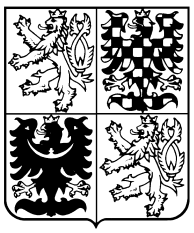

Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 5. prosince 2025

Vyhláška č. 505/2025 Sb.

Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu

505

VYHLÁŠKA

ze dne 28. listopadu 2025

o některých požadavcích pro zápis do katalogu cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 písm. a) až f) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb. a zákona č. 265/2025 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 § 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 orgánu veřejné správy nabízeným cloud computingem podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2

Vymezení pojmů

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, obrazová, audiovizuální nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) specifickými provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskytováním služby cloud computingu, která obsahují informace o identifikovaném nebo identifikovatelném uživateli,

f) 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 nebo zkombinování, omezení, výmaz nebo zničení, a

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

§ 3

Požadavky na způsobilost poskytovatele 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 poskytovatel za následujících podmínek:

a) má sídlo nebo bydliště v členském státě Evropské unie nebo má určeného svého zástupce v členském státě Evropské unie obdobně podle čl. 27 obecného nařízení o ochraně osobních údajů[1]),

b) poskytovatel ani jeho ovládající osoby[2]) nebyli v posledních 5 letech pravomocně uznáni vinnými ze spáchání přestupku spočívajícího v nesplnění některé z povinností uložené nápravným opatřením podle § 56 odst. 1 zákona o kybernetické bezpečnosti[3]) a

c) poskytovatel ani jeho ovládající osoby nebyli v posledních 5 letech více než jednou pravomocně uznáni vinnými ze spáchání přestupku spočívajícího v

   1. nesplnění povinnosti ohlásit službu podle § 6 odst. 1 zákona o kybernetické bezpečnosti,

   2. nesplnění povinnosti ohlásit změnu regulované služby podle § 9 odst. 1 zákona o kybernetické bezpečnosti,

   3. nesplnění povinnosti určit za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) zákona o kybernetické bezpečnosti nebo podpůrná aktiva podle § 12 odst. 2 písm. c) zákona o kybernetické bezpečnosti nebo v nesplnění povinnosti jejich určení pravidelně přezkoumávat nebo aktualizovat podle § 12 odst. 5 zákona o kybernetické bezpečnosti,

4. nesplnění povinnosti posoudit za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) zákona o kybernetické bezpečnosti souvisí s poskytováním regulované služby, nebo v nesplnění povinnosti toto posouzení pravidelně přezkoumávat nebo aktualizovat podle § 12 odst. 5 zákona o kybernetické bezpečnosti,
5. nesplnění povinnosti evidovat aktiva podle § 12 odst. 3 zákona o kybernetické bezpečnosti,
6. nesplnění povinnosti zavádět nebo provádět bezpečnostní opatření podle § 13 odst. 2 nebo § 18 odst. 1 zákona o kybernetické bezpečnosti,
7. nesplnění povinnosti vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo v nesplnění povinnosti zahrnovat požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5 zákona o kybernetické bezpečnosti,
8. nesplnění povinnosti předložit prvotní hlášení o incidentu podle § 16 odst. 1 zákona o kybernetické bezpečnosti nebo v nesplnění povinnosti doplnit některý z údajů o incidentu podle § 16 odst. 3 zákona o kybernetické bezpečnosti nebo v nesplnění povinnosti nahlásit kybernetický bezpečnostní incident podle § 18 odst. 2 zákona o kybernetické bezpečnosti,
9. nesplnění povinnosti poskytnout informace nebo součinnost při zvládání incidentu podle § 17 odst. 3 zákona o kybernetické bezpečnosti,
10. nesplnění rozhodnutím stanovené povinnosti nebo zákazu informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem podle § 19 odst. 1 zákona o kybernetické bezpečnosti,
11. nesplnění povinnosti informovat uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni, podle § 19 odst. 2 zákona o kybernetické bezpečnosti,
12. nesplnění povinnosti uložené rozhodnutím o výstraze podle § 21 odst. 1 zákona o kybernetické bezpečnosti,
13. nesplnění reaktivního protiopatření uloženého podle § 23 odst. 1 nebo § 23 odst. 4 zákona o kybernetické bezpečnosti,
14. nesplnění povinnosti uložené rozhodnutím podle § 24 odst. 1 zákona o kybernetické bezpečnosti,
15. nesplnění povinnosti ohlásit změnu regulované služby podle § 26 odst. 1 zákona o kybernetické bezpečnosti,
16. porušení podmínky nebo zákazu uložených v opatření obecné povahy podle § 29 zákona o kybernetické bezpečnosti,
17. nesplnění povinnosti zajišťovat dostupnost strategicky významné služby z území České republiky ve stanoveném čase nebo kvalitě podle § 33 odst. 1 zákona o kybernetické bezpečnosti,
18. nesplnění povinnosti prověřovat zajištění poskytování strategicky významné služby podle § 33 odst. 2 zákona o kybernetické bezpečnosti nebo nesplnění povinnosti o tomto prověření vyhotovit záznam,

19. nesplnění povinnosti provést v souvislosti se stavem kybernetického nebezpečí opatření k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru uložené rozhodnutím nebo opatřením obecné povahy podle § 39 zákona o kybernetické bezpečnosti,
20. nesplnění některé z povinností podle § 10 odst. 2 kontrolního řádu[4]) jako kontrolovaná osoba v souvislosti s kontrolou plnění povinností podle zákona o kybernetické bezpečnosti, nebo
21. nesplnění povinnosti podle § 10 odst. 3 kontrolního řádu[4]) jako povinná osoba v souvislosti s kontrolou plnění povinností podle zákona o kybernetické bezpečnosti.

