

## POZMEŇUJÚCI NÁVRH

poslanca Národnej rady Slovenskej republiky Ľubomíra Vážneho

**k vládnemu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa mení zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (tlač 1615)**

---

1. V čl. I sa za bod 1 vkladá nový bod 2, ktorý znie:

„2. V § 3 odsek 8 znie:

„(8) Citlivé vybavenie, stavebné práce citlivého charakteru a služba citlivého charakteru na účely tohto zákona je vybavenie, stavebné práce a služba na účely bezpečnosti, ktorá je spojená s utajovanou skutočnosťou<sup>27)</sup> alebo citlivou informáciou o kritickej infraštruktúre<sup>27a)</sup> (ďalej len „utajovaná skutočnosť“), vyžaduje si utajovanú skutočnosť alebo obsahuje utajovanú skutočnosť.“

Poznámka pod čiarou k odkazu 27a znie:

„<sup>27a)</sup> § 2 písm. k) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.““

Nasledujúce body sa primerane prečísľujú.

### **Odôvodnenie:**

*Navrhuje sa upraviť zákonnú definíciu citlivého vybavenia, stavebných prác citlivého charakteru a služby citlivého charakteru tak, aby definícia bola súladná s platnou Bezpečnostnou stratégiou štátu schválenou Národnou radou Slovenskej republiky 27. septembra 2005, ktorá v bode 49 uvádza: „SR prijme opatrenia na obmedzenie zraniteľnosti prvkov kritickej infraštruktúry, s dôrazom na informačné a komunikačné systémy, a na minimalizáciu negatívnych následkov útokov na ne. Bude pokračovať v aktivitách zameraných na bezpečnosť a integritu informačných a komunikačných systémov, zvlášť systémov nevyhnutných pre bezpečný výkon základných funkcií štátu. Bude pokračovať v spolupráci so zahraničnými partnermi na aktivitách zvyšujúcich bezpečnosť systémov vzájomnej komunikácie a výmeny informácií, zvlášť v oblasti prenosu a ochrany utajovaných informácií.“ V rámci úpravy sa navrhuje, aby sa definícia citlivého vybavenia vzťahovala aj na citlivé informácie podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov. Návrh zosúladzuje jednotlivé legálne definície, nakoľko podľa § 2 písm. k) zákona č. 45/2011 Z. z. o kritickej infraštruktúre citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) je neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku. Podľa § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre je prvkom kritickej infraštruktúry (ďalej len „prvok“) najmä inžinierska stavba,<sup>2)</sup> služba vo verejnom záujme*

*a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia. Navrhovaná úprava je v súlade so smernicou Európskeho parlamentu a Rady 2009/81/ES z 13. júla 2009 o koordinácii postupov pre zadávanie určitých zákaziek na práce, zákaziek na dodávku tovaru a zákaziek na služby verejnými obstarávateľmi alebo obstarávateľmi v oblastiach obrany a bezpečnosti a o zmene a doplnení smerníc 2004/17/ES a 2004/18/ES; osobitne možno poukázať na recitál 20 v spojení s čl. 1 ods. 7 a 8 tejto smernice. Tiež možno poukázať aj na zákon č. 319/2002 Z. z. o obrane Slovenskej republiky, ktorý v § 2 ods. 2 uvádza: „Obrana štátu sa zabezpečuje aj v kybernetickom priestore<sup>1a)</sup> prostredníctvom opatrení zameraných na riešenie závažných kybernetických bezpečnostných incidentov podľa osobitného predpisu<sup>1b)</sup> a obranu objektov osobitnej dôležitosti, ďalších dôležitých objektov a prvkov kritickej infraštruktúry<sup>1c)</sup> pred kybernetickým napadnutím, ktoré v tejto oblasti vykonáva Vojenské spravodajstvo.<sup>1d)</sup>“.*

2. V čl. I sa za bod 20 vkladá nový bod 21, ktorý znie:

„21. V § 43 odsek 4 znie:

„4) Ak prístup k dokumentom potrebným na vypracovanie ponuky, návrhu a na preukázanie splnenia podmienok účasti alebo k ich časti nemožno poskytnúť podľa odsekov 1 a 2 z dôvodu ochrany dôverných informácií podľa § 22 ods. 4 alebo z dôvodu, že tieto dokumenty obsahujú informácie alebo dokumenty chránené podľa osobitného predpisu<sup>52a)</sup>, verejný obstarávateľ a obstarávateľ uvedú v oznámení o vyhlásení verejného obstarávania, v oznámení použitom ako výzva na súťaž, v oznámení o koncesii alebo v oznámení o vyhlásení súťaže návrhov požiadavky a opatrenia, ktoré sa vyžadujú na ochranu dôverných informácií alebo na ochranu informácií alebo dokumentov chránených podľa osobitného predpisu a informáciu, ako možno získať prístup k príslušnému dokumentu.“.

Poznámka pod čiarou k odkazu 52a znie:

„<sup>52a)</sup> Napríklad zákon č. 215/2004 Z. z. v znení neskorších predpisov, zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.“.

Nasledujúce body sa primerane prečísľujú.

#### **Odôvodnenie:**

*Popri zákazkách v oblasti obrany a bezpečnosti (§ 3 ods. 6) aj pri zadávaní niektorých civilných zákaziek (§ 3 ods. 5) v praxi môže prichádzať k tomu, že hospodárskym subjektom je potrebné zo strany verejného obstarávateľa alebo obstarávateľa sprístupniť také informácie alebo dokumenty, ktoré sú chránené osobitnými zákonmi, najmä zákonom č. 214/2004 Z. z. o utajovaných skutočnostiach v znení neskorších predpisov alebo zákonom č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov. Podľa účinnej právnej úpravy takéto osobitne*

*chránené informácie alebo dokumenty síce boli vylúčené zo zverejnenia v profile v zmysle § 64 ods. 1 písm. a) zákona, nebol však jednoznačný ich právny režim v procese verejného obstarávania civilnej zákazky, najmä nebolo upravené, ako kním môže záujemca získať prístup. Bude povinnosťou verejného obstarávateľa alebo obstarávateľa uviesť požiadavky a opatrenia, ktoré sa vyžadujú na ochranu dôverných informácií a informáciu, ako možno získať prístup k príslušnému dokumentu. Konkrétne požiadavky a opatrenia budú určené spravidla na základe príslušného osobitného zákona, tzn. zákona č. 214/2004 Z. z. o utajovaných skutočnostiach v znení neskorších predpisov alebo zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.*

3. Za článok I sa vkladá nový článok II, ktorý znie:

## „Čl. II

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení zákona č. 69/2018 Z. z., zákona č. 177/2018 Z. z. a zákona č. 373/2018 Z. z. sa mení a dopĺňa takto:

1. V § 6 písmeno f) znie:

„f) schvaľuje bezpečnostný plán a jeho aktualizáciu; oznamuje ministerstvu predĺženie lehoty na zavedenie bezpečnostného plánu,“

2. V § 9 ods. 1 písm. b) sa slová „vyjadrení príslušného ústredného orgánu“ nahrádzajú slovami „schválení príslušným ústredným orgánom“.

### **Odôvodnenie:**

*Navrhuje sa zaviesť inštitút schvaľovania bezpečnostných plánov ústredným orgánom. Zmenou sa navrhuje zvýšenie úrovne konzistencie požiadaviek a opatrení v príslušnom sektore kritickej infraštruktúry, ako aj minimalizácia nepresných alebo potenciálne neobjektívnych požiadaviek a opatrení identifikovaných bezpečnostným plánom bez relevantného kontextu so skutočne identifikovanými rizikami. Prenesením zodpovednosti schvaľovania prevádzkovateľom vypracovaného bezpečnostného plánu ústredným orgánom dôjde k objektivizácii posudzovania a vyhodnocovania bezpečnostným plánom identifikovaných opatrení v kontexte prevádzkovateľom identifikovaných rizík. Rozširujú sa povinnosti prevádzkovateľa v súvislosti s prípadmi, ak majú byť dodávateľovi sprístupnené citlivé informácie.*

