Vyhláška č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody

ze dne 21. července 2016

Ministerstvo pro místní rozvoj stanoví podle § 213 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, (dále jen „zákon“):

§ 1
Předmět úpravy

(1) Tato vyhláška upravuje

a) podmínky poskytování a přístupu k dokumentům a informacím prostřednictvím elektronického nástroje,

b) podmínky doručování prostřednictvím elektronického nástroje,

c) podmínky podávání, příjmu a otevírání nabídek, žádostí o účast a návrhů v soutěži o návrh prostřednictvím elektronického nástroje,

d) požadavky na provádění elektronických úkonů při zadávání veřejných zakázek,

e) požadavky na pořizování záznamů o elektronických úkonech,

f) podmínky pro vydání certifikátu shody,

g) náležitosti a platnost certifikátu shody,

h) požadavky na funkční vlastnosti elektronického nástroje a prostředí, ve kterém má být elektronický nástroj provozován ve vztahu k certifikaci elektronického nástroje, a

i) technické náležitosti profilu zadavatele.

(2) Tato vyhláška se použije na právní vztahy, které nejsou upraveny přímo použitelným předpisem Evropské unie v oblasti služeb vytvářejících důvěru pro elektronické transakce1.

§ 2
Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) certifikačním auditem proces ověřování shody elektronického nástroje prováděný subjektem posuzování shody akreditovaným vnitrostátním akreditačním orgánem na základě jiného právního předpisu nebo podle přímo použitelného předpisu Evropské unie v oblasti akreditace a dozoru2 (dále jen „certifikační orgán“),

b) certifikačními pravidly souhrn podmínek a předpokladů, za nichž bude proveden certifikační audit, stanovených certifikačním orgánem,

c) certifikátem veřejného klíče datová zpráva, která důvěryhodným způsobem spojuje veřejný klíč zadavatele se zadavatelem, slouží k přenášení veřejného klíče a může sloužit k ověřování identity zadavatele a adresy jeho internetových stránek,

d) časovou informací zaznamenání data a času elektronického úkonu s uvedením hodiny, minuty a sekundy,

e) elektronickou adresou místo pro příjem zpráv v rámci elektronického nástroje,

f) funkcionalitou souhrn funkčních vlastností elektronického nástroje, které slouží k realizaci elektronických úkonů, a které jsou vymezeny v příloze k této vyhlášce,

g) prostředím podmínky, za kterých je elektronický nástroj provozován, které jsou stanoveny v příloze k této vyhlášce,

h) soukromým klíčem zadavatele jedinečná elektronická data, která jednoznačně odpovídají veřejnému klíči zadavatele a slouží zadavateli k odšifrování obsahu nabídky,

i) systémovým stavem stav, ve kterém se v daném okamžiku nachází elektronický nástroj, a který může nabývat hodnot

   1. v provozu,
   2. mimo provoz,
   3. omezení funkcionality neumožňující realizovat elektronické úkony, které jinak prostřednictvím elektronického nástroje realizovat lze,

j) veřejným klíčem zadavatele jedinečná elektronická data, která jednoznačně odpovídají soukromému klíči zadavatele a slouží dodavateli k zašifrování obsahu nabídky.

§ 3
Podmínky poskytování a přístupu k dokumentům a informacím na profilu zadavatele

(1) Zadavatel zajistí, aby se každý mohl vhodnou formou ujistit o jeho identitě ve smyslu přímo použitelného předpisu Evropské unie v oblasti služeb vytvářejících důvěru pro elektronické transakce3.

(2) Uveřejní-li zadavatel informace, zadávací dokumentaci nebo další dokumenty na svém profilu zadavatele, zajistí, aby

a) byly chráněny proti neoprávněné změně,

b) byly po stanovenou dobu nepřetržitě přístupné na profilu zadavatele a

c) byly uveřejněny bez požadavků na registraci či jakoukoliv identifikaci osoby, která k informacím, zadávací dokumentaci nebo dalším dokumentům přistupuje.

§ 4

Podmínky doručování prostřednictvím elektronického nástroje

(1) Doručením prostřednictvím elektronického nástroje je okamžik přijetí datové zprávy na elektronickou adresu adresáta či adresátů datové zprávy v elektronickém nástroji.

(2) O doručení prostřednictvím elektronického nástroje musí být pořízen záznam o elektronickém úkonu podle § 7.

§ 5

Šifrování a podávání nabídek v elektronické podobě

(1) Ustanovení této vyhlášky týkající se nabídky se použijí obdobně pro předběžnou nabídku, žádost o účast, žádost o zařazení do systému kvalifikace, žádost o účast nebo návrh v soutěži o návrh a podávání aukčních hodnot.

(2) Ve formuláři nebo ve výzvě, jejíž náležitosti jsou stanoveny v příloze č. 6 k zákonu, zadavatel uveřejní elektronickou adresu pro podávání nabídky.

(3) Nabídky musí být v elektronickém nástroji chráněny šifrováním jejich obsahu v souladu s požadavky stanovenými touto vyhláškou. To neplatí v případě podávání aukčních hodnot za podmínky, že je v souladu s touto vyhláškou zajištěno zachování důvěrnosti obsahu nabídky.

(4) Zadavatel zajistí, aby

a) veřejný klíč zadavatele určený k šifrování obsahu nabídek odpovídal soukromému klíči zadavatele,

b) nebylo možné bez vynaložení nepřiměřeného úsilí certifikát veřejného klíče padělat,

c) nebylo možné bez vynaložení nepřiměřeného úsilí soukromý klíč zadavatele padělat a

d) soukromý klíč zadavatele byl zajištěn proti ztrátě a neoprávněnému přístupu po celou dobu platnosti odpovídajícího certifikátu veřejného klíče.

(5) Zadavatel poskytuje dodavatelům za účelem šifrování obsahu nabídky certifikát veřejného klíče prostřednictvím svého profilu zadavatele, případně internetových stránek elektronického nástroje nebo zasláním na základě vyžádání.