§ 4

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

Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6n písm. b) zákona jsou stanoveny v přílohách č. 1 až 4 k této vyhlášce.

§ 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 § 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. 5 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 podle § 6y odst. 2 zákona jsou stanoveny v příloze č. 6 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 zpráva osvědčující existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii musí být vyhotovena subjektem nezávislým na poskytovateli a musí prokazovat ověření aplikace plánů při jejich testování.

(2) Má se za to, že znaky auditní zprávy podle odstavce 1 naplňuje auditní zpráva vydaná pro účel certifikace podle ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301, ISO 22301 od certifikačního orgánu, který byl akreditován některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2 nebo atestace podle CSA STAR Level 2. V rozsahu dané auditní zprávy musí být jmenovitě zahrnuta zapisovaná služba cloud computingu. V případě, že rozsah této auditní zprávy jmenovitě nezahrnuje zapisovanou službu cloud computingu, předloží poskytovatel čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) o rozsahu této auditní zprávy.

§ 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. 7 k této vyhlášce.

§ 9

Požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem

(1) Podklady k ověření splnění požadavku podle § 4 obsahují

a) popis splnění požadavku pro službu cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu, kterým poskytovatel dokládá splnění požadavku v přílohách č. 1 až 4 k této vyhlášce, a

b) dokumenty, kterými poskytovatel doloží splnění požadavku podle příloh č. 1 až 4 k této vyhlášce.

(2) Náležitosti podle odstavce 1 písm. a) dokládá poskytovatel na elektronickém formuláři, který se zveřejňuje na internetových stránkách Digitální a informační agentury.

(3) Struktura podkladů k ověření splnění požadavků podle § 4 musí být přehledná a srozumitelná. Za tímto účelem poskytovatel popíše splnění každého z požadavků pro každou službu cloud computingu, kterou žádá zapsat do katalogu cloud computingu. V případě, že poskytovatel v rámci jedné nabídky cloud computingu žádá zapsat více služeb cloud computingu spadajících do stejné bezpečnostní úrovně a splňujících požadavek shodným způsobem, je možné doložit splnění každého z požadavků pouze jednou a následně jednoznačně uvést všechny služby cloud computingu, na které se toto doložení vztahuje. V případě, že poskytovatel žádá zapsat nabídku cloud computingu, pro kterou je možné doložit splnění požadavků shodným podkladem, kterým byly prokázány již zapsané nabídky téhož poskytovatele, může se poskytovatel na tento podklad odkázat. Na takový odkaz se uplatní požadavky odstavce 4.

(4) V případě, že je pro doložení splnění požadavku podle § 4 nezbytné odkázat do jiného dokumentu, který je k formuláři připojen, provede se tak ve formuláři uvedením názvu připojeného dokumentu a kapitoly, strany, odstavce a případně i konkrétní věty, ze které splnění požadavku pro službu cloud computingu vyplývá.

(5) Pro účely podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 4 se rozumí

a) písemným popisem popis uvedený ve formuláři žádosti podle odstavce 1 písm. a) nebo v samostatném podkladu, na který je v popisu splnění požadavku odkazováno,

b) čestným prohlášením podklad, kterým je čestně prohlášeno splnění daného požadavku či jeho aspektu, ze kterého je patrné, kdo a kdy jej činí, co jím dokládá, a podepsaný osobou oprávněnou jednat za poskytovatele; v případě, že čestné prohlášení činí osoba odlišná od poskytovatele, je zároveň s čestným prohlášením dokládán i doklad o zmocnění opravňujícím tuto osobu k tomuto čestnému prohlášení,

c) smluvní dokumentací návrh smlouvy, smluvních podmínek, podmínek poskytování služby či podobný podklad pro služby cloud computingu, které poskytovatel žádá zapsat do katalogu cloud computingu,

d) další dokumentací produktová specifikace, technická dokumentace nebo další jiný popis služby, který není smluvní dokumentací, a

e) auditní zprávou

1. auditní zpráva vydaná pro certifikaci podle 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),
2. auditní zpráva SOC 2® Type 2,
3. auditní zpráva o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5), a to ve formě Type 2, nebo
4. auditní zpráva o vyhodnocení shody s požadavky této vyhlášky.

(6) Auditní zpráva podle odstavce 5 písm. e) musí být vydána subjektem nezávislým na poskytovateli, nesmí být ke dni podání žádosti o zápis nabídky cloud computingu do katalogu cloud computingu starší než 24 měsíců a do jejího rozsahu musí jmenovitě spadat posuzovaná služba cloud computingu.

§ 10

Přechodná ustanovení

(1) Žádosti o zápis poskytovatele do katalogu cloud computingu podle § 6q zákona a žádosti o zápis nabídky cloud computingu do katalogu cloud computingu podle § 6t zákona podané přede dnem nabytí účinnosti této vyhlášky se posuzují podle vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, s výjimkou požadavků uvedených v řádcích 4.1, 4.2, 7.1 a 7.2 přílohy č. 2 k vyhlášce č. 316/2021 Sb.

(2) Splnění požadavků v řádcích 8.1 a 8.2 příloh č. 3 a 4 k této vyhlášce a požadavků na strukturu a náležitosti zprávy o provedení penetračního testu a intervaly pro její předkládání podle § 6 je možné doložit splněním požadavků stanovených vyhláškou č. 316/2021 Sb., po dobu 24 měsíců ode dne nabytí účinnosti této vyhlášky.

§ 11

Zrušovací ustanovení

Vyhláška č. 316/2021 Sb. se zrušuje.

