Vládní návrh

**ZÁKON**

ze dne dd.mm.rrrr,

**o kybernetické bezpečnosti**

Parlament se usnesl na tomto zákoně České republiky:

# ČÁST PRVNÍKYBERNETICKÁ BEZPEČNOST

## HLAVA IZákladní ustanovení

### § 1Předmět úpravy

1. Tento zákon upravuje práva a povinnosti orgánů a osob a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) a dalších orgánů veřejné moci v oblasti kybernetické bezpečnosti.

*CELEX 32022L2555*

1. Tento zákon zapracovává příslušný předpis Evropské unie[[1]](#footnote-1)), navazuje na přímo použitelné předpisy Evropské unie[[2]](#footnote-2)) a upravuje zajišťování kybernetické bezpečnosti v České republice.

*CELEX 32022L2555, 32019R0881, 32011D1104, 32021R0887 32021R0696*

1. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

### § 2Vymezení pojmů

1. Pro účely tohoto zákona se rozumí
	1. aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě,
	2. primárním aktivem informace a služby, přičemž informacemi se rozumí také data, včetně provozních údajů, a službou se rozumí také procesy,
	3. podpůrným aktivem zaměstnanci, dodavatelé, objekty a technická aktiva,
	4. technickým aktivem technické a programové prostředky a vybavení, kdy technickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová, řídící nebo jiná obdobná specifická aktiva,
	5. regulovanou službou služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva,
	6. poskytovatelem regulované služby orgán nebo osoba, které poskytují jednu nebo více regulovaných služeb,
	7. řízením kybernetické bezpečnosti činnost poskytovatele regulované služby podle tohoto zákona směřující k zajištění kybernetické bezpečnosti regulované služby.
2. Pro účely tohoto zákona se dále rozumí
	1. kybernetickým prostorem digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat,
	2. bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat,
	3. kybernetickou hrozbou jakákoliv potenciální okolnost, událost nebo jednání, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby, a tím způsobit kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident,
	4. významnou kybernetickou hrozbou kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou majetkovou nebo nemajetkovou újmu,
	5. kybernetickou bezpečnostní událostí událost, která může způsobit kybernetický bezpečnostní incident,
	6. kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv,
	7. zvládáním kybernetického bezpečnostního incidentu úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a následného zotavení,
	8. významným dodavatelem ten, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti,
	9. strategicky významnou službou regulovaná služba, jejíž narušení bezpečnosti by mohlo vést k významnému omezení či ohrožení služeb pro občany státu a chodu státu,
	10. poskytovatelem strategicky významné služby poskytovatel regulované služby, který poskytuje jednu nebo více strategicky významných služeb,
	11. zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

*CELEX 32022L2555*

## HLAVA IIPoskytovatel regulované služby

## Díl 1Stanovení regulované služby a režimu poskytovatele regulované služby

### § 3Kritéria regulované služby

Regulovaná služba je stanovena kritérii pro identifikaci regulované služby nebo kritérii pro určení regulované služby.

### § 4 Kritéria pro identifikaci regulované služby

1. Kritéria pro identifikaci regulované služby jsou tvořena kritériem služby a kritériem poskytovatele regulované služby. Kritéria pro identifikaci regulované služby stanoví prováděcí právní předpis.
2. Prováděcí právní předpis stanoví kritéria pro identifikaci regulované služby v těchto odvětvích
	1. veřejná správa,
	2. energetika,
	3. výrobní průmysl,
	4. potravinářský průmysl,
	5. chemický průmysl,
	6. vodní hospodářství,
	7. odpadové hospodářství,
	8. doprava,
	9. digitální infrastruktura a služby,
	10. finanční trh,
	11. zdravotnictví,
	12. věda, výzkum a vzdělávání,
	13. poštovní a kurýrní služby,
	14. vojenský průmysl,
	15. vesmírný průmysl.

*CELEX 32022L2555*

### § 5Kritéria pro určení regulované služby

Regulovanou službou je dále služba stanovená u orgánu nebo osoby rozhodnutím Úřadu v případě, že

1. jde o službu uvedenou v prováděcím právním předpise stanovujícím kritéria pro identifikaci regulovaných služeb a
	1. orgán nebo osoba je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zachování nezbytných společenských nebo ekonomických činností ve státě,
	2. narušení této služby by mohlo mít významný dopad na veřejnou bezpečnost nebo veřejné zdraví,
	3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
	4. orgán nebo osoba je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví nebo typ služby nebo pro jiná vzájemně propojená odvětví v České republice,
2. její narušení může způsobit závažný zásah do života postihující více než 125 000 osob, a to prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního či veřejného pořádku, bezpečnosti nebo životního prostředí,
3. její narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu stejného nebo jiného poskytovatele regulované služby v režimu vyšších povinností, nebo
4. orgán nebo osoba je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu.

*CELEX 32022L2555*

### § 6Režim poskytovatele regulované služby

1. Režim poskytovatele regulované služby stanovuje míru povinností uložených poskytovateli regulované služby podle tohoto zákona.
2. Režim poskytovatele regulované služby je
	1. režim vyšších povinností, nebo
	2. režim nižších povinností.
3. Režim poskytovatele regulované služby je stanoven prováděcím právním předpisem. Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností.

*CELEX 32022L2555*

### § 7Režim poskytovatele regulované služby v případě poskytování více regulovaných služeb

1. Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim poskytovatele regulované služby.
2. Platí, že poskytovatel regulované služby, kterému je stanoven režim vyšších povinností pro alespoň jednu jím poskytovanou regulovanou službu, má stanoven režim vyšších povinností a plní povinnosti plynoucí z tohoto zákona v režimu vyšších povinností vůči všem regulovaným službám, které poskytuje.

*CELEX 32022L2555*

### § 8Registrace poskytovatele regulované služby

1. Poskytovatel regulované služby je povinen nahlásit Úřadu naplnění kritérií pro identifikaci regulované služby, a to vyplněním registračních údajů podle § 12 odst. 2 písm. a).
2. Registraci podle odstavce 1 je poskytovatel regulované služby povinen provést nejpozději do 30 dnů ode dne, kdy zjistí, že došlo k naplnění kritérií pro identifikaci regulované služby, nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo.
3. Úřad provede registraci poskytovatele regulované služby v případě, kdy se dozví o naplnění kritérií pro identifikaci regulované služby podle prováděcího právního předpisu a poskytovatel regulované služby neprovede registraci podle odstavce 1 ve lhůtě podle odstavce 2.
4. Úřad dále provede registraci poskytovatele regulované služby nebo regulované služby na základě rozhodnutí Úřadu o určení regulované služby podle § 5. V případě, že v důsledku rozhodnutí podle předchozí věty dojde ke změně režimu poskytovatele regulované služby z režimu vyšších povinností na režim nižších povinností, nové lhůty pro zahájení plnění povinností podle § 12 odst. 3, § 14 odst. 3 a § 16 odst. 4 neplynou.

*CELEX 32022L2555*

### § 9Změna registrace poskytovatele regulované služby

1. Poskytovatel regulované služby je povinen v případě naplnění kritérií pro identifikaci každé další regulované služby provést změnu registrace poskytovatele regulované služby a postupovat obdobně podle § 8 odst. 1 a 2.
2. Poskytovatel regulované služby je povinen v případě, že v rámci naplnění kritérií pro identifikaci regulované služby dojde ke změně režimu poskytovatele regulované služby, provést změnu registrace poskytovatele regulované služby a postupovat obdobně podle § 8 odst. 1 a 2. Při změně režimu poskytovatele regulované služby z režimu vyšších povinností na režim nižších povinností nové lhůty pro zahájení plnění povinností podle § 12 odst. 3, § 14 odst. 3 a § 16 odst. 4 neplynou.

### § 10Zápis do evidence poskytovatelů regulovaných služeb

1. Úřad bez zbytečného odkladu zapíše poskytovatele regulované služby a regulovanou službu do evidence poskytovatelů regulovaných služeb na základě registrace poskytovatele regulované služby či změny registrace poskytovatele regulované služby podle § 8 a § 9. O této skutečnosti Úřad poskytovatele regulované služby písemně vyrozumí.
2. Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.

*CELEX 32022L2555*

### § 11Výmaz z evidence poskytovatelů regulovaných služeb

1. Pokud se Úřad dozví, že poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb na základě registrace podle § 8 odst. 1 a 3 nebo § 9 odst. 1 nadále neposkytuje službu naplňující kritéria pro identifikaci regulované služby podle prováděcího právního předpisu, Úřad registrovanou regulovanou službu vymaže z evidence poskytovatelů regulovaných služeb a o této skutečnosti poskytovatele regulované služby písemně vyrozumí.
2. Pokud se Úřad dozví, že poskytovatel regulované služby, jehož služba byla určena rozhodnutím Úřadu podle § 5, nadále neposkytuje službu naplňující kritéria pro určení regulované služby, Úřad rozhodne o tom, že služba, kterou poskytovatel regulované služby poskytuje, nesplňuje kritéria pro určení regulované služby. Po nabytí právní moci rozhodnutí Úřad registrovanou regulovanou službu vymaže z evidence poskytovatelů regulovaných služeb a o této skutečnosti poskytovatele regulované služby písemně vyrozumí.
3. Pokud se Úřad dozví, že orgán nebo osoba zapsaná v evidenci poskytovatelů regulovaných služeb nadále neposkytuje žádnou službu naplňující kritéria pro identifikaci regulované služby nebo službu určenou rozhodnutím Úřadu pro naplnění kritérií pro určení regulované služby, Úřad tento orgán nebo osobu vymaže z evidence poskytovatelů regulovaných služeb a o této skutečnosti tento orgán nebo osobu písemně vyrozumí.

## Díl 2Povinnosti poskytovatele regulované služby

### § 12Hlášení údajů poskytovatelem regulované služby

1. Poskytovatel regulované služby hlásí registrační, kontaktní a další doplňující údaje a jejich změny Úřadu. Poskytovatel regulované služby odpovídá za správnost a úplnost nahlášených údajů.
2. Hlášenými údaji jsou
	1. registrační údaje, kterými se rozumí informace spojené s identifikací poskytovatele regulované služby a jím poskytované regulované služby,
	2. kontaktní údaje, kterými se rozumí informace spojené s identifikací fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem, a
	3. doplňující údaje, kterými jsou další informace potřebné pro výkon činnosti Úřadu podle tohoto zákona.
3. Poskytovatel regulované služby je povinen nahlásit údaje podle odstavce 2 písm. b) a c) pro každou regulovanou službu nejpozději do 30 dnů ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § 10 odst. 1.
4. Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 15 dnů od jejich změny.
5. Poskytovatel regulované služby je povinen zajistit dostatečnou zastupitelnost fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem.
6. Obsahové náležitosti, formát a způsob provedení hlášení registračních, kontaktních a doplňujících údajů stanoví prováděcí právní předpis.

*CELEX 32022L2555*

### § 13Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby

1. Poskytovatel regulované služby
	1. identifikuje všechna primární aktiva v rámci celé organizace,
	2. určí, která primární aktiva identifikovaná podle písm. a) souvisejí s poskytováním regulované služby,
	3. u primárních aktiv určených podle písm. b) identifikuje a určí související organizační části organizace a podpůrná aktiva.
2. Organizační části a aktiva identifikovaná podle odstavce 1 písm. b) a c) tvoří rozsah řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“).
3. O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.
4. Do doby splnění povinností podle odstavce 1 a 3 se má za to, že stanovený rozsah je tvořen regulovanou službou poskytovatele regulované služby a podpůrnými aktivy jsou všechna podpůrná aktiva organizace a další podpůrná aktiva související s poskytováním regulované služby.
5. Má se za to, že aktiva, která ještě nebyla identifikována a určena podle odstavce 1 nebo zahrnuta do stanoveného rozsahu podle odstavce 4, jsou součástí stanoveného rozsahu, dokud tyto změny nejsou zahrnuty v procesu identifikace a určování organizačních částí a aktiv tvořících stanovený rozsah podle odstavce 1 a není o nich veden dokumentovaný záznam podle odstavce 3.

