

KATALÓG KRITÉRIÍ VLÁDNEHO CLOUDU

pre cloudové služby
príloha č. 1D

Kompletný zoznam kritérií hodnotenia cloudových služieb pre zaradenie do katalógu hybridných služieb vládneho cloudu. Stanovuje kvalitatívne kritéria pre zaradenie služieb na rôznych úrovniach kvality. Dokument je súčasťou metodiky hodnotenia cloudových služieb.

Obsah

Obsah	1
Zoznam tabuliek.....	2
Úvod.....	3
1 Základné pojmy	3
1.1 Požiadavky katalógu kritérií.....	3
1.1.1 Všeobecné požiadavky	3
1.1.2 Požiadavky používateľov cloudu	4
1.1.3 Požiadavky na poskytovateľa cloudu	4
1.2 Rozsah zladenia a testovania.....	4
1.3 Minimálne požiadavky	5
1.4 Ďalší rozvoj a prevedenia katalógu	5
1.5 Použité zdroje.....	6
2 Štruktúra katalógu kritérií	7
2.1 Oblasti a kritériá	7
2.2 Minimálne požiadavky	11
3 Kritériá pre cloudové služby	12
3.1 EKONOMIKA A LEGISLATÍVA (EL).....	12
3.2 PREVÁDZKA (PR)	23
3.3 BEZPEČNOSŤ (SE)	29
3.4 ŠPECIFICKÉ (SS).....	34

Zoznam tabuliek

Tabuľka č. 1: Oblasti katalógu Vládneho cloudu.....	7
Tabuľka č. 2: Kritériá oblastí katalógu Vládneho cloudu	8
Tabuľka č. 3: Rozdelenie kritérií oblasti EKONOMIKA A LEGISLATÍVA	8
Tabuľka č. 4: Rozdelenie kritérií oblasti PREVÁDZKA	9
Tabuľka č. 5: Rozdelenie kritérií oblasti BEZPEČNOSŤ	10
Tabuľka č. 6: Rozdelenie kritérií oblasti ŠPECIFICKÉ	10
Tabuľka č. 7: Profil poskytovateľa cloudových služieb	12
Tabuľka č. 8: Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb	13
Tabuľka č. 9: Správa služieb.....	14
Tabuľka č. 10: Detailnejší profil spoločnosti.....	14
Tabuľka č. 11: Referenčné informácie o cloudovej službe.....	15
Tabuľka č. 12: Platné certifikáty.....	16
Tabuľka č. 13: Zmluvné náležitosti	17
Tabuľka č. 14: Pravidlá narábania s dátami	18
Tabuľka č. 15: Zmluvné požiadavky zabezpečenia a ochrany dát	19
Tabuľka č. 16: Zmluva o úrovni poskytovaných služieb (SLA).....	20
Tabuľka č. 17: Podmienky v prípade zastavenia poskytovania zazmluvnených služieb.....	21
Tabuľka č. 18: Ceny a nákladové položky za poskytované služby	21
Tabuľka č. 19: Špecifické okruhy otázok (voliteľné)	22
Tabuľka č. 20: Správa a prevádzka dátových centier	23
Tabuľka č. 21: Zákaznícka podpora.....	25
Tabuľka č. 22: Správa poskytovaných služieb.....	26
Tabuľka č. 23: Riadenie bezpečnosti	29
Tabuľka č. 24: Technická bezpečnosť	32
Tabuľka č. 25: Technické opatrenia na ochranu osobných údajov	33
Tabuľka č. 26: Referenčná architektúra	34
Tabuľka č. 27: Systémový manažment	34
Tabuľka č. 28: Bezpečnosť	35
Tabuľka č. 29: Manažment licencií (IaaS).....	36
Tabuľka č. 30: Referenčná architektúra (Paas).....	36
Tabuľka č. 31: Bezpečnosť (Paas)	36
Tabuľka č. 32: Správa (Paas)	37
Tabuľka č. 33: Interoperabilita (SaaS).....	37
Tabuľka č. 34: Podpora užívateľov (SaaS)	38

Úvod

Katalóg kritérií Vládneho Cloudu pre cloudové služby definuje minimálne požiadavky, ktoré cloudová služba musí spĺňať na získanie akreditácie vládneho cloudu a taktiež ich musí splniť, aby mohla byť uvedená na portáli vládneho cloudu.

Štruktúra dokumentu je uvedená nižšie. Kapitola 1 opisuje základné pojmy a požiadavky, na ktorých je založený katalóg kritérií vládneho cloudu, resp. štruktúra katalógu kritérií je vysvetlená v kapitole 2. Kapitola 3 podrobne opisuje kritériá a minimálne požiadavky katalógu kritérií, ktoré musia byť splnené na zaradenie cloudovej služby na portál vládneho cloudu.

1 Základné pojmy

Základné pojmy a požiadavky, ktoré boli začlenené do vývoja katalógu kritérií, sú popísané v tejto časti.

1.1 Požiadavky katalógu kritérií

Na vypracovanie katalógu kritérií boli zohľadnené nasledujúce požiadavky.

1.1.1 Všeobecné požiadavky

- katalóg kritérií obsahuje minimálne množstvo kritérií a kritéria na posúdenie cloudovej služby v požadovanej hĺbke pre Vládny cloud,
- kritériá musia preto pokrývať všetky oblasti relevantné pre používateľov cloudu: zmluvné aspekty, kvalita poskytovania služieb, súkromie údajov, bezpečnosť dát,
- katalóg kritérií definuje minimálne požiadavky, ktoré musí služba splniť, aby mohla byť uvedená na portáli Vládneho cloudu,
- kritériá musia byť vhodné na to, aby si ich vyžiadali a analyzovali v kontexte vlastných testov od poskytovateľa,
- katalóg kritérií musí byť predložený.

Požiadavky katalógu kritérií sa môžu líšiť aj podľa zainteresovaných strán portálu Vládneho cloudu, ktoré sú popísané v nasledujúcich častiach.

1.1.2 Požiadavky používateľov cloudu

Katalóg kritérií Vládneho cloudu je pre používateľa transparentný, kritériá sú vhodné na výber a porovnanie spoľahlivých služieb cloudu, t. z. uskutočňujú vyhlásenia týkajúce sa:

- zabezpečenia údajov,
- ochrany osobných údajov,
- právnej zhody,
- integrácie služieb do existujúcej infraštruktúry,
- zabráneniu vzniku ďalších závislostí,
- zabezpečenie investícií.

1.1.3 Požiadavky na poskytovateľa cloudu

Kritériá a charakteristiky musia byť zodpovedajúce a zároveň zrozumiteľné, t. z. musí byť transparentné a zrejmé, prečo sa požaduje dané kritérium. Minimálne požiadavky na zaradenie do zoznamu katalógu služieb musia byť dostupné už pred samotnou registráciou.

1.2 Rozsah zladenia a testovania

Aktuálna verzia katalógu kritérií Vládneho cloudu je založená na kritériách, ktoré prezentujú transparentnosť poskytovateľa, najmä na uvedení všetkých subdodávateľov zaoberajúcich sa poskytovaním služieb, ako je prevádzka dátových centier, návrh zmluvy a zabezpečenie kontroly používateľa nad svojimi údajmi.

Podrobné technické informácie a kontrolné mechanizmy zabezpečenia údajov nie sú súčasťou aktuálnej verzie katalógu kritérií. Tieto sa preukazujú príslušnými certifikátmi, certifikáciou cloudových služieb a použitou technickou infraštruktúrou.

Kritériá v oblasti ochrany údajov sú zamerané na prezentáciu implementácie legislatívnych požiadaviek nariadenia Európskej únie o ochrane osobných údajov (GDPR). Je potrebné preukázateľne zdokumentovať implementovanú úroveň ochrany osobných údajov.

Ďalším dôležitým cieľom katalógu kritérií pre Vládny cloud je popis cloudovej služby z pohľadu používateľa, ktorý spresňuje kritériá transparentnosti. Popri funkčnom opise služieb obsahuje katalóg takisto kritériá na prezentáciu technických a funkčných podmienok na použitie služby, migračné postupy, zmenové procedúry ako aj informácie o požadovaných procesoch poskytovania služieb a zabezpečenia dohôd o úrovni poskytovaných služieb (SLA) ako je dostupnosť poskytovanej služby a ostatné podporné služby.

Katalóg kritérií Vládneho cloudu bol navrhnutý tak, aby bol vyplnený právne záväzným sebahodnotením poskytovateľa cloudovej služby.