§ 12

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2026.

Ředitel:
Ing. Kintr v. r.

Příloha č. 1

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni nízká	Podklad, kterým poskytovatel doloží splnění požadavku
1. Místo zpracování a uložení dat		
1.1	Poskytovatel uvádí informace o všech státech, z jejichž území dochází k výkonu správy a dohledu nad službou cloud computingu.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
1.2	Poskytovatel uvádí informace o všech státech, na jejichž území 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 státech mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, na jejichž území předpokládá zpracování zákaznických dat a specifických provozních údajů. Platí, že státy, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat nebo specifických provozních údajů, nejsou A) státy, z jejichž území 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 specifikovány předem, nebo B) státy, z jejichž území 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.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
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 nebo specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo, v případě, že této žádosti vyhoví, o takové žádosti zákazníka bezodkladně informuje, pokud to právní řád, jemuž poskytovatel podléhá, poskytovateli nezakazuje. Poskytovatel dále po obdržení takové žádosti přezkoumá její zákonnost, 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 nebo 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	Čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku, část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku,

	orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat nebo specifických provozních údajů je přiměřený účelu žádosti. O podkladech sloužících k přezkoumání zákonnosti žádosti poskytovatel provede záznam, který uchová alespoň 5 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.	část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
2.2	Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení rozhodnutí o odpovídající ochraně (adequacy decision) podle článku 45 obecného nařízení o ochraně osobních údajů[1)], na jejichž území se nalézá datové centrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádku 1.2 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento 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. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
3. Oprávnění k provedení kontroly		
3.1	Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu s jím deklarovanými parametry, umožňuje Digitální a informační agentuře 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 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 doklad se nevyžaduje. Splnění tohoto požadavku ověří Národní úřad pro kybernetickou a informační bezpečnost z úřední činnosti.

4. Zajištění poskytování služby cloud computingu		
4.1	Poskytovatel má vyhotoven a udržuje plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu.	Plán zajištění kontinuity provozu a plán na obnovu po havárii, nebo auditní zpráva podle § 7 odst. 1 této vyhlášky.
4.2	Poskytovatel vždy zajišťuje primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že A) tato datová centra jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo že je přijato adekvátní bezpečnostní opatření, nebo B) se tato datová 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.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, nebo část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále zprávu nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, který obsahuje náležitosti uvedené v příloze č. 7 k této vyhlášce, ze kterého vyplývá splnění požadavku podle A), nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku podle B).
4.3	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace, například popis volitelné služby cloud

		computingu, podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5. Nakládání s daty		
5.1	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez předchozího svolení zákazníka. 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. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává 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 bodem 2.1 této přílohy. Pokud poskytovatel nemá zaveden proces pro přístup jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, tento požadavek se neuplatní. Každý přístup k nezašifrovaným zákaznickým datům, ke kterému dojde bez předchozího svolení zákazníka, se pak považuje za narušení bezpečnosti informací dle řádku 7.2 této přílohy a poskytovatel postupuje v souladu s tímto požadavkem.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.2	Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu po sítích mimo kontrolu poskytovatele a v úložištích ve službě cloud computingu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

6. Certifikace služby cloud computingu		
6.1	Poskytovatel provozuje službu cloud computingu v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností[5] nebo s požadavky podle ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.	Čestné prohlášení podle § 9 odst. 5 písm. b) a prohlášení o aplikovatelnosti jednotlivých opatření.
7. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty		
7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.[6]	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
7.2	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat nebo specifických provozních údajů dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.

8. Testování služby cloud computingu		
8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.	Tři záznamy o provedení skenů zranitelností v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, ze kterých vyplývá splnění požadavku, přičemž tyto záznamy nejsou ke dni podání žádosti o zápis zapisované služby do katalogu cloud computingu starší více než 12 měsíců a zároveň alespoň jeden z těchto záznamů nebude ke dni podání žádosti o zápis služby do katalogu cloud computingu starší více než 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku. Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni střední	Podklad, kterým poskytovatel doloží splnění požadavku
1. Místo zpracování a uložení dat		
1.1	Poskytovatel uvádí informace o všech státech, z jejichž území dochází k výkonu správy a dohledu nad službou cloud computingu.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
1.2	Poskytovatel uvádí informace o všech státech, na jejichž území 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 státech mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, na jejichž území předpokládá zpracování zákaznických dat a specifických provozních údajů. Platí, že státy, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat nebo specifických provozních údajů, nejsou A) státy, z jejichž území 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 specifikovány předem, nebo B) státy, z jejichž území 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.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.

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 nebo specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo, v případě, že této žádosti vyhoví, o takové žádosti zákazníka bezodkladně informuje, pokud to právní řád, jemuž poskytovatel podléhá, poskytovateli nezakazuje. Poskytovatel dále po obdržení takové žádosti přezkoumá její zákonnost, 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 nebo 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 nebo specifických provozních údajů je přiměřený účelu žádosti. O podkladech sloužících k přezkoumání zákonnosti žádosti poskytovatel provede záznam, který uchová alespoň 5 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.	Čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku, část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
2.2	Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení rozhodnutí o odpovídající ochraně (adequacy decision) podle článku 45 obecného nařízení o ochraně osobních údajů[1)], na jejichž území se nalézá datacentrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádku 1.2 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento 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. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.