3. V § 9 sa odsek 1 dopĺňa písmenami i) až k), ktoré znejú:

„i) posúdiť, či dodávateľ tovarov, stavebných prác a jeho subdodávateľa vrátane potenciálneho dodávateľa alebo poskytovateľ služieb a jeho subdodávateľa vrátane potenciálneho poskytovateľa k prvku alebo týkajúcich sa prvku (ďalej len „dodávateľ“) preukázateľne spĺňa požiadavky a má prijaté opatrenia podľa § 10a ods. 1, ak majú byť dodávateľovi sprístupnené citlivé informácie, a to pred sprístupnením citlivých informácií; toto posúdenie je prevádzkovateľ povinný vykonávať aj po sprístupnení

citlivej informácie, a to priebežne aspoň jedenkrát za rok počas celej doby prístupu dodávateľa k citlivým informáciám,

j) neuzavrieť s dodávateľom zmluvu o sprístupnení citlivej informácie podľa § 10a ods. 2, ak

1. nemá preukázané, že dodávateľ spĺňa požiadavky a má prijaté opatrenia podľa § 10a ods. 1 písm. a) a c), s výnimkou prípadu, ak je na preukázanie splnenia požiadaviek a prijatia opatrení podľa § 10a ods. 1 písm. c) potrebné dodávateľovi, ktorý spĺňa požiadavky a má prijaté opatrenia podľa § 10a ods. 1 písm. a), v nevyhnutnom rozsahu vopred sprístupniť citlivú informáciu; v tom prípade je prevádzkovateľ povinný v zmluve o sprístupnení citlivej informácie podľa § 10a ods. 2 dodávateľa zaviazat' k plneniu tých požiadaviek a prijatiu tých opatrení podľa § 10a ods. 1 písm. c), ktoré nie sú pokryté požiadavkami a opatreniami podľa § 10a ods. 1 písm. a) a určiť na to primeranú lehotu alebo

2. prevádzkovateľ má preukázateľné informácie alebo údaje vrátane informácií alebo údajov pochádzajúcich z chránených zdrojov, že dodávateľ nie je natoľko spoľahlivý, aby sa vylúčili riziká spojené s ochranou záujmov chránených týmto zákonom,

k) bezodkladne odstúpiť od zmluvy o sprístupnení citlivej informácie podľa § 10a ods. 2, ak

1. dodávateľ v lehote podľa písm. j) prvého bodu nesplní požiadavky alebo neprijme opatrenia podľa § 10a ods. 1 písm. c),

2. sa ukáže, že dodávateľ v čase uzavretia alebo počas trvania zmluvy o sprístupnení citlivej informácie podľa § 10a ods. 2 nespĺňal požiadavky alebo nemal prijaté opatrenia podľa § 10a ods. 1 písm. a) alebo c) alebo

3. ide o nespoľahlivého dodávateľa podľa písm. j) druhého bodu.“

#### **Odôvodnenie:**

*Rozširujú sa povinnosti prevádzkovateľa v súvislosti s prípadmi, ak majú byť dodávateľovi sprístupnené citlivé informácie. Základnou povinnosťou prevádzkovateľa bude posúdenie, či dodávateľ spĺňa zákonné požiadavky a má prijaté opatrenia na zabezpečenie ochrany citlivých informácií, pričom zákon za týmto účelom upravuje jednoznačné a záväzné pravidlá tak, aby postup prevádzkovateľa aj z pohľadu dodávateľa bol objektívny a predvídateľný. Zavádza sa aj povinnosť neuzavrieť s dodávateľom zmluvu ak sú preukázateľné informácie alebo údaje vrátane informácií alebo údajov pochádzajúcich z chránených zdrojov, že dodávateľ nie je natoľko spoľahlivý, aby sa vylúčili riziká spojené s ochranou záujmov Slovenskej republiky.*

4. Za § 10 sa vkladá § 10a, ktorý znie:

#### „§ 10a

(1) Ak majú byť dodávateľovi sprístupnené citlivé informácie, dodávateľ je povinný pred sprístupnením citlivých informácií a počas celej doby prístupu dodávateľa k citlivým informáciám preukázateľne

a) mať prijaté bezpečnostné opatrenia podľa osobitného predpisu,<sup>4a)</sup>

b) mať s prevádzkovateľom uzatvorenú zmluvu o sprístupnení citlivej informácie podľa odseku 2 a

c) spĺňať ďalšie požiadavky a mať prijaté ďalšie opatrenia v súlade s bezpečnostným plánom podľa § 10.

