NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Národní centrum kybernetické bezpečnosti

Informace o změnách zákona č. 181/2014 Sb., o kybernetické bezpečnosti účinných od 1. července 2017

Verze 1.0

Obsah

Úvod

Dokument obsahuje informace o změně zákona č. 181/2014 Sb., o kybernetické bezpečnosti zákonem č. 104/2017 Sb., kterým se mění zákon o informačních systémech veřejné správy, zákon o kybernetické bezpečnosti, a některé další zákony.

Níže popsané změny jsou účinné od 1. 7. 2017. Věnujte jim prosím pozornost.

V případě dotazů se prosím obracejte na sekretariát Národního centra kybernetické bezpečnosti:

Národní centrum kybernetické bezpečnosti
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 777

E-mail: nckb@nbu.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Shrnutí změn

Zákon č. 104/2017 Sb. přináší v rámci novely zákona o kybernetické bezpečnosti do tohoto zákona několik změn:

1) v § 2 písm. g) je nově upravena definice provozovatele informačních a komunikačních systémů,
2) v rámci § 3 písm. b) až e) se zavádí nová kategorie povinného subjektu, kterým je provozovatel,
3) v souvislosti se zavedením kategorie provozovatele zákon v § 6a nově upravuje vztah mezi správcem a provozovatelem,
4) dle § 8 odst. 4 je nově možné, aby bezpečnostní incident hlásil vedle správce také provozovatel a povinnost správce je v takové situaci splněna,
5) dle § 15a má na návrh správce Úřad nově pravomoc v případě hrozícího kybernetického incidentu uložit provozovateli rozhodnutím povinnost předat správci data, provozní údaje a informace, o které předtím správce marně provozovatele žádal dle § 6a,
6) novela zákona zavádí nové povinnosti a obecně zpřísňuje pokuty za jejich porušení. Nově je možné uložit za porušení povinností dle § 25 odst. 2 písm. a) až d), f), g) nebo j) pokutu až do výše 1 000 000 Kč a za porušení povinností dle § 25 odst. 2 písm. e) a h) pokutu až do výše 200 000 Kč,
7) v rámci přechodných ustanovení se lhůta pro splnění povinností, které má provozovatel dle § 30 písm. b) a c), zkracuje z jednoho roku na 6 měsíců.

Podrobný popis změn

Výše uvedené změny je možno blíže popsat takto (po podrobném popisu jednotlivých změn psaném tučně následuje přímá citace změn zákona psaná kurzívou):

Nový povinný subjekt a jeho definice

Novela zákona zavádí nový povinný subjekt, kterým je provozovatel informačního a komunikačního systému (dále jen „provozovatel“). Provozovatele definuje nově § 2 písm. g). Rozumí se jím ten, kdo zajišťuje funkčnost technických a programových prostředků předmětného systému. Stává se jím tedy obvykle klíčový dodavatel. V návaznosti na to je provozovatel uveden jako povinný subjekt v § 3, a to vždy vedle správce. Povinným subjektem se provozovatel stává ze zákona, v případě naplnění definičních znaků, čímž mu vznikají práva a povinnosti (např. hlášení kontaktních údajů, zavádění bezpečnostních opatření, apod.). Přesto lze doporučit správcům, aby své dodavatele na tuto skutečnost upozornili.

V § 2 se na konci písmene f) slovo „a“ zrušuje a za písmeno f) se vkládá nové písmeno g), které zní:
*„**g)** provozovatelem informačního nebo komunikačního systému orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém a“.*
Dosavadní písmeno g) se označuje jako písmeno h).
V § 3 písm. b) se za slovo „správcem“ vkládají slova „nebo provozovatelem“.
V § 3 písm. c) až e) se za slovo „správce“ vkládají slova „a provozovatel“.

Dodavatelské vztahy a zacházení s daty

Zákon následně blíže definuje vztah mezi správcem a provozovatelem. Správce může provozovatele pověřit provozováním informačního nebo komunikačního systému kritické informační infrastruktury a významného informačního systému, pokud to jiný zákon nevylučuje.

Provozovatel předává správci na vyžádání a bez zbytečného odkladu data, provozní údaje a ostatní související informace, stejně tak jako je předá v případě, že již nebude tento systém dále provozovat. V případě že již nebude dále systém provozovat, musí provozovatel také tato data, provozní údaje a

informace bezpečně zlikvidovat. Provozovatel má nárok na úhradu účelně vynaložených nákladů s tím souvisejících.

