316

VYHLÁŠKA
ze dne 24. srpna 2021
o některých požadavcích pro zápis do katalogu cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb., (dále jen „zákon“):

§ 1
Předmět úpravy

Tato vyhláška stanoví

a) požadavky na způsobilost poskytovatele cloud computingu (dále jen „poskytovatel“) zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona,
b) požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n písm. b) zákona,
c) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2 zákona,
d) požadavky na strukturu a náležitosti zprávy o provedení penetračního testu podle § 6t odst. 6 písm. d) a § 6t odst. 7 písm. e) zákona a intervaly pro její předkládání,
e) požadavky na náležitosti auditní zprávy osvědčující existenci plánu zajištění kontinuity provozu nabízeného cloud computingu a plánu na obnovu poskytování nabízeného cloud computingu po havárii podle § 6t odst. 6 písm. e) a § 6t odst. 7 písm. f) zákona,
f) požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik podle § 6t odst. 6 písm. f) a § 6t odst. 7 písm. g) zákona a
g) požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2
Základní pojmy

Pro účely této vyhlášky se rozumí

a) zákazníkem orgán veřejné správy využívající službu cloud computingu,

b) uživatelem ten, kdo službu cloud computingu prostřednictvím systému orgánu veřejné správy využívá nebo ji nastavuje,

c) zákaznickými daty všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu,

d) zákaznickým obsahem textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskytováním služby cloud computingu,

f) specifickými provozními údaji takové provozní údaje, které obsahují informace o identifikovaném nebo identifikovatelném uživateli,

g) zpracováním jakákoliv operace nebo soubor operací se zákaznickými daty a provozními údaji v elektronické podobě, prováděné pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení,

h) bezpečnostní úrovní nabízeného cloud computingu je taková bezpečnostní úroveň, do které nabízený cloud computing řadí poskytovatel.

§ 3

Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy

Poskytovatelem způsobilým zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona je ten, který splňuje požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy uvedené v příloze č. 1 k této vyhlášce odpovídající bezpečnostní úrovni nabízeného cloud computingu, v jaké žádá poskytovatel zapsat službu cloud computingu do katalogu cloud computingu, a třídě cloud computingu[1]), do které se služba cloud computingu řadí.

§ 4

Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem

Cloud computingem, který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6n zákona, je cloud computing splňující požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem uvedené v příloze č. 2 k této vyhlášce odpovídající bezpečnostní úrovni nabízeného cloud computingu, v jaké žádá poskytovatel zapsat službu cloud computingu do katalogu cloud computingu, a třídě cloud computingu, do které se služba cloud computingu řadí.

§ 5

Seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací, doklady o jejich splnění a intervaly pro předkládání těchto dokladů

Seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2 zákona jsou stanoveny v příloze č. 3 k této vyhlášce.

§ 6

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu a intervaly pro její předkládání

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu podle § 6t odst. 6 písm. d) a § 6t odst. 7 písm. e) zákona a intervaly pro její předkládání jsou stanoveny v příloze č. 4 k této vyhlášce.

§ 7

Požadavky na náležitosti auditní zprávy osvědčující existenci plánu zajištění kontinuity provozu nabízeného cloud computingu a plánu na obnovu poskytování nabízeného cloud computingu po havárii

(1) Auditní zprávou osvědčující existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii se rozumí auditní zpráva vyhotovená subjektem nezávislým na poskytovateli, která potvrzuje existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii a dokládá ověření jeho aplikace.

(2) Má se za to, že znaky auditní zprávy podle odstavce 1 naplňuje auditní zpráva vydaná pro účel certifikace ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301, ISO 22301, SOC 2® Type 2 nebo atestace podle CSA STAR Level 2. V rozsahu dané auditní zprávy musí být zahrnuta nabízená služba cloud computingu.

§ 8

Požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik

Požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik podle § 6t odst. 6 písm. f) a § 6t odst. 7 písm. g) zákona jsou stanoveny v příloze č. 5 k této vyhlášce.

§ 9

Požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací

(1) Struktura podkladů k ověření splnění požadavků podle § 3 a 4 musí být přehledná a srozumitelná. Za účelem dosažení přehlednosti a srozumitelnosti poskytovatel popíše a doloží pro každou jednotlivou službu cloud computingu, kterou žádá zapsat do katalogu cloud computingu, splnění požadavků podle § 4. V případě, že více služeb spadajících do stejné bezpečnostní úrovně nabízeného cloud computingu a stejné třídy cloud computingu splňuje požadavek podle § 4 stejně, je možné doložit splnění takového požadavku pouze jednou a jednoznačně uvést všechny služby cloud computingu, na které se toto doložení vztahuje.

(2) Podklady pro ověření splnění požadavků podle § 3 a 4 obsahují

a) identifikaci poskytovatele podle § 37 odst. 2 správního řádu,

b) popis splnění každého požadavku pro každou službu cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu, popřípadě popis skutečnosti, kterou poskytovatel dokládá splnění požadavku v přílohách č. 1 a 2 k této vyhlášce ve sloupci „Podklad, kterým poskytovatel doloží splnění požadavku“, a

c) podklady, kterými poskytovatel doloží splnění požadavku podle příloh č. 1 a 2 k této vyhlášce.