(6) Je-li stanovena lhůta pro podání nabídky, zadavatel zajistí, aby nabídka podaná na adresu podle odstavce 2

a) před uplynutím stanovené lhůty byla dále zpracována v souladu s touto vyhláškou a uložena v nezměněné podobě do doby jejího otevření; zároveň bude dodavateli na jeho elektronickou adresu odeslána informace o tom, že jeho nabídka byla přijata, a

b) po uplynutí stanovené lhůty byla označena jako podaná po lhůtě, a současně bylo dodavateli odesláno na jeho elektronickou adresu oznámení o této skutečnosti.

(7) Podání nabídky musí být v elektronickém nástroji opatřeno záznamem časové informace podle § 8.

§ 6
Podmínky pro odšifrování nabídek

(1) Zadavatel nebo osoby oprávněné k otevírání nabídek zajistí před otevřením nabídek odšifrování obsahu nabídek s využitím soukromého klíče zadavatele.

(2) Zadavatel zajistí, aby odšifrování i otevření nabídek s využitím soukromého klíče zadavatele prováděly oprávněné osoby tak, aby

a) odšifrování a otevření bylo provedeno vždy za účasti dvou nebo více oprávněných osob,

b) nebylo možné použít soukromý klíč zadavatele k odšifrování nabídek jiným způsobem, než za účasti oprávněných osob.

(3) Zadavatel zajistí, aby elektronický nástroj neumožnil odšifrování a otevření nabídky před lhůtou stanovenou k jejímu otevření. Čas odšifrování a otevření nabídky musí být v elektronickém nástroji v souladu s § 7 zaznamenán.

(4) Zadavatel zajistí, že nabídka zůstane po jejím otevření uložena v elektronickém nástroji v zašifrované podobě, v jaké byla zadavateli doručena. Zadavatel zároveň uloží nabídku v nešifrované podobě nebo jiným způsobem, který umožní přístup k obsahu nabídky po celou dobu stanovenou v § 216 odst. 1 zákona nezávisle na platnosti šifrovacího certifikátu.

§ 7
Pořizování záznamů o elektronických úkonech

(1) Zadavatel zajistí pořízení záznamů o provedených elektronických úkonech, veškerých dalších činnostech a systémovém stavu elektronického nástroje. Součástí tohoto záznamu musí být alespoň

a) určení elektronického úkonu nebo další činnosti elektronického nástroje,

b) čas provedení elektronického úkonu podle § 8,

c) jednoznačná identifikace osoby, která elektronický úkon provedla,

d) jednoznačná identifikace automatizované činnosti, kterou byl proveden elektronický úkon,

e) záznam o případném chybovém výsledku elektronického úkonu,

f) záznam o systémovém stavu elektronického nástroje, byl-li elektronický nástroj mimo provoz nebo byla-li omezena funkcionalita, v důsledku čehož nebylo možné realizovat elektronické úkony, které jinak prostřednictvím elektronického nástroje realizovat lze.

(2) Záznam uvedený v odstavci 1 písm. e) a f) obsahuje alespoň popis stavu a časovou informaci o začátku a konci stavu podle § 8.

(3) Záznamy musí být v elektronickém nástroji chráněny proti neoprávněnému přístupu, změně a zničení.

§ 8
Zaznamenávání časové informace

(1) Časová informace zaznamenávaná v elektronickém nástroji musí být poskytovaná operačním systémem navázaným na zdroj reprodukující světový koordinovaný čas UTC v České republice.

(2) Synchronizace času měřeného operačním systémem podle odstavce 1 s koordinovaným světovým časem se provádí alespoň jedenkrát za 24 hodin v průběhu zadávacího řízení.

(3) Synchronizace času musí být zajištěna i v případě výskytu přestupné sekundy.

§ 9
Certifikát shody

(1) Certifikační orgán posuzuje shodu elektronického nástroje z hlediska funkcionality elektronického nástroje a z hlediska prostředí, ve kterém je elektronický nástroj provozován. Podrobné požadavky týkající se funkčních vlastností elektronického nástroje a prostředí, ve kterém má být elektronický nástroj provozován, jsou uvedeny v příloze k této vyhlášce.

(2) Elektronické nástroje se pro účely posuzování shody elektronického nástroje z hlediska funkcionality dělí na elektronické nástroje splňující požadavky

a) na profil zadavatele,

b) pro elektronickou realizaci zadávacích řízení,

c) pro elektronickou aukci,

d) pro rámcové dohody,

e) pro dynamický nákupní systém,

f) pro elektronickou realizaci soutěží o návrh,

g) pro elektronický katalog.

(3) Certifikát shody musí obsahovat alespoň

a) identifikační údaje certifikačního orgánu, který certifikát shody vydal,

b) identifikační údaje žadatele a identifikační číslo osoby, bylo-li žadateli přiděleno,

c) obchodní označení a verzi elektronického nástroje,

d) uvedení skupin elektronických nástrojů v členění podle odstavce 2, pro které byl elektronický nástroj certifikován,

e) datum vydání certifikátu shody,

f) dobu platnosti certifikátu shody a

g) podpis osoby oprávněné jednat za certifikační orgán.

(4) Certifikát shody vydává certifikační orgán v listinné podobě nebo v elektronické podobě, a to v českém jazyce. Certifikát shody prokazuje, že v rozsahu funkčních vlastností a údajů uvedených v certifikátu shody splňuje elektronický nástroj požadavky stanovené zákonem a touto vyhláškou.

§ 10
Podmínky pro vydání certifikátu shody

(1) Žádost o vydání certifikátu shody podává žadatel certifikačnímu orgánu. Žadatel prokazuje v žádosti a následném certifikačním auditu shodu elektronického nástroje s požadavky stanovenými právními předpisy ve vztahu k funkcionalitě elektronického nástroje a ve vztahu k prostředí, v němž je elektronický nástroj provozován. Shodu elektronického nástroje prokáže žadatel, pokud elektronický nástroj splňuje alespoň požadavky stanovené v příloze k této vyhlášce.

(2) Pokud má elektronický nástroj platný certifikát shody ve vztahu k funkcionalitě a ve vztahu k prostředí a je provozován jinou osobou než žadatelem, kterému byl certifikát shody vydán, prokazuje tato jiná osoba jako žadatel certifikačnímu orgánu pouze splnění požadavků ve vztahu k prostředí.

