané do logovacích záznamů šifrovat. Každé šifrované zpráve musí předcházet stejná nešifrovaná zpráva bez citlivých údajů. Seznam citlivých údajů bude pro každý modul upřesněn v zadávací dokumentaci.

Defaultní log level je nastavitelný pomocí konfigurace modulu (v proměnné prostředí). Nicméně komponenty systému předřazené před volání samotného modulu (např. Portál, nebo Centrální API Modul) poskytují schopnost nastavovat požadovaný dynamický log level pro vykonávanou transakci (požadavek) na základě kontextuálních informací (např. potřeba logování v levelu DEBUG pouze pro uživatele XY). Dynamicky určený log level požadavku tedy jednotlivé aplikační moduly mohou pro danou transakci obdržet v HTTP hlavičce s názvem **X-Log-Level** daného volání. V případě podřazeného navazujícího volání dalších modulů musí modul tuto hlavičku dalším modulům také přeposlat.

Aplikační logika modulu musí zabezpečit, aby se pro logovací zprávy, pro které je potřeba náročnější příprava výstupních dat (např. serializace větších objektů do paměti atd.), tato příprava výstupních dat nevykonávala v případě, kdy odpovídající logovací zpráva nebude dle aktuálního log levelu zaslána na výstup (ať již z konfigurace nebo dle dynamicky vyžadované úrovně logování). Například, v úrovni DEBUG může v kódu probíhat logování celého obsahu HTTP transakcí. Je nežádoucí, aby se v případech, kdy je aktuální logovací úroveň nižší (ERROR až INFO), prováděla serializace obsahu HTTP transakcí do paměti, jelikož by to zcela zbytečně zabíralo jak procesorové, tak i paměťové prostředky systému při frekventovaném běhu takových transakcí.

Při použití některých externích knihoven může být komplikované zapisovat na výstup všechny zprávy v požadovaném strukturovaném formátu (knihovny můžou nějaké zprávy již generovat). Dodavatel by ale měl v součinnosti a na základě dohody se zadavatelem rozhodnout o odchytnutí těchto zpráv a jejich zapisování na výstup v požadovaném formátu, pakliže to nebude představovat nepřiměřenou vývojářskou náročnost.

HTML/JS frontend aplikace standardně logují do vývojářské konzole a do bufferu, v produkci je log do konzole vypnutý.

1.2.12 Tracing

Mezi hlavní cíle nasazení tracingu patří zobrazení trvání dotazů a souvisejících metadat, korelace latence napříč všemi moduly, dostupnost těchto informací i po kritickém selhání a odstranění kontejneru, nebo také vyhledávání informací týkajících se konkrétního modulu, kontejneru, časového rozmezí či požadavku.

Jako hlavní technologie pro implementaci tracingu v této architektuře systému jsou použité:

- OpenTelemetry
- Elastic APM

Je doporučeno pro implementaci modulů využít dostupnou instrumentaci pomocí OpenTelemetry SDK. Pro důležité logické celky aplikační logiky může být v zadávací dokumentaci modulu předepsána vlastní implementace nových měřených úseků (spanů). Dodavatel může taktéž navrhnout zadavateli vytvoření vlastních nových měřených úseků.

Sbírané tracing záznamy jsou odesílány knihovnou OpenTelemetry SDK do Elastic APM, kde jsou uchovávány, analyzovány a zobrazovány pro cílové uživatele těchto údajů. Přístup do Elastic APM (Kibana) bude v rámci DEV prostředí poskytnutý také dodavateli.

V případě nemožnosti použít OpenTelemetry SDK je možné vytvářet vlastní datové zprávy ve standardním otevřeném formátu OpenTelemetry a zasílat je pomocí standardních protokolů (OTLP/gRPC) do Elastic APM.

Trace musí obsahovat Correlation ID (viz sekce Síťový provoz), časovou značku, ID instance, unikátní ID v rámci celého systému, ID uživatele, status code, a informace o požadavcích vyvolaných tímto požadavkem. Případné další požadavky na obsah traců může být upřesněn v zadávací dokumentaci modulu.

Tracing daného modulu musí být vypínatelný a nastavitelný pomocí proměnných prostředí (konfigurace modulu).

1.2.13 Metriky a monitoring

Mezi důležité vlastnosti zvolené architektury patří také sběr metrik ze všech provozovaných modulů, kde metrikou se rozumí číselná řada popisující nějakou vlastnost systému/modulu v čase. Příkladem mohou být počty přijatých a odeslaných transakcí, jejich průměrná/minimální/maximální délka trvání, počet otevřených uživatelských sezení, rychlost vyřizování jednotlivých databázových dotazů, četnost spouštění jobů na pozadí atd. Tyto metriky jsou sbírané (nebo odesílané modulem) v pravidelných časových intervalech (např. jednou za minutu). Průměrně složitý modul může poskytovat stovky různých metrik.

Mezi hlavní důvody sběru metrik patří:

- **diagnostika systému/modulů**
- rutinní sledování provozu systému pomocí administrátorských dashboardů zobrazujících aktuální (živý) stav systému a přehled o jeho aktivitě
- analýza a sledování selhání a neočekávaných stavů
- zobrazení statistických informací o četnosti selhání v jednotlivých modulech
- poskytnutí informací, jež koncovému uživateli pomohou určit, zda chybný stav, jenž nastal, je způsoben chybou na straně systému nebo je externího původu
- vzájemná korelace statistických údajů všech modulů, instancí a HW prostředků
- **automatické notifikace v případě překročení povolených mezí vybraných metrik (alertování)**
- různé pohledy pro vlastníky systému, provozovatele, správce infrastruktury a vývojáře
- **reporting**

Tyto metriky jsou sbírané a ukládané ve specifické databázi určené pro ukládání numerických časových řad. Pro tento účel byla zvolena platforma Prometheus/Thanos. Agregované statistiky jsou automaticky analyzovány systémem Alertmanager, který v případě překročení očekávaných limitů automaticky vytvoří nový záznam (ticket) v systému Redmine a upozorní administrátory v aktuální on-call směně. Metriky je možné prohlížet pomocí aplikace Grafana, ke které v rámci DEV prostředí obdrží dodavatel přístup.

Pro automatický sběr musí každý modul vystavit endpoint s metrikami v Prometheus formátu. Alternativou je aktivní posílání metrik na Pushgateway. Forma odevzdávání metrik bude domluvena mezi zadavatelem a dodavatelem na začátku implementačního projektu daného modulu.

Mezi hlavní druh metrik budou patřit zejména informace o stavu, výkonu a vytížení modulu. Požadované metriky budou specifikovány v zadávací dokumentaci modulu. Dodavatel může po domluvě se zadavatelem dodat i další metriky související s implementací daného modulu pro informovanější monitoring a ladění systému. **Dodavatel musí dodat dokumentaci poskytovaných metrik (jednotky, způsob měření, přesná sémantika atd.) a doporučení pro nastavení alertů pomocí PromQL.**

Každý backendový modul bude standardně poskytovat zejména následující metriky:

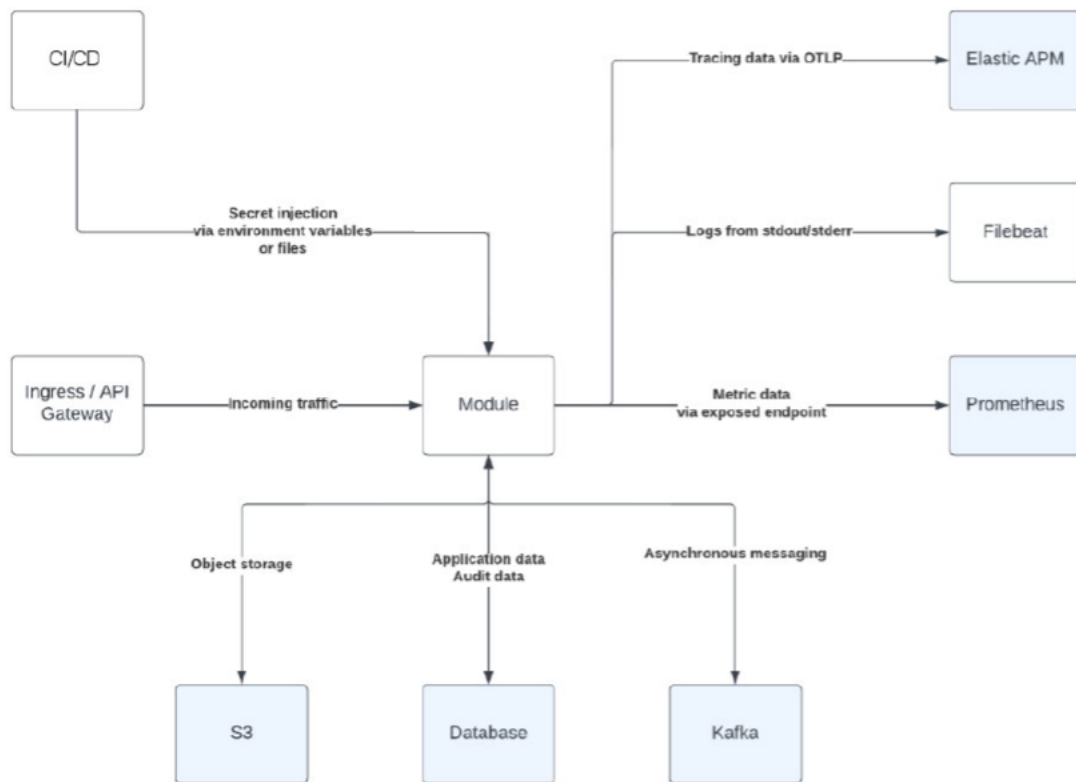
- počet přijatých HTTP requestů na HTTP rozhraní
- počet neúspěšných HTTP requestů
- počet úspěšných HTTP requestů
- velikost příchozích HTTP requestů v bytech – min, max, avg
- velikost odchozích HTTP responsů v bytech – min, max, avg
- Pro každý typ GET operace (čtení detailu):
 - počet operací čtení detailu (get)
 - doba odezvy čtení detailu (get) - min, max, avg
 - počet úspěšného čtení detailu
 - počet selhání čtecích operací rozdělený podle typů chyb (např. Požadavek na neexistující entitu, Chyba při práci s databází, apod.)
- Pro každou změnovou operaci
 - počet změnových operací definovaných údajů (put)
 - počet úspěšných změnových operací
 - počet selhání změnových operací
 - doba odezvy změnových operací (put) - min, max, avg
- doba odezvy práce s databází - min, max, avg – pro každý typ databázové interakce (prepared statement) zvlášť

Každý frontendový modul bude poskytovat zejména následující metriky:

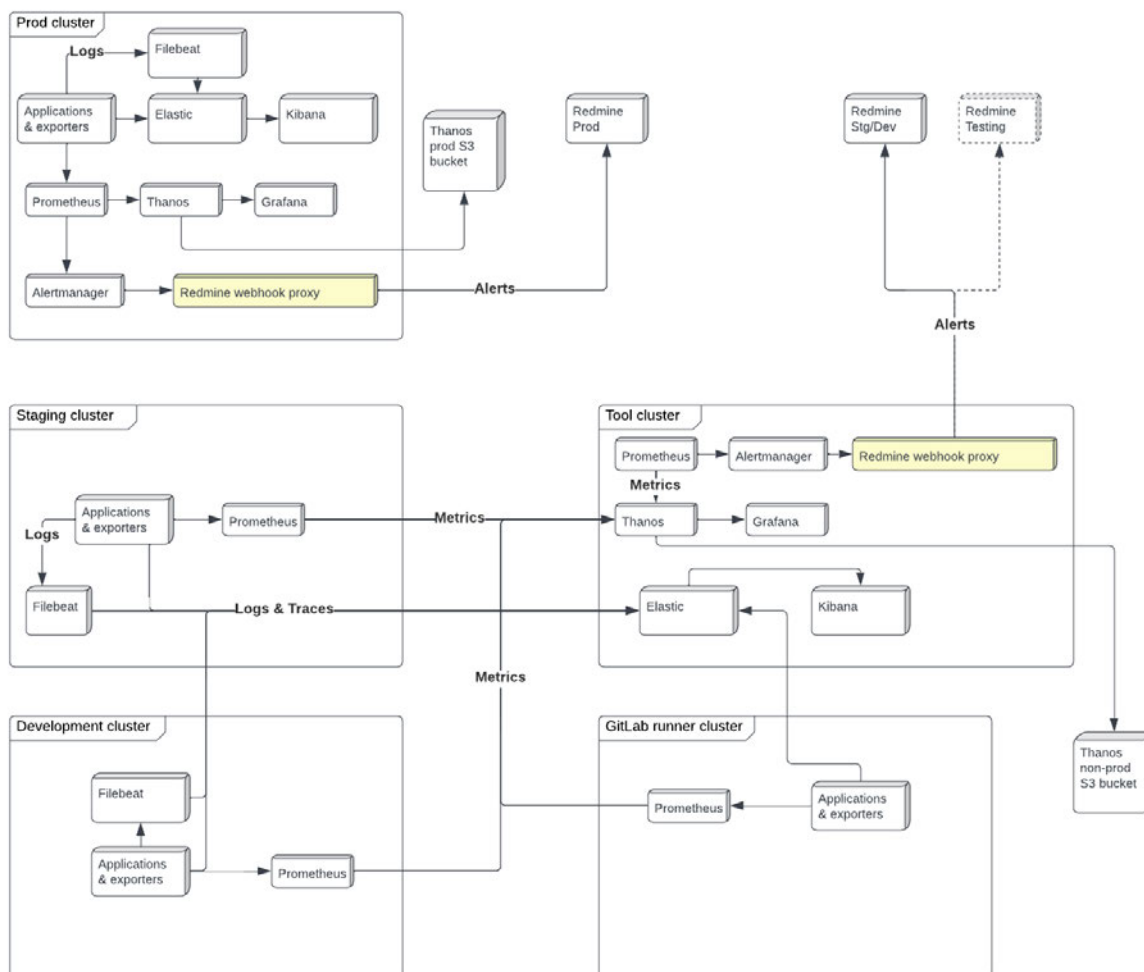
- počet přijatých HTTP requestů na HTTP rozhraní
- počet neúspěšných HTTP requestů
- počet úspěšných HTTP requestů
- velikost příchozích HTTP requestů v bytech – min, max, avg
- velikost odchozích HTTP responsů v bytech – min, max, avg
- Pro každý typ zobrazení detailu:
 - počet UI requestů na zobrazení detailu
 - doba odezvy vyřízení UI requestů na zobrazení detailu – min, max, avg (zvlášť pro každou stránku)
- Pro každý typ zobrazení detailu:
 - počet UI requestů na vyhledávání
 - doba odezvy vyřízení UI requestů na vyhledávání – min, max, avg (zvlášť pro každý typ vyhledávání)
- doba odezvy interakcí s backendovým modulem – min, max, avg - zvlášť pro každý typ API volání

