55

V Ý N O S

Ministerstva financií Slovenskej republiky

zo 4. marca 2014,

o štandardoch pre informačné systémy verejnej správy

[konsolidovaný s novelou č. 276/2014 Z. z.]

Ministerstvo financií Slovenskej republiky (ďalej len „ministerstvo“) podľa § 13 ods. 1 písm. a) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) ustanovuje:

Čl. I

Základné ustanovenia

§1
Štandardy pre informačné systémy verejnej správy

Týmto výnosom sa ustanovujú štandardy pre informačné systémy verejnej správy, ktorými sú

a) technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky, a to
   1. štandardy pre prepojenie,
   2. štandardy pre prístup k elektronickým službám,
   3. štandardy pre webové služby,
   4. štandardy pre integráciu dát,
b) štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona,
c) štandardy použitia súborov, vzťahujúce sa na formáty výmeny údajov,
d) štandardy názvoslovia elektronických služieb, vzťahujúce sa na sieťovú infraštruktúru,
e) bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje, a to
   1. štandardy pre architektúru riadenia,
   2. štandardy minimálneho technického zabezpečenia,
f) dátové štandardy, vzťahujúce sa na údaje, registre a číselníky,
g) štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona,
h) štandardy projektového riadenia, vzťahujúce sa na postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy,
i) štandardy poskytovania údajov v elektronickom prostredí, vzťahujúce sa na databázové prostredie, spoločné moduly, aplikačné programové vybavenie, údaje, registre, číselníky a formáty výmeny údajov,

j) štandardy poskytovania cloud computingu a využívania cloudových služieb, vzťahujúce sa na technické prostriedky a programové prostriedky,.

k) štandardy pre formáty elektronických dokumentov podpísateľných elektronickým podpisom,

l) štandardy pre základné číselníky.

§2
Vymedzenie základných pojmov

Na účely tohto výnosu sa rozumie

a) správcom obsahu povinná osoba zodpovedná za správu obsahu webového sídla a na ňom zverejnené informácie; správca obsahu je zároveň správcom daného informačného systému verejnej správy,

b) technickým prevádzkovateľom prevádzkovateľ informačného systému verejnej správy podľa zákona, ktorý vykonáva činnosti určené správcom obsahu v súvislosti s technickou prevádzkou webového sídla,

c) aktívami programové vybavenie, technické zariadenia, poskytované služby, kvalifikované osoby, dobré meno povinnej osoby a informácie, dokumentácia, zmluvy a iné skutočnosti, ktoré považuje povinná osoba za citlivé,

d) bezpečnostným incidentom akýkoľvek spôsob narušenia bezpečnosti informačných systémov verejnej správy, ako aj akékoľvek porušenie bezpečnostnej politiky povinnej osoby a pravidiel súvisiacich s bezpečnosťou informačných systémov verejnej správy,

e) technickými komponentmi informačného systému verejnej správy tie časti informačného systému verejnej správy a informačno-komunikačné technológie, ktoré nie sú určené na uchovávanie údajov, napríklad štruktúrovaná kabeláž, sieťové karty a zdroje,

f) zariadeniami informačného systému verejnej správy tie časti informačného systému verejnej správy, ktoré môžu uchovávať údaje, napríklad pamäťové médiá a počítače vrátane prenosných počítačov,

g) súborom postupnosť údajov v elektronickej forme, ktorá je označená názvom, informáciou o kapacite údajov a časovou značkou o jej poslednej zmene,

h) dátovým prvkom jednotka údajov, ktorá je jednoznačne a nedeliteľne špecifikovaná prostredníctvom súboru atribútov,

i) gestorom povinná osoba zodpovedná za správnosť a aktuálnosť atribútov dátového prvku; gestor nezodpovedá za obsah prenášaný dátovým prvkom,

j) používateľom služby osoba alebo informačný systém, ktorí používajú alebo požadujú poskytovanie služby verejnej správy,

k) gestorom služby osoba poverená vykonávať riadenie a koordinovanie určitého úseku verejnej správy,

l) projektom jednorazový proces zameraný na dosiahnutie definovaného cieľa, pozostávajúci zo súboru zosúladených, riadených a časovo ohraničených činností, ktorý

1. je pre danú organizáciu jedinečný, pričom to nie je pravidelná činnosť,
2. má presne určený začiatok a koniec trvania,
3. má definované najmenej finančné zdroje a ľudské zdroje, ak sú potrebné,

4. vyžaduje analýzu súčasného stavu, špecifikáciu cieľového stavu a spôsobu jeho dosiahnutia,

m) malým projektom projekt, ktorého celková cena je najviac 69 999 eur a zmluvná lehota jeho trvania nie je dlhšia ako 180 kalendárnych dní,

n) veľkým projektom projekt, ktorého celková cena je 1 000 000 eur alebo vyššia alebo zmluvná lehota jeho trvania je dlhšia ako 544 kalendárnych dní,

o) stredným projektom projekt, ktorý nespĺňa podmienky podľa písmen m) a n),

p) informačno-technologickým projektom projekt, ktorý súvisí so zavádzaním, správou alebo podporou informačno-komunikačných technológií a týka sa tvorby a úpravy informačných systémov verejnej správy,

q) programom skupina projektov riadených koordinovaným spôsobom za účelom dosiahnutia spoločného cieľa a zvýšených prínosov a umožnenia efektívnej kontroly projektov a efektívneho riadenia projektov, čo nie je možné dosiahnuť, ak by sa projekty riadili samostatne,

r) datasetom ucelená a samostatne použiteľná skupina súvisiacich údajov vytvorených a udržiavaných na určitý účel a uložených sapoločne podľa rovnakej schémy,

s) dátovým zdrojom pôvodné miesto evidencie datasetu,

t) referencovateľným identifikátorom identifikátor, ktorý

1. má formát Uniform~~ied~~ Resource Identifier (URI),
2. je jednoznačný,
3. je unikátny,
4. je dlhodobo stabilný,
5. je formátovo a štrukturálne konzistentný,
6. je manažovateľný tak, aby umožňoval logicky rozširovať stanovenú štruktúru,
7. je jasný, stručný a krátky,
8. je pre fyzickú osobu jednoducho čitateľný,
9. je bez súborových prípon,
10. neobsahuje programátorské kľúčové slová,
11. neobsahuje reťazec „www“,
12. neobsahuje interpunkciu okrem znakov lomka, pomlčka a bodka, diakritiku a medzery okrem identifikátora fyzickej osoby podľa osobitného predpisu,[1)] kde je možné použiť interpunkciu a diakritiku,

~~12.~~13. obsahuje iba malé písmená,

~~13.~~14. nahrádza špeciálne znaky, napríklad výkričník, úvodzovky, percento, hviezdička, zátvorka, dolár alebo mriežka, pomlčkami a podčiarkovníkmi,

u) tripletom znalosť vo forme „subjekt predikát objekt“,

v) identifikátormi prepojenými údajmi koncepčný model, pri ktorom triplety pozostávajú z referencovateľných identifikátorov automatizovane spracovateľných tak, že technické zariadenie, ktoré ich spracováva, porozumie ich významu,

w) metaúdajmi štruktúrované údaje obsahujúce informácie o primárnych údajoch, pričom primárne údaje spravidla reprezentujú určitý hmotný objekt alebo nehmotný objekt;

[1)] § 3 písm. j) zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).

metaúdaje sú určené najmä na vyhľadávanie, katalogizáciu a využívanie primárnych údajov,

x) cloud computingom model umožňujúci jednoduchý samoobslužný sieťový prístup k službám informačných technológií na vyžiadanie, poskytovaným vo virtuálnom prostredí konfigurovateľných výpočtových zdrojov, ktoré môžu byť pridelené alebo uvoľnené s minimálnym úsilím a časovým obmedzením, a to na základe voliteľného škálovania a navyšovania, nezávisle od lokality zdrojov alebo lokality prístupu k nim a bez osobného kontaktu s poskytovateľom cloudovej služby, pričom využitie týchto služieb je merané a hodnotené podľa ich skutočného využitia,

y) cloudovou službou ľubovoľný prostriedok alebo zdroj cloud computingu, poskytovaný vzdialeným prístupom na základe podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb,

z) dohodou o poskytovanej úrovni cloudových služieb zmluvný vzťah upravujúci parametre a kvalitu poskytovaných cloudových služieb, ktorá obsahuje úlohy a povinnosti zmluvných strán, pričom táto dohoda sa obvykle uzatvára medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb alebo sprostredkovateľom cloudových služieb,

aa) odberateľom cloudových služieb osoba, ktorá na základe dohody o poskytovanej úrovni cloudových služieb využíva cloudové služby poskytovateľa cloudových služieb,

ab) poskytovateľom cloudových služieb osoba zodpovedná za správu cloud computingu a poskytovanie cloudových služieb, a to podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb,

ac) prevádzkovateľom cloudových služieb osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb zabezpečuje technické podmienky na prevádzkovanie, prepojenie a prenos cloudových služieb,

ad) sprostredkovateľom cloudových služieb osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb prevádzkuje využívanie, výkon a dodávku cloudových služieb,

ae) audítorom cloudu osoba nezávislá od poskytovateľa cloudových služieb, určujúca na základe~~, ktorá má~~ poverenia~~e~~ od tohto poskytovateľa ~~určovať~~ kritéria auditu slúžiace na objektívne získavanie dôkazov o dodržiavaní podmienok poskytovania cloudových služieb a vykonávajúca na základe poverenia od tohto poskytovateľa~~vykonávať~~ systematický, nezávislý a zdokumentovaný proces ich vyhodnocovania,

~~ae)~~af) identifikačnou registráciou osoby proces, počas ktorého je osoba identifikovaná na základe určitých registračných údajov, z ktorých určené registračné údaje môžu byť potvrdzované, pričom výsledkom registrácie je priradenie určitej identity v určenom kontexte tejto osobe,

~~af)~~ag) registračnou autoritou identifikácie poskytovateľ identifikačnej registrácie,

ah) federáciou identít overovanie identít informačných systémov verejnej správy v správe najmenej dvoch povinných osôb, ktoré sa vykonáva u jedného poskytovateľa identít.

ai) priamo podpísaným elektronickým dokumentom podpísaný elektronický dokument, ku ktorému sú elektronický podpis alebo elektronická pečať, ktorými sa podpisuje, pripojené ako jeho súčasť,

aj) externe podpísaným elektronickým dokumentom podpísaný elektronický dokument, ku ktorému sú elektronický podpis alebo elektronická pečať, ktorými sa podpisuje, pripojené prostredníctvom podpisového kontajneru,

ak) kontajnerom pre podpísané XML údaje štruktúra vo formáte Extensible Markup Language (XML) slúžiaca na prenos podpísaných údajov v tomto formáte vrátane podpísaných vyplnených údajov elektronického formulára v tomto formáte a opis ich sémantického významu prostredníctvom pripojenej

1. definície dátovej štruktúry podpísaných údajov podľa prílohy č. 3 bodu 2.3.5 a
2. prezentačnej schémy s transformačným jazykom podľa prílohy č. 3 bodu 2.6.7 použitej na zobrazenie obsahu podpísaných údajov,

al) číselníkom množina údajov vo forme jednotlivých položiek číselníka, ktoré sú popísané najmenej dvojicou dátových prvkov „kód položky“ a „názov položky“; „kódom položky“ je textový reťazec, ktorý je v číselníku jedinečný,

~~ag)~~ai) am) základným číselníkom číselník vedený centrálne prostredníctvom informačného systému verejnej správy, slúžiaci na určenie prípustných hodnôt príslušných dátových prvkov.

Technické štandardy

Štandardy pre prepojenie

§ 3
Sieťové protokoly

Štandardom pre sieťové protokoly je

a) pre informačné systémy verejnej správy a ich komponenty, ktoré boli zavedené po 1. septembri 2009, používanie sieťového protokolu Internet Protocol vo verzii 6 (IP v6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),

b) pre informačné systémy verejnej správy a ich komponenty, ktoré boli zavedené pred 1. septembrom 2009 podpora sieťového protokolu Internet Protocol vo verzii 4 (IP v4) s podporou sieťovej technológie Dual stack spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP) pre informačné systémy verejnej správy alebo sieťového protokolu Internet Protocol vo verzii 6 (IP v6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),

c) používanie skupiny protokolov Internet Procotol Security (IPSEC) na zabezpečenie sieťových protokolov.

§ 4
Prenos dát

(1) Štandardom pre prenos dát je

a) používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext Transfer Protocol (HTTP),

b) podpora chráneného prenosu dát cez kryptografický protokol Secure Sockets Layer (SSL) minimálne vo verzii 3.0 alebo Transport Layer Security (TLS).

(2) Na prenos dát elektronickou poštou sa primerane vzťahuje § 6.

§ 5
Špecifikácie pre prepojenie pomocou sieťových služieb

Štandardom pre špecifikácie pre prepojenie pomocou sieťových služieb je používanie Domain Name Services (DNS) ako hierarchickej služby name servera v centrálnych bodoch internetu.

§ 6
Prenos elektronickej pošty

Štandardom pre prenos elektronickej pošty je

a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronických poštových správ,

b) podpora chráneného prenosu dát cez kryptografický protokol Secure Sockets Layer (SSL) minimálne vo verzii 3.0 alebo Transport Layer Security (TLS) na zabezpečenie prenosu elektronických poštových správ.