3. Oprávnění k provedení kontroly		
3.1	Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu s jím deklarovanými parametry, umožňuje Digitální a informační agentuře 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 doklad se nevyžaduje. Splnění tohoto požadavku ověří Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost z úřední činnosti.
4. Zajištění poskytování služby cloud computingu		
4.1	Poskytovatel má vyhotoven a udržuje plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu.	Plán zajištění kontinuity provozu a plán na obnovu po havárii, nebo auditní zpráva podle § 7 odst. 1 této vyhlášky.
4.2	Poskytovatel vždy zajišťuje primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že A) tato datová centra jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo že je přijato adekvátní bezpečnostní opatření, nebo B) se tato datová 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.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, nebo část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále zprávu nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, který obsahuje náležitosti uvedené v příloze č. 7 k této vyhlášce, ze kterého vyplývá splnění požadavku podle A), nebo

		část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku podle B).
4.3	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace, například popis volitelné služby cloud computingu, podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5. Nakládání s daty		
5.1	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. 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. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává 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 bodem 2.1 této přílohy. Pokud poskytovatel nemá zaveden proces pro přístup jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, tento požadavek se neuplatní. Každý přístup k nezašifrovaným zákaznickým datům, ke kterému dojde bez předchozího svolení zákazníka, se pak považuje za narušení bezpečnosti informací dle řádku 7.2 této přílohy a poskytovatel postupuje v souladu s tímto požadavkem.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

5.2	Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu po sítích mimo kontrolu poskytovatele a v úložištích ve službě cloud computingu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.3	Poskytovatel zákazníkovi umožňuje ochranu zákaznického obsahu šifrováním při přenosu po sítích mimo kontrolu poskytovatele a v úložištích ve službě cloud computingu pomocí některého ze schválených algoritmů uvedených v aktuálně platném doporučení v oblasti kryptografických prostředků vydaném v souladu s nejlepší praxí Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách, v rámci celé šifrovací sady. V případě, že poskytovatel nabízí šifrovací sady, které obsahují takové algoritmy, které nejsou schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, poskytovatel umožní zákazníkovi výběr těch šifrovacích sad, které aplikují algoritmy schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
6. Certifikace služby cloud computingu		
6.1	Poskytovatel je držitelem platné certifikace podle 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 náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017.	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu.
7. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty		
7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožňuje zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka. Nové události zpřístupní poskytovatel zákazníkovi bez zbytečného odkladu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

7.2	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat nebo specifických provozních údajů dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.
8. Testování služby cloud computingu		
8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.	Tři záznamy o provedení skenů zranitelností v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, ze kterých vyplývá splnění požadavku, přičemž tyto záznamy nejsou ke dni podání žádosti o zápis zapisované služby do katalogu cloud computingu starší více než 12 měsíců a zároveň alespoň jeden z těchto záznamů nebude ke dni podání žádosti o zápis služby do katalogu cloud computingu starší více než 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

		Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni vysoká	Podklad, kterým poskytovatel doloží splnění požadavku
1. Místo zpracování a uložení dat		
1.1	Poskytovatel uvádí informace o všech státech, z jejichž území dochází k výkonu správy a dohledu nad službou cloud computingu.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
1.2	Zákaznická data ve stavu neaktivních dat jsou ukládána nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Poskytovatel vždy uvádí úplný výčet datových center a jejich lokace po úroveň katastrálního území nebo obce, ve kterých jsou zákaznická data uložena ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uložena v pseudonymizované podobě, a dále A) v případě, že služba cloud computingu umožňuje splnění požadavku ukládat zákaznická data ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, takovou službu jasně označuje a deklaruje závazek ukládat zákaznická data ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, B) v případě, že služba cloud computingu neumožňuje splnění požadavku ukládat zákaznická data ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, takovou službu jasně označuje a zákaznická data ve stavu neaktivních dat jsou ukládána v pseudonymizované podobě, nebo C) v případě, že služba cloud computingu neumožňuje splnění požadavku ukládat zákaznická data ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu ani požadavku ukládat zákaznická data ve stavu neaktivních dat v pseudonymizované podobě, takovou službu jasně označuje.	Část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku podle A), B), nebo C).

	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 nebo 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.	
1.3	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. Poskytovatel vždy uvádí úplný výčet datových center a jejich lokace po úroveň katastrálního území nebo obce, ve kterých jsou specifické provozní údaje uloženy ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uložena v pseudonymizované podobě, a dále A) v případě, že služba cloud computingu umožňuje splnění požadavku ukládat specifické provozní údaje ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a deklaruje závazek ukládat specifické provozní údaje ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, B) v případě, že služba cloud computingu neumožňuje splnění požadavku ukládat specifické provozní údaje ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, takovou službu jasně označuje a specifické provozní údaje ve stavu neaktivních dat jsou ukládána v pseudonymizované podobě, nebo C) v případě, že služba cloud computingu neumožňuje splnění požadavku ukládat specifické provozní údaje ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu ani požadavku ukládat specifické provozní údaje ve stavu neaktivních dat v pseudonymizované podobě, takovou službu jasně označuje.	Část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku podle A), B), nebo C).

	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 nebo 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.	
1.4	Zákaznická data jsou zpracovávána pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.2 této přílohy, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být zákaznická data zpracovávána i na území jiných států, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací. Poskytovatel A) v případě, že služba cloud computingu umožňuje splnění požadavku na zpracovávání zákaznických dat pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a deklaruje závazek zpracování zákaznických dat na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, B) v případě, že služba cloud computingu neumožňuje splnění požadavku na zpracovávání zákaznických dat pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, ale umožňuje splnění požadavku na zpracovávání zákaznického obsahu pouze na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat bez zákaznického obsahu, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat bez zákaznického obsahu na příslušném předpokládaném území příslušných států, a dále 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 dále uvádí popis toho, jak budou chráněna ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů[1)], nebo	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku podle A), B), nebo C).