1.2.14 Diagramy primárních interakcí modulu

Následující diagram shrnuje hlavní komponenty infrastruktury, se kterými budou aplikační moduly přímo interagovat (mimo komunikaci s ostatními aplikačními moduly). Modře zvýrazněné komponenty vyžadují přímou integraci do kódu modulu.



Následující diagram popisuje tok metrik, logů, traců a alertů celým systémem. Sdílený monitoring pro Development a Staging cluster se nachází v Tool clusteru. Produkční cluster obsahuje svůj oddělený monitoring. Komponenty vyvíjeny interně na UK jsou zvýrazněny žlutě. Jednotlivé vyvíjené moduly jsou na diagramu zahrnuty pod komponentou "Applications & exporters".



1.2.15 Reporting

Každý aplikační modul musí poskytovat data pro sdílenou reporting infrastrukturu v takové míře, aby bylo možné splnit požadavky na reporting od stakeholderů – typicky se bude jednat o data z monitoringu a auditu, nicméně ve vybraných případech i o jiný způsob vhodného poskytnutí dat pro potřeby požadovaných reportů, např. ve formě API definovaného k tomuto účelu. Veškeré detaily budou upřesněny v zadávací dokumentaci modulu.

1.2.16 Dostupnost a spolehlivost (High Availability)

Všechny aplikační moduly by měly podporovat provoz ve vysoké dostupnosti (HA). Každý modul by tedy mělo být možné provozovat ve vícero instancích zároveň a umožnit tak i horizontální škálování systému. Přesnější výkonové požadavky a propustnost jednotlivých endpointů (množství požadavků za časové okno, rychlost odezvy atd.) budou specifikovány v zadávací dokumentaci daného modulu. V ideálním případě by všechny moduly měly být implementovány bezstavově (stateless) z důvodu jednoduché škálovatelnosti.

V některých konkrétních případech lze uvažovat i o implementaci bez podpory vysoké dostupnosti (např. kvůli zvýšení celkové propustnosti pro danou transakci za předpokladu, že požadovaný výkon není technologicky možné jinak docílit), nebo o implementaci vysoké dostupnosti modulů

vyžadujících stavovost pomocí tzv. sticky sessions (nikoliv plně stateless). Každá taková výjimka však musí být schválena zadavatelem, a to pouze ve specifických a dobře odůvodnitelných případech.

Změnu konfigurace modulu a nasazení nové verze by mělo být ve většině případů možné bez vypnutí modulu (rolling update) pro zabezpečení co nejvyšší dostupnosti systému. Samozřejmě v odůvodněných případech je možné nasazení nové verze také po čas plánovaného výpadku (downtime), například v situacích vyžadujících náročnější změnu struktury relační databáze, migrace dat atd.

1.3 Obecné technické požadavky na moduly

Každá aplikační doména (z pohledu koncového uživatele modul v Portálu SIS) bude implementována nejméně pomocí dvou modulů z pohledu runtime:

- **„Backendový“ modul** – zabezpečující implementaci byznys logiky, přístup k perzistentním datům, logickou autorizaci specifickou pro danou doménu, poskytování strukturovaných dat pro „frontendový“ modul generující uživatelské HTML rozhraní
- **„Frontendový“ modul** – zabezpečující HTML reprezentaci uživatelského rozhraní vloženého do hlavního Portálu SIS

Všechny moduly poběží v kontejnerizovaném prostředí Kubernetes jako nezávislé kontejnery. Pro každý modul (kontejner) bude vytvořen separátní GitLab projekt a CI/CD pipeline.

1.3.1 Technické požadavky na backendové moduly

Pro implementaci backendových modulů jsou povoleny následující technologie:

- Java/Kotlin (+ Spring Boot)
- TypeScript + Next.js/Nest.js
- Python + WSGI/ASGI
- C# + ASP.NET Core

1.3.2 Technické požadavky na frontendové moduly

Stěžejní základ pro implementaci frontendu pro specifickou portálovou aplikaci je zadavatelem dodána UX/UI analýza, jakožto součást zadávací dokumentace modulu. Pro dosažení jednotného designu bude dodavateli poskytnutá také knihovna společných komponent, vybudovaná s použitím konceptu Atomic Design¹, která bude postupně rozšiřována o nové komponenty a šablony.

Pro server-side část implementace frontendových modulů jsou povoleny stejné technologie jako pro implementaci backendových modulů, uvedené výše.

Pro browser-side část implementace frontendových modulů jsou povoleny následující technologie:

- HTML/CSS + Vanilla JS
- TypeScript + React

Uživatelská rozhraní musí podporovat zobrazování v různých jazykových mutacích. Jazyk zobrazení bude vyplývat z nastavení uživatelského profilu v rámci centrálního modulu Portál, který informaci o požadovaném jazyku přepoše specifickému frontend modulu pomocí cookie s názvem **sis_lang**

v HTTP hlavičce požadavku. Není-li určeno jinak, modul musí poskytovat českou i anglickou mutaci uživatelského rozhraní. Případné další požadované jazykové mutace budou specifikovány v zadávací dokumentaci modulu.

Při práci uživatelů ve webové aplikaci evidujeme i ID sezení (session), které trvá od autorizace uživatele na Portálu či v bráně veřejného API až po jeho odhlášení. Portál udržuje toto session-id v cookie s názvem `sis_sid` a vždy přeposílá tuto cookie ve volání specifického modulu.

Kromě jazyku zobrazení bude Portál posílat i následující HTTP hlavičky:

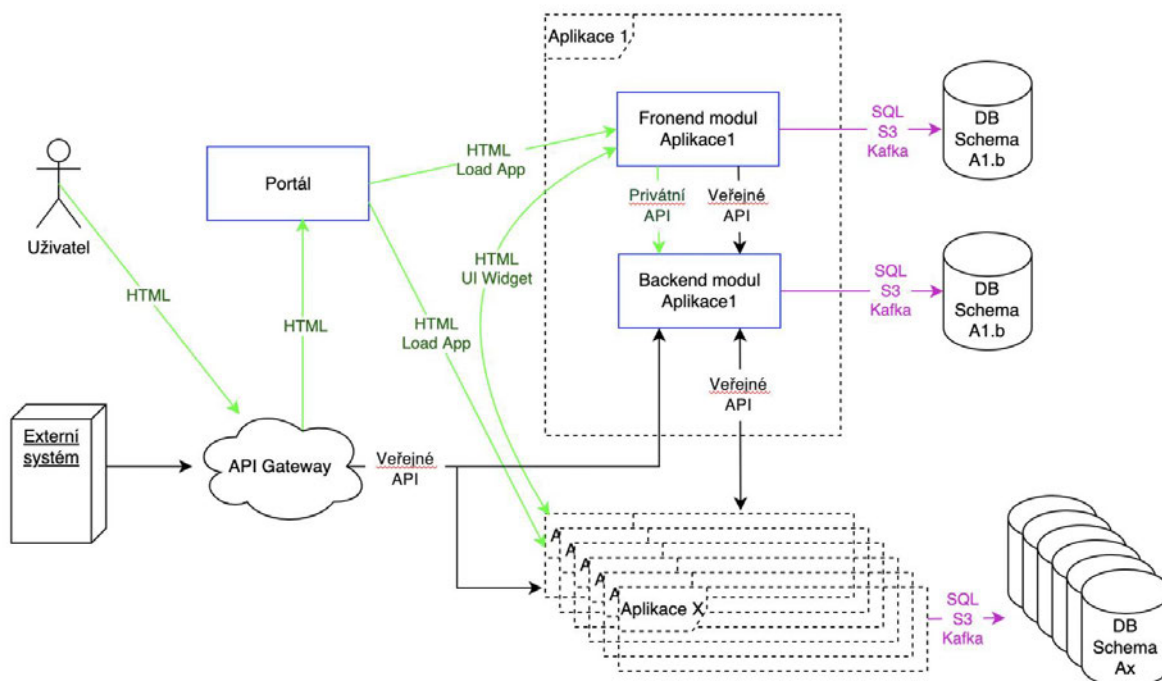
Jméno HTTP hlavičky	Popis
X-Correlation-Id	Unikátní ID zpracovávaného požadavku, které bylo přiřazeno pomocí platformy API brány při vstupu do systému. Všechny moduly v rámci architektury si při následných voláních tento identifikátor odevzdávají v HTTP hlavičkách.
X-Base-Path	Každá portálová aplikace bude mít přidělený nějaký namespace pro vytváření unikátních cest pro context-path HTTP requestů. Prefixem namespace aplikace bude vždy namespace centrálního Portálu, jehož hodnota je portálovým aplikacím odevzdávaná pomocí této HTTP hlavičky. Příklad zasílané basePath: „/portal“. Jestliže přiděleným identifikátorem portálové aplikace je například „app1“, bude finální namespace aplikace vypadat následovným způsobem: „/portal/app1/“. Veškeré další zdroje, které prohlížet bude potřebovat pro Aplikaci1 dotáhnout musí jako prefix context-path používat tento namespace, na základě kterého Portál ví, které portálové aplikaci má přeposlat požadavek na daný zdroj.
X-Log-Level	Dynamicky určený logovací level pomocí kterého má modul logovat aktuálně procesovaný požadavek. V případě podřazeného navazujícího volání dalších modulů musí modul tuto hlavičku dalším modulům také přeposlat. Možné hodnoty jsou ERROR, WARN, INFO, DEBUG, TRACE.
X-Parent-Id	ID přímo nadřazeného rodičovské logovací zprávy. Jestliže je aktuální požadavek vykonáván jako podřazená operace nějaké nadřazené části aplikační logiky, pošle nadřazený modul nebo komponenta modulu identifikátor rodičovské logovací zprávy (kořen logovacího podstromu) pomocí HTTP hlavičky X-Parent-Id, nebo pomocí interních komunikačních cest mezi interními komponenty moduly. Od podřazené aplikační logiky se pak očekává vyplňování tohoto identifikátoru do všech vytvářených zpráv až do momentu kdy nevznikne nový logovací podstrom. Způsob vytváření a užití parent id je také demonstrován pomocí zdrojového kódu vzorových modulů, které budou dodavateli zpřístupněny v rámci přístupu do GitLab
X-User-Id	Pro požadavky neanonymního uživatele přihlášeného na portálu je v hlavičce X-User-Id ID tohoto uživatele. V prostředí UK je tímto ID jednoznačné UKČO uživatele.

1.3.3 Interakce mezi moduly

Následující obrázek ukazuje schéma jednotlivých API volání pro dva různé případy užití.

1. Prvním je uživatel (osoba) přistupující na centrální Portál SIS s cílem vstoupit do portálové Aplikace1. Moduly Aplikace1 poskytnou Portálu HTML kód, který Portál vloží do celkového rámce HTML stránky vrácené prohlížeči uživatele. Úkolem frontendového modulu Aplikace1 je zabezpečit uživatelské HTML rozhraní pro Portál, a to primárně za pomoci backendového modulu Aplikace1, implementujícího aplikační logiku Aplikace1, případně jiných modulů systému (ať již backendových poskytujících např. REST API, nebo frontendových poskytujících embedovatelné HTML widgety). Volání, jejichž návratovou hodnotou je uživatelské rozhraní v HTML formátu, jsou vyznačena zelenou barvou. Na tomto místě je potřeba zmínit, že každý backendový modul může pro svůj frontendový modul vystavovat kromě zadávací specifikací předepsaného veřejného (aplikačního) API také privátní „frontendové“ API. Aplikační (veřejné) i neveřejné API pak společně poskytují frontendovému modulu potřebné funkce a data.

