**Dôvodová správa**

1. **Všeobecná časť**

Návrh zákona o výkone správy v oblasti informačných technológií verejnej správy a o zmene a doplnení niektorých zákonov sa predkladá na základe uznesenia vlády Slovenskej republiky č. 187/2016 z 18. mája 2016. Návrh zákona bol vypracovaný na základe legislatívneho zámeru, schváleného citovaným uznesením vlády Slovenskej republiky.

Informatizácia verejnej správy je riadený proces, ktorý sa realizuje v rámci celej štruktúry verejnej správy. Je to proces vytvárania spoločenských, legislatívnych, metodických, technologických a organizačno-personálnych podmienok pre efektívnu aplikáciu informačných technológií (ďalej len „IT“) vo výkone verejnej správy, ako aj riadený proces vlastnej aplikácie IT, pričom pod IT sa rozumie aj komunikačná infraštruktúra a komunikačné technológie, ktoré sú na prevádzku a používanie IT potrebné. Výsledkom tohto procesu by malo byť na jednej strane efektívne využívanie IT v procesoch verejnej správy a tomu zodpovedajúca úprava procesov verejnej správy a na strane druhej elektronická forma výkonu správy, t. j. e-Government.

Princípy informatizácie verejnej správy by preto mali byť založené na:

* právnom rámci, ktorý predstavuje systém všeobecne záväzných právnych predpisov, ale aj metodických aktov, ktoré spolu vytvárajú záväzné podmienky budovania informatizácie spoločnosti,
* infraštruktúre, ktorá je tvorená technologicko-komunikačnými prostriedkami (HW, WAN, LAN) a organizačným zabezpečením jej správy a prevádzky a predstavuje nástroje a prostriedky na výkon činností v rámci informatizácie a napĺňanie podmienok, ustanovených právnym rámcom,
* digitalizácii úsekov správy, ktorá predstavuje vlastnú aplikáciu IT v procesoch výkonu správy.

IT tvoria neoddeliteľnú súčasť výkonu verejnej správy a verejnej moci tak, že kvalita IT riešení má priamy vplyv na kvalitu ich výkonu. V protiklade k obdobiu, kedy vznikol a začal byť aplikovaný zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ISVS“) je dnešné obdobie charakterizované najmä dynamikou vývoja a zmien v oblasti IT. Stra­té­gia budovania IT riešení pre­to dnes už nez­na­me­ná len tvor­bu plá­nu (koncepcie), ale naj­mä tvor­bu pos­to­ja a rea­go­va­nie na zme­ny. Teda poskytnutie odpovedí na otázky čo také riešenie mu­sí spĺňať a čo mu­sí poskytovať, aby naj­lep­šie rea­go­va­lo na po­žia­dav­ky, kto­ré sa naň kla­dú. Tie­to odpovede sa po­tom pre­ta­vu­jú do kon­krét­nych ak­ti­vít v ob­las­tiach, ako je en­terpri­se ar­chi­tek­tú­ra, ma­naž­ment por­tfó­lia IT riešení, manažment riadenia projektov a manažment prevádzky informačno-komunikačných technológií (ďalej len „IKT“).

Najmä vplyvom globálnych trendov, zvýšených nárokov na IT a na stupeň digitalizácie a informatizácie spoločnosti stúpa zložitosť technológii, ako aj metód ich riadenia. Tento trend nie je možné ignorovať, nakoľko tieto technológie sú implementované aj v prostredí verejnej správy Slovenskej republiky. Očakávania používateľov a znalosti o IT tiež priebežne narastajú. Narastajú aj ich očakávania od dodávaných riešení.

Kým v minulom období sa dôraz z hľadiska právneho rámca kládol na technologický pohľad, teda na štandardy informačných systémov verejnej správy (ďalej len „ISVS“) a pohľad aplikačný, teda základné povinnosti pri správe IT riešení, po prijatí zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobností orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov došlo k posunu do roviny procesnej. Došlo k zavedeniu komplexnej úpravy, umožňujúcej elektronizáciu výkonu verejnej moci v celom priebehu konania orgánov verejnej moci a tým nepriamo aj k ustanoveniu požiadaviek na funkčnosť IT riešení, z hľadiska zabezpečenia elektronickej podoby výkonu verejnej moci.

Z pohľadu nastavenia správy ISVS však k tomuto posunu nedošlo, nehovoriac o nastavení pravidiel správy IT. Cieľom návrhu zákona je preto zmeniť základné filozofické a systémové nastavenie v tejto oblasti, ktoré dnes ustanovuje zákon o ISVS a rozšíriť oblasť úpravy z ISVS na správu IT verejnej správy (ďalej len „ITVS“) ako takých, aby boli jednotným spôsobom pokryté všetky oblasti vedenia a riadenia v správe ITVS, od fázy plánovania a organizácie až po monitoring a hodnotenie. Nadväzne na to je cieľom návrhu zákona ustanoviť jednotné vedenie pre výkon všetkých fáz riadenia v správe ITVS.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, nálezmi Ústavného súdu Slovenskej republiky, medzinárodnými zmluvami, ktorými je Slovenská republika viazaná a zákonmi a súčasne je v súlade s právom Európskej únie.