	C) v případě, že služba cloud computingu neumožňuje splnění požadavku na zpracovávání zákaznických dat pouze na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu ani požadavku na zpracovávání zákaznického obsahu pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování; u zákaznických dat zpracovávaných mimo území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu dále uvádí popis toho, jak budou chráněna alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů[1)]. Platí, že státy, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat, nejsou A) státy, z jejichž území 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, nebo B) státy, do jejichž území může poskytovatel 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.	
1.5	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 1.3 této přílohy, 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. Poskytovatel A) v případě, že služba cloud computingu umožňuje splnění požadavku na zpracovávání specifických provozních údajů pouze na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a deklaruje závazek zpracovávání specifických provozních údajů pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, nebo	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku podle A), nebo B).

	B) v případě, že služba cloud computingu neumožňuje splnění požadavku na zpracovávání specifických provozních údajů pouze na území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování specifických provozních údajů, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování specifických provozních údajů na příslušném předpokládaném území příslušných států, a dále 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 nebo členských států Evropského sdružení volného obchodu dále uvádí popis toho, jak budou chráněna alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů[1)]. Platí, že státy, na jejichž území dochází nebo může docházet ke zpracování specifických provozních údajů, nejsou A) státy, z jejichž území 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, nebo B) státy, do jejichž území může poskytovatel 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.	
1.6	Poskytovatel A) vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie nebo členských států Evropského sdružení volného obchodu, který je vyjádřen v samostatném dokumentu, který obsahuje údaj o státech, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat; poskytovatel informuje zákazníka o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na území příslušných států a o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování, nebo	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku podle A), nebo B).

	B) 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 nebo členských států Evropského sdružení volného obchodu.	
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 nebo specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo, v případě, že této žádosti vyhoví, o takové žádosti zákazníka bezodkladně informuje. Pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem. Poskytovatel v případě, že obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat nebo 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 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.	Čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku, část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
2.2	Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení rozhodnutí o odpovídající ochraně (adequacy decision) podle článku 45 obecného nařízení o ochraně osobních údajů[1)], na jejichž území se nalézá datové centrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádků 1.4 a 1.5 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento 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. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.

	prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.	
3. Oprávnění k provedení kontroly		
3.1	Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu s jím deklarovanými parametry, umožňuje Digitální a informační agentuře 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 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 doklad se nevyžaduje. Splnění tohoto požadavku ověří Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost z úřední činnosti.
4. Zajištění poskytování služby cloud computingu		
4.1	Poskytovatel má vyhotoven a udržuje plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu.	Plán zajištění kontinuity provozu a plán na obnovu po havárii, nebo auditní zpráva podle § 7 odst. 1 této vyhlášky.
4.2	Poskytovatel vždy zajišťuje primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že A) tato datová centra jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo že je přijato adekvátní bezpečnostní opatření, nebo	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, nebo část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze

	B) se tato datová 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.	které vyplývá splnění obecného požadavku, a dále zprávu nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, který obsahuje náležitosti uvedené v příloze č. 7 k této vyhlášce, ze kterého vyplývá splnění požadavku podle A), nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku podle B).
4.3	Poskytovatel umožnuje synchronní replikaci dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

4.4	Poskytovatel uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že primární i všechna záložní datová centra, ve kterých jsou uložena zákaznická data ve stavu neaktivních dat, se nacházejí buďto všechna v České republice, nebo alespoň na území dvou různých členských států Evropské unie nebo Evropského sdružení volného obchodu. Tento požadavek se neuplatní na služby cloud computingu uplatňující výjimku z požadavků na řádku 1.2 této přílohy.	Část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
4.5	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace, například popis volitelné služby cloud computingu, podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
4.6	Poskytovatel umožňuje obsluhu služby cloud computingu pomocí administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.

5. Nakládání s daty		
5.1	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. 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. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává 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 bodem 2.1 této přílohy. Pokud poskytovatel nemá zaveden proces pro přístup jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, tento požadavek se neuplatní. Každý přístup k nezašifrovaným zákaznickým datům, ke kterému dojde bez předchozího svolení zákazníka, se pak považuje za narušení bezpečnosti informací dle řádku 7.2 této přílohy a poskytovatel postupuje v souladu s tímto požadavkem.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.2	Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

5.3	Poskytovatel zákazníkovi umožňuje ochranu zákaznického obsahu šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu pomocí některého ze schválených algoritmů uvedených v aktuálně platném doporučení v oblasti kryptografických prostředků vydaném v souladu s nejlepší praxí Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách, v rámci celé šifrovací sady. V případě, že poskytovatel nabízí šifrovací sady, které obsahují takové algoritmy, které nejsou schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, poskytovatel umožní zákazníkovi výběr těch šifrovacích sad, které aplikují algoritmy schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.4	Poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů, a to buď jejich vygenerováním v certifikovaném hardware security modulu (HSM modulu) umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.
5.5	Poskytovatel umožňuje při ukončení služby cloud computingu bezpečnou likvidaci kryptografických klíčů, které šifrují zákaznický obsah v úložištích v souladu s přílohou č. 2 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.[7)]	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.

6. Certifikace služby cloud computingu		
6.1	Poskytovatel je držitelem platné certifikace podle 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 náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018.	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu, a dále příslušné prohlášení o aplikovatelnosti.

