

PARLAMENT ČESKÉ REPUBLIKY
Poslanecká sněmovna



VIII. volební období

Pozměňovací návrh

poslance Martina Kupky

k návrhu poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona o právu na digitální služby a o změně některých zákonů

(sněmovní tisk č. 447)

(ve znění komplexního pozměňovacího návrhu dle usnesení výboru pro veřejnou správu a regionální rozvoj č. 133 ze dne 5. září 2019 – č. 447/4)

Návrh úpravy tisku 447/4:

ČÁST TŘETÍ

Změna zákona o informačních systémech veřejné správy

§ 16

1. Bod 35 zní:

„Hlava VI

Využívání cloud computingu orgány veřejné správy

§ 6i

Působnost v oblasti využívání cloud computingu orgány veřejné správy

(1) Vláda

a) pověřuje státní orgán nebo osobu anebo jiné právní uspořádání poskytováním cloud computingu orgánům veřejné správy (dále jen „státní poskytovatel cloud computingu“),

b) schvaluje plán zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy včetně rozpočtového výhledu na 5 let.

(2) Ministerstvo

a) koordinuje využívání cloud computingu orgány veřejné správy,

- b) vydává metodické pokyny pro využívání cloud computingu orgány veřejné správy,
- c) zpracovává plán zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy včetně rozpočtového výhledu na 5 let a předkládá ho vládě,
- d) navrhuje opatření k zajištění dlouhodobě udržitelného financování využívání cloud computingu orgány veřejné správy,
- e) kontroluje kvalitu a cenu cloud computingu poskytovaného orgánům veřejné správy,
- f) spravuje informační systém cloud computingu pro orgány veřejné správy (dále jen „informační systém cloud computingu“),
- g) vede katalog cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“),
- h) ustanovuje poradní orgán pro oblast cloud computingu složený ze zástupců veřejné správy a odborné veřejnosti.

(3) Orgán veřejné správy poskytne na žádost ministerstva podklady pro zpracování plánu zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy.

§ 6j

Informační systém cloud computingu

(1) Zřizuje se informační systém cloud computingu, který je informačním systémem veřejné správy sloužícím k podpoře řízení využívání cloud computingu orgány veřejné správy.

(2) Správcem informačního systému cloud computingu je ministerstvo.

(3) Správce informačního systému cloud computingu může prostřednictvím informačního systému cloud computingu poskytovat službu dynamického nákupního systému podle zákona upravujícího zadávání veřejných zakázek.

(4) Správce informačního systému cloud computingu může prostřednictvím informačního systému cloud computingu poskytovat službu elektronického nástroje podle zákona upravujícího zadávání veřejných zakázek.

§ 6k

Katalog cloud computingu

(1) Katalog cloud computingu je veřejný seznam, který obsahuje údaje o cloud computingu využívaném orgány veřejné správy.

(2) Katalog cloud computingu je součástí informačního systému cloud computingu.

§ 6l

Využívání cloud computingu orgánem veřejné správy

(1) Orgán veřejné správy může využívat pouze cloud computing poskytovaný státním poskytovatelem cloud computingu nebo jiným poskytovatelem cloud computingu, než je státní poskytovatel cloud computingu, jestliže

a) splňuje bezpečnostní pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu,

b) splňuje kritéria pro zařazení do některé z bezpečnostních úrovní stanovené vyhláškou Národního úřadu pro kybernetickou a informační bezpečnost pro využívání cloud computingu orgány veřejné správy.

(2) Státní poskytovatel cloud computingu může poskytovat pouze cloud computing zařazený do nejvyšší bezpečnostní úrovně pro využívání cloud computingu orgány veřejné správy. Cena za poskytnutí cloud computingu státním poskytovatelem se stanoví podle cenových předpisů; působnost cenového orgánu pro poskytnutí cloud computingu orgánu veřejné správy vykonává ministerstvo.

(3) Jiný poskytovatel cloud computingu, než je státní poskytovatel cloud computingu, může poskytovat orgánu veřejné správy cloud computing kterékoli bezpečnostní úrovně, splní-li podmínky pro danou bezpečnostní úroveň stanovené vyhláškou Národního úřadu pro kybernetickou a informační bezpečnost.

