95

ZÁKON

z 27. marca 2019

o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

Základné ustanovenia

§ 1

(1) Tento zákon ustanovuje

a) organizáciu správy informačných technológií verejnej správy,

b) práva a povinnosti orgánu vedenia a orgánu riadenia v oblasti informačných technológií verejnej správy, na ktoré sa vzťahuje tento zákon,

c) základné požiadavky kladené na informačné technológie verejnej správy a na ich správu.

(2) Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky[1]) a bezpečnosti Slovenskej republiky.[1a]) Tento zákon sa nevzťahuje na skutočnosti, ktoré sú podľa osobitných predpisov utajované[1b]) a informácie, ktoré sú podľa osobitných predpisov citlivé.[2]) ~~Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností[1]) a citlivých informácií.[2])~~

(3) Tento zákon sa vzťahuje aj na správcov, ktorí sú prevádzkovateľmi základnej služby[2a]) alebo poskytovateľmi digitálnej služby[2b]) podľa osobitného predpisu;[3]) ich povinnosti a oprávnenia podľa osobitného predpisu[3]) týmto zákonom nie sú dotknuté. ~~Na správcov informačných technológií verejnej správy, ktorí sú prevádzkovateľmi základnej služby[2a]) alebo poskytovateľmi digitálnej služby[2b]) sa vzťahuje všeobecný predpis o kybernetickej bezpečnosti,[3]) ak tento zákon neustanovuje inak. Na informačné technológie verejnej správy sa vzťahuje osobitný predpis,[3]) ak tento zákon v § 18 až 22 neustanovuje inak.~~

(4) Tento zákon sa v rozsahu ustanovenom osobitnými predpismi[4]) vzťahuje aj na osoby, o ktorých to tieto osobitné predpisy ustanovia.

(5) Na webové sídla a mobilné aplikácie orgánu riadenia podľa osobitného predpisu[4a]) sa nevzťahujú štandardy, ktoré sa týkajú štandardov pre prístupnosť a funkčnosť webových sídiel a mobilných aplikácií, ako aj minimálne požiadavky na obsah webových sídiel.

§ 2

(1) Informačnou technológiou je na účely tohto zákona prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.

(2) Informačným systémom je na účely tohto zákona funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

(3) Informačnou technológiou verejnej správy je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe.

(4) Informačným systémom verejnej správy je informačný systém v pôsobnosti správcu

podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

(5) Správcom na účely tohto zákona je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.

(6) Prevádzkovateľom je na účely tohto zákona správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba. Správcom určený alebo osobitným predpisom ustanovený prevádzkovateľ vykonáva, v rozsahu povinností správcu, činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis; ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu. Určením alebo ustanovením prevádzkovateľa nie je dotknutá zodpovednosť správcu za plnenie povinností podľa tohto zákona.

§ 3

Na účely tohto zákona sa ďalej rozumie

a) informačnou činnosťou získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov,
b) metainformačným systémom verejnej správy informačný systém verejnej správy, prostredníctvom ktorého sa zhromažďujú a sprístupňujú informácie, ktoré bližšie špecifikujú určené kvalitatívne a kvantitatívne charakteristiky určených údajov, a ktorý umožňuje najmä ich vyhľadávanie, katalogizáciu a využívanie,
c) centrálnym metainformačným systémom verejnej správy informačný systém verejnej správy, ktorého obsahom sú najmä technologické, administratívne a organizačné údaje o prevádzkovaných informačných technológiách verejnej správy,
d) nadrezortným informačným systémom verejnej správy informačný systém verejnej správy, ktorý do hierarchicky vyššieho informačného systému verejnej správy v pôsobnosti jedného správcu hierarchicky integruje spoločné časti jednotlivých informačných systémov verejnej správy, ktoré sú v pôsobnosti iných správcov,
e) neverejnou časťou informačného systému verejnej správy časť informačného systému verejnej správy prístupná len pre orgán verejnej moci na základe schváleného prístupu v súlade s jeho právomocami, právami a povinnosťami, ktoré sú ustanovené osobitným predpisom,
f) infraštruktúrou technologicko-komunikačné prostredie zabezpečujúce implementáciu a prevádzkovanie informačných systémov verejnej správy, poskytovanie a rozvoj elektronických služieb verejnej správy,
g) integrovanou infraštruktúrou koordinovane budovaná a prevádzkovaná infraštruktúra zabezpečujúca prevádzku informačných systémov verejnej správy v centralizovanej architektúre,
h) centrálnou informačnou infraštruktúrou nadrezortné informačné systémy v správe ústredného orgánu štátnej správy a zároveň využívajúce spoločné moduly[5]) a ústredný portál verejnej správy[6]) (ďalej len „ústredný portál“),
i) technologickou infraštruktúrou sústava vzájomne prepojených technických prostriedkov a programových prostriedkov umožňujúcich implementáciu a prevádzku informačných systémov verejnej správy,
j) komunikačnou infraštruktúrou káblové, bezdrôtové, optické a iné prepojenia, pasívne prepojovacie prvky a aktívne prepojovacie prvky a súvisiace programové prostriedky, ktoré tvoria oddelenú neverejnú sieť určenú na vzájomnú bezpečnú komunikáciu orgánov riadeniaa na sprostredkovanie ich externej komunikácie s inými osobami,
k) službou verejnej správy výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsaha spôsob výkonu ustanovuje osobitný predpis,
l) elektronickou službou verejnej správy elektronická komunikácia s orgánom riadenia pri vybavovaní podania, oznámenia, pri prístupe k informáciám a ich poskytovaní alebo pri účasti

verejnosti na správe verejných vecí,

m) službou vo verejnom záujme výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah ustanovuje osobitný predpis, pričom spôsob jej výkonu osobitný predpis neustanovuje,

n) verejnou službou činnosť orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis a ktorej výsledok možno použiť pri výkone služby verejnej správy a služby vo verejnom záujme,

o) úsekom verejnej správy vecná oblasť, v ktorej právomoci, práva a povinnosti orgánu riadenia, ako aj spôsob ich výkonu ustanovuje osobitný predpis a ktorá obsahuje najmenej dve agendy verejnej správy,

p) agendou verejnej správy ucelený súhrn činností na konkrétnom úseku verejnej správy, ktoré vrátane spôsobu ich výkonu ustanovuje osobitný predpis,

q) životnou situáciou udalosť v živote fyzickej osoby alebo v životnom cykle právnickej osoby, ktorá je riešená službami verejnej správy, ako aj spôsob usporiadania služieb verejnej správyz ~~užívateľského~~ používateľského pohľadu osoby pri výkone práv a povinností vo vzťahu k orgánom riadenia,

r) číselníkom zoznam prípustných hodnôt údajového prvku, z ktorého sa hodnota preberá na základe definovaného kódu, ktorým môže byť aj textový reťazec,

s) webovou stránkou online dostupné miesto na sieti, najmä na internete, sprístupňované prostredníctvom webového prehliadača a využívajúce hypertextový prenosový protokol alebo jeho zabezpečenú verziu, ktoré tvorí jednu vizuálnu obrazovku webového sídla, aj ak je zložené z viacerých rámov,

t) webovým sídlom ucelený súbor webových stránok v pôsobnosti jedného správcu, ktorý má pridelenú najmenej jednu doménu a je prezentačným komponentom a technologickým rozhraním informačného systému verejnej správy.

u) ~~zraniteľnosťou slabé miesto, náchylnosť alebo chyba prostriedku, systému, procesu alebo kontroly, zneužiteľné v rámci hrozby[6aa]) pre informačnú technológiu,~~ aktívom programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno orgánu riadenia a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje orgán riadenia za citlivú,

v) ~~aktívom programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno orgánu riadenia a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje orgán riadenia za citlivú~~ strategickou architektúrou definovanie vysokoúrovňových cieľov, vízie a strategického smerovania organizácie ako celku,~~.~~

~~t)~~w) referenčnou architektúrou zoskupenie referenčných architektonických materiálov a podkladov, ktoré sa opakovan~~i~~e používajú pri špecifických opakujúcich sa aktivitách organizácie ako celku.

§ 4

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „ministerstvo investícií“)

a) zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu,

b) je správcom vládneho elektronického komunikačného systému Govnet podľa § 24b.

§ 5

Organizácia správy informačných technológií verejnej správy

(1) Správu informačných technológií verejnej správy vykonávajú

a) orgán vedenia, ktorým je ministerstvo investícií,

b) orgán riadenia vo vzťahu k informačným technológiám verejnej správy v jeho pôsobnosti.

(2) Orgánom riadenia na účely tohto zákona je

a) ministerstvo a ostatný ústredný orgán štátnej správy,

b) Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad,

Úrad pre reguláciu sieťových odvetví a iný štátny orgán,

c) obec a vyšší územný celok,

d) Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Najvyššieho správneho súdu Slovenskej republiky, Kancelária Súdnejrady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu,

e) právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),

f) komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,

g) osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,

h) záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.

§ 6

Základné povinnosti v správe informačných technológií verejnej správy

(1) Orgán vedenia a orgán riadenia sú v správe informačných technológií verejnej správy povinné

a) dodržiavať princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti,

b) postupovať tak, aby vynaložené náklady na informačné technológie boli primerané ich kvalite,

c) prednostne využívať už existujúce informačné technológie alebo informačné technológie určené na spoločné využitie viacerých orgánov riadenia, ak to nie je v rozpore s povinnosťami podľa písmena a) alebo písmena b) a ak to umožňujú technické možnosti a bezpečnostné požiadavky,

d) dbať na vytvorenie integrovaného prostredia informačných technológií verejnej správy na základe spoločných princípov definovaných v štandardoch a Národnej koncepcii informatizácie verejnej správy Slovenskej republiky (ďalej len „národná koncepcia“) s cieľom jednotného výkonu úloh podľa osobitných predpisov,

e) postupovať pri tvorbe, zmene alebo pri zabezpečovaní kontinuity prevádzky informačných technológií v súlade s časovým aspektom identifikovaných potrieb koncových ~~užívateľov~~ používateľov alebo s nadobudnutím účinnosti všeobecne záväzných právnych predpisov.

(2) Orgán vedenia a orgán riadenia využívajú v správe informačných technológií verejnej správy podnety a poznatky odbornej verejnosti a prihliadajú na spoločenské potreby používateľov služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb.

Vedenie v správe informačných technológií verejnej správy

§ 7

Vedenie v správe informačných technológií verejnej správy je činnosť orgánu vedenia v rozsahu jeho pôsobnosti podľa tohto zákona, ktorej účelom je riadny a efektívny výkon riadenia v správe informačných technológií verejnej správy podľa zákona a dosiahnutie cieľov informatizáciea rozvoja informačných technológií verejnej správy, ktoré vyplývajú z národnej koncepcie a ďalších koncepčných a strategických dokumentov s celoštátnou pôsobnosťou.

§ 8

(1) Orgán vedenia

a) monitoruje výkon riadenia v správe informačných technológií verejnej správy na účely sledovania

aktuálneho stavu v správe informačných technológií verejnej správy a ich vývoja sledovania spôsobov a postupov pri vykonávaní tejto správy,

b) vyhodnocuje informácie získané z monitorovania, kontroly a z iných podnetov na účely identifikácie rizík a nedostatkov v správe informačných technológií verejnej správy,

c) vydáva metodické usmernenia, usmerňuje a koordinuje orgány riadenia na účely jednotného spôsobu výkonu riadenia v správe informačných technológií verejnej správy a centrálneho riadenia informatizácie spoločnosti.

(2) Orgán riadenia je povinný poskytovať orgánu vedenia súčinnosť potrebnú na riadny výkon vedenia v správe informačných technológií verejnej správy a poskytovať mu prostredníctvom elektronickej služby verejnej správy údaje o informačných technológiách verejnej správy na účely štatistických analýz.

§ 9

(1) Orgán vedenia okrem činností podľa § 8

a) vypracúva, aktualizuje a predkladá vláde Slovenskej republiky (ďalej len „vláda“) národnú koncepciu,

b) usmerňuje tvorbu koncepcií rozvoja informačných technológií verejnej správy (ďalej len „koncepcia rozvoja“) orgánom riadenia,

c) určuje koncepciu štátnej politiky jednotného digitálneho trhu,

d) informuje vládu o stave a rozvoji informačných technológií verejnej správy,

e) koordinuje budovanie informačných technológií verejnej správy vrátane ich uvádzania do prevádzky a rozhoduje o využívaní finančných zdrojov na ich budovanie a rozvoj v rozsahu ustanovenom zákonom,

f) koordinuje tvorbu všeobecne záväzných právnych predpisov v oblasti informačných technológií verejnej správy,

g) konzultuje návrhy dokumentov, ktoré majú dosah na informačné technológie verejnej správy,s osobami dotknutými týmito dokumentmi,

h) ~~určuje centrálnu architektúru budovania a rozvoja informačných technológií verejnej správy (ďalej len „centrálna architektúra“) a referenčnú architektúru budovania a rozvoja informačných technológií verejnej správy (ďalej len „referenčná architektúra“),~~ určuje centrálnu architektúru informačných technológií verejnej správy (ďalej len „centrálna architektúra“), ktorá pozostáva zo strategickej architektúry a z referenčnej architektúry,

i) určuje kľúčové indikátory monitorovania pre jednotlivé úseky riadenia na účely monitorovania výkonu riadenia v správe informačných technológií verejnej správy,

j) vydáva štandardy a výkladové stanoviská,

k) vedie zoznam kľúčových parametrov pre riadenie prevádzky informačných technológií verejnej správy, ktorý obsahuje

1. elektronické služby verejnej správy, ktoré vyžadujú vysokú dostupnosť,
2. aktíva určené na spoločné využitie viacerými orgánmi riadenia,
3. údaje, monitorované na účely riadenia prevádzky, najmä riadenia kontinuity prevádzky,

l) zverejňuje na ústrednom portáli rozhodnutia, iné dokumenty a informácie týkajúce sa informačných technológií verejnej správy a informatizácie verejnej správy,

m) môže pre orgán riadenia zabezpečiť prístup k normám a referenčným rámcom, ktoré sú využívané v správe informačných technológií verejnej správy, ak nie sú bežne dostupné; ak ide o technické normy, ktorých poskytovanie upravuje osobitný predpis,[7]) prístup sa zabezpečuje prostredníctvom Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky spôsobom a za podmienok podľa tohto osobitného predpisu,

n) zabezpečuje zdieľanie informácií a skúseností medzi orgánmi riadenia prostredníctvom centrálneho metainformačného systému verejnej správy,

o) poskytuje v centrálnom metainformačnom systéme verejnej správy komunikačnú platformupre zadávanie podnetov k správe informačných technológií verejnej správy, službám verejnej správy, službám vo verejnom záujme a k verejným službám, vyhodnocuje tieto podnety a ich inovačný

potenciál a vedie mapu kritických miest integrovanej infraštruktúry,

p) zverejňuje dataset otvorených dát o podnetoch zadaných spôsobom podľa písmena o) vrátane spôsobu riešenia a časovej odozvy,

q) zabezpečuje organizačné predpoklady na zapojenie zástupcov odbornej verejnosti do tvorby pravidiel v správe informačných technológií verejnej správy a ich účasť na ich pripomienkovaní,

r) vydáva a spravuje zoznam základných číselníkov, základný číselník životných situácií a základný číselník úsekov verejnej správy a agend verejnej správy,

s) určuje gestora základného číselníka okrem základného číselníka životných situácií a základného číselníka úsekov verejnej správy a agend verejnej správy, riadi, koordinujea usmerňuje vydávanie, zverejňovanie a spravovanie základných číselníkov a rozhoduje spory medzi orgánmi riadenia týkajúce sa vytvárania, zverejňovania alebo správy základných číselníkov,

t) kontroluje dodržiavanie povinností orgánmi riadenia podľa tohto zákona,

u) prijíma opatrenia na nápravu zistených nedostatkov a ukladá pokuty za porušenie povinností ustanovených týmto zákonom,

v) zabezpečuje poskytovanie služieb v oblasti informačných technológií verejnej správy pre orgán riadenia po dohode s ním, ak je to potrebné na účely dosahovania cieľov v správe informačných technológií verejnej správy podľa § 7 alebo pre potreby verejného obstarávateľa na účely spolupráce podľa osobitného predpisu;[6a)] tieto služby môže zabezpečovať aj prostredníctvom právnickej osoby vo svojej zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti

~~v)~~w) koordinuje elektronizáciu agendy verejnej správy v rámci životnej situácie a usmerňuje medzirezortnú spoluprácu orgánov riadenia pri vytváraní, aktualizácii a poskytovaní elektronických služieb verejnej správy v rámci životnej situácie.