(2) Zmluva o sprístupnení citlivej informácie (ďalej len „zmluva“) musí obsahovať najmä špecifikáciu sprístupňovaných citlivých informácií, obdobie, počas ktorého budú citlivé informácie sprístupňované, zoznam osôb u dodávateľa oprávnených na oboznamovanie sa s citlivými informáciami a požiadavky na tieto osoby, rozsah činností s citlivými informáciami, rozsah kontrolných opatrení, povinnosť dodávateľa oznámiť zmeny majúce vplyv na ochranu citlivých informácií, sprístupňovanie citlivých informácií tretím osobám, povinnosti dodávateľa po zániku zmluvy a zmluvné sankcie v prípade porušenia povinností dodávateľa. Zmluva spravidla obsahuje aj úpravu vzťahu k zmluve, na základe ktorej dodávateľ dodáva alebo má dodávať prevádzkovateľovi tovary alebo stavebné práce alebo poskytuje alebo má poskytovať prevádzkovateľovi služby. Zmluva sa nesprístupňuje podľa osobitného predpisu.<sup>5)</sup>

(3) Dodávateľ je povinný zachovávať mlčanlivosť o citlivej informácii, a to aj po zániku jeho oprávnenia oboznamovať sa s citlivou informáciou.

(4) Požiadavky a opatrenia na ochranu utajovaných skutočností podľa osobitného predpisu<sup>4aa)</sup> nie sú odsekmi 1 až 3 dotknuté.

(5) Prevádzkovateľ môže odstúpiť od zmluvy, na základe ktorej dodávateľ dodáva alebo má dodávať prevádzkovateľovi tovary alebo stavebné práce alebo poskytuje alebo má poskytovať prevádzkovateľovi služby, ak dodávateľ poruší niektorú z povinností podľa odsekov 1 až 4; tým nie je dotknuté právo prevádzkovateľa odstúpiť od takejto zmluvy alebo jej časti podľa osobitného predpisu.<sup>4ab)</sup>

Poznámky pod čiarou k novým odkazom 4aa) a 4ab) znejú:

„<sup>4aa)</sup> Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

<sup>4ab)</sup> Napríklad Občiansky zákonník, Obchodný zákonník, zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.“

#### **Odôvodnenie:**

*Navrhuje sa presnejšie určiť a vymedziť požiadavky na dodávateľa tovarov, stavebných prác alebo poskytovateľa služieb vrátane všetkých subdodávateľov, ako aj potenciálneho dodávateľa tovarov, stavebných prác alebo poskytovateľa služieb (ďalej len „dodávateľ“) vo vzťahu k prvku, ktoré je dodávateľ povinný splniť. Špecifickosť postupov spojených s dodávaním tovarov, uskutočnením stavebných prác alebo poskytovaním služieb vo vzťahu k prvku je nevyhnutné zohľadniť v rámci požiadaviek na prijatie a udržiavanie opatrení na ochranu ako prvku, ako aj citlivých informácií. Vzhľadom k skutočnosti, že dodávateľ bude pri plnení zmluvy nevyhnutne prichádzať do styku s citlivými informáciami, dôvodnosť stanovenia požiadaviek na ich ochranu je jednoznačne opodstatnená. Rovnako aj potenciálny dodávateľ tovarov, stavebných prác alebo poskytovateľ služieb sa v rámci predzmluvných rokovaní, procesu verejného obstarávania alebo iných úkonov smerujúcich k uzavretiu*