§ 6m

Zápis a výmaz využívaného cloud computingu do katalogu cloud computingu

(1) Orgán veřejné správy zapíše cloud computing, který využívá, do katalogu cloud computingu, a to do 45 dnů ode dne nabytí platnosti smlouvy o poskytnutí cloud computingu.

(2) Orgán veřejné správy označí cloud computing, jehož využívání ukončil, za ukončený, a to do 45 dnů ode dne pozbytí platnosti smlouvy o poskytnutí cloud computingu.“

Dosavadní hlavy VI až IX se označují jako hlavy VII až X.

2. Za bod 50 se vkládá nový bod 51, který zní:

„§ 9e zní:

„§ 9e

(1) Provozovatel informačního systému veřejné správy předá na vyžádání správce tohoto systému bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému.

(2) Pokud provozovatel informačního systému veřejné správy nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a bezpečně zlikviduje ve svém digitálním prostředí jejich kopie. Způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis.

(3) Provozovatel informačního systému veřejné správy má právo na úhradu účelně

vynaložených nákladů za předání dat, a provozních údajů a informací podle odstavců 1 a 2.

(4) Ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat a provozních údajů podle odstavců 1 a 2 dotčena.“.“

Dosavadní body 51 až 55 se označují jako body 52 až 56.

3. V § 17 odst. 3 se věta poslední zrušuje.

ČÁST DEVÁTÁ

Změna zákona o kybernetické bezpečnosti

§ 24

4. Vkládá se nový bod 1, který zní:

„V § 4 odst. 5 písmeno a) zní:

„a) ustanovení obsahující povinnosti dodavatele dodržovat bezpečnostní politiku odběratele služeb nebo ustanovení o odsouhlasení bezpečnostní politiky dodavatele ze strany odběratele služeb,“.“

Dosavadní body 1 až 9 se označují jako body 2 až 10.

Odůvodnění:

Změna zákona o informačních systémech veřejné správy

K § 6i odst. 2:

Cloud computing je dynamicky se vyvíjející oblastí informačních technologií, která je založená na nejnovějších technologiích a úsporách z rozsahu. Je proto žádoucí, aby za účelem dobré využitelnosti těchto inovací ministerstvo průběžně koordinovalo vznikající procesy a regulace cloud computingu se zástupci odborné veřejnosti, nominovanými např. přes Hospodářskou komoru ČR.

K § 6k odst. 1:

Katalog cloud computingu je v tuto chvíli novým prvkem v procesu urychlení a zefektivnění nákupního procesu v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“). Lze očekávat, že praktická interpretace katalogu cloud computingu se ustálí až v průběhu zavádění navrhovaného nákupního mechanismu (dynamický nákupní systém). Na úrovni zákona není v danou chvíli žádoucí zacházet do hlubšího detailu, který se později může ukázat jako nepřesný či svazující.

K § 6l odst. 1:

V obecné rovině nutnou podmínkou využití cloud computingu orgány veřejné správy musí být splnění bezpečnostních pravidel a zařazení dané služby cloud computingu do některé z bezpečnostních úrovní tak, aby jednotlivé orgány veřejné správy nemusely proces hodnocení úrovně zabezpečení komerčních služeb cloud computingu znovu a znovu samy podstupovat. Nutnou podmínkou využití cloud computingu by však nemělo být zařazení do katalogu cloud computingu spravovaného ministerstvem. Cílem zřízení katalogu je primárně usnadnit nákup opakovaně využívaných služeb cloud computingu mechanismem dynamického nákupního systému (DNS). Tento mechanismus si však neklade za cíl pokrýt veškerý cloud computing, který může být „vysoutěžen“ orgány veřejné správy. Vzhledem k inovativnosti a narůstající konkurenci v tomto segmentu informačních a výpočetních technologií lze již nyní pozorovat rychlý nárůst nových služeb cloud computingu a zákon by proto neměl nastavovat podmínky, které by později mohly bránit urychlenému zavádění inovativních řešení a služeb.

K § 6l odst. 2:

Cílem nové úpravy je zajištění principu nekonkurence mezi poskytovateli komerční a státní částí eGovernment cloudu – nová úprava proto jasně uvádí, že státní poskytovatel smí nabízet cloud computing pouze v nejvyšší bezpečnostní úrovni, která je v zásadě cílena na oblast kritické informační infrastruktury. Aby mohly orgány veřejné správy vyhodnotit možné úspory spojené s využitím cloud computingu státním poskytovatelem, je důležité mít předem cenovou nabídku takové služby od státního poskytovatele.