Poskytovateľ môže overiť jednotlivé informácie predložením príslušných certifikátov. Samotné overenie vykoná príslušná organizácia prevádzkovateľa Vládneho cloudu prostredníctvom kontroly pravdivosti informácií o poskytovateľovi. V súčasnosti sa nevykonáva žiadny dodatočný audit poskytovateľa.

1.3 Minimálne požiadavky

Minimálne požiadavky rozlišujú medzi požiadavkami, ktoré slúžia na transparentné prezentovanie cloudovej služby a požiadavkami, ktoré definujú minimálnu charakteristiku špecifického kritéria kvality služby alebo poskytovania služieb.

Ďalšie informácie sú uvedené v časti 3.2 o ostatných minimálnych požiadavkách katalógu kritérií.

1.4 Ďalší rozvoj a prevedenia katalógu

Katalóg kritérií Vládneho cloudu je priebežne aktualizovaný a dopĺňaný príslušnou organizáciou prevádzkovateľa Vládneho Cloudu a je dostupný na jeho webovom sídle. Aktualizácie môžu obsahovať pridanie nových kritérií, zmenu existujúcich kritérií, ako aj úpravu minimálnych požiadaviek.

Úpravou katalógu kritérií sa nastaví nová verzia katalógu kritérií. Aktualizovaná verzia katalógu kritérií je záväzná pre zoznam nových služieb a obnovenie zoznamu existujúcich služieb. Poskytovateľ by mal vo vlastnom záujme zabezpečiť súlad kritérií svojej poskytovanej služby s aktualizovanými kritériami, čomu by mala zodpovedať aj motivácia napríklad formou atraktívnej cenovej politiky poplatkov za opätovné zaradenie služby do zoznamu.

Katalóg kritérií je navyše rozšírený o ďalšie varianty, napríklad pre rôzne aplikačné oblasti, ako napríklad oblasť zdravotníckych informácií (eHealth) alebo Industry 4.0. Varianty môžu rozšíriť kritériá katalógu všeobecných kritérií, napríklad doplnením zvýšených minimálnych požiadaviek alebo nových kritérií. Preto obsahuje úplný súbor kritérií, ktoré musia spĺňať službu pre zaradenie do zoznamu s príslušným variantom.

Varianty sú založené na verzii katalógu spoločných kritérií pre cloudovú službu, ktoré sú záväzné a na kritériách, špecifických pre príslušný variant. Hlavné číslo označuje verziu katalógu všeobecných kritérií, na ktorom je tento variant založený. Menšie číslo verzie označuje verziu variantu. Ak existuje nová verzia katalógu kritérií, všetky varianty musia byť tiež aktualizované.

1.5 Použité zdroje

Nasledujúce zdroje boli vyhodnotené a zahrnuté do koncepcie katalógu kritérií služby vládneho cloudu pre cloudové služby:

Odporúčania a princípy noriem:

- ISO/IEC 27000 pre riadenie informačnej bezpečnosti,
- ISO 20000 riadenie služieb pre informačné technológie,
- ISO 9000 systém riadenia kvality,
- Metodiky IT Infrastructure Library (ITIL) a ITSM,
- Odporúčania ENISA, NIST, BSI,
- Odporúčanie Európskej komisie pre oblasť cloudových služieb.

2 Štruktúra katalógu kritérií

Katalóg cloudových kritérií pre akreditáciu cloudových služieb vládneho cloudu pozostáva z niekoľkých oblastí, ktoré obsahujú série kritérií. Každé kritérium je rozdelené na jednu alebo viac charakteristík, ktoré musí poskytovateľ špecifikovať, aby opísal službu cloudu.

2.1 Oblasti a kritériá

Katalóg kritérií Vládneho cloudu je štruktúrovaný do štyroch nasledujúcich oblastí:

- (EL) Ekonomika a legislatíva
- (PV) Prevádzka
- (BZ) Bezpečnosť
- (SP) Špecifické

Tabuľka č. 1: Oblasti katalógu Vládneho cloudu

ID	Oblasť	Náplň
<i>EL</i>	Ekonomika a legislatíva	Pre poskytovateľov kritéria, poskytujú informácie o poskytovateľovi, vlastnícka štruktúra a schopnosť poskytovať cloudové služby. Zároveň posúdenie obsahu zmluvných podmienok pre poskytované služby s ohľadom na bezpečné využívanie cloudu.
<i>PR</i>	Prevádzka	Kritéria, ktoré poskytujú základný obraz akým spôsobom je služba poskytovaná a akú úroveň zabezpečenia prevádzkových procesov poskytovateľ pre službu zabezpečuje.
<i>SE</i>	Bezpečnosť	Ochrana informačných systémov, organizačné požiadavky, preventívne opatrenia, správa hesiel, správa hesiel, technické aspekty ochrany osobných údajov.
<i>SS</i>	Špecifické	Analýza nasadenej technológie, činnosti, na ktoré má zákazník oprávnenie, prístup hypervízora, operačné systémy, analýza nasadenej technológie, izolácia klientov, bezpečnostné technológie, nasadenie do prevádzky, exportné formáty, integrácia, dokumentácia.

Každá oblasť je rozdelená na niekoľko kritérií, ktoré sú uvedené v nasledujúcej tabuľke:

Tabuľka č. 2: Kritériá oblastí katalógu Vládneho cloudu

ID	Oblasť
EL	EKONOMIKA A LEGISLATÍVA
	Všeobecné informácie o poskytovateľovi cloudovej služby
	Zmluvné náležitosti a oblasť súladu
PR	PREVÁDZKA
	Správa a prevádzka dátových centier
	Zákaznícka podpora
	Správa poskytovaných služieb
SE	BEZPEČNOSŤ
	Riadenie bezpečnosti
	Technická bezpečnosť
	Technické opatrenia na ochranu osobných údajov
SS	ŠPECIFICKÉ
	Iaas
	Paas
	Saas

Jednotlivé oblasti sa ďalej delia:

Tabuľka č. 3: Rozdelenie kritérií oblasti EKONOMIKA A LEGISLATÍVA

Oblasť	ID	Kritérium
EL		Všeobecné informácie o poskytovateľovi cloudovej služby
	C1	Profil poskytovateľa cloudových služieb
	C2	Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb
	C3	Správa služieb

	C4	Detailnejší profil spoločnosti
	C5	Referenčné informácie o cloudovej službe
	C6	Platné certifikáty
	Zmluvné náležitosti a oblasť súladu	
	C7	Zmluvné náležitosti
	C8	Pravidlá narábania s dátami
	C9	Zmluvné požiadavky zabezpečenia a ochrany dát
	C10	Zmluva o úrovni poskytovaných služieb (SLA)
	C11	Podmienky v prípade zastavenia poskytovania zazmluvnených služieb
	C12	Ceny a nákladové položky za poskytované služby
	C13	Špecifické okruhy otázok (voliteľné)

Tabuľka č. 4: Rozdelenie kritérií oblasti PREVÁDZKA

Oblasť	ID	Kritérium
PR	Správa a prevádzka dátových centier	
	C1	Preukázanie minimálnych požiadaviek na správu a prevádzku dátového centra a príslušných zariadení.
		Základná miestna bezpečnosť
		Kontrola prístupov
		Bezpečná prevádzka
		Organizácia dátového centra
	Zákaznícka podpora	
	C2	Overenie služieb podpory
	Správa poskytovaných služieb	
	C3	Overenie základných princípov správy služieb
		Riadenie incidentov
		Manažment problémových stavov
		Riadenie zmien
		Manažment konfigurácií
		Manažment verzií
		Kapacitné plánovanie
		Riadenie dostupnosti služieb

		Manažment havarijných stavov
		Manažment rizík
		Riadenie prevádzky
		Správa zálohovania
		Časový interval zálohovania

Tabuľka č. 5: Rozdelenie kritérií oblasti BEZPEČNOSŤ

Oblasť	ID	Kritérium
SE	Riadenie bezpečnosti	
	C1	Organizačné požiadavky
		Preventívne opatrenia
	Technická bezpečnosť	
	C2	Ochrana informačných systémov
		Prispôsobiteľnosť
		Správa hesiel
	Technické opatrenia na ochranu osobných údajov	
	C3	Technické posúdenie ochrany osobných údajov

Tabuľka č. 6: Rozdelenie kritérií oblasti ŠPECIFICKÉ

Oblasť	ID	Kritérium
SS	IaaS	
	C1	Referenčná architektúra
	C2	Systémový manažment
	C3	Bezpečnosť
	C4	Manažment licencií
	PaaS	
	C5	Referenčná architektúra
	C6	Bezpečnosť
	C7	Správa

	SaaS	
	C8	Interoperabilita
	C9	Podpora užívateľov

2.2 Minimálne požiadavky

Katalóg kritérií akreditácie vládneho cloudu definuje tieto typy minimálnych požiadaviek:

- **Povinná informácia** – vlastnosti služby, ktoré sú nevyhnutné na splnenie podmienok zápisu služby do katalógu. Hodnotená služba ju musí spĺňať.
- **Voliteľná/Dodatočná informácia** -vlastnosti, ktoré sú špecifikované ako dodatočné a musia byť splnené v požadovanom objeme. Celkových dodatočných vlastností služieb.

