

MINIMÁLNÍ SMLUVNÍ PODMÍNKY SMLOUVY NA DODÁVKU SLUŽBY CLOUD COMPUTINGU

Obsah

MINIMÁLNÍ SMLUVNÍ PODMÍNKY SMLOUVY NA DODÁVKU SLUŽBY CLOUD COMPUTINGU.....	1
1. ÚVOD	2
2. MINIMÁLNÍ SMLUVNÍ PODMÍNKY.....	4
2.1 Úvod.....	4
2.2 BEZPEČNOSTNÍ OPATŘENÍ SLUŽBY	4
2.3 DOSTUPNOST SLUŽBY	4
2.4 PODPORA SLUŽBY.....	5
2.5 MĚŘENÍ DOSTUPNOSTI	7
2.6 MÍSTO DODÁNÍ	7
2.7 PLÁNOVANÁ ODSTÁVKA A VYHODNOCENÍ DOSTUPNOSTI SLA JEDNOTKY.....	8
2.8 MINIMÁLNÍ HODNOTY PRO STANOVENÍ VÝŠE PENALIZACE	9
2.9 MINIMÁLNÍ HODNOTY PENALIZACE.....	9
2.10 MOŽNOST PŘEDČASNÉHO UKONČENÍ SMLOUVY	10
2.11 UKONČENÍ SMLOUVY A SANKCE V PŘÍPADĚ HRUBÉHO PORUŠENÍ SLA	10
2.12 REPORTOVÁNÍ	11
3. SEZNAM ZKRATEK	12

1. Úvod

Tento dokument definuje **minimální smluvní podmínky, které musí respektovat každá smlouva mezi poskytovatelem služby eGovernment Cloudu (eGC) a zákazníkem eGC (orgánem veřejné správy)**¹. Za to, že smlouva s poskytovatelem respektuje zde uvedené minimální smluvní podmínky, zodpovídá zákazník.

Dle platné verze Zákona 365/2000 Sb. (ZoISVS) je výběr poskytovatele služeb eGC rozdělen do dvou fází. **V první fázi, v tzv. ex-ante kontrole**, DIA ve spolupráci s NÚKIB na základě stanovených bezpečnostních kritérií (vyhláška 316/2021 Sb.) certifikuje poskytovatele a jeho služby cloud computingu. Certifikované poskytovatele a jejich certifikované služby DIA zapisuje do katalogu cloud computingu. **Orgán veřejné správy může využívat pouze cloud computing, který je zapsán v katalogu cloud computingu** (Zákon 365/2000 Sb., §6I (1)).

Druhou fází, která se realizuje dle zákona o veřejných zakázkách (ZZVZ), je výběr poskytovatele a jeho služeb pro realizaci konkrétního ISVS. Ve veřejné zakázce zadavatel oslovuje pouze ty poskytovatele, jejichž služby prošly úspěšně ex-ante kontrolou, tzn. ty poskytovatele, jejichž služby byly zapsány do katalogu cloud computingu.

S ohledem na konkrétní účel a okolnosti využití poptávané cloudové služby zadavatel v zadání veřejné zakázky stanoví **další kritéria**, upřesňující požadavky na poptávané služby, která jdou nad bezpečnostní opatření prověřovaná při ex-ante kontrole a nad základní sadu kritérií/požadavků, uvedených v tomto dokumentu. Tato kritéria mohou být s ohledem na ZZVZ uplatněna jako povinné technické parametry nebo jako hodnotící kritéria. Taková další kritéria však musí být zadavatelem zdůvodněná. Pro lepší pochopení uvádíme několik příkladů upřesňujících kritérií, která jsou v dané situaci obvyklá:

- i. Zadavatel upřesní **bezpečnostní pravidla**, která musí splňovat poskytovatel a jeho služby nad rámec již provedené ex-ante kontroly tak, aby provozovaný ISVS splnil všechny bezpečnostní požadavky ZKB a Cloudové vyhlášky NÚKIB pro ISVS dané bezpečnostní úrovni.
- ii. Zadavatel upřesní **rozsah funkčnosti** poptávané služby v dané veřejné zakázce, např.: v oblasti IaaS/PaaS upřesní u serveru typ požadovaného operačního systému; v oblasti SaaS určí např. rozsah požadovaných submodulů v rámci služby ERP.
- iii. Zadavatel **zvýší nebo upřesní určité provozní parametry služby**, které lze vyjádřit číselně (měřitelně), např.: zvýšení požadované dostupnosti z 99,9% na 99,95%, nebo požadovat reakci podpory při nahlášení kritické úrovně incidentu do 30 minut, nebo objem poštovní schránky pro každého uživatele min. 5 GB dat, nebo maximální dobu odezvy důležitých transakcí u služeb SaaS.
- iv. Zadavatel upřesnění některé **kvalitativní vlastnosti služby**, např.: úložiště dat s rychlým přístupem (rychlé paměťové disky typu SSD, nezbytné pro práce s „velkými daty“), schopnost gramatické kontroly textového editoru v určitých jazycích, schopnost kontroly lokality IP adresy přihlašujícího se uživatele pro lepší

¹ Orgán veřejné správy využívá cloud computing poskytovaný poskytovatelem cloud computingu na základě písemné smlouvy o poskytování cloud computingu orgánu veřejné správy. (§ 6I odst. 3 Zákona č. 365/2000 Sb. o informačních systémech veřejné správy).

vyhodnocování rizik, schopnost notifikace správců zadavatele o provozních událostech služby pomocí emailu i SMS.

- v. Zadavatel upřesní svoje požadavky, které budou uplatněny, když poskytovatel dané služby v daném období nezajistí parametry služby (např. dostupnost, doba odezvy, bezpečnost apod.), jak byly stanoveny v SLA.
- vi. Případný požadavek zadavatele na **zahrnutí dodatečné služby správy a nastavení** poptávané služby nad rámec specifikace vlastní služby, neboť konkrétní zadavatel nedisponuje dostatečnými vlastními zdroji v této oblasti.

Při stanovení kvalifikačních a hodnotících kritérií služeb a rovněž při formulaci finálních podmínek smlouvy je žádoucí, aby zadavatelé zohlednili rozdíly mezi těmito dvěma typy cloudových služeb, lišících se mírou standardizace:

- A. **Standardní služby komerčního cloudu**, které nepodléhají specifikům legislativy v různých zemích a které jsou běžně dostupné na trhu jako komoditní a multitenantní (tedy služby, kde na jedinou instanci služby je připojeno mnoho zákazníků, nacházejících se i mimo ČR). Jedná se o služby IaaS, PaaS i SaaS, které jsou standardně uvedeny v katalogu služeb Poskytovatelů veřejných služeb cloudu. Sem patří i integrální (kompozitní) služby, pokud splňují podmínku výše. Pro tento typ standardních (komoditních) služeb eGC by měly být akceptovány běžné tržní smluvní podmínky, které nabízejí provozovatelé. Tyto služby se také nejrychleji inovují v globálním konkurenčním prostředí, a vykazují proto častější změny technických parametrů a funkční specifikace v určitých vývojových cyklech, které má zadavatel obvykle možnost ovlivnit pouze částečně. *V případě, že zákazník eGC bude požadovat odlišné podmínky, lze předpokládat, že nedosáhne ekonomických a provozních výhod, které komerční cloud nabízí, neboť úprava smluvních podmínek (pakliže ji vůbec poskytovatel bude schopen akceptovat) bude mít za následek výrazný nárůst ceny služby.*
- B. **Služby SaaS, které byly vytvořeny specificky pro legislativní prostředí v ČR** (např. ERP, HR, spisová služba apod.). Tento typ služeb bude reprezentovat provoz automatizovaných agend zákazníka eGC (ISVS a dalších provozních IS) formou cloudových služeb. Sem patří i služby integrátorů, kteří staví řešení pro potřeby organizací veřejné správy v právním prostředí ČR, a které využívající integrální (kompozitní) komoditní služby, pokud jsou dodavatelem spojeny do funkčního celku a doplněny službami s přidanou hodnotou. *Pro tento typ specifických služeb eGC bude zákazník eGC vyžadovat specifické smluvní podmínky pro kvalitu provozu dle oprávněných požadavků na provoz ISVS.*