Prijatie navrhovaného zákona nemá sociálne vplyvy, ani vplyvy na životné prostredie, ani vplyvy na služby verejnej správy pre občana, avšak bude mať vplyvy na rozpočet verejnej správy, vplyvy na informatizáciu spoločnosti a vplyvy na podnikateľské prostredie.

 Účinnosť zákona sa navrhuje 1. mája 2019, pričom pre vybrané články návrhu zákona sa navrhuje účinnosť 1. január 2019.

1. **Osobitná časť**

K čl. I

K § 1:

Predmet a pôsobnosť návrhu zákona sú ustanovené vo vzťahu k informačným technológiám verejnej správy a k ich správe – teda k právam a povinnostiam orgánov riadenia a k podmienkam budovania informačných technológií verejnej správy. Základným východiskom ukladaných povinností orgánom riadenia, vyjadreným v § 1 ods. 1 písm. b), je to, že ich rozsah vychádza z ITVS, ktoré majú v správe alebo ktoré prevádzkujú. Znamená to, že pokiaľ spravujú alebo prevádzkujú aj ITVS, na ktoré sa tento zákon nevzťahuje (napr. ITVS vyňaté z pôsobnosti zákona podľa § 1 ods. 2), na tieto sa povinnosti orgánu riadenia neuplatňujú.

Negatívna vecná pôsobnosť je zachovaná vo vzťahu k informačným technológiám verejnej správy, ktoré slúžia na zabezpečenie obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, utajovaných skutočností a citlivých informácií podľa § 3 ods. 14 a 15 zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pokiaľ ide o oblasť bezpečnosti, vzťah medzi návrhom zákona a právnou úpravou kybernetickej bezpečnosti je vyjadrený ako vzťah špeciálnej úpravy k úprave všeobecnej. Tento princíp sa následne premieta do ustanovení o bezpečnosti tak, že v súlade so zákonom o kybernetickej bezpečnosti bude návrh zákona upravovať len obsah bezpečnostných opatrení a všetky ostatné povinnosti, postupy a mechanizmy budú použité podľa zákona o kybernetickej bezpečnosti. Cieľom je neustanovovať dve odlišné právne úpravy bezpečnosti pre informačné technológie verejnej správy, ale vytvoriť z nich kompaktný celok, ktorý sa navzájom dopĺňa.

K § 2:

Keďže podstatou prínosu návrhu zákona bude zmena v systéme vedenia a riadenia v správe informačných technológií verejnej správy, je potrebné definovať pojem „informačné technológie“. V spojení so všeobecnou definíciou, že ide o prostriedky a postupy spracúvania údajov a informácií v elektronickej podobe sa regulácia v oblasti správy navrhuje uplatniť nielen na programové prostriedky, technické prostriedky a informačné systémy, či infraštruktúru, ale aj na úzko súvisiace oblasti personálneho zabezpečenie a procesných postupov v oblasti informačných technológií a na údaje samotné. Pod pojmom „informačné technológie verejnej správy“ sa rozumejú také informačné technológie, ktoré slúžia na výkon pôsobnosti v oblasti, v ktorej osoba vykonáva verejnú správu.

Definície informačných systémov, ako aj delenie medzi správcu a prevádzkovateľa zostáva zachované v intenciách dnes platnej právnej úpravy.

K § 3:

Pre zachovanie sémantickej kontinuity sa v ďalších základných pojmoch v podstatnej miere vychádza zo súčasnej úpravy zákona č. 275/2006 Z.z. Vzhľadom na to, že sa navrhuje nová právna úprava, dochádza zároveň v určitej miere aj k ich úprave, vychádzajúc z posunu v oblasti legislatívy upravujúcej elektronizáciu výkonu verejnej moci.

K § 4:

Základné kompetenčné členenie v rámci správy informačných technológií je rozdelenie na činnosti vedenia, ktoré návrh zákona zveruje ústrednému orgánu štátnej správy v tejto oblasti a na činnosti riadenia, ktoré sú zverené orgánom, majúcim v správe jednotlivé informačné technológie.

Na najvyššej úrovni detailu je možné vyjadriť vzťahy a interakcie medzi vedením a riadením v  správe informačných technológií vyjadriť nasledovne:

 

K § 5:

Navrhuje sa ustanoviť základné povinnosti pri správe informačných technológií verejnej správy, ktoré zároveň budú pôsobiť ako princípy na účely výkladu jednotlivých povinností a posudzovania výkonu správy jednotlivými orgánmi. Cieľom ustanovených povinností je dosiahnuť jednotné prostredie informačných technológií a tým aj jednotný spôsob výkonu kompetencií dotknutých orgánov elektronickým spôsobom. Vzhľadom na zmeny v predošlých rokoch a na vybudovanie centrálnych komponentov e-Governmentu je jednou zo základných povinností využívanie už existujúcich riešení a zabránenie duplicitám, s dôrazom na efektívne vynakladanie verejných prostriedkov pri informatizácii spoločnosti. Keďže konečným „odberateľom“ výstupov informatizácie sú v zásadnej miere subjekty súkromného práva, ako adresáti práv a povinností v jednotlivých konaniach, ustanovuje sa aj povinnosť prihliadať na potreby a spätnú väzbu od týchto subjektov a v ich kontexte budovať a upravovať informačné technológie a ich pôsobenie.

