

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD  
Národní centrum kybernetické bezpečnosti



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

Verze 1.0

## Obsah

Úvod .....	3
Shrnutí změn.....	4
Podrobný popis změn zákona o kybernetické bezpečnosti .....	5
Základní ustanovení.....	5
Nové instituty.....	5
Nové povinné subjekty.....	6
Systém zajištění kybernetické bezpečnosti.....	7
Bezpečnostní opatření.....	7
Smluvní vztahy.....	7
Vzájemná informační povinnost.....	8
Kybernetické bezpečnostní události a incidenty.....	9
Svobodný přístup k informacím.....	11
Ochranná a reaktivní opatření.....	11
Hlášení kontaktních údajů.....	11
Národní CERT.....	12
Vládní CERT.....	13
Stav kybernetického nebezpečí .....	13
Výkon státní správy - Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).....	13
Kontrola, nápravná opatření a přestupky .....	15

## Úvod

Dokument obsahuje informace o změně zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon“) zákonem č. 205/2017 Sb., kterým se mění zákon o kybernetické bezpečnosti a některé další zákony (dále jen „novela zákona“).

Níže popsané změny jsou účinné od 1. 8. 2017. Věnujte jim prosím pozornost.

Změny zákona účinné od 1. 7. 2017, které přinesl zákon č. 104/2017 Sb., kterým se mění zákon o informačních systémech veřejné správy, zákon o kybernetické bezpečnosti a některé další zákony, byly zpracovány v rámci samostatného dokumentu. Tento materiál je k dispozici na oficiálních stránkách Národního centra kybernetické bezpečnosti ([www.govcert.cz](http://www.govcert.cz)) v sekci [Legislativa](#), nebo přímo dostupný – ke stažení – [zde](#).

V případě dotazů se prosím obračejte 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](mailto: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

Novela zákona přináší, především v souvislosti s implementací směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské unii (směrnice NIS), do zákona velké množství změn, z nichž nejdůležitější jsou:

- 1) zavedení nových institutů (§ 2):
  - a. základní služby a
  - b. digitální služby,
- 2) zavedení nových povinných orgánů a osob (§ 3):
  - a. správce a provozovatele informačního systému základní služby,
  - b. provozovatele základní služby a
  - c. poskytovatele digitální služby,
- 3) nová zákonná úprava povinností v rámci uzavírání smluv mezi orgány veřejné moci a poskytovateli cloud computingu (§ 4),
- 4) nová informační povinnost mezi povinnými orgány a osobami (§ 4a),
- 5) rozšíření povinností při kybernetických bezpečnostních událostech i incidentech (§ 7 a § 8),
- 6) úprava poskytování informací v rámci oblasti kybernetické bezpečnosti veřejnosti (§ 10a),
- 7) rozšíření povinnosti provádět opatření dle zákona i na nové povinné subjekty (§ 11 – § 14),
- 8) rozšíření pravomocí národního CERT (§ 17),
- 9) rozšíření pravomocí vládního CERT (§ 20),
- 10) zřízení nového ústředního orgánu státní správy – Národního úřadu pro kybernetickou a informační bezpečnost a určení jeho práv a povinností (§ 21a – § 24b) a
- 11) nová úprava přestupků a pokut za ně (§ 25 – § 27).

## Podrobný popis změn zákona o kybernetické bezpečnosti

### Základní ustanovení

Novela zákona vznikla především z důvodu implementace směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské unii (dále jen „směrnice NIS“) do českého právního řádu. Zákon tedy na tuto směrnici nově odkazuje (§ 1 odst. 2). Novela zákona je z tohoto důvodu také podstatně rozsáhlejší, než jí předcházející novela prostřednictvím zákona č. 104/2017 Sb., kterým se měnil zákon s účinností od 1. července 2017.

### Nové instituty

Zavádí se nové instituty, kterými jsou **základní služba** (§ 2 písm. i) a **digitální služba** (§ 2 písm. l). Se základní službou souvisí i nové definice **informačního systému základní služby** (§ 2 písm. j) a **provozovatele základní služby** (§ 2 písm. k).