2. Druhým případem užití je přímé volání veřejného API systému externí aplikací. Volání veřejného (aplikačního) API jednotlivých modulů je vyznačeno černou barvou.



Příklad jednoduché ukázkové portálové aplikace poskytující uživatelské HTML rozhraní pro integraci do centrálního Portálu bude dodavateli zpřístupněno v rámci přidělení přístupu do platformy GitLab.

2 Obecné požadavky na uživatelská rozhraní

2.1 Obecné principy uživatelského rozhraní

Součástí zadávací dokumentace pro uživatelské rozhraní jsou:

1. Graficky zpracované náhledy pro rozpracovaný modul.

2. Samostatně zpracované komponenty, které se v modulu vyskytují

Grafická podoba zpracovaných náhledů není finální grafikou, ale pouze pracovním grafickým návrhem UI. Rozpracování finální grafiky není součástí zadání jednotlivých modulů. Přesto obrazovky a komponenty budou mít jednotný vzhled a společně budou tvořit jednotný design systému, jehož správná a důsledná implementace je potřebná pro rychlé a správné nasazení finální grafiky.

Komponenty UI, ze kterých se budou skládat moduly v jednotlivých zadáních budou tvořit společnou knihovnu, která se bude postupně doplňovat s každým nově zadaným modulem. Všechny komponenty UI přítomné v návrzích UI budou mít svůj zdroj v knihovně komponent.

Součástí knihovny budou “placeholders” prvků určené pro poskytování zpětné vazby UI v případě delší odezvy modulů. Finální podoba těchto prvků bude řešená v rámci grafického návrhů. Základní zpětná vazba (spinner) má být uživateli poskytnutá všude tam kde se očekává odezva delší než 1000 ms.

2.2 Předání grafických podkladů pro UI

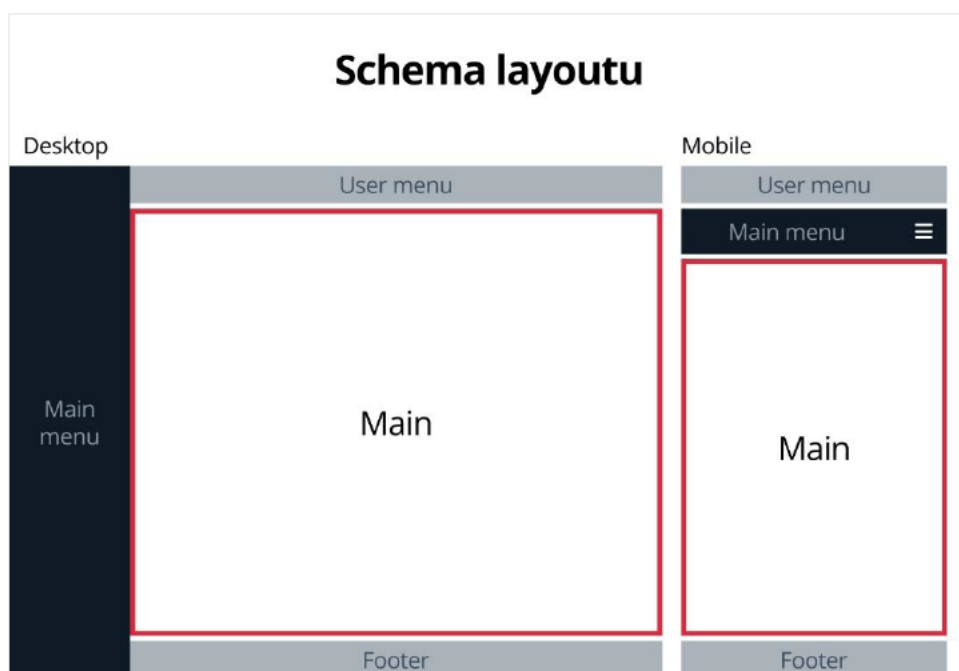
Zadávací dokumentace pro UI konkrétního modulu bude obsahovat:

1. Exporty návrhů ve dvou variantách - desktop (šířka 1512 px) a mobil (šířka 414 px) a ve dvou formátech JPG a PDF.
2. Přístup ke zdrojovým souborům návrhů (Figma). Odkaz na soubor s komponenty společnými pro všechny doposud zpracované moduly v rámci projektu (Figma).
3. Flowchart obrazovek
4. Interaktivní prototyp ve Figmě

2.3 Uživatelské rozhraní - popis základního layoutu

V této části jsou popsány vlastnosti layoutu z hlediska responzivního chování aplikace.

Uživatelské rozhraní modulů Studijního Informačního Systému vychází z modulární architektury systému a je navrženo tak, aby umožňovalo postupné začleňování nově vytvořených modulů do aplikace. Skládá se ze dvou ovládacích panelů – jeden pro volby uživatelského profilu a druhý pro navigaci v modulech, a ze sekce, určené pro zobrazení zvoleného modulu. Tyto prvky tvoří jednotný základní layout aplikace.



Pro účely zadání je podstatná definice responzivního chování sekce, do níž bude umístěn HTML kód modulu. Obsah zbývajících sekcí layoutu dodá centrální webový Portál.

2.3.1 Základní prvky uživatelského prostředí

- Hlavní navigační panel (MAIN MENU), který obsahuje branding a hlavní nabídku, která slouží k výběru jednotlivých modulů.
- Panel uživatelského menu (USER MENU) – obsahuje informace o uživateli, volby pro přepínání mezi rolemi uživatele a volby pro nastavení dalších preferencí na uživatelské úrovni
- Jednotná patička (FOOTER)
- Hlavní panel modulu (MAIN), ve kterém se zobrazuje aktuální modul

2.3.2 Responzivita a breakpoints

Uživatelské rozhraní je založené na fluidním layoutu a počítá s intenzivním využitím flex CSS komponenty. Breakpoints (BP) jsou minimalizované a jsou uplatněné pro každou ze základních komponent zvlášť. Nevztahují se nutně k velikostem konkrétních zařízení, ale vychází spíše z potřeby komponent. BP pro základní sekce layoutu jsou následovné:

1. MAIN MENU BP: **max-width: 1199px**
 - a. Pod tímto BP se panel zobrazuje nad hlavním obsahem a nabídka je schovaná pod ikonou.
 - b. Nad tímto BP se panel zobrazuje vlevo od hlavního obsahu
2. USER MENU BP: **max-width: 799px**
 - A. Pod tímto bodem jsou některé textové položky sdružené pod ikonku s dropdown menu
 - B. Nad tímto bodem jsou tyto položky umístěné přímo v liště
3. MAIN BP: **max-width: 499px** – tento BP se týká především chování flex prvků. Od tohoto bodu dolů se ruší sloupce ve formulářích a maximální počet sloupců v ostatních komponentách se redukuje na 2.

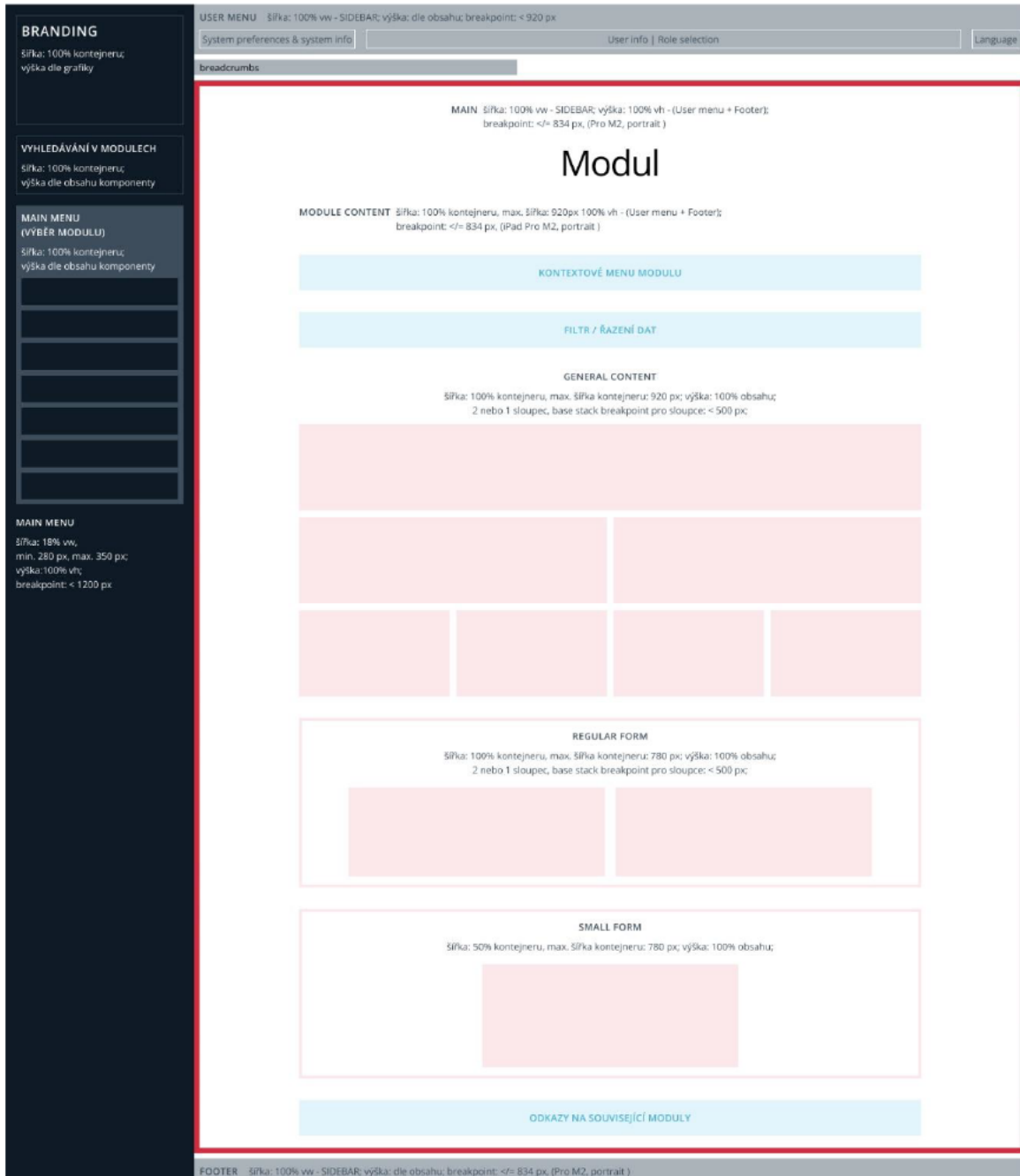
Potřeba dalších BP může přibývat s rozpracováním konkrétních modulů, přesto snaha bude držet se co nejvíce již zmíněných.

2.3.3 Dimenze základních sekcí layoutu

1. MAIN MENU **18% vw, max. šířka 280px**
2. Komponenty v sekci MAIN **100% nadřazeného prvku, max. šířka 920px**
3. Formuláře **100 % nadřazeného prvku, max. šířka 780px**
4. Malé formuláře **100 % nadřazeného prvku, max. šířka 460px**