K § 6:

Vedenie v správe informačných technológií návrh zákona ustanovuje ako ucelenú činnosť, smerujúcu k nastaveniu efektívneho prostredia informačných technológií tak, aby bolo možné dosiahnuť ciele informatizácie a rozvoja informačných technológií, ako ich predpokladajú koncepčné a strategické dokumenty a na ich základe prijaté všeobecne záväzné právne predpisy. Základnými cieľmi vedenia v správe bude efektívne využitie ľudských zdrojov, technických, programových a iných prostriedkov, zariadení, finančných prostriedkov a času spojeného s realizáciou projektov. V zmysle § 36 zákona č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov bude následne úrad podpredsedu zodpovedný za prehodnocovanie a úpravu nastavených pravidiel správy informačných technológií, na účely dosiahnutia stanovených cieľov, pričom sledovanie a vyhodnocovanie splnenia nastavených cieľov bude realizované v strategických dokumentoch, najmä v rámci pravidelného hodnotenia Národnej koncepcie informatizácie verejnej správy. Súčasťou vedenia v správe informačných technológií bude nevyhnutne monitorovanie a kontrola výkonu správy, ako nástroje na dosiahnutie výkonu správy informačných technológií v súlade so všeobecne záväznými právnymi predpismi, ako aj nástroje na získavanie spätnej väzby na účely vykonávania riadenia.

K § 7 až 9:

Vedenie v správe informačných technológií je činnosť v troch prepojených, ale samostatných oblastiach, a to

* usmerňovanie, ktorého obsahom bude najmä zjednocovanie spôsobov výkonu riadenia, a to na základe výsledkov vyhodnocovania výkonu riadenia v správe informačných technológií,
* vyhodnocovanie, ktorého obsahom bude najmä posudzovanie informácií získaných z monitorovania a iných podnetov, týkajúcich sa výkonu riadenia v správe informačných technológií a
* monitorovanie, ktorého obsahom bude najmä získavanie informácií na účely posudzovania výkonu riadenia v správe informačných technológií a na účely jeho usmerňovania.

Konkrétnymi výstupmi vedenia v správe informačných technológií bude najmä vytváranie pravidiel správy informačných technológií, optimalizácia jednotlivých riešení z hľadiska ich prínosu, s ohľadom na ich náklady, riadenie a optimalizácia rizík, optimalizácia vynakladaných zdrojov a zabezpečenie informovanosti a komunikácie s ohľadom na existujúce a plánované riešenia v oblasti informačných technológií a vyhodnocovanie podnetov dotknutých osôb.

Oblasť vytvárania pravidiel správy informačných technológií bude zahŕňať prípravu Národnej koncepcie informatizácie verejnej správy, vydávanie vykonávacích právnych predpisov podľa návrhu zákona, spoluprácu na tvorbe všeobecne záväzných právnych predpisov v oblasti informatizácie v pôsobnosti iných rezortov a metodickú činnosť.

Oblasti optimalizácie jednotlivých riešení, riadenia a optimalizácie rizík a optimalizácie vynakladaných zdrojov sú úzko spojené a ich výstupy budú dôležitým podkladom pre rozhodovanie v ostatných procesoch vedenia. Pôjde o činnosti, ktoré budú zabezpečované priebežne a ktoré budú spočívať v priebežnom posudzovaní existujúcich riešení a vytváraných riešení z hľadiska dosahovania cieľov, na ktoré sú určené či vytvárané, pri zohľadnení ich nákladov, z hľadiska ich rizík a z hľadiska existujúcich a plánovaných zdrojov, ktoré na ne majú byť vynaložené a ich dostupnosti. Cieľom týchto činností vedenia je zabezpečiť najväčší prínos riešenia s ohľadom na vynaložené náklady, identifikovať riziká a minimalizovať ich, ako aj udržiavať riziká najviac v určenej akceptovateľnej miere a tiež zabezpečiť, že ľudské, materiálne a finančné zdroje na rozvoj a správu informačných technológií budú dostupné pri vynaložení primeraných a optimálnych nákladov. Nástrojmi na dosahovanie a zabezpečenie týchto cieľov budú aj kontrola a ukladanie opatrení na nápravu zisteného stavu.

Oblasť zabezpečenia informovanosti a komunikácie spočíva v nastavení pravidiel poskytovania informácií smerom k úradu podpredsedu ohľadom informačných technológií v pôsobnosti orgánu riadenia, ako aj v nastavení odporúčaní na efektívnu komunikáciu medzi jednotlivými orgánmi, s cieľom dosiahnuť potrebnú mieru informovanosti medzi nimi, na účely poskytovania si vzájomnej súčinnosti a dosahovaniu synergií v tejto oblasti. Osobitnou povinnosťou je povinnosť poskytovania pravidelných informácií vláde o stave rozvoja a správy informačných technológií.

Základným strategickým nástrojom vedenia v správe informačných technológií bude naďalej Národná koncepcia informatizácie verejnej správy, ktorej právna úprava sa preberá z dnešnej platnej právnej úpravy.