*CELEX 32022L2555*

### § 14Bezpečnostní opatření

1. Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. Bezpečnostními opatřeními jsou organizační a technická opatření.
2. Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavést a provádět bezpečnostní opatření podle § 15 alespoň v míře a způsobem stanoveným prováděcím právním předpisem.
3. Poskytovatel regulované služby začne plnit povinnost zavádět a provádět bezpečnostní opatření podle odstavce 2 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § 10 odst. 1.
4. Prováděcí právní předpis stanoví bezpečnostní opatření odpovídající režimu poskytovatele regulované služby.

*CELEX 32022L2555*

### § 15Seznam bezpečnostních opatření

1. Pro poskytovatele regulované služby v režimu vyšších povinností jsou
	1. organizačními opatřeními
		1. systém řízení bezpečnosti informací,
		2. povinnosti vrcholného vedení,
		3. bezpečnostní role,
		4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
		5. řízení aktiv,
		6. řízení rizik,
		7. řízení dodavatelů,
		8. bezpečnost lidských zdrojů,
		9. řízení změn,
		10. akvizice, vývoj a údržba,
		11. řízení přístupu,
		12. zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
		13. řízení kontinuity činností a
		14. audit kybernetické bezpečnosti,
	2. technickými opatřeními
		1. fyzická bezpečnost,
		2. bezpečnost komunikačních sítí,
		3. správa a ověřování identit,
		4. řízení přístupových oprávnění,
		5. detekce kybernetických bezpečnostních událostí,
		6. zaznamenávání bezpečnostních a relevantních provozních událostí,
		7. vyhodnocování kybernetických bezpečnostních událostí,
		8. aplikační bezpečnost,
		9. kryptografické algoritmy,
		10. zajišťování dostupnosti regulované služby a
		11. zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.
2. Pro poskytovatele regulované služby v režimu nižších povinností jsou bezpečnostními opatřeními
	* 1. zajišťování minimální úrovně kybernetické bezpečnosti,
		2. povinnosti vrcholného vedení,
		3. řízení rizik,
		4. bezpečnost lidských zdrojů,
		5. řízení kontinuity činností,
		6. řízení přístupu,
		7. řízení identit a jejich oprávnění,
		8. detekce a zaznamenávání kybernetických bezpečnostních událostí,
		9. řešení kybernetických bezpečnostních incidentů,
		10. bezpečnost komunikačních sítí,
		11. aplikační bezpečnost a
		12. kryptografické algoritmy.

*CELEX 32022L2555*

### § 16Hlášení kybernetických bezpečnostních incidentů

1. Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru.
2. Poskytovatel regulované služby v režimu nižších povinností je povinen v rámci stanoveného rozsahu hlásit Národnímu CERT všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a mají významný dopad na poskytování regulované služby.
3. Způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby poskytovatelem regulované služby v režimu nižších povinností stanoví prováděcí právní předpis.
4. Poskytovatel regulované služby začne plnit povinnost hlásit kybernetické bezpečnostní incidenty podle odstavce 1 a 2 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § 10 odst. 1.
5. Orgán nebo osoba může prostřednictvím internetových stránek Úřadu dobrovolně hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, stejně tak jako hlásit kybernetické bezpečnostní události nebo kybernetické hrozby. Prostřednictvím internetových stránek Úřadu mohou být anonymně hlášeny také zranitelnosti, zejména pro účely zajištění koordinovaného zveřejňování zranitelností ze strany Vládního CERT. Tím není dotčena povinnost poskytovatele regulované služby podle odstavce 1 a 2.
6. Tímto ustanovením není dotčena informační povinnost podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů.

*CELEX 32022L2555*

### § 17Náležitosti hlášení kybernetických bezpečnostních incidentů

1. Poskytovatel regulované služby bez zbytečného odkladu po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.
2. Úřad sdělí poskytovateli regulované služby v režimu vyšších povinností bez zbytečného odkladu, nejpozději do 24 hodin po nahlášení kybernetického bezpečnostního incidentu podle odstavce 1 na základě obsahu hlášení a dalších relevantních informací, zda má kybernetický bezpečnostní incident u poskytovatele regulované služby v režimu vyšších povinností významný dopad na kybernetický prostor státu. Významnost dopadu na kybernetický prostor státu je dána významem dopadu na poskytování regulované služby, odvětvím, ve kterém se kybernetický bezpečnostní incident vyskytl, a aktuální situací v kybernetickém prostoru České republiky.
3. V případě hlášení kybernetického bezpečnostního incidentu s významným dopadem na poskytování regulované služby podle § 16 odst. 2 nebo na kybernetický prostor státu podle odstavce 2 předloží poskytovatel regulované služby nad rámec prvotního hlášení podle odstavce 1 Úřadu nebo Národnímu CERT
	1. bez zbytečného odkladu, nejpozději však do 72 hodin po zjištění kybernetického bezpečnostního incidentu oznámení, v němž aktualizuje informace uvedené v odstavci 1, předloží prvotní posouzení kybernetického bezpečnostního incidentu a uvede dopad a indikátory kompromitace, pokud jsou k dispozici; poskytovatel služeb vytvářejících důvěru[[3]](#footnote-3)) předloží oznámení podle tohoto písmene do 24 hodin od okamžiku, kdy se o tomto kybernetickém bezpečnostním incidentu dozvěděl,
	2. na žádost Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu, a
	3. nejpozději do 30 dnů od předložení oznámení podle písmene a) závěrečnou zprávu; v případě, že po uplynutí uvedené lhůty kybernetický bezpečnostní incident stále trvá, předloží poskytovatel regulované služby bez zbytečného odkladu po uplynutí lhůty průběžnou zprávu o aktuálním stavu zvládání kybernetického bezpečnostního incidentu a poté nejpozději do 30 dnů od vyřešení kybernetického bezpečnostního incidentu závěrečnou zprávu.
4. Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení podle tohoto zákona prostřednictvím Portálu NÚKIB. Nelze‑li využít Portálu NÚKIB, zašle poskytovatel regulované služby v režimu vyšších povinností hlášení na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Úřadu. Poskytovatel regulované služby v režimu nižších povinností zašle v takovém případě hlášení na adresu elektronické pošty Národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do jeho datové schránky.
5. Obsahové náležitosti, formát a způsob hlášení kybernetického bezpečnostního incidentu a náležitosti průběžné zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu a závěrečné zprávy stanoví prováděcí právní předpis.

*CELEX 32022L2555*

### § 18Zvládání kybernetických bezpečnostních incidentů

1. Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 17, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.
2. Na žádost dotčeného poskytovatele regulované služby poskytne Úřad nebo Národní CERT metodickou podporu k provádění možných zmírňujících opatření, a případnou další technickou podporu ke zvládání hlášeného kybernetického bezpečnostního incidentu s významným dopadem na poskytovatele regulované služby nebo na kybernetický prostor státu.
3. Každý je povinen poskytnout na výzvu Úřadu nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.
4. Údaje o kybernetických bezpečnostních incidentech, událostech, kybernetických hrozbách a zranitelnostech jsou vedeny v evidenci podle § 45.
5. Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených dobrovolně podle § 16 odst. 5 použijí obdobně.

*CELEX 32022L2555*

### § 19Informační povinnost poskytovatele regulované služby

1. Pokud to poskytovatel regulované služby považuje za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad je oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti.
2. Poskytovatel regulované služby je povinen bez zbytečného odkladu vhodným a srozumitelným způsobem informovat uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou, o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je to možné a vhodné, informuje poskytovatel regulované služby uživatele také o této významné kybernetické hrozbě.

*CELEX 32022L2555*

### § 20Protiopatření

1. Protiopatřeními se rozumí úkony, jichž je potřeba k ochraně aktiv před kybernetickou hrozbou nebo zranitelností v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem, anebo k řešení již nastalého kybernetického bezpečnostního incidentu.
2. Protiopatřeními jsou
	1. výstraha,
	2. varování a
	3. reaktivní protiopatření.
3. Nestanoví-li Úřad v protiopatření jinak, je poskytovatel regulované služby povinen bez zbytečného odkladu, nejpozději však ve lhůtě dané protiopatřením oznámit Úřadu provedení protiopatření a jeho výsledek. Obsahové náležitosti, formát a způsob oznámení stanoví prováděcí právní předpis. Každý je povinen poskytovat Úřadu při zajišťování podkladů pro vydání protiopatření nezbytnou součinnost. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

*CELEX 32022L2555*

### § 21Výstraha

1. Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám.
2. Úřad veřejnost o skutečnostech podle odstavce 1 informuje prostřednictvím svých internetových stránek.
3. Rozhodnutí Úřadu podle odstavce 1 může být prvním úkonem v řízení a rozklad proti němu nemá odkladný účinek.

*CELEX 32022L2555*

### § 22Varování

1. Úřad vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.
2. Poskytovatel regulované služby v režimu vyšších povinností zohlední varování v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.
3. Varování Úřad oznámí dotčeným poskytovatelům regulované služby a zveřejní jej na úřední desce Úřadu. Úřad varování nezveřejní, pokud by jeho zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle tohoto zákona, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat orgán nebo osobu, která kybernetickou hrozbu, zranitelnost nebo s tím související kybernetický bezpečnostní incident ohlásila.

*CELEX 32022L2555*

### § 23Reaktivní protiopatření

1. Úřad vydá rozhodnutí, ve kterém uloží poskytovateli regulované služby povinnost provést reaktivní protiopatření
	1. k řešení hrozícího či probíhajícího kybernetického bezpečnostního incidentu,
	2. k zabezpečení aktiv před kybernetickým bezpečnostním incidentem, nebo
	3. za účelem zvýšení ochrany aktiv na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.
2. Reaktivní protiopatření je povinen provádět poskytovatel regulované služby v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.
3. Rozhodnutí o povinnosti provést reaktivní protiopatření může být prvním úkonem v řízení. Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 72 hodin od jeho vydání, doručí se mu tak, že se vyvěsí na úřední desce Úřadu a tímto okamžikem je vykonatelné. Rozhodnutí podle věty první může Úřad vydat i v řízení na místě podle správního řádu. Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.
4. Má-li se protiopatření podle odstavce 1 týkat blíže neurčeného okruhu orgánů nebo osob, vydá jej Úřad formou opatření obecné povahy.
5. Opatření obecné povahy podle odstavce 4 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí poskytovatele regulované služby, kteří jsou jím dotčeni.
6. Dotčený poskytovatel regulované služby či kdokoliv, kdo prokáže, že jeho práva, povinnosti nebo zájmy mohou být opatřením obecné povahy přímo dotčeny, může k opatření obecné povahy vydanému podle odstavce 4 uplatnit připomínky ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.

*CELEX 32022L2555*

## Díl 3Vztah poskytovatele regulované služby a jeho dodavatelů

### § 24Řízení dodavatelů a vztah k zadávání veřejných zakázek

1. Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah.
2. Tam, kde je to možné, je poskytovatel regulované služby povinen zohlednit požadavky vyplývající z bezpečnostních opatření ve smlouvách se svými dodavateli.
3. Zohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

*CELEX 32022L2555*

### § 25Speciální úprava předání informací a dat od významného dodavatele

1. Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na podnět poskytovatele regulované služby v režimu vyšších povinností, který marně vyzval významného dodavatele ke splnění smluvního závazku předat informace a data, rozhodnutím uložit významnému dodavateli povinnost předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby. Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné po něm požadovat jejich opatření a vydání, může Úřad povinnost podle předchozí věty uložit i jinému orgánu nebo osobě, která požadovanými informacemi a daty disponuje. Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.
2. Podnět podle odstavce 1 musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi významným dodavatelem a poskytovatelem regulované služby v režimu vyšších povinností zejména s ohledem na nesplnění smluvního závazku významného dodavatele a možné následky, pokud nedojde k předání požadovaných informací a dat.
3. Rozhodnutí o uložení povinnosti předat informace a data podle odstavce 1 může být prvním úkonem v řízení. Rozklad proti rozhodnutí podle věty první nemá odkladný účinek.
4. Jednání o úhradě vynaložených nákladů na předání informací a dat nesmí být překážkou řádného splnění povinnosti předat informace a data.