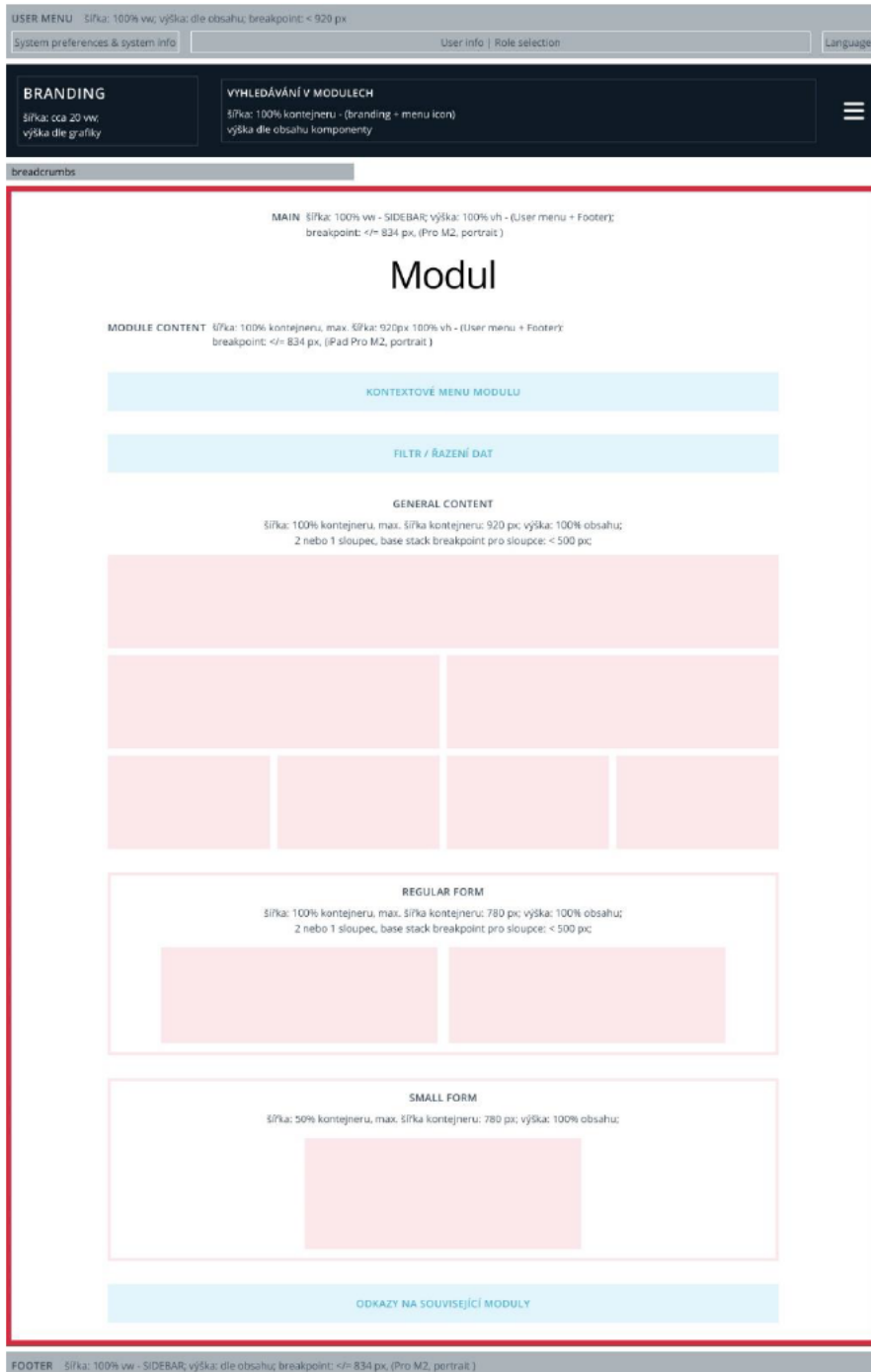
Základní layout - desktop

šířka obrazovky min. 1200 px



Základní layout - tablet

šířka obrazovky < 1200 px



Základní layout - small screen

šířka obrazovky < 800 px

USER MENU šířka: 100%; výška: dle obsahu; breakpoint: < 920 px

System preferences & system info USER MENU DROPDOWN Language

BRANDING
šířka: 100% kontejneru;
výška dle grafiky

VYHLEDÁVÁNÍ V MODULECH
šířka: 100% kontejneru;
výška dle obsahu komponenty

breadcrumbs

MAIN šířka: 100% vw - SIDEBAR; výška: 100% vh - (User menu + Footer);
breakpoint: < /= 834 px, (Pro M2, portrait)

Modul

MODULE CONTENT šířka: 100% kontejneru, max. šířka: 920px 100% vh - (User menu + Footer);
breakpoint: < /= 834 px, (iPad Pro M2, portrait)

KONTEXTOVÉ MENU MODULU

FILTR / ŘAZENÍ DAT

GENERAL CONTENT
šířka: 100% kontejneru, max. šířka kontejneru: 920 px; výška: 100% obsahu;
2 nebo 1 sloupec, base stack breakpoint pro sloupec: < 500 px;

REGULAR FORM
šířka: 100% kontejneru, max. šířka kontejneru: 780 px; výška: 100% obsahu;
2 nebo 1 sloupec, base stack breakpoint pro sloupec: < 500 px;

SMALL FORM
šířka: 50% kontejneru, max. šířka kontejneru: 780 px; výška: 100% obsahu;

ODKAZY NA SOUVISEJÍCÍ MODULY

FOOTER šířka: 100% vw - SIDEBAR; výška: dle obsahu; breakpoint: < /= 834 px, (Pro M2, portrait)

Základní layout - mobile

šířka obrazovky
<= 500 px

USER MENU Šířka: 100%; výška: dle obsahu; breakpoint: <= 920 px

Preferences & info USER MENU DROPDOWN Lang

BRANDING
Šířka: 100% kontejneru;
výška dle grafiky

VYHLEDÁVÁNÍ V MODULECH
Šířka: 100% kontejneru;
výška dle obsahu komponenty

☰

breadcrumbs

MAIN Šířka: 100% vw - SIDEBAR; výška: 100% vh - (User menu + Footer); breakpoint: <= 834 px, (Pro M2, portrait)

Modul

MODULE CONTENT Šířka: 100% kontejneru, max. šířka: 920px 100% vh; breakpoint: <= 834 px, (iPad Pro M2, portrait)

KONTEXTOVÉ MENU MODULU

FILTR / ŘAZENÍ DAT

GENERAL CONTENT
Šířka: 100% kontejneru, max. šířka kontejneru: 920 px; výška: 100% obsahu; 2 nebo 1 sloupec, base stack breakpoint pro sloupec: < 500 px;

REGULAR FORM
Šířka: 100% kontejneru, max. šířka kontejneru: 780 px; výška: 100% obsahu; 2 nebo 1 sloupec, base stack breakpoint pro sloupec: < 500 px;

SMALL FORM
Šířka: 100% kontejneru, max. šířka kontejneru: 780 px; výška: 100% obsahu;

ODKAZY NA SOUVISEJÍCÍ MODULY

FOOTER Šířka: 100% vw - SIDEBAR; výška: dle obsahu; breakpoint: <= 834

2.4 Požadavky na optimalizaci

Návrh uživatelského rozhraní (UI) aplikace musí brát v potaz fakt, že aplikace bude sloužit uživatelům s velmi odlišnými požadavky na zařízení a prohlížeče (zaměstnanci školy vs. studenti), proto je optimalizace většiny případů užítí pro mobilní zařízení i pro desktop počítač/notebook stejně důležitá.

- 1) Desktop
 - a) Windows / Chrome
 - b) Windows / Edge
 - c) Windows / Firefox
 - d) OS X / Safari 15+
 - e) OS X / Chrome
 - f) OS X / Firefox
- 2) Mobile
 - a) Android 10+ / Chrome
 - b) iOS 13+ / Safari
 - c) Android 10+ / Samsung internet

Tento seznam se zakládá na veřejných datech o nejpoužívanějších OS/prohlížečů v ČR a na interních uživatelských statistikách UK.

Minimální velikost obrazovky, pro kterou je aplikace určena je 375 x 667 pro mobilní zařízení a 768 x 1024 pro tablet. Aplikace se má zobrazovat s v souladu s grafickým návrhem jak na desktopovém zařízení, tak na obrazovkách těchto velikostí.

2.5 Požadavky na přístupnost a použitelnost

Aplikace musí splňovat úroveň shody **AA** dle WCAG 2.0. Splnění požadavky na přístupnost je potřeba doložit protokolem z automatické kontroly specializované on-line služby, která bude specifikována dodatečně s dodavatelem. V rámci protokolu jsou pro dodavatele závazné parametry, které jsou předmětem jeho kompetencí a součástí jemu určeného zadání. Splnění požadavky na přístupnost je potřeba doložit protokolem z automatické kontroly specializované on-line služby, která bude specifikována dodatečně s dodavatelem. V rámci protokolu jsou pro dodavatele závazné parametry, které jsou předmětem jeho kompetencí a součástí jemu určeného zadání.

Zde je minimální závazný seznam parametrů schody s WCAG 2.0, relevantní pro dodavatele sw:

1. Správná sémantická struktura HTML kódu
2. Správné zvětšení obsahu při zvětšení/zmenšení
3. Podpora navigace pomocí klávesnice
4. Správné typy formulářových polí dle HTML5
5. Pokud se obsah automaticky mění, uživatel musí mít možnost pozastavit automatické změny, případně přepnout na jejich manuální ovládání
6. Možnost procházet obsah pomocí čtečky obrazovky
7. Možnost přeskočit navigaci pomocí klávesnice
8. Automaticky přesouvat focus na modální okna, vyskakovací okna, upozornění atd.
9. Prevence automatického odhlášení uživatele.
10. Prevence automatického přehrávání zvuku a videa, pokud to není žádoucí chování.
11. Důsledné použití atributu HTML lang
12. Používat atributy ARIA tam, kde struktura HTML není jednoznačná

13. Alternativní způsoby konzumace multimediálních souborů (transkripce dialogů a popis obsahu)
14. Data pro grafy, tabulky, mapy, SVG atd. konzumovatelná prostřednictvím asistenčních technologií

3 Obecné požadavky na strojová rozhraní modulů

Z důvodu vysoké modularizace systému je nutné sjednotit podobu strojových (programovacích) rozhraní jednotlivých back-end modulů. Pod pojmem strojové rozhraní back-end modulu rozumíme rozhraní umožňující strojovou (programovanou) interakci s back-end modulem. Strojovou interakci s back-end modulem rozumíme komunikaci s jinými částmi systému (jiné back-end či front-end moduly), nebo vnějším světem, za účelem výměny dat a volání operací. Rozlišujeme několik druhů strojových rozhraní popsanych v následující tabulce.

Popis druhu strojového rozhraní	Název druhu strojového rozhraní	Vlastník	Specifikace
Volání aplikačních operací poskytovaných back-end modulem pro potřeby výkonu funkcionalit systému zahrnujících CRUD operace nad daty spravovanými modulem a operace implementující části byznys logiky zajišťované modulem.	Veřejné aplikační strojové rozhraní (veřejné API) – určené pro jiné moduly systému	UK	OpenAPI + JSON Schema odvozené z konceptuálního datového modlu
	Privátní aplikační strojové rozhraní (privátní API) – určené pro odpovídající front-end moduly	Dodavatel	OpenAPI + JSON Schema
Šíření a příjem notifikací o událostech, které nastaly uvnitř modulu a mají být pozorovatelné vně modulu, zahrnující události s významem odpovídajícím událostem nastávajícím v rámci byznys logiky zajišťované modulem.	Notifikační rozhraní	UK	JSON Schema odvozené z konceptuálního datového modelu
Přístup k datům spravovaných modulem pro potřeby datově řízené univerzity	Datové rozhraní	UK	Datové schéma (CSVW, JSON Schema, ...) odvozené z konceptuálního datového modelu

Back-endový modul musí poskytovat alespoň jedno veřejné API. Může obsahovat více různých veřejných API lišících se specifikací, soukromých API, notifikačních rozhraní a datových rozhraní.

Vlastník rozhraní je plně odpovědný za jeho specifikaci sestávající z definice struktury programovacího rozhraní (definice operací, definice datových struktur) a dokumentace programovacího rozhraní. Nikdo jiný než vlastník rozhraní, není oprávněn jeho specifikaci změnit.

Následují konkrétní obecné požadavky na jednotlivé druhy programovacích rozhraní. Požadavky jsou doplněny příkladem hypotetického back-end modulu Zábava (Amusement) umožňujícího studentům

nakupovat vstupenky na koncerty. Jedná se čistě o hypotetický příklad back-end modulu, který není součástí zadání.

3.1 Obecná pravidla

Nejprve uvedeme obecná pravidla, která platí pro všechny druhy rozhraní.

3.1.1 Jmenné konvence

- Všechna URL endpointů rozhraní jsou definována relativně vůči základnímu URL SIS (tzv. base URL). Toto základní URL se může lišit dle prostředí, a proto jej neuvádíme a není pro návrh rozhraní podstatné.
- Všechny složky relativních URL (kroky cest, parametry) jsou uváděny v angličtině v camelCase notaci.
- Jediným povoleným formátem používaným veřejnými, privátními a notifikačními rozhraními je formát JSON. Jediným povoleným jazykem pro definici datových struktur pro formát JSON je jazyk [JSON Schema](#) ve verzi 2020-12 nebo pozdější.
- Názvy prvků datových struktur (klíče JSON, případně elementy a atributy XML a sloupce CSV) jsou uváděny v angličtině v camelCase notaci.

3.1.2 Chování klientů rozhraní

- Všechna URL endpointů rozhraní slouží jako identifikátory i lokátory. Nejsou však nositeli aplikační/byznysové sémantiky. V žádném případě není možné je na klientovi parsovat a na výsledku parsování stavět aplikační logiku.

3.2 Obecné požadavky na veřejná API

Veřejné API nabízí sadu operací, které umožňují vykonávání byznys operací, ze kterých sestávají byznys procesy/případy užití definované v kapitole byznys analýzy dané zadávací dokumentace pro konkrétní modul.

Veřejné API je z technického hlediska RESTful API, tj.

- reprezentuje byznys entity jako zdroje
- umožňuje CRUD manipulaci se zdroji,
- používá JSON pro reprezentaci zdrojů,
- používá URL pro identifikaci zdrojů,
- je bezstavové,
- používá HTTP metody POST, GET, PUT, PATCH, DELETE, OPTIONS a HEAD pro CRUD manipulaci se zdroji,

Veřejná API jsou verzovaná. Verze číslujeme sémanticky ([semantic versioning](#)).

3.2.1 Zdroje a jejich typy

Zdroj je základním technickým konceptem REST. Zdrojem je konkrétní nebo abstraktní věc, která je byznys entitou vyplývající z byznys analýzy, o níž chceme prostřednictvím veřejného API zpřístupnit údaje a umožňovat s ní CRUD manipulaci.