V obou výše popsaných variantách je možné individuálně stanovit vybrané parametry služby jako hodnotící kritéria, a to v závislosti na konkrétních potřebách každé jednotlivé výzvy (viz §141 ZZVZ). Tímto postupem bude možné docílit soutěží potvrzeného nejefektivnějšího řešení, splňujícího reálné požadavky subjektu, s přiměřeným uplatněním individuálních smluvních požadavků zadavatele.

2. Minimální smluvní podmínky

2.1 Úvod

Každý ISVS se skládá z jedné nebo více komponent architektonických (např. jednotlivé funkční moduly, komponenty funkčního modulu: front-end, byznys logika, zpřístupnění a ukládání dat) a provozních (např. vývojové prostředí, testovací prostředí, provozní prostředí). Každá komponenta ISVS musí být správcem informačního systému zařazena do jedné ze čtyř bezpečnostních úrovní – nízká, střední, vysoká a kritická (Vyhláška 315/2021 Sb. – Vyhláška o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci). Dále „Vyhláška 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu“ stanoví minimální bezpečnostní opatření, které musí poskytovatel a jeho služba dané bezpečnostní úrovně splňovat, aby poskytovatel a jeho služba byli zapsáni do katalogu cloud computingu.

2.2 Bezpečnostní opatření služby

V podmínkách výběrového řízení a ve smlouvě na dodávku služby musí OVS respektovat bezpečnostní opatření stanovená Vyhláškou 316/2021 Sb.

Poznámka: S ohledem na skutečnost, že OVS smí využívat pouze služby cloud computingu, které jsou zapsané v katalogu cloud computingu (tzn. že má jistotu, že bezpečnostní opatření předepsaná vyhláškou pro daný typ služby již byla DIA a NÚKIBem prověřena), stačí když zajistí, že:

- v podmínkách veřejné soutěže uvede, že poskytovatel a jeho nabízené služby musejí být zapsány v katalogu cloud computingu,
- ve smlouvě bude uvedena povinnost poskytovatele splňovat v průběhu platnosti smlouvy všechna bezpečnostní opatření, které jsou Vyhláškou 316/2021 Sb. stanovena pro službu dané bezpečnostní úrovně.

2.3 Dostupnost služby

U dostupnosti služby je třeba rozlišovat čtyři pojmy: provozní doba, provozní doba pod SLA, doba podpory služby a dostupnost služby.

Provozní doba je vyjádřena denními nebo týdenními časovými intervaly, ve kterých poskytovatel služby eGC deklaruje záměr udržovat danou službu v provozu. Nepřetržitá provozní doba znamená, že poskytovatel deklaruje záměr provozovat službu 24 hod. 365 dní v roce.

Provozní doba pod SLA definuje dobu, ve které probíhá hodnocení dostupnosti služby a na kterou se vztahuje SLA a její případné sankce. Tato doba se může rovnat Provozní době, ale může být i vymezena Poskytovatelem na kratší časové intervaly (od-do, dny v týdnu, pracovní dny / dny prac. klidu / volna).

Doba podpory služby je definována dobou, ve které Poskytovatel přijímá a řeší incidenty hlášené zákazníkem. Doba podpory služby v nejvyšší prioritě incidentů („Kritický business

impact“) nesmí být kratší než Provozní doba pod SLA. Pokud doba podpory v nižších prioritách incidentů bude kratší než provozní doba pod SLA, pak by uživatelé měli mít možnost zadat incident elektronickou formou (aby bylo možné zachytit časový okamžik hlášení, a následně dobu řešení incidentu).