*CELEX 32022L2555*

## Díl 4Strategicky významná služba

### § 26Kritéria strategicky významné služby

Strategicky významná služba je stanovena kritérii pro identifikaci strategicky významné služby ve vymezených odvětvích nebo kritérii pro určení strategicky významné služby.

*CELEX 32022L2555*

### § 27Kritéria pro identifikaci a určení strategicky významné služby

1. Prováděcí právní předpis stanoví kritéria pro identifikaci strategicky významné služby v odvětvích
	1. veřejná správa,
	2. energetika,
	3. doprava a
	4. digitální infrastruktura a služby.
2. Strategicky významnou službou je dále regulovaná služba stanovená u poskytovatele regulované služby v režimu vyšších povinností rozhodnutím Úřadu v případě, že by narušení bezpečnosti informací regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek.

*CELEX 32022L2555*

## Díl 5Mechanismus prověřování bezpečnosti dodavatelského řetězce

### Prověřování rizik spojených s dodavatelem§ 28

1. Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele.
2. Činnosti podle odstavce 1 prioritizuje Úřad podle přístupu založeného na rizicích a dostupných kapacitách.
3. Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí
	1. kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem,
	2. bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu
		1. technického prostředku nebo vybavení s výpočetní kapacitou,
		2. programového prostředku nebo vybavení, nebo
		3. informační či komunikační služby,
	3. dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.
4. Nepominutelné funkce stanoveného rozsahu a kritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní předpis.

*CELEX 32022L2555*

### § 29

1. Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů stanovisko o naplnění kritéria rizikovosti dodavatele konkrétním orgánem či osobou, informace nebo jinou součinnost.
2. Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky za účelem výkonu činnosti podle § 28 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů požadované informace nebo jinou součinnost.
3. Nezíská-li Úřad z vlastní činnosti nebo postupem podle odstavce 1 a 2 informace potřebné pro výkon činnosti podle § 28 odst. 1, poskytnou na základě žádosti Úřadu tyto informace nebo jinou součinnost orgány a osoby neuvedené v odstavci 1 a 2.
4. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu. Tím není dotčena povinnost mlčenlivosti advokáta podle právního předpisu upravujícího výkon advokacie.

*CELEX 32022L2555*

### § 30Omezení rizik spojených s dodavatelem

1. Úřad vydá opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby.
2. Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány uvedenými v § 29 odst. 1 a 2 a Ministerstvem financí předloží Bezpečnostní radě státu
	1. pro informaci, jestliže lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky
		1. je stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu[[4]](#footnote-4)), jestliže ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo
		2. je alespoň 5 let, nebo
	2. k projednání, jestliže lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky
		1. není stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu4), jestliže ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo
		2. je kratší než 5 let.
3. Po informování členů Bezpečnostní rady státu podle odstavce 2 písmene a) nebo po projednání podle odstavce 2 písm. b) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.
4. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 1. Zjistí-li Úřad, že tyto skutečnosti pominuly, zruší opatření obecné povahy podle odstavce 1 postupem podle odstavce 1 a 2 obdobně.

*CELEX 32022L2555*

### § 31Výjimky z omezení rizik spojených s dodavatelem

1. Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § 30, jestliže by plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.
2. Řízení o povolení výjimky podle odstavce 1 lze zahájit na žádost poskytovatele strategicky významné služby nebo z moci úřední. Žadatel je povinen v rámci žádosti připojit důkazy prokazující skutečnosti, kterých se dovolává.
3. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší.
4. Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § 30.

*CELEX 32022L2555*

### § 32Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce

1. Poskytovatel strategicky významné služby je povinen
	1. zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a evidovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, a
	2. hlásit Úřadu informace podle písmena a) a jejich změny do 10 dnů od jejich zjištění; obsahové náležitosti, formát a způsob hlášení stanoví prováděcí právní předpis.
2. Poskytovatel strategicky významné služby začne plnit povinnost hlásit informace podle odstavce 1 pro každou strategicky významnou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § 10 odst. 1.
3. Informace ohlášené Úřadu podle odstavce 1 písm. b) a odstavce 2 a informace zjištěné postupem podle § 28 a § 29 jsou součástí evidence dodavatelů bezpečnostně významných dodávek.

*CELEX 32022L2555*

### § 33Omezení rizik spojených s dodavatelem ve veřejných zakázkách

Poskytovatel strategicky významné služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek může závazek ze smlouvy na veřejnou zakázku vypovědět bez zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by nebylo porušeno opatření obecné povahy podle § 30.

*CELEX 32022L2555*

## Díl 6Zajištění dostupnosti strategicky významné služby

### § 34

1. Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.
2. Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby v rozsahu kritické části stanoveného rozsahu z území České republiky nejméně jednou za dva roky.
3. Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2.
4. Stanovený čas a kvalitu služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu.
5. Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a).

*CELEX 32022L2555*

## HLAVA IIISubjekt poskytující službu registrace jmen domén

### Povinnosti subjektů poskytujících služby registrace jmen domén§ 35

1. Subjekt poskytující služby registrace jmen domén hlásí Úřadu bez zbytečného odkladu, nejpozději však do 30 dnů ode dne, kdy začal poskytovat službu registrace jmen domén, způsobem stanoveným prováděcím právním předpisem
	1. název subjektu,
	2. adresu hlavní provozovny a jeho dalších provozoven na území členských států Evropské unie, případně zástupce subjektu podle § 67,
	3. aktuální kontaktní údaje včetně e-mailových adres a telefonních čísel subjektu, případně jeho zástupce podle § 67,
	4. členské státy Evropské unie, v nichž subjekt poskytuje své služby a
	5. rozsah veřejných IP adres subjektu.
2. V případě změn v údajích nahlášených podle odstavce 1 aktualizuje subjekt poskytující služby registrace jmen domén nahlášené údaje bez zbytečného odkladu, nejpozději však do 90 dnů ode dne změny.

*CELEX 32022L2555*

### § 36

1. Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén shromažďují a uchovávají přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi v souladu s právními předpisy upravujícími ochranu osobních údajů, pokud jde o údaje, které jsou osobními údaji.
2. Databáze podle odstavce 1 obsahuje informace nezbytné k identifikaci a kontaktování držitelů jmen domén a kontaktních míst spravujících domény nejvyšší úrovně, a to zejména
	1. jméno domény,
	2. datum registrace,
	3. jméno žadatele o registraci,
	4. e-mailovou adresu žadatele o registraci,
	5. telefonní číslo žadatele o registraci,
	6. e-mailovou adresu a telefonní číslo kontaktního místa spravujícího jméno domény v případě, že se liší od žadatele o registraci.
3. Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén zavádí zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování. Tyto zásady a postupy jsou veřejně dostupné.
4. Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén bez zbytečného odkladu po registraci jména domény uveřejní její registrační údaje, které nejsou osobními údaji.
5. Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén poskytují přístup ke konkrétním údajům o registraci jména domény na základě zákonných a řádně odůvodněných žádostí oprávněných žadatelů o přístup v souladu s právními předpisy Evropské unie upravujícími ochranu osobních údajů, a to bez zbytečného odkladu, nejpozději do 72 hodin od žádosti o přístup. Zásady a postupy pro zveřejňování těchto údajů jsou veřejně dostupné.

*CELEX 32022L2555*

## HLAVA IVDalší nástroje zajišťování kybernetické bezpečnosti

### § 37Výjimka z práva na informace

Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidencích vedených Úřadem podle § 45, se podle právních předpisů upravujících svobodný přístup k informacím neposkytují.

### § 38Stav kybernetického nebezpečí

Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v kybernetickém prostoru, což by mohlo vést nebo vedlo k ohrožení zájmu České republiky. Tímto zájmem je zejména zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního či veřejného pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky, života, zdraví nebo majetku a životního prostředí a zajištění funkčnosti regulovaných služeb.

### § 39Vyhlášení stavu kybernetického nebezpečí

1. Stav kybernetického nebezpečí lze vyhlásit jen s uvedením důvodů a na nezbytně nutnou dobu. Stav kybernetického nebezpečí vyhlašuje ředitel Úřadu. Ředitel Úřadu o vyhlášení stavu kybernetického nebezpečí neprodleně informuje vládu. Stav kybernetického nebezpečí lze vyhlásit na dobu nejvýše 30 dnů. Tuto dobu může ředitel Úřadu prodloužit jen se souhlasem vlády.
2. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí musí obsahovat opatření k řešení stavu kybernetického nebezpečí a jejich rozsah. Rozhodnutí se zveřejňuje na úřední desce Úřadu a dalšími vhodnými způsoby, zejména prostřednictvím hromadných informačních prostředků. Provozovatel celoplošného televizního nebo rozhlasového vysílání je povinen na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí. Rozhodnutí nabývá účinnosti okamžikem, který se v něm stanoví. Změna opatření k řešení stavu kybernetického nebezpečí musí být vyhlášena obdobným způsobem jako stav kybernetického nebezpečí.
3. Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud ředitel Úřadu nebo vláda nerozhodnou o jeho zrušení před uplynutím této doby. Vláda stav kybernetického nebezpečí zruší též, pokud nejsou splněny podmínky pro jeho vyhlášení. Rozhodnutí ředitele Úřadu nebo vlády o zrušení stavu kybernetického nebezpečí se zveřejní na úřední desce Úřadu a dalšími vhodnými způsoby, zejména prostřednictvím hromadných informačních prostředků. Toto rozhodnutí nabývá účinnosti okamžikem, který se v něm stanoví.
4. Není-li možné účelně odvrátit vzniklé ohrožení v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu. Platnost opatření k řešení stavu kybernetického nebezpečí vyhlášených ředitelem Úřadu končí dnem vyhlášení nouzového stavu, pokud vláda nerozhodne jinak. Opatření k řešení stavu kybernetického nebezpečí, jejichž platnost zůstane zachována, se dále považují za krizová opatření nařízená vládou.
5. Na rozhodování a ukládání povinností podle tohoto zákona se v době stavu kybernetického nebezpečí nevztahuje správní řád.

### § 40Opatření k řešení stavu kybernetického nebezpečí

1. Ředitel Úřadu je v době stavu kybernetického nebezpečí za účelem jeho řešení oprávněn
	1. poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad, a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu, nebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem,
	2. vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních kapacitách a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě,
	3. vyžádat si na základě smlouvy nebo zápisu o sdílení personálních kapacit a věcných prostředků přednostní poskytnutí personálních kapacit nebo věcných prostředků a tyto personální zdroje a věcné prostředky využít, přičemž dožádané orgány a osoby mají povinnost žádosti Úřadu vyhovět,
	4. nařídit práci v pohotovostním režimu,
	5. zakázat orgánům a osobám, které k tomu byly Úřadem vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena,
	6. uložit orgánům či osobám povinnost provést opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu,
	7. nařídit orgánům a osobám provedení skenu zranitelností nebo penetračního testu, nebo
	8. nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu.
2. Za stavu kybernetického nebezpečí jsou orgány a osoby, které k tomu byly na základě vydaných opatření Úřadem vyzvány, povinny
	1. splnit opatření sloužící k řešení a nápravě stavu kybernetického nebezpečí,
	2. poskytnout součinnost při provádění skenu zranitelnosti nebo penetračního testu,
	3. poskytnout součinnost při zveřejňování informací o stavu kybernetického nebezpečí, nebo
	4. poskytnout součinnost při řešení a nápravě stavu kybernetického nebezpečí.