§ 7
Prístup k elektronickej poštovej schránke

Štandardom pre prístup k elektronickej poštovej schránke je

a) používanie protokolu Post Office Protocol vo verzii 3 (POP3) alebo protokolu Internet Message Access Protocol v revidovanej verzii 4.1 (IMAP4rev1) pre prístup k verejným elektronickým poštovým službám,

b) podpora kryptografického protokolu Secure Sockets Layer (SSL) minimálne vo verzii 3.0 alebo Transport Layer Security (TLS) pri chránenom prístupe k verejným elektronickým poštovým službám.

§ 8
Formát elektronických poštových správ

Štandardom pre formát elektronických poštových správ je

a) používanie formátu Multipurpose Internet Mail Extensions (MIME) pri prenose elektronických poštových správ,

b) používanie formátu Secure/Multipurpose Internet Mail Extensions (S/MIME) pri chránenom prenose elektronických poštových správ.

Štandardy pre prístup k elektronickým službám

§ 9
Aplikačné protokoly elektronických služieb

Štandardom pre aplikačné protokoly elektronických služieb je

a) používanie protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 s prenosom dát vo formáte Extensible HyperText Markup Language (XHTML) vo verzii 1.0 na komunikáciu medzi klientom a webovým serverom,
b) podpora protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 a Hypertext Transfer Protocol (HTTP) vo verzii 1.0 pri webových serveroch,
c) používanie mechanizmu Hypertext Transfer Protocol State Management Mechanism (HTTP Management Mechanism) na Hypertext Transfer Protocol Session Management (HTTP Session Management) a cookies,
d) používanie protokolu Hypertext Transfer Protocol over Secure Sockets Layer (HTTPs) alebo Transport Layer Security (TLS) pri chránenom prenose dát medzi klientom a webovým serverom a medzi webovými servermi.

§ 10
Adresárové služby

Štandardom pre adresárové služby je

a) používanie aplikačného protokolu Lightweighted Directory Access Protocol vo verzii 3 (LDAP v3) na verejný prístup k adresárovým službám,
b) používanie jazyka Directory Services Markup Language v2 (DSML v2),
c) podpora kryptografického protokolu Secure Sockets Layer (SSL) alebo Transport Layer Security (TLS) pri chránenom verejnom prístupe k adresárovým službám.

Štandardy pre webové služby

§ 11
Middleware protokoly sieťovej komunikácie

Štandardom pre middleware protokoly sieťovej komunikácie je používanie

a) protokolu Simple Object Access Protocol (SOAP) minimálne vo verzii 1.2 pri komunikácii medzi servermi v rámci jednej správy a komunikácii medzi klientom a serverom; pri otvorených údajoch je možné použiť aj protokol Representational State Transfer (REST),
b) webových služieb na prístup klientských aplikácií prostredníctvom internetu na serverové aplikácie správy,
c) protokolu Hypertext Transfer Protocol (HTTP) na poskytnutie vrstvy webovej služby pre existujúcu serverovú aplikáciu a komunikáciu na aplikačnej úrovni,
d) jazyka Web Services Description Language (WSDL) na definíciu webovej služby,
e) registra Universal Description, Discovery and Integration (UDDI) minimálne vo verzii 1.0 na komunikáciu medzi klientom a serverom,
f) špecifikácií pre mapové služby pod
   1. OpenGIS WebMap Service (WMS),
   2. OpenGIS Web Feature Service (WFS),
   3. OpenGIS Web Coverage Service (WCS),
   4. OpenGIS Web Processing Service (WPS),
   5. OpenGIS Catalog Service for Web (CSW).

g) schémy správ Sk-Talk minimálne vo verzii 2.0 pre asynchrónnu komunikáciu s ústredným portálom verejnej správy podľa aktuálne platnej technickej špecifikácie zverejnenej na ústrednom portáli verejnej správy.

Štandardy pre integráciu dát

§ 12
Popisný jazyk pre dátové prvky

Štandardom pre popisný jazyk pre dátové prvky je používanie jazyka Extensible Markup Language (XML) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pre dátové prvky pri vstupe na rozhranie informačného systému verejnej správy.

§ 13
Prenos dátových prvkov

Štandardom pre prenos dátových prvkov je používanie

a) jazyka schém XML Schema Definition (.xsd) minimálne vo verzii 1.0 podľa World Wide Web Consortium (W3C) na výmenu dátových prvkov medzi všetkými informačnými systémami verejnej správy nezávisle od účelu správy alebo jazyka Web Ontology Language (OWL), ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov,jazyka Extensible Markup Language (.xml) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pri výmene dátových prvkov, pričom ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov, je možné namiesto Extensible Markup Language použiť dátový model Resource Description Framework (RDF); pri otvorených údajoch je možné použiť aj formát CSV podľa § 23 písm. e) alebo formát JavaScript Object Notation (JSON),
b) jazyka Extensible Markup Language (.xml) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pri výmene dátových prvkov, pričom ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov, je možné namiesto Extensible Markup Language použiť dátový model Resource Description Framework (RDF); pri otvorených údajoch je možné použiť aj formát CSV podľa § 23 písm. e) alebo formát JavaScript Object Notation (JSON),
c) znakovej sady Unicode Character Set (UCS) podľa technickej normy[2)] v 8 bitovom kódovaní UTF-8,
d) transformačného jazyka XSL Transformations (XSLT) podľa World Wide Web Consortium (W3C) pri transformácii dátových prvkov,
e) modelovacieho jazyka Geography Markup Language (GML) pri výmene priestorových dátových prvkov.

Štandardy prístupnosti a funkčnosti webových stránok

§ 14
Prístupnosť webových stránok

Štandardom pre prístupnosť webových stránok je dodržiavanie pravidiel podľa prílohy č. 1 bodov 1.1, 1.3, 1.4, 1.6, 2.1, 2.2, 3.1, 3.4, 3.5, 3.6, 4.3, 5.1, 5.2, 5.4, 6.1, 6.2, 7.1, 7.3, 7.4,

[2)] ISO/IEC 10646:2012 Univerzálny kódovaný súbor znakov (UCS).

8.2, 8.3, 9.4, 10.1, 11.4, 12.1, 12.4, 12.5, 13.1, 13.3, 13.6, 13.11 písm. a), 13.14, 13.15, 14.1, 14.4, a ak je funkčnosť dôležitá a zároveň nie je prezentovaná ako prístupné riešenie aj na nejakom inom mieste aj dodržiavanie bodu 8.1.

§ 15
Obsah webového sídla

Štandardom pre obsah webového sídla je

a) uvedenie vyhlásenia o splnení pravidiel prístupnosti webového sídla alebo jeho časti podľa prílohy č. 1; nesplnenie konkrétnych bodov alebo pravidiel sa jednoznačne uvedie vo vyhlásení,
b) identifikácia správcu obsahu a technického prevádzkovateľa,
c) zverejnenie kontaktných informácií správcu obsahu a technického prevádzkovateľa dostupných zo všetkých stránok webového sídla, najmenej však dostupných alebo priamo uvedených na úvodnej webovej stránke,
d) uvedenie informácií, týkajúcich sa kompetencií a poskytovaných služieb správcu obsahu, ktoré vyplývajú z osobitných predpisov, a to na jednej webovej stránke webového sídla,
e) zverejnenie úradných hodín správcu obsahu, ak poskytuje služby verejnosti na vyhradených pracoviskách,
f) poskytnutie obsahu webového sídla v anglickom jazyku, a to najmenej v rozsahu informácií uvedených v písmenách b) až e) a v prílohe č. 1 bode 14.4,
g) nekombinovanie anglického obsahu a slovenského obsahu v anglickej verzii webového sídla, a to vrátane navigačných odkazov,
h) zverejnenie najmenej jedného verejného kľúča pre chránený prenos elektronických poštových správ, ak povinná osoba takýto prenos poskytuje; verejný kľúč pre chránený prenos elektronických poštových správ sa zverejňuje spolu s kontaktnými informáciami správcu obsahu podľa písmena c),
i) zverejnenie kontaktnej informácie, na ktorej je možné získať kontrolný reťazec znakov pre overenie pravosti certifikátov a verejných kľúčov používaných povinnou osobou pre elektronické služby verejnej správy a elektronické poštové správy,
j) uvedenie dátumu vytvorenia webovej stránky a dátumu jej poslednej aktualizácie na webovej stránke, ktorá obsahuje otvorené údaje podľa § 52 alebo povinne zverejňované informácie podľa osobitných predpisov.[3)]

§ 16
Komponenty a funkcionality webových sídiel

Štandardom pre komponenty a funkcionality webových sídiel je

a) poskytnutie Really Simple Syndication (RSS) kanála, ak je obsah webového sídla aktualizovaný častejšie ako jeden krát za týždeň,
b) poskytnutie vyhľadávania kľúčových výrazov, ak webové sídlo obsahuje kumulatívne viac ako 100 publikovaných informačných webových stránok,
c) optimalizácia webových stránok, ktoré obsahujú elektronické služby verejnej správy alebo povinne zverejňované informácie podľa osobitných predpisov[3)], pre aktuálne podporované

[3)] Napríklad § 5 až 5b 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.

verzie webových prehliadačov s podielom zastúpenia na trhu v Slovenskej republike viac ako 5% (ďalej len „podporovaná verzia webového prehliadača”), a to

1. používaním iba takých programovacích prvkov v kóde webových stránok, ktoré sú korektne interpretované vo všetkých podporovaných verziách webových prehliadačov alebo
2. aktívnym rozoznávaním typu prehliadača webovými stránkami, pomocou ktorého sú tieto webové stránky zobrazované, a na základe toho upravovaním ich vzhľadu a správania sa s cieľom dosiahnuť rovnakú použiteľnosť vo všetkých podporovaných verziách webových prehliadačov.

§17
Vizuálne rozloženie webových stránok

Štandardom pre vizuálne rozloženie webových stránok je

a) umiestnenie navigačného odkazu „kontakt“ alebo jeho ekvivalentu na začiatku alebo na konci hlavného navigačného menu, ak je navigačný odkaz jeho súčasťou,
b) jednoznačné odlíšenie navigačného odkazu „kontakt“ alebo jeho ekvivalentu od ostatného obsahu, ak nie je súčasťou hlavného navigačného menu,
c) jednoznačné odlíšenie kontaktných informácií od ostatného obsahu, ak sú priamo uvedené na úvodnej webovej stránke,
d) umiestnenie kontaktných informácií správcu obsahu a technického prevádzkovateľa alebo odkazu na kontaktné informácie aj osobitne v spodnej časti webovej stránky.

Štandardy použitia súborov

§ 18
Všeobecné použitie formátov

Štandardom pre všeobecné použitie formátov je

a) používanie ľubovoľného formátu pri výmene súborov vrátane ľubovoľných obmedzujúcich podmienok, ak vopred súhlasia všetky zúčastnené strany a technické podmienky to umožňujú,
b) používanie ľubovoľného formátu pri výmene a zverejňovaní iných typov súborov ako sú uvedené v § 19 až 25,
c) používanie najmä písiem Arial, Times New Roman a Courier New v textových súboroch, tabuľkových súboroch a ďalších typoch ~~v~~ súboroch~~,~~, kde je to technicky uskutočniteľné, a to pri zverejňovaní súborov, vrátane zverejňovania na webovom sídle, a ak je použitie fontov potrebné pre zobrazenie obsahu súborov,
d) spracovanie a rozoznávanie textových častí obsahu ľubovoľného formátu súboru v tlačených fontoch ako textu, ak je to technicky uskutočniteľné, a to najmä formátu textového súboru Portable Document Format (.pdf) minimálne vo verzii 1.3 a maximálne vo verzii 1.5, pričom
   1. takýto súbor nie je iba skenovaným obrázkom,
   2. sa v súbore správne špecifikuje použitý jazyk,
   3. obmedzenia používania súboru neobmedzujú funkčnosť asistenčných technológií pre prístupnosť,
   4. štruktúra súboru je prístupná a zrozumiteľná aj pri lineárnom usporiadaní,

5. sa správne používajú štýly pre vyjadrenie sémantickej štruktúry obsahu súboru,
6. pre netextové časti súboru sa poskytujú alternatívne textové opisy,
7. súbor v tomto formáte sa podľa možnosti správne označkuje a doplní navigačnými prvkami,

e) podpora vysporiadania autorských a licenčných práv podľa osobitných predpisov[4)] na ich ďalšie použitie, ak sa používajú fonty,

f) používanie správnych prípon súborov patriacich danému typu súboru.

~~f)~~g) spracovanie obsahu ľubovoľného formátu textového súboru alebo grafického súboru podľa prílohy č. 1 pravidla 2 obdobne ako pri webových stránkach.