3 Kritériá pre cloudové služby

3.1 EKONOMIKA A LEGISLATÍVA (EL)

Všeobecné informácie o poskytovateľovi cloudovej služby. Transparentné predstavenie poskytovateľa, jeho podnikový profil.

C1. Profil poskytovateľa cloudových služieb

Zmluvný partner, ponúkajúci klientom cloudové služby ako právny subjekt. Kritériá obsahujú informácie o totožnosti poskytovateľa, ako je adresa a číslo registrácie alebo daňové identifikačné číslo / identifikačné číslo DPH, informácie, ako aj kontaktné adresy hlavnej kontaktnej osoby. Dôkaz sa uskutočňuje prostredníctvom dodaného výpisu z obchodného alebo kooperačného registra alebo porovnateľného úradného registra alebo adresára.

Tabuľka č. 7: Profil poskytovateľa cloudových služieb

ID	Profil poskytovateľa cloudových služieb	Úroveň	Povinné
EL-C1-01	Názov spoločnosti (Zmluvný partner, ponúkajúci klientom cloudové služby ako právny subjekt)	U1	Áno
EL-C1-02	Adresa spoločnosti	U1	Áno
EL-C1-03	Mesto	U1	Áno
EL-C1-04	Štát	U1	Áno
EL-C1-05	Webová stránka spoločnosti (URL)	U1	Áno
EL-C1-06	Štát, v ktorom je spoločnosť registrovaná (Priložiť kópiu výpisu z obchodného registra / registračného záznamu)	U1	
EL-C1-07	IČO / registračné číslo spoločnosti	U1	Áno
EL-C1-08	Dátum zápisu do obchodného registra / registrácie	U1	Áno

EL-C1-09	Kontaktná osoba, zodpovedná za obchodnú činnosť (<i>Meno a priezvisko, e-mailová adresa, tel. číslo</i>)	U1	Áno
EL-C1-10	Kontaktná osoba, zodpovedná za technickú oblasť (<i>Meno a priezvisko, e-mailová adresa, tel. číslo</i>)	U1	
EL-C1-11	Kontaktná osoba, zodpovedná za dátovú bezpečnosť (<i>Meno a priezvisko, e-mailová adresa, tel. číslo</i>)	U1	
EL-C1-12	Kontaktná osoba, zodpovedná za právne a zmluvné náležitosti (<i>Meno a priezvisko, e-mailová adresa, tel. číslo</i>)	U1	

C2. Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb

Kritériá obsahujú informácie o fyzickom umiestnení (adresy) jednotlivých dátových centier, v ktorých je prevádzkovaná poskytovaná cloudová služba. Fyzická lokalizácia dátového centra je dôležitý údaj napr. pre splnenie legislatívnych požiadaviek (nariadenie GDPR) o mieste, na ktorom sú spracovávané osobné údaje (EÚ).

Tabuľka č. 8: Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb

ID	Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb	Úroveň	Povinné
EL-C2-01	Úplné kontaktné údaje a adresa primárneho dátového centra	U1	Áno
EL-C2-02	Primárne dátové centrum - názov a adresa (<i>Prosím uveďte oficiálnu adresu a kontakt na zmluvného partnera</i>)	U1	Áno
EL-C2-03	Vlastník dátového centra a jeho vlastnícka štruktúra	U1	
EL-C2-04	Úplné kontaktné údaje a adresa sekundárneho / záložného dátového centra	U1	
EL-C2-05	Sekundárne / záložné dátové centrum - názov a adresa (<i>Prosím uveďte oficiálnu adresu a kontakt na zmluvného partnera</i>)	U1	

EL-C2-06	Vlastník dátového centra a jeho vlastnícka štruktúra	U1	
----------	--	----	--

C3. Správa služieb

Táto informácia má špecifikovať pre každé dátové centrum alebo akéhokoľvek subdodávateľa, ktorý je priamo spojený s poskytovaním služieb, alebo nepriamo môže získať prístup k dátovým oblastiam služieb. Objasnenie umiestnenia údajov a súvisiacich subdodávateľov.

Tabuľka č. 9: Správa služieb

ID	Správa služieb	Úroveň	Povinné
EL-C3-01	Možnosti prístupu tretích strán (technický a prevádzkový personál), úroveň legislatívnych obmedzení (regulácia) (Prosím uveďte zoznam externých subjektov, ich štruktúru a pôsobnosť)	U1	Áno

C4. Detailnejší profil spoločnosti

Profil spoločnosti obsahuje informácie reprezentujúce veľkosť spoločnosti, ako aj informácie o skúsenostiach s poskytovaním cloudových služieb.

Tabuľka č. 10: Detailnejší profil spoločnosti

ID	Detailnejší profil spoločnosti	Úroveň	Povinné
EL-C4-01	Počet zamestnancov prevádzky cloudovej služby	U1	Áno

EL-C4-02	Centrála spoločnosti (<i>Prosím uveďte vlastnícku štruktúru spoločnosti spolu s kontaktnými údajmi</i>)	U1	
EL-C4-03	Celkový počet zamestnancov spoločnosti	U1	Áno
EL-C4-04	Postavenie spoločnosti (<i>ISV - nezávislý poskytovateľ služieb, Reseller - predajca služieb, Poskytovateľ cloudových služieb (IaaS), Poskytovateľ cloudových služieb (PaaS), Poskytovateľ cloudových služieb (SaaS), Iné</i>)	U1	
EL-C4-05	Úroveň / miera skúseností s poskytovaním služby	U1	Áno

C5. Referenčné informácie o cloudovej službe

Špecifikácia základných informácií pre opis služieb. Cieľom je základná klasifikácia služby podľa typu poskytovania služieb a modelu služieb.

Tabuľka č. 11: Referenčné informácie o cloudovej službe

ID	Referenčné informácie o cloudovej službe	Úroveň	Povinné
EL-C5-01	Názov cloudovej služby	U1	Áno
EL-C5-02	Stručný popis ponúkanej cloudovej služby	U1	Áno
EL-C5-03	Webová stránka ponúkanej cloudovej služby (<i>Prosím uveďte URL</i>)	U1	Áno
EL-C5-04	Celkový počet cloudových služieb (nie moduly) (<i>Prosím uveďte rozsah verejne ponúkaných cloudových služieb Vašou spoločnosťou</i>)	U1	
EL-C5-05	Počet zákazníkov cloudovej služby s ohľadom na jej posúdenie /certifikáciu	U1	
EL-C5-06	Počet používateľov cloudovej služby s ohľadom na jej posúdenie /certifikáciu	U1	

C6. Platné certifikáty

Podrobnosti o certifikáciách dátových centier a technickej infraštruktúry. Je možné zaregistrovať viac certifikátov. Ak je špecifikovaný certifikát, uvedú sa všetky uvedené vlastnosti certifikátu. Dôkaz sa uskutočňuje prostredníctvom prenesených dokumentov. Dôkaz o informáciách o implementovaných opatreniach v oblasti IT bezpečnosti, súkromia údajov, správy služieb atď., Subdodávateľov, ktorí sa podieľajú na poskytovaní služby alebo dátových centrách.