## HLAVA VVýkon státní správy

## Díl 1Instituce zapojené do výkonu státní správy v oblasti kybernetické bezpečnosti

### § 41Národní úřad pro kybernetickou a informační bezpečnost

1. Úřad je ústředním správním úřadem pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. Úřad se svou činností podílí na posilování bezpečnosti a odolnosti České republiky v kybernetickém prostoru. Sídlem Úřadu je Brno. Příjmy a výdaje Úřadu tvoří samostatnou kapitolu státního rozpočtu.
2. V čele Úřadu je ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává. Ředitel Úřadu je odpovědný předsedovi vlády nebo pověřenému členu vlády.
3. Úřad
	1. přijímá informace o naplnění kritérií pro identifikaci regulované služby a registruje poskytovatele regulovaných služeb,
	2. určuje rozhodnutím poskytovatele regulované služby a regulovanou službu, pokud naplní kritéria pro určení regulované služby,
	3. určuje rozhodnutím strategicky významnou službu podle § 27 odst. 2,
	4. zapisuje poskytovatele regulované služby do evidence poskytovatelů regulovaných služeb a provádí výmaz poskytovatele regulované služby z této evidence,
	5. rozhodnutím mění ve stanovených případech režim poskytovatele regulované služby,
	6. přijímá hlášení registračních, kontaktních a doplňujících údajů a jejich změn,
	7. stanoví bezpečnostní opatření odpovídající režimu poskytovatele regulované služby,
	8. spravuje a provozuje Portál NÚKIB,
	9. v souladu s postupy podle tohoto zákona informuje veřejnost o kybernetickém bezpečnostním incidentu*,*
	10. vydává protiopatření a přijímá oznámení o jejich provedení a výsledku,
	11. vede evidence a seznamy podle tohoto zákona a podle právních předpisů upravujících ochranu utajovaných informací,
	12. vydává rozhodnutí o povinnosti předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby,
	13. shromažďuje a vyhodnocuje informace a data podle § 28 odst. 1,
	14. stanovuje opatřením obecné povahy podmínky nebo zakazuje využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu,
	15. přezkoumává trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle písmene n),
	16. rozhoduje o žádostech o výjimku a povoluje výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § 31,
	17. sjednává s orgány a osobami smlouvy a zápisy o sdílení personálních kapacit a věcných prostředků za účelem plnění zákonných pravomocí Úřadu,
	18. vyhlašuje, řídí a koordinuje stav kybernetického nebezpečí, ukládá povinnosti a přijímá opatření k odvrácení stavu kybernetického nebezpečí a působí jako koordinační orgán za stavu kybernetického nebezpečí,
	19. během stavu kybernetického nebezpečí vyhlašuje opatření určená k řešení a nápravě stavu kybernetického nebezpečí,
	20. kontinuálně se připravuje na zajištění připravenosti na řešení a nápravu stavu kybernetického nebezpečí,
	21. uzavírá veřejnoprávní smlouvu s provozovatelem Národního CERT,
	22. provádí kontrolu plnění povinností podle tohoto zákona a ukládá nápravná opatření,
	23. ukládá správní sankce za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,
	24. provádí kontrolu plnění povinností podle tohoto zákona a poskytuje jinou nezbytnou součinnost na základě žádosti dozorového orgánu jiného členského státu,
	25. vydává rozhodnutí o pozastavení platnosti evropského certifikátu kybernetické bezpečnosti nebo o povinnosti subjektu posuzování shody pozastavit platnost certifikátu nebo osvědčení podle § 60,a
	26. podává soudu návrh na pozastavení výkonu řídicí funkce podle § 61a vydává osvědčení podle téhož ustanovení.
4. Úřad dále
	1. provádí analýzu a monitoring kybernetických hrozeb a rizik,
	2. zpracovává a vládě předkládá ke schválení národní strategii kybernetické bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,
	3. vykonává státní správu v oblasti bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi a v oblasti kryptografické ochrany, zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí,
	4. v oblasti kybernetické bezpečnosti, ve vybraných oblastech ochrany utajovaných informací a v souvislosti s nimi
		1. spolupracuje s orgány a osobami, které působí v těchto oblastech a v oblasti kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT,
		2. zajišťuje mezinárodní spolupráci a sjednává a uzavírá smlouvy o mezinárodní spolupráci,
		3. plní další úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána,
		4. zajišťuje prevenci, vzdělávání a metodickou podporu a
		5. zajišťuje výzkum a vývoj,
	5. podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu určuje prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti nebo zasílá Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu, a každé 2 roky ověřuje jejich aktuálnost,
	6. plní povinnosti vůči Evropské komisi, Agentuře Evropské unie pro kybernetickou bezpečnost, Skupině pro spolupráci, Síti CSIRT, Evropské síti styčných organizací pro řešení kybernetických krizí a dalším subjektům podle příslušného předpisu Evropské unie,
	7. je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie a je příslušným orgánem v České republice podle příslušného předpisu Evropské unie,
	8. v případě potřeby se podílí na procesu vzájemného hodnocení podle příslušného předpisu Evropské unie,

 *CELEX 32022L2555*

* 1. vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo, zejména plní funkce příslušného orgánu PRS podle čl. 5 rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU,

*CELEX 32011D1104*

* 1. vykonává působnost v dílčích oblastech souvisejících s bezpečností v rámci Kosmického programu Unie podle nařízení Evropského parlamentu a Rady č. 2021/696,

*CELEX 32021R0696*

* 1. je vnitrostátním orgánem certifikace kybernetické bezpečnosti podle čl. 58 aktu o kybernetické bezpečnosti,

*CELEX 32019R0881*

* 1. působí jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti pro Českou republiku podle přímo použitelného předpisu Evropské unie[[5]](#footnote-5)),

*CELEX 32021R0887*

* 1. zřizuje a podporuje platformy sloužící ke sdílení informací v oblasti kybernetické bezpečnosti a stanovuje pravidla jejich fungování,

*CELEX 32022L2555*

* 1. vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách a
	2. plní další úkoly stanovené tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti.
1. Vládní CERT jako součást Úřadu
	1. zajišťuje řešení, koordinaci, analýzu a preventivní působení vůči
		1. hrozbám v oblasti kybernetické bezpečnosti,
		2. zranitelnostem v oblasti kybernetické bezpečnosti, včetně vyhledávání zranitelností,
		3. kybernetickým bezpečnostním událostem a
		4. kybernetickým bezpečnostním incidentům, včetně jejich zvládání,
	2. působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu vyšších povinností,
	3. testuje zavedení a odolnost zabezpečení aktiv, včetně provádění penetračního testování se souhlasem dotčených orgánů či osob,
	4. je koordinátorem pro účely koordinovaného zveřejňování zranitelností,
	5. vede evidenci kybernetických bezpečnostních incidentů, událostí, kybernetických hrozeb a zranitelností,
	6. spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti,
	7. poskytuje orgánům a osobám konzultace v oblasti kybernetické bezpečnosti,
	8. přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti od orgánů a osob,
	9. může s orgány a osobami sdílet údaje a informace ze své činnosti a z evidencí vedených Úřadem, je-li to nezbytné pro zajišťování kybernetické bezpečnosti; pokud Vládní CERT stanoví úroveň ochrany takto sdílených informací, orgány a osoby mají povinnost tuto úroveň ochrany dodržovat,
	10. plní roli CSIRT týmu podle příslušného předpisu Evropské unie a zastupuje Českou republiku a podílí se na fungování relevantních mezinárodních uskupení a sdružení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,
	11. ve vhodných případech předává bez zbytečného odkladu informace o kybernetickém bezpečnostním incidentu s významným dopadem týkajícím se dvou nebo více členských států nahlášeném podle § 16 a § 17 dotčeným členským státům a Agentuře Evropské unie pro kybernetickou bezpečnost, přičemž zachovává důvěrnost poskytnutých informací, bezpečnost a obchodní zájmy ohlašovatele subjektu,
	12. se podílí na výzkumu a vývoji kybernetických bezpečnostních nástrojů a řešení a
	13. prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných kapacitách.

*CELEX 32022L2555*

### § 42Provozovatel Národního CERT

1. Provozovatelem Národního CERT může být pouze právnická osoba, která
	1. nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu právních předpisů upravujících ochranu utajovaných informací,
	2. spravuje a provozuje relevantní technická aktiva anebo se na jejich správě a provozu podílí, a to nejméně po dobu 5 let,
	3. má technické předpoklady k výkonu činností podle odstavce 3,
	4. je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,
	5. nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek a nemá v České republice splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění a na pojistném nebo na penále na sociální zabezpečení nebo příspěvku na státní politiku zaměstnanosti,
	6. nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,
	7. není zahraniční osobou podle jiného právního předpisu,
	8. nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele Národního CERT vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností uvedených v odstavci 3 a
	9. uzavřela s Úřadem veřejnoprávní smlouvu podle § 52.
2. Zájemce prokazuje splnění podmínek předložením
	1. čestného prohlášení v případě odstavce 1 písm. a) až d), g) a h) z jehož obsahu musí být zřejmé, že uchazeč splňuje příslušné předpoklady, a
	2. potvrzení příslušných orgánů Finanční správy České republiky, Celní správy České republiky, České správy sociálního zabezpečení a příslušné pojišťovny v případě odstavce 1 písm. e), která nesmí být starší než 30 dnů.
3. Provozovatel Národního CERT vykonává činnost Národního CERT, který
	1. zajišťuje v rozsahu podle tohoto zákona sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti a působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu nižších povinností,
	2. přijímá hlášení o kybernetických bezpečnostních incidentech, kybernetických bezpečnostních událostech, kybernetických hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti a tyto údaje vyhodnocuje, zaznamenává, uchovává a chrání,
	3. poskytovatelům regulovaných služeb v režimu nižších povinností poskytuje metodickou podporu, pomoc a součinnost při výskytu a zvládání kybernetického bezpečnostního incidentu s významným dopadem a při zveřejňování informací o zranitelnostech v oblasti kybernetické bezpečnosti,
	4. provádí vyhledávání a hodnocení zranitelností v oblasti kybernetické bezpečnosti,
	5. předává Úřadu údaje o nahlášených kybernetických hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech podle § 16 a zranitelnostech v oblasti kybernetické bezpečnosti,
	6. informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování regulované služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a soukromoprávní zájmy ohlašovatele,
	7. přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti od orgánů a osob,
	8. plní roli CSIRT týmu podle příslušného předpisu Evropské unie a podílí se na fungování mezinárodních uskupení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,
	9. se v případě potřeby podílí na procesu vzájemného hodnocení podle příslušného předpisu Evropské unie a
	10. prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných kapacitách.
4. Provozovatel Národního CERT při plnění povinností uvedených v odstavci 3 postupuje nestranně a koordinuje svou činnost s Úřadem.
5. Provozovatel Národního CERT vykonává činnosti podle odstavce 3 písm. a), b) a e) až h) bezúplatně. Provozovatel Národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v odstavci 3 nezbytné náklady.
6. Úřad zveřejní na svých internetových stránkách údaje o provozovateli Národního CERT, a to jeho obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.

*CELEX 32022L2555*

### § 43Stálá komise pro kontrolu činnosti Úřadu

1. Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán (dále jen „kontrolní orgán“).
2. Kontrolní orgán se skládá nejméně ze 7 členů. Poslanecká sněmovna stanoví počet členů tak, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách; počet členů je vždy lichý. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.
3. Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jiný právní předpis[[6]](#footnote-6)).
4. Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.
5. Ředitel Úřadu předkládá kontrolnímu orgánu
	1. zprávu o činnosti Úřadu,
	2. návrh rozpočtu Úřadu,
	3. podklady potřebné ke kontrole plnění rozpočtu Úřadu,
	4. vnitřní předpisy Úřadu,
	5. na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech poskytovatelů regulovaných služeb.
6. Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody občanů nebo že rozhodovací činnost Úřadu v rámci správního řízení je stižena vadami, je oprávněn požadovat od ředitele Úřadu potřebné vysvětlení.
7. Každé porušení zákona zaměstnancem Úřadu při plnění povinností podle tohoto zákona a ve vybraných oblastech podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli Úřadu a předsedovi vlády.
8. Povinnost zachovávat mlčenlivost uloženou členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle odstavce 7.