§ 19
Textové súbory

Štandardom pre textové súbory je

a) pri úkonoch súvisiacich s poskytovaním elektronických služieb verejnej správy alebo povinným poskytovaním informácií podľa osobitných predpisov[3)] prijímanie a čítanie všetkých doručených formátov textových súborov, ktorými sú

1. Hypertext Markup Language (.html, .htm) alebo Extensible Hypertext Markup Language (.xhtml) podľa World Wide Web Consortium (W3C),
2. Portable Document Format (.pdf) minimálne vo verzii 1.3 a maximálne vo verzii ~~1.5~~1.7,
   2a. neobsahujú animácie, audio alebo video záznamy,
   2b. neobsahujú dynamický obsah a aplikácie, najmä technológie XML Forms Architecture, Adobe JavaScript a 3D náhľady, môžu však obsahovať PDF AcroForms podľa prílohy č. 3 bodov 1.1.6 a 2.6.10 a
   2c. neobsahujú kryptograficky chránený obsah, napríklad na základe Digital Rights Management (DRM) alebo osobitného spôsobu šifrovania,
3. ~~2.~~Plain Text Format (.txt) v kódovaní UTF-8 podľa technických noriem[4a)],

b) prijímanie a čítanie ~~doručených~~ formátov textových súborov ~~na iné účely ako~~ podľa písmena a) a ďalších formátov na základe vlastného uváženia doručených, a to napríklad formátov textových súborov, ktorými sú

1. Open Document Format (.odt) maximálne vo verzii 1.2 podľa Organizácie na presadzovanie noriem pre štruktúrované informácie (OASIS),
2. Office Open XML (.docx) vo verzii podľa technickej normy,[5)]

c) používanie najmenej jedného z formátov textových súborov uvedených v písmene a) pri ich odosielaní alebo zverejňovaní[6)] vrátane ich zverejňovania na webovom sídle, ak sa nevyžaduje ďalšia úprava textového súboru, najmä formátu uvedeného v písmene a) druhom bode, ak je súčasťou textového súboru grafika,

Formátované: Zarážka: Vľavo: 1,25 cm, Opakovaná zarážka: 0,75 cm, Nezväzovať s nasledujúcim, Zarážky: 2 cm, Tabulátor pre zoznam + Nie je v 2,54 cm

---

[4)] Napríklad zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov.

[4a)] RFC 2046: Formát Multipurpose Internet Mail Extensions (MIME). Časť 2: Typy médií, RFC 3629:UTF-8 transformácia UCS (univerzálnej znakovej sady), ISO/IEC 10646 - Informačné technológie. Univerzálna znaková sada (UCS).

[5)] ISO/IEC 29500:2012 Formáty súborov Office Open XML.

[6)] § 4 ods. 3 zákona č. 211/2000 Z. z.

d) používanie formátu textových súborov uvedeného v písmene a) treťom bode alebo súčasné používanie formátov textových súborov uvedených v písmene b) s rovnakým obsahom, v rovnakej štruktúre a s použitím iba funkčností podľa písmena h) pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle, ak sa vyžaduje ďalšia úprava textového súboru,

e) používanie iného formátu textových súborov ako je uvedené v písmenách a) a b) pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle, ak je súčasne odoslaný alebo na rovnakom mieste alebo webovej stránke zverejnený rovnaký obsah v rovnakej štruktúre najmenej v jednom z formátov textových súborov uvedených v písmene a) alebo v písmene b),

f) poskytovanie formátov textových súborov uvedených v písmene b) na účely uvedené v písmene e) iba súčasne,

g) obmedzenie funkčností pri používaní formátov textových súborov podľa písmena b) na

1. štýly strany, odseku a znakov,
2. hlavičku a pätu strany,
3. číslovanie strán a odrážkové a číslované zoznamy,
4. vkladanie rastrovej grafiky,
5. vkladanie textových tabuliek, ktoré nie sú objektmi,
6. vkladanie poznámok pod čiarou a poznámok na konci textu; v texte sa nevkladajú komentáre a nepoužíva sa sledovanie zmien,

h) nevytváranie formátov textových súborov podľa písmena b) druhého bodu vo verzii podľa technickej normy[7)] informačnými systémami verejnej správy, ktoré vytvárajú textové súbory,

i) používanie formátu textového súboru uvedeného v písmene a) druhom bode pre odosielanie alebo zverejňovanie súborov s prezentáciou,

j) používanie iného formátu súborov s prezentáciou ako je uvedené v písmene i) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah v rovnakej štruktúre najmenej v jednom z formátov textových súborov uvedených v písmene a) prvom a druhom bode.

§ 20
Grafické súbory

Štandardom pre grafické súbory je pre

a) rastrovú grafiku prijímanie a čítanie všetkých doručených formátov grafických súborov, ktorými sú

1. Graphics Interchange Format (.gif),
2. Portable Network Graphics (.png) podľa technickej normy[7a)],
3. Joint Photographic Experts Group (.jpg, .jpeg, .jpe, .jfif, .jfi, .jif), najmä Joint Photographic Experts Group File Interchange Format (JFIF) podľa technickej normy[8)],
4. Tagged Image File Format (.tif, .tiff) vo verzii 6.0, najmä Baseline TIFF,

---

[7)] ISO/IEC 29500-4:2012 Formáty súborov Office Open XML. Prechodné migračné vlastnosti.

[7a)] ISO/IEC 15948: Informačné technológie. Počítačová grafika a spracovanie obrázkov. Prenosná sieťová grafika (PNG). Funkčná špecifikácia.

[8)] ISO/IEC 10918-5:2013 Digitálna kompresia a kódovanie kontinuálne tónovaných statických obrázkov. JPEG File Interchange Format (JFIF).

b) rastrovú grafiku používanie najmenej jedného z formátov grafických súborov uvedených v písmene a) pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle,

c) rastrovú grafiku používanie iného formátu grafických súborov ako je uvedené v písmene a) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah najmenej v jednom z formátov grafických súborov uvedených v písmene a),

d) vektorovú grafiku prijímanie a čítanie doručeného formátu grafických súborov, ktorým je Scalable Vector Graphics (.svg) podľa World Wide Web Consortium (W3C),

e) vektorovú grafiku používanie formátu grafických súborov uvedenom v písmene d) alebo formátu Portable Document Format (.pdf) minimálne vo verzii 1.3 a maximálne vo verzii 1.5 pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle; ak sa predpokladá ďalšia úprava, používa sa na tieto účely iba formát grafických súborov podľa písmena d) pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle,

f) vektorovú grafiku používanie iného formátu grafických súborov ako je uvedené v písmene d) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah najmenej vo formáte grafických súborov uvedenom v písmene d),

g) grafiku uloženú v textových súboroch dodržiavanie štandardu podľa písmen a) až f) a štandardu podľa § 19.

§ 21
Audio a video súbory

Štandardom pre audio a video súbory je

a) prijímanie a čítanie všetkých doručených kontajnerových formátov audio a video súborov, ktorými sú
   1. Moving Picture Experts Group (.mpg, .mpeg. .mp4, .m4a a podobne),
   2. OGG (.ogg, .oga, .ogv, .ogx),
   3. Waveform Audio File Format s obsahom kódovaným pomocou Linear Pulse Code Modulation (.wav),
   4. Audio Interchange File Format s obsahom kódovaným pomocou Linear Pulse Code Modulation (.aiff, .aif),

b) používanie najmenej jedného z kontajnerových formátov audio a video súborov uvedených v písmene a) pri ich odosielaní alebo zverejňovaní vrátane ich zverejňovania na webovom sídle,

c) používanie iného kontajnerového formátu audio a video súborov ako je uvedené v písmene a) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah najmenej v jednom z kontajnerových formátov audio a video súborov uvedených v písmene a),

d) prijímanie a čítanie všetkých doručených kompresných formátov audio a video súborov, ktorými sú
   1. MPEG-1, MPEG-2 a MPEG-4,
   2. MPEG-1 Audio Layer III (.mp3),
   3. H.263 a H.264,
   4. Ogg Vorbis (.ogg, .oga),

5. Ogg Theora (.ogv),

e) používanie najmenej jedného z kompresných formátov audio a video súborov uvedených v písmene d) pri ich odosielaní alebo zverejňovaní, vrátane ich zverejňovania na webovom sídle,

f) používanie iného kompresného formátu audio a video súborov ako je uvedené v písmene d) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah najmenej v jednom z kompresných formátov audio a video súborov uvedených v písmene d),

g) používanie jedného z formátov uvedených v písmenách a) a d) alebo formátu WMA DRM10 (.wma), ak sa vyžaduje poskytovanie licencovaného obsahu za účelom poskytnutia služieb zdravotne postihnutým osobám,

h) poskytnutie odkazu na stiahnutie audio alebo video súborov, ak sa pri poskytovaní týchto audio alebo video súborov z webových sídiel vyžaduje inštalácia alebo aktualizácia zásuvných modulov alebo doplnkov do podporovaných verzií webových prehliadačov, ktorá je nutná na prehliadnutie týchto audio a video súborov, a to na rovnakej webovej stránke.

§ 22
Súbory pre audio a video streaming

Štandardom pre súbory pre audio a video streaming je

a) používanie formátov Ogg Vorbis (.ogg, .oga), MPEG-4 Advanced Audio Coding alebo MPEG-1 Audio Layer III (.mp3) pre audio streaming,

b) používanie formátov MPEG-4 part 10, MPEG-4 part 2 alebo Ogg Theora (.ogv) pre video streaming,

c) používanie formátov MPEG-4 part 14 alebo Ogg pre kontajnerové formáty streamingu,

d) používanie najmenej jedného z protokolov pre prenos audia a videa prostredníctvom streamingu, ktorými sú

1. Real Time Streaming Protocol (RTSP) spolu s Real-time Transport Protocol (RTP),
2. Hypertext Transfer Protocol (HTTP),

e) poskytovanie iného formátu ako je uvedené v písmenách a) až c) za podmienky, ak sa zároveň poskytuje najmenej jeden z formátov uvedených v písmenách a) až c),

f) používanie iného protokolu pre prenos audia a videa ako je uvedené v písmene d), ak sa streaming zároveň poskytuje prostredníctvom jedného z protokolov uvedených v písmene d),

g) poskytovanie audio alebo video streamingu aj bez potreby použitia zásuvných modulov alebo doplnkov do webových prehliadačov, napríklad zverejnením odkazu na zdroj streamingu, a to na rovnakej webovej stránke a v tvare Uniform~~ied~~ Resource Locator (URL), ak sa pri poskytovaní audio alebo video streamingu z webových sídiel vyžaduje inštalácia alebo aktualizácia zásuvných modulov alebo doplnkov do webových prehliadačov podľa § 16 písm. c).

§ 23
Štandardy pre Internet Protocol (IP) telefóniu a videokonferenciu

Štandardom pre Internet Protocol (IP) telefóniu a videokonferenciu je používanie

a) najmenej jedného z kompresných formátov pre video komponent Internet Protocol (IP) telefónie alebo videokonferencie, ktorými sú H.261, H.262, H.263 alebo H.264,
b) najmenej jedného z kompresných formátov pre audio komponent Internet Protocol (IP) telefónie alebo videokonferencie, ktorými sú G.711, G.722 alebo G.726,
c) najmenej jedného z protokolov pre nadviazanie spojenia, ktorými sú
   1. Session Initiation Protocol (SIP) vo verzii 2.0,
   2. H.323,
d) iného formátu ako je uvedené v písmene a), ak je zároveň poskytnutý najmenej jeden z formátov uvedených v písmene a),
e) iného formátu ako je uvedené v písmene b), ak je zároveň poskytnutý najmenej jeden z formátov uvedených v písmene b).

§ 24
Súbory obsahujúce tabuľky

Štandardom pre súbory obsahujúce tabuľky je

a) prijímanie a čítanie všetkých doručených formátov súborov obsahujúcich tabuľky, ktorými sú formáty textových súborov uvedených v § 19 písm. a),
b) používanie elektronických formulárov pri úkonoch súvisiacich s poskytovaním elektronických služieb verejnej správy alebo povinným poskytovaním informácií podľa osobitných predpisov[3)]; ak to nie je technicky možné, používanie súborov obsahujúcich tabuľky, pričom ak tieto nie je možné poskytnúť vo forme webovej stránky pri ich zverejňovaní alebo nebol získaný súhlas podľa § 18 písm. a) pri ich odosielaní, ak
   1. sa majú zachovať aktívne vzorce alebo funkcie, používanie formátov podľa §19 písm. b) súčasne, a to v príslušných tvaroch (.ods) a (.xlsx),
   2. nie je potrebné zachovať aktívne vzorce alebo funkcie, používanie najmenej jedného z formátov súborov uvedených v § 19 písm. a) alebo formátu súboru obsahujúceho tabuľky Comma Separated Values (CSV),
c) pri iných úkonoch ako je uvedené v písmene b) odosielanie alebo zverejňovanie ľubovoľného formátu súborov obsahujúcich tabuľky vrátane zverejňovania na webovom sídle, pričom aj pri týchto úkonoch sa spravidla postupuje podľa písmena b),
d) podľa potreby súčasné odosielanie alebo zverejňovanie ľubovoľného iného doplňujúceho formátu súboru obsahujúceho tabuľky ku zverejnenému formátu podľa písmena b), pričom doplňujúci súbor má rovnaký a ekvivalentne vizuálne zobrazený obsah a odosiela alebo zverejňuje sa na rovnakom mieste; pri zverejňovaní na webovom sídle sa rovnakým miestom rozumie príslušná webová stránka,
e) používanie formátov podľa písmena b) prvého bodu pre účely písmena d) iba súčasne,
f) používanie formátov podľa písmena b) prvého bodu alebo písmena e) spravidla spolu so súborom s rovnakým obsahom vo formáte podľa § 19 písm. a) druhého bodu s cieľom zvýšenia ich čitateľnosti,
g) nevytváranie formátov súborov obsahujúcich tabuľky podľa písmena b) prvého bodu vo verzii podľa technickej normy[7)] informačnými systémami verejnej správy, ktoré vytvárajú súbory obsahujúce tabuľky,

h) používanie formátu Comma Separated Values (CSV) iba podľa technickej normy[9)] a dodržanie technických podmienok tvorby tohto formátu podľa prílohy č. 5.

