

INFORMAČNÍ LIST



Národní archiv

BULLETIN PRO OTÁZKY ELEKTRONICKÉ SPISOVÉ SLUŽBY A DOKUMENTŮ V DIGITÁLNÍ PODOBĚ

28. prosinec 2020

Ročník 2020

Částka 7

OBSAH

- č. 4/2020 Kontrola komponent ve validátoru SIP národního digitálního archivu
- č. 5/2020 Doporučení k vektorovým datovým formátům při příjmu/vyřazování
- č. 6/2020 Novela vyhlášky o významných informačních systémech (autor NÚKIB)

Přehled zkratk

- Příloha č. 1 k č. 4/2020 Formátová pravidla pro předávání souborů do archivu (*samostatný soubor*).
- Příloha č. 2 k č. 6/2020 Proces identifikace významného informačního systému (Schema-VIS_nova_3.0) (*samostatný soubor*).

Vydává Národní archiv jako účelové periodikum pro původce, archivy a dodavatele informačních systémů.
Další šíření dovoleno. Dostupné z <https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravnipuvodci/informacni-list> Informace a objednávka zasílání: infolist@nacr.cz.

ISSN 2694-6793

č. 4/2020

Kontrola komponent ve validátoru SIP národního digitálního archivu

V návaznosti na zveřejněná Pravidla vyplňování metadat komponent v balíčku SIP v bodě 3/2020 Informačního listu, částka 6/2020, sdělujeme, že od nejbližší nové verze validátoru SIP Národního archivu, přístupného na adrese <https://validatorsip.nacr.cz>, budou tato pravidla aplikována v nově zařazených kontrolách komponent a jejich metadat. Zatímco dosud byl u komponent pouze ověřován deklarovaný MIMETYPE vůči identifikovanému formátu (kontrola 16.4.), bude přehled pravidel obohacen **o novou kapitolu 27**, která bude obsahovat:

1. Kontroly metadat - vyplnění atributů prvku <nssess: Komponenta> **Pořadí, Verze, Druh**. Tyto kontroly se budou týkat digitálních dokumentů navrhovaných do výběru archiválií ve skartačním řízení i předávaných k trvalému uložení do archivu.
2. Kontroly, zda u dokumentu existuje verze komponenty, která odpovídá **Formátovým pravidlům pro předávání souborů do archivu**. Tzn. je porovnáván identifikovaný formát, deklarovaná **forma uchování** příslušné komponenty, případná souvislost s ostatními komponentami v dokumentu (např. pozdější verze originál ve výstupním datovém formátu po originálu) a Formátová pravidla pro předávání souborů. Tyto kontroly budou uplatněny pouze u digitálních dokumentů, uzavřených/vyřízených od 1. 8. 2012 včetně a předávaných k trvalému uložení do archivu.

Pro účely transparentního zveřejnění postupu kontrol identifikovaných souborů, byl vytvořen přehled formátů komponent (tzv. **Formátová pravidla pro předávání souborů do archivu**), který se stává součástí Přehledu pravidel Validátoru SIP a bude, spolu s validátorem SIP, průběžně aktualizován.

Jedná se o seznam formátů využívající primárně záznamy formátového registru PRONOM (<https://www.nationalarchives.gov.uk/PRONOM/Default.aspx>) s uvedením příslušného PUID (PRONOM Unique Identifier), MIMETYPE (pokud existuje), přípony (extenze), obecné kategorie formátu a doporučeného výstupního formátu (viz sloupce „Výstupní formát“ a „Výstupní formát alternativně I“ a „Výstupní formát alternativně II“).

Ve sloupci „Výstupní formát“ je vždy vyznačeno

- a) zda se jedná o výstupní datový formát podle § 23 Vyhlášky,
- b) výstupní datový formát vyplývající z Vyhlášky
- c) výstupní datový formát doporučený Národním archivem nebo
- d) informace, že lze daný formát ponechat (tzn. není nutné převádět do výstupního datového formátu).
- e) informace, že formát obsahuje adresáře nebo soubory, které je třeba rozbalit
- f) informace, že k dalšímu postupu v řízení je nutné individuální posouzení archivářem, který rozhodne, že daný formát lze přijmout k trvalému uložení (např. u formátů databází)

Ve sloupci „Výstupní formát alternativně I“ a „Výstupní formát alternativně II“ mohou být zaznamenány informace dle bodů b), c), d) a f).