Dostupnost služby se stanovuje procentem z provozní doby pod SLA, ve kterém poskytovatel garantuje, že služba bude v provozu a dostupná.

Níže uvedené **základní hodnoty dostupnosti** jsou odvozené od definice bezpečnostních úrovní a slouží jako kvalifikační základ při ex-ante kontrole. V rámci výzvy k podání nabídek (viz §141 ZZVZ) pak za účelem optimalizace kvality služby a kontrahované ceny může zadavatel **zvýšit nebo dále upřesnit požadavky na dostupnost** poptávané služby.

Bezp. Úroveň	Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků, s měsíčním vyhodnocáním
Nízká	96,16%	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovní dnů ² , na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96% (vztaženo na dobu pod SLA). Tato dostupnost může být např. vhodná pro některé back office systémy obcí a měst.	Max. 8 hod., avšak pouze v rámci definované pracovní doby
Střední	99,45%	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7
Vysoká	99,9%	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání, a pro ISVS pod ZKB). Určité služby SaaS, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7
Kritická	99,99%	Provozní doba pod SLA: 24x7 (připravenost pro systémy kritické informační infrastruktury pod ZKB). Vyhodnocování je zde z praktických důvodů na roční bázi, avšak jednotlivé výpadky bez penalizace jsou omezeny na max. 15 minut. Cloudové služby SaaS v této úrovni dopadu budou mít rovněž smluvně dané max. doby RPO / RTO.	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99%)

2.4 Podpora služby

Minimální doba podpory služby pro jednotlivé bezpečnostní úrovně:

² www.kalendar-online.cz

Bezp. úroveň	Doba podpory služby
Nízká	Podpora a servis pouze v pracovní dny a v určené pracovní době.
Střední	Podpora a servis 24x7 (Pro SaaS může být variantně určená Pracovní doba)
Vysoká	Podpora a servis 24x7 (Pro SaaS může být variantně určená Pracovní doba)
Kritická	Podpora a servis 24x7

Poskytovatel eGC uvede ve smlouvě podrobné parametry podpory výčtem úrovní podpory a dále očekávanou dobou reakce na různé priority incidentů, nejlépe formou tabulky níže.

Úrovně podpory služby a prioritizace hlášených incidentů ze strany zákazníka:

Úroveň podpory	Priority incidentu a očekávaná doba reakce		
	Nízký business impact	Střední business impact	Kritický business impact
Úroveň 1.	Max. 8 hodin, pouze v pracovní dny	Max 4 hod., 24x7, případně pouze po vymezenou pracovní dobu	Max. X hod., 24x7
Úroveň 2.	Max. X hod., pouze v pracovní dny	Max. X hod., 24x7	Max. X hod., 24x7
Úroveň 3.	Max. X hod., pouze v pracovní dny	Max. X hod., 24x7	Max. X hod., 24x7
Úroveň 4.	Max. X hod., pouze v pracovní dny	Max. X hod., 24x7	Max. X hod., 24x7

Toto je pouze příklad – každý poskytovatel nabídne vlastní časové parametry úrovní podpory, přičemž jako doporučení slouží tato vzorová prioritizace incidentů:

Kritický business impact: Služba není dostupná nebo vykazuje takové vlastnosti, které ji činí zcela nepoužitelnou ke stanovenému účelu. Incident vyžaduje okamžitou pozornost poskytovatele. Tato priorita se využívá k hlášení incidentů nedostupnosti, které se pak vyhodnocují vůči kritériím SLA.

Střední business impact: Služba je dostupná, avšak se značně zhoršenou odezvou, nebo některé moduly nepracují ve shodě se specifikací / dokumentací. Hlavní funkce organizace zákazníka služby mohou na snížené úrovni pokračovat.

Nízký business impact: Požadavky zákazníka na změnová řízení služby nebo eskalace, které bezprostředně nemají dopady na chod organizace (např. požadavky na změnu uživatelského rozhraní aplikace).