(2) Zoznam kľúčových parametrov pre riadenie prevádzky informačných technológií verejnej správy vedie orgán vedenia v štruktúrovanej podobe a zmeny v ňom vykonáva podľa aktuálnej potreby. Návrh na vydanie a návrh na zmenu zoznamu podľa prvej vety orgán vedenia zverejňuje na pripomienkovanie orgánom riadenia a iným osobám spôsobom, akým sa zverejňujú návrhy všeobecne záväzných právnych predpisov. Zoznam podľa prvej vety a jeho zmeny sa vydávajú sprístupnením v centrálnom metainformačnom systéme verejnej správy a orgán vedenia ich sprístupňuje aj na ústrednom portáli verejnej správy a na svojom webovom sídle. Zmeny v zozname podľa prvej vety sa vykonávajú tak, aby boli účinné najskôr tri mesiace odo dňa vydania, spravidla od prvého dňa nasledujúceho kalendárneho roka.

(3) Na postup pri výkone kontroly podľa odseku 1 písm. t) sa použijú základné pravidlá kontrolnej činnosti v štátnej správe.[9)] Vykonávaním niektorých činností pri kontrole dodržiavania štandardov, okrem kontroly dodržiavania podmienok týkajúcich sa bezpečnosti, môže orgán vedenia poveriť inú osobu, pričom rozsah týchto činností orgán vedenia určí v poverení v rozsahusvojej pôsobnosti.

(4) Postupom podľa odseku 3 nie je dotknutý výkon kontroly a auditu podľa osobitného predpisu.[10)]

§ 10
Národná koncepcia

(1) Národná koncepcia je súbor strategických cieľov, priorít, opatrení, programov, organizačných, technických a technologických nástrojov, ktorých účelom je na celoštátnej úrovni určiť centrálnu architektúru~~, referenčnú architektúru~~ a definovať politiku, regulačné a iné nástroje a konkrétnyplán úloh a zdrojov s cieľom budovania riadnej a efektívnej úrovne informatizácie vo verejnej správe.

(2) Národnú koncepciu schvaľuje vláda na návrh orgánu vedenia

Riadenie v správe informačných technológií verejnej správy

§ 11
Základné ustanovenia

(1) Riadenie v správe informačných technológií verejnej správy je činnosť orgánu riadenia, ktorej účelom je trvalo zabezpečiť a zlepšovať podmienky na elektronický výkon pôsobnosti orgánu riadenia podľa osobitných predpisov a rozvíjať informačné technológie, ktorých je správcom, v

súlade s týmto zákonom, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a národnou koncepciou.

(2) Za vytváranie, správu a rozvoj informačnej technológie verejnej správy zodpovedá správca.

(3) Informačnú činnosť vykonáva správca alebo prevádzkovateľ.

(4) Orgán riadenia plní povinnosti podľa § 143a až 23 ods. 1 a 2 v rozsahu a spôsobom v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov, ktorých sa týkajúa ktorých je správcom, a ak ide o povinnosti vzťahujúce sa na informačné technológie verejnej správy, projekt, zmenovú požiadavku v projekte, zmenovú požiadavku v prevádzke a servisnú požiadavku, aj v závislosti od ich veľkosti~~.~~, v rozsahu poskytovaných služieb alebo od spôsobu financovania. Na účelyklasifikácie informácií a kategorizácie sietí a informačných systémov sa použijú ustanovenia osobitného predpisu.[11])

(5) Pri vypracúvaní vnútorných predpisov na účely podľa § 143a až 17 a pri riadení bezpečnosti informačných technológií verejnej správy vychádza orgán riadenia

a) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajúz uznaných technických noriem, a
b) z metodických usmernení orgánu vedenia.

(6) Projekt informačných technológií verejnej správy a zmenová požiadavka v projekte sa na účely tohto zákona považujú za veľké, ak ich celková cena alebo lehota dodania presahuje cenu alebo lehotu dodania ustanovenú všeobecne záväzným právnym predpisom, ktorý vydáministerstvo investícií.

(7) Právny vzťah, ktorého predmetom je činnosť potrebná na zabezpečenie prevádzky informačnej technológie verejnej správy, riešenia servisných požiadaviek, alebo činnosť spočívajúca v riešení zmenových požiadaviek v prevádzke vrátane úpravy, rozvoja, opravy informačnej technológie verejnej správy alebo odstránenia prevádzkového incidentu na informačnej technológii verejnej správy (ďalej len „zmluva v prevádzke“) sa na účely tohto zákona považuje za veľký, ak celková cena presahuje cenu ustanovenú všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií. Celková cena na účely podľa prvej vety sa určuje aj ako súčet opakovaných finančných plnení alebo najvyššia dojednaná hodnota všetkých plnení zo zmluvy v prevádzke, alebo ako jednorazové plnenie zo zmluvy v prevádzke. Ak je uzatvorených viac zmlúv v prevádzke, na účely celkovej ceny sa posudzujú spoločne.

(8) Ak sa v tomto zákone ustanovuje povinnosť sprístupniť informácie alebo údajea neustanovuje sa konkrétny spôsob alebo miesto sprístupnenia, rozumie sa tým sprístupnenie najmenej na webovom sídle.

(9) Ak sa v tomto zákone ustanovuje povinnosť vypracovať vnútorný predpis, orgán riadenia jepovinný vydať najmenej jeden vnútorný predpis pokrývajúci všetky takéto prípady.

§ 12

(1) Orgán riadenia je povinný

a) zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných technológií verejnej správy, ktorých je správcom, vrátane organizačného, odborného a technického zabezpečeniaa zabezpečenia proti zneužitiu, a to v súlade s týmto zákonom, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a národnou koncepciou,
b) prostredníctvom centrálneho metainformačného systému verejnej správy bezodkladne sprístupňovať a aktualizovať informácie o informačných technológiách verejnej správy, ktorých je správcom, a o poskytovaných elektronických službách verejnej správy, ako aj o elektronických službách verejnej správy, ktoré plánuje poskytovať; informácie sa v rozsahu sprístupnenom orgánom riadenia použijú aj na účely využívania elektronickej služby a elektronickú komunikáciu s orgánom riadenia prostredníctvom ústredného portálu,[11a])~~,~~
c) administratívne spravovať príslušné číselníky a zabezpečiť ich zverejnenie podľa osobitného predpisu,12)
d) používať v informačnej činnosti základné číselníky,
e) sprístupňovať verejnosti údaje z informačných systémov verejnej správy, za podmienok ustanovených zákonom,[13])

f) zabezpečiť, aby informácia, dokument alebo údaj, ktoré je osoba povinná predkladať v konaní pred orgánom verejnej moci a ktoré sa nachádzajú v informačnom systéme verejnej správy, ktorého je správcom, boli dostupné aj iným orgánom verejnej moci a spôsobom podľa osobitného predpisu[14]) im ich bezodplatne sprístupňovať alebo na požiadanie poskytnúť,
g) poskytovať elektronické odpisy a výstupy z informačných systémov verejnej správy, ktorých je správcom, na účely podľa osobitných predpisov,[15])
h) zabezpečiť dostupnosť informačných technológií verejnej správy, ktorých je správcom, na účely elektronickej komunikácie podľa osobitných predpisov,[16])
i) zabezpečiť tvorbu informácií o svojej činnosti pre verejnosť a tieto zverejňovať a aktualizovať prostredníctvom ústredného portálu[17]) a svojho webového sídla,
j) bezodkladne nahlasovať orgánu vedenia zmeny úsekov verejnej správy a agend verejnej správy na účely vedenia základného číselníka úsekov verejnej správy a agend verejnej správy a spôsob, akým bola táto zmena uskutočnená,
~~j)~~k) sprístupňovať orgánom verejnej moci a právnickým osobám prostredníctvom modulu procesnej integrácie a integrácie údajov povinne vytvárané aplikačné rozhrania informačných technológií verejnej správy a informácie potrebné na ich použitie a títo sú oprávnení na účel použitia aplikačných rozhraní používať modul procesnej integrácie a integrácie údajov; týmto spôsobom možno sprístupniť aj iné aplikačné rozhrania informačných technológií verejnej správy.~~.~~

(2) Ministerstvo investícií je ako orgán riadenia správcom
a) integrovanej infraštruktúry,
b) centrálneho metainformačného systému verejnej správy,
c) nadrezortného informačného systému verejnej správy na úseku verejnej správy ministerstva investícií, ak správcu nadrezortného informačného systému verejnej správy neustanovuje osobitný predpis inak.

§ 13
Koncepcia rozvoja informačných technológií verejnej správy

(1) Koncepcia rozvoja je dokument vypracovaný orgánom riadenia pre informačné technológie verejnej správy, ktorých je správcom, definujúci ciele, organizačné, technické a technologické nástroje, architektúru informačných technológií verejnej správy ~~strategickú architektúru a referenčnú architektúru informačných technológií verejnej správy v správe orgánu riadenia~~ a plánovanie jednotlivých aktivít, najmä s cieľom riadneho a včasného naplnenia požiadaviek národnej koncepcie a strategických priorít informatizácie verejnej správy.

(2) Ak odseky 4 a 5 neustanovujú inak, koncepciu rozvoja predkladá orgán riadenia na schválenie orgánu vedenia najneskôr do 12 mesiacov od vzniku orgánu riadenia a následne najneskôr do šiestich mesiacov
a) pred uplynutím platnosti predošlej koncepcie rozvoja,
b) od schválenia národnej koncepcie,
c) od schválenia zmeny alebo doplnenia národnej koncepcie, ak ide o orgán riadenia, na ktorého sa táto zmena alebo doplnenie vzťahuje.

(3) Orgán vedenia schváli koncepciu rozvoja najneskôr do šiestich mesiacov odo dňa jej doručenia, ak je v súlade s týmto zákonom, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a národnou koncepciou; inak vyzve orgán riadenia na odstránenie nedostatkov v lehote, ktorú určí. Ak orgán riadenia v určenej lehote nedostatky neodstráni, orgán vedenia koncepciu rozvoja neschváli.

(4) Ak ide o orgán riadenia podľa § 5 ods. 2 písm. e), koncepciu rozvoja za neho vypracúva, aktualizuje a predkladá na schválenie ten orgán riadenia, ktorý voči nemu vykonáva zriaďovateľskú pôsobnosť alebo zakladateľskú pôsobnosť, a to ako samostatný dokument alebov rámci vlastnej koncepcie rozvoja.

(5) Obec a právnická osoba v jej zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti nie sú povinné predkladať koncepciu rozvoja na schválenie orgánu vedenia. Ak tak obec rozhodne,

koncepcia rozvoja obce alebo právnickej osoby v jej zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti podlieha schváleniu orgánom, ktorý určí obec.

(6) Orgán riadenia každoročne v termíne do 31. mája posúdi súlad koncepcie rozvoja s národnou koncepciou a na jej základe vydanými dokumentmi. ~~Ak orgán riadenia zistí nesúlad, je povinný aktualizovať koncepciu rozvoja.~~ Ak orgán riadenia zistí nesúlad podľa prvej vety alebo ak dôjde k zmenám podmienok, v ktorých informačné technológie verejnej správy existujú, je povinný aktualizovať koncepciu rozvoja.

~~(5)~~(7) Orgán riadenia predkladá ~~zverejňuje~~ koncepciu rozvoja a jej aktualizácie prostredníctvom centrálneho metainformačného systému.

§ 13a
Elektronizácia agendy verejnej správy a zlepšovanie kvality používateľskej skúsenosti

(1) Orgán riadenia priebežne vyhodnocuje agendu verejnej správy vo svojej pôsobnosti na účely zabezpečenia riadneho výkonu poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb, zabezpečenia riadnej prevádzky informačných technológií verejnej správy a dosahovania cieľov informatizácie. Orgán riadenia pri elektronizácii agendy vo svojej pôsobnosti, najmä ak ide o vytváranie a zásadnú zmenu elektronických služieb určených pre koncového používateľa, v rámci riadenia v správe informačných technológií verejnej správy

a) postupuje v súlade so základnými zásadami elektronizácie agendy verejnej správy, tvorby a rozvoja elektronických služieb a používateľských rozhraní a v súlade so známymi potrebami koncového používateľa,
b) umožňuje využívať prístup z pohľadu životnej situácie,
c) určuje prioritné ~~priorizuje~~ elektronické služby,
d) zabezpečuje jednotný vzhľad a prezentáciu grafického používateľského rozhrania elektronickej služby, webovej stránky zobrazujúcej elektronickú službu a hlavného webového sídla,
e) zabezpečuje vytvorenie verejne prístupného aplikačného programového rozhrania pre elektronické služby, ktoré sú dostupné prostredníctvom grafického používateľského rozhrania,
f) zlepšuje kvalitu používateľskej skúsenosti koncového používateľa.

(2) Na umožnenie využívania prístupu z pohľadu životnej situácie ~~je~~ orgán riadenia ~~povinný spolupracovať~~ poskytuje súčinnosť ~~s iným~~ iným orgánom riadenia pri vytváraní, zmene a poskytovaní elektronických služieb v rámci životnej situácie tak, aby predchádzajúce a nadväzujúce elektronické služby, ktoré koncový používateľ obvykle v rámci životnej situácie využíva, boli vytvorené a poskytované spôsobom, ktorý pre koncového používateľa vytvára plynulú používateľskú cestu. Na účely podľa prvej vety je orgán riadenia oprávnený požadovať potrebnú súčinnosť od iného orgánu riadenia a tento je povinný mu ju poskytnúť.

(3) Elektronickú službu, ktorá z hľadiska významu pre prostredie informačných technológií verejnej správy dosahuje kritériá ustanovené v štandardoch, určí orgán riadenia za prioritnú. Elektronickú službu, ktorá dosahuje kritériá podľa predchádzajúcej vety môže za prioritnú určiť aj orgán vedenia. ~~Orgán vedenia môže určiť, že elektronická služba je prioritnou elektronickou službou, a to na základe jej významu pre prostredie informačných technológií verejnej správy, z hľadiska početnosti jej používania alebo z iného objektívneho dôvodu.~~

(4) Ak ide o prioritnú elektronickú službu, orgán riadenia je povinný predložiť zámer na vytvorenie alebo zmenu tejto služby, ktorý obsahuje podrobnosti o postupe orgánu riadenia pri elektronizácii agendy a vytváraní alebo zmene elektronickej služby, na posúdenie a schválenie orgánu vedenia. Orgán vedenia môže schváliť zámer na vytvorenie alebo zmenu služby s podmienkou, že návrh elektronickej služby alebo jej zmeny bude vytvorený ako prototyp a poskytovanie elektronickej služby bude možné až po schválení prototypu orgánom vedenia. Orgán vedenia tiež môže určiť, že prototyp elektronickej služby bude v rámci schvaľovania prezentovaný aj odbornej verejnosti, budúcim koncovým používateľom a iným osobám, ktorých spätná väzba môže byť pre orgán vedenia prínosná. Ak sa orgán vedenia do 20

pracovných dní odo dňa predloženia úplného zámeru k zámeru nevyjadrí platí, že zámer schválil v predloženom znení.

(5) Orgán vedenia sprístupňuje zoznam prioritných elektronických služieb v centrálnom metainformačnom systéme. Orgán riadenia v rámci povinnosti podľa § 15 ods. 8 plní tieto povinnosti osobitne k aktívam, ktorými sú prioritné elektronické služby, a to najneskôr do šiestich~~6~~ mesiacov odo dňa určenia ~~prioritnej~~ elektronickej služby za prioritnú.