K § 10 až 12:

Pod riadením v správe informačných technológií návrh zákona rozumie činnosti vykonávané príslušným orgánom vo vzťahu k informačným technológiám, s trvalým cieľom zabezpečovať a zlepšovať podmienky na výkon svojej pôsobnosti v elektronickej podobe. Riadenie v správe informačných technológií by malo byť charakterizované aktívnosťou, iniciatívou, zameraním na trvalý rozvoj informatizácie v pôsobnosti orgánu, pri dodržiavaní všeobecne záväzných právnych predpisov a realizácii pôsobnosti v rámci výkonu verejnej moci či iných úloh vo verejnom záujme.

Z personálneho hľadiska je pôsobnosť návrhu zákona ustanovená na orgány, ktoré sú aj podľa dnešného právneho stavu povinnými osobami. Vzhľadom na skutočnosť, že rozsah povinných osôb sa osvedčil, aj návrh zákona vychádza z tohto rozsahu a ponecháva ho nezmenený.

Dôležitým princípom je nastavenie „škálovania“ rozsahu a spôsobu plnenia povinností vo vzťahu jednak ku kategóriám informačných technológií a údajov, ktoré spracúvajú, ako aj vo vzťahu k veľkosti projektov ich budovania, servisu, či zmien. Keďže návrh zákona o kybernetickej bezpečnosti zavádza na účely nastavenia bezpečnostných opatrení mechanizmus tejto kategorizácie, navrhuje sa aj na účely riadenia v správe informačných technológií vychádzať z tejto kategorizácie a tým predísť duplicitným, či rozdielnym právnym úpravám v jednej oblasti. Princíp, ktorý sa navrhuje uplatniť spočíva v tom, že návrh zákona pomenuje najširší možný rozsah a spôsob plnenia povinností v riadení informačných technológií, pričom vykonávacie predpisy, okrem podrobností, ustanovia aj spôsob, akým sa pre konkrétne kategórie tieto povinnosti uplatnia, ktoré sa budú vyžadovať v plnom rozsahu a ktoré, vzhľadom napríklad na dôležitosť systému, nebudú v konkrétnom prípade vyžadované. Keďže oblasť informačných technológií verejnej správy je rozsiahla a nie je homogénna ani z pohľadu činností, na ktoré technológie slúžia a ani z pohľadu dôležitosti, ktorú jednotlivé technológie majú, je tento mechanizmus zvolený ako vhodný spôsob, akým bude možné nastaviť rozsah povinností na konkrétne podmienky orgánu pri riadení jeho informačných technológií.

Návrh zákona pri ustanovení konkrétnych povinností vychádza z dnes platnej právnej úpravy, a to tak na úseku informačných systémov verejnej správy, ako aj na úseku pravidiel e-Governmentu. Zmenou, ktorú návrh zákona prináša, je teda najmä rozšírenie oblastí regulácie riadenia v správe informačných technológií, ako aj ustanovenie jednotného spôsobu plnenia povinností v rámci tohto riadenia. Kým dnešná právna úprava kladie dôraz na fázu prevádzky a regulácie technických štandardov, návrh zákona chápe riadenie v správe informačných technológií širšie – ako činnosť, ktorá začína už pri plánovaní a nastavovaní podmienok na realizáciu riadenia, pokračuje samotným obstaraním informačných technológií a ich implementáciou a cez fázu prevádzky a servisu presahuje aj do monitoringu a hodnotenia.

Obdobne, ako podľa platnej právnej úpravy zostáva v podmienkach jednotlivých správcov základným koncepčným dokumentom koncepcia rozvoja informačných technológií, ktorej regulácia vychádza z dnes platného právneho stavu.

K § 13:

Oblasť plánovania a organizácie obsahuje povinnosti, smerujúce dovnútra organizácie, ktoré sa týkajú nastavenia systému riadenia, určenie stratégie rozvoja a riadenia a predovšetkým architektúry informačných technológií, nastavenia organizačnej štruktúry, procesov a nástrojov, potrebných na riadenie v správe informačných technológií, riadenia kľúčových zdrojov, ktorými sú ľudské zdroje, finančné prostriedky a prípadné externé kapacity a nastavenie systému riadenia kvality, rizík a bezpečnosti.

Cieľom regulácie v tejto oblasti je najmä nastavenie dlhodobej a udržateľnej stratégie rozvoja a stratégie riadenia v správe informačných technológií, ktorá zadefinuje ciele orgánu v danej oblasti, ako aj rámcové nástroje na ich dosiahnutie. V súlade so stratégiou sa ustanovuje povinnosť vytvoriť také organizačné a procesné podmienky, aby jednak bolo možné realizovať povinnosti v riadení v správe informačných technológií a tiež realizovať určené strategické ciele. Medzi organizačné podmienky budú patriť najmä určenie zodpovedných organizačných útvarov a riadiacich pozícií, a to jednotne pre všetky orgány, vrátane základných personálnych predpokladov ich obsadenia. Procesné podmienky na druhej stane budú predstavovať najmä určenie postupov vo vzťahu k riadeniu a kontrole dodržiavania všeobecne záväzných právnych predpisov v tejto oblasti, ako aj k riadeniu kvality, rizík a bezpečnosti v rámci povinnej osoby, počas celého výkonu riadenia v správe informačných technológií. Aspekty riadenia bezpečnosti sú spresnené v samostatnom § 18. Dôraz za kladie aj na oblasť riadenia zmlúv o poskytovaní služieb, ktoré smerujú k aktívnemu riadeniu SLA služieb ktoré organizácia poskytuje, alebo odoberá.