Poskytovatel služby eGC může některé, případně všechny varianty služby podpory zpoplatnit.

I zde může v rámci výběrového řízení zadavatel za účelem snížení kontrahované ceny v jednotlivých případech snížit požadavky na Provozní dobu pod SLA a tím i na dobu podpory poptávané služby.

2.5 Měření dostupnosti

Jednotkou SLA rozumíme vymezení rozsahu služby nebo jejích funkčních částí, jejichž dostupnost je měřena, vyhodnocována, a penalizována samostatně. V případě nacenění služeb eGC způsobem „pay-as-you-consume“ musí mít každá jednotka SLA vlastní cenu tak, aby mohlo být rozhodnuto o výši případného měsíčního penále (kreditu).

Měření	Popis
Metoda měření	Poskytovatel služeb musí provozovat monitorovací systém, který je navázán na klíčové komponenty dodávané služby. Výstup z monitorovacího systému musí být k dispozici zákazníkům, a to v podobě (i) webového rozhraní, dostupného šifrovaným spojením přes veřejný Internet, a dále (ii) v podobě souhrnného reportingu za určité časové období, předávaného vhodným kanálem ve strojově čitelném formátu. Konkrétní metoda měření dostupnosti a případně dalších kvalitativních parametrů služby bude stanovena individuálně pro každý typ služby tak, aby odpovídala jejímu chování. Na základě vyhodnocení služby jako nedostupné nebo neplnící kvalitativní parametry zákazník sám hlásí incident (pokud není smluvně dohodnuto jinak) formou Trouble Ticketu (Poruchového lístku, dále též TT) v systému technické podpory Poskytovatele. Poskytovatel je povinen zajistit přístup k Trouble Ticket systému prostřednictvím webového rozhraní, dostupného šifrovaným spojením přes veřejný Internet. Výše případné kreditace je stanovována na základě reportu z Trouble Ticket systému Poskytovatele. Poskytovatel si může vyhradit právo neposkytnout kreditaci v průběhu určité části nedostupnosti služby, po kterou zákazník prokazatelně neposkytl potřebnou součinnost.
Časové vymezení	Kontrolní bod 1 – Začátek výpadku: Časová značka hlášení v monitorovacím nástroji, resp. logu ve smyslu „SLA jednotka je nedostupná“, pokud se poskytovatel a zákazník smluvně nedohodli na jiném modelu. Pokud Zákazník prokáže, že služba měla výpadek, tak je irrelevantní, když se v logu poskytovatele cloudu nenachází záznam o výpadku služby, a za začátek výpadku je považován čas prokázaný zákazníkem. V případě, že výpadek začne před, a pokračuje po začátku Provozní doby za začátek výpadku se považuje začátek Provozní doby. Kontrolní bod 2 – Konec výpadku: První následující pravdivé hlášení v monitorovacím nástroji, resp. logu ve smyslu „SLA jednotka je dostupná“, pokud se poskytovatel a zákazník smluvně nedohodli na jiném modelu. Pokud Poskytovatel prokáže, že služba byla obnovena a v logu či monitorovacím nástroji není o tomto záznam, tak za čas ukončení výpadku je považován prokázaný čas. V případě, že výpadek končí po konci Provozní doby, je za konec výpadku považovaný konec Provozní doby.
Časový interval	Dostupnost SLA jednotek se sleduje pro každou SLA jednotku zvlášť a vyhodnocuje se s ohledem na závazné hodnoty dostupnosti a Provozní dobu, a případně s ohledem na jiné kvalitativní parametry uvedené v SLA.
SLA jednotka	Pro služby IaaS/PaaS: Minimálně na úrovni separátně pro Compute a Storage a dále dle členění Poskytovatele. Pro služby SaaS: Služby s bohatší funkcí je vhodné rozčlenit do funkčních modulů, které jsou popsány jako SLA jednotky s vlastním vyhodnocováním dostupnosti.