(6) Na zabezpečenie jednotného vzhľadu a prezentácie je orgán riadenia povinný používať pri tvorbe a zmene grafického používateľského rozhrania elektronickej služby, webovej stránky zobrazujúcej elektronickú službu a hlavného webového sídla dizajnový manuál podľa § 24c. Povinnosť podľa predchádzajúcej vety sa

a) vzťahuje len na grafické používateľské rozhrania elektronických služieb určených verejnosti a na webové stránky ich zobrazujúce,

b) nevzťahuje na orgán riadenia podľa § 5 ods. 2 písm. c) a e) až h), Tlačovú agentúru Slovenskej republiky, Rozhlas a televíziu Slovenska a zdravotnú poisťovňu.

(7) Orgán riadenia na účely zlepšenia kvality používateľskej skúsenosti zabezpečuje priebežný zber spätnej väzby k poskytovaným prioritným elektronickým službám od koncových používateľov a jej vyhodnocovanie najmenej raz ročne. Ak o to orgán vedenia požiada, orgán riadenia mu v určenej lehote, najskôr 31. januára, predloží vyhodnotenie ~~Vyhodnotenie~~ spätnej väzby podľa prvej vety ~~zasiela orgán riadenia orgánu vedenia do 31. januára~~ za predchádzajúci kalendárny rok. Poznatky získané zo spätnej väzby orgán riadenia zohľadňuje v koncepcii rozvoja a v pláne postupu pre naplnenie požiadaviek na zlepšovanie kvality používateľskej skúsenosti (ďalej len „plán zlepšovania kvality“).

(8) Plán zlepšovania kvality slúži na zabezpečenie zlepšovania kvality používateľskej skúsenosti koncových používateľov pri používaní elektronických služieb a orgán riadenia ho uplatňuje v riadení ~~v správe~~ informačných technológií verejnej správy. Orgán riadenia vypracúva plán zlepšovania kvality na každý kalendárny rok a sprístupňuje ho orgánu vedenia prostredníctvom centrálneho metainformačného systému na príslušný kalendárny rok vždy do 31. mája. Orgán vedenia môže do 30 dní odo dňa sprístupnenia vyzvať orgán riadenia na odstránenie nedostatkov plánu zlepšovania kvality a určiť primeranú lehotu na ich odstránenie a orgán riadenia je povinný nedostatky v tejto lehote odstrániť.

(9) Pri plnení povinnosti podľa § 14 ods. 5 určí orgán riadenia osobu, ktorá v oblasti zlepšovania kvality používateľskej skúsenosti informačných technológií verejnej správy zodpovedá v rámci orgánu riadenia za

a) identifikovanie používateľských problémov informačných technológií verejnej správy a navrhuje riešenie týchto problémov,

b) vypracovanie plánu zlepšovania kvality a dohliada na jeho dodržiavanie,

c) komunikáciu s orgánom vedenia.

(10) Právnická osoba v zakladateľskej pôsobnosti orgánu riadenia podľa § 5 ods. 1 písm. a) až d), ktorá sa zúčastňuje na hospodárskej súťaži, aj keď nie je podnikateľom, zdravotná poisťovňa, Tlačová agentúra Slovenskej republiky a Rozhlas a televízia Slovenska, predkladajú dokumenty a informácie podľa odsekov 4, 7 a 8 prostredníctvom neverejnej časti centrálneho metainformačného systému a tieto sú prístupné len orgánu vedenia.

(11) Na zdravotnú poisťovňu sa nevzťahuje povinnosť vypracúvať plán zlepšovania kvality a povinnosti podľa odseku 9.

§ 14

Plánovanie a organizácia informačných technológií verejnej správy

(1) Správca je na úseku plánovania a organizácie informačných technológií verejnej správy

povinný

a) nastaviť systém riadenia,
b) určiť stratégiu rozvoja a riadenia,
c) zabezpečiť riadenie správy architektúry,
d) nastaviť organizačnú štruktúru, procesy a nástroje potrebné na riadenie,
e) zabezpečiť riadenie kľúčových zdrojov, ktorými sú ľudské zdroje, finančné prostriedky alebozdroje poskytované inými osobami,
f) riadiť nastavenie zmluvných vzťahov pre poskytovanie služieb,
g) zabezpečiť riadenie kvality,
h) zabezpečiť riadenie rizík,
i) zabezpečiť riadenie bezpečnosti.

(2) V rámci nastavenia systému riadenia je správca povinný vydať vnútorný predpis pre systém riadenia informačných technológií verejnej správy.

(3) ~~V rámci určovania stratégie rozvoja a riadenia správca zabezpečí aktualizáciu koncepcie rozvoja, ak dôjde k zmenám podmienok, v ktorých informačné technológie verejnej správy existujú, a to najneskôr do šiestich mesiacov odo dňa, keď k zmene dôjde.~~ Správca je povinný spolupracovať s ostatnými orgánmi riadenia pri tvorbe koncepcie rozvoja a v súčinnosti s nimi zabezpečovať uskutočňovanie koncepcie rozvoja vrátane organizačného, odborného a technického zabezpečenia.

(4) V rámci zabezpečenia riadenia správy architektúry informačných technológií verejnej správy správca udržuje architektúru informačných technológií verejnej správy v súlade s ~~referenčnou~~ centrálnou architektúrou (§ 10 ods. 1) a s koncepciou rozvoja a v súlade s ňou realizuje povinnosti podľa § 15.

(5) V rámci nastavenia organizačnej štruktúry, procesov a nástrojov potrebných na riadenie je správca povinný zabezpečiť také organizačné podmienky a procesné podmienky, aby zabezpečil riadny výkon povinností pri riadení informačných technológií verejnej správy a realizoval určené strategické ciele. Organizačnými podmienkami sa rozumie najmä určenie zodpovedných organizačných útvarov a riadiacich pozícií na strategickej, programovej, projektovej a operačnej úrovni riadenia. Procesnými podmienkami sa rozumie najmä určenie postupov riadenia informačných technológií verejnej správy a kontrola dodržiavania všeobecne záväzných právnych predpisov v tejto oblasti, ako aj riadenie kvality, rizík a bezpečnosti informačných technológií verejnej správy. Správca zabezpečuje organizačné podmienky a procesné podmienky, najmä potrebné riadiace pozície, kvalifikačné predpoklady a požiadavky na certifikáciu, v rozsahu a spôsobom v závislosti od veľkosti a od komplexnosti informačných technológií verejnej správya poskytovaných služieb.

(6) V rámci nastavenia zmluvných vzťahov pre poskytovanie služieb správca

a) identifikuje služby, ktoré vykonáva a poskytuje na účely poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb, a udržiava ich zoznam,
b) pre služby, ktoré vykonáva a poskytuje na účely poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb, definuje a udržiava potrebné úrovne ich poskytovania,
c) monitoruje a hodnotí dodržiavanie úrovne poskytovania služieb podľa písmena b) a informáciez monitoringu a hodnotenia v rozsahu ustanovenom štandardmi sprístupňuje verejnosti najmenej raz za šesť mesiacov prostredníctvom na to určenej funkcionality centrálneho metainformačného systému verejnej správy,
d) najmenej jedenkrát do roka vyhodnocuje plnenie služieb podľa písmena b), ktoré poskytuje iným osobám na základe zmlúv o poskytovaní služieb, a toto vyhodnotenie zverejňuje v centrálnom metainformačnom systéme verejnej správy,
e) identifikuje služby, ktoré na účely poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb odoberá od iných osôb než od orgánu riadenia.

(7) V rámci zabezpečenia riadenia kvality je správca povinný vydať vnútorný predpis pre riadenie kvality.

(8) V rámci zabezpečenia riadenia rizík je správca povinný vydať vnútorný predpis pre riadenie rizík.

§ 15

Obstarávanie a implementácia informačných technológií verejnej správy

(1) Správca je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný

a) zabezpečiť riadenie projektov,
b) identifikovať požiadavky na informačné technológie verejnej správy a podmienky ich zabezpečenia,
c) zabezpečiť riadenie dostupnosti a kapacity zdrojov,
d) zabezpečiť riadenie zmien na organizačnej a procesnej úrovni,
e) zabezpečiť riadenie aktív,
f) zabezpečiť riadenie konfigurácií.

(2) Vo fáze prípravy a obstarania projektu je správca povinný

a) identifikovať požiadavky podľa odseku 5,
b) nastaviť požiadavky prevádzky pre všetky informačné technológie verejnej správy, ktoré sú súčasťou projektu,
c) pre veľké projekty odôvodniť vybraté riešenie s ohľadom na možné alternatívy a odôvodniť, najmä z pohľadu hodnoty za peniaze, zvolený postup obstarania a implementácie a tieto informácie sprístupniť verejnosti,
d) akceptovať také zmluvné podmienky, podľa ktorých
   1. zdrojový kód vytvorený počas projektu bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu,[18]) a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu informačného systému verejnej správy,
   2. je jediným a výhradným disponentom so všetkými informáciami zhromaždenými alebo získanými počas projektu a prevádzky projektom vytvoreného riešenia vrátane jeho zmena servisu a
   3. pri zmene dodávateľa pôvodný dodávateľ poskytne správcovi úplnú súčinnosť pri prechode na nového dodávateľa, najmä v oblasti architektúry a integrácie informačných systémov.

(3) Vo fáze implementácie projektu je správca povinný

a) zabezpečovať riadenie zmien podľa odseku 7,
b) udržiavať technické informácie o realizovanom riešení v aktuálnom a správnom stave vrátane informácií o väzbách medzi jednotlivými jeho prvkami.

(4) V rámci zabezpečenia riadenia projektov v oblasti informačných technológií verejnej správy je správca povinný

a) vydať vnútorný predpis pre plánovanie projektov, procesné riadenie a implementáciu projektov,
b) zabezpečiť, aby realizované projekty boli uskutočňované v súlade s koncepciou rozvoja,
c) zabezpečiť, aby projekt mal určené merateľné ukazovatele súladu s koncepciou rozvoja, identifikované požiadavky, identifikované riziká, určené prínosy a určené merateľné kritériá kvality,
d) zabezpečiť, aby veľký projekt alebo projekt, ktorý nepozostáva len z dodania jedného funkčného celku, bol z hľadiska dodania rozdelený na čiastkové plnenia, pričom
   1. každé čiastkové plnenie musí mať vlastný prínos bez ohľadu na celkové plnenie,
   2. po každom čiastkovom plnení musí byť možné projekt ukončiť, ak stratil svoje pôvodné opodstatnenie,
   3. cena jedného čiastkového plnenia nesmie presiahnuť sumu ustanovenú všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií, a
   4. lehota dodania každého čiastkového plnenia nesmie presiahnuť lehotu ustanovenú všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií,
e) predložiť veľký projekt na posúdenie a schválenie orgánu vedenia a začať s jeho realizáciou až po jeho schválení
e)f) predložiť zámer na vytvorenie a prevádzkovanie mobilnej aplikácie na posúdenie a schválenie orgánu vedenia a začať s realizáciou len, ak orgán vedenia do 20 pracovných dní odo dňa

doručenia úplného zámeru nevysloví s realizáciou nesúhlas; na predkladanie zámeru sa § 13a ods. 10 použije rovnako ~~až po jeho schválení~~.

(5) V rámci identifikácie požiadaviek na informačné technológie verejnej správy a podmienok ich zabezpečenia správca

a) identifikuje požiadavky tak, aby v čo najväčšej miere zohľadňovali známe potreby koncových ~~užívateľov~~ používateľov a tieto potreby zisťuje používateľským prieskumom,
b) identifikuje dostupné kapacity informačných technológií a ľudských zdrojov,
c) vychádza z požiadaviek na architektúru informačných technológií verejnej správy, ktoré sú v súlade s ~~referenčnou~~ centrálnou architektúrou (§ 10 ods. 1) a s koncepciou rozvoja,
d) preferuje energeticky úsporné riešenia,
e) zhromažďuje a sprístupňuje podnety a poznatky odbornej verejnosti a jemu známe spoločenské potreby používateľov služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb, ak z nich pri identifikácii požiadaviek vychádzal.

(6) V rámci zabezpečenia riadenia dostupnosti a kapacity zdrojov správca

a) zabezpečuje taký rozsah zdrojov, aby bola zabezpečená potrebná úroveň poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb a riadna príprava a implementácia projektov,
b) pravidelne plánuje a kontroluje dostupnosť a kapacitu zdrojov.

(7) V rámci zabezpečenia riadenia zmien na organizačnej a procesnej úrovni správca riadi zmeny v projektoch tak, aby boli podmienené prínosmi a bola dosiahnutá najvyššia hodnota za peniaze vynaložené na realizáciu zmeny. Ak ide o veľkú zmenovú požiadavku v projekte, správca je povinný predložiťju na posúdenie a schválenie orgánu vedenia a začať s jej realizáciou až po jej schválení.

(8) V rámci zabezpečenia riadenia aktív v informačných technológiách verejnej správy správca

a) identifikuje a udržiava zoznam svojich aktív,
b) vyhodnocuje možnosti využitia existujúcich informačných technológií alebo informačných technológií určených na spoločné využitie viacerými orgánmi riadenia a možnosti zdieľania svojich aktív s iným orgánom riadenia,
c) identifikuje časti aktív, ktorých nedostupnosť alebo znížená kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb,
d) plánuje životný cyklus aktív v súlade so strategickými plánmi rozvoja informačných technológií verejnej správy a s aktuálnymi potrebami ich prevádzky.

(9) V rámci zabezpečenia riadenia konfigurácií je správca povinný

a) vydať vnútorný predpis pre riadenie konfigurácií,
b) udržiavať zoznam konfigurácií svojich aktív v informačných technológiách verejnej správy.

(10) Správca je povinný sprístupňovať na svojom webovom sídle projektovú dokumentáciu informačnej technológie verejnej správy, pričom na rozsah zverejňovaných informácií sa použijú ustanovenia osobitného predpisu,[19]) a nezverejní tie časti, ktorých zverejnenie by bolo rizikovéz pohľadu bezpečnosti informačnej technológie verejnej správy.

(11) Správca sprístupní elektronickú službu verejnej správy alebo inú informačnú technológiu verejnej správy na používanie verejnosti až po sprístupnení informácie o elektronickej službe verejnej správy alebo informačnej technológii verejnej správy v centrálnom metainformačnom systéme verejnej správy podľa § 12 ods. 1 písm. b).

(12) Orgán vedenia posudzuje zámer na vytvorenie a prevádzkovanie mobilnej aplikácie z pohľadu opodstatnenosti existencie takejto aplikácie v prostredí informačných technológií verejnej správy. Povinnosť podľa § 15 ods. 4 písm. f) sa nevzťahuje na

a) mobilnú aplikáciu, ktorá je určená výlučne pre potreby zamestnancov orgánu riadenia,

~~a)~~b) orgán riadenia podľa § 5 ods. 2 písm. c) a f), Tlačovú agentúru Slovenskej republiky, Rozhlas a televíziu Slovenska a zdravotnú poisťovňu.

§ 16

Prevádzka, servis a podpora informačných technológií verejnej správy

(1) Správca je na úseku prevádzky, servisu a podpory informačných technológií verejnej správy povinný

a) nastaviť riadenie prevádzky,
b) zabezpečiť riadenie prevádzky,
c) zabezpečiť riadenie kontinuity prevádzky,
d) zabezpečiť riadenie služieb bezpečnosti prevádzky.

(2) V rámci nastavenia riadenia prevádzky informačných technológií verejnej správy je správca povinný

a) vydať vnútorný predpis pre riadenie prevádzky,
b) klasifikovať aktíva podľa § 15 ods. 8 písm. c), a to najmä s použitím kritérií potrieb konkrétnych služieb verejnej správy a dodržania povinností podľa § 6 ods. 1 písm. a) a b),
c) zabezpečiť vysokú dostupnosť elektronickej služby verejnej správy uvedenej v zozname podľa § 9 ods. 1 písm. k) prvom bode, alebo klasifikovanej na túto úroveň podľa písmena b),
d) zaviesť systém riadenia prevádzky informačných technológií verejnej správy,
e) pravidelne monitorovať a vyhodnocovať údaje podľa § 9 ods. 1 písm. k) tretieho bodu a oznamovať ich hodnoty orgánu vedenia,
f) preferovať energeticky úsporné postupy pri riadení prevádzky.