6.2	Poskytovatel je držitelem auditní zprávy SOC 2® Type 2 nebo auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5), a to ve formě Type 2, kdy tato auditní zpráva je vždy vydaná na poskytovateli nezávislým auditorem, není ke dni podání žádosti o zápis nabídky cloud computingu do katalogu cloud computingu starší než 24 měsíců a do jejíhož rozsahu jmenovitě náleží posuzovaná služba cloud computingu.	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), a to ve formě Type 2, ze které vyplývá splnění požadavku a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu této auditní zprávy, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu této auditní zprávy.
7. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty		
7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožňuje zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka. Nové události zpřístupní poskytovatel zákazníkovi bez zbytečného odkladu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

7.2	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat nebo specifických provozních údajů dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.
8. Testování služby cloud computingu		
8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.	Tři záznamy o provedení skenů zranitelností v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, ze kterých vyplývá splnění požadavku, přičemž tyto záznamy nejsou ke dni podání žádosti o zápis zapisované služby do katalogu cloud computingu starší více než 12 měsíců a zároveň alespoň jeden z těchto záznamů nebude ke dni podání žádosti o zápis služby do katalogu cloud computingu starší více než 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

		Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.
8.2	Poskytovatel zajišťuje provádění penetračních testů podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM, standardu OWASP Top 10 nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP. Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.	Zpráva z provedení penetračního testu, ze které vyplývá splnění požadavku.
9. Připojení do výměnného uzlu internetu (IXP)		
9.1	Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.	Výpis z veřejně dostupné databáze subjektů připojených do výměnného uzlu internetu, platná smlouva s poskytovatelem služby výměnného uzlu internetu, nebo čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku.

Příloha č. 4

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem zařazeným v bezpečnostní úrovni kritická	Podklad, kterým poskytovatel doloží splnění požadavku
1. Místo zpracování a uložení dat		
1.1	Poskytovatel uvádí informace o všech státech, z jejichž území dochází k výkonu správy a dohledu nad službou cloud computingu.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
1.2	Zákaznická data a specifické provozní údaje jsou zpracovávány na území České republiky. Aniž je dotčen požadavek uvedený na řádku 4.4 této přílohy, 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. Poskytovatel vždy uvádí úplný výčet datových center a jejich lokace po úroveň katastrálního území nebo obce, ve kterých jsou zpracovávána zákaznická data a specifické provozní údaje, a dále v případě, že služba cloud computingu A) umožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a deklaruje závazek zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, B) neumožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování; dále vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat a specifických provozních údajů mimo území České republiky, který je vyjádřen v samostatném dokumentu, který obsahuje výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaj o	Část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku podle A), B), nebo C).

	předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování, nebo C) neumožňuje splnění požadavku na zpracovávání zákaznických dat a specifických provozních údajů pouze na území České republiky, jasně označuje takovou službu cloud computingu a uvádí výčet států, na jejichž území dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na území příslušných států, a dále údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování; dále vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat a specifických provozních údajů mimo území České republiky.	
2. Žádosti o zpřístupnění a předání dat		
2.1	Poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat nebo specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní.	Čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku, část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

2.2	Poskytovatel jasně a srozumitelně uvádí své povinnosti vyplývající z právních řádů států odlišných od členských států Evropské unie nebo odlišných od členských států Evropského hospodářského prostoru nebo u těch států, u kterých Evropská komise nerozhodla o udělení rozhodnutí o odpovídající ochraně (adequacy decision) podle článku 45 obecného nařízení o ochraně osobních údajů[1)], na jejichž území se nalézá datové centrum nebo jiná infrastruktura, ve které dochází ke zpracování zákaznických dat nebo specifických provozních údajů podle řádku 1.2 této přílohy týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů. Tento 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. Proto poskytovatel provede popis povinností obsahující informace o tom, který cizozemský orgán veřejné moci, jehož činnost spočívá v prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, zpravodajská služba, nebo jiný orgán s obdobným předmětem činnosti nebo obdobnými pravomocemi, může žádat o zpřístupnění a předání dat, za jakých podmínek může tento orgán žádat o zpřístupnění a předání dat a na jak dlouho, na jaká data se daná povinnost vztahuje a zda je možné žádost o zpřístupnění nebo předání dat přezkoumat nezávislým soudem.	Písemný popis podle § 9 odst. 5 písm. a) této vyhlášky, ze kterého vyplývá splnění požadavku.
3. Oprávnění k provedení kontroly		
3.1	Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu s jím deklarovanými parametry, umožňuje Digitální a informační agentuře 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 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 doklad se nevyžaduje. Splnění tohoto požadavku ověří Digitální a informační agentura nebo Národní úřad pro kybernetickou a informační bezpečnost z úřední činnosti.
4. Zajištění poskytování služby cloud computingu		
4.1	Poskytovatel má vyhotoven a udržuje plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu.	Plán zajištění kontinuity provozu a plán na obnovu po havárii, nebo auditní zpráva podle § 7 odst. 1 této vyhlášky.

4.2	Poskytovatel vždy zajišťuje primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, a uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále zajišťuje, že A) tato datová centra jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo že je přijato adekvátní bezpečnostní opatření, nebo B) se tato datová 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.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, nebo část platné auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění obecného požadavku, a dále zprávu nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, který obsahuje náležitosti uvedené v příloze č. 7 k této vyhlášce, ze kterého vyplývá splnění požadavku podle A), nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku podle B).
4.3	Poskytovatel umožnuje synchronní replikaci dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.