Uvažujeme následující typy zdrojů:

- zdroj typu objekt
 - reprezentuje byznys entitu nebo její část
 - např. student, koncert, interpret, vstupenka
- zdroj typu kolekce objektů

- reprezentuje kolekci všech byznys entity daného typu
 - např. kolekci všech studentů, kolekci všech koncertů, kolekci všech interpretů, kolekci všech vstupenek
- pro objekty v kolekci obsahuje pouze základní údaje, nikoliv jejich kompletní detail. Mezi základními údaji je vždy:
 - URL objektu (jedná se o zdroj)
 - typ případně typy objektu
 - byznysový identifikátor objektu
- zdroj typu vztah
 - reprezentuje byznys vztah dané byznys entity s jinou byznys entitou
 - např. vstupenka studenta (vztah studenta s jeho vstupenkou), majitel vstupenky (vztah vstupenky s jejím majitelem-studentem) nebo interpret vystupující na koncertu (vztah koncertu s interpretem, který na koncertu vystupuje)
- zdroj typu kolekce vztahů
 - reprezentuje kolekci vztahů, které reprezentují pro danou byznys entitu všechny její byznys vztahy odpovídající dané asociaci v konceptuálním datovém modelu
 - např. kolekce všech vstupenek daného studenta (0..*), kolekce všech majitelů dané vstupenky (0..1) nebo kolekce všech interpretů vystupujících na koncertu (1..*)
- zdroj typu ovladač (controller)
 - reprezentuje specifickou byznys operaci (akci) se zdrojem typu objekt, kterou není možné realizovat jako CRUD operaci
 - např. zneplatnění vstupenky.

Zdroj typu kolekce vztahů je kolekci, jejíž prvky nereprezentují byznys entity vztažené k dané byznys entitě, ale vztahy samotné.

Zdroje typu ovladač by měly být využívány co nejméně – pouze v případech, kdy není možné danou byznys operaci realizovat jako CRUD operaci nad zdrojem typu objekt nebo kolekce. Např. byznys operaci změny majitele vstupenky na koncert může být realizována jako operace Update (HTTP PUT) na zdroji typu objekt reprezentujícím majitele vstupenky. Nezavádíme proto zdroj typu ovladač pro změnu majitele vstupenky. Zdroj typu ovladač může být nutný pro změnu stavu byznys entity, která není přímo realizovatelná jako prostý Update nějaké její části. Např. se může jednat o změnu stavu byznys entity na stav zneplatněno, tj. operace zneplatnění vstupenky. Alternativou by bylo vytvoření zdroje typu objekt reprezentujícím platnost vstupenky. Pokud ale takový zdroj nemáme a nemůžeme jej z nějakého důvodu vytvořit, musíme vytvořit zdroj typu operace. Vždy ale preferujeme variantu vytvoření potřebných zdrojů, je-li to možné.

3.2.2 Pravidla pro určování zdrojů a tvorbu jejich URL

Každý zdroj je vystaven prostřednictvím endpointu na URL, které je veřejné v rámci systému, tj. lze na něj přistoupit z jiných částí systému.

URL zdroje je identifikátorem zdroje v rámci celého systému a zároveň jeho lokátorem. URL zdroje má následující tvar:

[základní URL]/[relativní URL modulu]/publicApi/[relativní URL veřejného API]/[verze API specifikace]/[relativní URL v rámci API]

kde

- **[základní URL]** je HTTP URL (tzv. base URL) společné pro všechny endpointy všech služeb a je určeno technickou infrastrukturou systému
- **[relativní URL modulu]** je relativní URL modulu, obvykle v podobě názvu modulu
- **[relativní URL veřejného API]** je relativní URL veřejného API v rámci modulu, obvykle v podobě názvu veřejného API, který musí být v rámci modulu unikátní. Ve výjimečných případech může být vynecháno, ale je to považováno za antipattern. Pokud v budoucnu dojde k rozhodnutí vytvořit druhé veřejné API, bude toto druhé muset být pojmenováno, čímž dojde k nekonzistenci v konvenci tvorby URL
- **[verze API specifikace]** dle [semantic versioning](#). Změna verze znamená změnu veřejného API. Změna modulu při zachování API nemění její verzi.
- **[relativní URL v rámci API]** je relativní URL daného zdroje, s nímž je možné prostřednictvím veřejného API manipulovat. Je unikátní v rámci veřejného API.

Základními pravidly při určování zdrojů jsou následující pravidla.

- Pro typ byznys entity popsany v byznys analýze určíme
 - zdroj typu kolekce objektů, který reprezentuje kolekci všech instancí tohoto typu. Platí, že **[relativní URL v rámci API] = [název typu v množném čísle]**, např.:
 - students
 - interprets
 - tickets
 - concerts
 - zdroje typu objekt, které reprezentují jednotlivé instance typu (tj. jednotlivé byznys entity). Platí, že **[relativní URL v rámci API] = [název typu v množném čísle]/{byznysový identifikátor pro tento typ byznys entity}**, např.:
 - students/12345678, kde 12345678 je číslo osoby (UKČO) studenta
 - interprets/pokac, kde pokac vyplývá z názvu interpreta, který je unikátní
 - tickets/v-xzfhrd, kde v-xzfhrd je kód vstupenky
 - concerts/4758, kde 4758 je číslo koncertu
- Pro asociaci mezi dvěma typy byznys entit popsanou v konceptuálním datovém modelu a její konec (S je typ výchozího konce v asociaci, T je druhý typ v asociaci) určíme
 - zdroj typu kolekce vztahů, který reprezentuje kolekci všech vztahů modelovaných asociací mezi danou instancí typu S a instancemi typu T. Platí, že **[relativní URL v rámci API] = [relativní URL v rámci API zdroje typu objekt reprezentujícího danou instanci typu S]/[název role asociačního konce nebo název asociace jako podstatné jméno]**. V případě maximální kardinality asociačního konce == 1 je název v relativním URL uveden v jednotném čísle. V případě > 1 je uveden v množném čísle. Např.:
 - students/12345678/tickets
 - tickets/k-xzfhrd/owner
 - concerts/4758/interprets
 - zdroje typu vztah, které reprezentují jednotlivé vztahy modelované asociací v jednom ze směrů. Platí, že **[relativní URL v rámci API] = [relativní URL v rámci API zdroje typu objekt reprezentujícího danou instanci typu S]/[název role asociačního konce nebo název asociace jako podstatné jméno]/{byznysový identifikátor pro typ T}**. V případě

maximální kardinality asociačního konce == 1 je název role v relativním URL uveden v jednotném čísle. V případě > 1 je uveden v množném čísle, např.:

- `students/12345678/tickets/k-xzfhhd`
- `tickets/k-xzfhhd/owner/12345678`
- `concerts/4758/interprets/pokac`
- Pro specifickou byznys operaci/akci se zdrojem typu objekt, kterou není možné realizovat jako CRUD operaci, určíme zdroj typu ovladač. Platí, že [relativní URL v rámci API] = [relativní URL v rámci API zdroje typu objekt]/[název byznys operace/akce jako podstatné jméno v jednotném čísle], např.:
 - `tickets/k-xzfhhd/invalidation`

Výše uvedené příklady jsou relativní URL v rámci API. Jejich plné relativní URL v rámci systému je pak tvořeno dle výše uvedeného předpisu [relativním URL modulu](#), [relativním URL API v rámci modulu](#), [verzí API](#) a [relativním URL v rámci API](#). Náš příklad je v kontextu modulu Zábava, tj. plná relativní URL jsou např.:

- `amusement/publicApi/basic/1.0.0/students`
- `amusement/publicApi/basic/1.0.0/students/12345678`
- `amusement/publicApi/basic/1.0.0/students/12345678/tickets`

Výše uvedené příklady ukazují, že byznysové identifikátory v relativních URL mohou být nečíselné. Pokud je to možné, preferujeme číselné byznysové identifikátory. Jejich (ne)existence však vyplývá z konceptuálního datového modulu. Pokud není v konceptuálním datovém modelu identifikován žádný číselný identifikátor, volíme nečíselný.

Použití byznysových identifikátorů je nutné. Pokud bychom použili umělé databázové primární klíče, hrozilo by pronikání interní databázové logiky modulu do systému, což je zakázáno.

Výše uvedená pravidla neaplikujeme maximalisticky. Není nutné vytvářet zdroje pro každý typ byznys entity a pro každou byznys asociaci. Pravidla aplikujeme dle potřeby. V případě jednodušších API můžeme mít dokonce jen jeden zdroj typu kolekce objektů (např. kolekce studentů) a pro každý objekt v kolekci zdroj (např. jednotlivé studenty). Prvky vnitřní struktury zdrojů (např. kontaktní údaje, bankovní účty) nemusíme nutně reprezentovat jako samostatné zdroje. Vždy vycházíme z konceptuálního datového modelu, modelu use cases, příp. byznys procesů.

Pokud ale nějaký zdroj určíme, musíme ho určit podle jednoho z výše uvedených pravidel. Určování jiných zdrojů podle jiných pravidel není povoleno.

3.2.3 Pravidla pro návrh operací pro manipulaci se zdroji

Definice CRUD operací musí vyplývat z byznys analýzy. Každá určená CRUD operace je mapována na odpovídající byznys operaci/akci popsané v byznys analýze. Při určování CRUD operací pro manipulaci s jednotlivými typy zdrojů se řídíme následující tabulkou.

	Kolekce objektů	Objekt	Kolekce vztahů	Vztah	Ovladač
POST (Create)	Vytvoření nového objektu	N/A	N/A	N/A	Vykonání ne-idempotentní operace na daném objektu
GET (Read)	Čtení kolekce objektů	Čtení detailu objektu	Čtení kolekce se základními údaji o vztazených objektech	N/A	N/A
PUT (Update, příp. idempotentní Create)	N/A	Aktualizace objektu poskytnutím jeho nové reprezentace	Vložení vztahu s objektem do kolekce. Pro kardinality ..1 to znamená zároveň odstranění existujícího vztahu, pokud existuje.	N/A	Vykonání idempotentní operace na daném objektu
PATCH (Update)	N/A	Aktualizace části údajů o objektu poskytnutím nových hodnot vybraných údajů	N/A	N/A	Vykonání idempotentní operace na daném objektu
DELETE (Delete)	N/A	Smazání objektu	N/A	Smazání vztahu	N/A

3.2.4 Pravidla pro stránkování a filtrování kolekcí pomocí parametrů v URL

Operace pro čtení kolekce (GET) může bez dalšího znamenat načtení dat o velkém množství byznys entit. Pokud je potřeba množství omezit, je možné URL zdroje typu kolekce doplnit stránkovacími a filtrovacími parametry.

Stránkovacími parametry jsou

- `_offset`, jehož hodnotou je celé číslo ≥ 0 , určuje pozici prvního prvku kolekce, který bude vypsán ve výsledku,
- `_limit`, jehož hodnotou je celé číslo > 0 které je shora omezeno (každou službou zvlášť), určuje počet prvků, které budou vypsány ve výsledku,
- `_orderBy`, jehož hodnotou je název vlastnosti prvků kolekce s primitivní hodnotou, podle které má být kolekce seřazena pro účely stránkování
 - pokud není parametr uveden, vyplývá seřazení z interní reprezentace dat v modulu, přičemž je takové seřazení zdokumentováno v dokumentaci modulu
 - seznam požadovaných atributů dle kterých je možné řadit bude explicitně stanoven v rámci definice API

Dokumentace zdroje typu kolekce uvádí, zda podporuje stránkování a stránkování s explicitní specifikací seřazení vč. seznamu vlastností, podle kterých je možné třídit. Musí se jednat o vlastnosti definované ve specifikaci datové struktury pro reprezentaci kolekce.

Filtrovacími parametry jsou

- `_type`, jehož hodnotou je seznam řetězců, které reprezentují typy prvků, které se mohou vyskytovat v kolekci a dle kterých je možné kolekci filtrovat
- další parametry odpovídající vlastnostem prvků kolekce s primitivní hodnotou, názvy parametrů nesmí začínat znakem `_`, který je jako prefix rezervovaný

Dokumentace zdroje typu kolekce uvádí, zda podporuje filtrování podle typu, včetně výčtu možných typů, jejich popisu a vazby na typy byznys entit. Dále uvádí, zda podporuje filtrování podle dalších parametrů, včetně výčtu vlastností, které lze použít jako filtrovací parametry. Musí se jednat o vlastnosti definované ve specifikaci datové struktury pro reprezentaci kolekce.

3.2.5 Pravidla pro definici zdrojů a operací pro manipulaci se zdroji

Veřejné API pro manipulaci se zdroji je formálně definováno s pomocí [OpenAPI](#) verze 3.0.3 nebo vyšší (dále jen Open API). Definice je vyjádřena jako YAML dokument nebo sada YAML dokumentů, která popisuje tvar URL zdrojů a možné CRUD operace nad těmito zdroji tak, jak byly navrženy dle výše uvedeného postupu. Vstupní parametry, které jsou součástí URL jsou definovány také jako součást specifikace. Vstupní parametry, které jsou předávány v těle požadavků, a výstupní reprezentace zdrojů, které jsou předávány v těle odpovědi, jsou reprezentovány jako JSON dokumenty, jejichž JSON struktura je popsána dle následující kapitoly a je obsažena v definici API nebo v samostatných souborech a je odkazována.