zmluvy môže v určitom rozsahu oboznamovať s citlivými informáciami, preto je potrebné uvedené požiadavky na ochranu prvku, resp. citlivých informácií uplatniť aj v tomto prípade. V zmysle uvedeného sa navrhuje identifikácia konkrétneho rozsahu opatrení, ku ktorých plneniu bude dodávateľ zaviazaný, a to stanovením minimálnej úrovne bezpečnosti v rozsahu požiadavky na prijatie bezpečnostných opatrení podľa § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „ZoKB“), ako aj ďalších požiadaviek na ochranu citlivých informácií špecifických pre ten ktorý prvok vyplývajúci z bezpečnostného plánu prevádzkovateľa podľa § 10. Doplnenie povinnosti prijatia bezpečnostných opatrení podľa § 20 ZoKB je významné najmä z toho dôvodu, že v zmysle § 3 písm. k) ZoKB sa základnou službou rozumie každá služba, ktorá je zaradená v zozname základných služieb a je prvkom kritickej infraštruktúry, pričom jej prevádzkovateľ je povinný opatrenia podľa § 20 ZoKB prijať. Z uvedeného dôvodu je teda nevyhnutné, aby dodávateľia vo vzťahu k prvku sami spĺňali opatrenia zaisťujúce dôvernú, dostupnú a integritu citlivých informácií, s ktorými prídu pri plnení zmluvy do styku. Nakoľko v zmysle § 2 ods. 1 ZoKB platí, že ZoKB ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, nie je vylúčené a súčasne je žiadané, aby z obsahu bezpečnostného plánu podľa § 10 a s ohľadom na špecifickosť prvku vyplývali aj ďalšie opatrenia, ktoré by dodávateľ k tomuto prvku nad rámec § 20 ZoKB ako minimálnych opatrení na zabezpečenie kybernetickej bezpečnosti vo vzťahu k ochrane citlivých informácií mal plniť. Posledným opatrením významným vo vzťahu k ochrane citlivých informácií je povinnosť uzatvorenia zmluvy o sprístupnení citlivej informácie s vopred určenými podstatnými náležitosťami zmluvy v zmysle novovytvoreného ods. 2. Uvedené opatrenie slúži na precizovanie ďalších povinností na strane príjemcu citlivých informácií, a to s ohľadom na charakter citlivých informácií a potenciálne následky spojené s ich zneužitím. Opodstatnenie takejto požiadavky vyplýva aj z už existujúcej povinnosti v zmysle § 44 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností, kedy je daná povinnosť uzatvorenia obdobnej zmluvy pre prípad sprístupnenia utajovanej skutočnosti, pričom utajovanú skutočnosť je potrebné v tomto kontexte rovnako vykladať ako informáciu určitej citlivosti reprezentovanej potenciálnymi negatívnymi následkami spojenými s jej prípadným zneužitím. Nakoľko zmluvu o sprístupnení citlivej informácie je s ohľadom na jej obsahové náležitosti týkajúce sa prvku možné ako takú považovať za citlivú informáciu, resp. obsahujúcu citlivé informácie, výnimka zo sprístupňovania podľa zákona č. 211/2000 Z. z. o slobode informácií ostáva zachovaná. Zákonná povinnosť mlčanlivosti dodávateľa sa navrhuje upraviť rovnako, ako v prípade oprávnenej osoby podľa platného § 12 ods. 2. Vzhľadom k skutočnosti, že dodávka tovarov, uskutočnenie stavebných prác alebo poskytovanie služieb vo vzťahu k prvku môžu byť spojené aj s oboznamovaním sa s utajovanými skutočnosťami v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností, požiadavky na ochranu utajovaných skutočností nie sú žiadnym spôsobom novostanovenými požiadavkami a opatreniami § 10a dotknuté. V takom prípade dodávateľ súčasne sa oboznamujúci s utajovanými skutočnosťami bude teda povinný popri požiadavkách a opatreniach novovytvoreného § 10a spĺňať aj

*požiadavky a opatrenia podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností.*

5. V § 15 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Dodávateľ sa dopustí správneho deliktu na úseku kritickej infraštruktúry, ak poruší niektorú z povinností podľa § 10a.“.

Doterajšie odseky 2 až 7 sa označujú ako odseky 3 až 8.

