ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2021

Vyhlásené: 22. 07. 2021 Časová verzia predpisu účinná od: 1. 08. 2021

287

ZÁKON

z 29. júna 2021,

ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z. a zákona č. 134/2020 Z. z. sa mení a dopĺňa takto:

1. V § 2 ods. 2 písmeno d) znie:

   „d) požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov,[3]) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,[4]) a ani na platobné systémy a na systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,[5])“.

2. V poznámke pod čiarou k odkazu 6 sa vypúšťa citácia „Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.“.

3. V poznámke pod čiarou k odkazu 7 sa za slovami „(zákon o ochrane pred odpočúvaním) v znení neskorších predpisov“ čiarka nahrádza bodkou a vypúšťa sa citácia: „zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.“.

4. V § 3 písmeno a) znie:

   „a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,[8])“.

   Poznámka pod čiarou k odkazu 8 znie:

   „[8]) § 2 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.“.

5. V § 3 sa za písmeno a) vkladá nové písmeno b), ktoré znie:

   „b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,“.

   Doterajšie písmená b) až o) sa označujú ako písmená c) až p).

6. V § 3 písm. l) prvom bode sa na konci pripája slovo „alebo“.

7. V § 3 písm. l) sa vypúšťa druhý bod.

   Doterajší tretí bod sa označuje ako druhý bod.

8. V § 3 písm. m) sa slová „písmena k)“ nahrádzajú slovami „písmena l)“.
9. V § 4 písm. b) sa vypúšťa slovo „úrad,“, za slovami „Ministerstvo životného prostredia Slovenskej republiky“ sa čiarka nahrádza slovom „a“, vypúšťajú sa slová „Slovenská informačná služba,“ a slová „a Vojenské spravodajstvo“.
10. V § 5 ods. 1 písm. v) sa slová „orgán posudzovania zhody“ nahrádzajú slovami „certifikovaného audítora kybernetickej bezpečnosti“.
11. V § 5 ods. 1 písm. w) sa za slovo „štandardy“ vkladajú slová „a zverejňuje ich na svojom webovom sídle,“.
12. V § 5 sa odsek 1 dopĺňa písmenami y) až af), ktoré znejú:

„y) je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu[10aa]),

z) plní úlohy kompetenčného a odvetvového centra podľa osobitného predpisu[10ab]),

aa) odníma certifikát kybernetickej bezpečnosti,

ab) v rámci systému certifikácie kybernetickej bezpečnosti vydáva bezpečnostné štandardy, certifikačné schémy a postupy,

ac) plní úlohy ústredného orgánu podľa prílohy č. 1,

ad) vedie a zverejňuje na svojom webovom sídle zoznam orgánov posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti, zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti,

ae) posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky,

af) predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o dodržiavaní noriem týkajúcich sa ochrany telekomunikačného tajomstva a osobných údajov občanov Slovenskej republiky.“.

Poznámky pod čiarou k odkazom 10aa a 10ab znejú:

„[10aa]) Čl. 58 a 60 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7. 6. 2019).

[10ab]) Čl. 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/887, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8. 6. 2021).“.

13. Za § 5 sa vkladá § 5a, ktorý znie:

„§ 5a

(1) Systémom certifikácie kybernetickej bezpečnosti je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov, služieb alebo procesov v oblasti sietí a informačných systémov, informačných a komunikačných technológií a kybernetickej bezpečnosti podľa osobitného predpisu.[10b])

(2) Úrad v rámci systému certifikácie kybernetickej bezpečnosti certifikuje produkty, služby a procesy[10c]) ako orgán posudzovania zhody podľa osobitného predpisu.[10d])

(3) Certifikačný orgán[10e]) orgánu posudzovania zhody podľa osobitného predpisu,[10f]) ktorý je verejným subjektom[10g]) a nie je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti, certifikuje produkty, služby a procesy podľa osobitného predpisu[10g]) v rámci systému certifikácie kybernetickej bezpečnosti.

(4) Úrad odníme európske certifikáty kybernetickej bezpečnosti, ktoré vydal, alebo európske certifikáty kybernetickej bezpečnosti vydané podľa čl. 56 ods. 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881“) orgánmi posudzovania zhody, ktoré nie sú v súlade s nariadením (EÚ) 2019/881 alebo s európskym systémom certifikácie kybernetickej bezpečnosti.

(5) Úrad môže odňať vydaný európsky certifikát kybernetickej bezpečnosti aj držiteľovi certifikátu, ak tento

a) poruší povinnosť podľa čl. 56 ods. 8 nariadenia (EÚ) 2019/881,

b) neumožní úradu získať prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881,

c) akýmkoľvek spôsobom znemožní vykonávať oprávnenie podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.

(6) Na účely tohto zákona sa rozumie

a) produktom produkt IKT podľa čl. 2 ods. 12 nariadenia (EÚ) 2019/881,

b) službou služba IKT podľa čl. 2 ods. 13 nariadenia (EÚ) 2019/881,

c) procesom proces IKT podľa čl. 2 ods. 14 nariadenia (EÚ) 2019/881.“.

Poznámky pod čiarou k odkazom 10b až 10g znejú:

„[10b]) Čl. 2 ods. 10 nariadenia (EÚ) 2019/881.

[10c]) Napríklad STN EN ISO/IEC 17065 Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb (ISO/IEC 17065) (01 5256).

[10d]) Čl. 52 ods. 5 až 7 nariadenia (EÚ) 2019/881.