(3) Certifikační orgán vydá certifikát shody pro elektronický nástroj, pokud byla zjištěna shoda elektronického nástroje s požadavky uvedenými v příloze k této vyhlášce, a to v rozsahu zjištěné shody. Certifikační orgán není oprávněn vydat certifikát shody pro elektronický nástroj nad rámec podané žádosti o vydání certifikátu shody.

§ 11
Náležitosti žádosti o vydání certifikátu shody

(1) V žádosti o vydání certifikátu shody uvede žadatel své identifikační údaje a identifikační číslo osoby, bylo-li žadateli přiděleno.

(2) V případě, že žadatelem o vydání certifikátu shody je osoba, která není výrobcem elektronického nástroje, uvede žadatel v žádosti o vydání certifikátu shody identifikační údaje výrobce v rozsahu podle odstavce 1.

(3) V žádosti o vydání certifikátu shody uvede žadatel obchodní označení a verzi elektronického nástroje a uvede v souladu s § 9 odst. 2 rozsah požadované certifikace funkčních vlastností elektronického nástroje.

(4) Žadatel v případě žádosti o vydání certifikátu shody ve vztahu k funkcionalitě elektronického nástroje v příloze žádosti předloží

a) popis naplnění obecných a specifických požadavků na funkční vlastnosti elektronického nástroje podle přílohy k této vyhlášce,

b) uživatelskou příručku popisující postup realizace jednotlivých druhů postupů podle zákona tak, jak jsou uvedeny v části II. přílohy k této vyhlášce ve schématu Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality, a

c) návrhy testovacích scénářů k ověření funkčních vlastností jednotlivých druhů postupů podle zákona tak, jak jsou uvedeny v části II. přílohy k této vyhlášce ve schématu Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality.

(5) Žadatel v případě žádosti o vydání certifikátu shody ve vztahu k prostředí, v němž je elektronický nástroj provozován, v příloze žádosti předloží popis naplnění požadavků na prostředí elektronického nástroje podle části XI. přílohy k této vyhlášce.

(6) V případě uvedeném v § 10 odst. 2 musí být přílohou žádosti o vydání certifikátu shody kopie platného listinného certifikátu shody nebo stejnopis platného elektronického certifikátu shody, který byl pro elektronický nástroj vydán.

§ 12
Platnost certifikátů shody

(1) Pokud žadatel prokáže certifikačnímu orgánu shodu elektronického nástroje s požadavky kladenými na funkční vlastnosti u elektronického nástroje, má certifikát shody v rozsahu funkčních vlastností elektronického nástroje podle § 9 odst. 2 uvedených v certifikátu shody platnost 6 let ode dne jeho vydání.

(2) Pokud žadatel prokáže certifikačnímu orgánu shodu elektronického nástroje s požadavky kladenými na prostředí, v němž je nebo má být elektronický nástroj provozován, má certifikát shody v rozsahu údajů uvedených v certifikátu shody, které se týkají prostředí, platnost 3 roky ode dne jeho vydání. Uplynutím uvedené doby není dotčena platnost certifikátu shody v rozsahu údajů týkajících se funkčních vlastností daného elektronického nástroje.

(3) Platnost certifikátu shody osvědčujícího soulad s požadavky kladenými na funkční vlastnosti elektronického nástroje je možné na žádost žadatele prodloužit o dalších 6 let a soulad s požadavky kladenými na prostředí o další 3 roky, a to i opakovaně.

(4) Dojde-li ke změně funkčních vlastností či prostředí elektronického nástroje oproti funkčním vlastnostem či prostředí elektronického nástroje, na základě kterých byl certifikát shody vydán, a tato změna by mohla mít za následek neprokázání shody s požadavky stanovenými právními předpisy ve stanoveném rozsahu, žadatel oznámí do 15 dnů ode dne, kdy ke změně došlo, tuto skutečnost certifikačnímu orgánu a současně předloží návrh opatření k nápravě. V opačném případě certifikační orgán odejme certifikát shody, případně změní jeho rozsah, pokud to změna vlastností či podmínek provozu elektronického nástroje umožňuje.

(5) Certifikační orgán dále odejme nebo změní certifikát shody v případě, že žadatel

a) nesplňuje podmínky pro vydání certifikátu shody, nebo

b) použil jako podklady pro vydání certifikátu shody doklady či informace, které se ukázaly jako nepravdivé či neúplné.

(6) Certifikační orgán odejme certifikát shody i z jiných důvodů na základě písemné žádosti žadatele.

(7) Žadatel je oprávněn podat návrh na změnu rozsahu certifikátu shody. V takovém případě prokáže žadatel certifikačnímu orgánu pouze splnění požadavků, kterých se změna týká.

§ 13

Přechodné ustanovení

Certifikáty shody vydané podle vyhlášky č. 9/2011 Sb., kterou se stanoví podrobnější podmínky týkající se elektronických nástrojů a úkonů učiněných elektronicky při zadávání veřejných zakázek a podrobnosti týkající se certifikátu shody, jsou použitelné pouze pro účely dokončení řízení podle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění účinném do dne nabytí účinnosti zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

§ 14

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. října 2016.

Ministryně:

Ing. **Šlechtová** v. r.

Příloha

SPECIFIKACE POŽADAVKŮ PRO PROKAZOVÁNÍ SHODY ELEKTRONICKÝCH NÁSTROJŮ

I. Seznam použitých zkratek a pojmů

Zákon	Zákon č. 134/2016 Sb., o zadávání veřejných zakázek
Pracovník	zaměstnanec žadatele nebo i jiná osoba, která se podílí na provozování elektronického nástroje
Automaticky provedený elektronický úkon	elektronický úkon ve vztahu k zadávacímu řízení provedený elektronickým nástrojem
Otevřený formát	formát podle § 18 odst. 2 vyhlášky č. 168/2016 Sb., o uveřejňování formulářů pro účely zákona o zadávání veřejných zakázek a náležitostech profilu zadavatele
PKI	Public Key Infrastructure: v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie
Zabezpečený dokument	dokument s omezeným přístupem podle stanovených přístupových oprávnění
Oprávněná osoba	statutární orgán zadavatele nebo jím pověřená osoba na základě plné moci či vnitřních předpisů

II. Úvodní ustanovení

Pro získání certifikátu shody musí žadatel o certifikaci elektronického nástroje poskytnout informace o sobě a o elektronickém nástroji podle § 11 této vyhlášky a prokázat splnění

1. obecných požadavků podle části III., a to bez ohledu na to, pro jaké funkcionality elektronických nástrojů žadatel žádá o vydání certifikátu shody,
2. specifických požadavků podle částí IV. až X., a to v rozsahu funkcionalit elektronického nástroje podle § 9 odst. 2 této vyhlášky, pro které žadatel žádá o vydání certifikátu shody,
3. požadavků na prostředí podle části XI., a to bez ohledu na to, pro jaký rozsah funkcionalit elektronického nástroje žadatel žádá o vydání certifikátu shody.