(3) V rámci zabezpečenia riadenia prevádzky informačných technológií verejnej správy je správca povinný

a) umožniť pre každú informačnú technológiu verejnej správy vo svojej správe nahlasovanie servisných požiadaviek, prevádzkových problémov a prevádzkových incidentov,
b) zabezpečiť riešenie a uzavretie servisných požiadaviek, prevádzkových problémov a prevádzkových incidentov spôsobom a v rozsahu v závislosti od ich úrovne ustanovenej všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií,
c) poskytnúť orgánu vedenia na požiadanie, najmenej raz za šesť mesiacov správu o počte a charaktere nahlásených, riešených a uzavretých servisných požiadaviek, prevádzkových problémov a prevádzkových incidentov, okrem informácií, ktorých zverejnenie by bolo rizikové z pohľadu bezpečnosti informačnej technológie verejnej správy, a to v rozsahu a spôsobom podľa dohody s orgánom vedenia,
d) zabezpečiť dostupnosť informácií potrebných na náhradné riešenie dostupnosti služieb verejnej správy a informačných systémov verejnej správy pri výskyte prevádzkového incidentu,
e) zaviesť systém riadenia správy prevádzkových problémov a systém riadenia servisných požiadaviek a zmenových požiadaviek v prevádzke, vrátane oznamovania pripravovaných zmenových požiadaviek v prevádzke orgánu vedenia,
f) predložiť veľkú zmluvu v prevádzke na posúdenie a schválenie orgánu vedenia a začať s jej realizáciou až po jej schválení,
g) zaviesť postup realizácie plnení z veľkej zmluvy v prevádzke a realizácie zmenových požiadaviek v prevádzke,
h) postupovať pri dojednaní zmluvných podmienok zmluvy v prevádzke podľa § 15 ods. 2 písm. d).

(4) V rámci zabezpečenia riadenia kontinuity prevádzky informačných technológií verejnej správy správca určuje

a) úroveň kontinuity pre služby verejnej správy, služby vo verejnom záujme, verejné služby, ďalšie služby informačných technológií a pre prevádzku aktív v informačných technológiách verejnej správy podľa kritérií ustanovených všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií,
b) systém riadenia kontinuity elektronických služieb verejnej správy a zavedie ho do prevádzky,
c) postup obnovy prevádzky informačných technológií verejnej správy.

§ 17

Monitoring a hodnotenie informačných technológií verejnej správy

(1) Správca na úseku monitoringu a hodnotenia informačných technológií verejnej správy je povinný

a) pravidelne monitorovať informačné technológie verejnej správy,
b) pravidelne monitorovať systém kontroly,
c) zabezpečiť súlad prevádzky s podmienkami ustanovenými všeobecne záväznými právnymi predpismi.

(2) V rámci zabezpečenia pravidelného monitorovania informačných technológií verejnej správy správca
a) prijme vnútorný predpis upravujúci spôsob monitorovania,
b) nastaví kľúčové indikátory hodnotenia a ich prahové hodnoty,
c) zabezpečuje zber monitorovaných údajov a ich oznamovanie orgánu vedenia v oblastiacha v rozsahu ustanovenom všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií.

(3) V rámci zabezpečenia pravidelného monitorovania systému kontroly informačných technológií verejnej správy je správca povinný pravidelne monitorovať a vyhodnocovať účinnosť nastavených postupov kontroly a navrhovať ich úpravu na účely ich riadneho fungovania.

(4) V rámci zabezpečenia súladu s podmienkami ustanovenými všeobecne záväznými právnymi predpismi je správca povinný udržiavať vnútorné postupy, ktorými sa zabezpečí súlad riadeniav správe informačných technológií verejnej správy a prevádzky informačných technológií verejnej správy so všeobecne záväznými právnymi predpismi.

(5) Informácie z činností podľa odseku 1 správca sprístupní verejnosti, pričom nezverejní tie časti, ktorých zverejnenie by bolo rizikové z pohľadu bezpečnosti informačnej technológie verejnej správy.

Bezpečnosť informačných technológií verejnej správy

§ 18
Základné ustanovenia

(1) Povinnosť správcu, ktorý je prevádzkovateľom základnej služby,[20]) prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje osobitný predpis.[21])

(2) Správca, ktorý je prevádzkovateľom základnej služby,[20]) prijíma a realizuje bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe podľa tohto zákona a osobitného predpisu,[21]) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje osobitý predpis.[22])

§ 19
Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie

(1) V rámci zabezpečenia riadenia bezpečnosti podľa § 14 ods. 1 písm. i) je správca povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý
a) určí ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti vo forme bezpečnostnej dokumentácie schválených procesov riadenia bezpečnosti informačných technológií verejnej správy,
b) zriadi riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené,
c) zabezpečí a zdokumentuje identifikovanie aktív v informačných technológiách verejnej správy a riadenie rizík, najmä vo forme bezpečnostnej dokumentácie vrátane bezpečnostného projektu podľa § 23 ods. 1 a 2,
d) určí a zavedie bezpečnostné opatrenia na procesnej, organizačnej a na technickej úrovni,
e) určí prostriedky a zdroje na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení,

f) určí prostriedky kontroly uplatňovania bezpečnostných opatrení,
g) určí postupy riešenia bezpečnostných incidentov.

(2) Správca prostredníctvom riadiacej zložky systému riadenia bezpečnosti zabezpečuje prerokovanie a schválenie

a) bezpečnostnej stratégie kybernetickej bezpečnosti a strategických opatrení týkajúcich sa bezpečnosti informačných technológií verejnej správy,
b) informácií o zaznamenaných závažných kybernetických bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného výskytu,
c) návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov kybernetickej bezpečnosti informačných technológií verejnej správy.

(3) Správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje

a) vypracovanie a aktualizáciu bezpečnostnej dokumentácie upravujúcej systém riadenia bezpečnosti podľa odseku 1,
b) preskúmanie stavu kybernetickej bezpečnosti informačných technológií verejnej správynajmenej jedenkrát do roka a informovanie riadiacej zložky o výsledkoch preskúmania,
c) realizáciu bezpečnostných opatrení,
d) plánovanie, koordináciu a vyhodnocovanie činností súvisiacich s riadením bezpečnostných rizík v oblasti bezpečnosti informačných technológií verejnej správy,
e) vnútornú koordináciu riešenia bezpečnostných incidentov,
f) organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií verejnej správy.

(4) Správca prostredníctvom kontrolnej zložky systému riadenia bezpečnosti zabezpečuje

a) nezávislú kontrolu dodržiavania povinností v oblasti bezpečnosti informačných technológiíverejnej správy,
b) hodnotenie súladu stavu bezpečnosti s požiadavkami všeobecne záväzných právnych predpisov.

(5) Správca pri plánovaní vytvorenia alebo nadobudnutia informačného systému verejnej správy

a) dodržiava bezpečnostnú stratégiu kybernetickej bezpečnosti,
b) určí osobu zodpovednú za bezpečnosť informačného systému verejnej správy,
c) identifikuje riziká prostredia, v ktorom bude informačný systém verejnej správy prevádzkovaný.

§ 20

Bezpečnosť informačných technológií verejnej správy v oblasti obstarávaniaa implementácie

(1) Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy

a) určí bezpečnostné požiadavky na informačný systém verejnej správy vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania informačného systému verejnej správy,
b) zabezpečí pre tento systém vypracovanie bezpečnostnej dokumentácie vrátane bezpečnostného projektu podľa § 23 ods. 1 a– 2.,

(2) Dodávateľ informačného systému verejnej správy pre vývoj tohto systému

a) zabezpečí
   1. bezpečné vývojové prostredie,
   2. dokumentáciu vývoja a testovania vrátane používateľskej dokumentácie a administrátorskej dokumentácie,
b) je povinný
   1. dodržiavať mlčanlivosť o dodávanom informačnom systéme verejnej správy aj po ukončení dodania a zaviazať rovnakou povinnosťou všetky osoby, ktoré sa na dodaní podieľali,
   2. doplniť bezpečnostné požiadavky na informačný systém verejnej správy podľa odseku 1 písm. a) a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude informačný systém verejnej správy prevádzkovaný,

3. preukázateľne odstrániť alebo znemožniť používanie funkcie informačného systému verejnej správy, ktoré by jemu alebo tretej strane umožňovali získať neoprávnený prístup do tohto systému a k údajom, ktoré obsahuje.

§ 21

Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory

(1) V rámci zabezpečenia riadenia služieb bezpečnosti prevádzky podľa § 16 ods. 1 písm. d) správca zabezpečuje

a) zavedenie informačného systému verejnej správy do prevádzky,
b) prevádzku informačného systému verejnej správy,
c) vyradenie informačného systému verejnej správy z prevádzky.

(2) V rámci zabezpečenia zavedenia informačného systému verejnej správy do prevádzky správca

a) overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek pred zavedením do prevádzky a nezavedie do prevádzky informačný systém verejnej správy, ktorý tieto požiadavky nespĺňa,
b) vykoná bezpečnostné testovanie informačného systému verejnej správy, ktorý má rozhranies verejnou sieťou internet a ktorý spracúva osobitné kategórie osobných údajov podľa osobitného predpisu[22a]) alebo informácie klasifikované z hľadiska dôvernosti ako chránené alebo prísne chránené podľa osobitného predpisu.[22b])

(3) V rámci zabezpečenia prevádzky informačného systému verejnej správy správca

a) zabezpečí pre informačný systém verejnej správy
   1. určenie a pravidelné aktualizovanie bezpečnostnej dokumentácie,
   2. dodržiavanie bezpečnostných opatrení,
b) v závislosti od zaradenia informačného systému verejnej správy z pohľadu klasifikácieinformácií a kategorizácie sietí a informačných systémov
   1. aktualizuje bezpečnostný projekt pre tento systém vypracovaný podľa § 23 ods. 1 a 2,
   2. zavedie jednotný systém riadenia informačnej bezpečnosti pre všetky informačné systémy, ktoré sú v jeho správe,
   3. zabezpečí riadenie konfigurácie informačného systému verejnej správy a jeho častí,
   4. určí bezpečnostne závažné operácie, ktorými sa rozumejú najmä správa prístupov a prístupových údajov, ukladanie záznamov o systémových udalostiach, realizácia bezpečného oddelenia vnútornej časti systému a siete od vonkajšej časti, a zavedie dokumentovanie postupov pre tieto operácie,
   5. zabezpečí nepretržitý monitoring informačného systému verejnej správy,
   6. zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch určených najmä s ohľadom na dôležitosť informačného systému verejnej správy a na minulé zistenia bezpečnostných auditov a pri zistení závažných bezpečnostných nedostatkov prepracuje bezpečnostný projekt a naň nadväzujúce dokumenty.

(4) V rámci vyradenia informačného systému verejnej správy z prevádzky správca

a) vypracuje plán vyradenia informačného systému verejnej správy z prevádzky, ktorý obsahuje najmä
   1. uchovanie informácií vyraďovaného informačného systému verejnej správy, ktoré sú potrebné pre funkčnosť iného informačného systému,
   2. spoľahlivé odstránenie informácií z pamäťových médií vyraďovaného informačného systému verejnej správy,
   3. postup vyraďovania programových prostriedkov a technických prostriedkov informačného systému verejnej správy,
b) zabezpečí, aby nedošlo ku strate alebo k úniku informácií a k narušeniu práv priemyselného vlastníctva a duševného vlastníctva.

§ 22

Bezpečnosť informačných technológií verejnej správy v oblasti monitoringu a hodnotenia

V oblasti monitoringu a hodnotenia správca vo vzťahu k informačným technológiám v jeho správe prijíma a vykonáva bezpečnostné opatrenia pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov podľa osobitného predpisu.[23])

§ 23

Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy

(1) Bezpečnostný projekt informačného systému verejnej správy sa vypracúva v súlade ~~s osobitným predpisom[21])~~so všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a tvorí súčasť bezpečnostnej dokumentácie. Vypracovanie bezpečnostného projektu informačného systému verejnej správy zabezpečí správca, vychádzajúc:

a) z bezpečnostnej stratégie kybernetickej bezpečnosti a bezpečnostných politík,
b) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajúz uznaných technických noriem,
c) z metodických usmernení orgánu vedenia.

(2) Správca vypracuje bezpečnostný projekt pre informačný systém verejnej správy, ktorý:

a) pri narušení bezpečnosti môže spôsobiť závažný kybernetický bezpečnostný incident,
b) tvorí základné registre alebo referenčné registre alebo je ich súčasťou,
c) je agendový informačný systém,
d) je nevyhnutný na rozhodovanie orgánu verejnej moci,
e) je špecializovaný portál,
f) spracúva osobitné kategórie osobných údajov podľa osobitného predpisu,[22a])
g) je zaradený do kategórie III. podľa osobitného predpisu.[22b])

(3) Orgán riadenia je povinný

a) ak je zaradený do registra prevádzkovateľov základných služieb alebo poskytovateľov digitálnych služieb podľa osobitného predpisu,3) nahlasovať spôsobom podľa osobitného predpisu3) aj kybernetický bezpečnostný incident,24) na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu;[3])
b) poskytnúť orgánu vedenia súčinnosť a spoluprácu pri plnení jeho úloh podľa § 23a a plniť pokyny orgánu vedenia pri výkone jeho oprávnení podľa § 23a,
c) zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c),
d) zasielať spôsobom určeným orgánom vedenia vládnej jednotke CSIRT vládnou jednotkou CSIRT určené systémové informácie o aktívach, rizikách, kontaktných bodoch a evidencii kybernetických bezpečnostných incidentov informačných technológií verejnej správy v rozsahu ustanovenom všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a aktualizovať zaslané údaje každých 14 dní,
e) zverejniť na svojom webovom sídle pravidlá na oznamovanie zraniteľností.

~~(3) Orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti sú povinní vo vzťahu k informačným technológiám verejnej správy~~

~~a) ak sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu,[24]) nahlasovať spôsobom podľa osobitného predpisu[25]) aj kybernetický bezpečnostný incident,[26]) na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu;[27]) ak nie sú do tohto registra zaradení, nahlasujú takýto kybernetický bezpečnostný incident orgánu vedenia ním určeným spôsobom,~~
~~b) poskytnúť orgánu vedenia súčinnosť a spoluprácu pri plnení jeho úloh podľa odseku 4,~~
~~c) zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c),~~
~~d) určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov podľa písmena a).~~

(4) Povinnosti podľa odseku 3 sa nevzťahujú na orgán riadenia:

a) podľa § 5 ods. 2 písm. f) a g) alebo

b) ktorý je prevádzkovateľom základnej služby[2a)] alebo poskytovateľom digitálnej služby[2b)] aj v inom sektore ako je sektor verejná správa.[25)] ~~ktorý je prevádzkovateľom základnej služby aj v inom sektore alebo podsektore[26)] ako je podsektor informačné systémy verejnej správy.“.~~

~~Orgán vedenia vo vzťahu k informačným technológiám verejnej správy~~

~~a) môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia kybernetického bezpečnostného incidentu, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti,~~

~~b) zbiera, spracúva a vyhodnocuje systémové informácie na účely predchádzania kybernetickým bezpečnostným incidentom, ich riešenia a obnovenia kybernetickej bezpečnosti,30)~~

~~c) vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu,~~

~~d)~~a) ~~môže na žiadosť orgánu riadenia za tento orgán riadenia vykonať bezpečnostný audit alebo preň vykonať hodnotenie zraniteľnosti~~.

(5) Orgán riadenia, ktorý nie je prevádzkovateľom základnej služby[2a)] alebo poskytovateľom digitálnej služby[2b)] podľa osobitného predpisu[3)] okrem povinností v odseku 3 je povinný

a) nahlasovať kybernetický bezpečnostný incident[24)] vládnej jednotke CSIRT,

b) bezodkladne riešiť kybernetický bezpečnostný incident a prijať opatrenia na zníženie rizika[26a)] vyplývajúceho zo zraniteľnosti bezodkladne po tom, ako sa o kybernetickom bezpečnostnom incidente alebo zraniteľnosti dozvedel,

c) poskytnúť orgánu vedenia súčinnosť a spoluprácu pri plnení jeho úloh podľa § 23a a plniť pokyny orgánu vedenia pri výkone jeho oprávnení podľa § 23a,

d) zasielať najmenej jedenkrát do roka orgánu vedenia zoznam aktív podľa § 19 ods. 1 písm. c),

e) prijať alebo upraviť bezpečnostné opatrenia, ak riešenie bezpečnostného incidentu, penetračné testovanie alebo hodnotenie zraniteľností alebo posúdenie bezpečnosti informačných technológií alebo informačných systémov orgánu riadenia a zistí riziko alebo hrozbu podľa osobitného predpisu[3)] pre bezpečnosť informačnej technológie verejnej správy alebo ak bola identifikovaná a vyhodnotená jej zraniteľnosť a oznámiť vládnej jednotke CSIRT prijaté bezpečnostné opatrenia,

f) viesť evidenciu kybernetických bezpečnostných incidentov, postupov na riešenie kybernetických bezpečnostných incidentov,

g) určiť a zverejniť na svojom hlavnom webovom sídle kontaktné údaje na kontaktný bod alebo primeraný počet kontaktných bodov na nahlasovanie kybernetického bezpečnostného incidentu.