Tabuľka č. 12: Platné certifikáty a štandardy

ID	Platné certifikáty	Úroveň	Povinné
EL-C6-01	Prosím uveďte všetky existujúce platné certifikáty z oblasti technickej <i>(dátumy platnosti a expirácie spolu s podrobnejším popisom obsahu, scan certifikátov spolu s evidenčnými číslami)</i>	U1	
EL-C6-02	Prosím uveďte všetky existujúce platné certifikáty z oblasti riadenia kvality <i>(dátumy platnosti a expirácie spolu s podrobnejším popisom obsahu, scan certifikátov spolu s evidenčnými číslami)</i>	U1	
EL-C6-03	Prosím uveďte všetky existujúce platné certifikáty z oblasti súladu a zhody <i>(dátumy platnosti a expirácie spolu s podrobnejším popisom obsahu, scan certifikátov spolu s evidenčnými číslami)</i>	U1	
EL-C6-04	Prosím uveďte všetky existujúce platné certifikáty z oblasti ochrany a bezpečnosti dát <i>(dátumy platnosti a expirácie spolu s podrobnejším popisom obsahu, scan certifikátov spolu s evidenčnými číslami)</i>	U1	
EL-C6-05	Prosím uveďte všetky odvetvovo špecifické certifikáty <i>(dátumy platnosti a expirácie spolu s podrobnejším popisom obsahu, scan certifikátov spolu s evidenčnými číslami)</i>	U1	
EL-C6-06	Čestne prehlasujete dodržiavanie štandardov podľa § 55 ods. 4 písm. d) výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov ? <i>(prosím uveďte zoznam štandardov, s ktorými ste v súlade)</i>	U1	

C7. Zmluvné náležitosti

Zastúpenie príslušných náležitostí zmluvy pre zabezpečenie použitia cloudovej služby. Obsahujú základné zmluvné podmienky a podmienky zrušenia zmluvy. Všeobecná transparentnosť zmluvy. Informácie o transparentnosti všeobecných zmlúv. Zmluvy sú plne dostupné pre užívateľov vopred a nachádzajú sa v priloženom odkaze.

Tabuľka č. 13: Zmluvné náležitosti

ID	Zmluvné náležitosti	Úroveň	Povinné
EL-C7-01	Sú základné zmluvné podmienky dostupné klientovi ešte pred tým, ako si objedná príslušnú službu ? (Základné informácie sú dostupné on-line alebo na vyžiadanie)	U1	
EL-C7-02	Sú všetky relevantné zmluvné podmienky zahrnuté a referencované (napr. všeobecné zmluvné podmienky, zásady ochrany osobných údajov, bezpečnostné politiky atď) ? (Či je dostupný hlavný dokument (napr. rámcová zmluva), kde sú uvedené zrejme odkazy na ponúkanú službu. Sú uvedené všetky súvisiace dohody uvedené v tomto dokumente.)	U1	
EL-C7-03	Je zabezpečené, že klient bude oboznámený so zmenami v zmluvných podmienkach zo strany poskytovateľa služieb ? (Klient je prizvaný pri zapracovaní významných zmien do zmluvných podmienok, ak by táto zmena mohla významne ovplyvniť jeho vlastné podmienky a pravidlá zhody)	U2	
EL-C7-04	Sú všetky relevantné zmluvné podmienky a požiadavky premietnuté aj do zmlúv so subdodávateľmi ? (Dôraz je kladený na SLA, ochranu osobných údajov a súkromie, služby zabezpečenia a podpory prevádzkovaných služieb, identifikácia potenciálnych rozdielov medzi povinnosťami poskytovateľa služieb a a povinnosťami prenesenými na subdodávateľov)	U1	
EL-C7-05	Je možné ukončiť zmluvu len oznámením alebo ohlásením ? (Musí byť uvedené minimálne štandardné ustanovenie o podmienkach ukončenia zmluvy)	U1	

EL-C7-06	Je k dispozícii zoznam možných okolností, za ktorých je možné obojstranné ukončenie zmluvného vzťahu ? (Zrozumiteľné vymenovanie podmienok pre ukončenie zmluvného vzťahu)	U2	
EL-C7-07	Je zmluvne zabezpečené oboznamovanie klienta so zmenami, týkajúcimi sa subdodávateľov poskytovaných služieb ? (Transparentnosť ohľadom zazmluvnených subdodávateľov služieb)	U2	
EL-C7-08	Má klient oprávnenie na ukončenie zmluvného vzťahu s poskytovateľom služieb v prípade zmien ohľadom subdodávateľov poskytovaných služieb ? (Klient má možnosť ukončiť zmluvu v prípade nespokojnosti s voľbou subdodávateľa poskytovaných služieb)	U3	

C8. Pravidlá narábania s dátami

Lokalizácia uchovávaných dát a prístup klienta k dátam

Tabuľka č. 14: Pravidlá narábania s dátami

ID	Všeobecné organizačno-bezpečnostné požiadavky	Úroveň	Povinné
EL-C8-01	Má klient k dispozícii informácie ohľadom lokality, kde sú fyzicky umiestnené spracovávané dáty, poštovú adresu a kontaktné údaje ? (Klient musí mať k dispozícii informácie o geografickom umiestnení osobných a finančných dát, ak to vyžaduje súlad s miestnou legislatívou)	U1	
EL-C8-02	Môže klient určiť, aby boli spracovávané dáta fyzicky umiestnené v konkrétnom regióne, krajine, na konkrétnej fyzickej adrese alebo v oblasti špecifickej právnej pôsobnosti, ak má poskytovateľ služby k dispozícii viacero fyzických lokalít pre umiestnenie dát ? (Musí byť zaručené, že aj služby týkajúce sa zálohovania a archivácie nebudú vykonávané v lokalitách mimo vymedzenú oblasť. Táto požiadavka sa vzťahuje aj na služby a prevádzkový personál, ktorý by mal byť lokalizovaný len v rámci špecifikovaného regiónu)	U2	
EL-C8-03	Má klient v prípade ukončenia poskytovania služieb aj naďalej prístup k svojim dátam bez akýchkoľvek obmedzení ? Ako je zabezpečená archivácia týchto dát ?	U1	

	<i>(Klient má mať právo na prístup k svojim dátam aj v prípade ukončenia poskytovania služieb z dôvodu neplnenia zmluvných podmienok a záväzkov. Poskytovanie ponúkaných služieb môže byť prerušené)</i>		
EL-C8-04	Zaručí poskytovateľ služieb, že v prípade mimoriadneho preušetrenia zmluvných vzťahov nebudú vymazané klientské dáta a že klientské archívy dát budú uchované ? (Záruka potenciálnej obnovy dát)	U3	
EL-C8-05	Je zabezpečená ochrana klientských dát a ich dostupnosť klientovi aj v prípade bankrotu poskytovateľa služieb ? (Proces a deklarácia, zaručujúca klientovi rovnakú úroveň prístupu k svojim dátam aj u nástupníckeho poskytovateľa služieb)	U3	

C9. Zmluvné požiadavky zabezpečenia a ochrany dát

Technické a organizačné procesy + Súlad s národnými legislatívnymi požiadavkami na ochranu a zabezpečenie dát

Tabuľka č. 15: Zmluvné požiadavky zabezpečenia a ochrany dát

ID	Všeobecné organizačno-bezpečnostné požiadavky	Úroveň	Povinné
EL-C9-01	Má klient k dispozícii jasnú špecifikáciu, ako ponúkané služby spracovávajú a narábajú s osobnými údajmi ? (Zrozumiteľný úplný popis rolí a procesov poskytovateľa služieb ako spracovateľa dát)	U2	
EL-C9-02	Je jednoznačne zmluvne zabezpečené, že akákoľvek zmena služby, ktorá by mohla ovplyvniť charakter spracovania osobných údajov, musí byť dohodnutá a potvrdená zákazníkom - správcom osobných údajov ? (Príručka pre audit spracovávania osobných údajov)	U2	
EL-C9-03	Sú definované postupy a procesy na opravu, vymazanie a uzamknutie osobných údajov na požiadanie dotknutej osoby ? Ak áno, ktoré procedúry a ako sú definované ? (Pozri príručku pre audit spracovávania osobných údajov)	U3	
EL-C9-04	Je jasne definované časové obdobie spracovania údajov a kedy dôjde k vymazaniu údajov ? (Dozorujúci kontrolný orgán je povinný viesť evidenciu o existujúcich osobných údajov spracovávaných poskytovateľom služieb)	U2	

EL-C9-05	Je zákazník oprávnený požadovať od poskytovateľa služieb podpísanú zmluvu v písomnej forme ? (Niektoré krajiny vyžadujú zmluvu v písomnej forme, pokiaľ sú legislatívne požadované a uplatňované pravidlá ochrany osobných údajov)	U2	
EL-C9-06	Sú podrobné popísané postupy, podľa ktorých sú vykonávané technické a organizačné procesy s cieľom splniť legislatívne povinnosti správcu údajov, nielen osobných ? (Pozri príručku pre audit spracovávaní osobných údajov)	U2	

C10. a C11. Zmluva o úrovni poskytovaných služieb (SLA)

Informácie o dohodách, o verifikovateľnosti úrovne poskytovaných služieb (SLA) a pravidlách porušovania. SLA sú súčasťou zmluvy a existujú pravidlá pre porušenie SLA.