Rozsah certifikace shody elektronického nástroje ve vazbě na rozsah funkcionality elektronického nástroje je uveden na schématu Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality. Certifikace bude vždy prováděna pro elektronické úkony vymezené funkcionalitami, které žadatel uvede v žádosti o vydání certifikátu.

Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality

Druh postupu podle zákona		Požadované funkcionality elektronických nástrojů podle § 9 odst. 2 této vyhlášky
Uveřejňování informací a dokumentů na profilu zadavatele podle § 214 zákona		1 - elektronické nástroje splňující požadavky na profil zadavatele
Zadávací řízení podle § 3 zákona	zjednodušené podlimitní řízení	1 - elektronické nástroje splňující požadavky na profil zadavatele 2 - elektronické nástroje splňující požadavky pro elektronickou realizaci zadávacích řízení
	otevřené řízení	
	užší řízení	
	jednací řízení s uveřejněním	
	jednací řízení bez uveřejnění	
	řízení se soutěžním dialogem	
	řízení o inovačním partnerství	
	koncesní řízení	
	řízení pro zadání veřejné zakázky ve zjednodušeném režimu	
Zvláštní postupy podle části šesté zákona	rámcová dohoda	1 - elektronické nástroje splňující požadavky na profil zadavatele 2 - elektronické nástroje splňující požadavky pro elektronickou realizaci zadávacích řízení 4 - elektronické nástroje splňující požadavky pro rámcové dohody
	dynamický nákupní systém	1 - elektronické nástroje splňující požadavky na profil zadavatele 2 - elektronické nástroje splňující požadavky pro elektronickou realizaci zadávacích řízení 5 - elektronické nástroje splňující požadavky pro dynamický nákupní systém
	soutěž o návrh	1 - elektronické nástroje splňující požadavky na profil zadavatele 6 - elektronické nástroje splňující požadavky pro elektronickou realizaci soutěží o návrh
Hodnocení nabídek s využitím elektronické aukce podle § 120 a 121 zákona		3 - elektronické nástroje splňující požadavky pro elektronickou aukci
Předložení nabídky formou elektronického katalogu		7 - elektronické nástroje splňující

podle § 215 zákona	požadavky pro elektronický katalog

Po ověření správnosti předložené dokumentace provede certifikační orgán na místě fyzické ověření shody tvrzení v dokumentaci s reálnou funkcionalitou elektronického nástroje.

Certifikační orgán provádějící certifikaci elektronických nástrojů má právo v případě pochybností o dostatečnosti předložených podkladů požadovat jejich doplnění.

III. Obecné technické požadavky na funkční vlastnosti pro všechny elektronické nástroje (0)

Obecné technické požadavky představují minimální úroveň, kterou musí elektronický nástroj splňovat. Elektronický nástroj může zajistit naplnění jednotlivých požadavků technicko-technologicky pokročilejším řešením/opatřením. Ověření shody elektronického nástroje bude certifikačním orgánem prováděno vždy v oblasti splnění obecných technických požadavků, a dále v oblasti požadavků pro jednotlivé skupiny elektronických nástrojů, přičemž budou akceptována i pokročilejší řešení/opatření.

Zaznamenání času elektronického úkonu (0.A)

Elektronický nástroj zajistí, aby zaznamenání času elektronického úkonu bylo provedeno připojením elektronického časového razítka k datové zprávě.

Pořízení záznamu o elektronickém úkonu (0.B)

Elektronický nástroj zajistí, aby veškeré záznamy o elektronických úkonech obsahovaly

1. jednoznačné určení daného konkrétního úkonu v rámci organizace zadavatele,
2. identifikaci osoby, která elektronický úkon provedla v případě, že jde o úkon učiněný konkrétní fyzickou osobou a nejedná se o úkon provedený automaticky elektronickým nástrojem (např. příjem nabídek),
3. záznam, že provedený elektronický úkon byl učiněn automatizovaně elektronickým nástrojem,
4. záznam informací o nestandardním výsledku úkonu za účelem shromáždění všech nezbytných podkladů pro dohledání příčiny vzniku a vyhodnocení dopadu chyby, pokud nastala při provedení úkonu chyba a
5. zaznamenání času elektronického úkonu podle oddílu 0.A.

Řízení přístupu v rámci zadávacích postupů (0.C)

Elektronický nástroj zajistí, aby řízení přístupu v rámci zadávacích postupů bylo zaznamenáváno a provedeno v souladu s § 7 odst. 1 písm. c) této vyhlášky jednou z následujících variant:

Pro profil zadavatele:

1. požadavky na řízení přístupu jsou stanoveny pouze pro zadavatele v rozsahu pořízení záznamů o elektronickém úkonu podle oddílu 0.B.

Pro ostatní zadávací postupy:

1. autentizace a autorizace přistupující osoby je založena na zadání jména a hesla.

   Zadavatel před vydáním jména a hesla pro přistupující osobu ověří, že o ně žádá oprávněná osoba a tato své oprávnění žadateli jednoznačně prokáže. Zadavatel osobě, která neprokáže, že je oprávněnou osobou, jména a hesla pro přistupující osoby nevydá. Zadavatel musí zajistit, aby distribuce jména a hesla přistupujícím osobám proběhla přiměřeně bezpečným způsobem,
2. autentizace a autorizace přistupující osoby je založena na certifikátu veřejného klíče přistupující osoby nebo
3. autentizace a autorizace přistupující osoby je založena i na jiných technologiích; vždy však musí probíhat prokazatelně, přiměřeně bezpečným způsobem a musí jednoznačně identifikovat osobu, která elektronický úkon provedla.