## Díl 2Nástroje výkonu státní správy

### § 44Portál NÚKIB

1. Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona.
2. Úkony podle § 8 odst. 1, § 9 odst. 1, § 12 odst. 1, § 16 odst. 1 a 2, § 20 odst. 3, § 32 odst. 1 písm. b) a § 57 odst. 1 je poskytovatel regulované služby povinen provádět výlučně elektronicky s využitím dálkového přístupu prostřednictvím formulářových podání. Jiným způsobem lze tyto úkony provést pouze, připouští‑li to odpovídající ustanovení tohoto zákona a není-li z objektivních příčin možné využít k provedení úkonu Portál NÚKIB. Úkon, který nebude proveden tímto způsobem, ve formátu a struktuře stanovené prováděcím právním předpisem, je neúčinný.
3. Technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provedení úkonů podle odstavce 2 stanoví prováděcí právní předpis.

*CELEX 32022L2555*

### § 45Evidence vedené Úřadem

1. Úřad vede evidenci
	1. poskytovatelů regulovaných služeb, subjektů poskytujících služby registrace jmen domén a jimi hlášených údajů,
	2. kybernetických bezpečnostních incidentů, událostí, kybernetických hrozeb a zranitelností,
	3. dodavatelů bezpečnostně významných dodávek,
	4. koordinovaného zveřejňování zranitelností,
	5. penetračních testů a
	6. provedených kontrol a protokolů o kontrole.
2. Úřad poskytuje v odůvodněných případech údaje z evidencí orgánům veřejné moci na jejich žádost, je-li to nezbytné pro výkon jejich působnosti. Poskytnuté údaje je možné využít jen pro potřeby, které byly uvedeny v žádosti. Žadatel vynaloží přiměřené úsilí k zajištění bezpečnosti informací takto poskytnutých údajů.
3. Úřad může v odůvodněných případech poskytovat údaje z evidencí Národnímu CERT, orgánům nebo osobám vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným orgánům nebo osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.
4. Zaměstnanci Úřadu jsou vázáni povinností mlčenlivosti o údajích z evidencí podle odstavce 1 písm. b) až e). Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu. Ředitel Úřadu může osoby uvedené v tomto odstavci zprostit povinnosti mlčenlivosti, a to s uvedením rozsahu údajů a rozsahu zproštění.

### § 46Autorizace subjektů posuzování shody podle aktu o kybernetické bezpečnosti

1. Stanoví-li přímo použitelný předpis Evropské unie vydaný na základě aktu o kybernetické bezpečnosti konkrétní nebo dodatečné požadavky na subjekty posuzování shody s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost, Úřad v souladu s čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti rozhoduje o žádostech o autorizaci subjektu posuzování shody, a pokud autorizovaný subjekt posuzování shody porušuje požadavky aktu o kybernetické bezpečnosti nebo přímo použitelného předpisu Evropské unie vydaného na základě aktu o kybernetické bezpečnosti, o pozastavení vykonatelnosti, o změně nebo o zrušení rozhodnutí o autorizaci.
2. Subjekt posuzování shody v žádosti o autorizaci podle odstavce 1 doloží plnění konkrétních nebo dodatečných požadavků stanovených přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti.
3. V rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci podle odstavce 1 stanoví Úřad lhůtu pro zjednání nápravy. Zjedná-li subjekt posuzování shody nápravu, sdělí tuto skutečnost bez zbytečného odkladu Úřadu. Shledá-li Úřad zjednání nápravy za dostačující, zruší rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci. Jestliže autorizovaný subjekt posuzování shody ve stanovené lhůtě nezjedná nápravu, rozhodne Úřad o změně či zrušení rozhodnutí o autorizaci.
4. Úřad rozhodne v řízení o žádosti o autorizaci podle odstavce 1 nejdéle do 120 dnů od zahájení řízení, v mimořádných případech do 180 dnů.

*CELEX 32019R0881*

### § 47Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti

1. Úřad jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti posuzuje podle přímo použitelného předpisu Evropské unie[[7]](#footnote-7)) způsobilost žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost[[8]](#footnote-8)) (dále jen „Komunita“).
2. Registrovaným členem Komunity může být pouze žadatel o registraci členství v Komunitě (dále jen „žadatel“), který Úřadu prokáže
	1. základní způsobilost žadatele a
	2. zvláštní způsobilost žadatele.
3. Žádost o registraci členství v Komunitě (dále jen „žádost“) se podává elektronicky prostřednictvím formuláře zveřejněného na internetových stránkách Úřadu.
4. Žadatel je povinen v žádosti uvést pravdivé a úplné údaje potřebné pro posouzení jeho základní a zvláštní způsobilosti Úřadem. Po dobu trvání členství v Komunitě je povinen žadatel, který byl registrovaný jako člen Komunity, nahlásit změnu těchto údajů, nebo skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti, a to ve lhůtě 30 dnů ode dne, kdy tato změna nebo skutečnost nastala, nebo se o ní žadatel dozvěděl.

*CELEX 32021R0887*

### § 48Základní způsobilost žadatele o registraci členství v Komunitě

1. Žadatel má základní způsobilost, pokud
	1. má sídlo nebo místo podnikání na území České republiky,
	2. není zapsaný na vnitrostátním sankčním seznamu[[9]](#footnote-9)),
	3. nebyl v posledních 5 letech před podáním žádosti pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání žadatele, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných; k zahlazeným odsouzením se nepřihlíží,
	4. nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek,
	5. nemá v České republice splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
	6. nemá v České republice splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a
	7. není v likvidaci[[10]](#footnote-10)), nebylo proti němu vydáno rozhodnutí o úpadku[[11]](#footnote-11)) a nebyla vůči němu nařízena nucená správa podle jiného právního předpisu[[12]](#footnote-12)).
2. Žadatel prokazuje splnění podmínek základní způsobilosti podle odstavce 1 předložením
	1. výpisu z evidence Rejstříku trestů ve vztahu k odstavci 1 písm. c), který nesmí být starší než 3 měsíce,
	2. potvrzení příslušného finančního úřadu ve vztahu k odstavci 1 písm. d), které nesmí být starší než 30 kalendářních dnů přede dnem podání žádosti,
	3. písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k odstavci 1 písm. d),
	4. písemného čestného prohlášení ve vztahu k odstavci 1 písm. e) a
	5. potvrzení příslušné okresní správy sociálního zabezpečení ve vztahu k odstavci 1 písm. f), které nesmí být starší než 30 kalendářních dnů přede dnem podání žádosti.
3. U žadatele, je-li právnickou osobou, Úřad zjistí údaje o jeho skutečném majiteli podle právního předpisu upravujícího evidenci skutečných majitelů[[13]](#footnote-13)) (dále jen „skutečný majitel“) z evidence skutečných majitelů podle téhož zákona (dále jen „evidence skutečných majitelů“).
4. Žadatel není způsobilý, pokud
	1. je právnickou osobou, která má skutečného majitele, pokud nebylo podle odstavce 3 možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů,
	2. skutečným majitelem je osoba usazená mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, nebo
	3. skutečným majitelem je osoba uvedená na vnitrostátním sankčním seznamu8).
5. Je-li žadatelem právnická osoba, musí podmínku podle odstavce 1 písm. c) splňovat tato právnická osoba a zároveň každý člen jejího statutárního orgánu. Je-li členem statutárního orgánu žadatele právnická osoba, musí podmínku podle odstavce 1 písm. c) splňovat
	1. tato právnická osoba,
	2. každý člen statutárního orgánu této právnické osoby a
	3. osoba zastupující tuto právnickou osobu ve statutárním orgánu žadatele.
6. Žadatel není způsobilý, pokud Úřad vydal opatření obecné povahy podle § 30 odst. 1, ve kterém stanovil podmínky pro využití plnění žadatele nebo zakázal využití plnění žadatele jako dodavatele bezpečnostně významné dodávky.

*CELEX 32021R0887*

### § 49Zvláštní způsobilost žadatele o registraci členství v Komunitě

Zvláštní způsobilost má žadatel, který prokáže, že je způsobilý k registraci podle přímo použitelného předpisu Evropské unie[[14]](#footnote-14)).

*CELEX 32021R0887*

### § 50Posouzení způsobilosti žadatele o registraci členství v Komunitě

1. V případě, že žadatel splní podmínky podle § 47 odst. 2, Úřad postoupí žádost žadatele registrujícímu orgánu podle přímo použitelného předpisu Evropské unie[[15]](#footnote-15)) (dále jen „registrující orgán“).
2. V případě pochybností, zda žadatel splňuje podmínky podle § 47 odst. 2, zahájí Úřad řízení o nezpůsobilosti žadatele k registraci členství v Komunitě.
3. Po právní moci rozhodnutí o nezpůsobilosti žadatele k registraci členství v Komunitě vydaného v řízení podle odstavce 2 Úřad postoupí registrujícímu orgánu žádost žadatele a současně vyrozumí registrující orgán o nezpůsobilosti žadatele k registraci členství v Komunitě.

*CELEX 32021R0887*

### § 51Způsobilost žadatele k členství v Komunitě

1. Úřad průběžně posuzuje plnění požadavků podle § 47 odst. 2 po celou dobu trvání členství žadatele v Komunitě, jehož žádosti o registraci v Komunitě bylo registrujícím orgánem vyhověno.
2. V případě, že žadatel, který je registrovaný jako člen Komunity, nesplňuje podmínky podle § 47 odst. 2, zahájí Úřad řízení o nezpůsobilosti žadatele k členství v Komunitě.
3. Po právní moci rozhodnutí o nezpůsobilosti žadatele k členství v Komunitě vydaného v řízení podle odstavce 2 Úřad vyrozumí registrující orgán o nezpůsobilosti žadatele k členství v Komunitě.

*CELEX 32021R0887*

### § 52Veřejnoprávní smlouva s provozovatelem Národního CERT

1. Úřad uzavírá veřejnoprávní smlouvu s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 42 odst. 3 (dále jen „veřejnoprávní smlouva“). Řízení o výběru žádosti vyhlašuje Úřad.
2. Veřejnoprávní smlouva obsahuje alespoň
	1. označení smluvních stran,
	2. vymezení předmětu smlouvy,
	3. práva a povinnosti smluvních stran,
	4. podmínky spolupráce smluvních stran,
	5. způsob a podmínky odstoupení smluvních stran od veřejnoprávní smlouvy,
	6. výpovědní lhůtu a výpovědní důvody,
	7. zákaz zneužití údajů získaných v souvislosti s výkonem činností uvedených v § 42 odst. 3,
	8. vymezení podmínek pro výkon činnosti Národního CERT podle § 42 odst. 1 písm. h)*,* a
	9. způsob předání a rozsah údajů předávaných Úřadu v případě zániku závazku.
3. Veřejnoprávní smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje ve Věstníku Úřadu, s výjimkou těch částí veřejnoprávní smlouvy, jejichž zveřejnění neumožňuje jiný právní předpis.
4. Není-li uzavřena veřejnoprávní smlouva podle odstavce 1, nebo v případě zániku závazku, vykonává činnost Národního CERT Úřad.

### § 53Zpracování osobních údajů

1. Úřad a provozovatel Národního CERT zpracovávají osobní údaje, jsou‑li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad a provozovatel Národního CERT předávají orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich úkolů a nedojde-li tím k porušení povinnosti mlčenlivosti podle tohoto zákona.
2. Úřad a provozovatel Národního CERT při zpracování osobních údajů, na které se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů,
	1. nemusí omezit zpracování osobních údajů v případě, že subjekt údajů popírá jejich přesnost nebo vznesl námitku proti tomuto zpracování a
	2. mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny.
3. Pokud Úřad nebo provozovatel Národního CERT v rámci činnosti, na kterou se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události, při prevenci kybernetických hrozeb nebo rizik anebo při výkonu kontroly obdrží osobní údaje, které zpracovávají pouze za účelem plnění povinností podle tohoto zákona, po dobu plnění těchto povinností dále nemusí
	1. poskytovat subjektu údajů informace o opravách nebo výmazech osobních údajů nebo omezení jejich zpracování,
	2. zajistit přístup subjektu údajů k osobním údajům, nebo
	3. opravit či doplnit osobní údaje na žádost subjektu údajů.