K § 6l odst. 3:

V průběhu prací na Souhrnné analytické zprávě eGovernment cloudu a další práce Řídícího orgány eGovernment cloudu dosud nebyla nalezena právní forma poskytovatele státní části eGovernment cloudu, která by splňovala všechny provozní aspekty a řešila rizika spojená s narušením veřejné soutěže dle ZZVZ. Navrhovaná formulace předpokládá, že generálním dodavatelem (systémovým integrátorem) dodávky cloud computingu může být i komerční poskytovatel, který si však v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“), a jeho prováděcími předpisy bude muset na určité části dodávky s nejvyššími bezpečnostními požadavky zajistit subdodávku služeb státního poskytovatele

eGovernment cloudu.

K § 6m až § 6p:

Viz odůvodnění k § 6k odst. 1 výše.

K § 6q (novému § 6m):

Z důvodu archivace již ukončených služeb cloud computingu se uvádí formulace „označí za ukončený“; vymazání by mohlo znamenat ztrátu této informace v čase.

K § 9e:

Znění ustanovení by mělo být uvedeno do souladu s aktuálním zněním § 6a odst. 2, 3 a 4 ZKB. Odlišné úpravy v ZKB a v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, by mohly vést k právní nejistotě.

Změna zákona o kybernetické bezpečnosti

K § 4 odst. 5 písm. a):

Navrhuje se upravit ustanovení § 4 odst. 5 písm. a) ZKB tak, aby toto ustanovení bylo uvedeno do souladu s navazujícími právními předpisy (vyhláška Národního úřadu pro kybernetickou a informační bezpečnost č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, Příloha 7). Stávající znění § 4 nezohledňuje situaci na trhu tzv. multitenantních cloudových služeb, kde si zadavatel (zákazník, správce informačního systému veřejné správy) obvykle vybírá v rámci technické kvalifikace takovou službu a její bezpečnostní politiku, která je kompatibilní s bezpečnostní politikou správce informačního systému veřejné správy.

Změna zákona o informačních systémech veřejné správy

Hlava VI

Využívání cloud computingu orgány veřejné správy

§ 6i

Působnost v oblasti využívání cloud computingu orgány veřejné správy

(1) Vláda

- a) pověřuje státní orgán nebo osobu anebo jiné právní uspořádání poskytováním cloud computingu orgánům veřejné správy (dále jen „státní poskytovatel cloud computingu“),
- b) schvaluje plán zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy včetně rozpočtového výhledu na 5 let.

(2) Ministerstvo

- a) koordinuje využívání cloud computingu orgány veřejné správy,
- b) vydává metodické pokyny pro využívání cloud computingu orgány veřejné správy,
- c) zpracovává plán zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy včetně rozpočtového výhledu na 5 let a předkládá ho vládě,
- d) navrhuje opatření k zajištění dlouhodobě udržitelného financování využívání cloud computingu orgány veřejné správy,
- e) kontroluje kvalitu a cenu cloud computingu poskytovaného orgánům veřejné správy,
- f) spravuje informační systém cloud computingu pro orgány veřejné správy (dále jen „informační systém cloud computingu“),
- g) vede katalog cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“),
- h) ustanovuje poradní orgán pro oblast cloud computingu složený ze zástupců veřejné správy a odborné veřejnosti.**

(3) Orgán veřejné správy poskytne na žádost ministerstva podklady pro zpracování plánu zajištění potřebné kapacity pro poskytování cloud computingu státním poskytovatelem cloud computingu orgánům veřejné správy.

§ 6j

Informační systém cloud computingu

(1) Zřizuje se informační systém cloud computingu, který je informačním systémem veřejné správy sloužícím k podpoře řízení využívání cloud computingu orgány veřejné správy.

(2) Správcem informačního systému cloud computingu je ministerstvo.

(3) Správce informačního systému cloud computingu může prostřednictvím informačního systému cloud computingu poskytovat službu dynamického nákupního systému podle zákona upravujícího zadávání veřejných zakázek.

(4) Správce informačního systému cloud computingu může prostřednictvím informačního systému cloud computingu poskytovat službu elektronického nástroje podle zákona upravujícího zadávání veřejných zakázek.