Tabuľka č. 16: Zmluva o úrovni poskytovaných služieb (SLA)

ID	Zmluva o úrovni poskytovaných služieb (SLA)	Úroveň	Povinné
EL-C10-01	Je dohoda o úrovni poskytovaných služieb (SLA) súčasťou celkovej zmluvy a popisuje dostatočne záruku kvality poskytovaných služieb ? (Uveďte parametre úrovne poskytovaných služby, ktoré môžu byť sledované a monitorované klientom)	U1	
EL-C11-01	Je plnenie zmluvy o úrovni a parametroch poskytovaných služieb (SLA) overiteľné klientom ? (Poskytovanie min. štvrťročne správy a výkazy alebo informačný nástroj s určenými ukazovateľmi KPI)	U2	
EL-C11-02	Obsahuje SLA sankčné ustanovenia v prípade nedostatočnej kvality poskytovaných služieb ? (Situácia, keď nie sú dodržiavané parametre úrovne poskytovaných služieb (SLA) môže mať vážne dôsledky pre zákazníka a musí byť deklarovaná na zmluvnej úrovni)	U3	

C12. Podmienky v prípade zastavenia poskytovania zazmluvnených služieb

Pravidlá prerušenia služby alebo platobnej neschopnosti. Poskytujú sa jasné pravidlá, ktoré kedykoľvek zaručujú spätnú väzbu s údajmi.

Tabuľka č. 17: Podmienky v prípade zastavenia poskytovania zazmluvnených služieb

ID	Všeobecné organizačno-bezpečnostné požiadavky	Úroveň	Povinné
EL-C12-01	Sú poskytované cloudové služby zabezpečené zmluvne s inými stranami, ktoré by mohli byť pokračovateľom poskytovaných služieb ? (Je špecifikovaný formálny nasledovník pre poskytované služby, ktorý by bol zodpovedný za podporu zákazníka pri archivácii a prenose údajov)	U3	
EL-C12-02	Sú zmluvne zabezpečené práva klienta ohľadom prístupu k jeho dátam v prípade bankrotu dodávateľa poskytovaných služieb ? (Zmluva alebo osobitné právne ustanovenie, zabezpečujúce prístup ku klientským dátam na fyzickom mieste uchovávaní údajov)	U2	
EL-C12-03	Existuje všeobecné neobmedzujúce právo klienta na prístup ku klientským dátovým archívom pre klienta s príslušnou dokumentáciou dátovej štruktúry ? (Špecifikácia procesov exportu a separácie údajov ako aj postupy odovzdávania dát a popis dátového formátu exportného typu dát)	U2	

C13. Ceny a nákladové položky za poskytované služby

Transparentný model cien. Informácie o použítom modeli cien, trvaní zmluvy a oznámení o zrušení. Vysledovateľný a transparentný výpočet služby

Tabuľka č. 18: Ceny a nákladové položky za poskytované služby

ID	Ceny a nákladové položky za poskytované služby	Úroveň	Povinné
----	--	--------	---------

EL-C13-01	Sú prehľadne uvedené jednotkové ceny a náklady na poskytované služby ? (Uvedenie vzorového výpočtu so všetkými nákladmi a dynamickými cenovými položkami)	U1	
EL-C13-02	Je klient oprávnený meniť počas doby poskytovania služby využívanie služieb na základe cenovej výhodnosti podľa odhadu využívania služieb ? (Ceny za poskytované služby by mali reflektovať zmeny cenových úrovní na trhu)	U3	

C14. Špecifické okruhy otázok (voliteľné)

Požiadavky pre špecifické požiadavky a prípady

Tabuľka č. 19: Špecifické okruhy otázok (voliteľné)

ID	Špecifické okruhy otázok (voliteľné)	Úroveň	Povinné
EL-C14-01	Sú postupy pre digitálne podpisovanie dátových objektov v súlade s platnými legislatívnymi predpismi ? (Účtovné postupy musia byť v súlade s lokálnou legislatívou)	U3	
EL-C14-02	Je zmluvne zabezpečený prístup oprávneného externého audítora v súlade s platnou legislatívou (prístup v režime len na čítanie) ? (Osobitné postavenie tretích strán, ako napríklad finančných úradov, umožňujúce prístup k údajom v režime čítania.)	U2	
EL-C14-03	Sú spracovávané údaje, relevantné pre daňové účely jasne zmluvne definované opísané a sú v súlade s lokálnou legislatívou ? (Certifikát súladu s platnými daňovými zákonmi)	U3	
EL-C14-04	Je akýkoľvek prístup a zmena spracovávaných dokumentov zaznamenaná v monitorovacom systéme ? Sú tieto systémy zabezpečené proti manuálnemu zásahu ?	U3	

EL-C14-05	Je možné zabrániť fyzickému vymazaniu spracovávaných dát, ak to vyžaduje lokálna legislatíva ?	U3	
-----------	--	----	--

3.2 PREVÁDZKA (PR)

Informácie o správe a prevádzke dátových centier, zákazníckej podpore a správe poskytovaných služieb

C1. Správa a prevádzka dátových centier

Popis riadenia prevádzky dátových centier, v ktorých je prevádzkovaná poskytovaná cloudová služba. Základom sú ustanovenie a odporúčania v súlade s normou ISO/IEC 27000, opis architektúry IS dátových centier s ohľadom na zabezpečenie ponúkanej miery spoľahlivosti, prevádzkovej bezpečnosti s dostupnosti poskytovanej cloudovej služby, opis komponentov fyzickej bezpečnosti a zabezpečenia.

Tabuľka č. 20: Správa a prevádzka dátových centier

ID	Správa a prevádzka dátových centier	Úroveň	Povinné
PR-C1-01	Spĺňa dátové centrum minimálne požiadavky ? (Súlad s ISO 27001 môže byť overený napr. Certifikáciou CSA, ECSA, BC5,)	U1	Áno
PR-C1-02	Existuje nebezpečenstvo alebo analýza rizík pre fyzické umiestnenie / lokalitu dátového centra ? (Transparentnosť ohľadom potenciálnych lokálnych rizík)	U2	Áno
PR-C1-03	Existuje primeraný fyzický prístup a bezpečnostná koncepcia pre dátové centrum ? (Fyzická ochrana a ochrana pred neoprávneným vstupom)	U1	Áno
PR-C1-04	Je prístup do priestorov, kde je prevádzkovaná poskytovaná služba zabezpečený proti neoprávnenému vstupu ? (Preukázanie zodpovedajúcej miery ochrany pred neoprávneným prístupom do prevádzkových priestorov)	U1	Áno
PR-C1-05	Existuje redundantný záložný zdroj napájania a UPS ? (Zabezpečenie nepretržitej prevádzky pri výpadku dodávky elektrickej energie)	U1	Áno

PR-C1-06	Existuje redundantné pripojenie do internetu ? (<i>Dátové centrum má mať aspoň 2 oddelené nezávislé dátové linky do internetu</i>)	U3	
PR-C1-07	Je napájanie infraštruktúry redundantné ? (<i>Redundantné privody a príslušné zariadenia v dátovom centre</i>)	U2	Áno
PR-C1-08	Sú klimatizačné systémy redundantné ? (<i>Zabezpečenie nepretržitej prevádzky v prípade výpadku klimatizácie</i>)	U1	Áno
PR-C1-09	Sú hardvérové komponenty primerane oddelené od inej infraštruktúry ? Je možná škálovateľnosť v prípade potreby ? (<i>Zodpovedajúca miera oddelenia komponentov a rozšíriteľnosť</i>)	U1	
PR-C1-10	Aká je percentuálna miera dostupnosti jednotlivých dátových centier ? (<i>A > 99,5</i>)	U2	
PR-C1-11	Aká je percentuálna miera dostupnosti jednotlivých dátových centier ? (<i>B > 99,0</i>)	U1	Áno
PR-C1-12	Aká je percentuálna miera dostupnosti jednotlivých dátových centier ? (<i>C > 98,5</i>)	U2	
PR-C1-13	Ako vysoká je úroveň miery dostupnosti redundantnej architektúry dátového centra ? (<i>mala by byť 99,9</i>)	U3	Áno
PR-C1-14	Je k dispozícii prevádzkový manuál dátového centra ? (<i>Ak áno, poskytnite</i>)		Áno
PR-C1-15	Existuje núdzový plán v prípade neočakávanej / katastrofickej udalosti a existujú záložné pracovné stanice ?	U3	Áno
PR-C1-16	Je redundancia dátových centier zabezpečená formou distribuovaných / zrkadlených / záložných dátových centier ? (<i>Preukázanie scenárov záložného prebratia prevádzky bez viditeľných dopadov na zákazníka</i>)	U3	Áno
PR-C1-17	Existuje správa o protipožiarnej ochrane ? (<i>Preukázanie protipožiarnych opatrení</i>)	U3	Áno

C2. Zákaznícka podpora

Popis služieb zákazníckej podpory k poskytovanej cloudovej službe, HelpDesk a jeho dostupnosť, reakčná doba na podnet, klasifikácia miery závažnosti podnetov, lehoty na vyriešenie podnetu, prístup zákazníka k záznamom o podnetoch. Zákaznícka podpora významnou mierou prispieva k úrovni kvality poskytovaných služieb..