§ 25
Formáty pre kompresiu súborov

(1) Štandardom pre formáty pre kompresiu súborov je

a) prijímanie a čítanie všetkých doručených formátov pre kompresiu súborov, ktorými sú
   1. ZIP (.zip) vo verzii 2.0,
   2. TAR (.tar),
   3. GZIP (.gz),
   4. TAR kombinovaný s GZIP (.tgz, .tar.gz),
b) používanie najmenej jedného z typov formátov pre kompresiu súborov uvedených v písmene a) pri ich odosielaní alebo zverejňovaní, vrátane ich zverejňovania na webovom sídle,
c) používanie iného formátu pre kompresiu súborov ako je uvedené v písmene a) pri jeho zverejňovaní na webovom sídle, ak je súčasne na rovnakej webovej stránke zverejnený rovnaký obsah najmenej v jednom z formátov pre kompresiu súborov uvedených v písmene a).

(2) Na súbory obsiahnuté v kompresných súboroch sa vzťahujú ustanovenia § 18 až 24.

Štandardy názvoslovia elektronických služieb

§ 26
Tvar e-mailových adries používateľov informačných systémov verejnej správy

Štandardom pre tvar e-mailových adries používateľov informačných systémov verejnej správy je

a) používanie celého mena a priezviska používateľa pri názvoch osobných e-mailových adries zamestnancov povinnej osoby poskytnutých prevádzkovateľom informačného systému verejnej správy,
b) používanie e-mailovej adresy používateľa bez diakritiky pred deliacim znakom @ v tvare „meno.priezvisko“,
c) používanie čísla za priezviskom, bez medzery, ak je identické meno aj priezvisko viacerých používateľov,
d) uskutočnenie sekundárnej identifikácie oddelením bodkou, a to v tvare „meno.priezvisko.identifikácia@“, ak je potrebná sekundárna identifikácia organizácií pri spoločnom rovnakom tvare adresy za deliacim znakom @.

§ 27
Tvar generických e-mailových adries používateľov informačných systémov verejnej správy

Štandardom pre tvar generických e-mailových adries používateľov informačných systémov verejnej správy je

---

[9)] RFC 4180 Spoločný formát a MIME typ pre Comma Separated Values (CSV) súbory.

a) používanie pravidiel, že

1. generické e-mailové adresy špecifických funkcií v orgánoch verejnej správy majú pred deliacim znakom @ názov funkcie bez diakritiky, napríklad „minister“, „tajomnik“, „veduci“, „predseda“, „primator“, „starosta“,
2. e-mailové adresy orgánov verejnej správy slúžiace na poskytovanie informácií osobám podľa osobitného predpisu[10)] a slúžiace na prijímanie sťažností podľa osobitného predpisu[11)] majú pred deliacim znakom @ tvar „info“; na prijímanie sťažností môže byť používaná aj osobitná e-mailová adresa „staznosti@“,
3. e-mailové adresy prevádzkovateľov webových stránok orgánov verejnej správy slúžiace pre ich komunikáciu s inými orgánmi verejnej správy a verejnosťou majú pred deliacim znakom @ tvar „webmaster“,
4. e-mailová adresa orgánu verejnej správy, ktorá prevádzkuje elektronickú podateľňu slúžiacu pre kontakt s ňou, má pred deliacim znakom @ tvar „podatelna“,
5. e-mailové adresy útvarov orgánov verejnej správy slúžiace pre ich komunikáciu s inými orgánmi verejnej správy a verejnosťou majú pred deliacim znakom @ iba zaužívanú skratku útvaru,
6. e-mailová adresa gestorov štandardov pre informačné systémy verejnej správy, ktorá slúži pre komunikáciu s inými orgánmi verejnej správy a verejnosťou týkajúcu sa štandardov, ktoré sú v ich gescii, má pred deliacim znakom @ tvar „standard“,

b) používanie e-mailových adries uvedených v písmene a) v prvom až šiestom bode pri elektronickej komunikácii s orgánmi verejnej správy a s verejnosťou,

c) uskutočnenie sekundárnej identifikácie oddelením bodkou, a to v tvare „generickáadresa.identifikácia@“, ak je potrebná sekundárna identifikácia organizácií pri spoločnom rovnakom tvare adresy za deliacim znakom @.

§ 28
Tvar doménových mien webových sídiel orgánov štátnej správy

(1) Štandardom pre tvar doménových mien webových sídiel orgánov štátnej správy je používanie tvaru „www.zaužívaná skratka bez diakritiky.gov.sk“ pre názvy webových sídiel orgánov štátnej správy, ktoré sú uzlami siete GOVNET.

(2) Ak dva alebo viac orgánov štátnej správy, ktoré sú uzlami siete GOVNET, majú rovnakú zaužívanú skratku, skratka sa doplní o nasledujúce písmená z názvu týchto orgánov.

Bezpečnostné štandardy

Štandardy pre architektúru riadenia

§ 29
Riadenie informačnej bezpečnosti

Štandardom pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby, ktorej obsahom je

---

[10)] Zákon č. 211/2000 Z. z.

[11)] Zákon č. 9/2010 Z. z. o sťažnostiach.

1. určenie bezpečnostných cieľov povinnej osoby z hľadiska informačnej bezpečnosti,
2. určenie spôsobov vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania ich dosahovania, spôsobov priebežného hodnotenia ich adekvátnosti a spôsobov kontroly postupov využívaných na ich dosahovanie,
3. určenie úlohy vedenia povinnej osoby pri zaisťovaní informačnej bezpečnosti a uvedenie vyhlásenia vedenia povinnej osoby o podpore bezpečnostnej politiky povinnej osoby,
4. určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti,
5. určenie povinnosti pre zaistenie nenarušenia informačnej bezpečnosti povinnej osoby,
6. zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,
7. určenie požiadaviek na informačné systémy verejnej správy, vyplývajúce zo všeobecne záväzných právnych predpisov, vnútorných predpisov povinnej osoby a jej zmluvných záväzkov a určenie spôsobu vedenia a aktualizácie dokumentácie o informačných systémoch verejnej správy,
8. určenie rozsahu a úrovne ochrany všetkých informačných systémov verejnej správy vrátane hodnotenia slabých miest a ohrození,
9. určenie rámca pre manažment rizík u povinnej osoby v súvislosti s aktívami, od ktorých závisí činnosť informačných systémov verejnej správy, alebo ktoré závisia od činnosti informačných systémov verejnej správy; rámec určí, najmä ktoré aktíva sú pre povinnú osobu kritické, čo ich ohrozuje a zásady ich ochrany,
10. určenie rozsahu a periodicity auditu informačnej bezpečnosti u povinnej osoby a zároveň určenie udalosti v informačných systémoch verejnej správy, o ktorých sa vytvára záznam auditu,
11. určenie operačných smerníc pre zálohovanie a určenie ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe,
12. určenie periodicity monitorovania bezpečnosti a aktualizácie softvéru,
13. určenie dokumentov, ktoré povinná osoba na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam,
14. určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby,

b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby,

c) určenie osoby alebo osôb zodpovedných za informačnú bezpečnosť povinnej osoby vrátane zodpovednosti za bezpečnosť všetkých informačných systémov verejnej správy,

d) určenie jednotlivých úloh osoby alebo osôb zodpovedných za informačnú bezpečnosť v súlade s bezpečnostnou politikou povinnej osoby,

e) zabezpečenie koordinácie aktivít organizačných zložiek povinnej osoby pri riešení informačnej bezpečnosti,

f) určenie konkrétnej zodpovednosti za jednotlivé aktíva povinnej osoby,

g) určenie privilegovaných používateľských rolí v informačných systémoch verejnej správy, určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a určenie, ktoré používateľské roly nie je možné navzájom zlúčiť; privilegovanými

používateľskými roľami sú najmä správca systému, operátor, používateľ, audítor a programátor.

§ 30
Personálna bezpečnosť

Štandardom pre personálnu bezpečnosť je

a) zabezpečenie, aby boli všetci zamestnanci povinnej osoby a osoby, ktoré vykonávajú činnosti pre povinnú osobu vyplývajúce zo zmluvných záväzkov (ďalej len „tretia strana“) poučení o schválenej bezpečnostnej politike povinnej osoby a o povinnostiach z nej vyplývajúcich,

b) zabezpečenie, aby boli zamestnanci povinnej osoby a tretia strana poučení o svojich právach a povinnostiach predtým, ako získajú prístup k informačnému systému verejnej správy; v prípade rozdielnych práv a povinností pre rôzne informačné systémy verejnej správy sa poučenie zopakuje a jeho obsah sa primerane upraví,

c) zabezpečenie, aby povinnosti vyplývajúce z bezpečnostnej politiky povinnej osoby a z pracovného zaradenia zamestnanca boli uvedené v jeho pracovnej zmluve alebo inom dokumente týkajúcom sa jeho právneho vzťahu s povinnou osobou,

d) vypracovanie postupu pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušia bezpečnostnú politiku povinnej osoby alebo niektorý zo súvisiacich predpisov,

e) zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty v súlade s postupmi podľa § 37,

f) vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí

1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,
2. navrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
3. odstránenie informácií povinnej osoby zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
4. zrušenie prístupových práv v informačných systémoch verejnej správy,
5. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

§ 31
Manažment rizík pre oblasť informačnej bezpečnosti

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti je

a) implementácia systému riadenia a monitorovania rizík v súvislosti s informačnými systémami verejnej správy, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami,

b) používanie systému riadenia a monitorovania rizík pri všetkých procesoch riadenia informačnej bezpečnosti,

c) identifikácia, analýza a hodnotenie rizík spojených s využívaním aktív a informačných systémov verejnej správy mimo priestorov povinnej osoby a zavedenie primeraných postupov a opatrení na redukciu týchto rizík,

d) analyzovanie procesov povinnej osoby, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti na informačných systémoch verejnej správy a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú kritickými procesmi,

e) analyzovanie rizík, vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy; tieto informačné systémy sú kritickými informačnými systémami verejnej správy,

f) vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy.

§ 32
Kontrolný mechanizmus riadenia informačnej bezpečnosti

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je

a) dodržiavanie bezpečnostnej politiky povinnej osoby a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti, ktorého periodicita sa určuje v bezpečnostnej politike povinnej osoby,

b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ.

Štandardy minimálneho technického zabezpečenia

§ 33
Ochrana proti škodlivému kódu

Štandardom pre ochranu proti škodlivému kódu je

a) zavedenie ochrany informačných systémov verejnej správy pred škodlivým kódom najmenej v rozsahu
   1. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
   2. detekcie prítomnosti škodlivého kódu na všetkých používaných zariadeniach informačného systému verejnej správy,
   3. kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
   4. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach povinnej osoby,

b) zavedenie ochrany pred nevyžiadanou elektronickou poštou,

c) používanie len takého softvéru, ktorý je legálny a povolený príslušnými vnútornými predpismi povinnej osoby,

d) určenie pravidiel pre sťahovanie súborov prostredníctvom externých sietí,

e) podpora zabezpečenia autenticity a integrity súborov pomocou kryptografických prostriedkov, ktorým je najmä elektronický podpis,

f) podpora šifrovania elektronických dokumentov.

§ 34

Sieťová bezpečnosť

Štandardom pre sieťovú bezpečnosť je

a) zabezpečenie ochrany vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (firewall) pre informačné systémy verejnej správy,

b) vedenie evidencie o všetkých miestach prepojenia sietí v správe povinnej osoby vrátane prepojení s externými sieťami,

c) zabezpečenie, aby pre každé prepojenie podľa písmena b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami podľa § 41.

§ 35
Fyzická bezpečnosť a bezpečnosť prostredia

Štandardom pre fyzickú bezpečnosť a bezpečnosť prostredia je

a) umiestnenie informačného systému verejnej správy v takom priestore, aby informačný systém verejnej správy alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“),

b) oddelenie zabezpečeného priestoru od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami,

c) zabezpečenie, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť informačný systém verejnej správy umiestnený v tomto zabezpečenom priestore,

d) vypracovanie a implementácia pravidiel pre prácu v zabezpečenom priestore,

e) zabezpečenie ochrany pred výpadkom zdroja elektrickej energie pre tie časti informačného systému verejnej správy, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, aby takýto výpadok nenastal,

f) zabezpečenie, aby boli existujúce záložné kapacity informačného systému verejnej správy, zabezpečujúce funkčnosť alebo náhradu informačného systému verejnej správy, umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru,

g) zabezpečenie, aby bola prevádzka, používanie a manažment informačného systému verejnej správy v súlade s osobitnými predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,

h) vypracovanie, zavedenie a kontrola dodržiavania pravidiel pre

   1. údržbu, uchovávanie a evidenciu technických komponentov informačného systému verejnej správy a zariadení informačného systému verejnej správy,
   2. používanie zariadení informačného systému verejnej správy na iné účely, na aké boli pôvodne určené,
   3. používanie zariadení informačného systému verejnej správy mimo určených priestorov,
   4. vymazávanie, vyraďovanie a likvidovanie zariadení informačného systému verejnej správy a všetkých typov relevantných záloh,
   5. prenos technických komponentov informačného systému verejnej správy alebo zariadení informačného systému verejnej správy mimo priestorov povinnej osoby,

6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačného systému verejnej správy tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,

i) stanovenie parametrov pre informačné systémy verejnej správy, ktoré definujú maximálnu prípustnú dobu výpadku informačného systému verejnej správy a vytvorenie a zavedenie opatrení, ktoré sú zamerané na riešenie obnovy prevádzky v prípade výpadku informačného systému verejnej správy.