(3) Náležitosti podle odstavce 2 písm. a) a b) dokládá poskytovatel na elektronickém formuláři, který se zveřejňuje na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost.

(4) V případě, že je pro doložení splnění požadavků podle § 3 a 4 nezbytné odkázat do jiného dokumentu, který je k formuláři připojen, provede se tak ve formuláři uvedením kapitoly, strany, odstavce a případně i konkrétní věty.

(5) Formulář i veškeré přílohy se předkládají v elektronické podobě, ve strojově čitelném formátu zaručujícím neměnnost obsahu jednotlivých dokumentů.

(6) V případě, že je splnění některého z požadavků podle § 3 a 4 dokládáno čestným prohlášením, musí z něho být patrné, kdo a kdy jej činí a co se jím dokládá. V případě, že čestné prohlášení činí osoba odlišná od poskytovatele, je přílohou žádosti o zápis nabídky cloud computingu do katalogu cloud computingu i doklad o zmocnění opravňující tuto osobu k tomuto čestnému prohlášení.

§ 10

Přechodné ustanovení

Splnění požadavků uvedených v řádcích 7.8, 7.9 a 8.7 přílohy č. 2 k této vyhlášce se vyžaduje ode dne 1. ledna 2024.

§ 11

Účinnost

Tato vyhláška nabývá účinnosti dnem následujícím po dni jejího vyhlášení.

Ředitel:
Ing. Řehka v. r.

Příloha č. 1 k vyhlášce č. 316/2021 Sb.

Řádek	Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy	Podklad, kterým poskytovatel doloží splnění požadavku	Bezpečnostní úroveň nabízeného cloud computingu				Třída cloud computingu		
			Nízká	Střední	Vysoká	Kritická	cloud computing ve formě infrastruktury	cloud computing ve formě platformy	cloud computing ve formě aplikačního programového vybavení
1	Poskytovatel má sídlo nebo bydliště v členském státu Evropské unie nebo má určeného svého zástupce ve členském státu Evropské unie obdobně podle čl. 27 obecného nařízení o ochraně osobních údajů[2)].	Výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán; je-li poskytovatel evidován ve veřejném rejstříku podle zákona upravujícího veřejné rejstříky právnických a fyzických osob, žádný podklad se nevyžaduje.	X[3)]	X	X	X	X	X	X
2	Poskytovatel ani jeho ovládající osoby[4)] nebyli v posledních 5 letech pravomocně uznáni vinnými ze spáchání přestupku, za který jim byla uložena pokuta alespoň ve vý-	Informace z interních systémů Národního úřadu pro kybernetickou a informační bezpečnost. Žádný podklad se nevyžaduje.	X	X	X	X	X	X	X

	ši 1 000 000 Kč, spočívajícího v nezavedení nebo neprovedení bezpečnostního opatření podle zákona o kybernetické bezpečnosti. Poskytovatel ani jeho ovládající osoby[4)] nebyli v posledních 5 letech pravomocně uznáni vinnými ze spáchání přestupku, za který jim byla uložena pokuta alespoň ve výši 500 000 Kč, spočívajícího a) v nepředání dat, provozních údajů a informací podle § 6a odst. 2 zákona o kybernetické bezpečnosti, b) v nepředání dat, provozních údajů a informací podle § 6a odst. 3 zákona o kybernetické bezpečnosti, c) v nezničení kopií dat, provozních údajů a informací podle § 6a odst. 3 zákona o kybernetické bezpečnosti, d) v nedetekování kybernetických bezpečnostních událostí podle § 7 odst. 3 zákona o kybernetické bezpečnosti, e) v neohlášení kybernetického bezpečnostního incidentu podle § 8 odst. 1 až 4 zákona o kybernetické bezpečnosti, f) v nesplnění povinnosti uložené Národním úřadem pro kybernetickou a informační bezpečnost podle § 13 nebo 14 zákona o kybernetické bezpečnosti, g) v nesplnění povinnosti uložené Národním úřadem pro kybernetickou a informač-									

	ní bezpečnost v rozhodnutí podle § 15a odst. 1 zákona o kybernetické bezpečnosti, h) v nesplnění některé z povinnosti uložených nápravným opatřením podle § 24 zákona o kybernetické bezpečnosti, i) v nezavedení nebo neprovedení bezpečnostního opatření podle § 4 odst. 3 zákona o kybernetické bezpečnosti. Poskytovatel ani jeho ovládající osoby[4)] nebyli v posledních 5 letech pravomocně uznáni vinnými ze spáchání přestupku podle kontrolního řádu v souvislosti s kontrolou plnění povinností podle zákona o kybernetické bezpečnosti, za který jim byla uložena pokuta alespoň ve výši 150 000 Kč, spočívajícího v nesplnění některé z povinností podle § 10 odst. 2 nebo § 10 odst. 3 kontrolního řádu.								