Tabuľka č. 21: Zákaznícka podpora

ID	Zákaznícka podpora	Úroveň	Povinné
PR-C2-01	Ako prebieha autentifikácia používateľa v súvislosti s podporou služieb ? (Úroveň oprávnenia pracovníkov podpory služieb pri schválení žiadosti špecifickej požiadavky zákazníka)	U1	Áno Podľa: C1F05, C1F06, C1OR08
PR-C2-02	Ako prebieha autentifikácia používateľa v súvislosti s podporou služieb ?	U2	Áno
PR-C2-03	Ako prebieha autentifikácia používateľa v súvislosti s podporou služieb ?	U3	
PR-C2-04	Aká je zaručená doba odozvy ? (Zaručená doba odozvy (nie lehota vyriešenia požiadavky) na servisnú požiadavku)	U1	
PR-C2-05	Aká je zaručená doba odozvy ?	U2	
PR-C2-06	Aká je zaručená doba odozvy ?	U3	
PR-C2-07	Aká je priemerná lehota na vyriešenie servisnej požiadavky ? (Priemerný čas vyriešenia požiadavky podľa štandardizovaných priorít)	U1	
PR-C2-08	Aká je priemerná lehota na vyriešenie servisnej požiadavky ? (Priemerný čas vyriešenia požiadavky podľa štandardizovaných priorít)	U2	
PR-C2-09	Aká je priemerná lehota na vyriešenie servisnej požiadavky ? (Priemerný čas vyriešenia požiadavky podľa štandardizovaných priorít)	U3	
PR-C2-10	Rozlíšenie podľa stupňa závažnosti.	U1	Áno Podľa: C1OR07, C1OR08
PR-C2-11	Rozlíšenie podľa stupňa závažnosti.	U2	
PR-C2-12	Rozlíšenie podľa stupňa závažnosti.	U3	

PR-C2-13	Má zákazník prístup (len na čítanie) k systému evidencie servisných požiadaviek prevádzkovateľa služby. (Zákazník má možnosť sledovať stav / aktivity ohľadom jednotlivých servisných požiadaviek)	U3	
PR-C2-14	Má zákazník prístup (len na čítanie) k systému evidencie servisných požiadaviek prevádzkovateľa služby. (Zákazník má možnosť sledovať stav / aktivity ohľadom jednotlivých servisných požiadaviek)	U2	Áno
PR-C2-15	Má zákazník prístup (len na čítanie) k systému evidencie servisných požiadaviek prevádzkovateľa služby. (Zákazník má možnosť sledovať stav / aktivity ohľadom jednotlivých servisných požiadaviek)	U1	Áno
PR-C2-16	Aká je dostupnosť linky servisnej podpory ? (prevádzkové hodiny 24x7)	U3	Áno
PR-C2-17	Aká je dostupnosť linky servisnej podpory ? (prevádzkové hodiny 5x10)	U2	Áno
PR-C2-18	Aká je dostupnosť linky servisnej podpory ? (prevádzkové hodiny resp. prezentácia dostupnosti služieb podpory)	U1	

C3. Správa poskytovaných služieb

Popis interných prevádzkových procesov poskytovateľa cloudovej služby, prezentácia súladu s ustanoveniami a odporúčaniami normy ISO/IEC 27000, opis manažmetu zmien, implementácie softvéru a manažmentu problémových situácií, opis procesov zabezpečenia nepretržitej prevádzky (Business continuity)

Tabuľka č. 22: Správa poskytovaných služieb

ID	Správa poskytovaných služieb	Úroveň	Povinné
PR-C3-01	Sú základné kritériá splnené v súlade s požiadavkami normy ISO 20000-1 ? (Splnenie požiadaviek na systém riadenia služieb (Service Management System, SMS))	U2	Áno

PR-C3-02	Je zavedený systém riadenia incidentov ? Je prístupný pre zákazníka poskytovanej služby ? <i>(Príslušné nástroje pre riešenie incidentov v oblasti poskytovaných služieb)</i>	U2	Áno
PR-C3-03	Sú príslušní subdodávateľia dôsledne integrovaní do systému riadenia incidentov ? <i>(Zahrnutie všetkých subdodávateľov do systému riadenia incidentov)</i>	U3	Áno
PR-C3-04	Sú definované role a príslušné úlohy pre systém správy problémov ? <i>(Efektívny manažment problémových stavov)</i>	U1	Áno
PR-C3-05	Sú zmeny v službách oznamované zákazníkovi dopredu, ak sa očakáva vplyv na prevádzkovanú službu ? <i>(Patričné informovanie zákazníka o možnom narušení / zmene poskytovanej služby)</i>	U1	Áno
PR-C3-06	Je manažment konfigurácií zdokumentovaný a vhodný pre príslušný typ poskytovanej služby ? <i>(Preukázanie manažmentu / správy konfigurácií v súvislosti s poskytovanou cloudovou službou)</i>	U2	Áno
PR-C3-07	Je nasadený koncept vývojového, testovacieho a prevádzkového systému ? <i>(Oddelenie prevádzkových systémov od vývojových a testovacích systémov, dodržiavanie pravidiel riadenia kvality pri nasadzovaní do prevádzky)</i>	U2	
PR-C3-08	Sú prevádzkované systémy nepretržite monitorované ? <i>(Proaktívny monitoring s cieľom identifikácie nezhôd s SLA)</i>	U1	Áno
PR-C3-09	Sú stanovené hraničné hodnoty, po prekročení ktorých majú byť nasedené doplnkové zdroje ? <i>(Preukázanie možností škálovania poskytovanej cloudovej služby)</i>	U2	
PR-C3-10	Je implementované riadenie dostupnosti poskytovaných služieb v súvislosti s technickými zdrojmi ? <i>(Špeciálne postupy pre riadenie dostupnosti technických zdrojov)</i>	U1	Áno
PR-C3-11	Je implementované riadenie dostupnosti poskytovaných služieb v súvislosti s aplikáciami ? <i>(Špeciálne postupy pre riadenie dostupnosti aplikácií)</i>	U1	Áno
PR-C3-12	Je implementovaný havarijný plán s presnými definíciami havarijných stavov a procesmi, podľa ktorých je potrebné postupovať v prípade výskytu takéhoto havarijného stavu ? <i>(Jednoznačné procesy pri havarijných situáciách s cieľom zníženia / eliminácie dopadov na zákazníka služby)</i>	U3	Áno
PR-C3-13	Je dostupná príručka s popisom havarijných stavov a akčným plánom činností v prípade havárie ? <i>(Postupy a kroky pri riešení núdzových situácií)</i>	U3	Áno

PR-C3-14	Existuje analýza rizík pre odhad škôd poskytovateľa služby v prípade výpadku v dátovom centre ? <i>(Interná analýza rizika poskytovateľa služieb)</i>	U2	Áno
PR-C3-15	Existujú prevádzkové manuály pre všetky aplikácie prevádzkované v dátovom centre a súvisiace s cloudovými službami ? <i>(Zodpovedajúce riadenie portfólia poskytovaných servisných služieb)</i>	U3	
PR-C3-16	Je implementovaný systém riadenia zálohovania ? <i>(Postupy pri zálohovaní)</i>	U1	Áno
PR-C3-17	Na aký typ médií sú dáta zálohované a na ako dlho ? <i>(Zálohovanie na zodpovedajúce médiá a zodpovedajúca doba uchovávaní dát)</i>	U1	Áno
PR-C3-18	Môže zákazník požadovať obnovu svojich dát ? Za aký čas bude obnova vykonaná ? <i>(Je možná individuálna obnova špecifických zákazníckych dát na požiadanie)</i>	U2	Áno
PR-C3-19	V akých časových intervaloch sú vykonávané zálohy dát ? <i>(Frekvencia zálohovacích cyklov)</i>	U3	Áno
PR-C3-20	V akých časových intervaloch sú vykonávané zálohy dát ? <i>(Frekvencia zálohovacích cyklov)</i>	U2	
PR-C3-21	V akých časových intervaloch sú vykonávané zálohy dát ? <i>(Frekvencia zálohovacích cyklov)</i>	U1	Áno
PR-C3-22	Sú zálohovacie médiá (pásky, CD, DVD ...) bezpečne uchovávané (trezor, oddelené miesto ...) ? <i>(Bezpečné archívy spracovávaných dát)</i>	U2	Áno
PR-C3-23	Sú aplikačné údaje zrkadlené s cieľom trvalej dostupnosti ? Existujú procedúry pre okamžité obnovenie prístupu k prevádzkovaným dátam ? <i>(Plná redundancia poskytovaných služieb)</i>	U3	
PR-C3-24	Je implementovaný systém riadenia kvality pri vývoji softvérových aplikácií ? <i>(Kvalita aplikácie)</i>	U2	
PR-C3-25	Sú definované, priebežne kontrolované a zdokumentované kritériá kvality procesov vývoja softvérových aplikácií ? <i>(Kvalita aplikácie)</i>	U3	

3.3 BEZPEČNOSŤ (SE)

Informácie týkajúce sa riadenia bezpečnosti, technickej bezpečnosti a technických opatrení na ochranu osobných údajov.

