ZÁKONY PRO LIDI

Vyhláška č. 334/2025 Sb.

Vyhláška o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony

https://www.zakonyprolidi.cz/cs/2025-334

Částka	**334/2025**
Platnost od	**09.09.2025**
Účinnost od	**01.11.2025** **(za 1 měsíc)**

Budoucí znění 01.11.2025

334

VYHLÁŠKA

ze dne 27. srpna 2025

o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 6 odst. 1, § 16 odst. 5, § 34 odst. 3 a § 45 odst. 3 zákona č. 264/2025 Sb., o kybernetické bezpečnosti, (dále jen „zákon“):

---

§ 1

Předmět úpravy

Tato vyhláška stanoví

a) formát a způsob ohlášení regulované služby podle § 6 odst. 1 zákona,

b) obsahové náležitosti, formát a způsob hlášení kybernetického bezpečnostního incidentu, průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu, průběžné zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu a závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu,

c) formát a způsob hlášení údajů osob poskytujících služby registrace doménových jmen podle § 34 odst. 1 zákona a

d) technické a organizační podmínky používání Portálu Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Portál Úřadu“), obsahové náležitosti, formát, strukturu a způsob provedení úkonů podle § 45 odst. 2 zákona.

§ 2

Portál Úřadu

(1) Přístup do Portálu Úřadu se provádí prostřednictvím internetových stránek Úřadu po přihlášení pomocí přihlašovacích údajů.

(2) Úřad v rámci Portálu Úřadu umožní provedení nebo podání

a) ohlášení regulované služby podle § 6 odst. 1 zákona,

b) ohlášení změny regulované služby podle § 9 odst. 1 a § 26 odst. 1 zákona,

c) žádosti o zrušení registrace regulované služby podle § 10 odst. 2 zákona,

d) hlášení údajů podle § 11 zákona,

e) hlášení incidentů podle § 15 a 16 zákona,

f) oznámení provedení reaktivního protiopatření podle § 23 odst. 6 zákona a

g) hlášení informací o dodavatelích podle § 31 odst. 1 písm. c) zákona.

§ 3

Druhy hlášených údajů

(1) Druhy hlášených údajů se pro účely této vyhlášky rozumí registrační údaje, kontaktní údaje a doplňující údaje.

(2) Registračními údaji se rozumí

a) identifikační údaje poskytovatele regulované služby, kterými jsou jeho název, identifikační číslo osoby, bylo-li mu přiděleno, sídlo, případně adresa hlavní provozovny a dalších provozoven v jiných členských státech, a

b) seznam poskytovaných regulovaných služeb a splněných podmínek významnosti poskytovatele podle vyhlášky upravující regulované služby.

(3) Kontaktními údaji se rozumí

a) identifikační údaje fyzické osoby, která je oprávněna jednat za poskytovatele regulované služby ve věcech upravených zákonem, a

b) funkce nebo pracovní zařazení, telefonní číslo a adresa elektronické pošty fyzické osoby, která je oprávněna jednat za poskytovatele regulované služby ve věcech upravených zákonem.

(4) Doplňujícími údaji se rozumí

a) doménová jména a rozsahy IP adres, které jsou využívány k poskytování regulované služby,

b) informace o geografickém rozšíření regulované služby a o jejím přeshraničním poskytování a

c) informace o členství poskytovatele regulované služby v koncernu a o jeho účasti v komunitě pro sdílení informací v oblasti kybernetické bezpečnosti.

§ 4

Hlášení kybernetického bezpečnostního incidentu

(1) Hlášení kybernetického bezpečnostního incidentu poskytovatelem regulované služby obsahuje

a) identifikační údaje poskytovatele regulované služby,

b) doplňující údaje k zasaženým aktivům,

c) informace o kybernetickém bezpečnostním incidentu, zejména datum a čas zjištění, stav řešení incidentu, pravděpodobnou příčinu incidentu, popis incidentu a indikátory kompromitace, jsou-li tyto informace dostupné,

d) informace vymezující dopad incidentu, zejména funkční dopad, odhad rozsahu a počtu zasažených aktiv nebo osob, čas a zdroje potřebné k obnově poskytování zasažené služby, lokaci incidentu, citlivost zasažených dat a případný přeshraniční dopad incidentu, jsou-li tyto informace dostupné, a

e) informace o reakci na kybernetický bezpečnostní incident, zejména o požadované podpoře ze strany Úřadu, přijatých a probíhajících opatřeních ke zmírnění následků a výčtu subjektů, které byly v souvislosti s incidentem informovány.