§ 23a
Vedenie na úseku bezpečnosti informačných technológií verejnej správy

(1) Orgán vedenia

a) metodicky usmerňuje správcov na účely dosiahnutia a udržania bezpečnosti informačných technológií verejnej správy a zvyšuje povedomie správcov a verejnosti v oblasti kybernetickej bezpečnosti vo verejnej správe,

~~b) poskytuje údaje a informácie o stave kybernetickej bezpečnosti[26a)] v podsektore informačné systémy verejnej správy okrem informácií, ktorých zverejnenie by bolo rizikové z pohľadu bezpečnosti informačnej technológie verejnej správy.~~

b)~~c)~~ na žiadosť orgánu riadenia môže vykonať ~~bezpečnostný audit orgánu riadenia,~~ hodnotenie zraniteľností alebo posúdenie bezpečnosti informačných technológií alebo informačných systémov orgánu riadenia a s tým súvisiace činnosti.

~~(2) Vládna jednotka CSIRT vykonáva pre všetky orgány riadenia preventívne služby a reaktívne služby podľa osobitného prepdisu.[26b)] Vládna jednotka CSIRT tiež vykonáva riadenie riešenia kybernetických bezpečnostných incidentov a zraniteľností v pôsobnosti orgánu riadenia povinného nahlasovať kybernetické bezpečnostné incidenty podľa § 23 ods. 3 písm. a), ktoré zahŕňa najmä~~

~~a) asistenciu,~~
~~b) metodickú činnosť,~~
~~c) spoluprácu s orgánom riadenia pri riešení kybernetického bezpečnostného incidentu,~~
~~d) na žiadosť orgánu riadenia prevzatie časti riešenia kybernetického bezpečnostného incidentu a vydávanie pokynov, ktoré je orgán riadenia povinný plniť, ak je to nevyhnutné.~~

(2~~3~~) Orgán vedenia prostredníctvom vládnej jednotky CSIRT
a) na žiadosť správcu vykonáva činnosti nepretržitého monitorovania informačných technológií verejnej správy v jeho správe,
b) vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií verejnej správy poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu,
c) s predchádzajúcim súhlasom správcu vykonáva hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií verejnej správy poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu, ktoré boli zistené pri pravidelnom neinvazívnom hodnotení zraniteľností podľa písmena b),
d) zbiera, spracúva a vyhodnocuje systémové informácie informačných technológií verejnej správy podľa § 19 ods. 1 písm. c) a § 23 ods. 3 písm. d), v rozsahu ustanovenom všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a určuje periodicitu ich zberu,
e) môže na žiadosť orgánu riadenia vykonávať činnosti na účely riešenia kybernetického bezpečnostného incidentu, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti ~~zbiera, spracúva a vyhodnocuje systémové informácie o riadení rizík a bezpečnostných auditoch informačných technológií verejnej správy podľa § 19 ods. 1 písm. c) v rozsahu ustanovenom všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a údaje z evidencie kybernetických bezpečnostných incidentov[24]) podľa § 23 ods. 3 písm. f), na účely predchádzania kybernetickým bezpečnostným incidentom,[24]) ich riešenia a obnovenia kybernetickej bezpečnosti.~~

~~(4) Osobné údaje spracúvané na účely riešenia kybernetického bezpečnostného incidentu podľa odseku 2, monitorovania informačných technológií verejnej správy v pôsobnosti správcu na jeho žiadosť a ďalších činnostiach podľa odseku 3, spracúva a uchováva vládna jednotka CSIRT po dobu nevyhnutnú na naplnenie účelov, najneskôr do ukončenia konaní súvisiacich s kybernetickým bezpečnostným incidentom alebo do ukončenia monitorovania informačných technológií verejnej správy podľa osobitnej dohody so správcom.~~

~~(5) Vládna jednotka CSIRT pri spracúvaní osobných údajov podľa odseku 4 nie je povinná~~
~~a) poskytovať dotknutým osobám informácie o opravách, výmazoch alebo obmedzení spracúvania osobných údajov,~~
~~b) zaistiť prístup dotknutých osôb k osobným údajom, ani~~
~~c) opraviť alebo doplniť osobné údaje na žiadosť dotknutej osoby.~~

~~(6) Orgán vedenia prostredníctvom vládnej jednotky CSIRT plní úlohy koordinátora pre zverejňovanie zraniteľností informačných technológií verejnej správy.~~

~~(7) Vládna jednotka CSIRT je oprávnená zbierať, spracúvať a vyhodnocovať systémové informácie súvisiace s výkonom činností podľa tohto zákona alebo osobitných predpisov[26c]) a správca je povinný jej ich poskytnúť, ak nejde o utajovanú skutočnosť.[1]) Postupom podľa predchádzajúcej vety nie je dotknutá povinnosť ochrany informácií podľa osobitných predpisov[26d]) správcom, ktorý takúto informáciu poskytol, ani vládnou jednotkou CSIRT.~~

§ 24

Štandardy a výkladové stanoviská

(1) Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných technológií verejnej správy, ktorých účelom je vytvorenie jednotného prostredia umožňujúceho výmenu a spoločné používanie údajov a spoločných modulov medzi jednotlivými informačnými systémami verejnej správy a na účel ich prístupnosti a poskytovania pre verejnosť, a to najmä

a) štandard vzťahujúci sa na technické prostriedky, sieťovú infraštruktúru a na programové prostriedky,
b) štandard pre prístupnosť a funkčnosť webových sídiel a aplikácií a minimálne požiadavky na obsah webového sídla,
c) štandard použitia súborov,
d) štandard názvoslovia elektronických služieb,
e) dátové štandardy vzťahujúce sa na údaje, registre a na číselníky,
f) štandard poskytovania cloud computingu a využívania cloudových služieb vzťahujúci sa na technické prostriedky a na programové prostriedky,
g) štandard pre základné číselníky,
h) štandard pre elektronické formuláre,
i) štandard pre formáty, ktoré je možné autorizovať elektronickým podpisom alebo iným spôsobom autorizácie,
j) štandard pre projektové riadenie,
k) štandard pre dizajnový manuál,
~~j)~~l) štandard pre kritériá prioritnej elektronickej služby.

(2) Štandardy určujú podmienky, ktoré sa uplatňujú na informačné technológie verejnej správy,a orgán riadenia podľa nich postupuje pri riadení informačných technológií verejnej správy. Štandardy musia byť otvorené a technologicky neutrálne.

(3) Výkladové stanoviská vydáva orgán vedenia k ustanoveniam tohto zákona, ustanoveniam všeobecne záväzných právnych predpisov vydaných na jeho vykonanie a k štandardom, najmä ak ide o dôležité otázky alebo ak výkon správy informačných technológií nie je jednotný.

(4) Výkladové stanoviská vydáva orgán vedenia ich sprístupnením na svojom webovom sídle a na ústrednom portáli.

(5) Orgán riadenia môže vydávať technické pravidlá obdobné štandardom v oblastiach, v ktorých štandardy nie sú vydané, len ak sa tak vopred dohodne s orgánom vedenia.

§ 24a
Vládny cloud

(1) Vládny cloud je cloud computing prevádzkovaný vo forme hybridného cloudu, ktorý je tvorený vládnymi cloudovými službami.

(2) Vládnou cloudovou službou je cloudová služba, ktorá je zapísaná v evidencii vládnych cloudových služieb. Evidenciu vládnych cloudových služieb vedie orgán vedenia a sprístupňuje ju v centrálnom metainformačnom systéme verejnej správy.

(3) Orgán vedenia zapíše cloudovú službu do evidencie vládnych cloudových služieb na žiadosť poskytovateľa cloudovej služby, ak sú splnené podmienky podľa odseku 7 a má preukázané, že cloudová služba spĺňa štandardy poskytovania cloud computingu a využívania cloudových služieb podľa § 24 ods. 1 písm. f). Žiadosť podľa prvej vety sa podáva elektronicky, obsahuje identifikačné údaje poskytovateľa cloudovej služby, prevádzkovateľa cloudovej služby a opis cloudovej služby a prikladajú sa k nej dokumenty preukazujúce splnenie podmienok podľa prvej vety a vzorové zmluvy, ktoré sú s používaním cloudovej služby odberateľom cloudovej služby spojené. Ak ide o cloudovú službu určenú miestnej územnej samospráve, orgán vedenia si pred rozhodnutím o žiadosti vyžiada stanovisko správcu dátového centra obcí.36)

(4) Zápis podľa odseku 3 sa vykonáva s platnosťou na dva roky a poskytovateľ vládnej cloudovej služby môže požiadať o zápis na ďalšie dva roky najskôr šesť mesiacov pred uplynutím tejto doby; ustanovenia odseku 3 sa použijú rovnako. Ak dôjde k zmene vládnej cloudovej služby alebo jej podstatných parametrov, orgán vedenia vykoná opätovné posúdenie splnenia podmienok na zápis do evidencie vládnych cloudových služieb podľa odseku 3. Ak vládna cloudová služba prestane spĺňať podmienky na jej zápis do evidencie vládnych cloudových služieb podľa odseku 3, orgán vedenia ju z evidencie vymaže.

(5) Štandardy podľa § 24 ods. 1 písm. f) ustanovia úrovne cloudových služieb podľa odseku 8 písm. e), pri ktorých dosiahnutí môže orgán riadenia na účely konania v rozsahu podľa osobitných predpisov vo veciach práv, právom chránených záujmov a povinností fyzických osôb alebo právnických osôb odoberať a využívať len cloudové služby, ktoré sú vládnymi cloudovými službami.

(6) Odberateľom vládnych cloudových služieb môže byť len orgán riadenia. Orgán riadenia je povinný oznamovať orgánu vedenia, ktoré vládne cloudové služby využíva vrátane orgánom vedenia určených informácií potrebných na plnenie jeho úloh podľa odseku 8; na tento účel orgán vedenia sprístupňuje pre orgány riadenia elektronickú službu.

(7) Poskytovateľom cloudovej služby a prevádzkovateľom cloudovej služby v časti privátneho cloudu v modeli infraštruktúra ako služba a platforma ako služba môže byť spomedzi orgánov riadenia len Ministerstvo vnútra Slovenskej republiky, pričom pre tieto služby výpočtové zdroje zabezpečujú datacentrum v správe Ministerstva vnútra Slovenskej republiky a datacentrum v správe Ministerstva financií Slovenskej republiky; ak je to potrebné, orgán vedenia môže rozhodnúť, že v časti privátneho cloudu môže zabezpečovať výpočtové zdroje a poskytovať alebo prevádzkovať cloudovú službu v modeli infraštruktúra ako služba a platforma ako služba aj iná osoba, ktorá je správcom nadrezortného informačného systému verejnej správy.

(8) Orgán vedenia koordinuje poskytovanie a používanie vládnych cloudových služieb a na tento účel
a) kontroluje splnenie a dodržiavanie podmienok na zaradenie cloudovej služby do evidencie vládnych cloudových služieb podľa odseku 3,
b) usmerňuje orgány riadenia pri poskytovaní a používaní vládnych cloudových služieb a pri správe zmluvných vzťahov s nimi súvisiacich vrátane koordinácie požiadaviek na dohody o úrovni poskytovania vládnych cloudových služieb a dohľadu nad ich dodržiavaním,
c) vypracúva plán implementácie, rozvoja a centralizácie datacentier v správe orgánov riadenia a dohliada na jeho uplatňovanie,
d) vyhodnocuje požiadavky na vládne cloudové služby, ich používanie a stav ich poskytovania,
e) štandardizuje kategorizácie cloudových služieb podľa úrovne bezpečnosti v nadväznosti na kategorizáciu údajov, ktorých sa ich používanie týka.

(9) Zmluvy o používaní vládnej cloudovej služby musia obsahovať náležitosti podľa osobitného predpisu,30a) ktoré sa použijú v prípade, ak bude poskytovateľ vládnej cloudovej služby spracúvať osobné údaje v mene odberateľa cloudovej služby.

§ 24b
Govnet

(1) Govnet je vládny elektronický komunikačný systém vytvorený na účely plnenia úloh vyplývajúcich orgánom riadenia z osobitných predpisov, ktorý je tvorený z elektronických komunikačných sietí a elektronických komunikačných služieb. Elektronické komunikačné služby sú súčasťou Govnetu v rozsahu podľa všeobecne záväzného právneho predpisu vydaného ministerstvom investícií.

(2) Správca Govnetu poverí prevádzkou a rozvojom Govnetu príspevkovú organizáciu zriadenú na tento účel, ktorá je podnikom podľa osobitného predpisu.[30b]) Výdavky správcu Govnetu, vynaložené na zabezpečenie prevádzky a rozvoja Govnetu, sú výdavkami tohto správcu vynaloženými na plnenie jeho úloh.

(3) Ak prevádzku Govnetu nie je technicky možné zabezpečiť vlastnými prostriedkami prevádzkovateľa, možno na účely zabezpečenia prevádzky Govnetu využiť verejnú elektronickú komunikačnú sieť.

(4) Govnet nie je verejnou sieťou[30c]) a nie je tvorený verejne dostupnými službami.[30d)] Do Govnetu sa pripája orgán riadenia, ktorý je štátnou rozpočtovou organizáciou. Orgán riadenia, ktorý nie je štátnou

rozpočtovou organizáciou sa môže pripojiť do Govnetu, ak sa tak dohodne so správcom Govnetu.

(5) Pre orgán riadenia, ktorý je štátnou rozpočtovou organizáciou, je používanie Govnetu bezodplatné; pre iný orgán riadenia je používanie Govnetu spojené s povinnosťou úhrady podľa cenníka úhrad za používanie Govnetu podľa všeobecne záväzného právneho predpisu vydaného ministerstvom investícií.

(6) Prevádzka Govnetu musí byť plynulá, bezpečná a spoľahlivá a musí byť vykonávaná v súlade s bezpečnostnými a technickými pravidlami prevádzky Govnetu podľa všeobecne záväzného právneho predpisu vydaného ministerstvom investícií.

(7) Činnosti súvisiace s nepretržitým monitorovaním na účely zabezpečenia kybernetickej bezpečnosti Govnetu vykonáva aj vládna jednotka ~~pre riešenie kybernetických bezpečnostných incidentov.~~CSIRT.[30f])“.

§ 24c

Dizajnový manuál

(1) Dizajnový manuál upravuje vzhľad a zobrazenie grafického používateľského rozhrania elektronickej služby, webovej stránky zobrazujúcej elektronickú službu a hlavného webového sídla.

(2) Orgán vedenia

a) zodpovedá za aktualizáciu, rozvoj a správu dizajnového manuálu,

b) poskytuje orgánom riadenia podporu pri tvorbe grafického používateľského rozhrania elektronickej služby, webovej stránky zobrazujúcej elektronickú službu a hlavného webového sídla podľa štandardu dizajnového manuálu.

(3) Orgán riadenia môže vyvíjať vlastné komponenty podľa princípov dizajnového manuálu, ak ide o komponenty, ktoré nie sú ustanovené štandardmi dizajnového manuálu alebo upravovať už existujúce komponenty podľa svojej potreby a na základe dohody s orgánom vedenia.

(4) Ak orgán riadenia zásadne mení už existujúcu elektronickú službu určenú koncovému používateľovi, ktorý nie je orgánom riadenia a- súčasťou zásadnej zmeny je aj zmena grafického používateľského rozhrania, postupuje podľa štandardov dizajnového manuálu.