Sloupec „Originál vždy (doporučeno)“ zahrnuje formáty, u kterých se doporučuje předat i originál/koncept v původním formátu (např. z důvodu možného strojového zpracování).

Pro snazší orientaci bude u chyb vyvolaných nesouladem v identifikaci formátu ve webovém validátoru <https://validatorsip.nacr.cz> vypsán identifikovaný formát a příslušný očekávaný formát, příp. akce „rozbalit“.

Upozorňujeme, že pro ověření MIMETYPE vůči formátovým registrům (kontrola č. 16.1.3) a kromě již aplikovaného porovnání s IANA byl v návaznosti na postup identifikace formátu pomocí nástroje DROID

<http://digital-preservation.github.io/droid/>, přidán i referenční registr PRONOM (<https://www.nationalarchives.gov.uk/PRONOM/Default.aspx>).

č. 5/2020

Doporučení k vektorovým datovým formátům při příjmu/vyřazování

Čím dál více veřejnoprávních původců je nuceno přijímat anebo přímo vyžaduje a pracuje s vektorovými datovými objekty, které jsou uloženy v proprietárních formátech, jako např. ESRI Arc/View ShapeFile SHP a jiné. Národní archiv v takových případech doporučuje upřednostnit otevřený formát Geography Markup Language GML. V případech, kdy taková možnost není, je nezbytné, aby balíček SIP s tímto typem dat obsahoval kromě originálního datového souboru i jeho podobu ve výstupním formátu dle §23 vyhlášky. Např. v případech, kdy vektorová data jsou statická, je vhodné vytvořit jednoduchý model nebo náhled ve formátu PDF/A, aby bylo dlouhodobě poznat, co originální soubor zobrazoval. Pokud původce nedisponuje software, který vytvoření takového modelu/náhledu umožňuje, doporučujeme požadovat doplnění podání nebo přímo zveřejnit tento požadavek na úřední desce.

č. 6/2020

Novela vyhlášky o významných informačních systémech (autor NÚKIB)

Regulace zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“) stanovuje povinnosti pouze vybraným osobám, které spravují nebo provozují informační systémy s vyšší mírou důležitosti pro chod státu, život jeho občanů a poskytování služeb těmto občanům.

Významné informační systémy představují jeden z těchto typů systémů a jejich důležitost je dána tím, že podporují výkon veřejné moci orgány veřejné moci. Pro určení, zda je systém užívaný při činnostech orgánu veřejné moci natolik zásadní, že by měl být identifikován jako významný informační systém a následně by mělo dojít k plnění povinností daných ZKB slouží právě vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích (dále jen „vyhláška o VIS“). **Od 1. 1. 2021 pak začíná platit její novelizované znění (novelu provádí vyhláška č. 360/2020 Sb.), které má za cíl zpřesnit kritéria a proces identifikace významných informačních systémů, kterou provádějí na základě kritérií v ní obsažených samy orgány veřejné moci.**

Vyhláška o VIS i po své novele vyjímá ze své působnosti informační systémy obcí, těch se tedy bez ohledu na jejich velikost regulace vyhláškou o VIS nedotýká.

Nejzásadnější změnou vyhlášky o VIS je stanovení **závazného seznamu typových informačních systémů** v § 2 odst. 1 vyhlášky o VIS, **kteří jsou u organizačních složek státu, krajů a hlavního města Prahy považovány za významné informační systémy bez dalšího.** Jedinou podmínku pro jejich identifikaci u tohoto okruhu adresátů tak představuje, že **daný informační systém slouží pro výkon působnosti orgánu veřejné moci** a nejedná se tedy typicky o ty systémy, které podporují toliko vnitřní chod dané organizace nebo slouží k jiným účelům. Toto platí obecně pro veškeré významné informační systémy, tedy i pro ty, které mají být identifikovány ostatními orgány veřejné moci vyjma obcí. Vzhledem k nákladové náročnosti je však účinnost § 2 rozložena do 3 let, jak ilustruje následující tabulka.