**Základní služba** je definována jako služba, která naplní všechny tři definiční znaky uvedené v zákoně.

- Prvním znakem je, že se jedná jen o takovou službu, která zabezpečuje společenské nebo ekonomické činnosti v zákonem uvedených odvětvích. Těchto odvětví je osm a jsou jimi energetika, doprava, bankovníctví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl.
- Druhým znakem je, že poskytování této služby musí být závislé na sítích elektronických komunikací nebo informačních systémech.
- Posledním znakem je, že narušení těchto sítí elektronických komunikací nebo informačních systémů by mohlo mít na zabezpečení společenských nebo ekonomických činností v rámci těchto služeb významný dopad.

**Provozovatel základní služby** je pak takový subjekt, který základní službu poskytuje a zároveň byl určen rozhodnutím Národního úřadu pro kybernetickou a

informační bezpečnost (dále jen „Úřad“). Pro potřeby plnění informační povinnosti z pohledu směrnice NIS je za provozovatele základní služby považován také správce a provozovatel komunikačního nebo informačního systému kritické informační infrastruktury (§ 2 písm. k). Úřadu se za tímto účelem ukládá **stanovit vyhláškou dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení takové služby** (§ 28 odst. 2 písm. e). Úřad určí **provozovatele základní služby a informační systémy základní služby do 9. listopadu 2018** (bod 1., přechodná ustanovení zavedená novelou zákona).

**Digitální služba** je služba informační společnosti – tedy dle zákona č. 480/2004 Sb., o některých službách informační společnosti jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat – a spočívá v provozování on-line tržiště, internetového vyhledávače nebo cloud computingu. Tyto pojmy novela zákona také definuje (§ 2 písm. l, body 1, 2 a 3).

### **Nové povinné subjekty**

Na základě výše uvedeného se tedy i povinné subjekty rozšiřují o **správce a provozovatele informačního systému základní služby** (§ 3 písm. f), **provozovatele základní služby** (§ 3 písm. g) a **poskytovatele digitální služby** (§ 3 písm. h).

Zákon se však vztahuje pouze na takové poskytovatele digitálních služeb, kteří nenaplní definici malého podniku či mikropodniku, tedy takových, kteří mají více než 50 zaměstnanců nebo roční obrát, popřípadě bilanci v rozvaze, od 10 milionů EUR výše (§ 33 odst. 3).

Pokud má poskytovatel digitální služby sídlo v jiném členském státě, zákon se na něj nevztahuje (§ 33 odst. 4). Pokud však jde o takového poskytovatele digitální

služby, který poskytuje digitální službu v České republice a nemá v Evropské unii ani sídlo, ani svého zástupce, je takový poskytovatel digitální služby **povinen si svého zástupce ustanovit v České republice** (§ 3a odst. 1). V takovém případě se má za to, že je v České republice usazen a vztahují se na něj povinnosti dle zákona (§ 3a odst. 2).

Poskytovatelé digitálních služeb začnou, s výjimkou hlášení kontaktních údajů, plnit zákonem uložené povinnosti do 1. srpna 2018 (bod 3., přechodná ustanovení zavedená novelou zákona).

## System zajištění kybernetické bezpečnosti

### Bezpečnostní opatření

**Bezpečnostní opatření** se nově vztahují i na správce a provozovatele informačních systémů základní služby (§ 4 odst. 2), stejně tak jako na poskytovatele digitálních služeb (§ 4 odst. 3). Vybrané povinné subjekty musí i nadále zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele, nově ovšem musí tyto požadavky zahrnout také přímo do smlouvy (§ 4 odst. 4).

V souvislosti s bezpečnostními opatřeními se také ukládá Úřadu povinnost vyhláškou stanovit **způsob likvidace dat, provozních údajů a informací a jejich kopií** (§ 28 odst. 2 písm. f).