Použití otevřených formátů datových zpráv (0.D)

Elektronický nástroj zajistí, aby formátem datových zpráv, které jsou vyměňovány během zadávacích postupů, byl otevřený formát datové zprávy.

Uchování dokumentace o veřejné zakázce (0.E)

Elektronický nástroj zajistí, aby dokumentace o veřejné zakázce byla uchovávána v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly podle oddílu 0.C. Elektronický nástroj musí zajistit, aby při uložení dokumentace do datového úložiště bylo k dokumentaci připojeno elektronické časové razítko.

Dokumenty o veřejné zakázce, které byly předloženy v šifrované podobě nebo obsahují důvěrné informace, musí být uchovávány v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly podle oddílu 0.C. Dokumenty mohou být uchovávány ve své šifrované podobě. Pokud jsou dokumenty uchovávány v šifrované podobě (na bázi technologie PKI), musí zadavatel bezpečně uchovávat soukromý klíč zadavatele, odpovídající veřejnému klíči zadavatele, kterým byl dokument šifrován. Doba uchování soukromého klíče zadavatele musí odpovídat době uchování dokumentů. Současně zadavatel uloží dokument v nešifrované podobě nebo jiným způsobem, který umožní přístup k obsahu dokumentu po celou dobu stanovenou v § 216 odst. 1 zákona nezávisle na platnosti šifrovacího certifikátu.

Elektronický nástroj musí k ukončené veřejné zakázce umožnit kompletní export všech:

1. záznamových souborů,
2. automaticky generovaných dokumentů,
3. ručně vložených dokumentů,
4. datových zpráv,
5. strukturovaných dat podle přílohy č. 8 k vyhlášce č. 168/2016 Sb., o uveřejňování formulářů pro účely zákona o zadávání veřejných zakázek a náležitostech profilu zadavatele a
6. metadat.

Exportovaný soubor k ukončené veřejné zakázce musí mít formu jednoho souboru ve formátu zip, rar nebo 7z opatřeného kvalifikovaným elektronickým časovým razítkem a musí obsahovat i popis

exportované struktury v rozsahu nezbytném pro další automatizované zpracování elektronickými nástroji či informačními systémy.

Zajištění zákazu diskriminace (0.F)

Elektronický nástroj musí být provozován v takovém prostředí a takovým způsobem, aby užívání elektronického nástroje nebylo podmiňováno používáním běžně nedostupných nebo nákladných technologií, což by způsobilo vyloučení určitého dodavatele z účasti na zadávacích postupech.

Zpřístupnění informací pro využití elektronického nástroje (0.G)

Elektronický nástroj musí umožnit zadavateli poskytovat dodavatelům, kteří mají zájem účastnit se zadávacích postupů, aby měli k dispozici veškeré informace technické povahy, včetně případného kódování a šifrování, které jsou nezbytné pro komunikaci elektronickými prostředky, zejména pro elektronické podání nabídek, a to po celou dobu používání elektronického nástroje.

Zadavatel zajistí, aby informace pro využití elektronického nástroje byly aktuální a dostupné z nebo na úvodní straně profilu zadavatele.

Zajištění technické podpory a servisu elektronického nástroje (0.H)

Pro elektronický nástroj musí být zajištěna technická podpora a servis v takové míře, aby bylo možné zajistit řádný provoz elektronického nástroje a splnění ostatních požadavků této vyhlášky. Technická podpora a servis musí být poskytovány v rozsahu přiměřeném složitosti funkcionality elektronického nástroje.

Kontrola auditní stopy zakázky v elektronickém nástroji (0.1)

Elektronický nástroj musí umožnit pro účely kontroly oprávněné osobě zobrazit, případně exportovat či vytisknout všechny údaje pořízené podle oddílu 0.B za určené období, a to jak přes jednotlivé veřejné zakázky, tak i přes všechny veřejné zakázky zadavatele.

Důvěryhodné doručování v elektronickém nástroji (0.J)

Elektronický nástroj musí pro účely důvěryhodného doručování naplňovat požadavky nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, a to v rozsahu implementované funkcionality.

IV. Požadavky - profil zadavatele (1)

Zpřístupnění zabezpečeného dokumentu omezeným dálkovým přístupem (1.A)

O zpřístupnění zabezpečeného dokumentu zadavatelem omezeným dálkovým přístupem bude pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D. K dokumentu musí být řízený přístup. Řízení přístupu k dokumentu se musí řídit pravidly podle oddílu 0.C.

Zpřístupnění zabezpečeného dokumentu neomezeným dálkovým přístupem (1.B)

O zpřístupnění zabezpečeného dokumentu zadavatelem neomezeným dálkovým přístupem bude pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D.

Zpřístupnění dokumentu neomezeným dálkovým přístupem (1.C)

O zpřístupnění dokumentu zadavatelem neomezeným dálkovým přístupem bude pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D.

Náležitosti profilu zadavatele (1.D)

Profil zadavatele musí splňovat požadavky § 17 a následujících vyhlášky č. 168/2016 Sb., o uveřejňování formulářů pro účely zákona o zadávání veřejných zakázek a náležitostech profilu zadavatele.

Dále musí profil zadavatele splňovat požadavky vyhlášky č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti).

Profil zadavatele musí neomezeným a přímým dálkovým přístupem zpřístupnit základní informace o veřejné zakázce v rozsahu a struktuře podle přílohy č. 8 k vyhlášce č. 168/2016 Sb., o uveřejňování formulářů pro účely zákona o zadávání veřejných zakázek a náležitostech profilu zadavatele.