Příloha č. 2 k vyhlášce č. 316/2021 Sb.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem	Podklad, kterým poskytovatel doloží splnění požadavku	Bezpečnostní úroveň nabízeného cloud computingu				Třída cloud computingu		
			Nízká	Střední	Vysoká	Kritická	cloud computing ve formě infrastruktury	cloud computing ve formě platformy	cloud computing ve formě aplikačního programového vybavení
1. Místo zpracování a uložení dat									
1.1	Poskytovatel uvádí informace o všech územích států, ve kterých jsou nebo mohou být uložena zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat, a dále uvádí informace o všech územích států mimo území členských států Evropské unie a členských států Evropského sdružení vol-	Písemný popis, ze kterého bude vyplývat, na území jakých států jsou nebo mohou být uložena zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat a na území jakých států mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu se předpokládá zpracování zákaznických dat a na území jakých států se předpokládá zpracování specifických provozních údajů.	X	X			X	X	X

	ného obchodu, ve kterých předpokládá zpracování zákaznických dat a specifických provozních údajů.	Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování zákaznických dat nebo specifických provozních údajů nejsou: - území států, z nichž se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele cloud computingu za účelem technické podpory služby cloud computingu, která se v čase mění a nemohou být specifikována předem; - území států, do nichž poskytovatel může předávat zákaznická data nebo specifické provozní údaje za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě cloud computingem, aktivované podle volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data nebo specifické provozní údaje, a je-li to možné, blíže specifikuje, jaká zákaznická data nebo jaké specifické provozní údaje zpravidla předává a na jakou předpokládanou dobu zákaznická data nebo specifické provozní údaje předává.							
1.2	Poskytovatel uvádí informace o všech územích států, ze kterých dochází k výkonu správy a dohledu nad službou cloud computingu.	Písemný popis, ze kterého bude vyplývat, z území jakých států dochází k výkonu správy a dohledu nad službou cloud computingu.	X	X	X	X	X	X	X

1.3	Zákaznická data ve stavu neaktivních dat jsou ukládána nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. V případě, že služba cloud computingu daný požadavek nesplňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba cloud computingu ukládá zákaznická data ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě. Poskytovatel uvádí místo uložení zákaznických dat ve stavu neaktivních dat. Na základě označení služby cloud computingu jako služby cloud computingu, která nesplňuje požadavek na uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, bude tato služba cloud computingu uvedena na internetových stránkách Národ-	Odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu nevztahuje na danou službu, jasné označení takové služby a zároveň odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat v pseudonymizované podobě, nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu neuplatní na danou službu a zároveň taková služba ukládá zákaznická data ve stavu neaktivních dat v nepseudonymizované podobě, jasné označení takové služby. Poskytovatel dále doloží odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpeč-			X		X	X	X

	ního úřadu pro kybernetickou a informační bezpečnost a daný požadavek se na ni neuplatní. Taková služba cloud computingu bude rovněž označena v katalogu cloud computingu jako služba cloud computingu zapsaná na základě uvedené výjimky citací uvedené výjimky.	nosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou zákaznická data uložena ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uložena v pseudonymizované podobě.							
1.4	Specifické provozní údaje jsou ve stavu neaktivních dat ukládány nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. V případě, že služba cloud computingu daný požadavek nesplňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba cloud computingu ukládá specifické provozní údaje ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě. Poskytovatel uvádí místo uložení specifických provozních údajů ve stavu neaktivních dat.	Odkaz na část smluvních podmínek, kde je vymezen závazek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, nebo v případě, že se požadavek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu nevztahuje na danou službu, jasné označení takové služby a zároveň odkaz na část smluvních podmínek, kde je vymezen závazek uložení specifických provozních údajů ve stavu neaktivních dat v pseudonymizované podobě, nebo v případě, že se požadavek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného ob-			X		X	X	X

	Na základě označení služby cloud computingu jako služby cloud computingu, která nesplňuje požadavek na uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, bude tato služba cloud computingu uvedena na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost a daný požadavek se na ni neuplatní. Taková služba cloud computingu bude rovněž označena v katalogu cloud computingu jako služba cloud computingu zapsaná na základě uvedené výjimky citací uvedené výjimky.	chodu neuplatní na danou službu a zároveň taková služba ukládá specifické provozní údaje ve stavu neaktivních dat v nepseudonymizované podobě, jasné označení takové služby. Poskytovatel dále doloží odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou specifické provozní údaje uloženy ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uloženy v pseudonymizované podobě.							
1.5	Zákaznická data jsou zpracovávána na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.3 přílohy č. 2 k této vyhlášce, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být zákaznická data	1. Poskytovatel uvede u služby cloud computingu, a) která zpracovává zákaznická data pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu: - jasné označení takové služby cloud computingu a			X		X	X	X

	zpracovávána i na území jiných států, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací.	- deklaraci závazku zpracování zákaznických dat na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, b) která zpracovává zákaznický obsah pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu a která zpracovává nebo může zpracovávat zákaznická data bez zákaznického obsahu mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu: - jasné označení takové služby cloud computingu, - údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat bez zákaznického obsahu, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat bez zákaznického obsahu na příslušném předpokládaném území státu, a údaj o tom, zda jsou nebo nejsou zákaznická data bez zákaznického obsahu pseudonymizována v případě tohoto zpracování. U zákaznických dat bez zákaznického obsahu zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů,							

c) která zpracovává nebo může zpracovávat zákaznická data mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu,

- jasné označení takové služby cloud computingu,

- údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování. U zákaznických dat zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů.

2. Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování zákaznických dat, nejsou:

- území států, z nichž se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele za účelem technické podpory služby cloud

		computingu, která se v čase mění a nemohou být specifikována předem; - území států, do nichž poskytovatel může předávat zákaznická data za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě službou cloud computingu, aktivované podle volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data, a je-li to možné, blíže specifikuje, jaká zákaznická data zpravidla předává a na jakou předpokládanou dobu zákaznická data předává.							
1.6	Specifické provozní údaje jsou zpracovávány na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.4 přílohy č. 2 k této vyhlášce, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být specifické provozní údaje zpracovávány i na území jiných států, pokud poskytovatel popíše, jak budou specifické provozní údaje chráněny před narušením bezpečnosti informací.	1. Poskytovatel uvede u služby cloud computingu, a) která zpracovává specifické provozní údaje pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu: - jasné označení takové služby cloud computingu a - deklaraci závazku zpracování specifických provozních údajů na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, b) která zpracovává nebo může zpracovávat specifické provozní údaje mimo území členských států			X		X	X	X

Evropské unie a členských států Evropského sdružení volného obchodu:

- jasné označení takové služby cloud computingu,

- údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování specifických provozních údajů, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování specifických provozních údajů na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou specifické provozní údaje pseudonymizovány v případě tohoto zpracování. U specifických provozních údajů zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněny alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů.

2. Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování specifických provozních údajů, nejsou:

- území států, z nichž se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele cloud computingu za účelem technické podpory služby cloud computingu, která se v čase mění a nemohou být specifikována předem;

		- území států, do nichž poskytovatel může předávat specifické provozní údaje za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě cloud computingem, aktivované podle volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat specifické provozní údaje, a je-li to možné, blíže specifikuje, jaké specifické provozní údaje zpravidla předává a na jakou předpokládanou dobu specifické provozní údaje předává.							
1.7	Poskytovatel vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, který je vyjádřen v samostatném dokumentu, který obsahuje údaj o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat. Poskytovatel informuje zákazníka o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a o tom, zda jsou nebo	Dokument oddělený od podmínek poskytování služby či smlouvy, nebo odkaz na zřetelně uvedený text smluvní dokumentace, jimiž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, které obsahují údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, nebo odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smluvní dokumentace nebo produktovou specifikaci, ze které bude patrné, že poskytovatel v základním nastavení služby vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat mimo území člen-			X		X	X	X

	nejsou zákaznická data pseudonymizována v případě tohoto zpracování. Alternativně k vyžadování souhlasu a informování zákazníka poskytovatel v základním nastavení služby cloud computingu vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat v každém jednotlivém případě zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu.	ských států Evropské unie a členských států Evropského sdružení volného obchodu.							
1.8	Zákaznická data a specifické provozní údaje jsou zpracovávány na území České republiky. Aniž je dotčen požadavek uvedený na řádku 6.6 přílohy č. 2 k této vyhlášce, mimo území České republiky mohou být zákaznická data a specifické provozní údaje zpracovávány pouze v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací,	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které je závazek zpracovávat zákaznická data a specifické provozní údaje pouze na území České republiky, a dále odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou zákaznická data a specifické provozní údaje zpracovávány.				X	X	X	X

	a pouze s výslovným písemným svolením zákazníka, který je vyjádřen na samostatném dokumentu, který obsahuje údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování, nebo pouze pokud poskytovatel vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat a specifických provozních údajů mimo území České republiky.	U služby cloud computingu, která zpracovává nebo může zpracovávat zákaznická data a specifické provozní údaje mimo území České republiky, poskytovatel takovou službu jasně označí a uvede údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování. U služby cloud computingu, která zpracovává nebo může zpracovávat zákaznická data a specifické provozní údaje mimo území České republiky, poskytovatel doloží dokument oddělený od podmínek poskytování služby či smlouvy, nebo odkaz na zřetelně uvedený text smluvní dokumentace, jimiž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území České republiky, které obsahují údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo								

		nejsou zákaznická data pseudonymizována v případě tohoto zpracování, nebo odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smluvní dokumentace nebo produktovou specifikaci, ze které bude patrné, že poskytovatel vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat mimo území České republiky.							
2. Žádosti o zpřístupnění a předání dat									
2.1	Poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, pokud to právní řád, jemuž poskytovatel podléhá, poskytovateli nezakazuje.	Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část,	X	X			X	X	X

		ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje.							
2.2	Poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje. Pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé. Pokud nedosáhne zrušení povinnosti zákazu informování zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období	Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, nebo pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé, a pokud nedosáhne zrušení povinnosti zákazu informování zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem,			X	X	X	X	X

	mlčenlivosti nařízeného zákonem nebo soudem.	nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, nebo pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé, a pokud nedosáhne zrušení povinnosti zákazu informování zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po zrušení povinnosti mlčenlivosti stanovené zákonem nebo nařízené soudem							
2.3	Poskytovatel v případě, že obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů,	Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytova-	X	X			X	X	X

	přezkoumá zákonnost takové žádosti, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti. Poskytovatel se zavazuje, že předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti. O podkladech sloužících k posouzení poskytovatel provede záznam, který uchová alespoň 5 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.	tel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a poskytovatel předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je							