### Smluvní vztahy

Speciální novou úpravu přináší novela zákona do uzavírání smluv s poskytovatelem cloud computingu v případě orgánů veřejné moci, pokud jsou povinnými subjekty. **Novela zákona stanoví výčet náležitostí, které musí tyto smlouvy obsahovat.** Těmi jsou například ustanovení k zajištění dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu, výslovné zakotvení povinnosti poskytovatele služeb cloud computingu respektovat bezpečnostní politiku odběratele, stanovení úrovně služeb těchto služeb, zavedení systému schvalování subdodavatelů a další povinné náležitosti (§ 4 odst. 5 až 7).

Pokud nejsou podmínky smluvního vztahu některého z povinných subjektů s jeho dodavateli v souladu s požadavky zákona nebo jeho prováděcích předpisů, má povinný subjekt povinnost do 1. srpna 2018 uvést podmínky takového smluvního vztahu do souladu se zákonem (bod 4., přechodná ustanovení zavedená novelou zákona).

### Vzájemná informační povinnost

Nově se zavádí **vzájemná informační povinnosti mezi jednotlivými povinnými subjekty** (§ 4a). Povinné subjekty, kterým je tato povinnost uložena, musí tuto informaci podat neprodleně a prokazatelně.

Novela zákona stanoví, že **správce informačního nebo komunikačního systému kritické informační infrastruktury**, anebo **správce významného informačního systému**, musí informovat provozovatele takového systému (tedy toho o kom na základě uzavřené smlouvy ví, že je orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořící konkrétní informační nebo komunikační systém), že se stává provozovatelem takového systému, a tedy, že se na něj nově vztahuje zákon (§ 4a odst. 1).



Obr. 1 Zjednodušené schéma informační povinnosti dle § 4a odst. 1

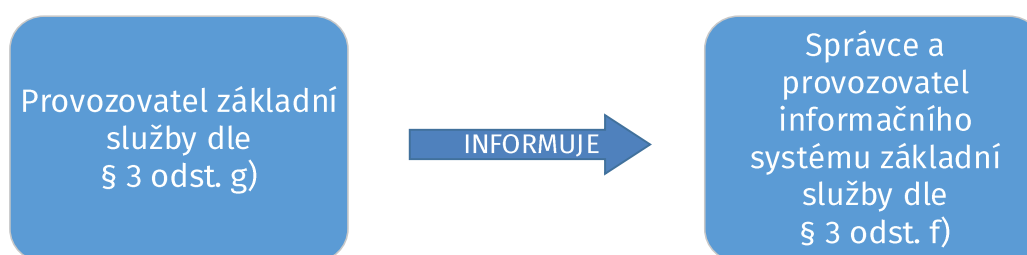
**Správce a provozovatel** informačního nebo komunikačního **systému kritické informační infrastruktury** musí navíc informovat subjekt, který mu zajišťuje pro spravovaný či provozovaný informační nebo komunikační systém kritické informační infrastruktury přímé připojení k síti elektronických komunikací o tom, že se tento stává „významnou sítí“ podle § 3 písm. b).





Obr. 2 Zjednodušené schéma informační povinnosti dle § 4a odst. 2

V rámci kategorií **provozovatele základní služby a správce a provozovatele informačního systému základní služby** je důležité brát v potaz, že se může, ale nemusí, jednat o stejný subjekt. Na základě toho je pak povinný subjekt určený jako provozovatel základní služby, který ale není zároveň správcem nebo provozovatelem svých informačních systémů základní služby povinen tyto správce a provozovatele informačního systému základní služby informovat (§ 4a odst. 3). Na rozdíl od poskytovatelů digitálních služeb neplní správci a provozovatelé informačních systémů základní služby povinnosti uložené jim zákonem ve lhůtě ode dne účinnosti novely zákona, ale ode dne, kdy byli provozovatelem základní služby informováni. Od tohoto data je jim tedy uloženo do 30 dní oznámit kontaktní údaje dle § 16 odst. 2 písm. b), stejně tak jako do 1 roku od tohoto data plnit i všechny ostatní povinnosti uložené jim zákonem (bod 2., přechodná ustanovení zavedená novelou zákona).