*CELEX 32022L2555*

### § 54Vzájemná součinnost s členskými státy Evropské unie

1. Úřad spolupracuje při uplatňování tohoto zákona s příslušnými orgány jiných členských států Evropské unie (dále jen „jiný členský stát“), zejména může poskytovat a žádat o součinnost ve formě
	1. sdílení informací,
	2. provedení kontroly nebo jiných úkonů vůči poskytovateli regulované služby, nebo
	3. koordinace při kontrolách poskytovatelů regulovaných služeb poskytujících regulované služby ve více členských státech, včetně možnosti přizvání zástupců příslušných orgánů jiného členského státu k účasti na kontrole.
2. Úřad může žádost o součinnost odmítnout pouze
	1. není-li příslušný nebo nemá-li pravomoc provést požadovaný úkon,
	2. je-li žádost o součinnost s ohledem na kapacity Úřadu zjevně nepřiměřená, nebo
	3. týká-li se žádost informací nebo zahrnuje-li činnosti, které by v případě zveřejnění nebo provedení byly v rozporu se zásadními zájmy České republiky v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.
3. Poskytuje-li poskytovatel regulované služby, který má sídlo v jiném členském státě Evropské unie, v rámci České republiky službu
	1. překladu jmen domén (DNS),
	2. správy a provozu registru internetových domén nejvyšší úrovně,
	3. cloud computingu,
	4. datového centra,
	5. sítě pro doručování obsahu (CDN),
	6. on-line tržiště,
	7. internetového vyhledávače,
	8. platformy sociální sítě,
	9. řízené služby (MSP), nebo
	10. řízené bezpečnostní služby (MSSP),

je Úřad oprávněn vůči této osobě provést kontrolu nebo jiný úkon na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.

1. Nachází-li se v rámci České republiky aktiva sloužící k poskytování některé ze služeb uvedených v odstavci 3, ale poskytovatel regulované služby má umístěnu svou hlavní provozovnu v jiném členském státě, je Úřad oprávněn ve vztahu k těmto aktivům sloužícím k poskytování těchto služeb provést kontrolu nebo jiný úkon na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.
2. Umístěním hlavní provozovny se rozumí místo v Evropské unii, kde osoba poskytující služby uvedené v odstavci 3 převážně přijímá rozhodnutí související s řízením rizik v oblasti kybernetické bezpečnosti. Nelze-li takové místo určit podle věty první, nebo nejsou-li taková rozhodnutí přijímána v Evropské unii, má se za to, že je hlavní provozovna umístěna v členském státě Evropské unie, kde se provádějí faktické úkony vedoucí k zajištění kybernetické bezpečnosti. Nelze-li takové místo určit podle věty první a druhé, má se za to, že je hlavní provozovna umístěna v členském státě Evropské unie, kde má osoba provozovnu s nejvyšším počtem zaměstnanců.
3. Ustanovení odstavce 3 se uplatní i vůči subjektu poskytujícímu službu registrace doménových jmen v rámci České republiky.

*CELEX 32022L2555*

### § 55Prováděcí právní předpisy a zmocňovací ustanovení

1. Prováděcí právní předpis stanoví
	1. kritéria pro identifikaci regulované služby (§ 4),
	2. způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),
	3. bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4),
	4. způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3),
	5. obsahové náležitosti, formát a způsob oznámení provedení protiopatření a jeho výsledku (§ 20 odst. 3),
	6. kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1),
	7. nepominutelné funkce stanoveného rozsahu (§ 28 odst. 4),
	8. kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4),
	9. způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a
	10. technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44odst. 2 (§ 44 odst. 3).
2. Prováděcí právní předpisy podle odstavce 1 vydá Úřad ve formě vyhlášky.

## HLAVA VIKontrola, nápravná opatření, přestupky a sankce

### § 56Kontrola vykonávaná Úřadem

1. Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti.
2. Při výkonu kontroly se postupuje podle kontrolního řádu.
3. Kontrolu podle tohoto ustanovení vykonávají pověření zaměstnanci Úřadu.

*CELEX 32022L2555*

### § 57Nápravná opatření

1. Zjistí-li Úřad při kontrole nedostatky, může rozhodnutím uložit kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určit jakým způsobem. Úřad může v rozhodnutí uložit orgánu nebo osobě povinnost oznámit Úřadu provedení nápravného opatření a jeho výsledek ve stanovené lhůtě. Náležitosti a způsob hlášení stanoví prováděcí právní předpis.
2. Považuje-li Úřad skutková zjištění za dostatečná, může uložit nápravné opatření podle odstavce 1 i bez provedení kontroly.
3. Rozklad proti rozhodnutí o uložení nápravného opatření nemá odkladný účinek.

*CELEX 32022L2555*

### § 58 Přestupky

1. Poskytovatel regulované služby v režimu vyšších povinností se dopustí přestupku tím, že
	1. neprovede registraci nebo změnu registrace poskytovatele regulované služby podle § 8 odst. 1 a 2 nebo § 9 odst. 1 nebo 2,
	2. nenahlásí registrační, kontaktní údaje nebo další údaje nebo jejich změnu Úřadu podle § 12 odst. 1 a 4,
	3. nezajišťuje dostatečnou zastupitelnost fyzických osob oprávněných jednat za poskytovatele regulované služby podle § 12 odst. 5,
	4. při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna primární aktiva podle § 13odst. 1 písm. a),
	5. při stanovení rozsahu řízení kybernetické bezpečnosti neurčí všechna primární aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm.  b) nebo organizační části a podpůrná aktiva podle § 13 odst. 1 písm. c),
	6. nevede dokumentovaný záznam o identifikaci a určení organizačních částí a aktiv podle § 13 odst. 3,
	7. v rozporu s § 14 nezavede nebo neprovádí bezpečnostní opatření,
	8. neohlásí kybernetický bezpečnostní incident podle § 16 odst. 1 nebo nepředloží prvotní hlášení o incidentu podle § 17 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 17 odst. 3,
	9. neposkytne informace nebo součinnost při zvládání incidentu podle § 18 odst. 3,
	10. neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovenou rozhodnutím Úřadu podle § 19 odst. 1,
	11. neplní povinnost informovat uživatele regulované služby o významné kybernetické hrozbě a krocích, které může uživatel služby učinit v reakci na ni podle § 19 odst. 2,
	12. neoznámí provedení protiopatření uložené Úřadem a jeho výsledek podle § 20 odst. 3,
	13. neplní povinnost uloženou Úřadem rozhodnutím o výstraze podle § 21,
	14. neplní povinnost uloženou rozhodnutím o vydání reaktivního protiopatření nebo opatřením obecné povahy vydaným Úřadem podle § 23,
	15. nezohlední požadavky vyplývající z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem v rozporu s § 24 odst. 1 nebo 2, nebo
	16. neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření podle § 57.
2. Poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku tím, že
	1. neprovede registraci nebo změnu registrace poskytovatele regulované služby podle § 8 odst. 1 a 2 nebo § 9 odst. 1 nebo 2,
	2. nenahlásí registrační, kontaktní údaje nebo další údaje nebo jejich změnu Úřadu podle § 12 odst. 1 a 4,
	3. nezajišťuje dostatečnou zastupitelnost fyzických osob oprávněných jednat za poskytovatele regulované služby podle § 12 odst. 5,
	4. při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna primární aktiva podle § 13 odst. 1 písm. a),
	5. při stanovení rozsahu řízení kybernetické bezpečnosti neurčí všechna primární aktiva související s poskytováním regulované služby podle § 13 odst. 1 písm.  b) nebo organizační části a podpůrná aktiva podle § 13 odst. 1 písm. c),
	6. nevede dokumentovaný záznam o identifikaci a určení organizačních částí a aktiv podle § 13 odst. 3,
	7. v rozporu s § 14 nezavede nebo neprovádí bezpečnostní opatření,
	8. neohlásí kybernetický bezpečnostní incident podle § 16 odst. 2 nebo nepředloží prvotní hlášení o incidentu podle § 17 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 17 odst. 3,
	9. neposkytne informace nebo součinnost při zvládání incidentu podle § 18 odst. 3,
	10. neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovenou rozhodnutím Úřadu podle § 19 odst. 1,
	11. neplní povinnost informovat uživatele regulované služby o významné kybernetické hrozbě a krocích, které může uživatel služby učinit v reakci na ni podle § 19 odst. 2,
	12. neoznámí provedení protiopatření uložené Úřadem a jeho výsledek podle § 20 odst. 3,
	13. neplní povinnost uloženou Úřadem rozhodnutím o výstraze podle § 21*,*
	14. neplní povinnost uloženou rozhodnutím o vydání reaktivního protiopatření nebo opatřením obecné povahy vydaným Úřadem podle § 23,
	15. nezohlední požadavky vyplývající z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem v rozporu s § 24 odst. 1 nebo 2, nebo
	16. neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření podle § 57.
3. Poskytovatel strategicky významné služby se dopustí přestupku tím, že
	1. poruší podmínku nebo zákaz uložený Úřadem v opatření obecné povahy podle § 30,
	2. nevynaloží přiměřené úsilí k zjištění informace o dodavateli bezpečnostně významné dodávky podle § 32 odst. 1 písm. a),
	3. neeviduje informace o dodavateli bezpečnostně významné dodávky podle § 32 odst. 1 písm. a),
	4. neohlásí Úřadu informace o dodavateli bezpečnostně významné dodávky nebo jejich změnu podle § 32 odst. 1 písm. b),
	5. nezajišťuje dostupnost strategicky významné služby z území České republiky ve stanoveném čase a kvalitě podle § 34 odst. 1, nebo
	6. netestuje schopnost zajištění poskytování strategicky významné služby podle § 34 odst. 2.
4. Subjekt poskytující služby registrace jmen domén se dopustí přestupku tím, že
	1. nenahlásí Úřadu údaje podle § 35odst.1nebo jejich změnu podle § 35 odst. 2,
	2. neshromažďuje nebo neuchovává přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi podle § 36 odst. 1 v souladu s požadavky § 36 odst. 2,
	3. nezavede nebo nezveřejní zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování podle § 36 odst. 3,
	4. bez zbytečného odkladu po registraci jména domény neuveřejní její registrační údaje, které nejsou osobními údaji, podle § 36 odst. 4, nebo
	5. neposkytne přístup ke konkrétním údajům o registraci jména domény podle § 36 odst. 5*.*
5. Subjekt spravující a provozující registr internetových domén nejvyšší úrovně se dopustí přestupku tím, že
	1. neshromažďuje nebo neuchovává přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi podle § 36 odst. 1 v souladu s požadavky § 36 odst. 2,
	2. nezavede nebo nezveřejní zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování podle § 36 odst. 3,
	3. bez zbytečného odkladu po registraci jména domény neuveřejní její registrační údaje, které nejsou osobními údaji, podle § 36 odst. 4, nebo
	4. neposkytne přístup ke konkrétním údajům o registraci jména domény podle § 36 odst. 5.
6. Orgán nebo osoba se dopustí přestupku tím, že
7. neposkytne součinnost při zajišťování podkladů pro vydání protiopatření podle § 20 odst. 3,
8. nepředá data a informace podle § 25 odst. 1,
9. neposkytne informace nebo jinou součinnost na základě žádosti Úřadu podle § 29 odst. 3,
10. neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření podle § 57, nebo