3.2.6 Pravidla pro návrh a popis JSON datových struktur

Zdroje a vstupní parametry CRUD operací předávané v tělech požadavků jsou reprezentovány v datovém formátu JSON. Datová struktura pro reprezentaci zdroje je navržena odvozením z odpovídající části konceptuálního datového modelu, jehož strukturu odpovídá. Může být doplněna o technické datové prvky bez sémantického významu zachyceného v konceptuálním datovém modelu.

Datová struktura je popsána datovým schématem vyjádřeným v jazyku JSON Schema (zapsaném v syntaxi YAML, příp. JSON). Datové prvky definované ve schématu, které nejsou technickými datovými prvky, jsou napojeny na prvky konceptuálního datového modelu. Datová schémata tak nepopisují pouze syntax ale také sémantiku pomocí pojmů definovaných v konceptuálním datovém modelu.

Existuje katalog datových struktur, které je povinné používat při definici nových datových struktur. Katalog definuje základní datové struktury, např. pro reprezentaci specifikace časových údajů, množství, adres apod.

Operace na zdrojích musí na vstupu (v rámci těla HTTP požadavku) i na výstupu (v rámci těla HTTP odpovědi) data o zdrojích reprezentovat v k tomu navržených datových strukturách dle odpovídajících JSON schémat. Každá operace je tak doplněna o definici vstupní a výstupní datové struktury. Vstupy a výstupy jednotlivých volání operací musí být validní vůči JSON schématům definujících tyto datové struktury. Požadavek na veřejné API s nevalidním vstupem musí být odmítnut s příslušným chybovým HTTP kódem.

3.3 Obecné požadavky na privátní API

Privátní API je kolekcí operací, které naplňují specifické potřeby odpovídajících front-end modulů daného back-end modulu. Privátní API je určeno pouze a jenom pro potřeby front-endu daného modulu. Nesmí být použito pro žádné jiné účely. Nesmí zajišťovat funkcionality, které jsou poskytovány veřejným API, tj. privátní API ani žádná jeho část nesmí striktně ani volně kopírovat funkcionality veřejného API nebo jeho části.

Protože není vystaveno veřejně do systému, nejsou na něj kladeny tak striktní požadavky jako na veřejné API.

Technicky se jedná o JSON API, které

- umožňuje čtení dat reprezentujících byznys entity,
- umožňuje operace pro práci s dalšími daty, které nevyplývají z byznys analýzy, ale jsou potřebné pro správné fungování uživatelského front-endu daného modulu,
- Umožňuje operace pro práci s daty, které vyplývají z byznys analýzy, ale zadavatel je ve veřejném API nedefinoval. Přitom jsou ale potřeba pro naplnění funkčních požadavků kladených zadavatelem na modul. Jedná se typicky o situace, kdy v budoucnu bude toto zajištěno voláním API jiného back-end modulu, který ještě nebyl definován a implementován.
- používá JSON pro reprezentaci dat,
- je bezstavové.

Privátní API musí být zdokumentováno a datové struktury pro reprezentaci dat v datovém formátu JSON musí být popsány v jazyku JSON Schema. Pokud nějaká datová struktura privátního API sémanticky odpovídá nějakému typu byznys entit popsaných v konceptuálním datovém modlu, musí být tato souvislost zaznamenána v dokumentaci.

Zadavatel si vyhrazuje právo z privátního API nebo jeho části vytvořit veřejné API. Zodpovědnost za privátní API nebo jeho část při využití tohoto práva převezme za API odpovědnost a zajistí, aby splňovalo výše uvedené podmínky na veřejné API. Dodavatel, který privátní API nebo část využíval, musí svůj kód potřebným způsobem upravit tak, aby pracoval s vytvořeným veřejným ekvivalentem.

4 Datový interface pro integraci se stávající databází SISu

Pro integraci nových modulů bude ve stávající Oracle databázi vytvořeno nové servisní schéma, v němž budou postupně vytvářeny potřebná views pro čtení a procedury pro zápis dat do stávající databáze.

Pro každý z modulů pak bude v databázi vytvořen další uživatel (schéma), pomocí něž se bude nová aplikace připojovat. Do tohoto schematu připravíme synonyma na používané objekty a potřebná oprávnění.

4.1 Konfigurační parametry

Moduly používají konfigurační parametry s dvouúrovňovou hierarchií – konfigurace na úrovni celé univerzity a konfigurace na úrovni fakulty. Chování modulu je pak ovlivněno dle příslušnosti přihlášeného uživatele k fakultě. Modul si konfigurační položky načte jednorázově při startu a bude vhodným způsobem udržovat v cache.

4.2 Langy

Všechny textové informace načítané frontendovými moduly budou dvojjazyčné (eng, cze), konfigurovatelné a uložené v databázi. Položky langů mají dvouúrovňovou hierarchii – na úrovni univerzity a na úrovni fakulty. Zobrazení příslušného textu je pak ovlivněno dle příslušnosti přihlášeného uživatele k fakultě. Modul si používané textové položky načte jednorázově při startu a bude vhodným způsobem udržovat v cache. Během implementace bude dohodnuta přesná struktura, dodavatel dodá prvotní seznam lang klíčů a jejich hodnoty.

5 Zajištění jakosti (QA) a dokumentace

5.1 Obecné požadavky na kvalitu kódu a bezpečnost

5.1.1 Kvalita kódu

Zdrojový kód každého modulu musí procházet kontrolou linteru a nástroje na statickou analýzu kódu s cílem odhalení chyb již v čase kompilace. Tento nástroj musí odpovídat zvolené technologii implementace daného modulu.

Zdrojový kód každého modulu musí procházet kontrolou nástroje na formátování odpovídající standardům a dobrým zvykům pro zvolenou technologii implementace.

5.1.2 Bezpečnost

Požadavky na implementaci modulů:

1. Modul musí být implementovaný tak, aby byl odolný vůči známým bezpečnostním hrozbám
2. Kód modulu prochází kontrolou **Static Vulnerability Scan**
 - Neobsahuje závažné/critical chyby
3. Kód prochází kontrolou **Dependency Vulnerability Check**
 - Neobsahuje závažné/critical chyby
4. Kód prochází kontrolou **Dynamic Vulnerability Analysis**
 - Neobsahuje závažné/critical chyby
5. Modul používá knihovny třetích stran, k nimž je poskytována LTS (long term support), nebo u nichž lze předpokládat střednědobá podpora (5-10 let) – například na základě popularity použití dané knihovny v rámci komunity

Pro prokázání splnění podmínek uvedených v bodech 2, 3, 4 dodavatel dodá pro každou novou verzi reporty z úspěšného ověření bezpečnosti pro jednotlivé položky. U false-positive případů uvedených v dodaných reportech bude poskytnuto písemné odůvodnění proč dodavatel považuje daný bod reportu za false-positive. Zadavatel bude namátkově a v některých případech automaticky pravidelně provádět tuto kontrolu také.

Následující tabulka uvádí přehled typických nástrojů pro provádění požadovaných skenů a reportů.

Druh skenu	Typické nástroje
Static Vulnerability Scan	IBM AppScan, Fortify, Veracode, FindSecBugs, Brakeman, Bandit
Dependency Vulnerability	OWASP Dependency Check, Bundler Audit, Safety
Dynamic Vulnerability Analysis	Burp Suite, OWASP ZAP, HP WebInspect

5.2 Obecné požadavky na dokumentaci

Pro každý modul musí být dodavatelem odevzdána následující dokumentace:

1. Instalační a konfigurační příručka
 - Znalost systémových požadavků
 - Znalost způsobu konfigurace modulu
 - Znalost postupu instalace na lokální stanici a ve vývojovém prostředí
2. Dokumentace funkčních a nefunkčních požadavků
 - Znalost happy paths i unhappy paths
 - Napomáhá odhalení regresních závad na úrovni modulu
3. Dokumentace privátního (frontendového) i veřejného API standardizovaným strojově čitelným formátem
 - Verzované API v gitu
 - Znalost API zachycená pro vývojáře ostatních modulů
 - Možnost generovat klienty a mock servery pro dané API automaticky
4. Dokumentace umístění dat používaných modulem a možnosti jejich anonymizace (tam kde je to aplikovatelné)
 - Pro potřeby zálohování a správy dat využívaných modulem
 - Splnění požadavků dle GDPR před provedením kopií, záloh atd.
5. Dokumentace technické architektury modulu/aplikace
 - Interní architektura modulu
 - Komunikace s jinými moduly
 - Možnosti provozu modulu v HA
 - Popis autorizačních rozhodnutí prováděných modulem
6. Dokumentace generovaných auditních událostí
7. Dokumentace generovaných metrik
 - Popis všech metrik (jednotky, způsob měření, přesná sémantika atd.)
 - Doporučení pro nastavení alertů pomocí PromQL
8. Dokumentace vlastních přidaných datových polí (fieldů) do strukturovaných logovacích záznamů
9. Popis všech použitých knihoven třetích stran a zdůvodnění jejich použití
10. Technická dokumentace netriviálních algoritmů
11. Popis SQL skriptů pro vytvoření potřebné databázové struktury a iniciální naplnění dat/číselníků
12. Popis datových migračních skriptů
13. Dokumentace testovací strategie, testovacích scénářů, výkonnostních testů a vytvořených testovacích, simulačních a mockovacích nástrojů

14. Doporučená systémová (hardwarová) konfigurace pro nasazení do testovacího (Stage) i produkčního (Prod) prostředí, odpovídající požadovaným výkonnostním parametrům
15. Uživatelská příručka pro administraci pomocí administračního UI rozhraní (jestli nějaké existuje)
16. Uživatelské příručka pro běžné uživatele

Očekávané technologie a standardy:

- Gherkin – pro popis testovacích scénářů
- OpenAPI 3.0 / GraphQL Schema – dokumentace API
- Markdown – formátovaný text
- UML diagramy
- README.md – informace pro vývojáře a operations tým, co daný modul dělá, jak ho rychle spustit ve vývojovém prostředí a jak pro něj vyvíjet

5.3 Obecné požadavky na QA

5.3.1 Obecné požadavky na testování

Pro potřeby ověření kvality dodaného software (Quality Assurance - QA) je kromě dodání samotné aplikace očekáváno také dodání několika druhů automatických, poloautomatických a manuálních testů, a to v následujících kategoriích:

- **Unit a integrační testy**
 - Cíl: zvýšená šance odhalení regresních závad na úrovni modulu, a to zejména při úpravách a refactoringu
 - Zejména netriviální procesy a algoritmy by měly být pokryté pomocí automatizovaných (unit) testů
 - Bezchybná komunikace mezi jednotlivými komponentami uvnitř aplikace, ale také mezi rozhraním různých systémů by měly být pokryté pomocí automatizovaných (integračních) testů
 - Technická implementace testů bude závislá na zvolené technologii pro implementaci jednotlivých modulů
 - Dodavatel musí poskytnout zadavateli veškeré potřebné nástroje a dokumentaci pro automatické spouštění testů jako součásti CI/CD pipeline (build modulu)
 - Minimální požadované pokrytí kódu unit testy je 80 %. U složitějších procesů a algoritmů je očekávané pokrytí 100 %. Všechny testy musí proběhnout úspěšně. Výjimky musí schválit zadavatel.
 - Procento pokrytí testy a míra automatizace může být dále upřesněna v zadávací dokumentaci modulu.
- **Systémové „end-to-end“ testy**
 - Cíl: zvýšená šance odhalení regresních závad na úrovni vzájemné integrace modulů při úpravách a refactoringu
 - Cíl: dokumentace technického postupu jednotlivých uživatelských cest (user journeys) pro vzájemnou validaci korespondence s byznys analýzou modulu
 - Všechny uživatelské cesty (user journeys) a automatizované procesy musí být pokryté pomocí end-to-end testů (testovací scénáře)
 - Testovací scénáře mohou být automatizované, poloautomatické nebo zcela manuální, s maximální možnou (rozumnou) mírou plné automatizace co největšího

počtu testovacích scénářů, s cílem zapojení testů do pravidelného (nočního) spouštění všech plně automatizovaných scénářů v testovacím prostředí zadavatele.

- Testovací scénáře budou vytvářeny ve formátu Gherkin
- Zadávací dokumentace konkrétního modulu může dále dopřesnit další požadavky na testovací scénáře.

- **Výkonnostní testy**

- Cíl: zvýšená šance odhalení výkonnostních nedostatků při úpravách a refactoringu
- Pokrytí všech výkonnostně citlivých částí systému výkonnostními testy
- Výkonnostní testy musí být automatizované v maximální možné míře
- Společně s testy poskytne dodavatel zadavateli i detailní technickou dokumentaci popisující fungování, přípravu dat a způsob jejich spouštění.
- Jako základní sadu výkonnostních testů dodavatel připraví sadu testů pro běžné operace:
 - Testy současného použití GET operací na detail.
 - Testy současného běhu GET operací nad seznamy dat s filtrem.
 - Testy současného běhu definovaných UPDATE operací.
 - Kombinované testy současného běhu typických uživatelských scénářů vyplývajících z User stories definovaných Business analýzou.
- Výkonnostní testy musí umožnit test aplikace při běžném a při špičkovém zatížení a musí umožnit ověření, že:
 - Při běžném zatížení je 99,9% požadavků vyřízeno v době pod 300ms.
 - Při špičkovém zatížení je 98% požadavků vyřízeno v době pod 500ms, maximální odezva nepřesáhne 3s.
 - Systém udrží výše uvedenou odezvu i při špičkovém zatížení trvajícím více než 10 minut.
- Všechny výkonnostní testy musí využívat dostatečnou různorodost vstupních parametrů klientských požadavků.
- Běžné a špičkové zatížení modulu a speciální výkonnostní požadavky pro vyjmenované funkce systému mohou být dále doplněny v zadávací dokumentaci modulu.