§ 6k

Katalog cloud computingu

(1) ~~Katalog cloud computingu je veřejný seznam, který obsahuje údaje o poptávkách orgánů veřejné správy po poskytnutí cloud computingu (dále jen „poptávka cloud computingu“), nabídkách poskytnutí cloud computingu orgánům veřejné správy (dále jen „nabídka cloud computingu“) a o cloud computingu využívaném orgány veřejné správy.~~

(2) Katalog cloud computingu je součástí informačního systému cloud computingu.

§ 6l

Využívání cloud computingu orgánem veřejné správy

(1) Orgán veřejné správy může využívat pouze cloud computing poskytovaný státním poskytovatelem cloud computingu nebo jiným poskytovatelem cloud computingu, než je státní poskytovatel cloud computingu, ~~obsažený v nabídce cloud computingu zapsané v katalogu cloud computingu~~ jestliže

a) splňuje bezpečnostní pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu,

b) splňuje kritéria pro zařazení do některé z bezpečnostních úrovní stanovené vyhláškou Národního úřadu pro kybernetickou a informační bezpečnost pro využívání cloud computingu orgány veřejné správy.

(2) ~~Poskytovatelem cloud computingu zařazeného do nejvyšší bezpečnostní úrovně orgánu veřejné správy může být pouze státní poskytovatel cloud computingu. Státní poskytovatel cloud computingu může poskytovat pouze cloud computing zařazený do nejvyšší bezpečnostní úrovně pro využívání cloud computingu orgány veřejné správy. Cena za poskytnutí cloud computingu státním poskytovatelem orgánu veřejné správy se stanoví podle cenových předpisů; působnost cenového orgánu pro poskytnutí cloud computingu orgánu veřejné správy vykonává ministerstvo.~~

(3) Jiný poskytovatel cloud computingu, než je státní poskytovatel cloud computingu, může poskytovat orgánu veřejné správy cloud computing kterékoli

bezpečnostní úrovně, splní-li podmínky pro danou bezpečnostní úroveň stanovené vyhláškou Národního úřadu pro kybernetickou a informační bezpečnost.

~~§ 6m~~

~~Zápis poptávky cloud computingu do katalogu cloud computingu~~

~~(1) Ministerstvo zapíše poptávku cloud computingu do katalogu cloud computingu na základě žádosti orgánu veřejné správy, který poptává poskytnutí cloud computingu, a to do 45 dnů ode dne podání žádosti. Ministerstvo dále zapíše poptávku cloud computingu do katalogu cloud computingu na základě vlastního vyhodnocení potřeby využívání cloud computingu orgány veřejné správy.~~

~~(2) Orgán veřejné správy uvede v žádosti podle odstavce 1 kromě obecných náležitostí podání stanovených správním řádem údaje o poptávce cloud computingu v rozsahu údajů, které se o poptávce cloud computingu vedou v katalogu cloud computingu.~~

~~(3) Podmínkou zápisu poptávky cloud computingu do katalogu cloud computingu je, že poptávaný cloud computing~~

~~a) splňuje bezpečnostní pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu,~~

~~b) splňuje kritéria pro zařazení do některé z bezpečnostních úrovní pro využívání cloud computingu orgány veřejné správy,~~

~~c) neodpovídá svým obsahem jinému poptávanému cloud computingu, který je již zapsán v katalogu cloud computingu, a~~

~~d) je proveditelný.~~

~~(4) Splnění podmínek podle odstavce 3 posoudí ministerstvo ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost.~~

~~(5) Nesplňuje-li poptávaný cloud computing podmínky podle odstavce 3 a je-li žadatelem státní orgán, ministerstvo jej o nesplnění podmínek podle odstavce 3 vyrozumí prostřednictvím informačního systému cloud computingu; ve vyrozumění uvede, v čem spatřuje nesplnění podmínek podle odstavce 3.~~

~~(6) Nesplňuje-li poptávaný cloud computing podmínky podle odstavce 3 a je-li žadatelem orgán územního samosprávného celku, ministerstvo vydá rozhodnutí, kterým žádost o zápis poptávky cloud computingu do katalogu cloud computingu zamítne, a písemné vyhotovení rozhodnutí doručí žadateli prostřednictvím informačního systému cloud computingu. Proti rozhodnutí podle věty první není rozklad přípustný.~~

~~§ 6n~~

~~Výmaz poptávky cloud computingu z katalogu cloud computingu~~

~~(1) Ministerstvo vymaže z katalogu cloud computingu poptávku cloud computingu,~~