V období od 1. ledna 2021 do 31. prosince 2021 se § 2 týká těchto systémů

Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění

- a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci, nebo
- b) kontrolní nebo inspekční činnosti anebo státního dozoru.

1. ledna 2022 jsou do § 2 doplněny následující systémy

- c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
- d) výkonu spisové služby, nebo
- e) vedení úřední desky způsobem umožňujícím dálkový přístup.

1. ledna 2023 jsou do § 2 doplněny následující systémy

- f) mezinárodní spolupráce, nebo
- g) zadávání veřejných zakázek.

Oproti původnímu znění vyhlášky o VIS je také nově stanovena **všem orgánům veřejné moci vyjma obcí povinnost vést seznam všech svých informačních systémů** a u každého z nich uvést, jak bylo posouzeno naplnění kritérií daných vyhláškou o VIS.

Proces identifikace významného informačního systému je pak možné zjednodušit následovně:

- Každý orgán veřejné moci vyjma obcí vytvoří seznam všech svých informačních systémů.
- U každého informačního systému jednotlivě posoudí, zda objektivně naplňuje zákonnou definici, přičemž zohlední obsah § 2 a § 3 vyhlášky o VIS.
 - Ustanovení § 2 vyhlášky VIS je určeno pouze organizačním složkám státu, krajům a hlavnímu městu Praze.
 - Ustanovení § 3 vyhlášky o VIS je určeno všem orgánům veřejné moci (uplatňují ho tedy pro své doposud podle § 2 neidentifikované systémy i organizační složky státu, kraje a hlavní město Praha)
- Orgán veřejné moci začne plnit povinnosti podle zákona o kybernetické bezpečnosti.
 - **Hlášení kontaktních údajů** (§ 16 ZKB), a to do 30 dnů od naplnění kritérií pro identifikaci
 - **Hlášení kybernetických bezpečnostních incidentů** (§ 8 ZKB), a to do 1 roku od naplnění kritérií pro identifikaci
 - **Implementace a provádění bezpečnostních opatření** (§ 4 ZKB), a to do 1 roku od naplnění kritérií pro identifikaci
 - **Provádění opatření** (§ 11 až § 14 ZKB), a to okamžitě po naplnění kritérií pro identifikaci

Bližší informace o institutu významného informačního systému a jeho identifikaci lze nalézt na webu Národního úřadu pro kybernetickou a informační bezpečnost. Je zde umístěn výkladový dokument „Průvodce identifikací významného informačního systému“, „Vzor seznamu informačních systémů orgánu veřejné moci“ a schéma „Proces identifikace významných informačních systémů“, které jsme rovněž zařadili do přílohy.

Výše popsané dokumenty jsou dostupné v části věnované významným informačním systémům na tomto odkaze: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

Zkratky

eSSL – elektronický systém spisové služby nebo informační systém spravující dokumenty

nařízení GDPR - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

nařízení eIDAS - 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

ISDS – informační systém datových schránek

ISSD – informační systém pro správu dokumentů

NSESSS – národní standard pro elektronické systémy spisové služby

SIP - informační balíček („Submission Information Package“) určený k exportu nebo přenosu entit z eSSL do digitálního archivu včetně balíčku tvořícího seznam dokumentů ke skartačnímu řízení

„Vyhláška“ – vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů

„Zákon“ – zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů

zákon č. 300/2008 Sb. – zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

zákon č. 297/2016 Sb. – zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Přílohy	Národní archiv - Informační list	Částka 7 (2020)
---------	----------------------------------	-----------------

Přílohy 1 a 2 jsou samostatné soubory