5) Pri zásadnej zmene vizuálnej podoby hlavného webového sídla postupuje orgán riadenia podľa štandardov dizajnového manuálu.

(6)~~(5)~~ Zásadnou zmenou sa na účely odsekov 4 a 5 rozumie zásadná zmena grafického používateľského rozhrania alebo zmena vizuálnej podoby, ktorá spočíva najmä v zmene typografie, farby a rozloženia prvkov hlavičky, farby a rozloženia prvkov päty~~Pri zmene vizuálnej podoby hlavného webového sídla, ktorá spočíva najmä v zmene typografie, farby a rozloženia prvkov hlavičky, farby a rozloženia prvkov päty postupuje orgán riadenia podľa štandardov dizajnového manuálu. Povinnosť podľa prvej vety sa nevzťahuje na orgány riadenia podľa § 5 ods. 2 písm. c) a e) až h), zdravotné poisťovne, Tlačovú agentúru Slovenskej republiky a Rozhlas a televíziu Slovenska~~.

§ 25

Základné číselníky

(1) Základným číselníkom je číselník zaradený v zozname základných číselníkov.

(2) Orgán vedenia zaradí číselník do zoznamu základných číselníkov. Zoznam základných číselníkov je vydaný jeho zverejnením v centrálnom metainformačnom systéme verejnej správy.

(3) Zoznam základných číselníkov obsahuje názov základného číselníka, kód základného číselníka, názov gestora základného číselníka a dátum účinnosti určenia gestora základného číselníka.

(4) Orgán vedenia určí za gestora základného číselníka orgán riadenia jeho zverejnenímv zozname základných číselníkov.

(5) Gestor základného číselníka je povinný

a) vydať základný číselník, ktorého je gestorom, zverejnením prostredníctvom centrálneho metainformačného systému verejnej správy do jedného mesiaca odo dňa, keď jeho určenie za gestora tohto základného číselníka nadobudlo účinnosť,
b) riadne spravovať a aktualizovať základný číselník, ktorého je gestorom.

(6) Ak úsek verejnej správy alebo agenda verejnej správy, ktorých sa základný číselník týka, patria podľa osobitných predpisov do pôsobnosti viacerých orgánov riadenia, orgán vedenia môže určiť viacero gestorov základného číselníka, pričom zároveň

a) určí, ktorý z gestorov základného číselníka je hlavným gestorom základného číselníka a ktorí gestori základného číselníka sú vedľajšími gestormi základného číselníka, a uvedie to v zozname základných číselníkov,
b) povinnosť podľa odseku 5 písm. a) a povinnosť riadne spravovať základný číselník plní hlavný gestor základného číselníka,
c) povinnosti poskytovať do základného číselníka údaje a udržiavať ho aktuálny plnia hlavnýgestor základného číselníka a vedľajší gestori základného číselníka v rozsahu údajov, v akom podľa osobitných predpisov patria do ich pôsobnosti úseky verejnej správy alebo agendy verejnej správy, ktorých sa základný číselník týka.

(7) Orgán vedenia poskytuje gestorom základného číselníka súčinnosť pri prístupek centrálnemu metainformačnému systému verejnej správy na účely plnenia ich povinností podľa odsekov 5 a 6.

§ 26

Vydávanie elektronického odpisu a výstupu z informačného systému verejnej správy

(1) Na žiadosť oprávnenej osoby a po splnení podmienok ustanovených osobitnými predpismi[31]) vydávajú prevádzkovatelia informačných systémov verejnej správy elektronický odpis a výstupz týchto systémov.

(2) Výstup vydáva aj osvedčujúca osoba, ak to umožňujú technické podmienky na strane osvedčujúcej osoby alebo na strane prevádzkovateľa informačného systému verejnej správy; na tento účel prevádzkovateľ informačného systému verejnej správy odošle osvedčujúcej osobe na jej žiadosť elektronický odpis, ktorý je autorizovaný[32]) a má pripojenú kvalifikovanú elektronickú časovú pečiatku.[33]) Osvedčujúcimi osobami sú orgán verejnej moci, ktorý osvedčuje podľa osobitných predpisov,[34]) a notár. Činnosti osvedčujúcej osoby vykonáva aj poštový podnik poskytujúci univerzálnu službu so 100-percentnou majetkovou účasťou štátu.

(3) Elektronický odpis je súhrn údajov z informačného systému verejnej správy v elektronickej podobe, ktorý je autorizovaný a ku ktorému je pripojená kvalifikovaná elektronická časová pečiatka.

(4) Výstup je súhrn údajov z informačného systému verejnej správy v listinnej podobe, ktorý je vytvorený zaručenou konverziou[35]) elektronického odpisu. Výstup, ktorý obsahuje údaje zapísané do informačného systému verejnej správy na základe listín vydaných orgánom verejnej moci, je verejnou listinou.

(5) Z neverejných častí informačných systémov verejnej správy sa vydáva elektronický odpis

a) osobe, ktorá má oprávnenie oboznamovať sa s týmito údajmi podľa osobitného predpisu,
b) osvedčujúcej osobe, ktorú o to písomne požiada osoba, ktorá má oprávnenie oboznamovať sa s týmito údajmi, ak osobitný predpis neustanovuje inak.

(6) Z neverejných častí informačných systémov verejnej správy je prevádzkovateľ informačného systému verejnej správy povinný elektronický odpis odoslať tak, aby bol jeho obsah zodpovedajúcim spôsobom chránený pred neoprávneným prístupom zo strany tretích osôb.

(7) Prevádzkovateľ informačného systému verejnej správy je povinný zistiť totožnosť osoby žiadajúcej o vydanie elektronického odpisu alebo výstupu, ak to vyplýva z osobitného predpisu.[31])

(8) Prevádzkovateľ informačného systému verejnej správy zodpovedá za súlad elektronického

odpisu s aktuálnym stavom údajov v informačnom systéme verejnej správy v čase vydania elektronického odpisu.

(9) Poštový podnik podľa odseku 2 má za činnosť osvedčujúcej osoby nárok na úhradu podľa sadzobníka úhrad ustanoveného všeobecne záväzným právnym predpisom, ktorý vydá ministerstvo investícií.

Osobitné postupy

§ 27

(1) Ak sú splnené podmienky podľa odseku 2, orgán riadenia môže požiadať orgán vedenia o povolenie zmeny v rozsahu alebo spôsobe plnenia povinností podľa tohto zákona, všeobecne záväzných predpisov vydaných na jeho vykonanie alebo štandardov (ďalej len „rozhodnutie o osobitnom postupe“).

(2) Orgán vedenia môže vydať rozhodnutie o osobitnom postupe, ak

a) by postup podľa tohto zákona, všeobecne záväzných právnych predpisov vydaných na jeho vykonanie alebo štandardov bol pre orgán riadenia, s ohľadom na jeho finančné, personálne alebo technické kapacity alebo s ohľadom na dôležitosť využívania informačných technológií na plnenie jeho úloh podľa osobitných predpisov, spojený s mimoriadnou náročnosťou, podmienený prekonaním mimoriadnych prekážok alebo by podstatne ohrozil plnenia iných zákonných povinností,
b) nie je možné použiť postup podľa § 28 ods. 2,
c) to osobitný predpis nezakazuje, a
d) tým nedôjde k ohrozeniu plynulosti, bezpečnosti, prístupnosti a spoľahlivosti prevádzky informačných technológií verejnej správy v správe orgánu riadenia.

(3) Rozhodnutie o osobitnom postupe musí byť riadne odôvodnené a možno ho vydať s platnosťou len na nevyhnutne potrebný čas a v nevyhnutnom rozsahu. Každé rozhodnutie o osobitnom postupe je orgán vedenia povinný zverejniť v centrálnom metainformačnom systéme verejnej správy, inak nevyvolá účinky. Rozhodnutie o osobitnom postupe zverejní orgán vedenia na ústrednom portáli a odkaz na toto zverejnenie aj na svojom webovom sídle.

(4) Ak je to účelné, orgán vedenia môže vydať rozhodnutie o osobitnom postupe, ak sú splnené podmienky podľa odseku 2, aj bez návrhu orgánu riadenia, ak sa rozhodnutie o osobitnom postupe má vzťahovať na viaceré orgány riadenia alebo na viaceré informačné technológie verejnej správy. Ak orgán vedenia postupuje podľa prvej vety, v rozhodnutí o osobitnom postupe musia byť dotknuté orgány riadenia alebo informačné technológie verejnej správy najmenej druhovo určené; ustanovenia odseku 3 sa použijú rovnako.

§ 28

(1) Za orgán riadenia, ktorým je obec, a vo vzťahu k informačným technológiám verejnej správy, ktorých prevádzkovanie zabezpečuje obec prostredníctvom dátového centra obcí,[36]) plní povinnosti podľa § 8 ods. 2, § 12 ods. 1 písm. a) a b) a § 14 ods. 3 správca informačného systému dátového centra obcí.

(2) Ak je to dôvodné a ak tým nedôjde k ohrozeniu plynulosti, bezpečnosti, prístupnosti a spoľahlivosti prevádzky informačných technológií verejnej správy, za orgán riadenia podľa § 5 ods. 2 písm. e) môže plniť povinnosti podľa tohto zákona, všeobecne záväzných právnych predpisov vydaných na jeho vykonanie alebo štandardov ten orgán riadenia, ktorý voči nemu vykonáva zriaďovateľskú pôsobnosť alebo zakladateľskú pôsobnosť. Orgán riadenia, ktorý vykonáva zriaďovateľskú pôsobnosť alebo zakladateľskú pôsobnosť, môže postupovať podľa prvej vety, len ak to vopred písomne oznámi orgánu vedenia a orgán vedenia do 60 dní odo dňa doručenia oznámenia nevysloví s takýmto postupom nesúhlas. Nesúhlas orgánu riadenia môže byť odôvodnený len ohrozením plynulosti, bezpečnosti, prístupnosti a spoľahlivosti prevádzky informačných technológií verejnej správy, musí byť písomný a doručuje sa orgánu riadenia, ktorý písomné oznámenie orgánu vedenia doručil. Každý prípad postupu podľa prvej vety je orgán riadenia, ktorý vykonáva zriaďovateľskú pôsobnosť alebo zakladateľskú pôsobnosť, povinný zverejniť v centrálnom metainformačnom systéme verejnej správy, inak orgán riadenia takto postupovať nemôže; informáciu o postupe zverejní aj na ústrednom portáli a odkaz na toto zverejnenie aj na svojom

webovom sídle.

§ 29
Správne delikty

(1) Orgán vedenia uloží pokutu

a) od 500 eur do 35 000 eur správcovi, ktorý poruší povinnosť podľa § 6 ods. 1, § 12 ods. 1 písm. a), § 14 ods. 6, § 15 ods. 2 alebo § 16 ods. 3 písm. e) alebo povinnosti na úseku bezpečnosti informačných technológií verejnej správy podľa § 19 až 21 alebo § 23 alebo 23a,

b) od 250 eur do 35 000 eur

1. správcovi, ktorý poruší povinnosť podľa § 12 ods. 1 písm. b), g), h), povinnosť vypracovať koncepciu rozvoja podľa § 13, ~~alebo~~ povinnosť aktualizovať koncepciu rozvoja podľa § 14 ods. 3 alebo povinnosť podľa § 15 ods. 11,
2. prevádzkovateľovi informačného systému verejnej správy, ktorý poruší povinnosť podľa § 26 ods. 2, 6 alebo ods. 7, alebo ak elektronický odpis nie je, v momente jeho vydania, v súlade s aktuálnym stavom údajov v informačnom systéme verejnej správy,

c) od 250 eur do 25 000 eur

1. správcovi, ktorý poruší povinnosť podľa § 12 ods. 1 písm. e) alebo písm. f) alebo povinnosť dodržiavať štandardy,
2. orgánu riadenia, ktorý poruší povinnosť podľa § 8 ods. 2, § 12 ods. 1 písm. c) alebo písm. j), § 15 ods. 4 písm. d) alebo písm. e), § 16 ods. 3 písm. d) alebo § 24a ods. 5,
3. orgánu riadenia, ktorý poruší povinnosť podľa § 13a~~2~~ ods. ~~1 písm. m)~~2 opakovane a nevykoná nápravu ani po výzve od orgánu vedenia,

d) od 125 eur do 5 000 eur orgánu riadenia alebo osvedčujúcej osobe, ak poruší inú povinnosť podľa tohto zákona, než je uvedená v písmenách a) až c).

(2) ~~Pri~~ Na konanie o ukladaní pokút podľa odseku 1 sa ~~postupuje~~ vzťahuje ~~podľa~~ všeobecn~~ého~~ý predpis~~u~~ o správnom konaní[36a]).

~~(2)~~(3) Pri ukladaní pokuty orgán vedenia prihliadne na závažnosť, spôsob, trvanie a následky protiprávneho konania, na opakované porušenie povinností alebo na porušenie viacerých povinností. Od uloženia pokuty možno upustiť, ak s prihliadnutím na okolnosti podľa prvej vety postačí na nápravu samotné prejednanie správneho deliktu.

~~(3)~~(4) Pokuta je splatná do 15 dní odo dňa, keď rozhodnutie o jej uložení nadobudlo právoplatnosť.

~~(4)~~(5) Pokuty sú príjmom štátneho rozpočtu.

~~(5)~~(6) Pokutu možno uložiť do troch rokov odo dňa porušenia povinnosti.

Spoločné, prechodné a záverečné ustanovenia

§ 30

(1) Správca majetku štátu[37]) môže prenechať informačný systém alebo jeho časť, ktoré sú vo vlastníctve Slovenskej republiky, na základe písomnej zmluvy orgánu riadenia do užívania vrátane ich rozvoja alebo rozšírenia, ak tomu nebránia podmienky, za ktorých boli nadobudnuté alebo za ktorých sa užívajú.

(2) Zmluva podľa odseku 1 obsahuje najmä

a) identifikáciu informačného systému alebo jeho časti vrátane identifikácie technických prostriedkov, ak sa tieto poskytujú spolu s programovými prostriedkami informačnéhosystému,

b) odplatu za užívanie, prevádzku alebo aplikačnú podporu informačného systému alebo programových prostriedkov, ak je dohodnutá,

c) určenie rozsahu užívacích práv k informačnému systému alebo jeho časti a rozsahu elektronických služieb verejnej správy, na ktorých poskytovanie slúži.

(3) Na užívanie majetku vo vlastníctve Slovenskej republiky podľa odseku 1 sa nevzťahuje osobitný predpis.[38])

(4) Správca majetku štátu môže hnuteľný majetok vo vlastníctve Slovenskej republiky, tvoriaci

technické prostriedky a programové prostriedky informačného systému, vypožičať inému správcovi majetku štátu, obci alebo vyššiemu územnému celku, a to aj keď nie je dočasne prebytočný.