4.4	Poskytovatel uvádí úplný výčet datových center, ze kterých je služba cloud computingu poskytována, a jejich lokace po úroveň katastrálního území nebo obce a dále 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.	Část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
4.5	Poskytovatel je schopen poskytovat nástroj nebo službu pro detekci a zmírnění útoků typu odepření služby (DoS/DDoS) jak na síťové, tak aplikační úrovni.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace, například popis volitelné služby cloud computingu, podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
4.6	Poskytovatel umožňuje obsluhu služby cloud computingu pomocí administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.

5. Nakládání s daty		
5.1	Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo v daném případě bez přechozího svolení zákazníka. 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. Poskytovatel umožňuje zákazníkovi přístup k tomuto záznamu, a za tím účelem jej uchovává 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 bodem 2.1 této přílohy. Pokud poskytovatel nemá zaveden proces pro přístup jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům bez předchozího svolení zákazníka, tento požadavek se neuplatní. Každý přístup k nezašifrovaným zákaznickým datům, ke kterému dojde bez předchozího svolení zákazníka, se pak považuje za narušení bezpečnosti informací dle řádku 7.2 této přílohy a poskytovatel postupuje v souladu s tímto požadavkem.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.2	Poskytovatel vždy chrání zákaznický obsah šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.3	Poskytovatel zákazníkovi umožňuje ochranu zákaznického obsahu šifrováním při všech síťových přenosech a v úložištích ve službě cloud computingu pomocí některého ze schválených algoritmů uvedených v aktuálně platném doporučení v oblasti kryptografických prostředků vydaném v souladu s nejlepší praxí Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách, v rámci celé šifrovací sady.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku,

	V případě, že poskytovatel nabízí šifrovací sady, které obsahují takové algoritmy, které nejsou schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, poskytovatel umožní zákazníkovi výběr těch šifrovacích sad, které aplikují algoritmy schválené v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost.	část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
5.4	Poskytovatel umožňuje uložení šifrovacích klíčů v certifikovaném hardware security modulu (HSM modulu) úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria Protection Profile (PP) EN 419 221-5 minimálně na EAL4 a vyšší, který je pod vzdálenou správou zákazníka nebo instalaci HSM modulu zákazníka do infrastruktury poskytovatele. Poskytovatel dále umožňuje bezpečnou likvidaci kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM modulu) řízenou zákazníkem a, v případě, že umožňuje uložení šifrovacích klíčů v certifikovaném HSM modulu, který je pod vzdálenou správou zákazníka, zajišťuje likvidaci vrchního přístupového klíče při ukončení služby cloud computingu, nebo, v případě, že umožňuje instalaci HSM modulu zákazníka do infrastruktury poskytovatele, umožňuje likvidaci vrchního přístupového klíče při ukončení služby cloud computingu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.
6. Certifikace služby cloud computingu		
6.1	Poskytovatel je držitelem platné certifikace podle 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 náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018.	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN

		ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu, a dále příslušné prohlášení o aplikovatelnosti.
6.2	Poskytovatel je držitelem auditní zprávy SOC 2® Type 2 nebo auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5), a to ve formě Type 2, kdy tato auditní zpráva je vždy vydaná na poskytovateli nezávislým auditorem, není ke dni podání žádosti o zápis nabídky cloud computingu do katalogu cloud computingu starší než 24 měsíců a do jejíhož rozsahu jmenovitě náleží posuzovaná služba cloud computingu.	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), a to ve formě Type 2, ze které vyplývá splnění požadavku a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu této auditní zprávy, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu této auditní zprávy.

7. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty		
7.1	Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožňuje zákazníkovi vzdálený přístup k informacím o všech událostech týkajících se daného zákazníka. Nové události zpřístupní poskytovatel zákazníkovi bez zbytečného odkladu.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
7.2	Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat nebo specifických provozních údajů bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat nebo specifických provozních údajů dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje poskytovatel zákazníka o přijatých opatřeních.	Část smluvní dokumentace podle § 9 odst. 5 písm. c) této vyhlášky, ze které vyplývá splnění požadavku, nebo část další dokumentace podle § 9 odst. 5 písm. d) této vyhlášky, ze které vyplývá splnění požadavku.
8. Testování služby cloud computingu		
8.1	Poskytovatel pravidelně provádí skeny zranitelností služby cloud computingu v intervalu alespoň jeden sken zranitelností každé 3 měsíce a v případě zjištění zranitelností zavádí nápravná opatření.	Tři záznamy o provedení skenů zranitelností v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, ze kterých vyplývá splnění požadavku, přičemž tyto záznamy nejsou ke dni podání

		žádosti o zápis zapisované služby do katalogu cloud computingu starší více než 12 měsíců a zároveň alespoň jeden z těchto záznamů nebude ke dni podání žádosti o zápis služby do katalogu cloud computingu starší více než 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku. Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.
8.2	Poskytovatel zajišťuje provádění penetračních testů podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP. Dojde-li k aktualizaci metodiky Národního úřadu pro kybernetickou a informační bezpečnost, poskytovatel předkládá podklady ke splnění požadavku v souladu s aktualizovanou metodikou po 24 měsících od data zveřejnění aktualizované metodiky.	Zpráva z provedení penetračního testu, ze které vyplývá splnění požadavku.

9. Připojení do výměnného uzlu internetu (IXP)		
9.1	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 podle § 9 odst. 5 písm. b) této vyhlášky, ze kterého vyplývá splnění požadavku.