		přiměřený účelu žádosti, a poskytovatel předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti.							
2.4	Poskytovatel v případě, že obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, přezkoumá zákonnost takové žádosti, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních	Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů,			X		X	X	X

	předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů. O podkladech sloužících k posouzení poskytovatel provede záznam, který uchová alespoň 10 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.	nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů.							
2.5	Poskytovatel jasně a srozumitelně uvádí jeho povinnosti vyplývající z právních předpisů států odlišných od členských států Evropské unie,	Písemný popis povinností vyplývajících z právních předpisů států odlišných od členských států Evropské unie, v nichž poskytovatel předpokládá zpracování zákaznických dat dle řádků 1.1, 1.5 a 1.6 přílohy	X	X	X	X	X	X	X

	v nichž poskytovatel předpokládá zpracování zákaznických dat dle řádků 1.1, 1.5 a 1.6 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů.	č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Písemný popis musí být v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů.							
2.6	Poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydává a nezpřístupňuje.	Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní.				X	X	X	X

3. Oprávnění k provedení kontroly									
3.1	Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu vůči deklarovaným parametrům, umožňuje Ministerstvu vnitra nebo Národnímu úřadu pro kybernetickou a informační bezpečnost zdarma ve vztahu k dané službě cloud computingu provedení kontroly splnění požadavků podle § 6i odst. 2 a 3 zákona o informačních systémech veřejné správy a podle kontrolního řádu na všech místech a zařízeních, souvisejících s poskytováním služby cloud computingu, a zároveň poskytuje veškerou součinnost, kterou si tyto orgány vyžádají, vyjma zpřístupnění či předání zákaznických dat bez souhlasu dotčeného zákazníka.	Žádný podklad se nevyžaduje. Splnění tohoto požadavku ověří Ministerstvo vnitra nebo Národní úřad pro kybernetickou a informační bezpečnost z vlastní činnosti.	X	X	X	X	X	X	X
4. Úrovně dostupnosti služby									
4.1	Poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s nepřetržitou provozní dobou alespoň v uvedených úrovních vyhod-	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které bude poskytovatel garantovat zajištění dostupnosti alespoň v uvedených úrovních,	-	99,45 (%)	99,90 (%)	99,99 (%)	X	X	X

	nocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem.	nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s nepřetržitou provozní dobou alespoň v uvedených úrovních vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem.							
4.2	Poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s provozní dobou alespoň 10 hodin v pracovní dny v uvedené úrovni vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které bude poskytovatel garantovat zajištění dostupnosti alespoň v uvedených úrovních, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je scho-	96,16 (%)	-	-	-	X	X	X

		pen zajišťovat dostupnost služby cloud computingu s provozní dobou alespoň 10 hodin v pracovní dny v uvedené úrovni vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem.							
5. Připojení do výměnného uzlu internetu (IXP)									
5.1	Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.	Výpis z veřejně dostupné databáze subjektů připojených do výměnného uzlu internetu, nebo platná smlouva s poskytovatelem služby výměnného uzlu internetu, nebo čestné prohlášení poskytovatele, že má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.			X	X	X	X	X
6. Zajištění poskytování služby cloud computingu									
6.1	Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v řádcích 4.1 a 4.2 přílohy č. 2 k této vyhlášce.	Strategie zajištění kontinuity provozu a strategie na obnovu po havárii, nebo auditní zpráva vyhotovená subjektem nezávislým na poskytovateli, která potvrzuje existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování	X	X			X	X	X

		nabízené služby cloud computingu po havárii a dokládá ověření jeho aplikace, zejména auditní zpráva vydaná pro účel certifikace ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO 22301, SOC 2® Type2 nebo atestace podle CSA STAR Level 2 nebo platný certifikát ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO 22301 vydaný subjektem nezávislým na poskytovateli. V rozsahu dané certifikace nebo auditní zprávy musí být zahrnuta nabízená služba cloud computingu. V případě, že rozsah auditní zprávy nebo certifikace nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, doloží poskytovatel čestné prohlášení, které služby cloud computingu do rozsahu auditní zprávy nebo certifikace spadají.							
6.2	Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v řádcích 4.1 a 4.2 přílohy č. 2 k této vyhlášce.	Strategie zajištění kontinuity provozu a strategie na obnovu po havárii, nebo auditní zpráva vyhotovená subjektem nezávislým na poskytovateli, která potvrzuje existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii a dokládá ověření jeho aplikace, zejména auditní zpráva vydaná pro účel certifikace ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO			X	X	X	X	X