§ 31

Všeobecne záväzný právny predpis, ktorý sa v Zbierke zákonov Slovenskej republiky vyhlasuje uverejnením úplného znenia a ktorý vydá ministerstvo investícií, ustanoví

a) jednotlivé kategórie informačných technológií verejnej správy a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu na účely podľa § 11 ods. 4,
b) najvyššiu celkovú cenu a najdlhšiu lehotu dodania na účely podľa § 11 ods. 6,
c) podrobnosti o zmluve v prevádzke, najvyššiu celkovú cenu na účely § 11 ods. 7 a spôsob jej určenia,
d) ~~c)~~ podrobnosti o zabezpečení organizačných podmienok a procesných podmienok podľa § 14 ods. 5,
e) ~~d)~~ podrobnosti o riadení projektov podľa § 15 ods. 4 a najvyššiu cenu čiastkového plnenia a najdlhšiu lehotu dodania čiastkového plnenia podľa § 15 ods. 4 písm. d) tretieho bodu a štvrtého bodu,
f) ~~e)~~ úrovne prevádzkových problémov a prevádzkových incidentov podľa § 16 ods. 3 písm. b) a kritériá na určenie úrovne kontinuity podľa § 16 ods. 4 písm. a)
g) ~~f)~~ podrobnosti o
    1. nastavení riadenia prevádzky informačných technológií verejnej správy podľa § 16 ods. 2,
    2. zabezpečení riadenia prevádzky informačných technológií verejnej správy vrátane zmenových požiadaviek v prevádzke, servisných požiadaviek, zmlúv v prevádzke, správy prevádzkových problémov, prevádzkových incidentov podľa § 16 ods. 3 a
    3. zabezpečení riadenia kontinuity prevádzky informačných technológií verejnej správy podľa § 16 ods. 4,
h) ~~g)~~ rozsah a oblasti zberu údajov podľa § 17 ods. 2 písm. c),
i) ~~h)~~ rozsah a spôsob plnenia povinností podľa § 14~~3~~a až 17, iných ako podľa písmen c) až g) v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov,
j) ~~i)~~ na úseku bezpečnosti informačných technológií verejnej správy
    1. podrobnosti o bezpečnosti informačných technológií verejnej správy,
    2. bezpečnostné opatrenia,
    3. rozsah a spôsob prijímania a realizácie bezpečnostných opatrení v závislosti od klasifikácie informácií~~i~~ a od kategorizácie sietí a informačných systémov,
    4. obsah a štruktúru bezpečnostného projektu,
    ~~podrobnosti o spôsobe nahlasovania zraniteľností,~~
    5. rozsah údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT podľa § 18 až 23a,
    ~~1. , podrobnosti o bezpečnosti informačných technológií verejnej správy podľa § 18 až 23, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietía informačných systémov,~~
~~j)~~k) základné zásady elektronizácie agendy verejnej správy, tvorby a rozvoja elektronických služieb a používateľských rozhraní, spôsob a postupy pri elektronizácii agendy verejnej správy orgánu riadenia na účely zabezpečenia riadneho výkonu poskytovania služieb verejnej správy, služieb vo verejnom záujme a verejných služieb a zabezpečenia riadnej prevádzky informačných technológií verejnej správy,
~~k)~~l) štandardy podľa § 24
~~l)~~m) cenník úhrad za používanie Govnetu podľa § 24b ods. 5, rozsah elektronických komunikačných služieb Govnetu a bezpečnostné a technické pravidlá prevádzky Govnetu,
~~m)~~n) sadzobník úhrad podľa § 26 ods. 9.

§ 32

Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné

systémy verejnej správy v znení neskorších predpisov vydaný podľa doterajšieho zákona zostáva platný a účinný do nadobudnutia účinnosti vykonávacieho právneho predpisu podľa § 31, najneskôr však do 1. mája 2020.

§ 33

(1) Informačné systémy verejnej správy podľa doterajších predpisov sú informačnými systémami verejnej správy podľa tohto zákona.

(2) Národná koncepcia schválená podľa doterajších predpisov je národnou koncepciou podľa tohto zákona v rozsahu, v akom je s ním v súlade. Koncepcia rozvoja schválená podľa doterajších predpisov je koncepciou rozvoja podľa tohto zákona v rozsahu, v akom je s ním v súlade. Orgán vedenia vypracuje návrh novej národnej koncepcie v lehote podľa odseku 4.

(3) Povinná osoba podľa doterajších predpisov je orgánom riadenia podľa tohto zákona.

(4) Správca je povinný zosúladiť informačné technológie verejnej správy v jeho správe, ktoré sú vytvorené alebo nadobudnuté ku dňu účinnosti tohto zákona, ako aj tie, vo vzťahu ku ktorým ku dňu účinnosti tohto zákona začal verejné obstarávanie alebo obdobnú činnosť na účely ich nadobudnutia, s ustanoveniami tohto zákona do dvoch rokov odo dňa účinnosti tohto zákona. Povinnosť podľa prvej vety sa nevzťahuje na také povinnosti podľa tohto zákona, ktoré sa, najmäna úseku obstarávania a implementácie, viažu na nadobudnutie informačnej technológie verejnej správy a nie je ich objektívne možné splniť alebo ich splnenie nie je vo výlučnej dispozícii správcua bolo by pre správcu neprimerane náročné.

(5) Do uplynutia 30 dní odo dňa zriadenia a uvedenia do prevádzky jednotného informačného systému kybernetickej bezpečnosti[39]) nahlasuje orgán riadenia podľa § 5 ods. 2 písm. a) a b)a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, ktorí sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu, kybernetický bezpečnostný incident podľa § 23 ods. 3 písm. a) orgánu vedenia ním určeným spôsobom.

(6) Konanie o uložení pokuty začaté podľa doterajších predpisov a právoplatne neukončené ku dňu účinnosti tohto zákona sa dokončí podľa doterajších predpisov a pri ukladaní pokút sa použije tento zákon, ak je to pre páchateľa správneho deliktu priaznivejšie.

§ 33a
Prechodné ustanovenia k úpravám účinným od 1. novembra 2022

(1) Orgán vedenia zverejní zoznam kľúčových parametrov pre riadenie prevádzky informačných technológií verejnej správy na pripomienkovanie podľa § 9 ods. 2 najneskôr 31. marca 2023.

(2) Vládny cloud, vládna cloudová služba a evidencia vládnych cloudových služieb podľa predpisov účinných do 31. októbra 2022 sú vládnym cloudom, vládnou cloudovou službou a evidenciou vládnych cloudových služieb podľa tohto zákona v znení účinnom od 1. novembra 2022.

(3) Orgán riadenia, ktorý je štátnou rozpočtovou organizáciou je povinný postupovať podľa § 24b ods. 4 najneskôr od 1. augusta 2024.

§ 34

Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v prílohe.

§ 35

Zrušujú sa:

1. zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení čl. II zákona č. 678/2006 Z. z., čl. II zákona č. 385/2008 Z. z., čl.I zákona č. 553/2008 Z. z., čl. I zákona č. 570/2009 Z. z., čl. IV zákona č. 69/2012 Z. z., čl.I zákona č. 289/2012 Z. z., čl. I zákona č. 202/2013 Z. z., čl. VIII zákona č. 305/2013 Z. z., čl.X zákona č. 176/2015 Z. z., čl. XI zákona č. 273/2015 Z. z., čl. VIII zákona č.

238/2017
Z. z. a čl. II zákona č. 313/2018 Z. z.,

2. výnos Ministerstva financií Slovenskej republiky č. 478/2010 Z. z. o základnom číselníku úsekov verejnej správy a agend verejnej správy.

Čl. II

Zákon č. 85/1990 Zb. o petičnom práve v znení zákona č. 242/1998 Z. z., zákona č. 112/2010
Z. z. a zákona č. 29/2015 Z. z. sa dopĺňa takto:

1. Za § 6a sa vkladajú § 6b až 6e, ktoré vrátane nadpisov znejú:

„§ 6b

Podpora iniciatívy občanov členských štátov Európskej únie

Na postup pri organizovaní a podpore iniciatívy občanov členských štátov Európskej únie (ďalej len „občan"), ako aj na podmienky výkonu iniciatívy občanov sa vzťahuje osobitný predpis.[5a])

§ 6c

Posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov

(1) Posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov vykonáva Úradom vlády Slovenskej republiky na tento účel poverená osoba (ďalej len „posudzovateľ systému zberu"), znalec alebo znalecký ústav v príslušnom odbore a odvetví.[5b]) Poverenie posudzovateľa systému zberu uskutočňuje Úrad vlády Slovenskej republiky na základe výzvy zverejnenej na svojom webovom sídle. Posudzovateľom systému zberu môže byť len osoba, ktorá spĺňa odborné predpoklady na posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov uvedené vo výzve podľa druhej vety. Posudzovateľ systému zberu je povinný spĺňať tieto predpoklady po celý čas vykonávania posudzovania elektronického systému zberu vyhlásení o podpore iniciatívy občanov. Zoznam posudzovateľov systému zberu a jeho zmeny zverejňuje Úrad vlády Slovenskej republiky na svojom webovom sídle. Ak posudzovateľ systému zberu nemôže vykonávať posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov, je povinný túto skutočnosť s uvedením dôvodov bezodkladne oznámiť Úradu vlády Slovenskej republiky.

(2) Posudzovateľ systému zberu je povinný vykonávať posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov v súlade s osobitným predpisom[5c]) na základe listinnej žiadosti alebo elektronickej žiadosti o posúdenie elektronického systému zberu vyhlásení o podpore iniciatívy občanov (ďalej len „žiadosť o posúdenie systému zberu") podanej Úradu vlády Slovenskej republiky. Vzor žiadosti o posúdenie systému zberu je uvedený v prílohe.

(3) Ak žiadosť o posúdenie systému zberu neobsahuje náležitosti uvedené v prílohe, Úrad vlády Slovenskej republiky vyzve žiadateľa, aby v lehote piatich dní odstránil jej nedostatky. Ak žiadateľ v tejto lehote nedostatky neodstráni, Úrad vlády Slovenskej republiky žiadosť o posúdenie systému zberu vráti žiadateľovi a bezodkladne oznámi túto skutočnosť posudzovateľovi systému zberu. Posudzovateľ systému zberu je povinný bezodkladne po doručení tohto oznámenia vrátiť žiadateľovi uhradené náklady spojené s posudzovaním elektronického systému zberu vyhlásení o podpore iniciatívy občanov.

(4) Žiadosť o posúdenie systému zberu, ktorá obsahuje náležitosti uvedené v prílohe, Úrad vlády Slovenskej republiky bezodkladne zašle posudzovateľovi systému zberu uvedenému v tejto žiadosti. Posudzovateľ systému zberu po posúdení elektronického systému zberu vyhlásení o podpore iniciatívy občanov uvedie v žiadosti o posúdenie systému zberu vyjadrenie, či tento systém spĺňa, alebo nespĺňa požiadavky podľa osobitného predpisu.[5d])

(5) Ak elektronický systém zberu vyhlásení o podpore iniciatívy občanov spĺňa požiadavky podľa osobitného predpisu, Úrad vlády Slovenskej republiky vydá osvedčenie[5e]) o súlade elektronického systému zberu vyhlásení o podpore iniciatívy občanov s osobitným predpisom a zašle ho žiadateľovi o posúdenie systému zberu do jedného mesiaca od podania úplnej žiadosti o posúdenie systému zberu.

(6) Ak elektronický systém zberu vyhlásení o podpore iniciatívy občanov nespĺňa požiadavky podľa osobitného predpisu, Úrad vlády Slovenskej republiky zamietne žiadosť o posúdenie systému zberu a oznámi túto skutočnosť žiadateľovi o posúdenie systému zberu s uvedením dôvodov nesplnenia týchto požiadaviek do jedného mesiaca od podania úplnej žiadosti o posúdenie systému zberu.

(7) Náklady spojené s posudzovaním elektronického systému zberu vyhlásení o podpore iniciatívy občanov uhrádza žiadateľ, ktorý uhradí tieto náklady pred podaním žiadostio posúdenie systému zberu. Doklad o úhrade týchto nákladov je prílohou k žiadosti o posúdenie systému zberu. Posudzovateľ systému zberu je povinný bezodkladne po poverení podľa odseku 1 vypracovať a zaslať Úradu vlády Slovenskej republiky sadzobník úhrad nákladov spojených s posudzovaním elektronického systému zberu vyhlásení o podporeiniciatívy občanov vrátane čísla účtu, na ktoré sa tieto náklady uhradia; Úrad vlády Slovenskej republiky tento sadzobník zverejní na svojom webovom sídle. Ak posudzovateľ systému zberu vypracuje zmeny tohto sadzobníka, je povinný ich bezodkladne zaslať Úradu vlády Slovenskej republiky, ktorý ich zverejní na svojom webovom sídle.

(8) Ak posudzuje elektronický systém zberu vyhlásení o podpore iniciatívy občanov znalec alebo znalecký ústav, podmienky výkonu znaleckej činnosti pri posudzovaní tohto systémua podmienky poskytnutia odmeny, náhrady hotových výdavkov a náhrady za stratu času zatúto činnosť ustanovuje osobitný predpis,[5b]) pričom ustanovenia odsekov 2, 3 prvej a druhejvety a odsekov 4 až 6 sa použijú rovnako a ustanovenie odseku 7 sa nepoužije.

§ 6d

Overovanie vyhlásení o podpore iniciatívy občanov

Na účely koordinácie procesu overovania a osvedčovania vyhlásení o podpore iniciatívy občanov v listinnej podobe podľa osobitného predpisu[5f]) je príslušným Úrad vlády Slovenskej republiky.

§ 6e

Pokuty na úseku podpory iniciatívy občanov

(1) Úrad vlády Slovenskej republiky uloží pokutu

a) od 2 000 eur do 35 000 eur posudzovateľovi systému zberu, ak poruší povinnosť ustanovenú v § 6c,

b) od 500 eur do 10 000 eur organizátorovi,[5g]) ak pri

1. plnení povinností podľa osobitného predpisu[5a]) poskytne nepravdivé vyhlásenie alebo
2. použije údaje získané pri organizovaní iniciatívy občanov na iný účel, než na ktorý boli poskytnuté,

c) od 125 eur do 2 500 eur organizátorovi, ak poruší povinnosť ustanovenú osobitnýmpredpisom,[5a]) za ktorú sa neukladá pokuta podľa písmena b).

(2) Pri ukladaní pokuty Úrad vlády Slovenskej republiky prihliadne na závažnosť, spôsob, trvanie a následky protiprávneho konania, na opakované porušenie povinností alebo na porušenie viacerých povinností.

(3) Pokuta je splatná do 15 dní odo dňa, keď rozhodnutie o jej uložení nadobudlo právoplatnosť.

(4) Pokuty sú príjmom štátneho rozpočtu.

(5) Pokutu možno uložiť do troch rokov odo dňa porušenia povinnosti.

(6) Na konanie o ukladaní pokút sa vzťahuje všeobecný predpis o správnom konaní.[5h])“.

Poznámky pod čiarou k odkazom 5a až 5h znejú:

„[5a]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 211/2011 zo 16. februára 2011 o iniciatíveobčanov (Ú. v. EÚ L 65, 11. 3. 2011) v platnom znení.

[5b]) Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorýchzákonov v znení neskorších predpisov.

[5c]) Čl. 6 a príloha IV nariadenia (EÚ) č. 211/2011.

[5d]) Čl. 6 ods. 4 nariadenia (EÚ) č. 211/2011.

[5e]) Príloha IV nariadenia (EÚ) č. 211/2011.

[5f]) Čl. 8 a čl. 15 ods. 2 nariadenia (EÚ) č. 211/2011.

[5g]) Čl. 2 ods. 3 nariadenia (EÚ) č. 211/2011.

[5h]) Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.“.

2. V § 9 sa nad slovom „konaní“ doterajší odkaz „[7a])“ nahrádza odkazom „[5h])“ a na konci sa bodka nahrádza čiarkou a pripájajú sa tieto slová: „ak tento zákon neustanovuje inak.“.

   Poznámka pod čiarou k odkazu 7a sa vypúšťa.

3. Za § 9b sa vkladá § 9c, ktorý vrátane nadpisu znie:

„§ 9c

Prechodné ustanovenia k úpravám účinným od 1. mája 2019

(1) Osoba poverená Ministerstvom financií Slovenskej republiky na posudzovanie elektronického systému zberu vyhlásení o podpore iniciatívy občanov podľa predpisov účinných do 30. apríla 2019 je posudzovateľom systému zberu podľa tohto zákona. Konanie o poverenie osoby podľa prvej vety začaté podľa predpisov účinných do 30. apríla 2019 a právoplatne neukončené pred 1. májom 2019 dokončí Ministerstvo financií Slovenskej republiky podľa tohto zákona.

(2) Konanie o žiadosti o posúdenie elektronického systému zberu vyhlásení o podpore iniciatívy občanov začaté podľa predpisov účinných do 30. apríla 2019 a právoplatne neukončené pred 1. májom 2019 sa dokončí podľa tohto zákona.

(3) Osvedčenia o súlade elektronického systému zberu vyhlásení o podpore iniciatívy občanovs osobitným predpisom vydané podľa predpisov účinných do 30. apríla 2019 sú osvedčeniamio súlade elektronického systému zberu vyhlásení o podpore iniciatívy občanov s osobitným predpisom podľa tohto zákona.“.

4. Zákon sa dopĺňa prílohou, ktorá znie:

„Prílohak zákonu č. 85/1990 Zb.