2.6 Místo dodání

Místem dodání služby je rozhraní konkrétního produktu/služby, které je podrobněji definováno v popisu jednotlivých produktů/služeb cloudového poskytovatele. Obvykle je definováno jako rozhraní určitého datového centra poskytovatele, připojeného k Internetu. Připojení k Internetu si zadavatel standardně zajišťuje sám. V případě, že zadavatel požaduje SLA pokrývající i konektivitu k tomuto bodu, musí zakoupit variantu služby eGC, která toto obsahuje. Současně navrhujeme v rámci bezpečnostních opatření, aby všichni dodavatelé cloud služeb deklarovali šířku pásma připojení do některého

peeringového bodu v České republice³, preferovaně **NIX.CZ**. Současná praxe ukazuje, že Internetová konektivita mezi hlavními peeringovými body v Evropě je zajištěna masívní redundancí páteřních sítí a případné výpadky se okamžitě řeší přesměrováním páteřního provozu.

2.7 Plánovaná odstávka a vyhodnocení dostupnosti SLA jednotky

Dostupnost je definována a reportována pro každou SLA jednotku, která je využívána pro provoz dané služby. Výpadek služby je jakýkoliv výpadek SLA jednotky, jehož délka a doba trvání nebyly ohlášeny stanoveným způsobem jako „plánovaná odstávka služby“. Provozovatel služby publikuje předem časová okna, v rámci kterých může předem ohlásit zákazníkům plánovanou odstávku. Plánované odstávky mohou být vyhlášeny pouze mimo obvyklou pracovní dobu (tj. pracovní dny a dobu 8:00 až 18:00 CET, pokud není smluvně určeno jinak), a preferovaně o víkendech.

Pro služby IaaS a PaaS se dostupnost či nedostupnost vyhodnocuje obvykle za celou službu, neboť výpadky SLA jednotek v nižších architektonických vrstvách obvykle znamenají dopad na všechny uživatele aplikační vrstvy:

$$\text{dostupnost} = \frac{\text{Celková provozní doba pod SLA} - \text{doba výpadku}}{\text{Celková provozní doba pod SLA}} \times 100\%$$

Poskytovatel může nabízet funkčně stejnou službu, avšak s různými hodnotami SLA a s různými cenami pro různá použití (vývoj, testování, produkci), a v tom případě může definovat další dodatečné aspekty výpočtu dostupnosti.

Jednotky SLA, které adresují některé specifické funkčnosti virtuálních výpočetních prostředků (jako např. Storage service, Search engine, služby umělé inteligence) mohou použít jiný vzorec SLA, který lépe zohlední kvalitativní parametry služby než pouhou dostupnost služby.

Pro služby SaaS, které mají přímé uživatelské rozhraní se dostupnost či nedostupnost vyhodnocuje se zohledněním skutečného dopadu na určité skupiny uživatelů. Ve službách SaaS totiž často nastává situace, kdy výpadek postihuje jen část uživatelů (např. jen ty co se nově chtějí zalogovat do služby, nebo jen ty kteří k práci využívají určitý aplikační modul).

$$\text{dostupnost} = \frac{\text{Celková prov. doba pod SLA} \times \text{počet všech uživ.} - \text{doba výpadku} \times \text{počet zasažených uživ.}}{\text{Celková provozní doba pod SLA} \times \text{počet všech uživatelů}} \times 100\%$$

³ Viz výpis z peeringové databáze, např. <https://www.peeringdb.com/ix/71> pro NIX.CZ

2.8 Minimální hodnoty pro stanovení výše penalizace

DOSTUPNOST			
Bezpečnostní úroveň	Zelená (Green)	Žlutá (Yellow)	Červená (Red)
Kritická	$A \geq 99,99\%$	$99,99\% > A \geq 99,5\%$	$A < 99,5\%$
Vysoká	$A \geq 99,9\%$	$99,9\% > A \geq 99\%$	$A < 99\%$
Střední	$A \geq 99,45\%$	$99,45\% > A \geq 97\%$	$A < 97\%$
Nízká	$A \geq 96,16\%$	$96,16\% > A \geq 90\%$	$A < 90\%$