~~a) o jejíž zápis do katalogu cloud computingu požádal orgán veřejné správy, na základě žádosti tohoto orgánu veřejné správy, a to do 45 dnů ode dne podání žádosti o výmaz,~~

b) o jejíž zápis do katalogu cloud computingu požádal orgán veřejné správy, po uplynutí 1 roku ode dne, kdy byla poptávka cloud computingu do katalogu cloud computingu zapsána,

e) o jejíž zápis do katalogu cloud computingu požádal orgán veřejné správy, na základě zápisu cloud computingu, který je předmětem poptávky cloud computingu, do katalogu cloud computingu podle § 6q odst. 1,

d) kterou zapsalo do katalogu cloud computingu podle § 6m odst. 1 věty druhé, na základě vlastního vyhodnocení potřeby využívání cloud computingu orgány veřejné správy.

~~(2) Ministerstvo vyrozumí orgán veřejné správy, na základě jehož žádosti byla poptávka cloud computingu do katalogu cloud computingu zapsána, o výmazu poptávky cloud computingu podle odstavce 1 písm. a) a b) prostřednictvím informačního systému cloud computingu.~~

~~§ 6o~~

~~Zápis nabídky cloud computingu do katalogu cloud computingu~~

~~(1) Ministerstvo запиše nabídku cloud computingu do katalogu cloud computingu na základě žádosti poskytovatele cloud computingu, a to do 45 dnů ode dne podání žádosti.~~

~~(2) Poskytovatel cloud computingu uvede v žádosti podle odstavce 1 kromě obecných náležitostí podání stanovených správním řádem údaje o nabídce cloud computingu v rozsahu údajů, které se o nabídce cloud computingu vedou v katalogu cloud computingu.~~

~~(3) Podmínkou zápisu nabídky cloud computingu do katalogu cloud computingu je, že nabízený cloud computing splňuje~~

~~a) bezpečnostní pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu a~~

~~b) kritéria pro zařazení do některé z bezpečnostních úrovní pro využívání cloud computingu orgány veřejné správy.~~

~~(4) Splnění podmínek podle odstavce 3 posoudí ministerstvo ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost.~~

~~(5) Nesplňuje-li nabízený cloud computing podmínky podle odstavce 3, ministerstvo vydá rozhodnutí, kterým žádost o zápis nabídky cloud computingu do katalogu cloud computingu zamítne. Proti rozhodnutí podle věty první není rozklad přípustný.~~

~~§ 6p~~

~~Výmaz nabídky cloud computingu z katalogu cloud computingu~~

~~(1) Ministerstvo vymaže z katalogu cloud computingu nabídku cloud computingu,~~

~~a) o jejíž zápis do katalogu cloud computingu požádal poskytovatel cloud computingu, na základě žádosti tohoto poskytovatele cloud computingu, a to do 45 dnů ode dne podání žádosti o výmaz,~~

~~b) zjistí-li, že nabízený cloud computing přestal splňovat podmínky podle § 6o odst. 3; ministerstvo tak učiní bezodkladně po posouzení plnění podmínek podle § 6o odst. 3 ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost, nebo~~

~~e) a to po uplynutí 3 let ode dne, kdy byla nabídka cloud computingu do katalogu cloud computingu zapsána:~~

~~(2) Ministerstvo vyrozumí poskytovatele cloud computingu, na základě jehož žádosti byla nabídka cloud computingu do katalogu cloud computingu zapsána, o výmazu nabídky cloud computingu podle odstavce 1 písm. a) a e) prostřednictvím informačního systému cloud computingu.~~

~~(3) Ministerstvo vydá o výmazu nabídky cloud computingu z katalogu cloud computingu podle odstavce 1 písm. b) rozhodnutí. Proti rozhodnutí podle věty první není rozklad přípustný.~~

~~§ 6q~~ § 6m

Zápis a výmaz využívaného cloud computingu do katalogu cloud computingu

(1) Orgán veřejné správy zapíše cloud computing, který využívá, do katalogu cloud computingu, a to do 45 dnů ode dne nabytí platnosti smlouvy o poskytnutí cloud computingu.

(2) Orgán veřejné správy **vymaže označí** cloud computing, jehož využívání ukončil, **za ukončený**, a to do 45 dnů ode dne pozbytí platnosti smlouvy o poskytnutí cloud computingu.