[10e]) Čl. 60 ods. 2 a príloha nariadenia (EÚ) 2019/881.

[10f]) Čl. 56 ods. 5 písm. b) nariadenia (EÚ) 2019/881.

[10g]) Čl. 52 ods. 5 a 6 nariadenia (EÚ) 2019/881.“.

14. V § 6 ods. 1 prvej vete sa za slovo „Úrad“ vkladajú slová „zriaďuje Národné centrum kybernetickej bezpečnosti ako svoju organizačnú zložku, ktorá“.

15. V § 8 ods. 5 sa vkladá nové písmeno f), ktoré znie:

„f) Úrad pre reguláciu elektronických komunikácií a poštových služieb,“.

Doterajšie písmeno f) sa označuje ako písmeno g).

16. V § 9 ods. 1 písm. b) sa za slovo „úlohy“ vkladajú slová „spravodajskej služby“.

17. V § 9 odsek 2 znie:

„(2) Ústredný orgán na plnenie úloh podľa odseku 1 písm. a) v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1 využíva Národné centrum kybernetickej bezpečnosti alebo zriaďuje a prevádzkuje vlastnú akreditovanú jednotku CSIRT alebo využíva akreditovanú jednotku CSIRT v pôsobnosti ústredného orgánu, ak sa tak zmluvne dohodnú.“.

18. V § 9 sa vypúšťa odsek 3.

19. Nadpis § 10 znie: „Kybernetická bezpečnosť iného orgánu štátnej správy“.

20. V § 10 sa vypúšťa odsek 2. Súčasne sa zrušuje označenie odseku 1.

21. Za § 10 sa vkladá § 10a, ktorý vrátane nadpisu znie:

„§ 10a
Súčinnosť

(1) Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa prílohy č. 1 sú povinní poskytnúť úradu na plnenie jeho úloh pri riešení kybernetického bezpečnostného incidentu podľa tohto zákona požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu; informácie sa poskytujú len za podmienky, že sú nevyhnutné pre riešenie kybernetického bezpečnostného incidentu a ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu[13a)] alebo spravodajskej služby podľa osobitného predpisu[13]) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.

(2) Žiadosť o súčinnosť musí byť riadne odôvodnená a musí obsahovať konkrétny rozsah požadovanej súčinnosti podľa tohto zákona.“.

Poznámka pod čiarou k odkazu 13a znie:

„[13a]) Napríklad zákon č. 747/2004 Z. z. v znení neskorších predpisov.“.

22. V § 13 ods. 2 sa slová „ústredný orgán, ktorý má plniť úlohy jednotky CSIRT;“ nahrádzajú slovami „orgán verejnej moci, ktorý“.
23. V § 13 ods. 6 sa vypúšťajú slová „ústredného orgánu, ktorý má plniť úlohy jednotky CSIRT,“.
24. V § 17 ods. 1 sa bodka na konci nahrádza čiarkou a pripájajú sa tieto slová: „najneskôr však do 60 dní, odkedy k prekročeniu došlo.“.
25. V § 17 ods. 2 úvodnej vete sa slová „podľa § 3 písm. k)“ nahrádzajú slovami „podľa § 3 písm. l)“.
26. V § 17 sa vypúšťa odsek 3.

    Doterajšie odseky 4 až 6 sa označujú ako odseky 3 až 5.
27. V § 17 ods. 3 sa slová „podľa § 3 písm. k) tretieho bodu“ nahrádzajú slovami „podľa § 3 písm. l) druhého bodu“.
28. V § 18 ods. 4, § 19 ods. 7 a § 30 ods. 1 písm. b) sa slová „§ 17 ods. 5“ nahrádzajú slovami „§ 17 ods. 4“.
29. V § 19 ods. 1 sa slovo „šiestich“ nahrádza číslovkou „12“.
30. V § 19 odseky 2 a 3 znejú:

    „(2) Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík.

    (3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke.“.
31. V § 20 ods. 1 druhej vete sa slovo „kontinuitu“, nahrádza slovom „bezpečnosť“.
32. V § 20 odsek 3 znie:

    „(3) Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

    a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,

b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,

c) personálnej bezpečnosti,

d) riadenia prístupov,

e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,

f) bezpečnosti pri prevádzke informačných systémov a sietí,

g) hodnotenia zraniteľností a bezpečnostných aktualizácií,

h) ochrany proti škodlivému kódu,

i) sieťovej a komunikačnej bezpečnosti,

j) akvizície, vývoja a údržby informačných sietí a informačných systémov,

k) zaznamenávania udalostí a monitorovania,

l) fyzickej bezpečnosti a bezpečnosti prostredia,

m) riešenia kybernetických bezpečnostných incidentov,

n) kryptografických opatrení,

o) kontinuity prevádzky,

p) auditu, riadenia súladu a kontrolných činností.“.

33. V § 20 ods. 4 sa vkladá nové písmeno a), ktoré znie:

„a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,“.

Doterajšie písmená a) až e) sa označujú ako písmená b) až f).

34. V § 20 sa za odsek 4 vkladá nový odsek 5, ktorý znie:

„(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

a) plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách,

b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“),

c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany,

d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,

e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky.

Politické riziká schvaľuje vláda Slovenskej republiky na základe stanoviska úradu. Stanovisko úradu sa predkladá Bezpečnostnej rade Slovenskej republiky. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti. Úrad v analýze politického rizika zohľadní vyjadrenie Ministerstva zahraničných vecí a európskych záležitostí