Obr. 3 Zjednodušené schéma informační povinnosti dle § 4a odst. 3

## Kybernetické bezpečnostní události a incidenty

**Kybernetické bezpečnostní události** je nyní nutné detekovat i v informačních systémech základní služby (§ 7 odst. 3).

**Kybernetické bezpečnostní incidenty** jsou povinné subjekty nově povinny hlásit Úřadu, respektive vládnímu CERT (§ 20 písm. b) i v rámci informačních systémů základní služby. Jestliže má kybernetický bezpečnostní incident **významný dopad na kontinuitu poskytování základní služby** je provozovatel této služby povinen to oznámit Úřadu (§ 8 odst. 1). Stejně tak v případě, kdy má kybernetický bezpečnostní incident u poskytovatele digitální služby významný dopad na

kontinuitu poskytování základní služby, je provozovatel dotčené základní služby povinen oznámit tuto skutečnost Úřadu (§ 8 odst. 8).

Také poskytovatel digitální služby je povinen hlásit kybernetický bezpečnostní incident s významným dopadem na digitální službu, kterou poskytuje (§ 8 odst. 2). Poskytovatel digitální služby hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT (aktuálně je jeho provozovatelem společnost CZ.NIC).

**Subjekty, které nejsou povinnými subjekty dle zákona, mohou hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT, nebo Úřadu (§ 8 odst. 6).**

Povinný orgán nebo osoba	Příslušný CERT
správce a provozovatel informačního systému kritické informační infrastruktury (§ 3 písm. c)	Vládní CERT
správce a provozovatel komunikačního systému kritické informační infrastruktury (§ 3 písm. d)	
správce a provozovatel významného informačního systému (§ 3 písm. e)	
správce a provozovatel informačního systému základní služby (§ 3 písm. f)	
provozovatel základní služby (§ 3 písm. g)	
orgán nebo osoba zajišťující významnou síť, pokud není správcem nebo provozovatelem komunikačního systému kritické informační infrastruktury (§ 3 písm. b)	Národní CERT
poskytovatel digitální služby (§ 3 písm. h)	

Tabulka 1 CERT příslušný dle zákona pro hlášení kybernetického bezpečnostního incidentu

Poskytovatel služby elektronických komunikací nebo subjekt zajišťující síť elektronických komunikací (§ 3 písm. a) incidenty hlásit povinně nemusí, hlášení je dobrovolné (§ 8 odst. 6).

Vedle toho se také hlášení o kybernetickém bezpečnostním incidentu, která přijímá vládní CERT od jiných, než povinných subjektů, nově stávají součástí evidence incidentů vedené Úřadem (§ 9 odst. 2).

## Svobodný přístup k informacím

Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost vydaného opatření, stejně tak jako informace, které jsou vedeny v evidenci incidentů, a je z nich možno identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím (tedy především dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím) **neposkytují** (§ 10a).

## Ochranná a reaktivní opatření

**Ochranná opatření** jsou nově povinni provádět i správci a provozovatelé informačního systému základní služby (§ 11 odst. 3 a odst. 4). **Stejně tak mají i povinnost provádět ochranná opatření**, která vydal Úřad na základě již vyřešeného kybernetického bezpečnostního incidentu (§ 14).

Dále jsou správci a provozovatelé informačního systému základní služby **povinni oznamovat Úřadu i provedení reaktivních opatření a jejich výsledek** (§ 13 odst. 4).

Úřad je oprávněn z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu po konzultaci s povinným subjektem, který byl dotčen kybernetickým bezpečnostním incidentem, **informovat o takovém incidentu veřejnost** nebo uložit povinnému subjektu, aby tak provedl sám (§ 12 odst. 3).

## Hlášení kontaktních údajů

**Poskytovatel digitální služby oznámí kontaktní údaje provozovateli národního CERT** (§ 16 odst. 2 písm. a). Na základě přechodných ustanovení novely zákona musí poskytovatelé digitálních služeb oznámit kontaktní údaje do 31. srpna 2017 také Úřadu (bod 3. písm. a, přechodná ustanovení zavedená novelou zákona). Úřad je oprávněn si pro účely kontroly tyto kontaktní údaje od provozovatele národního CERT vyžádat (§ 16 odst. 6). Kontaktní údaje hlásí poskytovatel digitální služby prostřednictvím univerzálního formuláře pro hlášení kontaktních údajů, který je

k dispozici na oficiálních stránkách Úřadu ([www.govcert.cz](http://www.govcert.cz)) v sekci [Formuláře](#), nebo přímo dostupný – ke stažení – [zde](#).