K § 14:

Oblasť obstarania a implementácie reguluje v prvom rade činnosti pri realizácii projektov budovania informačných technológií, spojených s riadením projektov, identifikovaním požiadaviek na riešenia a podmienok ich realizácie, potrebou zabezpečenia zdrojov, vykonaním potrebných zmien na úrovni organizačnej, ale aj procesnej, riadením jednotlivých zdrojov a riadením konfigurácii.

Pre úplnosť je potrebné výslovne uviesť, že tento zákon nie je osobitným predpisom vo vzťahu k procesu verejného obstarávania a ani nevstupuje do procesov obstarávania, ktoré sú upravené zákonom o verejnom obstarávaní.

Cieľom je v prvom rade zabezpečiť, aby všetky realizované projekty v oblasti informačných technológií boli uskutočňované v súlade s definovanou stratégiou rozvoja a správy informačných technológií, vychádzajúc z plánovaného a koordinovaného postupu a realizované s použitím štandardných modelov projektového riadenia. Na dosiahnutie tohto cieľa sa navrhuje pred začatím projektu riadne identifikovať a popísať funkčné a technické požiadavky, vrátane identifikácie a úrovne možných rizík, s ohľadom na reálne potreby orgánu a so zohľadnením dopadov zvoleného riešenia a dostupnými zdrojmi na jeho realizáciu. Osobitnou časťou prípravy projektu musí byť zhodnotenie alternatívnych riešení, z technického aj ekonomického pohľadu a ekonomické zdôvodnenie projektu.

Dvomi zásadnými novými povinnosťami sú povinnosť zmluvného dojednania licenčných podmienok v súlade s EUPL pre tie informačné systémy, ktoré budú vyvíjané, ako aj povinnosť nastaviť zmluvné vzťahy na dodanie čiastkových plnení veľkých projektov alebo projektov, ktoré nepozostávajú len z dodania jedného funkčného celku tak, aby každé z nich malo svoj vlastný prínos a po každom z nich bolo možné projekt ukončiť. Čiastkovým plnením sa rozumie také dodanie tovaru alebo služby, ktoré predstavuje časť celkového plnenia, na ktoré je uzavretá zmluva – v praxi je ho možné chápať aj ako tzv. míľnik. Podmienky, ktoré sa naň kladú by mali viesť k tomu, aby boli čiastkové plnenia v zmluve nastavené tak, že po vykonaní príslušnej časti vznikne v nejakom zmysle funkčne „samostatne použiteľný“ výstup aj v prípade, ak sa celkové dodanie nezrealizuje.

Dôvodom týchto nových povinností je jednak snaha vyhnúť sa tzv. vendor lock-in stavu a tiež snaha umožniť pri budovaní systémov v každom momente prehodnotiť potreby orgánu najmä z hľadiska funkčnosti systému a nebyť viazaný dodaním celého riešenia, ak aj jeho čiastkové dodanie z funkčného hľadiska postačuje pre potreby plnenia úloh odberateľa. Od licenčných podmienok v súlade s EUPL pre vyvíjané riešenia sa okrem pozitívneho ekonomického a prevádzkového dopadu z titulu eliminácie vendor lock-in stavu, očakáva aj zlepšenie kontroly nad vyvíjanými riešeniami a tým pádom aj zlepšenie kvality dodávaných riešení.

Vo fáze implementácie riešenia sa navrhuje ustanoviť povinnosti vo vzťahu k realizácii zmien, ktoré si predmetné riešenie vyžiada a správnemu nakladaniu s existujúcimi zdrojmi, potrebnými na realizáciu daného riešenia. Aktívami sa rozumejú najmä technické a programové vybavenie, vrátane práv duševného vlastníctva, ktoré majú pre orgán riadenia hodnotu. Ich zdieľanie je vždy podmienené v prvom rade splnením podmienok, ktoré na takéto nakladanie s nimi kladú osobitné predpisy alebo zmluvné dojednania. Súčasne s tým sa navrhuje ustanoviť povinnosti, ktoré zabezpečia udržiavanie technických informácií o realizovanom riešení v aktuálnom a správnom stave, vrátane informácií o väzbách medzi jednotlivými jeho prvkami.

Na účely zabezpečenia riadneho plnenia povinností v oblasti obstarania a implementácie informačných technológií dopĺňa komplex povinností jednotlivých orgánov aj oprávnenia úradu podpredsedu vo vzťahu k schvaľovaniu konkrétnej koncepcie budovania či rozvoja informačných technológií, ako aj projektu realizácie tohto budovania či rozvoja.

Pokiaľ ide o povinnosť zverejňovania projektovej dokumentácie, jej realizácia má byť taká, že správca síce nezverejní „citlivé“ časti, avšak uvedie, ktoré časti neboli zverejnené - inými slovami zabezpečí, aby bolo z dokumentu zrejmé, čo sa nezverejnilo.