VZOR

Žiadosť o posúdenie elektronického systému zberu vyhlásení o podpore iniciatívyobčanov

Dátum doručenia žiadosti o posúdenie systému zberu: (miesto pre úradný záznam Úraduvlády Slovenskej republiky)

Číslo evidencie žiadosti o posúdenie systému zberu:
Žiadosť o posúdenie elektronického systému zberu vyhlásení o podpore iniciatívy občanov

Časť yplní žiadateľ o posúdenie systému zberu

Označenie elektronického systému zberu vyhlásení o podpore iniciatívy občanov:
Žiadateľ o posúdenie systému zberu meno a priezvisko
Korešpondenčná adresa žiadateľa o posúdenie systému zberu(ulica, číslo SČ, mesto):
ontaktné údaje žiadateľa o posúdenie systému zberu (číslo tele nu číslo a u e-mailová adresa bankové spojenie
iesto umiestnenia elektronického systému zberu vyhlásení o podpore iniciatívy občanov:
ázov iniciatívy občanov:
Posudzovateľ systému zberu znalec alebo znalecký ústav
Označenie prílohy napríklad doklad o úhrade nákladov spojených s posudzovanímelektronického systému zberu vyhlásení o podpore iniciatívy občanov)

V ..... dňa .....

_____

Podpis žiadateľa o posúdenie systému zberu

* Označenie posudzovateľa systému zberu vybraného zo zoznamu posudzovateľov systému zberu obchodné meno ČO, pri fyzickej osobe meno a priezvisko), znalca (meno a priezvisko, evidenčné číslo alebo znaleckého ústavu názov obchodné meno evidenčné číslo vybraného zo zoznamu znalcov a znaleckých ústavov v príslušnom odbore a odvetví
Časť yplní posudzovateľ systému zberu znalec alebo znalecký ústav Dátum doručenia žiadosti o posúdenie systému zberu
Vyjadrenie posudzovateľa systému zberu znalca alebo znaleckého ústavu

lektronický systém zberu vyhlásení o podpore iniciatívy občanov sp ňa nesp ňa požiadavky podľa nariadenia ur pskeho parlamentu a ady Ú č zo ebruára o iniciatíve občanov
značenie prílohy

** Nehodiace sa prečiarknite.

V ..... dňa .....

_____

Odtlačok pečiatky (pri listinnej podobe žiadosti a podpis osoby oprávnenej konať za posudzovateľa systému zberu znalca alebo osoby oprávnenej konať za znalecký ústav “.

Čl. III

Zákon Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení zákona Národnej rady Slovenskej republiky č. 26/1993 Z. z., zákona Národnej rady Slovenskej republiky č. 159/1993 Z. z., zákona Národnej rady Slovenskej republiky č. 249/1994 Z. z., zákona Národnej rady Slovenskej republiky č. 374/1994 Z. z., zákona Národnej rady Slovenskej republiky č. 202/1995 Z. z., zákona Národnej rady Slovenskej republiky č. 118/1996 Z. z., zákonač. 348/1999 Z. z., zákona č. 149/2001 Z. z., zákona č. 602/2003 Z. z., zákona č. 747/2004 Z. z., zákona č. 519/2005 Z. z., zákona č. 659/2007 Z. z., zákona č. 492/2009 Z. z., zákonač. 403/2010 Z. z., zákona č. 373/2014 Z. z., zákona č. 91/2016 Z. z., zákona č. 125/2016 Z. z. a zákona č. 177/2018 Z. z. sa mení a dopĺňa takto:

1. V § 38 ods. 2 sa na konci pripája táto veta: „Národná banka Slovenska pri výbere, poverovaní a pri zadávaní zákaziek externým audítorom na overovanie účtovných závierok Národnej banky Slovenska uplatňuje osvedčené postupy vydané Európskou centrálnou bankou na výber a poverovanie externých audítorov pre centrálne banky Eurosystému podľa osobitného predpisu[8]) vrátane uplatňovania pravidiel o periodickej rotácii pri vykonávaní štatutárnych auditov tak, že ten istý štatutárny audítor, tá istá audítorská spoločnosť a tiež ten istý kľúčový audítorský partner môže bez rotácie vykonávať overovanie účtovných závierok Národnej banky Slovenska najviac za obdobie siedmich po sebe nasledujúcich rokov.“.

   Poznámka pod čiarou k odkazu 8 znie:

   „[8]) Čl. 27 ods. 27.1 Protokolu o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016).“.
2. Za § 44 sa vkladá § 44a, ktorý znie:

„§ 44a

Národná banka Slovenska je pre webové sídla a mobilné aplikácie vo svojej správe povinná zabezpečovať prístupnosť a funkčnosť webových sídiel a mobilných aplikácií, ako aj minimálne požiadavky na obsah webových sídiel najmenej na úrovni rovnocennej s úrovňou štandardov vydaných podľa osobitného predpisu.[10c])“.

Poznámka pod čiarou k odkazu 10c znie:

„[10c]) § 24 ods. 1 písm. b) a § 31 písm. k) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.“.

3. V § 45 ods. 2 sa slovo „dvoch“ nahrádza slovom „troch“.
4. Za § 49ae sa vkladá § 49af, ktorý vrátane nadpisu znie:

„§ 49af

Prechodné ustanovenia k úpravám účinným od 1. mája 2019

(1) Ak ide o webové sídlo Národnej banky Slovenska, ktoré bolo uverejnené pred 1. májom 2019, povinnosti pre prístupnosť, funkčnosť a minimálne požiadavky na obsah webového sídla podľa § 44a je Národná banka Slovenska povinná zabezpečiť najneskôr od 23. septembra 2020.

(2) Národná banka Slovenska je povinná zabezpečiť prístupnosť mobilných aplikácií podľa § 44a najneskôr od 23. júna 2021.“.

5. Za § 49b sa vkladá § 49c, ktorý znie:

„§ 49c

Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v prílohe.“.

6. Zákon sa dopĺňa prílohou, ktorá vrátane nadpisu znie:

„Príloha

k zákonu Národnej rady Slovenskej republiky č. 566/1992 Zb.

ZOZNAM PREBERANÝCH PRÁVNE ZÁVÄZNÝCH AKTOV EURÓPSKEJ ÚNIE

Smernica Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora (Ú. v. EÚ L 327, 2. 12. 2016).“.

Čl. IV

Zákon č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení zákona č. 209/2002 Z. z., zákona č. 401/2002 Z. z., zákona č. 442/2003 Z. z., zákona č. 465/2003 Z. z., zákona č. 528/2003 Z. z., zákona č. 365/2004 Z. z., zákona č. 455/2004 Z. z., zákona č. 523/2004 Z. z., zákona č. 578/2004 Z. z., zákona č. 5/2005 Z. z., zákona č. 332/2005Z. z., zákona č. 363/2007 Z. z., zákona č. 129/2008 Z. z., zákona č. 144/2008 Z. z., zákonač. 282/2008 Z. z., zákona č. 462/2008 Z. z., zákona č. 496/2009 Z. z., zákona č. 133/2010 Z. z., zákona č. 199/2010 Z. z., nálezu Ústavného súdu Slovenskej republiky č. 333/2010 Z. z., zákona č. 6/2011 Z. z., zákona č. 125/2011 Z. z., zákona č. 250/2011 Z. z., zákona č. 390/2011 Z. z., zákona č. 57/2012 Z. z., zákona č. 455/2012 Z. z., zákona č. 312/2013 Z. z., zákona č. 352/2013Z. z., zákona č. 436/2013 Z. z., zákona č. 464/2013 Z. z., zákona č. 281/2015 Z. z., zákonač. 422/2015 Z. z., zákona č. 270/2018 Z. z. a zákona č. 318/2018 Z. z. sa dopĺňa takto:

1. V § 20 sa odsek 1 dopĺňa písmenom j), ktoré znie:

„j) pre webové sídla a mobilné aplikácie vo svojej správe dodržiavať štandardy pre prístupnosťa funkčnosť webových sídiel a mobilných aplikácií, ako aj minimálne požiadavky na obsah webových sídiel vydané podľa osobitného predpisu.[20c])“.

Poznámka pod čiarou k odkazu 20c znie:

„[20c]) § 24 ods. 1 písm. b) a § 31 písm. k) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.“.

2. Za § 113ah sa vkladá § 113ai, ktorý vrátane nadpisu znie:

„§ 113ai

Prechodné ustanovenia k úpravám účinným od 1. mája 2019

(1) Ak ide o webové sídlo verejnej vysokej školy, ktoré bolo uverejnené pred 1. májom 2019, štandardy pre prístupnosť, funkčnosť a minimálne požiadavky na obsah webových sídiel podľa osobitného predpisu[20c]) je verejná vysoká škola povinná dodržiavať najneskôr od 23. septembra 2020.

(2) Verejná vysoká škola je povinná dodržiavať štandardy pre prístupnosť mobilných aplikácií podľa osobitného predpisu[20c]) najneskôr od 23. júna 2021.“.

3. Doterajší text prílohy č. 4 sa označuje ako prvý bod a dopĺňa sa druhým bodom, ktorý znie:

„2. Smernica Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora (Ú. v. EÚ L 327, 2. 12. 2016).“.

Čl. V

Účinnosť

Tento zákon nadobúda účinnosť 1. mája 2019.

Andrej Kiska v. r.
Andrej Danko v. r.
Peter Pellegrini v. r.

Príloha
k zákonu č. 95/2019 Z. z.

ZOZNAM PREBERANÝCH PRÁVNE ZÁVÄZNÝCH AKTOV EURÓPSKEJ ÚNIE

Smernica Európskeho parlamentu a Rady (EÚ) 2016/2102 z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora (Ú. v. EÚ L 327, 2. 12. 2016).

1) Napríklad zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov.
1a) Napríklad zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 541/2004 Z. z. v znení neskorších predpisov, zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.
~~1) § 2 písm. a) zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.~~
1b) § 2 písm. a) zákona č. 215/2004 Z. z.
2) Napríklad § 3 ods. 16 a 17 zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení zákona č. 96/2017 Z. z., § 2 písm. k) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.
2a) § 3 písm. m~~l~~) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 2~~7~~87/2021 Z. z.
2b) § 3 písm. o~~n~~) zákona č. 69/2018 Z. z. v znení zákona č. 2~~7~~87/2021 Z. z.
3) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
4) Napríklad § 20 ods. 1 písm. j) zákona č. 131/2002 Z. z. o vysokých školách a o zmenea doplnení niektorých zákonov v znení zákona č. 95/2019 Z. z., § 44a zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení zákona č. 95/2019 Z. z.
4a) Zákon č. 532/2010 Z. z. o Rozhlase a televízii Slovenska a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
5) § 10 zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej mocia o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.
6) § 6 zákona č. 305/2013 Z. z. v znení neskorších predpisov.
6a) § 1 ods. 10 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení zákona č. 395/2021 Z. z.
~~6aa) § 3 písm. j) zákona č. 69/2018 Z. z. v znení zákona č. 278/2021 Z. z.~~
7) Zákon č. 60/2018 Z. z. o technickej normalizácii.
9) Druhá časť zákona Národnej rady Slovenskej republiky č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.
10) Zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorýchzákonov v znení zákona č. 177/2018 Z. z.
11) § 20 ods. 2 zákona č. 69/2018 Z. z.
11a) § 6 ods. 3 zákona č. 305/2013 Z. z. v znení neskorších predpisov.~~zákona č. 211/2019 Z. z.~~
12) Zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov.
13) Napríklad zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, zákon č. 272/2015 Z. z. o registri právnických osôb, podnikateľov a orgánov verejnej moci a o zmenea doplnení niektorých zákonov v znení zákona č. 52/2018 Z. z.
14) § 17 ods. 5 až 7 zákona č. 305/2013 Z. z. v znení zákona č. 238/2017 Z. z.
15) Napríklad § 55 zákona č. 305/2013 Z. z. v znení zákona č. 273/2015 Z. z., § 1 zákonač. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii).
16) Napríklad § 6 ods. 3 písm. b) zákona č. 305/2013 Z. z., § 14 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
17) § 6 ods. 3 písm. a) zákona č. 305/2013 Z. z.
18) Vykonávacie rozhodnutie Komisie (EÚ) 2017/863 z 18. mája 2017, ktorým sa aktualizuje verejná open source softvérová licencia Európskej únie (EUPL) v záujme ďalšej podpory zdieľania a opätovného používania softvéru vyvinutého verejnými správami (Ú. v. EÚ L 128, 19. 5. 2017).

19) § 8 až 13 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.
19a) § 11 zákona č. 69/2018 Z. z.
20) § 3 písm. m) zákona č. 69/2018 Z. z.

21) Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
22) § 20 zákona č. 69/2018 Z. z.
22a) Čl. 9 ods. 1 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4. 5. 2016) v platnom znení.
22b) Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
23) § 20 ods. 3 písm. k) zákona č. 69/2018 Z. z.
24) ~~§ 17 ods. 3 zákona č. 69/2018 Z. z.~~§ 3 písm. k) zákona č. 69/2018 Z. z. v znení zákona č. 2~~7~~87/2021 Z. z.
25) § 24 ods. 4 zákona č. 69/2018 Z. z.
26) Príloha č. 1 k zákonu č. 69/2018 Z. z. v znení ~~zákona č. 278/2021 Z. z.~~ neskorších predpisov ~~§ 3 ods. j) zákona č. 69/2018 Z. z.~~
26a) § 3 písm. i) zákona č. 69/2018 Z. z. v znení zákona č. 287/2021 Z. z
~~27) § 24 ods. 1 zákona č. 69/2018 Z. z.~~
~~28) § 3 písm. h) zákona č. 69/2018 Z. z.~~
~~29) § 3 písm. i) zákona č. 69/2018 Z. z.~~
~~30) § 3 písm. g) zákona č. 69/2018 Z. z.~~
~~26a) § 3 písm. h) zákona č. 69/2018 Z. z. v znení zákona č. 278/2021 Z. z.~~
~~26b) § 15 zákona č. 69/2018 Z. z.~~
~~26c) Napríklad zákon č. 69/2018 Z. z. v znení neskorších predpisov.~~
~~26d) Napríklad čl. 37 ods. 1 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky (Ú. v. EÚ C 202, 7. 6. 2016) v platnom znení, § 17 až 20 Obchodného zákonníka, § 39 zákona Slovenskej národnej rady č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, § 23 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z., § 20 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení neskorších predpisov, zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 23 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení neskorších predpisov, zákon č. 215/2004 Z. z. v znení neskorších predpisov, § 24 a 25 zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 11 zákona č. 563/2009 Z. z. v znení neskorších predpisov, zákon č. 45/2011 Z. z. v znení neskorších predpisov, § 10 zákona č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláška č. 362/2018 Z. z.~~
30a) Čl. 28 nariadenia (EÚ) 2016/679.
30b) § 3 písm. a) zákona č. 452/2021 Z. z. o elektronických komunikáciách.
30c) § 2 ods. 3 zákona č. 452/2021 Z. z..
30d) § 2 ods. 22 zákona č. 452/2021 Z. z..
30e) § 11 zákona č. 69/2018 Z. z. v znení zákona č. 134/2020 Z. z~~.~~
31) Napríklad zákon č. 330/2007 Z. z. o registri trestov a o zmene a doplnení niektorých zákonovv znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 162/1995
Z. z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny

zákon) v znení neskorších predpisov.
32) § 23 ods. 1 zákona č. 305/2013 Z. z. v znení zákona č. 273/2015 Z. z.
33) Čl. 3 ods. 34 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28. 8. 2014).
34) Napríklad zákon č. 599/2001 Z. z. o osvedčovaní listín a podpisov na listinách okresnými úradmi a obcami v znení neskorších predpisov, zákon č. 151/2010 Z. z. o zahraničnej službea o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
35) § 35 ods. 2 zákona č. 305/2013 Z. z. v znení zákona č. 273/2015 Z. z.
36) § 9a zákona č. 305/2013 Z. z. v znení zákona č. 273/2015 Z. z.
36a) Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov
37) § 1 ods. 1 zákona Národnej rady Slovenskej republiky č. 278/1993 Z. z. o správe majetkuštátu v znení neskorších predpisov.
38) § 1 ods. 2 písm. b) zákona Národnej rady Slovenskej republiky č. 278/1993 Z. z. v znení neskorších predpisov.
39) § 8 zákona č. 69/2018 Z. z.