



**Bezpečnost a integrita veřejných komunikačních sítí a
služeb elektronických komunikací z pohledu zákona
č. 127/2005 Sb.,
o elektronických komunikacích a o změně některých
souvisejících zákonů
(zákon o elektronických komunikacích)
(§ 88-91, § 98, § 99)**

Štefan Koreň
odbor krizového řízení



Český telekomunikační úřad

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Hlava V

Ochrana údajů, služeb a sítí elektronických komunikací

§ 98

Bezpečnost a integrita veřejných komunikačních sítí a služeb elektronických komunikací

(1) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinen zajišťovat bezpečnost a integritu své sítě a bezpečnost služeb, které poskytuje. Za tím účelem je podnikatel zejména povinen přijmout technicko-organizační pravidla vytvořená v souladu se síťovými plány podle odstavce 2. S ohledem na technické možnosti tato pravidla zajistí takovou úroveň bezpečnosti, která odpovídá míře existujícího rizika s cílem předejít nebo minimalizovat dopad událostí na uživatele a na vzájemně propojené sítě. Bezpečností sítě a služby se rozumí jejich schopnost odolávat náhodným incidentům nebo neoprávněným či svévolným zásahům, které závažně narušují dostupnost nebo interoperabilitu služeb a integritu sítí.

(2) Pro zajištění integrity veřejných komunikačních sítí Úřad vydává síťové plány (§ 62 a OOP), ve kterých vymezí základní vlastnosti těchto sítí a jejich rozhraní, které jsou nezbytné pro vzájemné propojování veřejných komunikačních sítí, pro přístup k nim, pro připojování neveřejných komunikačních sítí a zajištění kontinuity dodávek služeb, které jsou prostřednictvím veřejných komunikačních služeb poskytovány.



(3) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací může v případech, kdy hrozí nebo dojde k závažnému narušení bezpečnosti a integrity jeho sítě z důvodů poškození nebo zničení elektronického komunikačního zařízení, zejména vlivem velkých provozních havárií nebo živelních pohrom, přerušit poskytování služby nebo odepřít přístup ke službě. Přerušování nebo odepření musí být omezeno pouze na dobu nezbytně nutnou, a je-li to technicky možné, musí být zachován přístup k číslům tísňového volání.

(4) O závažném narušení bezpečnosti a ztrátě integrity sítě, rozsahu a důvodech přerušování poskytování služby nebo odepření přístupu k ní, přijatých opatřeních a o předpokládaném termínu odstranění příčiny podle odstavce 3 je podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinen bezodkladně informovat Úřad, subjekty provozující pracoviště pro příjem tísňového volání a vhodným způsobem i uživatele. Rozsah a formu předávání informací stanoví Úřad prováděcím právním předpisem ([čeká na schválení v R ČTÚ](#)). Úřad může v případě, že je zveřejnění těchto informací ve veřejném zájmu, informovat o tom vhodným způsobem veřejnost.

(5) Úřad předkládá každoročně Komisi a Evropské agentuře pro bezpečnost sítí a informací (ENISA) souhrnnou zprávu za předchozí kalendářní rok, která informuje o oznámeních a opatřeních přijatých podle odstavců 3 a 4, a to v rozsahu a formátu stanoveném Komisí.



(6) Podnikateli zajišťujícímu veřejnou komunikační síť nebo poskytujícímu veřejně dostupnou službu elektronických komunikací může Úřad uložit povinnost provést bezpečnostní audit. Tento audit musí být proveden kvalifikovaným nezávislým subjektem a na náklady podnikatele. Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je dále povinen na žádost Úřadu předložit mu informace potřebné k posouzení bezpečnosti a integrity sítí a bezpečnosti služeb, bezpečnostní audit a jeho výsledky.

§ 99

Bezpečnost, integrita a poskytování služeb za krizových stavů

(1) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je za krizového stavu povinen podle svých technicko-organizačních pravidel zabezpečit bezpečnost a integritu své sítě a interoperabilitu poskytovaných služeb. Náležitosti uvedených technicko-organizačních pravidel stanoví Úřad prováděcím právním předpisem ([čeká na schválení v R ČTÚ překlopení OOP](#)).