§ 9e

(1) ~~Provozovatel informačního systému veřejné správy předá bezodkladně na vyžádání správce informačního systému veřejné správy data a provozní údaje týkající se provozovaného informačního systému veřejné správy. Provozovatel informačního systému veřejné správy předá na vyžádání správce tohoto systému bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému.~~

(2) ~~Provozovatel informačního systému veřejné správy předá bezodkladně po ukončení provozování informačního systému veřejné správy data a provozní údaje týkající se provozovaného informačního systému veřejné správy správci informačního systému veřejné správy a kopie těchto dat a provozních údajů zlikviduje. Pokud provozovatel informačního systému veřejné správy nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a bezpečně zlikviduje ve svém digitálním prostředí jejich kopie. Způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis.~~

~~(3) Provozovatel informačního systému veřejné správy zlikviduje kopie dat a provozních údajů týkajících se provozovaného informačního systému veřejné správy způsobem stanoveným prováděcím právním předpisem. Provozovatel informačního systému veřejné správy umožní správci informačního systému veřejné správy dohled nad průběhem likvidace kopií dat a provozních údajů.~~

~~(4) Provozovatel informačního systému veřejné správy vyhotoví o průběhu likvidace~~

~~kopii dat a provozních údajů týkajících se provozovaného informačního systému veřejné správy protokol, který předá správci informačního systému veřejné správy bezodkladně po provedení likvidace kopii dat a provozních údajů. Správce informačního systému veřejné správy uchová protokol alespoň po dobu 10 let.~~

~~(5)(3) Provozovatel informačního systému veřejné správy má právo na úhradu účelně vynaložených nákladů za předání dat, a provozních údajů a informací podle odstavců 1 a 2.~~

~~(6)(4) Ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat a provozních údajů podle odstavců 1 a 2 dotčena.~~

§ 17

Přechodná ustanovení

1. Orgán veřejné správy zapíše cloud computing, který využívá ke dni nabytí účinnosti tohoto zákona, do katalogu cloud computingu do 3 měsíců ode dne nabytí účinnosti tohoto zákona.

2. Orgán veřejné správy může využívat cloud computing, který využívá ke dni nabytí účinnosti tohoto zákona a který nesplňuje podmínky ~~pro zápis do katalogu~~ cloud computingu podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění účinném ode dne nabytí účinnosti tohoto zákona, nejvýše po dobu 3 let ode dne nabytí účinnosti tohoto zákona.

3. Orgán veřejné správy může využívat cloud computing, který využívá ke dni nabytí účinnosti tohoto zákona a který může podle zákona č. 365/2000 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, poskytovat pouze státní poskytovatel cloud computingu, nejvýše po dobu 3 let ode dne nabytí účinnosti tohoto zákona. ~~Věta první se nepoužije, splní-li cloud computing podle věty první do doby 3 let ode dne nabytí účinnosti tohoto zákona podmínku § 61 odst. 2 zákona č. 365/2000 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona.~~

Změna zákona o kybernetické bezpečnosti

HLAVA II

SYSTEM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Bezpečnostní opatření

§ 4

(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací¹⁾ v kybernetickém prostoru.

(2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.

(3) Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládnutí kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.

(4) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

(5) Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Dalšími nezbytnými náležitostmi smlouvy jsou

a) ~~zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,~~ **ustanovení obsahující povinnosti dodavatele dodržovat bezpečnostní politiku odběratele služeb nebo ustanovení o odsouhlasení bezpečnostní politiky dodavatele ze strany odběratele služeb,**

b) stanovení úrovně poskytovaných služeb,

c) systém schvalování subdodavatelů služby cloud computingu,

d) podmínky ukončení smluvního vztahu z pohledu bezpečnosti,

e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,

f) určení vlastníka uchovávaných dat,

g) dohoda o důvěrnosti smluvního vztahu,

h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,

i) pravidla zákaznického auditu,

j) stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.

(6) Poskytovatel služby cloud computingu a orgány a osoby uvedené v § 3 písm. c) až

g), které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel a realizaci bezpečnostní politiky odběratele.

(7) Zohlednění požadavků vyplývajících z bezpečnostní politiky, bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě podle odstavce 5, které jsou nezbytné pro splnění povinností podle tohoto zákona, nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.