*CELEX 32022L2555*

1. neposkytne informace nebo jinou součinnost nezbytnou k posouzení naplnění kritérií regulované služby podle § 63 odst. 2.
2. Orgán nebo osoba, která není poskytovatelem regulované služby, se dopustí přestupku tím, že neposkytne součinnost při zvládání incidentu podle § 18 odst. 3.
3. V souvislosti se stavem kybernetického nebezpečí se orgán nebo osoba dopustí přestupku tím, že
	1. nesplní opatření sloužící k řešení a nápravě stavu kybernetického nebezpečí podle § 40 odst. 2 písm. a),
	2. neposkytne součinnost při provádění skenu zranitelností nebo penetračního testu podle § 40 odst. 2 písm. b),
	3. neposkytne součinnost při zveřejňování vyhlášení, průběhu a ukončení stavu kybernetického nebezpečí podle § 40 odst. 2 písm. c), nebo
	4. neposkytne součinnost při řešení a nápravě stavu kybernetického nebezpečí podle § 40 odst. 2 písm. d).
4. Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 45 odst. 4.
5. Žadatel se dopustí přestupku tím, že v žádosti o registraci podle § 47 odst. 4 uvede nepravdivé nebo hrubě zkreslené údaje nebo podstatné údaje zamlčí.
6. Žadatel se dopustí přestupku tím, že v době trvání členství v Komunitě podle § 47 neuvede změnu údajů potřebných pro posouzení jeho základní a zvláštní způsobilosti Úřadem, jejich změnu zamlčí nebo neuvede další skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti, nebo tyto skutečnosti zamlčí.
*CELEX 32021R0887*
7. Držitel evropského certifikátu kybernetické bezpečnosti se dopustí přestupku tím, že neinformuje příslušné subjekty posuzování shody o veškerých později zjištěných zranitelnostech nebo nesrovnalostech.
8. Výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající EU prohlášení o shodě se dopustí přestupku tím, že
	1. vydá EU prohlášení o shodě, ač pro jeho vydání nejsou splněny podmínky stanovené aktem o kybernetické bezpečnosti[[16]](#footnote-16)),
	2. neuchovává dokumenty a informace podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti,
	3. nepředloží vyhotovení EU prohlášení o shodě Úřadu a agentuře ENISA podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti, nebo
	4. neposkytuje informace o kybernetické bezpečnosti v rozsahu a způsobem uvedeným v čl. 55 aktu o kybernetické bezpečnosti.
9. Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že
	1. zneužije známku nebo označení evropského systému certifikace kybernetické bezpečnosti, evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
	2. padělá nebo pozmění evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
	3. provede činnost posouzení shody podle aktu o kybernetické bezpečnosti na úroveň záruky „vysoká“, přestože k tomu není oprávněna podle čl. 56 odst. 6 aktu o kybernetické bezpečnosti,
	4. jako subjekt posuzování shody autorizovaný podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti vydá evropský certifikát kybernetické bezpečnosti k produktu, procesu nebo službě, které nesplňují kritéria obsažená v přímo použitelném předpise Evropské unie vydaném na základě aktu o kybernetické bezpečnosti,
	5. provede bez autorizace činnost posouzení shody, vyhrazenou přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti autorizovanému subjektu posuzování shody,
	6. vystupuje jako akreditovaný subjekt posuzování shody bez akreditace podle čl. 60 odst. 1 aktu o kybernetické bezpečnosti nebo mimo rozsah této akreditace, nebo
	7. jako subjekt posuzování shody nesplní Úřadem uloženou povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení podle § 60 odst. 1.

*CELEX 32019R0881*

1. Za přestupek lze uložit pokutu do
	1. 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), písm. d) až k) a písm. m) až p), odstavce 3 písm. a), e) a f), odstavce 6 písm. b) a odstavce 8 písm. a) a b).
	2. 175 000 000 Kč nebo do výše 1,4 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), písm. d) až k) a písm. m) až p) a odstavce 8 písm. d).

*CELEX 32022L2555*

* 1. 100 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. b), odstavce 3 písm. b) a c),
	2. 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. c) a l), odstavce 2 písm. b), odstavce 3 písm. d), odstavce 4 písm. a) až e), odstavce 5 písm. a) až d), odstavce 6 písm. a) a c) až e), odstavce 7 a odstavce 13 písm. a),
	3. 35 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. c) a l) a odstavce 8 písm. c),
	4. 20 000 000 Kč, jde-li o přestupek podle odstavce 13 písm. b) až d) a odstavce 14 písm. a) až c) a písm. e) až g),

*CELEX 32019R0881*

* 1. 2 000 000 Kč, jde-li o přestupek podle odstavců 10, 11 a 12 a odstavce 14 písm. d),

*CELEX 32019R0881, 32021R0887*

* 1. 50 000 Kč, jde-li o přestupek podle odstavce 9.

### § 59Společná ustanovení k přestupkům

1. Přestupky podle tohoto zákona projednává a pokuty vybírá Úřad.
2. Má se za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý.
3. Na postup Úřadu podle tohoto zákona se ustanovení § 43, § 68 písm. b), § 70, § 71, § 80 odst. 3, § 88 odst. 2, § 89, § 90 odst. 3, § 95 odst. 3 a § 96 odst. 1 písm. b) zákona o odpovědnosti za přestupky a řízení o nich[[17]](#footnote-17)) nepoužijí.
4. Platí, že přestupky spočívající v porušení povinnosti uložené rozhodnutím, opatřením obecné povahy nebo nápravným opatřením, přestupky spočívající v neprovedení registrace poskytovatele regulované služby, přestupky související se stanovením rozsahu řízení kybernetické bezpečnosti, přestupky související se zohledněním požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem, přestupky spočívající v porušení povinností z mechanismu prověřování bezpečnosti dodavatelského řetězce a přestupky spočívající v neoznámení informací a udržování stavu neinformování Úřadu nebo uživatelů regulované služby jsou trvajícími přestupky.

*CELEX 32022L2555*

### § 60Pozastavení platnosti certifikace

1. Úřad může v případě nesplnění povinnosti odstranit nedostatky zjištěné při kontrole uložené rozhodnutím Úřadu poskytovateli regulované služby v režimu vyšších povinností, který je držitelem evropského certifikátu kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby, pozastavit tomuto poskytovateli regulované služby platnost evropského certifikátu kybernetické bezpečnosti vydaného Úřadem nebo uložit subjektu posuzování shody povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení, a to až do doby odstranění nedostatků zjištěných při kontrole, nejméně však na 6 měsíců.
2. Rozhodnutí Úřadu podle odstavce 1 může být prvním úkonem v řízení a rozklad proti němu nemá odkladný účinek.
3. Účastníkem řízení o vydání rozhodnutí podle odstavce 1 je vždy poskytovatel regulované služby v režimu vyšších povinností, o platnosti jehož certifikátu je rozhodováno.
4. Informaci o pozastavení platnosti certifikátu nebo osvědčení Úřad zveřejní na svých internetových stránkách.
5. Úřad provede, nejdříve však po uplynutí lhůty podle odstavce 1, kontrolu splnění povinnosti odstranit nedostatky zjištěné při kontrole a v případě, že zjistí, že nedostatky byly odstraněny, Úřad o tomto vydá osvědčení, které je podkladem pro obnovení platnosti certifikátu nebo osvědčení.

*CELEX 32022L2555*

### § 61Pozastavení výkonu řídicí funkce

1. Soud může na návrh Úřadu rozhodnout, že člen statutárního orgánu právnické osoby, vedoucí odštěpného závodu, prokurista nebo podnikající fyzická osoba, která v přímé souvislosti s plněním rozhodnutí Úřadu, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit nedostatky zjištěné při kontrole, opakovaně nebo závažně porušila své povinnosti při výkonu své řídicí funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, nesmí až do doby odstranění nedostatků zjištěných při kontrole, nejméně však po dobu 6 měsíců vykonávat tuto řídicí funkci.
2. Návrh lze podat pouze vůči osobě vykonávající řídicí funkci u poskytovatele regulované služby v režimu vyšších povinností a pouze ve vztahu k řídicí funkci, která není veřejnou funkcí vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby nebo jmenováním podle zvláštních právních předpisů.
3. Ustanovení zákona o obchodních korporacích[[18]](#footnote-18)) upravující vyloučení člena statutárního orgánu z výkonu funkce se v částech právních účinků pravomocného rozhodnutí o vyloučení člena statutárního orgánu, informování rejstříkového soudu a odpovědnosti za porušení dočasného zákazu výkonu funkce použijí obdobně.
4. Informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce Úřad zveřejní na svých internetových stránkách.
5. Úřad, nejdříve však po uplynutí lhůty podle odstavce 1, provede kontrolu splnění povinnosti odstranit nedostatky zjištěné při kontrole a v případě, že zjistí, že nedostatky byly odstraněny, Úřad o tomto vydá osvědčení, které je podkladem pro výmaz údaje o pozastavení řídicí funkce z obchodního rejstříku podle zákona o veřejných rejstřících právnických a fyzických osob.

*CELEX 32022L2555*

### § 62Vztah ke správnímu a kontrolnímu řádu

1. Úřad může uložit pořádkovou pokutu až do výše 100 000 Kč. Pořádkovou pokutu lze uložit i opakovaně. Celková výše opakovaně ukládaných pokut nesmí přesáhnout 10 000 000 Kč nebo 1 % z čistého obratu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je vyšší.
2. Úřad může za účelem vymáhání splnění povinnosti uložené rozhodnutím Úřadu ukládat donucovací pokuty až do výše 10 000 000 Kč nebo 1 % z čistého obratu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je vyšší.
3. Za přestupek, kterého se poskytovatel regulované služby dopustí tím, že jako kontrolovaná osoba nesplní některou z povinností podle kontrolního řádu[[19]](#footnote-19)), lze uložit pokutu do 10 000 000 Kč.
4. Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci odebráním movité věci.

# ČÁST DRUHÁUSTANOVENÍ SPOLEČNÁ A PŘECHODNÁ

## HLAVA ISpolečná ustanovení

### § 63Součinnost

1. Orgány veřejné moci jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty poskytnout Úřadu podněty, informace a jiné formy součinnosti potřebné k výkonu pravomocí a za účelem splnění povinností Úřadu, které jsou stanoveny tímto zákonem. Orgány veřejné moci a Úřad při výkonu pravomocí svěřených Úřadu tímto zákonem vzájemně spolupracují, jsou oprávněny vyžadovat stanoviska k připravovaným rozhodnutím vydávaným v mezích jejich působnosti a usilují při tom o dosažení shody těchto stanovisek. Orgány veřejné moci a Úřad dále v rozsahu, který je nezbytný pro plnění úkolů orgánů veřejné moci a Úřadu, sdílí informace o kybernetických hrozbách, zranitelnostech a incidentech a o opatřeních přijatých v reakci na tyto hrozby, zranitelnosti a incidenty. Ustanovení § 45 odst. 2 a 3 tím nejsou dotčena.
2. Orgány a osoby, o kterých lze důvodně předpokládat, že naplňují kritéria pro identifikaci nebo určení regulované služby, jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty poskytnout informace nezbytné k posouzení naplnění kritérií regulované služby a další nezbytnou součinnost. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti.
3. Ministerstva, jiné ústřední správní úřady a Česká národní banka, odpovědné za určování prvků kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu, bez zbytečného odkladu informují Úřad o určení prvků kritické infrastruktury a o důvodech určení.
4. Úřad je oprávněn od Generálního finančního ředitelství požadovat poskytnutí informací získaných při správě daní, které jsou nezbytné pro posouzení, zda orgán nebo osoba naplňuje kritéria pro identifikaci regulované služby podle § 3. Generální finanční ředitelství žádosti vyhoví, ledaže by poskytnutím informací mohlo dojít k narušení řádného výkonu správy daní. Poskytnutí informací podle tohoto ustanovení není porušením povinnosti mlčenlivosti podle daňového řádu, porušením této mlčenlivosti není ani použití těchto informací Úřadem podle tohoto zákona.
5. Úřad a Úřad pro ochranu osobních údajů jsou vzájemně oprávněny požadovat informace a vyžadovat spolupráci za účelem zamezení dvojího trestání porušení téže povinnosti uložené jak tímto zákonem, tak právními předpisy upravujícími ochranu osobních údajů. Ukládání jiných sankcí podle tohoto zákona tím není dotčeno.
6. Pro účely výkonu působnosti Úřadu podle tohoto zákona umožní Ministerstvo spravedlnosti Úřadu získat způsobem umožňujícím dálkový přístup z evidence skutečných majitelů úplný výpis platných údajů a údajů, které byly vymazány bez náhrady nebo s nahrazením novými údaji podle právního předpisu upravujícího evidenci skutečných majitelů.