C1. Riadenie bezpečnosti

Prezentácia súladu s ustanoveniami a odporúčaniami normy ISO / IEC 27000 ohľadom informačnej bezpečnosti, opis súladu s lokálnymi právnymi predpismi, popis vykonávaných opatrení na zabezpečenie aktívnej a pasívnej bezpečnosti informačných systémov, popis prvkov ochrany, vzdelávanie zamestnancov a dokumentácia.

Tabuľka č. 23: Riadenie bezpečnosti

ID	Riadenie bezpečnosti	Úroveň	Povinné
SE-C1-01	Je vytvorený systém riadenia informačnej bezpečnosti (ISMS) podľa ISO 27001 ? <i>(Informácie o implementovanom systéme riadenia bezpečnosti)</i>	U1	Áno
SE-C1-02	Sú implementované bezpečnostné zásady v súlade s ISO 27002 alebo normami ENISA ? <i>(Informácie o štandardných kontrolných mechanizmoch opatreniam ne elimináciu nových hrozieb)</i>	U2	Áno
SE-C1-03	Je bezpečnostná architektúra služby v súlade s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti" pre úroveň "musí"? <i>(Architektúra musí byť v súlade s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti</i>	U1	Áno

	informačnej bezpečnosti" https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/metodika-zabezpecenia-ikt-8a6.html v aktuálnej verzii)		
SE-C1-04	Je bezpečnostná architektúra služby v súlade s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti" pre úroveň "malo by [byť]"? (Architektúra musí byť v súlade s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti" https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/metodika-zabezpecenia-ikt-8a6.html v aktuálnej verzii)	U1	Áno
SE-C1-05	Je vzdialený prístup s administrátorskými oprávneniami k citlivým systémom (manažment identity, databázy a osobné údaje) dostatočne chránený? (napr. zablokovaný prístup cez VPN, vyhradené virtuálne stanice bez možnosti prenosu dát ...)	U2	Áno
SE-C1-06	Je implementovaný manažment / riadenie používania kryptografických kľúčov? Sú kľúčoví používatelia nezávislí od správcov kryptografických kľúčov? (Preukázať systém riadenia a správy bezpečnostných kľúčov)	U3	Áno
SE-C1-07	Je v prípade narušenia bezpečnosti a neoprávneného prístupu k údajom zabezpečená komunikácia s príslušnými zodpovednými subjektmi? (Komunikačný plán so všetkými zainteresovanými subjektmi v prípade porušenia bezpečnosti v rámci bezpečnostných politík)	U3	Áno
SE-C1-08	Sú pravidelne školení pracovníci v oblasti bezpečnosti informačných technológií? (Preukázateľné školenia a preskúšanie školiacim inštitútom pre IEC 62443)	U3	
SE-C1-09	Sú pravidelne školení pracovníci v oblasti bezpečnosti informačných technológií? (Preukázateľné školenia a preskúšanie)	U2	Áno
SE-C1-10	Sú pravidelne školení pracovníci v oblasti bezpečnosti informačných technológií? (Plán školení a plán účasti zodpovedných pracovníkov na školeniach)	U1	Áno
SE-C1-11	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov? (Špecializované školenia s následnou certifikáciou)	U3	Áno
SE-C1-12	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov? (Implementované pravidlá, individuálne potvrdené každým jednotlivcom)	U2	Áno

SE-C1-13	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov ? (Pravidlá sú uvedené v pracovnej zmluve)	U1	Áno
SE-C1-14	Sú pravidelne vykonávané bezpečnostné a penetračné testy ? (Proaktívny bezpečnostný monitoring a overenie bezpečnostných postupov)	U3	Áno
SE-C1-15	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov ? (Preukázateľné školenia a preskúšanie školiacim inštitútom pre IEC 62443)	U3	
SE-C1-16	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov ? (Preukázateľné školenia a preskúšanie)	U2	Áno
SE-C1-17	Je prevádzkový personál vyškolený v oblasti pravidiel týkajúcich sa prístupu k osobným údajom a ochrany osobných údajov ? (Plán školení a plán účasti zodpovedných pracovníkov na školeniach)	U1	Áno
SE-C1-18	Sú pravidelne vykonávané a zdokumentované nácviky krízových situácií ? (Preukázanie schopnosti zvládnuť krízovú situáciu, minimalizácia rizík a redukcia dĺžky výpadku poskytovanej služby)	U3	Áno
SE-C1-19	Je spôsob pridelovania práv a oprávnení pre nových zákazníkov vhodný a bezpečný ? (Ochrana ostatných zákazníkov pred možným ohrozením napr. počítačovou kriminalitou ...)	U2	Áno
SE-C1-20	Sú pravidelne vykonávané a zdokumentované nácviky krízových situácií ?	U1	Áno
SE-C1-21	Sú implementované bezpečnostné opatrenia zodpovedajúce aktuálnym požiadavkám na bezpečnosť webových aplikácií a aplikácií vzhľadom na zvolenú technológiu ?	U2	Áno

C2. Technická bezpečnosť

Popis hardvérových a softvérových komponentov, implementovaných pre zabezpečenie technickej bezpečnosti a dostupnosti prevádzkovanvej cloudovej služby.

Tabuľka č. 24: Technická bezpečnosť

ID	Technická bezpečnosť	Úroveň	Povinné
SE-C2-01	Zabezpečuje systém firewall infraštruktúru podľa aktuálnej úrovne technológií ? (Preukázanie zodpovedajúcej miery ochrany)	U1	Áno
SE-C2-02	Zabezpečuje systém firewall infraštruktúru podľa aktuálnej úrovne technológií ?	U1	Áno
SE-C2-03	Je systém chránený pred DOS a DDOS útokmi z prostredia internetu ? (Preukázanie zodpovedajúcej miery ochrany)	U2	Áno
SE-C2-04	Je prístup k poskytovanej službe zabezpečený prístupom cez virtuálnu privátnu sieť (VPN) alebo virtuálny privátny cloud (VPC) ? (Preukázanie miery oddelenia užívateľov pre mimoriadne citlivé oblasti, napr. uchovávanie zdravotných záznamov ...)	U2	Áno
SE-C2-05	Je implementovaná antivírusová ochrana (ochrana pred škodlivým kódom, malware ...) ? (Zodpovedajúca miera ochrany pred kybernetickými ohrozeniami)	U3	Áno
SE-C2-06	Je implementovaný tzv. load-balancing pre zvýšenie miery spoľahlivosti a škálovateľnosti ? (Preukázanie vhodnej technológie rozdeľovania záťaže vo všetkých redundantných službách)	U3	
SE-C2-07	Je systém pridelenia a správy hesiel automatizovaný ? (Nie je dovolený administrátorský vstup pre správu zákazníckych hesiel)	U1	Áno
SE-C2-08	Sú heslá zabezpečené pred neoprávneným prístupom ? (Ochrana hesiel pred rozšifrovaním a neoprávneným prístupom)	U1	Áno

C3. Technické opatrenia na ochranu osobných údajov

Popis hardvérových a softvérových prostriedkov, implementovaných v prostredí poskytovateľa cloudovej služby pre zabezpečenie zodpovedajúcej miery ochrany osobných údajov (súlada s GDPR), popis kryptovacích mechanizmov.