**Správci a provozovatelé informačního systému základní služby, stejně jako provozovatelé základní služby oznámí kontaktní údaje Úřadu (§ 16 odst. 2 písm. b), respektive vládnímu CERT (§ 20 písm. a). Povinností těchto subjektů je oznámit kontaktní údaje do 30 dní ode dne, kdy byly dle § 4a odst. 3 informováni provozovatelem základní služby o tom, že jsou povinnými subjekty.**

### **Národní CERT**

S ohledem na výše uvedené přijímá **provozovatel národního CERT** oznámení kontaktních údajů (§ 17 odst. 2 písm. a), hlášení o kybernetických bezpečnostních incidentech, která eviduje, uchovává, chrání (§ 17 odst. 2 písm. b) a vyhodnocuje (§ 17 odst. 2 písm. c) **nově také od poskytovatele digitální služby.**

Vedle toho poskytovateli digitální služby národní CERT poskytuje i metodickou podporu (§ 17 odst. 2 písm. d) a působí pro ně jako kontaktní místo (§ 17 odst. 2 písm. e).

Provozovatel národního CERT také předává Úřadu údaje o kybernetických informačních incidentech hlášených orgány nebo osobami zajišťujícími významnou síť nebo poskytovateli digitálních služeb. Tyto údaje ovšem předává bez uvedení jejich ohlašovatele (§ 17 odst. 2 písm. g). Za stavu kybernetického nebezpečí nebo pro potřeby kontroly předává na žádost Úřadu i kontaktní údaje (§ 17 odst. 2 písm. h).

Dále pak provozovatel národního CERT plní roli CSIRT (§ 17 odst. 2 písm. i), spolupracuje s CSIRT dalších členských států (§ 17 odst. 2 písm. k) a tyto také informuje o případném kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základní služby nebo digitální služby v tomto státě. Tyto údaje předává bez uvedení jejich ohlašovatele a zároveň o tomto postupu informuje Úřad (§ 17 odst. 2 písm. j).

V neposlední řadě také provozovatel národního CERT přijímá hlášení o kybernetických bezpečnostních incidentech od jiných, než povinných subjektů, pokud to jeho kapacity umožňují (§ 17 odst. 2 písm. l).

K plnění všech těchto činností je povinen vynaložit nezbytné náklady. Tyto činnosti s výjimkou poskytování metodické podpory a provádění hodnocení zranitelnosti v oblasti kybernetické bezpečnosti provádí národní CERT bezúplatně (§ 18 odst. 5).

### **Vládní CERT**

**Vládní CERT** nově přijímá oznámení kontaktních údajů (§ 20 písm. a) a hlášení o kybernetických bezpečnostních incidentech (§ 20 písm. b) i od správců a provozovatelů informačních systémů základních služeb a od provozovatelů základních služeb, stejně tak jako jim poskytuje metodickou podporu a pomoc (§ 20 písm. d) a součinnost při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události (§ 20 písm. e).

### **Stav kybernetického nebezpečí**

V rámci stavu kybernetického nebezpečí byla přeformulována část jeho definice. Ohrožení integrity služeb elektronických komunikací bylo vyřazeno jako definiční kritérium tohoto stavu (§ 21 odst. 1).

### **Výkon státní správy - Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**

Novela zákona nově zřizuje **Národní úřad pro kybernetickou a informační bezpečnost** jako ústřední orgán státní správy pro oblast kybernetické bezpečnosti a vybrané oblasti ochrany utajovaných informací (§ 21a).

