Návrh implementace § 12, 12a a 13 ZoPDS a souvisejících povinností

§ 12

Právo na elektronickou identifikaci a autentizaci

(1) Není-li v katalogu služeb pro využití digitální služby stanovena úroveň záruky prostředku pro elektronickou identifikaci, uživatel služby má právo provést svou identifikaci a autentizaci prostředkem pro elektronickou identifikaci podle své volby nejméně v úrovni značná.

(2) Uživatel služby má právo, aby před osobním provedením úkonu, pro který je v katalogu služeb uvedena možnost doplnění fyzického prokázání totožnosti autentizací s využitím dat potřebných pro elektronickou identifikaci a autentizaci, orgán veřejné moci vyžadoval autentizaci jako podmínku provedení digitálního úkonu. Orgán veřejné moci vystaví na žádost uživatele služby, který provedl autentizaci, potvrzení o autentizaci.

(3) Uživatel služby uplatní požadavek na vyžadování autentizace podle odstavce 2 u Agentury. Agentura zveřejní elektronický formulář k uplatnění požadavku na portálu veřejné správy.

(4) Agentura spravuje elektronickou aplikaci pro autentizaci podle odstavce 2. Agentura umožní využít aplikaci i při fyzickém prokazování totožnosti pomocí identifikačního dokladu vůči fyzické osobě nebo právnické osobě.

(5) Umožní-li fyzická osoba nebo právnická osoba doplnění fyzického prokázání totožnosti pomocí identifikačního dokladu autentizací s využitím dat potřebných pro elektronickou identifikaci a autentizaci spojených s identifikačním dokladem, vystaví na žádost toho, kdo provedl autentizaci, potvrzení o autentizaci.

§ 12a

(1) Uživatel služby má právo na informaci, zda kombinace identifikačních údajů, které mu o sobě poskytla fyzická osoba nebo které obdržel od jiné osoby na základě prokazatelného právního vztahu, který měl právo uzavřít, odpovídá kombinaci údajů vedených o fyzické osobě jako referenční údaje v registru obyvatel.

(2) Právo podle odstavce 1 uplatní uživatel služby u správce národního bodu pro identifikaci a autentizaci.

(3) Uživatel služby je povinen při uplatnění práva podle odstavce 1 prokázat správci národního bodu pro identifikaci a autentizaci svou totožnost a sdělit mu kombinaci poskytnutých identifikačních údajů v rozsahu

a) příjmení,

b) jméno, popřípadě jména,

c) adresa místa pobytu,

d) datum narození a

e) čísla a druhy identifikačních dokladů.

(4) Údaj podle odstavce 3 písm. c), d) nebo e) lze sdělit pouze společně s údaji podle odstavce 3 písm. a) a b).

(5) V případě, že kombinace identifikačních údajů, které uživateli služby o sobě poskytla fyzická osoba, odpovídá kombinaci údajů vedených o fyzické osobě jako referenční údaje v registru obyvatel, správce národního bodu pro identifikaci a autentizaci vydá uživateli služby bezvýznamový směrový identifikátor fyzické osoby. V opačném případě správce národního bodu pro identifikaci a autentizaci vyrozumí uživatele služby, že shoda kombinací údajů nebyla nalezena anebo odpovídá více fyzickým osobám. Pokud byla v rámci kombinace údajů podle věty první tohoto odstavce sdělena kombinace údajů podle odstavce 3 písmen a), b) a e), správce národního bodu pro identifikaci a autentizaci sdělí uživateli služby též údaje podle odstavce 3 písm. a), b) a e) ve tvaru odpovídajícím současnému stavu.

(6) Uživatel služby nesmí získaný bezvýznamový směrový identifikátor sdělovat třetím osobám s výjimkou orgánu veřejné moci.

(7) Informaci, zda kombinace identifikačních údajů, které uživateli služby o sobě poskytla fyzická osoba, odpovídá kombinaci údajů vedených o fyzické osobě jako referenční údaje v registru obyvatel, podá správce národního bodu pro identifikaci a autentizaci rovněž na základě sdělené kombinace poskytnutých identifikačních údajů vedených jako referenční údaje, jsou-li poskytnuté identifikační údaje ve tvaru předcházející současný stav a jsou-li vedeny v informačním systému evidence obyvatel, informačním systému cizinců, informačním systému evidence občanských průkazů nebo informačním systému evidence cestovních dokladů. S identifikačními údaji lze dále poskytnout údaj o rodném čísle, je-li veden v informačním systému evidence obyvatel nebo informačním systému cizinců.