V. Požadavky - elektronická realizace zadávacích řízení (2)

Odeslání šifrované datové zprávy (2.A)

Přípustné formáty odesílané datové zprávy musí stanovit zadavatel. Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D. Elektronický protokol použitý k přenosu datové zprávy stanoví zadavatel. Příjemce datové zprávy musí odesílateli poskytnout certifikát veřejného klíče. Datová zpráva musí být šifrována veřejným klíčem příjemce. Pokud je zpráva odesílána zadavatelem, musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Odeslání otevřené datové zprávy (2.B)

Přípustné formáty odesílané datové zprávy stanoví zadavatel. Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D. Elektronický protokol použitý k přenosu datové zprávy stanoví zadavatel. Pokud je zpráva odesílána zadavatelem, musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Příjem otevřené datové zprávy (2.C)

Při příjmu datové zprávy musí zadavatel respektovat formát a elektronický protokol příchozí zprávy. Pokud je zpráva přijímána zadavatelem, musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Odeslání datové zprávy v rámci organizace zadavatele (2.D)

Formát datové zprávy odesílané v rámci organizace zadavatele bude zvolen podle potřeb zadavatele. Zadavatel vždy zvolí takový formát, který ochrání dokument proti neoprávněné změně. Elektronický protokol použitý k přenosu datové zprávy bude zvolen podle potřeb zadavatele. Zadavatel určí, zda datová zpráva bude šifrována a určí pravidla, jaký klíč bude používán k šifrování. O odeslání datové zprávy musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Příjem datové zprávy v rámci organizace zadavatele (2.E)

V případě šifrované datové zprávy zadavatel stanoví pravidla určující, zda bude datová zpráva odšifrována. O příjmu datové zprávy musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Příjem šifrované datové zprávy (2.F)

Pokud je datová zpráva odšifrována, o odšifrování musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B. Zadavatel uloží datovou zprávu v nešifrované podobě nebo jiným způsobem, který umožní přístup k obsahu datové zprávy po celou dobu stanovenou v § 216 odst. 1 zákona nezávisle na platnosti šifrovacího certifikátu.

Příjem a uložení nabídky (2.G)

Datová zpráva nabídky nesmí být do doby otvírání nabídek odšifrována. Musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B. V průběhu příjmu nabídky nesmí být pořízeny žádné kopie datové zprávy nabídky.

Elektronický nástroj zajistí, aby po příjmu datové zprávy nabídky neprodleně následovalo bezpečné uložení datové zprávy nabídky. Bezpečné uložení datové zprávy nabídky musí být provedeno způsobem, aby přístup zadavatele k šifrované nabídce, uložené v datovém úložišti, nebyl možný před uplynutím lhůty pro podání nabídek.

Elektronický nástroj zajistí, aby datová zpráva nabídky byla uložena takovým způsobem, aby byl zjistitelný pokus o přístup k uložené nabídce před termínem otevírání nabídek. Při jakémkoli takovém pokusu o přístup k nabídce před termínem otevírání nabídek musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Otevírání nabídek podaných elektronickými prostředky (2.H)

Elektronický nástroj zajistí, aby otevření nabídek podaných elektronickými prostředky bylo provedeno jednou z následujících variant:

1. otevření nabídky podané elektronickými prostředky bude provedeno způsobem navazujícím na příjem nabídky podle oddílu 2.H. Přístup k šifrované nabídce uložené v datovém úložišti bude proveden součinností minimálně dvou osob, resp. i většího počtu osob, stanoví-li tak zadavatel,

s neúplnými právy přístupu k uložené nabídce. Kombinací přístupových práv těchto osob bude umožněn přístup k uložené nabídce. Nabídka pak bude odšifrována soukromým klíčem zadavatele příslušejícím veřejnému klíči zadavatele, který byl použit k šifrování datové zprávy nabídky nebo

2. otevření nabídky podané elektronickými prostředky bude provedeno způsobem, navazujícím na příjem nabídky podle oddílu 2.H. Šifrovaná datová zpráva nabídky je odšifrována součinností osob, majících přístup k soukromým klíčům zadavatele příslušejícím veřejným klíčům zadavatele, které byly použity k šifrování datové zprávy nabídky.

Pokud elektronický nástroj automaticky po otevření nabídky uloží odšifrovanou nabídku k zakázce, provede o tom záznam podle oddílu 0.B. Elektronický nástroj uloží nabídku v nešifrované podobě nebo jiným způsobem, který umožní přístup k obsahu nabídky po celou dobu stanovenou v § 216 odst. 1 zákona nezávisle na platnosti šifrovacího certifikátu.

Jednání komise / zadavatele (2.I)

Elektronický nástroj umožní, aby jako součást záznamu o jednání komise / zadavatele byl zadavatelem vložen dokument zápisu z jednání. Musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

VI. Požadavky - elektronická aukce (3)

Identifikace účastníků aukce (3.A)

Elektronický nástroj nesmí umožnit v průběhu zadávacího řízení až do ukončení elektronické aukce, aby se mohli její účastníci vzájemně identifikovat. O přidělení anonymního identifikátoru účastníku elektronické aukce musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Výzva k zadání nových aukčních hodnot (3.B)

Přípustné formáty odesílané výzvy stanoví zadavatel. Formát dokumentu musí odpovídat požadavkům podle oddílu 0.D. Elektronický protokol použitý k přenosu výzvy stanoví zadavatel. O odeslání výzvy účastníkům musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Matematický vzorec pro výpočet pořadí účastníků (3.C)

Elektronický nástroj musí zadavateli trvale poskytnout informaci o použitém matematickém vzorci, který se při elektronické aukci použije pro určení automatických změn pořadí na základě podaných nových aukčních hodnot. Tento vzorec musí zahrnovat všechna kritéria stanovená zadavatelem v elektronickém nástroji pro hodnocení nabídek.

Zpřístupnění informací během elektronické aukce (3.D)

Elektronický nástroj musí po celou dobu elektronické aukce účastníkovi elektronické aukce zpřístupnit informaci o jeho aktuálním pořadí. Elektronický nástroj musí umožnit poskytovat také další informace o aukčních hodnotách za předpokladu, že si to zadavatel vyhradil v zadávacích podmínkách a určil způsob jejich poskytnutí. Elektronický nástroj musí umožnit zadavateli zobrazit

účastníkům elektronické aukce kdykoli v průběhu elektronické aukce počet účastníků elektronické aukce.