Seznam certifikací pro oblast ochrany důvěrnosti, integrity a dostupnosti informací	
Pro řádek 6.1 přílohy č. 2 k této vyhlášce	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu.
Pro řádek 6.1 přílohy č. 3 a 4 k této vyhlášce	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu, a dále příslušné prohlášení o aplikovatelnosti.
Pro řádek 6.2 přílohy č. 3 a 4 k této vyhlášce	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), a to ve formě Type 2, kdy tato auditní zpráva je vždy vydaná na poskytovateli nezávislým auditorem, není ke dni podání žádosti o zápis nabídky cloud computingu do katalogu cloud computingu starší než 24 měsíců a do jejíhož rozsahu jmenovitě náleží posuzovaná služba cloud computingu a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu této auditní zprávy, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu této auditní zprávy.
Poskytovatel po dobu evidence služby cloud computingu v katalogu cloud computingu vedeném Digitální a informační agenturou dodá do 2 měsíců od data konce platnosti předchozího doloženého certifikátu	
Pro řádek 6.1 přílohy č. 2 k této vyhlášce	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu.

Pro řádek 6.1 přílohy č. 3 a 4 k této vyhlášce	Platný certifikát podle 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 posuzovanou službu cloud computingu, která je provozována v souladu s postupy normy ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27017 nebo ISO/IEC 27017 a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018, ČSN EN ISO/IEC 27018 nebo ISO/IEC 27018 a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu tohoto certifikátu, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu tohoto certifikátu, a dále příslušné prohlášení o aplikovatelnosti.
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu vedeném Digitální a informační agenturou	
Pro řádek 6.2 přílohy č. 3 a 4 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), a to ve formě Type 2, kdy tato auditní zpráva je vždy vydaná na poskytovateli nezávislým auditorem, není ke dni podání starší než 24 měsíců a do jejíhož rozsahu jmenovitě náleží posuzovaná služba cloud computingu a v případě, že posuzovaná služba cloud computingu není jmenovitě zahrnuta v rozsahu této auditní zprávy, dále čestné prohlášení poskytovatele podle § 9 odst. 5 písm. b) této vyhlášky o rozsahu této auditní zprávy.

Požadavky na strukturu a náležitosti zprávy o provedení penetračního testu	
Pro řádek 8.1 přílohy č. 1, 2, 3 a 4 k této vyhlášce	Tři záznamy o provedení skenů zranitelností provedených v souladu s platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, ze kterých vyplývá splnění požadavku, přičemž tyto záznamy nejsou ke dni podání žádosti o zápis zapisované služby do katalogu cloud computingu starší více než 12 měsíců a zároveň alespoň jeden z těchto záznamů nebude ke dni podání žádosti o zápis služby do katalogu cloud computingu starší více než 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
Pro řádek 8.2 přílohy č. 3 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM, standardu OWASP Top 10 nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP.
Pro řádek 8.2 přílohy č. 4 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP.
Poskytovatel dodá každých 24 měsíců evidence služby cloud computingu v katalogu cloud computingu Digitální a informační agenturou	
Pro řádek 8.1 přílohy č. 1, 2, 3 a 4 k této vyhlášce	Záznamy o provedení skenů zranitelností služby cloud computingu provedených alespoň jednou za každé 3 měsíce, nebo část auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky, ze které vyplývá splnění požadavku.
Pro řádek 8.2 přílohy č. 3 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM, standardu OWASP Top 10 nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců od data vyhotovení předchozí předložené zprávy o provedení penetračního testu. Z předložené zprávy o provedení penetračního testu nebo z auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky nebo prohlášení o aplikovatelnosti dokládaných podle přílohy č. 5 musí vyplývat, že poskytovatel zavádí nápravná opatření vzhledem k nálezům předchozích penetračních testů.

Pro řádek 8.2 přílohy č. 4 k této vyhlášce	Zprávu z provedení penetračního testu provedeného podle aktuálně platného standardu NIST 800-115, metodiky OSSTMM nebo standardu OWASP ASVS Level 1 odpovídající charakteru zapisované služby cloud computingu a v souladu s aktuálně platnou metodikou vydanou Národním úřadem pro kybernetickou a informační bezpečnost, která je zveřejněna na jeho internetových stránkách, nebo v souladu s metodikou FedRAMP. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců od data vyhotovení předchozí předložené zprávy o provedení penetračního testu. Z předložené zprávy o provedení penetračního testu nebo z auditní zprávy podle § 9 odst. 5 písm. e) této vyhlášky nebo prohlášení o aplikovatelnosti dokládaných podle přílohy č. 5 musí vyplývat, že poskytovatel zavádí nápravná opatření vzhledem k nálezům předchozích penetračních testů.

Pro řádek 4.2 přílohy č. 1, 2, 3 a 4 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]) 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).

[2]) § 74 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích).

[3]) Zákon č. 264/2025 Sb., o kybernetické bezpečnosti.

[4]) Zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

[5]) Vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

[6]) § 2 odst. 2 písm. e) zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

[7]) Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

ISSN 3029-5092

Vydavatel: Ministerstvo vnitra, Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7 • **Redakce Sbírky zákonů a mezinárodních smluv**: Ministerstvo vnitra, nám. Hrdinů 1634/3, poštovní schránka 155/SB, 140 21, Praha 4, telefon: 974 817 289, e-mail: sbirka@mv.gov.cz • Sazba: Tiskárna Ministerstva vnitra, Bartůňkova 1159/4, poštovní schránka 10, 149 00 Praha 11-Chodov • **Právně závazná elektronická verze Sbírky zákonů a mezinárodních smluv je k dispozici na www.e-sbirka.cz** • Tištěnou verzi částky Sbírky zákonů a mezinárodních smluv lze objednat u Tiskárny Ministerstva vnitra, telefon: 974 887 312, e-mail: info@tmv.cz, www.tmv.cz • Předplatné je od 1. 1. 2024 ukončeno.