5.3.2 Mock, simulační nástroje a nástroje na generování dat

Testy ze všech kategorií, zejména pak testy funkčních požadavků je potřebné umět spouštět jak v rámci plně nasazeného prostředí, tak i proti lokální instanci daného modulu (pro možnost otestování před nasazením do prostředí). Pro tuto potřebu poskytne dodavatel zadavateli také odpovídající nástroje:

- Mock nástroje (nástroje simulující funkci třetích komponent pomocí definovaného rozhraní komponenty)
- Mocky všech backendových modulů (Tyto mocky poskytují testovací data bez nutnosti připojení k databázi, např. na základě fixního konfiguračního textového souboru.)
- Nástroje a generátory pro automatizované vytváření testovacích datových sad
- Simulační nástroje (generátory klientského provozu pomocí API rozhraní modulu, nástroje simulující uživatelský provoz atd.)

Požadovaný seznam nástrojů relevantní k funkcím daného modulu může být dále upřesněn v zadávací dokumentaci.

5.3.3 Doporučená systémová konfigurace

Jako součást dokumentace poskytne dodavatel zadavateli také popis doporučené systémové (hardwarové) konfigurace pro nasazení do jak do testovacího (Stage) tak i do produkčního (Prod) prostředí, odpovídající požadovaným výkonnostním parametrům systému/modulu.

6 Způsob řízení projektu a administrace

6.1 Požadavky na způsob řízení, komunikaci a podporu

6.1.1 Způsob řízení

- Požadujeme ustanovení řešitelského týmu, jehož členem je zástupce zadavatele.
- Řešitelský tým se schází na pravidelné bázi, frekvence dohodnuta se zástupcem dodavatele (např. jednou týdně).
- Smyslem setkání je
 - monitoring a koordinace vnitřní realizace modulu s cílem zajistit dodržení
 - požadované architektury
 - vnitřního rozhraní pro přístup k datům ve staré databázi SIS
 - vnějších rozhraní poskytovaných modulem (veřejné aplikační rozhraní, datová rozhraní)
 - vnějších rozhraní jiných modulů využívaných modulem
 - napojení na infrastrukturu
 - funkční specifikace v kontextu byznys analýzy
 - test coverage (funkční i kvalitativní /performance, .../)
 - koordinace s paralelní realizací jiných modulů
 - definice průběžných milestones dle potřeb zadavatele/dodavatele
 - monitoring plnění termínu dodávky, případně termínů průběžných milestones
- Na setkání musí proběhnout alespoň:
 - kontrola postupu prací v uplynulém období
 - stanovení postupu prací na následující období
 - rozprava o stávajících překážkách a nejasnostech

6.1.2 Způsob komunikace

- Komunikace prostřednictvím komunikační platformy zadavatele (Redmine)
- Groupware pro rychlou týmovou ad-hoc komunikaci
- Issue&tasks tracking (Redmine)
- Zápisy setkání týmu
- Monitoring plnění termínu dodávky, monitoring termínů průběžných milestones

6.1.3 Školení administrátorů

Cílem školení administrátorů systému je připravit pověřené pracovníky zadavatele pro výkon funkce správy systémových parametrů IS.

Součástí školení administrace systému bude přehled všech funkčností, vazeb mezi funkčnostmi a implementovaných rozhraní, včetně monitoringu a správy těchto rozhraní.

V rámci tohoto školení zajistí dodavatel vyškolení max. 15 uživatelů.

6.2 Časový harmonogram

Harmonogram realizace modulu. Tento by měl splňovat kromě jiného následující minimální požadavky:

- Datum začátku realizace, a to nejpozději do 14 kalendářních dnů od podpisu smlouvy. Za zahájení realizace se považuje iniciální schůzka dodavatele se zadavatelem.
- Datum konce realizace, a to nejpozději do 30.6.2024. Za konec realizace je považováno datum, ke kterému bude akceptován kompletní předmět této veřejné zakázky bez výhrad ze strany zadavatele.
- Data předání průběžných výstupů dodavatelem zadavateli. Těmi jsou zejména:
 - a. backendovou část implementující API s REST testovacím klientem
 - b. frontendovou část modulu proti mock backendové části
 - c. plně naimplementovaná observability a audit
 - d. plné QA
 - e. knowledge transfer

Výše uvedený výčet je nutným minimem, nicméně harmonogram předložený dodavatelem by měl samozřejmě obsahovat i další, co možná nejpodrobnější informace popisující, jakým způsobem a v jakých etapách dodavatel plánuje zamýšlenou realizaci.

6.3 Dokumentace a požadavky na dodávku

Seznam požadovaných výstupů v oblasti dokumentace a QA:

1. Instalační a konfigurační příručka
 - Znalost systémových požadavků
 - Znalost způsobu konfigurace modulu
 - Znalost postupu instalace
2. Dokumentace funkčních a nefunkčních požadavků
 - Znalost happy paths i unhappy paths
 - Napomáhá odhalení regresních závad na úrovni modulu
3. Dokumentace privátního (frontendového) i veřejného API standardizovaným strojově čitelným formátem
 - Verzované API v git
 - Znalost API zachycená pro vývojáře ostatních modulů
 - Možnost generovat klienty a mock servery pro dané API automaticky
4. Dokumentace umístění dat používaných modulem a možnosti jejich anonymizace (tam kde je to aplikovatelné)
 - Pro potřeby zálohování a správy dat využívaných modulem
 - Splnění požadavků dle GDPR před provedením kopií, záloh atd.
5. Dokumentace technické architektury modulu/aplikace
 - Interní architektura modulu
 - Komunikace s jinými moduly
 - Možnosti provozu modulu v HA
 - Popis autorizačních rozhodnutí prováděných modulem
6. Dokumentace generovaných auditních událostí
7. Dokumentace generovaných metrik
 - Popis všech metrik (jednotky, způsob měření, přesná sémantika atd.)
 - Doporučení pro nastavení alertů pomocí PromQL
8. Dokumentace vlastních přidávaných datových polí (fieldů) do strukturovaných logovacích záznamů
9. Popis všech použitých knihoven třetích stran a zdůvodnění jejich použití
10. Technická dokumentace netriviálních algoritmů
11. Popis SQL skriptů pro vytvoření potřebné databázové struktury a iniciální naplnění dat/číselníků
12. Popis datových migračních skriptů
13. Dokumentace testovací strategie, testovacích scénářů, výkonnostních testů a vytvořených testovacích, simulačních a mockovacích nástrojů

14. Doporučená systémová (hardwarová) konfigurace pro nasazení do testovacího (Stage) i produkčního (Prod) prostředí, odpovídající požadovaným výkonnostním parametrům
15. Uživatelská příručka pro administraci pomocí administračního UI rozhraní (jestli nějaké existuje)
16. Uživatelské příručka pro běžné uživatele

Příloha č. 2 – Položkový rozpočet

Položka	Dílčí plnění	Jednotka	Počet jednotek	Jednotková cena (v Kč)		Celková cena (v Kč)	
				bez DPH	vč. DPH	bez DPH	vč. DPH
A1	Vývoj, implementace datových rozhraní, integrace, unit testy a instalace iniciální verze modulu Předměty a studijní plány SIS UK	člověkoden	129	10 000,00 Kč	12 100,00 Kč	1 290 000,00 Kč	1 560 900,00 Kč
A2	Testování, tvorba testovacích scénářů a nástroje	člověkoden	45	10 000,00 Kč	12 100,00 Kč	450 000,00 Kč	544 500,00 Kč
A3	Školení správců	člověkoden	6	10 000,00 Kč	12 100,00 Kč	60 000,00 Kč	72 600,00 Kč
A4	Vytvoření dokumentace	člověkoden	15	10 000,00 Kč	12 100,00 Kč	150 000,00 Kč	181 500,00 Kč
A5	Licence programového vybavení třetích stran, pokud je jejich dodání nezbytné k implementaci řešení a nejde o licence operačních systémů ani virtualizačních platforem, a jejich instalaci v prostředí Zadavatele	-	-	-	-	-	-
A	Licence a implementace (celkem A1 až A5)*	-	-	-	-	1 950 000,00 Kč	2 359 500,00 Kč
B	Zajištění servisní činnosti a technické podpory**	měsíc	24	30 000,00 Kč	36 300,00 Kč	720 000,00 Kč	871 200,00 Kč
Celková nabídková cena						2 670 000,00 Kč	3 230 700,00 Kč

* Položka bude spolufinancována ze zdrojů EU, prostřednictvím Národního plánu obnovy pro oblast vysokých škol.

** Položka bude hrazena z finančních prostředků zadavatele.

Příloha č. 4 - Složení týmu Objednatele a Dodavatele

Vedoucí týmu za Objednatele:
(tj. projektový manažer)

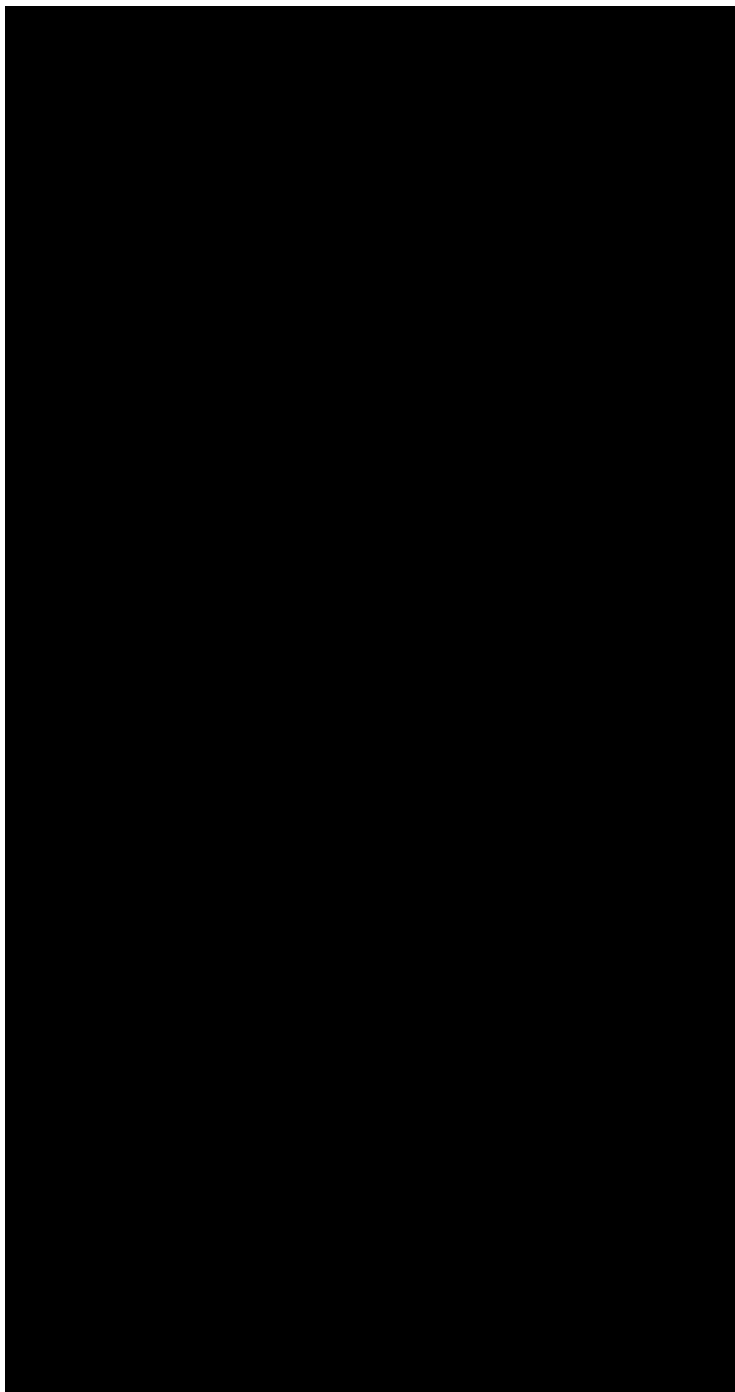
Hlavní architekt řešení:

Vedoucí vývojového týmu:

Vedoucí týmu Dodavatele:
(tj. projektový manažer)

IT analytik:

Programátor:



Další složení týmu Dodavatele je uvedeno v příloze č. 3 Smlouvy.

Příloha č. 5 – Seznam poddodavatelů

Dodavatel nepředpokládá zapojení žádného poddodavatele.