**Úřad přebírá pravomoci, které před novelou zákona v oblasti kybernetické bezpečnosti vykonával Národní bezpečnostní úřad, resp. Národní centrum kybernetické bezpečnosti jako jeho součást. Současně novela zákona tyto pravomoci v souvislosti se vznikem Úřadu dále rozšiřuje (§ 22).**

Novela zákona v souvislosti se zavedením kategorie základní služby stanoví i způsob určení jejího provozovatele, stejně tak jako způsob určení

**informačního systému základní služby.** Úřad tak činí rozhodnutím, proti kterému je rozklad nepřipustný, na základě naplnění odvětvových a dopadových kritérií, zohledňujících významnost služeb ve výše zmíněných osmi odvětvích (energetika, doprava, bankovníctví a další) a dopad případného kybernetického bezpečnostního incidentu. Dopadová a odvětvová kritéria stanoví v budoucnu prováděcí předpis – vyhláška Úřadu. Úřad naplnění kritérií nejméně každé dva roky ověřuje. Pokud je služba poskytována i v jiném členském státě, provede Úřad před vydáním rozhodnutí konzultaci s příslušným orgánem dotčeného státu (§ 22a).

Pro účely výkonu jeho působnosti jsou Úřadu poskytovány údaje z vybraných registrů (§ 22b).

Novela zákona také rozšiřuje zmocnění Úřadu k vydání jednotlivých prováděcích předpisů.

Úřad vydá nebo rozšíří prováděcí předpisy a nově stanoví	Příslušné zmocňovací ustanovení
rozsah bezpečnostních opatření pro správce a provozovatele základní služby	§ 6 písm. c)
obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu	§ 6 písm. e)
hodnocení významnosti dopadu kybernetického bezpečnostního incidentu	§ 8 odst. 7 písm. a)
dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností	§ 28 odst. 2 písm. e)
způsob likvidace dat, provozních údajů, informací a jejich kopií	§ 28 odst. 2 písm. f)

Tabulka 2 Přehled nových oblastí, pro které Úřad vydá prováděcí předpisy

Výkon práv a povinností z veřejnoprávní smlouvy uzavřené dle zákona před 1. srpnem 2017 přechází na Úřad (bod 6., přechodná ustanovení zavedená novelou zákona).

Národní bezpečnostní úřad předá Úřadu do 1. února 2018 veškeré doklady a údaje týkající se výkonu jeho působnosti (bod 7., přechodná ustanovení zavedená novelou zákona).

K 1. srpnu 2017 na Úřad také přechází veškerý výkon práv a povinností vyplývajících z pracovněprávních vztahů a Úřad získává příslušnost k hospodaření s určeným majetkem státu, který pro účely zajišťování činnosti dle zákona příslušel Národnímu bezpečnostnímu úřadu (body 8. a 9., přechodná ustanovení zavedená novelou zákona).

### **Kontrola, nápravná opatření a přestupky**

Úřad nově vykonává kontrolu v oblasti kybernetické bezpečnosti i u správce a provozovatele informačního systému základní služby a u provozovatele základní služby. U poskytovatele digitální služby může Úřad provést kontrolu v případě, kdy je důvodné podezření, že neplní povinnosti stanovené zákonem (§ 23 odst. 1). Kontrolu provádějí pověřeni zaměstnanci Úřadu, a to přiměřeně dle kontrolního řádu (§ 23 odst. 2 a 3).

**Možnost uložit povinnému subjektu zákaz používání systému, který je bezprostředně ohrožen kybernetickým bezpečnostním incidentem, se nově rozšiřuje i o informační systémy základní služby (§ 24 odst. 2).**

Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna prostřednictvím zvláštního kontrolního orgánu (§ 24a, § 24b a § 24c).

**Novelou zákona se mění a rozšiřuje stávající právní úprava přestupků a pokut za ně (§ 25 až § 27). Vzhledem k množství změn a jejich složitosti se této problematice bude v budoucnu věnovat samostatný podpůrný dokument.**

Probíhající řízení o přestupcích vedená dle zákona dokončí Úřad (bod 5., přechodná ustanovení zavedená novelou zákona).

### Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
26. 7. 2017	1.0	Oddělení regulace, auditu a podpory	Vytvoření dokumentu