K § 15:

Oblasť prevádzky, servisu a podpory zodpovedá v jej základnom nastavení dnešným, všeobecne ustanoveným povinnostiam vo vzťahu k plynulosti a bezpečnosti prevádzky informačných systémov verejnej správy. V jej rámci sa navrhujú ustanoviť povinnosti smerujúce k zabezpečeniu plynulej a spoľahlivej prevádzky, odstraňovania porúch a problémov pri prevádzke a kontroly prevádzky, ako aj k nastaveniu postupov vo vzťahu k poskytovaniu služieb pri poruchách a problémoch pri prevádzke informačných technológií.

Cieľom je zabezpečenie riadneho poskytovania elektronických služieb, teda riadneho výkonu pôsobnosti dotknutého orgánu. Ide o oblasť, ktorá je podľa dnešného právneho stavu regulovaná najviac, preto návrh zákona prináša len zmeny vo vzťahu k určeniu jednotného spôsobu zabezpečenia riadnej prevádzky, riešenia situácií, kedy dôjde k poruchám, chybám a výpadkom a nastavenie požadovaných úrovní tohto riešenia, ako aj zabezpečenie bezpečnosti a riadenia prístupov k spracúvaným údajom.

K § 16:

Oblasť monitoringu a hodnotenia výkonu riadenia v správe informačných technológií je sústredená na tri vecné okruhy, a to riadne fungovanie prostredia IT informačných technológií, systém kontroly a súlad s podmienkami ustanovenými všeobecne záväznými právnymi predpismi.

Ustanovenia upravujú kontrolu vykonávanú priamo orgánom, ktorá zahŕňa v prvom rade pravidelné monitorovanie prostredia informačných technológií, zber údajov o jeho fungovaní a vyhodnocovanie splnenia funkčných a výkonnostných požiadaviek. V rámci monitoringu a hodnotenia výkonu je ustanovená povinnosť pravidelne monitorovať a vyhodnocovať účinnosť nastavených postupov kontroly a navrhovať ich úpravu, ak nefungujú riadne. Informácie monitoringu a hodnotenia výkonu riadenia v správe informačných technológií budú verejne prístupné.

Osobitným okruhom monitoringu a kontroly je posudzovanie zhody (compliance), teda vnútorné postupy, ktorých úlohou je zabezpečiť, že všetky riadenie v správe informačných technológií a fungovanie informačných technológií sú v súlade so všeobecne záväznými právnymi predpismi a ostatnými záväznými požiadavkami, napríklad zmluvného charakteru.

K § 17 až 21:

Oblasť bezpečnosti informačných technológií sa navrhuje upraviť v úzkej súčinnosti s postupmi a opatreniami, ktoré budú ustanovené návrhom zákona o kybernetickej bezpečnosti. Keďže predmetný zákon ustanovuje oblasť informačných systémov verejnej správy ako osobitný podsektor a zavádza reguláciu tak systémov, ako aj ich prevádzkovateľov, vrátane nahlasovania a riešenia bezpečnostných incidentov, dochádza do veľkej miery k prekryvu s tým, čo sa v oblasti bezpečnosti informačných technológií navrhuje regulovať v tomto návrhu zákona. Z toho dôvodu sa navrhuje ponechať pre informačných technológií podľa tohto zákona celý režim návrhu zákona o kybernetickej bezpečnosti s tým, že „len“ samotný obsah a rozsah bezpečnostných opatrení, ako aj povinnosť vypracúvať bezpečnostný projekt, budú ustanovené týmto návrhom zákona.

Táto oblasť je z dôvodu prehľadnosti pre špecifickú tému bezpečnosti uvedená v samostatných paragrafoch §17 až §22 a jednotlivé ustanovenia sú zosúladené s oblasťami riadenia v správe informačných technológií. V časti bezpečnosti informačných technológii verejnej správy v oblasti plánovania a organizácie sa jedná najmä o nastavenie pravidiel pre zavedenie systému riadenia informačnej bezpečnosti v organizácii. K organizačne procesným podmienkam patria činnosti, ktoré majú vykonávať riadiace, výkonné a kontrolné zložky systému riadenia bezpečnosti.

V ďalších častiach je regulácia koncipovaná predovšetkým s dôrazom na životný cyklus informačného systému verejnej správy. Stanovujú sa špecifické povinnosti v oblasti bezpečnosti informačných systémov verejnej správy pri plánovaní, vytváraní alebo nadobudnutí, ďalej tiež pri zavedení, prevádzke a vyradení informačného systému verejnej správy.

K § 22:

Dôležitým nástrojom pre komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek a návrh spôsobu ich efektívneho naplnenia je bezpečnostný projekt informačného systému. Inštitút bezpečnostného projektu je taktiež previazaný na životný cyklus informačného systému verejnej správy. Špecificky vypracovávanie bezpečnostného projektu je previazané na riadenie aktív v informačných technológiách verejnej správy uvedené v §14 ods. 8, pričom toto ustanovenie je východiskové pre plnenie viacerých povinností v § 17 až 22, a keď nie je priamo uvedené v časti bezpečnosti.

Bezpečnostný projekt sa povinne vypracúva pre tie informačné systémy verejnej správy, ktoré sú z hľadiska klasifikácie považované za „najdôležitejšie“, resp. „najviac kritické“. Pre ostatné systémy je možné uložiť povinnosť vypracovať bezpečnostný projekt len z dôvodu výsledkov bezpečnostného auditu alebo penetračných testov, ktoré preukážu nedostatky v bezpečnosti takého charakteru, ktorý si vyžaduje vypracovanie bezpečnostného projektu.