§ 36
Aktualizácia softvéru

Štandardom pre aktualizáciu softvéru je

a) zabezpečenie aktualizácie verzií inštalovaného ochranného softvéru, zabezpečujúceho ochranu podľa § 33 písm. a) a b) a § 34 písm. a), vrátane zabezpečenia všetkých ostatných komponentov a pripájaných prostriedkov,

b) vykonanie aktualizácie minimálne v súlade s bezpečnostnou politikou povinnej osoby.

§ 37
Monitorovanie a manažment bezpečnostných incidentov

Štandardom pre monitorovanie a manažment bezpečnostných incidentov je

a) vypracovanie interného aktu obsahujúceho

1. postup pri ohlasovaní bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy, najmä za účelom včasného prijatia preventívnych a nápravných opatrení,
2. postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob ich vyhodnocovania,
3. spôsob evidencie bezpečnostných incidentov a použitých riešení,

b) zabezpečenie, aby o postupoch podľa písmena a) boli primeraným spôsobom informovaní všetci používatelia informačného systému verejnej správy, a aby boli tieto postupy dodržiavané,

c) zavedenie evidencie každého výpadku informačného systému verejnej správy a spôsobu jeho riešenia,

d) pre povinné osoby podľa § 3 ods. 1 písm. a) zákona používanie systému na detekciu prienikov, ktorý monitoruje bezpečnosť najmenej v rozsahu Intrusion Detection System (IDS),

e) vytvorenie a prevádzka kontaktného miesta povinnej osoby pre ohlasovanie bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy v správe povinnej osoby.

§ 38
Periodické hodnotenie zraniteľnosti

Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému verejnej správy identifikovaných podľa bezpečnostnej politiky povinnej osoby s periodicitou najmenej raz ročne.

§ 39
Zálohovanie

Štandardom pre zálohovanie je

a) zabezpečenie vytvorenia archivačnej zálohy a prevádzkovej zálohy podľa periodicity určenej v bezpečnostnej politike povinnej osoby, najmenej raz za týždeň, ak ide o prevádzkovú zálohu a najmenej raz za dva mesiace, ak ide o archivačnú zálohu,
b) vyhotovenie archivačnej zálohy v dvoch kópiách,
c) zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a v prípade nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči,
d) zabezpečenie vykonania testu obnovy informačného systému verejnej správy a údajov z prevádzkovej zálohy najmenej raz za jeden rok.

§ 40
Fyzické ukladanie záloh

Štandardom pre fyzické ukladanie záloh je

a) fyzické ukladanie prevádzkových záloh, jednej kópie archivačnej zálohy a dátových nosičov s licencovaným softvérom do uzamykateľného priestoru,
b) fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte ako sa nachádzajú technické prostriedky informačného systému verejnej správy, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.

§ 41
Riadenie prístupu

Štandardom pre riadenie prístupu je

a) zavedenie identifikácie používateľa a následnej autentizácie pri vstupe do informačného systému verejnej správy,
b) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založenej na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh,
c) určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom,
d) určenie požiadaviek, ktoré majú používatelia v súlade s bezpečnostnou politikou povinnej osoby dodržiavať pri používaní informačného systému verejnej správy,
e) automatické zaznamenávanie zmien v pridelenom prístupe a ich archivácia počas celej doby činnosti informačného systému verejnej správy,
f) určenie bezpečnostných zásad pre mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),
g) zabezpečenie, aby používatelia nepoužívali informačné systémy verejnej správy na nelegálne účely,
h) umožniť fyzickým osobám zodpovedným za správu a prevádzku informačných systémov verejnej správy prístup iba k takým údajom a funkciám v týchto informačných systémoch verejnej správy, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh,

i) automatické zaznamenávanie každého prístupu každého používateľa vrátane administrátora do informačného systému verejnej správy, zamedzenie možnosti zmeny týchto záznamov a zamedzenie možnosti vymazania týchto záznamov bez schválenia zodpovednou osobou určenou podľa § 29 písm. c),

j) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy.

§ 42
Aktualizácia informačno-komunikačných technológií

Štandardom pre aktualizáciu informačno-komunikačných technológií je

a) zavedenie postupov s počiatočným stanovením a zahrnutím bezpečnostných požiadaviek a schvaľovacieho procesu pre
   1. zmenu konfigurácie, zavádzanie nových alebo aktualizáciu a rozširovanie funkcionality existujúcich informačných systémov verejnej správy alebo ich častí; v prípade automatizovanej on-line aktualizácie sa schvaľovanie zavádza iba, ak si vyžaduje finančné zdroje alebo je aktualizácia príliš rozsiahla,
   2. zavádzanie nových informačno-komunikačných technológií u povinnej osoby najmä s ohľadom na zaistenie kompatibility a zachovanie potrebnej úrovne bezpečnosti,

b) vymenovanie zástupcu správcu alebo prevádzkovateľa informačného systému verejnej správy, zodpovedného za informačnú bezpečnosť a činnosti podľa písmena a),

c) vymenovanie zástupcu dodávateľa, ak je dodávateľom činnosti podľa písmena a) tretia strana, zodpovedného za informačnú bezpečnosť,

d) vykonanie testovania pre činnosti podľa písmena a) a vytvorenie dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch, a to najmenej vykonanie interného používateľského testovania v rozsahu najmenej jedného týždňa pred odovzdaním informačného systému verejnej správy, jeho časti alebo súvisiacej aplikácie dodávateľom a zahrnutie jeho výstupov do dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch,

e) uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy alebo ich častiach, ktorá obsahuje
   1. používateľskú dokumentáciu, ktorou je návod na používanie informačného systému verejnej správy,
   2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku informačného systému verejnej správy,
   3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému verejnej správy alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy.

§ 43
Účasť tretej strany

Štandardom pre účasť tretej strany je

a) analýza rizík v súvislosti s informačnými systémami verejnej správy podľa § 31, vyplývajúcich z činnosti tretích strán v týchto informačných systémoch, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb a zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích

strán v informačných systémoch verejnej správy, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

b) zabezpečenie, aby boli v zmluvách s treťou stranou o poskytovaní služieb súvisiacich s informačným systémom verejnej správy uvedené bezpečnostné požiadavky na tieto služby,

c) zamedzenie prístupu tretích strán ku všetkým údajom v informačnom systéme verejnej správy, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom na základe zmluvy tak, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

d) zabezpečenie kontroly plnenia bezpečnostných požiadaviek podľa písmena b),

e) zabezpečenie, aby nesplnenie bezpečnostných požiadaviek podľa písmen b) a c) alebo podľa § 42 písm. a), c) a d) bolo dôvodom na neukončenie príslušnej etapy projektu alebo neschválenie prevzatia vykonávanej činnosti.

§ 44

Federácia identít

Štandardom pre federáciu identít je používanie protokolu Security Assertion Markup Language (SAML) vo verzii 2.0 podľa Organization for the Advancement of Structured Information Standards (OASIS) pri federácii identít informačných systémov verejnej správy, pričom ak je poskytovateľom identít správca ústredného portálu verejnej správy

a) pre protokol Security Assertion Markup Language (SAML) sa používa
   1. profil Web Browser Single Sign-On Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST alebo HTTP-Redirect, alebo
   2. profil Single Logout Profile s technickým spôsobom jeho vykonania prostredníctvom HTTP-POST, HTTP-Redirect alebo Simple Object Access Protocol (SOAP) minimálne vo verzii 1.2,

b) dátová štruktúra Security Assertion Markup Language (SAML) Assertion pre prenos autentifikačných informácií medzi poskytovateľom služby a poskytovateľom identity má atribúty podľa prílohy č. 8.

Dátové štandardy

§ 45

Výmena údajov medzi informačnými systémami verejnej správy

Štandardom pre výmenu údajov medzi informačnými systémami verejnej správy je pri výmene obsahovo príslušných informácií použitie dátových prvkov uvedených v prílohe č. 2. Ak neexistujú obsahovo vhodné dátové prvky, použijú sa vlastné dátové prvky.

§ 46

Referencovateľný identifikátor

Štandardom pre referencovateľný identifikátor je

a) používanie referencovateľného identifikátora v štruktúre „{základná Uniform~~ied~~ Resource Identifier (URI)}{zdrojová cesta}/{typ}/{trieda}/{podtrieda1/podtrieda2/…}/{referencia}“, pričom
   1. základnú Uniform~~ie~~d Resource Identifier (URI) tvorí „http://”,

2. zdrojovú cestu tvorí „data.gov.sk“,
3. typ tvorí jeden z reťazcov, ktorými sú
   3a. „id”, ak sa identifikuje neinformačný zdroj, ktorým je entita skutočného sveta,
   3b. „doc“, ak sa identifikuje dokument, vrátane takého dokumentu, ktorý opisuje neinformačný zdroj,
   3c. „def“, ak sa identifikuje definícia konkrétneho konceptu,
   3d. „set“, ak sa identifikuje súbor údajov,
4. triedu tvorí slovo alebo reťazec, ktoré zachytávajú podstatu identifikovanej entity skutočného sveta, napríklad „škola“, a to podľa zoznamučíselníka tried referencovateľných identifikátorov zverejňovaného prostredníctvom webového sídla ministerstva,
5. podtriedu tvorí slovo alebo reťazec sekundárnej klasifikácie triedy, ak je to potrebné; podtrieda nemusí byť použitá a môže vytvárať aj viacnásobnú štruktúru sekundárnych klasifikácií, a to podľa zoznamu referencovateľných identifikátorov zverejňovaného prostredníctvom webového sídla ministerstva,
6. referenciu tvorí reťazec, ktorý sa používa na identifikáciu jednotlivých inštancií konceptu, obvykle v tvare kódu z číselníka,; štruktúra reťazca je vytváraná v súlade so zoznamom referencovateľných identifikátorov zverejňovaným prostredníctvom webového sídla ministerstva,

b) používanie anglického jazyka pre vytváranie triedy, podtriedy a referencie podľa písmena a); to neplatí, ak je pre referenciu nevyhnutné použitie slovenského jazyka, napríklad skratky zo slov v slovenskom jazyku.

Štandardy elektronických služieb verejnej správy

§ 47
Vlastnosti elektronických služieb verejnej správy

Štandardom vlastností elektronických služieb verejnej správy je

a) rozdelenie elektronických služieb verejnej správy podľa úrovne elektronizácie na šesť úrovní, ktorými sú
   1. úroveň 0, označovaná aj ako úroveň off-line, pri ktorej služba nie je on-line elektronicky dostupná,
   2. úroveň 1, označovaná aj ako informatívna úroveň, pri ktorej je informácia, potrebná na začatie alebo vykonanie služby, dostupná v elektronickej forme, najmä informácia o mieste, čase, spôsobe a podmienkach vybavenia služby, pričom samotná služba nie je elektronicky poskytnutá, ani nie je poskytnutý príslušný formulár v elektronickej forme,
   3. úroveň 2, označovaná aj ako úroveň jednosmernej interakcie, pri ktorej nastáva jednosmerná elektronická komunikácia; pri jednosmernej elektronickej komunikácii je možné stiahnuť príslušný formulár v elektronickej forme, ale podanie sa nevykonáva elektronickými prostriedkami,
   4. úroveň 3, označovaná aj ako úroveň obojsmernej interakcie, pri ktorej nastáva obojsmerná elektronická komunikácia pri vybavovaní služby; pri obojsmernej elektronickej komunikácii prebieha vybavovanie služby elektronicky, avšak pri preberaní výsledku služby sa vyžaduje osobný alebo listinný kontakt,

5. úroveň 4, označovaná aj ako transakčná úroveň, ktorá umožňuje úplné vybavenie služby elektronickými prostriedkami, najmä vybavenie on-line, a to vrátane rozhodnutia, zaplatenia a doručenia, ak sa to vyžaduje; pri tejto úrovni sa vylučuje akýkoľvek osobný alebo listinný kontakt,
6. úroveň 5, označovaná aj ako proaktívna úroveň, ktorá obsahuje funkčnosť úrovne 3 alebo úrovne 4, a pri ktorej sa naviac využívajú personalizované nastavenia používateľa a možnosť proaktívneho automatizovaného vykonávania častí služby,

b) poskytovanie notifikácie klientovi služby o jej použití pre elektronické služby verejnej správy podľa písmena a) štvrtého až šiesteho bodu,

c) poskytovanie informácie o cene jednotlivých častí elektronickej služby verejnej správy, a ak je to možné, aj výslednú cenu za jej použitie, a to najmenej pred potvrdením použitia elektronickej služby verejnej správy,

d) rozdelenie elektronických služieb verejnej správy podľa úrovní autentifikácie uvedených v prílohe č. 6,

e) označenie poskytovaných elektronických služieb verejnej správy príslušnou úrovňou autentifikácie podľa písmena d),

f) zabezpečenie dodržania podmienok a postupov pre príslušnú úroveň autentifikácie pri poskytovaných elektronických službách verejnej správy.