2.9 Minimální hodnoty penalizace

V rámci smlouvy o poskytování služby musí být definován jednoznačný a reálně vymahatelný způsob penalizace za nedodržení parametru služby. Je přitom třeba nalézt takový mechanismus penalizace, který umožní reálně vynutit kvalitu poskytované služby a nebude moci být odpuštěn na základě faktu, že orgánu státní správy či samosprávy je služba poskytována jiným orgánem státní správy či samosprávy či státem vlastněnou či spoluvlastněnou organizací či podnikem.

Výpočet minimální smluvní pokuty za nedodržení parametru služby (dále jen „Penalizace“) nedodržení parametrů služby se určuje podle následujícího schématu:

Na každý SLA parametr dané SLA jednotky, jehož SLA hodnota bude v daném reportovacím období zjištěna jako „nedodržená“ (mimo pásmo „Green/zelená“ dle definice minimálních hodnot výše), se v daném měsíci uplatní tato minimální penalizace.

Yellow/Žlutá: Minimální penalizace formou **kreditu ve výši 10% ceny plnění** v daném reportovacím období.

Red/Červená: Minimální penalizace formou **kreditu ve výši 25% ceny plnění** v daném reportovacím období.

25% je hodnota kreditu, kterou může zákazník obdržet jako kompenzaci za nedostupnost služeb v oblasti IaaS a PaaS (nevyjedná-li v rámci veřejné zakázky jinou penalizaci). V případě, že se jedná o službu typu SaaS, která je specifická pro eGC (viz kapitola 1 – cloudová služba typu B) a její opakovaná či nadměrná nedostupnost může způsobit zásadní zhoršení služby zákazníka eGC jeho koncovým uživatelům, je možné v rámci specifických požadavků pro danou kategorii SaaS služeb požadovat kredit vyšší než 25%.

Tyto hodnoty penalizace byly zjištěny v době vydání metodiky eGC jako tržně obvyklé a slouží jako vodítko pro minimální penalizační schéma, přičemž nic neomezuje poskytovatele eGC, aby ve výběrovém řízení nabídli kredity vyšší než zde uvedené. Obdobně zadavateli není možné upřít právo zvolit si v rámci výběrového řízení jiný mechanismus výpočtu penále, avšak důsledkem může být rapidní snížení počtu poskytovatelů služeb eGC, kteří budou ochotni na takový mechanismus přistoupit.

2.10 Možnost předčasného ukončení smlouvy

Smlouva musí definovat podmínky pro předčasné ukončení smlouvy a povinnosti obou stran při ukončení smlouvy (zejména způsob a termín předání dat zákazníkovi).

V případě smluv typu „pay-as-you-consume“ musí být standardně zabudována možnost zadavatele ukončit smlouvu s výpovědí nejpozději na konci následujícího kalendářního měsíce, což řeší i situace ukončení smlouvy z důvodu porušení SLA. Doba výpovědi ≥ 30 dní je optimální z hlediska doby nutné k výběru jiného poskytovatele a migrace do jeho prostředí.

V případě smluv na fixní časové období musí být ve smlouvě obsaženy podmínky výpovědi v souladu s požadavky ZZVZ. Dále musí být ve smlouvě ustanovení, umožňující předčasné ukončení smlouvy bez sankcí ze strany poskytovatele v případě nedodržení kvalifikačních podmínek výběrového řízení nebo jiného prokazatelného nedodržení smluvních podmínek v průběhu trvání smlouvy (požadavky pro danou bezpečnostní úroveň, ztráta některé certifikace apod.).

