



Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 14. října 2025

Vyhláška č. 411/2025 Sb.

**Vyhláška o bezpečnostních úrovních
informačních systémů veřejné správy**

411
VYHLÁŠKA
ze dne 26. září 2025

o bezpečnostních úrovních
informačních systémů veřejné správy

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 písm. g) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 265/2025 Sb., (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví bezpečnostní úroveň informačních systémů veřejné správy podle § 6l odst. 3 zákona a blíže upravuje postup zařazení do bezpečnostní úrovně.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

- a) oblastí dopadu oblast vymezená přílohou k této vyhlášce, v rámci které může mít dopad kybernetického bezpečnostního incidentu na informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, vliv na bezpečnost nebo zdraví lidí, ochranu osobních údajů, trestní řízení, veřejný pořádek, mezinárodní vztahy, důvěryhodnost orgánu veřejné správy, finanční ztráty nebo zajišťování služeb, a
- b) úrovní dopadu nízká, střední, vysoká nebo kritická hodnota, která vyplývá ze závažnosti dopadu kybernetického bezpečnostního incidentu na informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, v každé oblasti dopadu.

§ 3

Bezpečnostní úroveň

Bezpečnostní úroveň je

- a) nízká,
- b) střední,
- c) vysoká, nebo
- d) kritická.

§ 4

**Zařazení informačního systému veřejné správy,
k zajištění jehož provozu má být využíván cloud computing,
do bezpečnostní úrovně**

- (1) Zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně provede orgán veřejné správy podle přílohy k této vyhlášce. Orgán veřejné správy zhodnotí naplnění úrovně dopadu, které je informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, schopen dosáhnout v rámci každé oblasti dopadu. Úroveň dopadu je v rámci každé oblasti dopadu dána nejzávažnějším možným dopadem kybernetického bezpečnostního incidentu.
- (2) Při zjišťování nejzávažnějšího možného dopadu kybernetického bezpečnostního incidentu orgán veřejné správy zohlední možné narušení důvěrnosti, integrity a dostupnosti informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, a povahu tohoto systému jako celku. V případě, že má být cloud computingem zajištěn provoz pouze určité části informačního systému veřejné správy, zohlední se při hodnocení úrovně dopadu a zařazování této části do bezpečnostní úrovně také vztah této části k bezpečnostní úrovni informačního systému veřejné správy jako celku.
- (3) Výsledná bezpečnostní úroveň informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, je shodná s nejvyšší úrovní dopadu dosaženou při hodnocení jednotlivých oblastí dopadu.
- (4) Nejvyšší stanovená bezpečnostní úroveň informačního systému veřejné správy jako celku musí být stanovena alespoň pro jednu část informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing.
- (5) O procesu stanovení bezpečnostní úrovně informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, podle předchozích odstavců se provede písemný záznam.

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. listopadu 2025.

Ředitel:

Ing. Kintr v. r.

Příloha

Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně

Oblasti dopadu								
Úroveň dopadu	A. Bezpečnost nebo zdraví lidí	B. Ochrana osobních údajů	C. Trestní řízení a páchaní trestné činnosti	D. Veřejný pořádek	E. Mezinárodní vztahy	F. Důvěryhodnost orgánů veřejné správy	G. Finanční ztráty	H. Zajišťování služeb
1. Nízká	Nemůže vést k poruše zdraví jednotlivce ani skupiny lidí.	Nemůže ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, nebo může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje nejvýše dvě kritéria z první skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Nemůže vytvořit podmínky pro páchaní trestných činů присвоjení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozmenění veřejné listiny ani nemůže ztížit jejich vyšetřování.	Nemůže zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek.	Nemůže negativně ovlivnit obraz České republiky v zahraničí.	Nemůže negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, nebo může vztahy s nimi negativně ovlivnit, avšak negativní následky mohou být nejvýše lokální.	Nemůže ani přímo vést k finančním ztrátám, nebo může vést k finančním ztrátám menším než 1 % běžných výdajů ročního rozpočtu orgánu veřejné správy.	Nemůže způsobit omezení, narušení nebo nedostupnost žádných poskytovaných služeb, nebo může způsobit omezení, narušení nebo nedostupnost poskytovaných služeb pro 5 000 a méně osob.
2. Střední	Může vést k poruše zdraví jednotlivce nebo skupiny nejvíce 100 lidí.	Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje tři a více kritérií z první	Může vytvořit podmínky pro páchaní trestných činů присвоjení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozmenění veřejné	Může zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek s lokálními dopady.	Může negativně ovlivnit obraz České republiky v sousedních státech.	Může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše regionální.	Může vést k finančním ztrátám ve výši mezi 1 % a 5 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 5 000, nejvíce však 50 000 osob.