(2) Podnikatel uvedený v odstavci 1 je povinen předložit Úřadu na jeho vyžádání dokumenty specifikující technicko-organizační pravidla podle odstavce 1 a umožnit Úřadu kontrolovat dodržování těchto pravidel. Úřad je oprávněn při zjištění rozporu těchto dokumentů s právními předpisy sdělit dotčenému podnikateli tuto skutečnost a stanovit mu přiměřenou lhůtu k odstranění nedostatků.



3) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou telefonní službu je oprávněn při nebezpečí vzniku krizové situace a za krizového stavu³⁹⁾ na žádost Ministerstva vnitra poskytovat přednostně připojení k veřejné komunikační síti a přístup k veřejně dostupné telefonní službě účastníkům krizové komunikace podle zvláštního právního předpisu⁽¹⁾. Za tímto účelem je v rozsahu nezbytně nutném oprávněn omezit nebo přerušit poskytování veřejně dostupné telefonní služby. O omezení nebo přerušení poskytování veřejně dostupné telefonní služby, včetně jeho rozsahu, je povinen bezprostředně informovat Úřad. Toto omezení může trvat pouze po dobu nezbytně nutnou a musí být zachován přístup k číslům tísňového volání.

(4) Podnikatel uvedený v odstavci 1 je za krizového stavu povinen bezodkladně informovat Úřad o ohrožení nebo narušení bezpečnosti a integrity své sítě a bezpečnosti služeb, včetně přijatých nebo zamýšlených opatření k nápravě a o předpokládaném termínu odstranění příčiny.

1) § 18 zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.



Zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací

(1) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen

a) zajistit technicky a organizačně bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob v souladu se zvláštním právním předpisem, ochranu provozních a lokalizačních údajů a důvěrnost komunikací fyzických a právnických osob při poskytování této služby; pokud je to nutné, ochranu zajistí po písemné dohodě i v součinnosti s podnikatelem zajišťujícím veřejnou komunikační síť,

b) zajistit, aby provozní a lokalizační údaje uchovávané podle § 97 odst. 3 měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně jako provozní a lokalizační údaje při poskytování služby elektronických komunikací,

c) zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací podle písmen a) a b) vnitřní technicko-organizační předpis; ochranu údajů a důvěrnost komunikací zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany,

d) informovat dotčené účastníky o specifickém riziku porušení bezpečnosti sítě ve vztahu k ochraně údajů podle písmene a), a pokud toto riziko přesahuje rozsah jím přijímaných opatření, je povinen účastníky informovat i o veškerých možnostech docílení nápravy, včetně souvisejících nákladů,



e) vytvořit vnitřní postupy pro vyřizování žádostí o přístup k osobním údajům uživatelů; na žádost Úřadu pro ochranu osobních údajů mu podnikatelé poskytující veřejně dostupnou službu elektronických komunikací poskytnou informace o těchto postupech, počtu přijatých žádostí, o právním odůvodnění těchto žádostí a o jejich zodpovězení.

(2) Podnikatel poskytující veřejně dostupnou službu elektronických komunikací je povinen předložit Úřadu na jeho vyžádání předpis uvedený v odstavci 1 písm. c). Zjistí-li Úřad, že je předpis uvedený v odstavci 1 písm. c) v rozporu s tímto zákonem, sdělí tuto skutečnost bezodkladně dotčenému podnikateli a stanoví mu přiměřenou lhůtu k odstranění nedostatků.

(3) Úřad je, po předchozím vyžádání předpisu uvedeného v odstavci 1 písm. c), oprávněn u podnikatelů poskytujících veřejně dostupnou službu elektronických komunikací kontrolovat dodržování tohoto předpisu, s výjimkou kontroly plnění povinností týkajících se ochrany osobních údajů. Při výkonu uvedené kontrolní činnosti jsou pověřeni zaměstnanci Úřadu oprávněni vstupovat do provozních a obchodních prostor podnikatelů a seznamovat se s osobními údaji v souvislosti s dodržováním předpisu.



Děkuji vám za pozornost



Český telekomunikační úřad