VII. Požadavky - rámcové dohody (4)

Jednotná evidence (4.A)

Elektronický nástroj musí vést a zadavateli zobrazit jednotnou evidenci rámcových dohod s vazbou na plnění z těchto rámcových dohod. O každé změně v evidenci musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Načítání plnění (4.B)

Elektronický nástroj musí umožnit jednotlivé načítání dílčí veřejné zakázky po jejím zadání pro každou konkrétní rámcovou dohodu. O každém načítání musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Zakázka na základě rámcové dohody (4.C)

Elektronický nástroj musí pro zvolenou rámcovou dohodu umožnit zadavateli zadávat jednotlivé zakázky. O nabídce musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

VIII. Požadavky - dynamický nákupní systém (5)

Jednotná evidence (5.A)

Elektronický nástroj musí vést a zadavateli zobrazit jednotnou evidenci zavedených dynamických nákupních systémů s vazbou na plnění z těchto dynamických nákupních systémů. O každé změně v evidenci musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Načítání plnění (5.B)

Elektronický nástroj musí umožnit jednotlivé načítání dílčí veřejné zakázky po jejím zadání pro každý konkrétní dynamický nákupní systém. O každém načítání musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Kategorie (5.C)

Elektronický nástroj musí umožnit zadavateli rozdělit připravovaný dynamický nákupní systém do kategorií. O definovaných kategoriích a jejich změnách musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Zakázka v **rámci dynamického nákupního systému (5.D)**

Elektronický nástroj musí pro zvolený dynamický nákupní systém umožnit zadavateli zadávat jednotlivé zakázky. O nabídce musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Evidence dodavatelů v dynamickém nákupním systému (5.E)

Elektronický nástroj musí v rámci jednotlivých dynamických nákupních systémů umožnit zadavateli vést a zobrazit evidenci dodavatelů, kteří:

a) podali žádost o účast,

b) byli vyloučeni z účasti v dynamickém nákupním systému,

c) byli zařazeni do dynamického nákupního systému.

O každé změně v evidenci musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

IX. Požadavky - elektronická realizace soutěží o návrh (6)

Zpřístupnění návrhu v soutěži o návrh soutěžní porotě (6.A)

Elektronický nástroj musí zadavateli umožnit zpřístupnění návrhu v soutěži o návrh soutěžní porotě tak, aby pro osoby, jež jsou součástí soutěžní poroty, nebylo možné na základě informací poskytnutých elektronickým nástrojem identifikovat dodavatele, který návrh podal (dále jen „anonymizace návrhu“). K anonymizaci návrhu musí dojít až po otevření a odšifrování návrhu. Soutěžní porotě zpřístupní zadavatel anonymizovaný návrh v odšifrované podobě. O otevření, odšifrování a anonymizaci návrhu musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

Elektronický nástroj musí i po anonymizaci návrhu poskytnout zadavateli informaci o dodavateli, jež návrh podal.

O zpřístupnění návrhu v soutěži o návrh soutěžní porotě musí být pořízen záznam o elektronickém úkonu podle oddílu 0.B.

X. Požadavky - elektronický katalog (7)

Technické náležitosti elektronického katalogu (7.A)

Pro tvorbu elektronického katalogu se použije některý z následujících formátů:

a) pdf (Portable Document Formát),

b) PDF/A (Portable Document Format for the Long-term Archiving),

c) xml (Extensible Markup Language Document),

d) fo/zfo (602XML Filler dokument),

e) html/htm (Hypertext Markup Language Document),

f) odt (Open Document Text),

g) ods (Open Document Spreadsheet),

h) rtf (Rich Text Format),

i) doc/docx (MS Word Document),

j) xls/xlsx (MS Excel Spreadsheet),

k) další oborově obvyklé formáty s podporovaným a zdarma dostupným prohlížečem a editorem

daného formátu.

Formát (včetně použitých technických prostředků), obsah a strukturu elektronického katalogu definuje zadavatel v zadávací dokumentaci a stanoví, které údaje jsou určeny k vyplnění na straně dodavatele. Elektronický katalog vložený zadavatelem do elektronického nástroje musí umožňovat editaci na straně dodavatele a jeho odeslání elektronickými prostředky v zašifrované podobě jako nabídku či součást nabídky.

XI. Obecné požadavky na prostředí, v němž je elektronický nástroj provozován

1. Kvalita provozu elektronického nástroje

Základním kvalitativním požadavkem na provoz elektronického nástroje je prokázání důvěryhodnosti jeho provozování. Tato důvěryhodnost je měřena přes důvěrnost, dostupnost a integritu informací, které jsou prostřednictvím elektronického nástroje v daném prostředí zpracovávány. Měření kvality probíhá podle níže uvedených požadavků na systém řízení provozu elektronického nástroje, za který odpovídá žadatel. Žadatel pro potřeby certifikace prostředí prokáže plnění požadavků této vyhlášky.

2. Deklarace systému řízení

Žadatel musí stanovit politiku provozu elektronického nástroje, která bude obsahovat minimálně:

- Vymezení postupu zajišťování dostatečných zdrojů pro provoz elektronického nástroje vedením společnosti žadatele;
- Rozsah provozovaných funkčních vlastností elektronického nástroje;
- Výčet požadavků stanovených v zákoně, normativních a smluvních požadavků aplikovaných na provoz elektronického nástroje;
- Stanovení odpovědných rolí za provoz elektronického nástroje včetně jejich pravomocí a odpovědností;
- Vymezení postupu řízení služeb jiných stran, které mají dopad na provoz elektronického nástroje;
- Vymezení postupu pravidelného ohodnocování a řízení aktiv a rizik spojených s provozem elektronického nástroje;
- Vymezení kontrolních mechanismů k monitorování provozu elektronického systému a způsobu zajištění včasné a efektivní identifikace nových hrozeb a rizik.