V případě, že provozovatel nebude systém dále provozovat a nepředá data, provozní údaje nebo informace, případně nezničí jejich kopie, může mu Úřad uložit pokutu až do výše 1 000 000 Kč. Pokud provozovatel neumožní správci dohled nad zničením dat, provozních údajů a informací, může Úřad uložit provozovateli pokutu až do výše 200 000 Kč. Pokutu ve stejné výši může Úřad uložit provozovateli také v případě, že provozovatel nepředá data, provozní údaje nebo informace na vyžádání správce dle § 6a odst. 2.

Za § 6 se vkládá nový § 6a, který zní:

§ 6a

*„**(1)** Správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému může pověřit provozováním informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému jiný orgán nebo osobu, pokud to jiný zákon nevylučuje.*

***(2)** Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému předá na vyžádání správce tohoto systému bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému. Ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena.*

***(3)** Pokud provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a bezpečně zlikviduje ve svém digitálním prostředí jejich kopie.*

***(4)** Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému má nárok na úhradu účelně vynaložených nákladů za předání*

dat, provozních údajů a informací podle odstavců 2 a 3; náklady provozovateli uhradí správce takového systému.“.

Hlášení kybernetických bezpečnostních incidentů provozovatelem

Povinnost hlásit kybernetické bezpečnostní incidenty podle § 8 odst. 1 se vztahuje jak na správce, tak nově na provozovatele. Tato povinnost je pak splněna i v případě, že byl kybernetický bezpečnostní incident hlášen provozovatelem informačního systému namísto správce. Provozovatel v takovém případě informuje o svém hlášení také správce, a to bez zbytečného odkladu.

V § 8 se za odstavec 3 vkládá nový odstavec 4, který zní:
„(4) Povinnost podle odstavce 1 je správcem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému splněna i tehdy, pokud byl kybernetický bezpečnostní incident hlášen provozovatelem tohoto systému. Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému informuje správce tohoto systému o hlášených kybernetických bezpečnostních incidentech bez zbytečného odkladu.“.
Dosavadní odstavec 4 se označuje jako odstavec 5.

Pravomoc Úřadu k uložení povinnosti předat data v případě hrozícího kybernetického incidentu

V situaci, kdy hrozí kybernetický bezpečnostní incident a nedošlo ke splnění povinností provozovatele podle § 6a, může Úřad na návrh správce uložit provozovateli rozhodnutím povinnost předat data, provozní údaje a informace související s provozováním systému. Návrh správce musí obsahovat odůvodnění požadavku, podrobný popis dosavadního jednání mezi správcem a provozovatelem v této věci a možné následky, pokud by k předání dat, údajů a informací nedošlo.

Rozhodnutí Úřadu v této věci je vykonatelné doručením rozhodnutí a je proti němu možný rozklad, který však nemá odkladný účinek. Provozovatel má nárok na úhradu účelně vynaložených nákladů souvisejících s předáním těchto dat, provozních údajů a informací, situace je v tomto případě stejná jako v § 6a.

V případě nesplnění rozhodnutím uložené povinnosti může Úřad provozovateli uložit pokutu až do výše 1 000 000 Kč.

Za § 15 se vkládá nový § 15a, který zní:

§ 15a

*„**(1)** Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na návrh správce informačního systému, který marně vyzval provozovatele ke splnění povinnosti předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, rozhodnutím uložit provozovateli tohoto systému povinnost předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému; návrh musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi provozovatelem a správcem tohoto systému zejména s ohledem na nesplnění smluvní povinnosti provozovatele a možné následky, pokud nedojde k předání požadovaných dat, provozních údajů a informací.*

***(2)** Rozhodnutí o uložení povinnosti předat data, provozní údaje a informace podle odstavce 1 je prvním úkonem v řízení, je vykonatelné dnem doručení rozhodnutí a rozklad proti němu nemá odkladný účinek.*

***(3)** Pro úhradu nákladů vynaložených provozovatelem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému na předání dat, provozních údajů a informací podle odstavce 1 se ustanovení § 6a odst. 4 použije obdobně.“.*

Přestupky a pokuty za ně

V souvislosti s nově vzniklými povinnostmi pro provozovatele uvádí novela i nové přestupky a pokuty za ně.

V případě nesplnění povinnosti uložené rozhodnutím Úřadu dle §15a, stejně tak jako v případě nepředání nebo nezničení kopií dat, provozních údajů a informací dle § 6a odst. 3 může Úřad uložit provozovateli pokutu až do výše 1 000 000 Kč.

Stejně tak se zvyšuje výše pokuty z 100 000 Kč na 1 000 000 Kč v případě, že právnická nebo podnikající fyzická osoba dle § 3 písm. a) až e) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci, neohlásí kybernetický bezpečnostní incident

dle § 8 odst. 1 a 3, nesplní povinnost uloženou Úřadem v rozhodnutí nebo opatření obecné povahy podle § 13 nebo 14, případně neohlásí některou povinnost uloženou nápravným opatřením podle § 24.