Tabuľka č. 25: Technické opatrenia na ochranu osobných údajov

ID	Technické opatrenia na ochranu osobných údajov	Úroveň	Povinné
SE-C3-01	Je komunikácia medzi užívateľom a poskytovanou službou plne kryptovaná ? (Komunikácia možná len na báze https)	U1	Áno
SE-C3-02	Sú používané kryptovacie technológie dostatočne bezpečné ? (Miera kryptovania zodpovedá aktuálnym štandardom)	U1	Áno
SE-C3-03	Sú všetky ukladané dáta kryptované na dátových nosičoch v dátových úložiskách ? (Uviesť mechanizmus kryptovania uchovávaných údajov)	U3	Áno
SE-C3-04	Sú zálohy uchovávaných údajov dostatočne zabezpečené pred neoprávneným prístupom ? (Archivované údaje musia byť súčasťou bezpečnostných mechanizmov)	U1	Áno
SE-C3-05	Je implementované tzv. end-to-end kryptovanie až do úrovne ukladania na dátové nosiče ? Je implementovaná ochrana pred neoprávneným prístupom administrátorov alebo tretích strán ? (Spravovanie kryptovacích kľúčov je na strane zákazníka. Poskytovateľ služby by nemal byť schopný dekryptovať uložené údaje)	U2	Áno
SE-C3-06	Je zabezpečené oddelenie osobných a transakčných údajov ? (Zamedzenie možnej kombinácie osobných údajov s transakciou na základe jedného účtu v databáze)	U2	Áno
SE-C3-07	Je kombinovaný pohľad na osobné používateľské údaje a transakčné dáta prostredníctvom zadefinovania rolí ? Je to podporené technickým dizajnom ?	U3	Áno

	<i>(Zamedzenie moźnej kombinácie osobných údajov s transakciou na základe jedného účtu v databáze)</i>		
SE-C3-08	Existuje záznam o všetkých prihlasovacích aktivitách ? Môže tieto aktivity preveriť zákazník ? <i>(Transparentnosť pre zákazníka ohľadom všetkých prihlasovacích aktivít)</i>	U3	Áno
SE-C3-09	Je zákazník oprávnený priradovať role a prístupové práva pre všetky relevantné dátové objekty ? <i>(Zákazník môže určiť granularitu prístupových oprávnení)</i>	U3	

3.4 ŠPECIFICKÉ (SS)

Požiadavky na informácie ohľadom aspektov, špecifických pre jednotlivé platformy (IaaS, PaaS, SaaS). Popis úrovne zdokumentovania jednotlivých technológií, možností konfigurovania služieb, opis prevádzkových aspektov a licenčného vysporiadania, prehľad možností monitorovania a administrácie služieb, ozrejenie úrovni zabezpečenia, interoperabilita služieb a vzdelávanie klientov.

C1. Referenčná architektúra (IaaS)

Tabuľka č. 26: Referenčná architektúra

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C1-01	Je celá použitá cloudová technológia dôsledne zdokumentovaná ? <i>(Transparentý prehľad technických služieb, kľúčových služieb a servisnej podpory, pohľad z hľadiska funkcionality a technických parametrov)</i>	U2	Áno

C2. Systémový manažment (IaaS)

Tabuľka č. 27: Systémový manažment

ID	Platformovo špecifické aspekty	Úroveň	Povinné
----	--------------------------------	--------	---------

SS-C2-01	Je zákazník oprávnený sám si rezervovať a konfigurovať požadované služby ? Sú tieto procesy zdokumentované ? (<i>Režim samoobsluhy</i>)	U2	
SS-C2-02	Môže administrátor zákazníka monitorovať stav systému ? Je tento proces zdokumentovaný ? (<i>Riadenie a monitorovanie poskytovaných služieb zákazníkom</i>)	U2	

C3. Bezpečnosť (IaaS)

Tabuľka č. 28: Bezpečnosť

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C3-01	Je umožnená dvojfaktorová autentifikácia pre prístup k samoobslužným službám ? (<i>Bezpečný administrátorský prístup</i>)	U1	Áno Podľa: C1F05 , C1F06, C1OR04 až C1OR06
SS-C3-02	Môže zákazník použiť pre administrátorský prístup ním vyhradené priame pripojenie ? (<i>Sieťový prístup k administrátorskému rozhraniu môže byť redukovaný na zákazníkom určené priame pripojenie</i>)	U3	
SS-C3-03	Existujú užívateľské smernice na zaistenie bezpečnosti virtuálnych strojov ? (<i>Príručky na zamedzenie zraniteľnosti užívateľom spravovaných systémov</i>)	U1	Áno Podľa: C1OR04 až C1OR06
SS-C3-04	Sú operačné systémy automaticky chránené pred známymi zraniteľnosťami ? (<i>Zamedzenie bezpečnostných hrozieb, ktorými sú ohrozené staršie verzie operačných systémov</i>)	U2	
SS-C3-05	Sú operačné systémy vo virtuálnom prostredí bezpečnostne ošetrené ? (<i>Všetky poskytované operačné systémy sú ošetrené podľa špecifických odporúčaní ich výrobcov</i>)	U3	

C4. Manažment licencií (IaaS)

Tabuľka č. 29: Manažment licencií (IaaS)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C4-01	Sú všetky poskytované operačné systémy licenčne vysporiadané ? <i>(Preukázanie platných licencií na všetky poskytované a ponúkané operačné systémy)</i>	U1	Áno Podľa: C1OR03

C5. Referenčná architektúra (Paas)

Tabuľka č. 30: Referenčná architektúra (Paas)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C5-01	Je celá použitá cloudová technológia dôsledne zdokumentovaná ? <i>(Transparentý prehľad technických služieb, kľúčových služieb a servisnej podpory, pohľad z hľadiska funkcionality a technických parametrov)</i>	U1	Áno Podľa: C1OR04, C1OR06

C6. Bezpečnosť (Paas)

Tabuľka č. 31: Bezpečnosť (Paas)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C6-01	Sú ponúkané aplikácie patrične izolované od ostatných aplikácií ? Je táto izolovanosť potvrdená príslušným testovaním ? <i>(Žiadny vplyv inej zákazníkovej aplikácie v aplikačnom prostredí PaaS)</i>	U1	Áno

SS-C6-02	Sú bezpečnostné opatrenia primerané ponúkanej PaaS technológii ? Je zaručená primeraná webová a aplikačná bezpečnosť ? (Základná bezpečnosť)	U1	Áno
----------	--	----	-----

C7. Správa (Paas)

Tabuľka č. 32: Správa (Paas)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C7-01	Je proces nasadzovania jednotlivých PaaS komponentov do prevádzky primeraný príslušným procesom (vývoj, testovanie) ? (Striktné oddelenie prevádzky od vývojového a testovacieho prostredia, dodržiavanie procesov riadenia kvality pri nasadzovaní do prevádzkového prostredia)	U2	

C8. Interoperabilita (SaaS)

Tabuľka č. 33: Interoperabilita (SaaS)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C8-01	Existuje zodpovedajúca dokumentácia ohľadom exportných formátov ? (Prenositelnosť užívateľských dát)	U1	Áno
SS-C8-02	Je zaručené, že vo exporte je zachovaná celá referenčná integrita, vrátane prístupových oprávnení ? (Prenositelnosť užívateľských dát bez straty transakčných informácií a metadát)	U1	
SS-C8-03	Ktoré exportné formáty sú k dispozícii ? (Primerané štandardné formáty exportu dát)	U2	
SS-C8-04	Sú rozhrania použiteľné vo viacerých verziách ? (Umožniť zákazníkovi naplánovať školenia a migračné procedúry pred tým, ako budú aplikované významné zmeny v rozhraniach)	U3	
SS-C8-05	Sú všetky metadáta k dispozícii ako dátové objekty ? (Úplná auditovateľnosť exportovaných dát)	U2	

SS-C8-06	Je možná migrácia dát nezávislá od príslušného výrobcu aplikácie / softvéru ? (Prenositel'nosť)	U2	
SS-C8-07	Sú k dispozícii aplikačné programové rozhrania (API) na integráciu ponúkaného riešenia do iných služieb ? (Interoperabilita)	U3	
SS-C8-08	Existuje súbor softvérových vývojových nástrojov (SDK) / vývojová platforma pre integráciu aplikačných programových rozhraní (API) ? (Interoperabilita)	U3	

C9. Podpora užívateľov (SaaS)

Tabuľka č. 34: Podpora užívateľov (SaaS)

ID	Platformovo špecifické aspekty	Úroveň	Povinné
SS-C9-01	Existuje užívateľská dokumentácia ? (Užívateľské príručky)	U1	
SS-C9-02	Existuje plán školení ? (Školenia pre užívateľov)	U2	