(2) V rámci hlášení kybernetického bezpečnostního incidentu může poskytovatel regulované služby provést

a) prvotní hlášení podle § 16 odst. 1 zákona,

b) oznámení incidentu podle § 16 odst. 3 písm. a) zákona,

c) podání průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. b) zákona,

d) podání závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. c) zákona a

e) podání průběžné zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. c) zákona.

(3) Průběžná zpráva o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. b) zákona obsahuje informace o doposud učiněných krocích ke zvládání incidentu a informace o případných nových skutečnostech.

(4) Závěrečná zpráva o vyřešení kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. c) zákona obsahuje aktualizované informace podle odstavce 1.

(5) Průběžná zpráva o aktuálním stavu zvládání kybernetického bezpečnostního incidentu podle § 16 odst. 3 písm. c) zákona obsahuje informace o doposud učiněných krocích ke zvládání incidentu, informace o případných nových skutečnostech, plánované kroky k vyřešení incidentu a vysvětlení, z jakého důvodu doposud nedošlo k jeho vyřešení.

(6) Hlásí-li poskytovatel regulované služby kybernetický bezpečnostní incident v souladu s § 16 odst. 4 zákona jinak než prostřednictvím Portálu Úřadu, uplatní se obsahové náležitosti podle odstavce 1 obdobně.

(7) Hlásí-li kybernetický bezpečnostní incident prostřednictvím internetových stránek Úřadu dobrovolný ohlašovatel podle § 15 odst. 5 zákona, který není poskytovatel regulované služby, obsahuje hlášení

a) identifikační a kontaktní údaje ohlašovatele nebo jiné kontaktní osoby,

b) identifikaci a popis informačního systému nebo služby zasažené kybernetickým bezpečnostním incidentem,

c) informace o kybernetickém bezpečnostním incidentu, zejména datum a čas zjištění, druh hrozby nebo základní příčinu, která incident spustila, odhad rozsahu zasažení systémů, odhad počtu zasažených uživatelů, podrobný popis incidentu a případný přeshraniční dopad incidentu, jsou-li tyto informace dostupné, a

d) informace o reakci na kybernetický bezpečnostní incident, zejména stav zvládání incidentu a přijatá a probíhající opatření ke zmírnění následků.

§ 5

Obsahové náležitosti některých úkonů

(1) Ohlášení regulované služby podle § 6 zákona nebo pro ohlášení změny regulované služby podle § 9 a 26 zákona obsahuje registrační údaje, případně jejich změnu.

(2) Žádost o zrušení registrace regulované služby podle § 10 odst. 2 zákona obsahuje

a) registrační údaje regulované služby, o jejíž výmaz je žádáno, a

b) odůvodnění žádosti o výmaz.

(3) Hlášení údajů podle § 11 zákona obsahuje

a) identifikační údaje poskytovatele regulované služby,

b) kontaktní údaje a

c) doplňující údaje.

(4) Oznámení provedení reaktivního protiopatření podle § 23 odst. 6 zákona obsahuje

a) identifikační údaje poskytovatele regulované služby,

b) doplňující údaje relevantní s ohledem na obsah reaktivního protiopatření,

c) identifikace reaktivního protiopatření a

d) informaci o provedení reaktivního protiopatření a jeho výsledku.

(5) Hlášení informací o dodavatelích podle § 31 odst. 1 písm. c) zákona obsahuje

a) identifikační údaje poskytovatele regulované služby,

b) identifikační údaje dodavatele bezpečnostně významné dodávky,

c) identifikaci bezpečnostně významné dodávky,

d) identifikaci kritické části stanoveného rozsahu, do níž směřuje bezpečnostně významná dodávka,

e) identifikaci regulované služby, k níž se váže bezpečnostně významná dodávka, a

f) informaci o vztahu poskytovatele regulované služby s dodavatelem.

§ 6

Hlášení údajů osob poskytujících služby registrace doménových jmen

Údaje podle § 34 zákona se hlásí prostřednictvím formuláře uveřejněného na internetových stránkách Úřadu.

§ 7

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. listopadu 2025.

Ředitel:

Ing. Kintr v. r.

Souvislosti

Provádí předpis

264/2025 Sb.	Zákon o kybernetické bezpečnosti

Odkazuje na

264/2025 Sb.	Zákon o kybernetické bezpečnosti

Verze

č.	Znění od - do	Novely	Poznámka

č.	Znění od - do	Novely	Poznámka
1.	**01.11.2025**		Budoucí znění
0.	09.09.2025		Vyhlášené znění