3. Požadavky na řízení zdrojů

Žadatel musí určovat a zajistit dostatečné zdroje potřebné pro efektivní a účinný provoz elektronického nástroje. Zdroje pro účely tohoto standardu tvoří:

1. prostředí, ve kterém je elektronický nástroj provozován a které zahrnuje hardware, operační systémy a další systémové programové vybavení a prostory nezbytné pro zajištění požadovaných parametrů elektronického nástroje a
2. lidské zdroje, které jsou nezbytné pro provozování elektronického nástroje (správu

a obsluhu) v zamýšleném rozsahu a pro dodržování stanovených požadavků na elektronický nástroj. Žadatel musí specifikovat požadavky na řízení zdrojů (provozního prostředí a lidských zdrojů) a jeho části tak, aby bylo zajištěno, že elektronický nástroj plní stanovené požadavky při jeho provozování v provozním prostředí v zamýšleném rozsahu.

3.1. Požadavky na prostředí

Žadatel musí dokumentovaným způsobem stanovit požadavky na prostředí, a to zejména hardware, software a prostory nezbytné pro provozování elektronického nástroje v zamýšleném rozsahu. Musí vést záznamy o tom, že jsou tyto požadavky při provozu elektronického nástroje plněny. Rozsah požadavků je závislý na složitosti elektronického nástroje (tj. kompatibilitě funkcionality).

3.2. Požadavky na procesy řízení lidských zdrojů

Žadatel musí provést taková opatření v oblasti řízení lidských zdrojů, která minimalizují negativní vliv pracovníků na provoz elektronického nástroje ve stanoveném rozsahu při dodržení všech stanovených požadavků. Způsob naplnění níže uvedených požadavků musí být dokumentován a musí existovat záznamy jako důkazy o plnění požadavků.

Žadatel musí minimálně:

- Stanovit role, jejich popis, pracovní povinnosti, odpovědnosti a pravomoci;
- Stanovit požadavky na odbornou způsobilost pracovníka pro danou roli;
- Stanovit způsob ustanovení pracovníka do role a způsob jeho proškolení;
- Plánovat v pravidelných intervalech vzdělávací aktivity a následně je podle plánu realizovat;
- Stanovit pravidla uplatňování odpovědnosti a udělování sankcí za porušení stanovených povinností při provozu elektronického nástroje;
- Stanovit pravidla ukončení práce pracovníka v roli.

Před započetím práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje žadatel provádí výběr vhodných pracovníků do rolí podle požadavků na roli, stanovené odborné způsobilosti a dalších vlastností, které žadatel určí pro danou roli.

Před započetím práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje žadatel ověří kvalifikaci a proškolení nových pracovníků pro role nutné pro provozování elektronického nástroje, jejich odpovědnosti, pravomoci a požadavky na odbornou způsobilost, a to před ustanovením pracovníka do role.

Během práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje žadatel plánuje a zajišťuje vzdělávací aktivity, prostřednictvím nichž zajistí, že pracovníci trvale splňují požadavky na odbornou způsobilost stanovenou pro zastávanou roli. V případě, že jsou činnosti zajištěny smluvní stranou, žadatel vyžaduje naplnění tohoto požadavku po smluvní straně.

Žadatel řeší s pracovníkem případy porušení stanovených povinností při provozu elektronického nástroje v souladu se stanovenými pravidly uplatňování odpovědnosti a udělování sankcí.

Při ukončení práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje

Žadatel stanoví konkrétní časový plán pro řádný průběh ukončení práce pracovníka s elektronickým nástrojem (včetně ukončení případných smluvních vztahů), které zahrnují zejména odevzdání přidělených aktiv a odejmutí přístupových práv k elektronickému nástroji.

4. Systémové požadavky na elektronický nástroj

Prostřednictvím systémových požadavků na elektronické nástroje zajišťuje žadatel plnění požadavků stanovených v zákoně již v průběhu návrhu a vývoje elektronického nástroje a po celou dobu provozování elektronického nástroje.

4.1. Požadavky na řízení provozu

Žadatel musí dokumentovaným způsobem zabezpečit dostupnost, integritu a důvěrnost, a to aplikováním vybraných postupů mezinárodních norem v oblasti bezpečnosti informací a kvality služeb v IT, které jsou etalonem pro naplnění níže uvedených požadavků.

Žadatel musí v pravidelných intervalech, minimálně jednou ročně a při každé větší změně:

- Provádět, řídit a hodnotit aktiva a rizika;
- Zpracovávat a naplňovat plán zvládání rizik;
- Přehodnocovat již přijatá opatření;
- Provádět kontrolu a vyhodnocení procesů a činností prováděných jinými stranami, které mají dopad na provoz elektronického nástroje;
- Vytvářet, udržovat a řídit dokumenty a záznamy nezbytné pro provoz elektronického nástroje;
- Plánovat, realizovat, monitorovat a přezkoumávat postupy pro řízení provozu elektronického nástroje;
- Provádět interní audity a přezkoumání vedením včetně přezkoumání shody s požadavky zákona a jeho prováděcích předpisů a dalších normativních a smluvních závazků.

Dále musí:

- Řídit proces plánování změn provozu elektronického nástroje;
- Řídit proces provozu elektronického nástroje a poskytovat zadavateli operativní i pravidelné měsíční informace o stavu provozu včetně všech anomálií, nedostupností a dalších informací, které jsou z pohledu provozu elektronického nástroje pro zadavatele významné;
- Mít zpracovány a funkční plány kontinuity a dostupnosti;
- Řídit prostředky a kapacity v čase a místě tak, aby nedocházelo k ohrožení provozu elektronického nástroje;
- Prokazatelně seznamovat pracovníky zadavatele se změnami v provozu elektronického nástroje;

- Řídit vztahy se zadavateli i účastníky zadávacích řízení v rozsahu provozovaného elektronického nástroje;
- Řídit incidenty, problémy, konfigurace a změny a vést o nich prokazatelné záznamy.

4.2. Požadavky na kvalitu řešení

Pro potřeby certifikace je jako akceptovatelná úroveň provozu elektronického nástroje stanovena:

- Celková roční dostupnost elektronického nástroje je nejméně 98 %, přičemž jednotlivý výpadek provozu nesmí překročit 3 hodiny v pracovní dny a 12 hodin ve dnech pracovního volna;
- Zálohovací plán musí být nastaven tak, aby při jeho dodržování došlo v případě incidentu ke ztrátě dat v elektronickém nástroji maximálně jeden kalendářní den.

Poznámky pod čarou:

1 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

2 Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

3 Článek 45 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.