		22301, SOC 2® Type 2 nebo atestace podle CSA STAR Level 2. V rozsahu dané auditní zprávy musí být zahrnuta nabízená služba cloud computingu. V případě, že rozsah auditní zprávy nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, doloží poskytovatel čestné prohlášení, které služby cloud computingu do rozsahu auditní zprávy spadají.							
6.3	Poskytovatel umožnuje synchronní replikaci (zálohování) dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné umožnění synchronní replikace (zálohování) dat do záložního datového centra.			X	X		X	X
6.4	Poskytovatel zajišťuje, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, jsou v dostatečné vzdálenosti od přírodních	Odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů	X	X	X	X	X	X	X

	zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo je přijato adekvátní bezpečnostní opatření, nebo se primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km a u obou datových center je navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.	a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo z auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné zajištění alespoň jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a pro doložení dostatečné vzdálenosti nebo přijetí adekvátního bezpečnostního opatření zpráva nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, které obsahuje náležitosti uvedené v příloze č. 5 k této vyhlášce, nebo pro doložení vzájemné vzdálenosti nejméně 50 km a návrhu a aplikace fyzické ochrany proti přírodním katastrofám, úmyslnému útoku nebo haváriím odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ze kterých je služba cloud computin-								

		gu poskytována a ze které bude patrné, že fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím je navržena a aplikována.							
6.5	Poskytovatel zajišťuje, že primární i záložní datové centrum, ve kterých jsou uložena zákaznická data ve stavu neaktivních dat, se nacházejí buď to všechna v České republice, nebo alespoň na území dvou různých členských států Evropské unie a Evropského sdružení volného obchodu. Tento požadavek se neuplatní na služby cloud computingu uplatňující výjimku z požadavků na řádku 1.4 přílohy č. 2 k této vyhlášce.	Odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých jsou uložena zákaznická data ve stavu neaktivních dat.			X		X	X	X
6.6	Poskytovatel zajišťuje, že primární i všechna záložní datová centra, ze kterých je poskytována služba cloud computingu, se nacházejí v České republice, vyjma případů výslovného písemného svolení zákazníka s ukládáním zákazníkem zašifrovaných zákaznických dat ve stavu neaktivních dat na území jiného členského státu Evropské unie a členského státu Evropského sdružení volného obchodu.	Odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých bude zákaznický obsah dlouhodobě uložen ve stavu neaktivních dat.				X	X	X	X

6.7	Poskytovatel je schopen poskytovat nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/ DDoS.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo na popis volitelné služby cloud computingu, ze které bude patrný nástroj nebo služba využívaná pro zvýšení odolnosti vůči útokům typu DoS/DDos, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je schopen poskytovat nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS, a ze které bude patrný nástroj nebo služba využívané pro zvýšení odolnosti vůči útokům typu DoS/DDos.	X	X	X	X	X	X	X
6.8	Poskytovatel umožňuje obsluhu služby cloud computingu pomocí management portálu nebo jiné formy administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo technickou dokumentaci, ze které bude patrné, že poskytovatel umožňuje obsluhu služby cloud computingu pomocí management portálu nebo jiné formy administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.			X	X	X	X	X
7. Nakládání s daty									

7.1	Poskytovatel umožňuje import či export dat v objemu větším než 2 TB prostřednictvím zaslání šifrovaných paměťových médií.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy, nebo produktovou specifikaci, ze které bude patrné, že poskytovatel umožňuje import či export dat v objemu větším než 2 TB prostřednictvím zaslání šifrovaných paměťových médií.			X	X	X	X	X
7.2	Poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu.	X	X	X	X	X	X	X
7.3	Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu a v úložištích ve službě cloud computingu pomocí některé-	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud compu-		X	X	X	X	X	X

	ho z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách.	tingu, ze které bude patrný způsob šifrování při přenosu a v úložištích ve službě cloud computingu.							
7.4	Poskytovatel umožňuje zákazníkovi využití vlastního šifrovacího klíče (BYOK).	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů, a to buď jejich vygenerováním v certifikovaném hardware security modulu (dále jen "HSM modulu") umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka.			X		X	X	X
7.5	Poskytovatel umožňuje uložení šifrovacích klíčů v certifikovaném HSM modulu úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria minimálně na EAL4 a vyšší, který je pod vzdálenou správou zákazníka nebo instalaci HSM modulu zákazníka do infrastruktury poskytovatele.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel umožňuje uložení klíčů v certifikovaném HSM modulu úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria minimálně na EAL4 a vyšší, který je pod správou zákazníka, nebo instalaci certifikovaného HSM modulu zákazníka do infrastruktury poskytovatele.				X	X	X	X

7.6	Poskytovatel umožňuje bezpečnou likvidaci kryptografických klíčů uložených v certifikovaném HSM modulu řízenou zákazníkem.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné umožnění bezpečné likvidace kryptografických klíčů uložených v certifikovaném HSM modulu řízené zákazníkem a závazek umožnit/zajistit při ukončení služby cloud computingu likvidaci vrchního přístupového klíče.				X	X	X	X
7.7	Poskytovatel umožňuje při ukončení služby cloud computingu bezpečnou likvidaci kryptografických klíčů, které šifrují zákaznický obsah v úložištích v souladu s vyhláškou o kybernetické bezpečnosti.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrný popis bezpečné likvidace dat v souladu s vyhláškou o kybernetické bezpečnosti.			X		X	X	X
7.8	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo bez přechozího svolení zákazníka v daném případě. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel vyhoto-	X	X	X	X	X	X	X

		vuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo bez přechozího svolení zákazníka v daném případě, a že tento záznam obsahuje důvod, čas, trvání, typ a rozsah přístupu.							
7.9	Poskytovatel umožňuje zákazníkovi přístup k záznamu vytvořenému dle řádku 7.8 přílohy č. 2 k této vyhlášce, a za tím účelem ho poskytovatel uchová alespoň po dobu 7 dní. Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s body 2.1, 2.2 přílohy č. 2 této vyhlášky.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel umožnuje zákazníkovi přístup k záznamu vytvořenému dle řádku 7.8 přílohy č. 2 k této vyhlášce, a že takový záznam uchová alespoň po dobu 7 dní.	X	X	X	X	X	X	X
8. Certifikace služby cloud computingu									
8.1	Poskytovatel provozuje službu cloud computingu v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o ky-	Čestné prohlášení, že systém řízení bezpečnosti informací, v jehož rozsahu je služba cloud computingu provozována, je v souladu s požadavky vyhlášky o kybernetické bezpečnosti nebo s požadavky ČSN	X				X	X	X

	bernetické bezpečnosti nebo s požadavky ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.	EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 a prohlášení o aplikovatelnosti jednotlivých opatření.							
8.2	Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu.	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.		X			X	X	X
8.3	Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud			X	X	X	X	X

	Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu.	computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.							
8.4	Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017.	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.		X			X	X	X

8.5	Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN EN ISO/IEC 27017 nebo EN ISO/IEC 27017.	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.			X	X	X	X	X
8.6	Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s po-			X	X	X	X	X

	náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018.	stupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.							
8.7	Poskytovatel je držitelem auditní zprávy SOC 2® Type 2 nebo auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue C5 vydaný BSI, a to ve formě Type 2, která není starší než 24 měsíců, do jejíhož rozsahu náleží posuzovaná služba cloud computingu, vydaná nezávislým auditorem.	Auditní zpráva SOC 2® Type 2 v doménách bezpečnosti, dostupnosti, procesní integrity, důvěrnosti a soukromí nebo auditní zpráva o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5) vydaný BSI, a to ve formě Type 2.			X	X	X	X	X
9. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty									
9.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel má zaveden nástroj na sle-	X				X	X	X

		dování a vyhodnocování kybernetických bezpečnostních událostí, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.							
9.2	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi. Nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze kterých bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí a umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu, nejpozději však do 24 hodin po vzniku události, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systé-		X	X	X	X	X	X

		mů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí, umožní zpřístupnění vzdáleně všech událostí tykajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin.							
9.3	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.	Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl	X	X	X	X	X	X	X
10. Testování služby cloud computingu									
10.1	Poskytovatel provádí pravidelně skeny zranitelností. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu skenu zranitelností.	Tři záznamy o provedení skenů zranitelností provedených maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu,	X	X	X	X	X	X	X

		nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 3 skeny zranitelností maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.							
10.2	Poskytovatel zajišťuje provádění penetračních testů subjektem, který je nezávislý na poskytovateli. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu penetračního testu.	Zpráva z provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.			X	X	X	X	
10.3	Poskytovatel zajišťuje provádění penetračních testů subjektem, který je nezávislý na poskytovateli. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu penetračního testu.	Zpráva z provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním			X	X			X

		žádosti o zápis služby cloud computingu do katalogu cloud computingu.							

Příloha č. 3 k vyhlášce č. 316/2021 Sb.

Seznam certifikací pro oblast ochrany důvěrnosti, integrity a dostupnosti informací	
• ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 • ČSN ISO/IEC 27017 nebo ISO/IEC 27017 • ČSN ISO/IEC 27018 nebo ISO/IEC 27018	
Doklady o splnění	
Pro řádek 8.2 přílohy č. 2 k této vyhlášce	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.3 přílohy č. 2 k této vyhlášce	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.4 přílohy č. 2 k této vyhlášce	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá

	poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.5 přílohy č. 2 k této vyhlášce	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.6 přílohy č. 2 k této vyhlášce	Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.7 přílohy č. 2 k této vyhlášce	Auditní zprávu SOC 2® Type 2 v doménách bezpečnosti, dostupnosti, procesní integrity, důvěrnosti a soukromí nebo auditní zprávu o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5) vydaný BSI, a to ve formě Type 2, přičemž tyto auditní zprávy nesmí být starší než 24 měsíců k datu podání žádosti o zápis do katalogu cloud computingu.
Poskytovatel dodá každých 15 měsíců evidence služby cloud computingu v katalogu cloud computingu vedeném Ministerstvem vnitra	
Pro řádek 8.2 přílohy č. 2 k této vyhlášce	Doklad platnosti certifikátu nebo platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, ne starší než 3 měsíce v době jeho dodání, kdy

	rozsah certifikace jmenovitě zahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.3 přílohy č. 2 k této vyhlášce	Doklad platnosti certifikátu nebo platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, ne starší než 3 měsíce v době jeho dodání, kdy rozsah certifikace jmenovitě zahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.4 přílohy č. 2 k této vyhlášce	Doklad platnosti certifikátu nebo platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, ne starší než 3 měsíce v době jeho dodání, kdy rozsah certifikace jmenovitě zahrnuje v katalogu cloud computingu zapsanou službu cloud computingu provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 8.5 přílohy č. 2 k této vyhlášce	Doklad platnosti certifikátu nebo platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, ne starší než 3 měsíce v době jeho dodání, kdy rozsah certifikace jmenovitě zahrnuje v katalogu cloud computingu zapsanou službu cloud computingu provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.