Pokutu až do výše 200 000 Kč může nově Úřad uložit v případě, provozovatel neumožní správci dohled nad zničením dat, provozních údajů a informací dle § 6a odst. 3, a také v případě, že provozovatel nepředá data, provozní údaje nebo informace na vyžádání správce dle § 6a odst. 2.

V nezměněné výši pak zůstává pouze výše pokuty za neoznámení kontaktních údajů podle § 16 odst. 2, písm. b), a to 10 000 Kč.

Přestupky a pokuty přehledně ilustruje následující tabulka:

§ 25	Přestupek	Pokuta	Povinný subjekt
odst. 1	Neplnění povinností uložených rozhodnutím nebo opatřením obecné povahy při SKB nebo uložených nápravných opatření podle § 24	1 000 000 Kč	Poskytovatel služby a subjekt zajišťující síť el. komunikací, subjekt zajišťující významnou síť
odst. 2 písm. a)	Nezavedení nebo neprovádění bezpečnostních opatření, nevedení bezpečnostní dokumentace	1 000 000 Kč	Správce a provozovatel informačního a komunikačního systému kritické informační infrastruktury, nebo významného informačního systému
odst. 2 písm. b)	Neohlášení kybernetického bezpečnostního incidentu	1 000 000 Kč	
odst. 2 písm. c) a d)	Nesplnění povinnosti uložené rozhodnutím nebo opatřením obecné povahy podle § 13, § 14 nebo rozhodnutím podle § 15a	1 000 000 Kč	
odst. 2 písm. e)	Nepředání dat, provozních údajů a informací podle § 6a odst. 2	200 000 Kč	
odst. 2 písm. f)	Nepředání dat, provozních údajů a informací podle § 6a odst. 3	1 000 000 Kč	
odst. 2 písm. g)	Nezničení kopií dat, provozních údajů a informací podle § 6a odst. 3	1 000 000 Kč	
odst. 2 písm. h)	Neumožnění dohledu nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3	200 000 Kč	
odst. 2 písm. i)	Neoznámení kontaktních údajů nebo jejich změny Úřadu podle § 16 odst. 2 písm. b)	10 000 Kč	
odst. 2 písm. j)	Nesplnění některé z povinností uložené nápravným opatřením podle § 24.	1 000 000 Kč	

V § 25 odst. 2 se za písmeno c) vkládají nová písmena d) až h), která znějí:
„d) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,

e) nepředá data, provozní údaje a informace podle § 6a odst. 2,
f) nepředá data, provozní údaje a informace podle § 6a odst. 3,
g) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3,
h) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3,“.
Dosavadní písmena d) a e) se označují jako písmena i) a j).
V § 25 odst. 3 písm. a) se částka „100000 Kč“ nahrazuje částkou „1000000 Kč“ a text „a) až c) nebo e)“ se nahrazuje textem „a) až d), f), g) nebo j)“.
V § 25 odst. 3 písm. b) se text „písm. d)“ nahrazuje textem „písm. i)“.
V § 25 se na konci odstavce 3 tečka nahrazuje čárkou a doplňuje se písmeno c), které zní:
„c) 200000 Kč, jde-li o správní delikt podle odstavce 2 písm. e) a h).“.
V § 28 odst. 2 písm. b) se číslo „4“ nahrazuje číslem „5“.

Přechodná ustanovení – přechodné lhůty pro plnění povinností

Pro případy plnění povinnosti stanovené podle § 16, § 8 odst. 1 a 3 zákona, stejně tak jako pro případ zavádění bezpečnostních opatření podle § 4 odst. 2 zákona se lhůta pro provozovatele informačního nebo komunikačního systému kritické informační infrastruktury nebo významného informačního systému stanovuje na 30 dní od účinnosti této novely pro hlášení kontaktních údajů Úřadu a na 6 měsíců od účinnosti této novely v případě zavádění bezpečnostních opatření a detekci a hlášení kybernetických bezpečnostních incidentů. Lhůty pro správce systémů se nemění.

Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému určeného podle zákona č. 181/2014 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona,
***a)** oznámí kontaktní údaje podle § 16 zákona č. 181/2014 Sb. nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona,*
***b)** začne plnit povinnost stanovenou v § 8 odst. 1 a 3 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona a*
***c)** zavede bezpečnostní opatření podle § 4 odst. 2 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona. V případě zavedení bezpečnostních opatření má provozovatel nárok na úhradu nákladů spojených*

s přijetím bezpečnostního opatření; náklady provozovateli uhradí správce daného systému.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
22. 6. 2017	1.0	Odd. regulace auditu a podpory	Vytvoření dokumentu