Osobitnou úpravou je úprava vo vzťahu k nahlasovaniu, riešeniu a spolupráci pri riešení bezpečnostných incidentov, ktoré nie sú pokryté reguláciou nahlasovania a ukladania povinností riešiť incident podľa zákona o kybernetickej bezpečnosti. Ide o svojho druhu nadstavbu k zákonu o kybernetickej bezpečnosti, ktorá, v súlade s týmto zákonom, rozširuje požiadavky na zabezpečenie sietí a informačných systémov v sektore informačných systémov verejnej správy, s cieľom dosiahnuť vyššiu úroveň ich bezpečnosti.

K § 23:

Oblasť technických štandardov sa navrhuje upravovať rovnakým spôsobom ako doteraz, teda vykonávacím predpisom k návrhu zákona.

Pokiaľ ide o normy a referenčné rámce vo vzťahu k novým pravidlám správy ITVS, návrh zákona a podzákonné predpisy budú vychádzať najmä z týchto dokumentov:

* COBIT® 5,
* STN ISO/IEC 38500: 2011 Korporátna governancia informačných technológií (37 9791),
* STN ISO/IEC 20000-1: 2014 Informačné technológie. Manažérstvo služieb. Časť 1: Požiadavky na systém manažérstva služieb (36 9788),
* STN ISO/IEC 20000-2: 2008 Informačné technológie. Manažment služieb. Časť 2: Odporúčania z praxe (36 9788),
* ITIL® v3,
* TOGAF® v9.

K § 24:

Úprava základných číselníkov sa preberá z dnes platného zákona č. 275/2006 Z.z., pričom vychádzajúc z praktických skúseností sa všetky základné číselníky navrhujú upravovať ich zverejňovaním v centrálnom metainformačnom systéme verejnej správy a nie vo vykonávacom predpise.

K § 25:

Úprava vydávania elektronických odpisov a listinných výstupov z informačných systémov verejnej správy sa preberá z dnes platného zákona č. 275/2006 Z.z.

K § 26:

Predmetné ustanovenia sú jedným z mechanizmov, ktorým bude možné pružne reagovať na „prílišnú tvrdosť zákona“ v prípadoch, kedy by plnenie povinností na úseku správy informačných technológií mohlo ohroziť riadne fungovanie dotknutého orgánu, pričom vzhľadom na dotknuté informačné technológie nie je pre ich fungovanie nevyhnutné, aby podliehali celej sade pravidiel podľa tohto zákona. Udelenie výnimky podlieha predchádzajúcemu posúdeniu každej situácie a musí byť následne zverejnené. Navrhuje sa, aby sa takýmto spôsobom dala udeliť aj bloková výnimka pre konkrétne druhy informačných technológií alebo skupiny ich správcov.

Ustanovenie je inšpirované úpravou v predošlom zákone o verejnom obstarávaní (zákon č. 25/2006 Z.z.), ktorý v § 1 ods. 5 umožňoval obdobným spôsobom udeľovať výnimky z podlimitných postupov vo verejnom obstarávaní.

K § 27:

Obdobne, ako v predošlom paragrafe, sa navrhuje ustanoviť možnosť „výnimky“, avšak nie z plnenia povinností podľa zákona, ale zo subjektu, ktorý ich je povinný plniť. Predmetné ustanovenie reflektuje existenciu združenia DEUS, ktorého základným poslaním je práve aj výkon niektorých činností správy za obce a mestá. V obdobnom režime tiež umožňuje zakladateľom a zriaďovateľom plniť povinnosti za nimi založené a zriadené osoby, čím sa tiež umožní naplnenie princípu hospodárnosti a efektívnosti pri výkone správy informačných technológií.

K § 28:

Systém správnych deliktov je upravený obdobne, ako v dnes platnom zákone č. 275/2006 Z.z.. Za porušenie povinností budú ako sankcie ukladané pokuty, pričom návrh zákona ustanovuje skutkové podstaty správnych deliktov pre najzávažnejšie porušenia povinností s osobitnými sadzbami pokút a všeobecnú skutkovú podstatu porušenia inej zákonnej povinnosti s jednotnou sadzbou pokuty.

K § 29:

Na účely odstránenia praktických problémov pri aplikácii predpisov o správe majetku štátu v oblasti zmeny v osobe užívateľa informačného systému, sa navrhuje upraviť osobitný inštitút zmluvy o užívaní informačného systému vo vlastníctve Slovenskej republiky, ktorá by okrem užívania mohla upravovať aj vzťahy súvisiace s jeho rozvojom a rozširovaním. Umožní sa tým inštitucionalizovať zmluvnú bázu pre tento postup, ktorý sa v praxi využíva.

Tiež sa navrhuje prebrať dnes platné ustanovenie, na základe ktorého je možné uskutočňovať výpožičky technického a programového vybavenia medzi jednotlivými správcami majetku štátu a z praktického hľadiska ich rozšíriť aj na obce a vyššie územné celky.