**Odôvodnenie:**

*Navrhuje sa rozšírenie skutkovej podstaty správneho deliktu na úseku kritickej infraštruktúry aj v súvislosti s porušením povinnosti dodávateľa k prvku alebo týkajúcich sa prvku.*

6. V § 15 odsek 3 znie:

„(3) Ústredný orgán, v ktorého pôsobnosti došlo k porušeniu povinnosti zakladajúcej správny delikt, uloží pokutu

a) prevádzkovateľovi od 500 eur do 50 000 eur, ak poruší niektorú z povinností podľa § 9 ods. 2,

b) prevádzkovateľovi od 1 000 eur do 200 000 eur, ak poruší niektorú z povinností podľa § 9 ods. 1,

c) dodávateľovi od 1 000 eur do 200 000 eur, ak poruší niektorú z povinností podľa § 10a.“.

**Odôvodnenie:**

*V nadväznosti na rozšírenie skutkovej podstaty správneho deliktu na úseku kritickej infraštruktúry je aj v súvislosti s porušením povinnosti dodávateľa potrebné upraviť aj príslušnú výšku pokuty.*

7. V § 16 odsek 5 znie:

„(5) Ustanovenia § 1 ods. 1 písm. b) a c), § 2 písm. b), c), i), k) a l), § 4 písm. d), § 5 písm. e), f) a j), § 6 písm. b), c) a i), § 9 ods. 1 úvodnej vety, § 9 ods. 1 písm. a), b), e), g), h), i), j) a k), § 9 ods. 2 písm. a) a b), § 10 ods. 1 až 3, § 10a, § 16 ods. 2, § 17 ods. 3 a 4 a prílohy č. 2 sa vzťahujú aj na prvok európskej kritickej infraštruktúry.“.

**Odôvodnenie:**

*Vo výpočte ustanovení, ktoré sa vzťahujú aj na prvok európskej kritickej infraštruktúry, je potrebné zohľadniť doplnenia povinností prevádzkovateľa v § 9 ods. 1 písm. i, j a k, ako aj doplnenie nového ustanovenia § 10a.*

8. § 17 sa dopĺňa odsekmi 6 a 7, ktoré znejú:

„(6) Bezpečnostný plán a jeho aktualizácia, ku ktorým sa ústredný orgán vyjadril podľa tohto zákona v znení účinnom do 31. decembra 2019 sa považujú za schválené podľa

tohto zákona v znení účinnom od 1. januára 2020 a ich právne účinky zostávajú zachované.

(7) Dodávatelia, ktorí od prevádzkovateľa získali prístup k citlivým informáciám podľa tohto zákona v znení účinnom do 31. decembra 2019, sa vo vzťahu k tomuto prevádzkovateľovi považujú za dodávateľov preukázateľne spĺňajúcich požiadavky a opatrenia § 10a podľa tohto zákona v znení účinnom od 1. januára 2020.“.

**Odôvodnenie:**

*Navrhuje sa v prechodných ustanoveniach stanoviť fikcia schválenia tých bezpečnostných plánov, ku ktorým sa ústredný orgán vyjadril ešte pred účinnosťou tohto zákona, aby nevznikli pochybnosti o relevantnosti obsahu bezpečnostných plánov, ktoré prevádzkovatelia po vyjadrení ústredného orgánu zaviedli alebo priebežne zavádzajú. V odseku 7 sa navrhuje osobitne upraviť situáciu tých dodávateľov, ktorým pred dňom nadobudnutia účinnosti tohto zákona už boli citlivé informácie sprístupnené zo strany prevádzkovateľov prvkov kritickej infraštruktúry.*

Nasledujúce články sa primerane prečísľujú.

V nadväznosti na vloženie nového článku II sa upraví názov návrhu zákona.

## POZMEŇUJÚCI NÁVRH

poslanca Národnej rady Slovenskej republiky Ľubomíra Vážneho

k vládnemu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa mení zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (tlač 1615)

Meno a priezvisko

1. ĽUBOMÍR VÁŽNÝ
2. VLADIMÍR FAZÁR
3. Augustín Hambálek
4. MAROŠ KONDRÁT
5. PAVOL GOBÁ
6. Dušan Bušlany
7. MARIÁN KENY

Podpis