§ 48

Používanie zásuvných modulov a doplnkov webových prehliadačov a klientskych aplikácií

Štandardom pre používanie zásuvných modulov a doplnkov webových prehliadačov a klientskych aplikácií je

a) poskytovanie ~~elektronických služieb verejnej správy alebo~~ poskytovanie webových stránok~~,~~ obsahujúcich povinne zverejňované informácie podľa osobitných predpisov~~1b~~3) alebo poskytovanie elektronických služieb verejnej správy tak, aby ich funkčnosť vo webových prehliadačoch nevyžadovala inštalácie zásuvných modulov, doplnkov alebo klientskych aplikácií,

b) umožnenie vyžadovania zásuvných modulov alebo doplnkov webových prehliadačov alebo klientskych aplikácií pri poskytovaní elektronických služieb verejnej správy, ak tieto služby nie je možné preukázateľne a objektívne poskytnúť v súlade s písmenom a), pričom vyžadované zásuvné moduly a doplnky webových prehliadačov a klientske aplikácie poskytujú rovnakú plnú funkčnosť minimálne v desktopových operačných systémoch Windows vo verzii XP a novších verziách, Mac OS X a GNU/Linux a obvykle tiež v klientskych operačných systémoch s podielom zastúpenia na trhu v Slovenskej republike najmenej 5%; pri vyžadovaní zásuvných modulov a doplnkov webových prehliadačov alebo klientskych aplikácií sa poskytuje aj odôvodnenie ich vyžadovania, presný opis inštalácie, systémových požiadaviek a účelu ich použitia a návod na použitie, a to na mieste poskytovania príslušných elektronických služieb verejnej správy,

c) zásuvné moduly, doplnky webových prehliadačov alebo klientske aplikácie, ktoré sú poskytované povinnými osobami na stiahnutie, sa obvykle poskytujú z webového sídla povinnej osoby prostredníctvom chráneného prenosu dát.

Formátované: Zarážka: Opakovaná zarážka: 0,63 cm, Nezväzovať s nasledujúcim, Zarážky: 0,63 cm, Tabulátor pre zoznam + Nie je v 4,44 cm

§ 49

Elektronické formuláre

Štandardom pre elektronické formuláre je

a) použitie dátových prvkov uvedených v prílohe č. 2 pre tvorbu elektronických formulárov; ak neexistujú obsahovo totožné dátové prvky, je možné použiť vlastné dátové prvky,

b) dodržiavanie pravidiel podľa prílohy č. 3 pri výmene informácií medzi používateľom služby a gestorom služby,

c) poskytovanie elektronických služieb verejnej správy podľa § 47 písm. a) štvrtého až šiesteho bodu pomocou elektronických formulárov, ak sa od používateľa elektronickej služby vyžaduje vyplnenie údajov.

Štandardy projektového riadenia

§ 50
Riadenie informačno-technologických projektov

Štandardom pre riadenie informačno-technologických projektov je

a) pre všetky veľkosti projektu povinné vykonanie činnosti v prípravnej fáze podľa prílohy č. 4 bodu 3.1,

b) v závislosti od veľkosti projektu vypracovanie záverečných verzií dokumentov podľa prílohy č. 4

1. bodu 7.2.1 písm. a) až d), bodu 7.2.2 písm. a) až c), bodu 7.2.3 písm. a) a bodu 7.2.4 písm. a) pre malý projekt,
2. bodu 7.2.1 písm. a) až d), bodu 7.2.2 písm. a) až d), f) a g), bodu 7.2.3 písm. a) a b) a bodu 7.2.4 písm. a) pre stredný projekt,
3. bodu 7.2.1 písm. a) až f), bodu 7.2.2 písm. a) až l), bodu 7.2.3 písm. a) až f) a bodu 7.2.4 písm. a) a b) pre veľký projekt.

Štandardy poskytovania údajov v elektronickom prostredí

§ 51
Kvalita datasetu poskytovaného povinnou osobou

(1) Štandardom kvality datasetu poskytovaného povinnou osobou je rozdelenie kvality datasetu na šesť úrovní, ktorými sú

a) úroveň 0, pri ktorej nie je dataset poskytovaný v elektronickej forme,

b) úroveň 1, pri ktorej je dataset dostupný vo webovom prostredí,

c) úroveň 2, pri ktorej je splnená požiadavka uvedená v písmene b) a obsah datasetu je štruktúrovaný tak, že umožňuje automatizované spracovanie,

d) úroveň 3, pri ktorej sú splnené požiadavky uvedené v písmene c) a dataset je poskytovaný v otvorenom formáte, nezávislom na konkrétnom proprietárnom softvéri,

e) úroveň 4, pri ktorej sú splnené požiadavky uvedené v písmene d) a na identifikáciu údajov datasetu a ich vzťahov sa používajú refencovateľné identifikátory,

f) úroveň 5, pri ktorej sú splnené požiadavky uvedené v písmene e) a dataset a jeho interné a externé vzťahy majú charakter identifikátormi prepojených údajov.

(2) Ak sa údaje poskytujú pre automatizované spracovanie, štandardom kvality datasetu poskytovaného povinnou osobou je aj ich poskytovanie ako datasetu s otvorenými údajmi podľa § 53 a v kvalite najmenej úrovne 3.

§ 52

Otvorené údaje

(1) Štandardom pre označenie údaja ako otvoreného údaja je

a) poskytovanie údaja v datasete v kvalite poskytovaného datasetu najmenej úrovne 3,

b) poskytovanie údaja otvoreným spôsobom použitia, ktorý je splnený, ak

1. sú právne aspekty prístupu k údaju a jeho používaniu explicitne vysporiadané,
2. je umožnené vytvorenie právnych vzťahov pre používanie údaja aj prostredníctvom anonymného vzdialeného automatizovaného prístupu,
3. je prístup k údaju umožnený všetkým osobám za rovnakých podmienok, pričom tieto podmienky sú explicitne uvedené,
4. je údaj možné použiť na nekomerčný aj komerčný účel, a je možné ho kombinovať s inými údajmi, dopĺňať, opravovať, modifikovať alebo použiť z datasetu bez povinnosti použitia ostatných údajov datasetu,
5. sú činnosti podľa štvrtého bodu bezodplatné.

(2) Ak dataset obsahuje najmenej jeden otvorený údaj, označuje sa ako dataset s otvorenými údajmi.

§ 53

Poskytovanie otvorených údajov

Štandardom pre poskytovanie otvorených údajov je

a) označenie každého poskytovaného datasetu s otvorenými údajmi dosiahnutou úrovňou kvality podľa § 51,

b) pri poskytovaní datasetu s otvorenými údajmi použitie jedného z formátov podľa § 13 písm. b), pričom pri použití formátov Comma Separated Values (CSV) a JavaScript Object Notation (JSON) je najvyššia dosiahnuteľná úroveň kvality poskytovaného datasetu 3 a pri použití ostatných formátov podľa § 13 písm. b) je najvyššia dosiahnuteľná úroveň 5,

c) pri poskytovaní datasetu s otvorenými údajmi poskytnutie schémy údajov datasetu vo formáte podľa § 13 písm. a) alebo, ak je použitý formát Comma Separated Values (CSV) alebo JavaScript Object Notation (JSON), poskytnutie textového opisu, obsahujúceho pre každý typ údaja najmä

1. poradové číslo typu údaja a názov typu údaja, ak je použitý,
2. opis dátového druhu typu údaja, napríklad v tvare „identifikátor“, „číslo“, „text“ a podobne,
3. vecný opis typu údaja, napríklad v tvare „meno“ alebo „priezvisko“, a najmä pre údaj typu identifikátor aj referenciu na externú definíciu,
4. ohraničenia pre hodnotu typu údaja, ak existujú,

d) pre identifikáciu každého údaja v poskytovanom datasete s otvorenými údajmi používanie

1. referencovateľného identifikátora,
2. kódu podľa príslušného číselníka alebo
3. hodnoty predstavujúcej tento údaj,

e) sprístupnenie otvorených údajov aplikačným rozhraním podľa § 13 písm. a) alebo sprístupnenie datasetu s otvorenými údajmi v ucelenej forme protokolom podľa § 4 ods. 1,

f) zaevidovanie datasetu s otvorenými údajmi v centrálnom katalógu otvorených údajov „data.gov.sk“,

g) poskytovanie datasetu s otvorenými údajmi tak, aby bolo umožnené

1. zistiť pre každý údaj okamih alebo dobu, v ktorej bol platný,
2. zistiť po aktualizácii údajov, ktoré údaje boli zmenené,
3. zistiť či je dataset aktualizovaný v reálnom čase alebo v určitej periodicite a v akej,
4. odlíšiť chybné alebo nepresné údaje od správnych alebo presných údajov; ak to nie je možné, odlíšiť celý dataset ako dataset obsahujúci chybné alebo nepresné údaje,

h) poskytovanie metaúdajov pre dataset s otvorenými údajmi priamo na mieste poskytnutia datasetu alebo prostredníctvom katalógu otvorených údajov, ktorým je miesto evidencie otvorených údajov povinnej osoby, a to najmenej v rozsahu podľa prílohy č. 9 bodov 1 až 6.

Štandardy poskytovania cloud computingu a využívania cloudových služieb

§ 54

Modely poskytovania cloudových služieb a typy cloud computingu

(1) Štandardom modelov poskytovania cloudových služieb je rozdelenie modelov poskytovania cloudových služieb najmä na model

a) infraštruktúra ako služba, označovaný aj ako IaaS, pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry,

b) platforma ako služba, označovaný aj ako PaaS, pri ktorom cloudovú službu predstavuje poskytovanie hardvérovej a softvérovej platformy, potrebnej na vytvorenie a správu aplikácií, vrátane umožnenia ich navrhovania, vývoja, testovania a nasadzovania do produkčnej prevádzky, pričom tieto aplikácie ostávajú v správe odberateľa cloudových služieb,

c) softvér ako služba, označovaný aj ako SaaS, pri ktorom cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií.

(2) Štandardom pre typy cloud computingu je rozdelenie typov cloud computingu najmä na

a) privátny cloud, pri ktorom je cloud computing alokovaný výhradne pre potreby jednej organizácie, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť táto organizácia,

b) komunitný cloud, pri ktorom cloud computing využíva niekoľko organizácií, ktoré tvoria jednu komunitu, zdieľajúcu podobné záujmy, napríklad ciele, požiadavky na bezpečnosť, politiku a dodržiavanie záujmov, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť ani jedna z týchto organizácií,

c) verejný cloud, pri ktorom je cloud computing zdieľaný ľubovoľnými odberateľmi cloudových služieb, pričom ani jeden z nich nemusí byť poskytovateľom cloudových služieb alebo prevádzkovateľom cloudových služieb,

d) hybridný cloud, ktorý predstavuje kompozitné využitie cloudových služieb dvoch alebo viacerých typov cloud computingu, pričom využívané cloudové služby sú naďalej podporované jednotlivými infraštrukturálnymi prostriedkami daných typov cloud computingu, ale ako také sú vzájomne spojené štandardizovanými alebo proprietárnymi technológiami, ktoré umožňujú prenositeľnosť údajov a aplikácií.

§ 55

Správa cloud computingu

(1) Štandardom pre správu cloud computingu v správe povinnej osoby je správa cloud computingu zabezpečovaná tak, aby bola primerane v súlade so štandardom pre

a) riadenie informačnej bezpečnosti podľa § 29, pričom pre
   1. požiadavku podľa § 29 písm. a) sú súčasťou bezpečnostnej politiky povinnej osoby aj podmienky zosúlaďovania bezpečnostných požiadaviek alebo cieľov poskytovateľa cloudových služieb s bezpečnostnými požiadavkami alebo cieľmi odberateľa cloudových služieb,
   2. požiadavku podľa § 29 písm. a) deviateho bodu sú aktívami najmä poskytované cloudové služby a infraštruktúra, prostredníctvom ktorej sú tieto služby poskytované, vrátane
      2a. uzlov pre prepojenie sietí z pohľadu dostupnosti sieťového pripojenia; tieto sú zároveň kritickým aktívom,
      2b. hardvéru, ktorým je najmä dátové úložisko, jednotlivé prvky siete a servery,
      2c. softvéru, ktorým je najmä softvér pre správu cloud computingu, hypervízor a operačný systém,
b) personálnu bezpečnosť podľa § 30,
c) manažment rizík pre oblasť informačnej bezpečnosti podľa § 31, pričom analýza rizík vyhodnocuje najmä hrozby, ktorými sú
   1. strata alebo nedostupnosť cloudových služieb,
   2. nedostatok zdrojov alebo neschopnosť dodať požadovaný výkon,
   3. zlyhanie alebo nedostatočná izolácia prostredia,
   4. neoprávnený prístup k izolovanému prostrediu,
   5. narušenie bezpečnosti hypervízora, ktorým je najmä virtualizačný server, virtualizačná pamäť, virtuálny úložný priestor, virtuálny sieť alebo virtuálny operačný systém,
   6. nedostatočný monitoring jednotlivých komponentov cloud computingu,
   7. nebezpečné alebo neefektívne odstránenie údajov,
   8. kompromitácia vrstvy správy cloud computingu z dôvodu výskytu možných zraniteľností hypervízora alebo nedostatočnej izolácie prostredia,
   9. zneužitie alebo kompromitácia privilegovaných oprávnení,
   10. kompromitácia šifrovacích kľúčov,
   11. zlyhanie správy šifrovacích kľúčov,
   12. zlyhanie alebo nedostatočný manažment zmenových požiadaviek a záplat, najmä vo vzťahu k funkčnosti informačných systémov verejnej správy využívajúcich cloudové služby,
   13. narušenie funkčnosti cloudových služieb z dôvodu zlyhania iných cloudových služieb na základe závislosti na spoločných zdrojoch,
d) kontrolný mechanizmus riadenia informačnej bezpečnosti podľa § 32, pričom pre požiadavku podľa § 32 písm. a) sa minimálne raz ročne
   1. vykonáva audit informačnej bezpečnosti audítorom cloudu~~nezávislou treťou stranou~~,
   2. umožňuje odberateľovi cloudových služieb vykonať prostredníctvom audítora cloudu alebo po dohode s poskytovateľom cloudových služieb inou osobou audit informačnej bezpečnosti všetkých zdrojov, ktoré využívajú jemu poskytované cloudové služby

alebo sa týkajú jemu poskytovaných cloudových služieb, a to podľa podmienok upravenýchpričom podmienky sa môžu upraviť v dohode o poskytovanej úrovni cloudových služieb, pričom ak nastane bezpečnostný incident týkajúci sa týchto zdrojov, ktorý ovplyvní kvalitu príslušných poskytovaných cloudových služieb, umožňuje sa vykonať takýto audit bezodkladne po tomto incidente nezávisle od počtu auditov vykonávaných ročne podľa tohto bodu