Pro řádek 8.6 přílohy č. 2 k této vyhlášce	Doklad platnosti certifikátu nebo platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, ne starší než 3 měsíce v době jeho dodání, kdy rozsah certifikace jmenovitě zahrnuje v katalogu cloud computingu zapsanou službu cloud computingu provozovanou v souladu s postupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje v katalogu cloud computingu zapsanou službu cloud computingu, čestné prohlášení o tom, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.
V případě, že některou ze skutečností dokládá poskytovatel předložením auditní zprávy SOC 2® Type 2, nesmí být tato auditní zpráva starší než 24 měsíců k datu podání žádosti o zápis do katalogu cloud computingu nebo k datu dokládané skutečnosti.	
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu vedeném Ministerstvem vnitra	
Pro řádek 8.7 přílohy č. 2 k této vyhlášce	Auditní zprávu SOC 2® Type 2 v doménách bezpečnosti, dostupnosti, procesní integrity, důvěrnosti a soukromí nebo auditní zprávu o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5) vydaný BSI, a to ve formě Type 2, přičemž tyto auditní zprávy nesmí být starší než 24 měsíců.

Příloha č. 4 k vyhlášce č. 316/2021 Sb.

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu	
Pro řádek 10.1 přílohy č. 2 k této vyhlášce	Tři záznamy o provedení skenu zranitelností provedených maximálně 3 měsíce před podáním žádosti o zápis do katalogu cloud computingu nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 3 skeny zranitelností maximálně 3 měsíce před podáním žádosti o zápis do katalogu cloud computingu.
Pro řádek 10.2 přílohy č. 2 k této vyhlášce	Zprávu o provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM, provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis do katalogu cloud computingu.
Pro řádek 10.3 přílohy č. 2 k této vyhlášce	Zpráva o provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis do katalogu cloud computingu.
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu Ministerstvu vnitra	
Pro řádek 10.1 přílohy č. 2 k této vyhlášce	Čtyři záznamy o provedení skenu zranitelností provedených každých 6 měsíců evidence v katalogu cloud computingu nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou

	prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 4 skeny zranitelností každých 6 měsíců evidence v katalogu cloud computingu.
Pro řádek 10.2 přílohy č. 2 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM, provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 23 měsíců od zápisu do katalogu cloud computingu nebo dodání předchozí zprávy o provedení penetračního testu.
Pro řádek 10.3 přílohy č. 2 k této vyhlášce	Zprávu o provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks provedeného subjektem, který je nezávislý na poskytovateli. Zpráva o provedení penetračního testu nesmí být starší než 23 měsíců od zápisu do katalogu cloud computingu nebo dodání předchozí zprávy o provedení penetračního testu.

Příloha č. 5 k vyhlášce č. 316/2021 Sb.

Pro řádek 6.4 přílohy č. 2 k této vyhlášce	**Zpráva nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka musí obsahovat přehledně a srozumitelně:**
	• označení subjektu poskytovatele cloud computingu,
	• označení posuzovaných lokalit primárního/záložního datového centra,
	• označení zpracovatele zprávy,
	• datum zpracování zprávy.
	1. Situační, dispoziční a konstrukční řešení objektu primárního/záložního datového centra – stručný popis stavby z hlediska dispozičního uspořádání a umístění stavby ve vztahu k okolní zástavbě a geolokaci, případně popis technologie provozu.
	2. Analýzu ohrožení každého primárního/záložního datového centra, ze kterého je poskytována služba cloud computingu, zahrnující:
	a) identifikaci zdrojů rizik,
	b) pravděpodobnost aktivace zdroje rizik,
	c) míru dopadu,
	d) popis možné škody,
	e) označení rizika v matici rizik,

f) vyjádření významnosti rizika,
g) aplikovaná protiopatření.
3. Přílohou zprávy budou zvolené škály pravděpodobnosti aktivace zdroje rizik a míry dopadu, kritéria pro hodnocení významnosti rizik a zpracovaná matice rizik, která kombinuje pravděpodobnost aktivace zdroje rizik a míru dopadu a ukazuje jaká rizika z toho vyplývají s jakou mírou přijatelnosti.
Zpráva zohlední zejména tyto zdroje rizik:
• požár,
• vydatné srážky,
• povodeň,
• tsunami,
• krupobití,
• extrémně vysoké teploty,
• dlouhodobé sucho
• extrémní vítr,
• tornádo,

• extrémně nízké teploty,
• sněhová kalamita,
• sněhová lavina,
• náledí a ledovka,
• geomagnetické anomálie,
• zemětřesení,
• propad zemských dutin,
• svahová nestabilita,
• sopečná erupce,
• závažná nehoda – pád letadla,
• epidemie – hromadné nákazy osob,
• závažné narušení bezpečnosti komunikační sítě a ztráta integrity komunikační sítě,
• narušení dodávek elektrické energie velkého rozsahu,
• radiační havárie.

[1]) § 2 písm. a) vyhlášky č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.

[2]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[3]) Symbol „X“ označuje existenci povinnosti splnit požadavky v uvedené bezpečnostní úrovni nabízeného cloud computingu a třídě cloud computingu.

[4]) § 74 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.