Příloha č. 6 – Bezpečnostní požadavky

Článek 1

Úvod

1. Tento dokument popisuje bezpečnostní požadavky kladené na Dodavatele v rámci realizace veřejné zakázky „RUK – ÚVT - Dodávka modulu Osobní údaje Studijního informačního systému na Univerzitě Karlově“, zejména pro naplnění požadavků vyplývajících pro Dodavatele ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti (dále jen „VyKB“).
2. Dodavatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy oblasti bezpečnostních opatření kybernetické bezpečnosti ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle ZoKB. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této příloze, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

Článek 2

Bezpečnostní požadavky

2.1. Účel

1. Tento dokument stanoví způsoby a úrovně realizace bezpečnostních opatření pro Dodavatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatelem a Dodavatelem. Požadavky na Dodavatele jsou definovány dle platné právní úpravy, především pak dle ZoKB, VyKB.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek Smlouvy zohledňující takové požadavky.

2.2. Obecné požadavky

1. Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:
 - a. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Dodavatele, jakožto budoucího významného dodavatele provozovatele základní služby, ze ZoKB, VyKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu;
 - b. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Dodavateli Objednatelem, resp. platné řídicí dokumentace Objednatele či její části anebo platné řídicí dokumentace, k jejímuž dodržování se Objednatel zavázal, pokud byl Dodavatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace poskytovateli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Poskytovateli na sdílené úložiště aj.);
 - c. rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se

podílejí na plnění Smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně Dodavatele podílející se na plnění Smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro Objednatele v souvislosti s plněním této Smlouvy;

- d. zaznamenávat podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.) a informovat o nich Objednatele;
- e. přidělovat svým jednotlivým pracovníkům zaměstnancům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;
- f. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují k předmětu plnění dle této Smlouvy;
- g. průběžně detekovat technické zranitelnosti a konfigurační nesoulady předmětu plnění Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Dodavatele. Nápravná opatření musí být schválena Objednatelem;
- h. realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy.

2.3. Bezpečnost informací

1. Dodavatel je povinen zajistit utajení získaných důvěrných informací objednatelů způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této smlouvy. Dodavatel je povinen zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.
2. Právo užívat, poskytovat a zpřístupnit důvěrné informace má Dodavatel pouze v rozsahu a za podmínek nezbytných pro řádné plnění práv a povinností vyplývajících z této Smlouvy.
3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují veškeré informace, které nebyly Objednatelem označeny jako veřejné a které se týkají této Smlouvy a jejího plnění (zejména informace o právech a povinnostech smluvních stran jakož i informace o cenách), které se týkají Objednatele, jeho smluvních partnerů, pacientů, obchodní tajemství, anebo informace pro nakládání, s nimiž je stanoven právními předpisy zvláštní režim utajení. Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně Objednatelem označeny.
4. Za důvěrné informace se v žádném případě nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany, dále informace získané na základě postupu nezávislého na této Smlouvě a informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany.
5. Dodavatel je povinen zajistit bezpečnost informací z pohledu dostupnosti. Informace se z pohledu dostupnosti považují za bezpečné, jestliže jsou dostupné autorizovaným uživatelům v době, kdy jsou potřeba.
6. Dodavatel je povinen zajistit bezpečnost informací z pohledu integrity. Informace se z pohledu integrity považují za bezpečné, jestliže je zaručena jejich správnost, bezchybnost a jsou vyloučeny jejich neautorizované změny.

2.4. Oprávnění užívat data

1. Dodavatel je při poskytování plnění pro Objednatele oprávněn užívat informace předaná Dodavatelí Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
2. Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s informacemi pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.5. Řetězení a řízení dodavatelů

1. Dodavatel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího poddodavatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele.
2. Dodavatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů.
3. Dodavatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
4. Pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy.
5. Dodavatel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Smlouvy.
6. Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy.

2.6. Řízení změn

1. Dodavatel se zavazuje provést hodnocení dopadů Objednatelem navrhovaných změn na termíny a cenu předmětu plnění Smlouvy. Pokud by však takovéto hodnocení vyžadovalo dodatečné náklady anebo by nepříznivě ovlivnilo pracovní vytížení zaměstnanců nebo využití jiných prostředků určených k provádění předmětu plnění, Dodavatel tuto skutečnost oznámí Objednateli a hodnocení provede pouze na základě písemného pověření Objednatelem. V takovém případě bude hodnocení hrazeno podle stráveného času v sazbách platných v době hodnocení.
2. Dodavatel u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování informačního systému a zajistí možnost navrácení do původního stavu.
3. Dodavatel má povinnost informovat Objednatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany Dodavatele.
4. Dodavatel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn
5. Dodavatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
6. V případě realizace penetračního testování nebo testování zranitelnosti řešení poskytne Dodavatel Objednateli veškerou potřebnou součinnost.

2.7. Akvizice, vývoj a údržba

1. Dodavatel se zavazuje v rozsahu plnění na své straně zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
2. Dodavatel se zavazuje předat Objednateli dokumentaci předmětu plnění obsahující zejména:
 - a. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
 - b. dokumentaci obsahující popis autorizačního konceptu a oprávnění;
 - c. dokumentaci obsahující instalační a konfigurační postupy.
3. V případě, že předmět plnění zahrnuje vývoj software, zavazuje se Dodavatel:
 - a. dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu, nebo dodaného Objednatelem;
 - b. na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit Objednateli vyvíjený kód SW;
 - c. poskytnout Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či kdykoli po jeho předání;
 - d. zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve Smlouvě (např. že SW nebude obsahovat žádné nepotřebné komponenty, programové vzorky apod.);
 - e. pokud je součástí plnění i instalace operačního systému případně SW třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v IT prostředí Objednatele;
 - f. zajistit bezpečnost testovacího prostředí u Dodavatele a ochranu poskytnutých testovacích dat Objednatelem;
 - g. zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem Smlouvy specifikovaný kompilovaný, resp. spustitelný kód a další nezbytná data pro provozování předmětu plnění;
 - h. instalovat SW pouze na základě Objednatelem předem schválených migračních postupů;
 - i. předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu;
 - j. zajistit řízení verzí zdrojového kódu;
 - k. zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;
 - l. nevyvíjet, nekompilovat a nešířit v IT prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

2.8. Zvládání kybernetických bezpečnostních událostí a incidentů

1. Dodavatel se při poskytování plnění pro Objednatele zavazuje v rozsahu poskytovaných služeb dle Smlouvy, že:
 - a. stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládnutí kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů na osobu odpovědnou za kybernetickou bezpečnost, v případech, kdy situace nestrpí odklad telefonicky.
 - b. nastavená pravidla pro zvládnutí bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získání musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;
 - c. navrhne řešení tak, aby byl systém detekce a zvládnutí bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním

- incidentům a omezením dostupnosti;
- d. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.9. Informační povinnost a povinnosti při výměně informací

1. Dodavatel se během poskytování plnění pro Objednatele zavazuje Objednatele informovat o:
 - a. způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;
 - b. změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy, a změně oprávnění nakládat s těmito aktivy, a to nejpozději do tří pracovních dnů po uskutečnění této změny.
2. Dodavatel se během poskytování plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.

2.10. Řízení kontinuity činností

1. Objednatel má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Dodavatele do plánu kontinuity činností, který souvisí s informačním systémem a souvisejících služeb a/nebo zahrnutí Dodavatele do Plánu obnovy (DRP) Objednatele. Objednatel má oprávnění požadovat po Dodavateli zpracování Plánů obnovy (DRP) disaster recovery postupů.
2. Objednatel má povinnost informovat Dodavatele o způsobu zapojení do řízení kontinuity činností.

2.11. Bezpečnost lidských zdrojů

1. Dodavatel zajistí poučení všech svých zaměstnanců podílejících se na dodávce o bezpečnostních pravidlech uvedených v těchto Bezpečnostních požadavcích, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynuocovacích mechanismů. Rozsah poučení podléhá schválení Objednatele osobou určenou za kybernetickou bezpečnost.
2. Dodavatel se zaváže zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost zaměstnanců).
3. Dodavatel je povinen vést písemnou evidenci uskutečněných poučení v rozsahu předmět poučení, datum a seznam poučených osob. Dodavatel se zavazuje předložit tuto evidenci objednateli bezodkladně poté, co k tomu bude Objednatelem vyzván.

2.12. Bezpečnost komunikace

1. Zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě Univerzity Karlovy (většinou na konkrétní server), odpovídají za své činnosti prováděné v rámci interní sítě Univerzity Karlovy. Z důvodu zajištění bezpečnosti zaměstnanci Dodavatele nesmí zejména:
 - a. zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě;
 - b. šířit škodlivý kód;
 - c. připojovat do sítě jiná, než schválená zařízení Dodavatelem (včetně USB zařízení, soukromých mobilních zařízení, IoT zařízení apod.);
 - d. využívat nástroje sloužící k maskování identity;
 - e. provádět bezdůvodné skenování portů;
 - f. provádět jakoukoliv formou monitorování počítačové sítě, které může vést k

- zachycení informací/dat, pokud není předmětem plnění smlouvy;
- g. obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, počítačové sítě;
 - h. provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům;
 - i. užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes počítačovou síť, internet nebo intranet;
 - j. využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemcem, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů);
 - k. předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec Univerzity Karlovy, pokud jsou takové informace nutné z hlediska přípravy či plnění smluvního vztahu.
2. Při práci na pracovní stanici, mobilním zařízení připojeného do sítě nebo do informačního systému Univerzity Karlovy musí Dodavatel dodržovat tyto základní zásady:
- a. umožnit přístup jen poučenému zaměstnanci Dodavatele;
 - b. chránit ICT prostředky Univerzity Karlovy;
 - c. po ukončení práce provést neprodleně odhlášení tak, aby se zamezilo zneužití jeho přístupových práv.

2.13. Řízení přístupu

1. Dodavatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze fyzické identitě zaměstnance Dodavatele poučené o těchto Bezpečnostních požadavcích, a to na základě požadavku Dodavatele na přístup.
2. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle) a není nárokové.
3. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci
4. Dodavatele.
5. Dodavatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny osobou odpovědnou za kybernetickou bezpečnost na straně Objednatele a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.
6. Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Dodavatel bere na vědomí, že přístup do interní sítě a/nebo k technologickým a komunikačním systémům bude realizován výhradně s využitím zařízení Objednatele.
7. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídicí dokumentace a mohou být uplatněny příslušné postupy zvládnutí bezpečnostního incidentu.
8. Dodavatel se zavazuje, že nebude instalovat a používat zejména nástroje typu Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
9. Dodavatel bere na vědomí, že postup zvládnutí bezpečnostního incidentu či skutečnost

vzniklá v důsledku porušení bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Objednatele.

10. Na základě smluvního vztahu může být konkrétním zaměstnancům Dodavatele umožněn přístup k předmětným ICT prostředkům pomocí vzdáleného přístupu přes VPN. Pracovní stanice, přenosná zařízení zaměstnanců Dodavatele přistupující k ICT prostředkům Objednatele musí mít instalován výrobcem podporovaný aktualizovaný operační systém a systém pro ochranu před škodlivým kódem (antivirový program) s nejnovější verzí virové databáze.
11. Lokální přístup Dodavatele do provozního prostředí může být povolen pouze v odůvodněných případech. Tento přístup musí probíhat ve zvláštním režimu dohledu ze strany Univerzity Karlovy.

2.14. Ochrana před škodlivým kódem

1. Dodavatel se zavazuje, že zajistí maximální ochranu před zavlečením škodlivého SW do interní sítě Objednatele. Zaměstnanci, resp. subdodavatelé Dodavatele mají zakázáno používat soukromou výpočetní techniku pro připojování do interní sítě Objednatele.

2.15. Monitorování činností

1. Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy.

2.16. Kontrola souladu s požadavky bezpečnosti

1. Dodavatel se zavazuje umožnit Objednateli nebo jím pověřené třetí osobě provést audit plnění povinností Dodavatele dle této Smlouvy, zejména způsobu plnění bezpečnostních opatření, způsobu řízení dodavatelů, nakládání s daty, způsobu identifikace a hlášení kybernetických bezpečnostních incidentů. Objednatel se zavazuje vyrozumět Dodavatele o termínu a případně osobě pověřené provedením auditu alespoň 3 pracovní dny předem. Dodavatel se zavazuje umožnit provedení auditu ve všech prostorách, v nichž dochází k plnění předmětu této Smlouvy. Náklady na uskutečnění auditu ponese každá smluvní strana zvlášť; Dodavatel nemá právo na poskytnutí úhrady nákladů či jakéhokoliv jiného plnění v souvislosti s auditem. V případě, že výsledkem auditu budou zjištěny o pochybeních na straně Dodavatele, zavazuje se Dodavatel bezodkladně po výzvě Objednatele veškeré takové nedostatky na své náklady odstranit. Dodavatel je povinen zajistit umožnění auditu za stejných podmínek i u svých poddodavatelů.
2. Dodavatel je povinen pravidelně provádět také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Objednatelem, na žádost Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá Dodavatel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.17. Porušení Bezpečnostních požadavků

1. Dodavatel odpovídá za to, že jeho zaměstnanci a/nebo poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy. V případě, že dojde k nedodržení těchto požadavků ze strany zaměstnance a/nebo poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle této Smlouvy.