		skupiny kritérií nebo jedno kritérium z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	listiny nebo může ztížit jejich vyšetřování.	Může zapříčinit hromadné nepokoje nebo jinak závazně narušit veřejný pořádek s regionálními dopady.	Může negativně ovlivnit obraz České republiky ve světě.	Může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobé s mezinárodním prvkem.	100 000 Kč a vyšší. V případě, že výše finanční ztráty odpovídá částce nižší než 100 000 Kč, použije se úroveň dopadu nízká.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 50 000 osob.
3. Vysoká	Může vést k poruše zdraví skupiny více než 100 lidí a nejvíce 2 500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí.	Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Může vést k narušení vyšetřování trestné činnosti nebo k narušení soudního řízení trestního.	Může zapříčinit hromadné nepokoje nebo jinak závazně narušit veřejný pořádek s regionálními dopady.	Může negativně ovlivnit obraz České republiky ve světě.	Může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobé s mezinárodním prvkem.	100 000 Kč a vyšší. V případě, že výše finanční ztráty odpovídá částce nižší než 100 000 Kč, použije se úroveň dopadu nízká.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 50 000 osob.

4. Kritická	Může vést k poruše zdraví skupiny více než 2 500 lidí nebo k přímému ohrožení nebo ztrátě života skupiny více než 250 lidí.	Může vést k závažnému narušení a dlouhodobému vyšetřovat trestnou činnost nebo ke zpochybnění zákonnosti soudního řízení trestního.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může vést k přímému poškození nebo přerušení diplomatických vztahů České republiky se zahraničními partnery.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností a negativní následky mohou být dlouhodobé a s mezinárodním prvkem.	Může vést k finančním ztrátám vyšším než 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty České republiky vyšší než 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 10 000 000 Kč, použije se úroveň dopadu vysoká.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 lidí.
----------------	---	---	--	--	---	--	---

Skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů

1) První skupinu kritérií tvoří tato kritéria:

- a) zpracovávají se osobní údaje umožňující bez dalšího vystupovat nebo jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti nebo charakteru nebo umožňující na účet subjektu údajů odebírat služby, zboží, popřípadě vybírat peníze nebo jiné majetkové hodnoty,
- b) zpracovávají se osobní údaje, podle kterých je subjekt údajů zařaditelný jako člen skupiny s časově omezenou nebo situačně danou zranitelností,
- c) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno 5 000 až 10 000 subjektů údajů,
- d) osobní údaje jsou veřejně přístupné neomezenému počtu orgánů nebo osob a
- e) jedná se o zpracování osobních údajů systémem s propojením na jiná zpracování prováděná stejným správcem osobních údajů nebo se jedná o osobní údaje získané od jiných správců osobních údajů.

2) Druhou skupinu kritérií tvoří tato kritéria:

- a) zpracovávají se zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy, zejména finanční údaje o stavu majetku, výši finančních prostředků, dluhů nebo půjčkách nebo platební morálce, záznamy o historii soukromých volání subjektů údajů, údaje z elektronické pošty subjektů údajů a podobně,
- b) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno více než 10 000 subjektů údajů a
- c) dochází k automatizovanému rozhodování, které se dotýká subjektu údajů.

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@mvcz.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.