*CELEX 32022L2555*

### § 64Informační povinnost Úřadu

Úřad za účelem plnění informační povinnosti podle příslušného předpisu Evropské unie[[20]](#footnote-20))

* 1. každé 2 roky informuje Evropskou komisi a Skupinu pro spolupráci o počtech poskytovatelů regulovaných služeb naplňujících kritéria pro identifikaci regulované služby v jednotlivých odvětvích,
	2. každé 2 roky informuje Evropskou komisi o počtech poskytovatelů regulovaných služeb naplňujících kritéria pro určení regulované služby v jednotlivých odvětvích, službách, které poskytují, a kritériích, pro která byli určeni,
	3. každé 3 měsíce předkládá Agentuře Evropské unie pro kybernetickou bezpečnost souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o kybernetických bezpečnostních incidentech, kybernetických hrozbách a významných kybernetických bezpečnostních událostech oznámených podle § 16,
	4. poskytuje Agentuře Evropské unie pro kybernetickou bezpečnost identifikační údaje o subjektech poskytujících služby registrace jmen domén a poskytovatelích regulovaných služeb uvedených v § 54 odst. 3, kteří mají hlavní provozovnu na území České republiky nebo kteří mají na území České republiky ustaveného svého zástupce,
	5. poskytuje Agentuře Evropské unie pro kybernetickou bezpečnost informace ke koordinovanému zveřejňování zranitelností,
	6. informuje Evropskou komisi o přijetí národní strategie kybernetické bezpečnosti a v rozsahu, ve kterém nebudou ohroženy bezpečnostní zájmy České republiky, o obsahu strategie,
	7. sdělí Evropské komisi identifikační údaje orgánu odpovědného za dozor v oblasti kybernetické bezpečnosti, jednotného kontaktního místa pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie, orgánu pro řešení kybernetických krizí, týmu CSIRT a koordinátora určeného pro účely koordinovaného zveřejňování zranitelností,
	8. poskytuje Evropské komisi a Agentuře Evropské unie pro kybernetickou bezpečnost další informace a nezbytnou součinnost.

 *CELEX 32022L2555*

### § 65Společná a zvláštní ustanovení o řízení před Úřadem

1. Na postupy Úřadu podle § 8, § 9, § 10 a § 11 odst. 1 a 3 se ustanovení správního řádu upravující vedení správního řízení nepoužijí.
2. Řízení o určení regulované služby podle § 5 lze zahájit pouze z moci úřední.
3. Proti rozhodnutí o určení regulované služby podle § 5 a rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2 není rozklad přípustný.
4. Pokud má být řízení o výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2 zahájeno z moci úřední, může být rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb prvním úkonem v řízení; v takovém případě se rozhodnutí písemně nevyhotovuje, záznamem ve spisu rozhodnutí o výmazu nabývá právní moci a Úřad provede výmaz z evidence poskytovatelů regulovaných služeb.

### § 66Ochrana informací

Části písemností a záznamy, které obsahují utajované informace nebo informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření podle § 20 nebo opatření obecné povahy podle § 30, uchovává Úřad v řízeních podle § 20, § 30 a § 31 odděleně mimo spis.

### § 67Zástupce pro Českou republiku

1. Subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladu jmen domén (DNS), poskytovatelem správy a provozu registru internetových domén nejvyšší úrovně, poskytovatelem služby cloud computingu, poskytovatelem služby datového centra, poskytovatelem služby sítě pro doručování obsahu (CDN), poskytovatelem služby on-line tržiště, poskytovatelem služby internetového vyhledávače, poskytovatelem služby platformy sociální sítě, poskytovatelem řízené služby (MSP) nebo poskytovatelem řízené bezpečnostní služby (MSSP), který poskytuje tuto službu v České republice, nemá umístěnu hlavní provozovnu v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie, je povinen ustavit si svého zástupce v České republice. Zástupcem je osoba usazená v České republice, které poskytovatel některé z uvedených regulovaných služeb udělil zmocnění zastupovat jej ve vztahu k povinnostem podle tohoto zákona. Ustavením zástupce není dotčena odpovědnost poskytovatele regulované služby nebo subjektu poskytující služby registrace jmen domén za dodržování tohoto zákona.
2. V případě, že subjekt poskytující služby registrace jmen domén nebo poskytovatel některé z regulovaných služeb uvedených v odstavci 1 má hlavní provozovnu mimo Evropskou unii a ustavil si svého zástupce v České republice, platí, že je usazen v České republice a vztahují se na něj povinnosti podle tohoto zákona. To platí i v případě, že poskytovatel některé z uvedených regulovaných služeb má hlavní provozovnu mimo Evropskou unii a neustavil si svého zástupce v žádném členském státě Evropské unie.
3. Ustanovením zástupce není dotčena odpovědnost poskytovatele regulované služby nebo subjektu poskytujícího služby registrace jmen domén za dodržování tohoto zákona.

*CELEX 32022L2555*

### § 68Finanční zabezpečení stavu kybernetického nebezpečí

Finanční zabezpečení stavu kybernetického nebezpečí na běžný rozpočtový rok se provádí podle jiného právního předpisu[[21]](#footnote-21)). Za tímto účelem

* 1. Úřad v rozpočtu své kapitoly na příslušný rok vyčleňuje objem finančních prostředků potřebný k zajištění přípravy na stav kybernetického nebezpečí; a dále ve svém rozpočtu na příslušný rok vyčleňuje účelovou rezervu finančních prostředků na řešení stavů kybernetického nebezpečí a odstraňování jejich následků a
	2. se finanční prostředky potřebné k zajištění přípravy na stav kybernetického nebezpečí a odstraňování jeho následků vyčleňované Úřadem úřady v rozpočtech kapitol považují za závazný ukazatel státního rozpočtu na příslušný rok.

### § 69Zpravodajské služby

1. V případě zpravodajských služeb[[22]](#footnote-22)) se tento zákon použije pouze v rozsahu ustanovení
	1. části první v rozsahu hlavy první, ustanovení § 8, § 9, § 10, § 11, § 12s výjimkou údajů podle odst. 2 písm. c), § 13, § 14, § 15, § 22 a § 24 odst. 2 a hlavy čtvrté, a
	2. části druhé v rozsahu § 65 odst. 1, 3 a 4.
2. Tam, kde je pro plnění povinnosti podle předchozího odstavce nutné stanovit režim poskytovatele regulované služby, platí, že zpravodajská služba vystupuje jako poskytovatel regulované služby v režimu vyšších povinností.
3. Ustanovení § 29 odst. 2 a § 63 se použije, pokud plnění těchto povinností nebrání zvláštní předpis[[23]](#footnote-23)) nebo zákonná nebo státem uznaná povinnost mlčenlivosti.

*CELEX 32022L2555*

### § 70Vztah k odvětvovým právním předpisům Evropské unie

1. Pokud přímo použitelný právní předpis Evropské unie stanoví orgánům nebo osobám povinnosti v oblasti zavádění a provádění bezpečnostních opatření nebo hlášení kybernetických bezpečnostních incidentů a tyto povinnosti mají alespoň srovnatelný účinek jako povinnosti, které jsou těmto orgánům nebo osobám stanoveny podle tohoto zákona, ustanovení tohoto zákona upravující povinnosti zavést a provádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty se vůči těmto orgánům a osobám neuplatní, a to včetně ustanovení o dozoru nad dodržováním uvedených povinností.
2. Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se považují taková ustanovení přímo použitelného právního předpisu Evropské unie, která
	1. ve vztahu k povinnosti zavést a provádět bezpečnostní opatření odpovídají alespoň požadavkům stanoveným v § 14 a § 15, nebo
	2. ve vztahu k povinnosti hlásit kybernetické bezpečnostní incidenty odpovídají alespoň požadavkům stanoveným § 16 a § 17.
3. Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se dále považují taková ustanovení přímo použitelného právního předpisu Evropské unie, o nichž to přímo použitelný právní předpis Evropské unie sám stanoví.

## HLAVA IIPřechodná ustanovení

### § 71Přechodná ustanovení

1. Správci informačních systémů základní služby, správci informačních a komunikačních systémů kritické informační infrastruktury, správci významných informačních systémů nebo poskytovatelé digitální služby podle § 3 zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, jimiž poskytované služby naplňují kritéria regulované služby podle tohoto zákona, plní pro služby a informační systémy regulované podle dosavadních právních předpisů v rozsahu, ve kterém jsou tyto služby a aktiva regulovány tímto zákonem, alespoň
2. povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu vyšších povinností, nebo
3. povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, v rozsahu povinností uložených tímto zákonem poskytovatelům regulovaných služeb v režimu nižších povinností v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu nižších povinností, a to od okamžiku nabytí účinnosti tohoto zákona až do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona, s výjimkou způsobu hlášení kybernetických bezpečnostních incidentů, který jsou tito poskytovatelé regulované služby povinni realizovat podle tohoto zákona od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb.
4. V řízeních týkajících se splnění povinnosti uložené zákonem nebo na základě zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se postupuje podle dosavadních právních předpisů.
5. Varování vydaná podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se považují za varování vydaná podle tohoto zákona.
6. Reaktivní opatření a ochranná opatření, vydaná podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona se považují za reaktivní protiopatření vydaná podle tohoto zákona.
7. Nabytím účinnosti tohoto zákona není dotčena platnost veřejnoprávních smluv uzavřených podle zákona č. 181/2014 Sb. přede dnem nabytí účinnosti tohoto zákona.

# ČÁST TŘETÍZÁVEŘEČNÁ USTANOVENÍ A ÚČINNOST

### § 72Zrušovací ustanovení

Zrušují se

1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
2. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.
3. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.
4. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
5. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.
6. Vyhláška č. XX/XXXX Sb., o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci.

### § 73Účinnost

Tento zákon nabývá účinnosti dnem 18. října 2024.

*CELEX 32022L2555*

V Praze dne dd.mm.rrrr

Předseda vlády

1. ) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). [↑](#footnote-ref-1)
2. ) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU.

Rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo. [↑](#footnote-ref-2)
3. ) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. [↑](#footnote-ref-3)
4. ) Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů. [↑](#footnote-ref-4)
5. ) Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021. [↑](#footnote-ref-5)
6. ) Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů. [↑](#footnote-ref-6)
7. ) Čl. 8 odst. 4 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021. [↑](#footnote-ref-7)
8. ) Čl. 8 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021. [↑](#footnote-ref-8)
9. ) Zákon č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon). [↑](#footnote-ref-9)
10. ) § 187 občanského zákoníku. [↑](#footnote-ref-10)
11. ) § 136 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů. [↑](#footnote-ref-11)
12. ) Například zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, zákon č. 363/1999 Sb., o pojišťovnictví a o změně některých souvisejících zákonů. [↑](#footnote-ref-12)
13. ) Zákon č. 37/2021 Sb., o evidenci skutečných majitelů. [↑](#footnote-ref-13)
14. ) Čl. 8 odst. 3 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021. [↑](#footnote-ref-14)
15. ) Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021. [↑](#footnote-ref-15)
16. ) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). [↑](#footnote-ref-16)
17. ) Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů. [↑](#footnote-ref-17)
18. ) Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů. [↑](#footnote-ref-18)
19. ) § 10 odst. 2 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů. [↑](#footnote-ref-19)
20. ) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022. [↑](#footnote-ref-20)
21. ) Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů. [↑](#footnote-ref-21)
22. ) § 3 zákona č. 153/1994 Sb., o zpravodajských službách, ve znění pozdějších předpisů. [↑](#footnote-ref-22)
23. ) Například zákon č. 153/1994 Sb., o zpravodajských službách, ve znění pozdějších předpisů. [↑](#footnote-ref-23)