K § 30:

Splnomocňovacími ustanoveniami sa navrhuje upraviť základ pre vydávanie podzákonných predpisov v oblastiach, v ktorých úpravu podrobností, či iných náležitostí regulácie návrh zákona predpokladá.

K § 31:

Navrhuje sa zachovať účinnosť dnes vydaného vykonávacieho predpisu do doby, kým bude účinný nový vykonávací predpis k návrhu zákona. Dôvodom je zabezpečenie kontinuity v oblasti štandardov pre informačné systémy verejnej správy

K § 32:

Navrhujú sa prechodné ustanovenia k existujúcemu právnemu stavu, ktorých cieľom je v prvom rade zabezpečiť kontinuitu existujúcich inštitútov.

Pokiaľ ide o nové povinnosti, navrhuje sa dostatočné časové obdobie na prispôsobenie sa, najmä pre správcov a prevádzkovateľov informačných systémov verejnej správy.

K § 33:

Navrhuje sa ustanoviť odkaz na prílohu s uvedením transponovanej smernice.

K § 34

Navrhuje sa zrušenie dnes účinných právnych predpisov, ktoré budú nahradené návrhom zákona a k nemu vydaného podzákonného predpisu.

K čl. II

Predmetná novela preberá dnes platný právny stav v oblasti posudzovania systémov zberu vyhlásení o podpore iniciatívy občanov. Vzhľadom na to, že vecne je táto úprava najbližšie petičnému právu, navrhuje sa jej začlenenie do zákona o petičnom práve.

K čl. III a IV

K bodu 1:

Navrhnutým doplnením § 38 odseku 2 zákona o NBS sa vytvárajú legislatívne predpoklady na plnohodnotné plnenie činností Národnej banky Slovenska (NBS) v rámci Eurosystému, ktoré aj pre NBS vyplývajú z osvedčených postupov vydaných Európskou centrálnou bankou na výber a poverovanie externých audítorov pre centrálne banky Eurosystému (Good practices for the selection and mandate of External Auditors for the Eurosystem central banks), ktoré Európska centrálna banky vydala v záujme zabezpečiť v rámci celého Eurosystému harmonizovanú implementáciu ustanovení čl. 27 ods. 27.1 Protokolu o Štatúte o Štatúte Európskeho systému centrálnych bánk (ESCB) a Európskej centrálnej banky (ECB) v platnom znení. Pritom navrhnutú úpravu dosiaľ neobsahuje zákon o NBS ani žiadny iný slovenský právny predpis a práve preto navrhnuté doplnenie § 38 ods. 2 zákona o NBS je potrebné v SR na zabezpečenie harmonizovanej implementácie ustanovení čl. 27 ods. 27.1 Protokolu o Štatúte ESCB a ECB v zmysle vydaných osvedčených postupov ECB na výber a poverovanie externých audítorov pre centrálne banky Eurosystému.

K bodom 2 a 3:

V nadväznosti na Smernicu Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora sa navrhuje vztiahnuť ustanovenia o používaní štandardov prístupnosti pre webové sídla a mobilné aplikácie aj na subjekty, ktoré nie sú zahrnuté v osobnej pôsobnosti návrhu zákona.

K čl. IV

V nadväznosti na Smernicu Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora sa navrhuje vztiahnuť ustanovenia o používaní štandardov prístupnosti pre webové sídla a mobilné aplikácie aj na subjekty, ktoré nie sú zahrnuté v osobnej pôsobnosti návrhu zákona.

K čl. V

Navrhuje sa posunúť dátum povinnej aktivácie elektronickej schránky pre právnické osoby, nezapísané v obchodnom registri, a to v nadväznosti na priebeh zavádzania registra mimovládnych neziskových organizácií.

K čl. VI:

Za účelom vytvorenia dostatočného časového priestoru na zabezpečenie nastavenia centrálneho informačného systému štátnej služby (ďalej len „CISŠS“), jeho implementácie a plynulej prevádzky, sa posúva účinnosť zriadenia registra štátnozamestnaneckých miest a registra štátnych zamestnancov, ktoré majú byť jeho súčasťou. Vzhľadom na úzku vecnú aj technickú prepojenosť registra štátnozamestnaneckých miest s registrom štátnych zamestnancov sa ustanovuje zriadenie oboch registrov k jednému spoločnému dátumu, a to k 1. augustu 2021. V súvislosti so spomínanými registrami je potrebné o. i. vykonať technicky zložité interné integrácie na súvisiace registre CISŠS, externé integrácie na iné informačné systémy verejnej správy, prepojiť CISŠS (registre) s vládnym cloudom a vykonať ďalšie súvisiace migrácie. Nastavenie registrov zároveň ovplyvňuje aj prijatie nového zákona
č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a európska legislatívu o ochrane osobných údajov.

K čl. VII:

Účinnosť sa navrhuje 1. mája 2019, z dôvodu poskytnutia legisvakančnej lehoty na prispôsobenie sa navrhovaným zmenám. Vo vzťahu k ustanoveniam, zavádzajúcim povinnosti s dopadom na organizačné a technické, ale aj finančné zabezpečenie, sa navrhuje prechodné obdobie na splnenie nových povinností.

Pokiaľ ide o ustanovenia čl. V, účinnosť sa navrhuje 1. januára 2019.