3. umožňuje odberateľovi cloudových služieb vykonať prostredníctvom audítora cloudu alebo po dohode s poskytovateľom cloudových služieb inou osobou penetračný test, týkajúci sa cloudových služieb poskytovaných tomuto odberateľovi cloudových služieb, pričom takýto test je pripravený podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb a tak, aby neovplyvnil kvalitu poskytovaných cloudových služieb alebo ju ovplyvnil v rozsahu dohodnutom medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb,

e) ochranu proti škodlivému kódu podľa § 33, pričom
   1. pre požiadavku podľa § 33 písm. a) druhého bodu sa zabezpečuje detekcia útokov na prostredie cloud computingu, a to vrátane útokov na komponenty určené pre správu cloud computingu,
   2. pre požiadavku podľa § 33 písm. e) sa zaisťuje aj podpora zabezpečenia dôvernosti, autenticity a integrity prenášaných dát pomocou kryptografických opatrení,
f) sieťovú bezpečnosť podľa § 34, pričom sa zabezpečuje aj podpora
   1. virtualizovaných firewallov a iných prvkov siete,
   2. segmentácie siete, napríklad vo forme Virtual Local Area Network (VLAN),
   3. detekcie škodlivému kódu a jeho odstraňovania na sieťovej úrovni,
g) fyzickú bezpečnosť a bezpečnosť prostredia podľa § 35, pričom pre požiadavku podľa § 35 písm. i) sa
   1. vytvára aj plán kontinuity činnosti,
   2. definuje v dohode o poskytovanej úrovni cloudových služieb aj doba obnovy; dobou obnovy je čas, do ktorého je poskytovateľ cloudových služieb v prípade výpadku povinný obnoviť ich poskytovanie,
h) aktualizáciu softvéru podľa § 36, pričom sa zabezpečuje aj testovanie aktualizácie virtualizačného prostredia a softvéru pre správu cloudu v testovacom prostredí,
i) monitorovanie a manažment bezpečnostných incidentov podľa § 36, pričom sa
   1. pri požiadavke podľa § 37 písm. c) monitoruje aj správna funkčnosť všetkých komponentov cloud computingu,
   2. pri požiadavke podľa § 37 písm. d) zabezpečuje aj podpora detekcie útokov na sieti, napríklad vo forme Intrusion Detection System (IDS) alebo Intrusion Prevention System (IPS),
   3. poskytuje podpora zmiernenia a eliminácie útokov typu Denial of Service (DoS) a Distributed Denial of Service (DDoS),
   4. zabezpečuje aj synchronizácia systémového času všetkých komponentov cloud computingu s cieľom používania jednotného času v celom prostredí cloud computingu,
j) periodické hodnotenie zraniteľnosti podľa § 38,
k) zálohovanie podľa § 39,

l) fyzické ukladanie záloh podľa § 40, pričom pre požiadavku podľa § 40 písm. b) je nevyhnutné uchovávať v súlade s týmto ustanovením aj prevádzkovú zálohu a dokumentáciu, súvisiacu s poskytovaným cloud computingom,

m) riadenie prístupu podľa § 41, pričom sa

1. pre požiadavku podľa § 41 písm. a) používa pri správe modulov podľa prílohy č. 7 jednotná služba pre účely identifikácie, autentifikácie a autorizácie systémových správcov a odberateľov cloudových služieb,
2. pre požiadavku podľa § 41 písm. i)
   - 2a. automaticky zaznamenávajú aj všetky udalosti, spojené s úspešným alebo neúspešným prístupom, vrátane vzdialeného prístupu,
   - 2b. zabezpečuje aj automatické zaznamenávanie všetkých činností spojených s aktiváciou alebo deaktiváciou cloudových služieb,
   - 2c. zabezpečuje aj automatické zaznamenávanie všetkých udalostí spojených s funkčnosťou cloud computingu,
   - 2d. zabezpečuje aj automatické zaznamenávanie detegovaných neoprávnených aktivít, najmä zo strany privilegovaných používateľských rolí, zariadení a softvéru, zaisťujúcich bezpečnosť cloud computingu,
   - 2e. zabezpečuje aj automatické zaznamenávanie všetkých udalostí spojených so zmenami súvisiacimi najmä so sieťou, správou cloud computingu, hypervízorom, používaným operačným systémom, monitoringom, zálohovaním a obnovou,
   - 2f. vyhodnocujú automatické záznamy za účelom identifikácie bezpečnostne relevantných udalostí, ktoré môžu viesť k bezpečnostným incidentom,
   - 2g. vytvárajú automatické záznamy tak, aby obsahovali relevantné informácie a presný časový údaj,
   - 2h. zabezpečujú všetky automatické záznamy pred neoprávnenou manipuláciou, zmenou a vymazaním,
   - 2i. zálohujú automatické záznamy po dobu najmenej jedného roka,
3. pri správe modulov podľa prílohy č. 7 pre požiadavku podľa § 41 písm. j) podporuje riadenie prístupových oprávnení na základe rolí,
4. pri správe modulov podľa prílohy č. 7 umožňuje zmena hesiel pre prednastavené účty,
5. pri správe modulov podľa prílohy č. 7 umožňuje používanie politiky tvorby hesiel, ktorá zabezpečuje najmä adekvátnu komplexnosť hesiel, zobrazovanie informácie o úspešnom alebo neúspešnom prihlásení tak, aby z nej nebolo možné prečítať systémové informácie, určenie doby platnosti hesiel, exspirovanie prístupu po určenej dobe nečinnosti a blokovanie prístupu po určenom počte neúspešných prihlásení,

n) aktualizáciu informačno-komunikačných technológií podľa § 42,

o) účasť tretej strany podľa § 43.

(2) Na účely podľa odseku 1 sa povinnou osobou rozumie poskytovateľ cloudových služieb a informačným systémom verejnej správy sa rozumie cloud computing, okrem § 29 písm. a) ôsmeho bodu a § 29 písm. c), kde sa informačnými systémami verejnej správy rozumejú časti cloud computingu.

(3) Súčasťou štandardu pre správu cloud computingu v správe povinnej osoby podľa odseku 1 je aj bezpečnosť zdieľaného prostredia, pričom sa

a) pri výpadku cloudových služieb v súlade s podmienkami a garantovanými parametrami dostupnosti~~niektorého fyzického komponentu alebo virtuálneho komponentu~~ zabezpečuje

migrácia do záložného prostredia podľa vopred určeného scenára tak, aby dodávka cloudových služieb nebola dlhodobo ohrozená,

b) umožňuje oddeliť údaje jednotlivých odberateľov cloudových služieb, pričom spôsob oddelenia je obsiahnutý v dohode o poskytovanej úrovni cloudových služieb,

c) virtuálne komponenty oddeľujú do bezpečnostných zón podľa typu použitia s cieľom zníženia rizika neautorizovaného prístupu alebo zmien.

(4) Súčasťou štandardu pre správu cloud computingu v správe povinnej osoby podľa odseku 1 je aj správa cloud computingu zabezpečovaná tak, aby

a) boli v dohode o poskytovanej úrovni cloudových služieb obsiahnuté aj podmienky a garantované parametre dostupnosti cloudových služieb a spracúvaných údajov,

b) bolo odberateľovi cloudových služieb na základe žiadosti umožnené úplné skopírovanie jeho údajov na ďalšie použitie, pričom podmienky, lehoty a výstupné formáty údajov sú obsahom dohody o poskytovanej úrovni cloudových služieb, pričom lehota na skopírovanie údajov sa v dohode nedohodne na dlhšie ako tri mesiace; takými údajmi sa rozumejú údaje, ktoré do cloud computingu vložil alebo si nastavil odberateľ cloudových služieb na základe dohody o poskytovanej úrovni cloudových služieb,

c) bolo odberateľovi cloudových služieb umožnené úplné vymazanie jeho údajov, a to vrátane všetkých kópií a záloh v cloud computingu, pričom pri ukončení zmluvného vzťahu s odberateľom cloudových služieb sa takéto vymazanie zabezpečuje bezodkladne bez nutnosti osobitnej žiadosti odberateľa cloudových služieb; takéto vymazanie sa netýka údajov, pri ktorých to podmienky podľa osobitného predpisu neumožňujú alebo pre ktoré je to v príslušnej dohode o poskytovanej úrovni cloudových služieb dohodnuté inak, pričom lehota pre úplné vymazanie údajov sa v dohode o poskytovanej úrovni cloudových služieb nedohodne na dlhšie ako tri mesiace, a

d) bolo súčasťou dohody o poskytovanej úrovni cloudových služieb vyhlásenie poskytovateľa cloudových služieb o súlade s príslušnými štandardmi podľa tohto výnosu, a to v rozpise podľa jednotlivých štandardov.

§ 56

Vytváranie a rozvoj cloud computingu

Štandardom pre vytváranie a rozvoj cloud computingu v správe povinnej osoby je vytváranie a rozvoj architektúry cloud computingu podľa prílohy č. 7.

§ 57

Používanie cloudových služieb

(1) Štandardom pre používanie cloudových služieb je používanie

a) cloudových služieb informačnými systémami verejnej správy iba z takého cloud computingu, ktorý preukázateľne dodržiava požiadavky štandardu pre správu cloud computingu, a to aj ak správa nie je zabezpečovaná povinnou osobou,

b) iba takej dohody o poskytovanej úrovni cloudových služieb, ktorá je dohodou o poskytovanej úrovni cloudových služieb podľa § 2 písm. z),

c) cloudových služieb informačnými systémami verejnej správy, iba ak

Formátované: Zarážka: Vľavo: 0 cm, Opakovaná zarážka: 0,63 cm, Zarážky: Nie je v 2,54 cm

1. má poskytovateľ cloudových služieb sídlo alebo miesto podnikania v členskom štáte Európskej únie, zmluvnej strane Dohody o Európskom hospodárskom priestore alebo krajine s primeranou ochranou osobných údajov podľa osobitného predpisu,[11a)]
2. má sprostredkovateľ cloudových služieb sídlo alebo miesto podnikania v členskom štáte Európskej únie, zmluvnej strane Dohody o Európskom hospodárskom priestore alebo krajine s primeranou ochranou osobných údajov podľa osobitného predpisu,[11a)] ak sa predpokladá alebo existuje zmluvný vzťah so sprostredkovateľom cloudových služieb,
3. sa spracúvanie a uloženie údajov uskutočňuje na území členských štátov Európskej únie, zmluvných strán Dohody o Európskom hospodárskom priestore a krajín s primeranou ochranou osobných údajov podľa osobitného predpisu[11a)] a
4. je pre takýto informačný systém verejnej správy vypracovaná a udržiavaná aktuálna klasifikácia údajov, ktoré obsahuje.

(2) Obmedzenie podľa odseku 1 písm. c) prvého až tretieho bodu sa nevzťahuje na otvorené údaje.

Štandardy pre formáty elektronických dokumentov podpísateľných elektronickým podpisom

§ 57a
Prijímanie a čítanie podpísaných elektronických dokumentov

Štandardom pre prijímanie a čítanie podpísaných elektronických dokumentov je prijímanie a čítanie

a) priamo podpísaných elektronických dokumentov vo formáte textových súborov Portable Document Format vo verzii A-1a (PDF/A-1a) a podľa technickej normy,[11b)]
b) externe podpísaných elektronických dokumentov vo formáte
   1. textových súborov Portable Document Format vo verzii A-1a (PDF/A-1a) a podľa technickej normy,[11c)]
   2. textových súborov podľa § 19 písm. a) tretieho bodu,
   3. grafických súborov podľa § 20 písm. a) druhého bodu,
c) elektronických dokumentov vo formáte jazyka pre prenos dátových prvkov podľa § 12 v štruktúre podľa prílohy č. 11 (ďalej len „kontajner XML údajov“), pričom ak nejde o vyplnené údaje elektronického formulára, zároveň
   1. sa v tomto elektronickom dokumente používa znaková sada podľa § 13 písm. c),
   2. schéma tohto elektronického dokumentu je vytvorená v súlade s § 13 písm. a),
   3. transformácia tohto elektronického dokumentu je vytváraná v súlade s § 13 písm. d) a zabezpečuje vytvorenie podpisovej prezentácie vo formáte podľa prílohy č. 3 bodu 2.6.7,
d) iných formátov elektronických dokumentov ako uvedených v písmenách a) až c), ak sa na tom zasielateľ a prijímateľ dohodnú,

---

[11a)] § 31 ods. 1 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z.