2.11 Ukončení smlouvy a sankce v případě hrubého porušení SLA

V kvalifikačních podmínkách výběrového řízení musí být definováno „hrubé porušení SLA“. Za hrubé porušení SLA se rozumí situace, kdy v kterémkoli měsíci:

kumulovaná dostupnost služby dle její definice v SLA (s ohledem na definovanou „provozní dobu služby pod SLA“) klesne pod **hraniční hodnotu 66%** a/nebo poskytovatel přestal splňovat některé z **opatření, vyžadované bezpečností úrovně služby**.

V takovém případě musí mít zadavatel možnost smlouvu okamžitě ukončit a nastartovat změnový proces k jinému poskytovateli nebo do prostředí on-premise. Toto hrubé porušení SLA bude kromě sjednaného kreditu (dle tabulky prahových hodnot výše nebo dle aktuálního smluvního ustanovení) doprovázeno odškodněním, kterým poskytovatel služby eGC **uhradí ve smlouvě sjednanou výši odhadovaných migračních nákladů** zadavatele k jinému poskytovateli eGC. Tato částka bude jako možná výše odškodnění uvedena každým zadavatelem individuálně v rámci každé veřejné zakázky. **Povinností dodavatele je uzavřít si adekvátní pojištění profesní odpovědnosti za škody způsobené zákazníkům v oblasti poskytovaných ICT služeb, a to dle maximální výše náhrady škody, kterou si zadavatel ve výběrovém řízení sám stanoví.**

V případě jednoho případu hrubého porušení SLA pro více zákazníků daného poskytovatele současně, nebo v případě opakovaného hrubého porušení SLA pro různé zákazníky v různých obdobích **může být poskytovatel vyloučen ze soutěžního mechanismu eGC** (vymazán z katalogu certifikovaných poskytovatelů), pokud se prokáže, že neučinil vše, co po něm může být oprávněně požadováno k řádnému zajištění služby (např. u vendora SaaS promtním přechodem na jiného dodavatele IaaS/PaaS). Aby se mohl takto vyloučený poskytovatel znovu ucházet o kvalifikaci do eGC, musí předložit Ministerstvu redesign dané služby spolu s opatřeními, která mají hrubému porušení SLA do budoucna zabránit.

2.12 Reportování

Provozní / bezpečnostní notifikace a záznamy ze strany Poskytovatele

- Poskytovatel služby eGC je povinen dát svým zákazníkům k dispozici monitorovací systém či systémy provozního stavu služby s rozpadem minimálně na SLA jednotky a se schopností logování v čase, a to minimálně po dobu 30 dní zpětně.
- Služba musí dále nabízet zdokumentované rozhraní, kterým lze ze strany zákazníka načítat systémové události v reálném čase pro vlastní vyhodnocování provozních a bezpečnostních událostí a incidentů a pro jejich delší archivaci.
- Poskytovatel musí dále umožňovat notifikace administrátorům zákazníka o změnách dostupnosti služby v čase. Poskytovatel dále nabídne nějaký systém notifikace plánovaných odstávek. Rozsah notifikací nedostupnosti ze strany poskytovatele (kromě situací plánovaných odstávek) však nijak neomezuje zákazníky cloudových služeb reportovat jimi zjištěné případy nedostupnosti a případně i vymáhat smluvní penále.

Podklady pro vyúčtování

- V případě účtování typu „pay-as-you-consume“ dává Poskytovatel eGC svým zákazníkům k dispozici podrobný přehled vyúčtování s členěním na jednotlivé elementy služeb (rozpad minimálně dle jednotek SLA) a v intervalech ne delších než 1 měsíc. Tato vyúčtování musí být možné stáhnout ve strojově čitelném formátu pro další analytické zpracování na straně zákazníka.

3. Seznam zkratek

Zkratka	Význam
CC	Cloud Computing
eGC	eGovernment Cloud
ISVS	informační systém veřejné správy
OVS	orgán veřejné správy
SLA	smlouva o poskytování služby (Service level agreement)
ZKB	Zákon 181/2014 Sb. o kybernetické bezpečnosti
ZoISVS	Zákon 365/2000 Sb o informačních systémech veřejné správy