ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2019

Vyhlásené: 23. 2. 2019 Časová verzia predpisu účinná od: 1. 3.2019

41

VYHLÁŠKA
Úradu pre verejné obstarávanie

z 11. februára 2019,

ktorou sa ustanovujú podrobnosti o technických a funkčných požiadavkách pre nástroje a zariadenia používané na elektronickú komunikáciu vo verejnom obstarávaní

Úrad pre verejné obstarávanie podľa § 186 ods. 6 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení zákona č. 345/2018 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

(1) Nástroje a zariadenia podľa § 20 ods. 1 zákona (ďalej len „systém“) sú spôsobilé na elektronickú komunikáciu a výmenu informácií vo verejnom obstarávaní, ak umožňujú realizovať úkony v procese verejného obstarávania spôsobom ustanoveným v zákone a spĺňajú požiadavky ustanovené v § 20 zákona a v tejto vyhláške.

(2) Systémom je informačný systém, ktorý zabezpečuje elektronickú komunikáciu a výmenu informácií vo verejnom obstarávaní, funguje vo vyhovujúcom prostredí, je dostupný a je zdokumentovaný.

§ 2

(1) Fungovaním systému vo vyhovujúcom prostredí je prevádzkovanie systému v takom prostredí a takým spôsobom, aby používanie systému nebolo podmieňované použitím bežne nedostupných alebo neprimerane nákladných technológií, čo by spôsobilo neprimeranú prekážku v účasti záujemcu alebo uchádzača vo verejnom obstarávaní.

(2) Systém je dostupný, ak

a) funguje prostredníctvom siete internet nepretržite počas určenej doby jeho prevádzky okrem nepredvídateľných udalostí a plánovaných technických odstávok a

b) na jeho použitie postačuje aktuálna bezplatne poskytovaná a podporovaná verzia webového prehliadača bez potreby inštalácie osobitných aplikácií.

(3) Systém je zdokumentovaný, ak

a) existuje aktuálna administrátorská a prevádzková dokumentácia podľa osobitného predpisu[1]) a

b) existuje a je udržiavaná aktuálna používateľská príručka dostupná na webovom sídle prevádzkovateľa systému, ktorá podrobne opisuje všetky funkcionality systému alebo inak znázorňuje a vysvetľuje používanie systému a je k nej zabezpečený priamy a bezplatný prístup.

§ 3

Zabezpečenie riadenia prístupu k systému pozostáva z identifikácie a autentifikácie používateľa. Identifikácia a autentifikácia používateľa je založená minimálne na zadaní používateľovho mena a hesla, pričom distribúcia hesla musí byť vykonávaná hodnoverným spôsobom podľa osobitného predpisu.[2])

§ 4

(1) Požiadavky podľa § 20 ods. 11 písm. a) a g) zákona sa považujú za splnené, ak systém

a) vedie záznamy úkonov úplným, presným a neodstrániteľným spôsobom,

b) poskytuje záznam úkonov len s právami na čítanie a umožňuje jeho exportovateľnosť do formátov podľa osobitného predpisu[3]) a jeho exportovateľnosť na priamu tlač aj v podobe slovného opisu vykonaného úkonu a

c) vedie záznam úkonov v štruktúre

1. presný čas vykonania úkonu s uvedením dátumu, hodiny, minúty a sekundy,
2. jednoznačné určenie konkrétneho úkonu,
3. identifikácia používateľa informačného systému, ktorý úkon vykonal, alebo identifikácia systému, ktorý úkon vykonal,
4. IP (Internet Protocol) adresa, z ktorej pristupuje do systému používateľ informačného systému, ktorý úkon vykonal,
5. informácia o výsledku úkonu.

(2) Úkonom podľa odseku 1 sa rozumie aktivita osôb zapojených do verejného obstarávania v systéme alebo aktivita systému, ktorej uskutočnenie má alebo môže mať vplyv na priebeh alebo výsledok verejného obstarávania.

§ 5

(1) Na účely splnenia požiadaviek podľa § 20 ods. 11 písm. c) až f) zákona je potrebné, aby systém zabezpečoval

a) autorizáciu pristupujúcej osoby, ktorá je riadená pomocou roly alebo používateľských skupín, a

b) oddelenie roly.

(2) Oddelením roly sa najmä zabezpečuje, aby v systéme v rámci jednej roly nebolo možné vykonávať úkony v mene alebo v prospech inej roly.

§ 6

Systém zabezpečuje integritu a zachovanie dôvernosti údajov uvedených v ponuke, návrhu alebo žiadosti o účasť, ak

a) vytvára k predloženej ponuke, žiadosti o účasť alebo návrhu digitálny odtlačok vytvorený pomocou hašovacej funkcie SHA256 alebo vyššej a

b) komunikuje s používateľmi prostredníctvom protokolu Hypertext Transfer Protocol s použitím kryptografického protokolu podľa osobitného predpisu[4]) minimálne na strane webového servera, na ktorom je prevádzkovaný systém; certifikáty musia byť platné, vydané nezávislou certifikačnou autoritou, neboli odvolané a zodpovedajú všetkým doménovým menám, ktoré webové sídlo systému používa.