[11b)] ETSI TS 103 172 V2.2.2: Elektronické podpisy a infraštruktúry (ESI): Základný profil PadES.

[11c)] ISO 19005-1:2005: Správa dokumentov. Formát súboru elektronického dokumentu pre dlhodobé uchovávanie. Časť 1: Používanie PDF 1.4 (PDF/A-1).

e) formátov elektronických dokumentov podľa písmen a) až d) s obmedzeniami podľa osobitného predpisu,[11d)]

f) podpísaných elektronických dokumentov podľa písmena a) podpísaných viacerými osobami, iba ak tieto osoby podpísali rovnaký informačný obsah elektronického dokumentu,

g) podpísaných elektronických dokumentov podľa písmena a) podpísaných viacerými osobami, ak niektorá z týchto osôb podpísala iný informačný obsah tohto elektronického dokumentu ako ostatné osoby, ak sa o tom zasielateľ a prijímateľ dohodnú.

§ 57b

Prijímanie a čítanie podpisových kontajnerov

Štandardom pre prijímanie a čítanie podpisových kontajnerov je prijímanie a čítanie

a) podpisového kontajneru vo formáte Associated Signature Containers (.asics, .scs, .asice, .sce) podľa technických noriem,[11e)] a to aj viacnásobne vnoreného, pričom ak ide o degradovaný Associated Signature Containers, tento je vo verzii podľa § 25 ods. 1 písm. a) prvého bodu,

b) iných formátov podpisových kontajnerov ako uvedených v písmene a), ak sa na tom zasielateľ a prijímateľ dohodnú.

§ 57c

Vytváranie podpisových kontajnerov a podpísaných elektronických dokumentov

Štandardom pre vytváranie podpisových kontajnerov a podpísaných elektronických dokumentov podpísaných elektronickým podpisom alebo elektronickou pečaťou je

a) pri úkonoch súvisiacich s poskytovaním elektronických služieb verejnej správy, povinným poskytovaním informácií podľa osobitných predpisov,[3)] alebo ak je podpísaním vykonaná autorizácia podľa osobitného predpisu,[11f)] používanie formátov podľa § 57a písm. a) až e) a § 57b písm. a),

b) používanie iných formátov ako uvedených v písmene a), napríklad ostatných formátov podľa § 19 až 24, ak sa na tom všetky strany príslušnej komunikácie dohodnú, s vedomím možných škôd a nezrovnalostí v ďalšom konaní vyplývajúcich z takého postupu,

c) spravidla nevytváranie viacnásobne vnorených podpisových kontajnerov.

[11d)] § 3 ods. 5 vyhlášky Národného bezpečnostného úradu č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku.

[11e)] ETSI TS 102 918 Elektronické podpisy a infraštruktúry (ESI): Formát Associated Signature Containers (ASiC), ETSI TS 103 174 V2.2.1: Elektronické podpisy a infraštruktúry (ESI): Základný profil Associated Signature Containers (ASiC).

[11f)] Zákon č. 305/2013 Z. z.

§ 57d

Identifikovanie formátu podpísaného elektronického dokumentu, identifikovanie formátu podpisového kontajneru a identifikovanie podpísaného elektronického dokumentu

(1) Štandardom pre identifikovanie formátu podpísaného elektronického dokumentu sú hodnoty identifikátorov podľa prílohy č. 12 prvého bodu.
(2) Štandardom pre identifikovanie formátu podpisového kontajneru sú hodnoty identifikátorov podľa prílohy č. 12 druhého bodu.
(3) Štandardom pre identifikovanie podpísaného elektronického dokumentu je identifikátor hašovacej funkcie použitej na výpočet digitálneho odtlačku a hodnota digitálneho odtlačku z podpísaného elektronického dokumentu podľa osobitného predpisu.[11g)]

§ 57e

Prostriedky týkajúce sa overovania a vytvárania zaručeného elektronického podpisu a zaručenej elektronickej pečate

Štandardom pre používanie prostriedkov týkajúcich sa overovania a vytvárania zaručeného elektronického podpisu a zaručenej elektronickej pečate je používanie certifikovaných prostriedkov podľa osobitného predpisu[11h)] pri overovaní platnosti alebo vytváraní zaručeného elektronického podpisu alebo zaručenej elektronickej pečate prostredníctvom informačného systému orgánu verejnej moci.

Štandardy pre základné číselníky

§ 57f

Základné číselníky

(1) Štandardom pre základné číselníky zverejňované alebo sprístupňované pre použitie inými informačnými systémami verejnej správy je

a) používanie dátovej štruktúry základného číselníka podľa prílohy č. 13,
b) vytváranie názvu základného číselníka tak, aby stručne a zrozumiteľne popisoval obsah tohto číselníka,
c) vytváranie položiek základného číselníka najmenej v slovenskej jazykovej verzii,
d) vytváranie jazykových verzií položky základného číselníka prostredníctvom príslušných dátových prvkov ako súčasti príslušnej položky základného číselníka,
e) poskytovanie jazykovej verzie, iba ak sú hodnoty dátového prvku „Názov položky“ všetkých položiek základného číselníka vyplnené v príslušnej jazykovej verzii,

---

[11g)] Vyhláška Národného bezpečnostného úradu č. 135/2009 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky) v znení neskorších predpisov.

[11h)] § 24 ods. 8 zákona č. 215/2002 Z. z. v znení neskorších predpisov.

f) vytváranie dátových prvkov položky základného číselníka typov „Lokalizovaný dátový prvok“ a „Lokalizovaný dátový prvok s históriou“ v jednom jazyku jedenkrát,

g) nevytváranie súčasne účinných dátových prvkov položky základného číselníka typov „Dátový prvok s históriou“ a „Lokalizovaný dátový prvok s históriou“,

h) upravovanie alebo pridávanie hodnôt dátových prvkov položky základného číselníka typov „Dátový prvok s históriou“ alebo „Lokalizovaný dátový prvok s históriou“, ktorá nadobudla účinnosť ukončením účinnosti príslušného pôvodného dátového prvku, ak existuje, a vznikom nového dátového prvku s upravenou alebo pridanou hodnotou a s účinnosťou nasledujúcou bezprostredne po ukončenej účinnosti pôvodného dátového prvku na úrovni sekúnd; ak ide o nový dátový prvok, ktorý položka dovtedy neupravovala alebo ktorý nemal hodnotu, účinnosť sa určuje na základe vlastného uváženia,

i) upravovanie alebo pridávanie hodnôt dátových prvkov položky základného číselníka iného typu ako uvedeného v písmene h) priamym prepísaním existujúcich hodnôt alebo pridaním nových hodnôt,

j) nemožnosť vymazania položky základného číselníka, ktorá nadobudla účinnosť, a to ani po jej ukončení,

k) vytváranie položky základného číselníka s obnovenou účinnosťou zmenou dátového prvku „Účinný od“ tejto položky postupom podľa písmena h); iné dátové prvky tejto položky sa vtedy neupravujú,

l) poskytovanie všetkých povinných dátových prvkov položky základného číselníka podľa prílohy č. 13 s vyplnenými hodnotami, a to pre všetky položky základného číselníka,

m) vytváranie identifikátorov položiek základného číselníka ako referencovateľných identifikátorov, a to podľa zoznamu referencovateľných identifikátorov zverejňovaného prostredníctvom webového sídla ministerstva.

(2) Štruktúru základného číselníka podľa odseku 1 písm. a) je možné na vnútorné účely použitia iným informačným systémom verejnej správy v tomto informačnom systéme rozšíriť o nové atribúty alebo položky; takto upravený číselník sa označuje ako rozšírený číselník, pričom tento číselník nie je základným číselníkom.

(3) Základné číselníky sa v elektronických formulároch používajú spravidla so všetkými položkami, ktoré sú v období účinnosti príslušného elektronického formulára legislatívne uznateľné.

(4) Pri prenose dátových prvkov alebo ich atribútov, ktorých hodnoty sú založené na základných číselníkoch, sa používa najmenej hodnota dátového prvku základného číselníka „kód položky“ alebo identifikátor položky základného číselníka.

Záverečné, prechodné a zrušovacie ustanovenia

§ 58
Prechodné ustanovenia k úpravám účinným od 15. júla 2010

Ustanovenia § 50 a prílohy č. 4 sa vzťahujú na projekty, ktoré sú súčasťou programu a ktorých prípravná fáza sa začne najskôr od 15. júla 2014.

§ 59
Prechodné ustanovenia k úpravám účinným od 15. marca 2014

~~(2)~~(3) Pri odosielaní alebo zverejňovaní textových súborov vrátane ich zverejňovania na webovom sídle sa pred 15. marcom 2015 postupuje podľa predpisu účinného do 14. marca 2014, pričom súbory zverejnené v tomto formáte pred 15. marcom 2015 je možné takto zverejňovať aj po 14. marci 2015.

~~(3)~~(4) Pri zverejňovaní grafických súborov vo formáte Shockwave Flash (.swf) vrátane ich zverejňovania na webovom sídle sa pred 15. marcom 2015 postupuje podľa predpisu účinného do 14. marca 2014, pričom súbory zverejnené v tomto formáte pred 15. marcom 2015 je možné takto zverejňovať aj po 14. marci 2015.

§ 60

Prechodné ustanovenia k úpravám účinným od 15. marca 2015

(1) Súbory obsahujúce tabuľky zverejnené podľa predpisu účinného do 14. marca 2015 je možné takto zverejňovať aj po 14. marci 2015.

(2) Audio a video súbory zverejnené na webovom sídle podľa predpisu účinného do 14. marca 2015 je možné takto zverejňovať aj po 14. marci 2015.

(3) Audio a video streaming zverejnený na webovom sídle podľa predpisu účinného do 14. marca 2015 je možné takto zverejňovať aj po 14. marci 2015.

§ 60a

Prechodné ustanovenia k úpravám účinným od 15. septembra 2015

Zverejňovanie, sprístupňovanie a používanie základných číselníkov pre iné informačné systémy verejnej správy sa do 15. októbra 2015 uskutočňuje v dátovej štruktúre základného číselníka aj podľa právnych predpisov účinných do 14. októbra 2014.

§ 61

Prechodné ustanovenia k úpravám účinným od 15. marca 2016

(1) Pri používaní sieťového protokolu Internet Protocol vo verzii 4 (IP v4), sieťového protokolu Internet Protocol vo verzii 6 (IP v6) a sieťovej technológie Dual stack sa pred 15. marcom 2016 postupuje podľa predpisu účinného do 14. marca 2014.

(2) Súbory obsahujúce tabuľky vytvorené informačnými systémami verejnej správy pred 15. marcom 2016 je možné ponechať v pôvodnom formáte aj po 14. marci 2016.

§ 62
Zrušovacie ustanovenie

Zrušuje sa výnos Ministerstva financií Slovenskej republiky z 9. júna 2010 č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy.

§ 63
Účinnosť

Tento výnos nadobúda účinnosť 15. marca 2014 okrem § 19 písm. c), d), f) a g), § 21, písm h), § 22 písm. d) až g), § 23, § 24 písm. b) až f) a h), § 44, § 47 písm. e) a f), § 48, § 51 ods. 2, § 52, § 53, § 55 až 57, bodov 1.6, 3.1, 5.4, 7.3 a 9.4 prílohy č. 1 a prílohy č. 3 až 10, ktoré nadobúdajú účinnosť 15. marca 2015 a okrem § 3, písm. a) a b), § 19 písm. h) a § 24 písm. g), ktoré nadobúdajú účinnosť 15. marca 2016.

Čl. II

Tento výnos [novela] nadobúda účinnosť 15. októbra 2014 okrem bodov

10 [§ 18 písm. g],

11 [novela § 19 písm. a) druhého a tretieho bodu],

13 [novela § 20 písm. a) druhého bodu],

§ 57a až 57d v bode 25,

bodov 28 [„V prílohe č. 2 sa v celom texte pred slovo „číselník“ vo všetkých tvaroch vkladá slovo „základný“ v príslušnom tvare“],

29 [„V prílohe č. 2 sa v celom texte vypúšťajú slová „Uvádza sa atribút KODPOL.“, „(atribút POZN)“ a „Uvádza sa položka NAZSKS.“],

31 [„V prílohe č. 2 bode D.1.2.9 Základné imanie (Equity) tabuľke Popisné atribúty riadku Definícia a stĺpci Hodnota sa slovo „soby“ nahrádza slovom „osoby“ “],

38 [Nový bod 2.3.2 v prílohe č. 3],

39 [„V prílohe č. 3 bode 2.3.3 sa slovo „prvým“ nahrádza slovom „druhým“.“] a

79 [Nové prílohy č. 11 až 13], ktoré nadobúdajú účinnosť 15. októbra 2015.

V. z. Peter Pellegrini
minister financií