(8) Právní nástupce uživatele služby má právo požádat o vytvoření nových bezvýznamových směrových identifikátorů fyzické osoby na základě předání seznamu bezvýznamových směrových identifikátorů fyzické osoby svého právního předchůdce správci národního bodu pro identifikaci a autentizaci.

§ 13

Právo na technologickou neutralitu

(1) Orgán veřejné moci zpřístupní digitální službu uživateli služby bez závislosti na konkrétní platformě či technologii, ledaže by takové řešení bylo nepřiměřeně ekonomicky náročné, nesplňovalo požadavky na bezpečnost informačního systému veřejné správy nebo mu bránil jiný právním předpisem chráněný veřejný zájem.

(2) Orgán veřejné moci poskytne uživateli výstupy digitální služby v otevřeném, a je-li to možné, též strojově čitelném formátu.

1 Předpoklady a souvislosti návrhu

Tento dokument vychází z následujících předpokladů:

1. Digitální a informační agentura (dále jen „DIA“) připravila tento dokument na základě vlastních zkušeností a diskuzí vedených v rámci meziresortní pracovní skupiny organizované DIA k výkladu zákona 12/2020 Sb., o právu na digitální služby (dále jen „ZoPDS“).

2. DIA není orgánem příslušným k poskytnutí závazného výkladu ZoPDS. Dokument tak přináší výhradně návrh řešení.

3. Dokument prezentuje návrh pro první etapu implementace ustanovení ZoPDS, který z pohledu některých orgánů veřejné moci (dále jen „OVM“) nemusí zcela bez dalšího naplňovat znění ZoPDS. Jde však o návrh řešení, který se za současného stavu relevantních právních předpisů a technických řešení jeví jako nejpřívětivější pro uživatele a jako jednoduché, účelné, efektivní a hospodárné z pohledu technického řešení pro OVM.

4. Je na odpovědnosti každého jednotlivému OVM, jaké řešení pro implementaci tohoto ustanovení zvolí, tedy zda bude v rámci první etapy implementace tohoto ustanovení následovat dále prezentovaný návrh řešení a následně hledat řešení, které bude z jeho pohledu vhodnější, anebo pro implementaci zvolí zcela jiné řešení.

5. Pokud s některým z dále prezentovaným závěrem nesouhlasil některý z členů meziresortní pracovní skupiny k výkladu ZoPDS, byl mu dán prostor v tomto dokumentu svůj odlišný závěr uvést.

2 Elektronická identifikace

Elektronickou identifikací je postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu. Obecně je upravena v 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 v České republice je upravena především v zákoně č. 250/2017 Sb., o elektronické identifikaci. Ten stanovuje pravidla a povinnosti mezi tzv. kvalifikovanými poskytovateli, kvalifikovanými správci, národním bodem pro identifikaci a autentizaci a uživateli využívající elektronickou identifikaci. Tyto pojmy vymezujeme dále:

- **Kvalifikovaný poskytovatel.** V terminologii někdy také označovaný jako SeP (z angl. Service provider) je každý, komu je zákonem nebo výkonem působnosti daná povinnost ověřovat totožnost uživatele svých služeb.
- **Kvalifikovaný správce.** V terminologii někdy také označovaný jako IdP (z angl. Identity provider) je pouze státní orgán nebo osoba, které byla udělena akreditace pro správu kvalifikovaného systému.
- **Kvalifikovaný systém.** Kvalifikovaným systémem je systém elektronické identifikace, který:
    - spravuje kvalifikovaný správce,
    - splňuje předpisy Evropské unie upravující minimální technické specifikace, normy a postupy pro úrovně záruky prostředků pro elektronickou identifikaci,
    - umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci,
    - osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání prostředku pro elektronickou identifikaci jsou spojeny s danou osobou,
    - používá pouze prostředek pro elektronickou identifikaci, který je spojen s osobou, kterou identifikuje.
- **Národní bod pro identifikaci a autentizaci.** Někdy též označovaný jako NIA (Národní identitní autorita) informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému. Funguje jako prostředník mezi kvalifikovanými poskytovateli a kvalifikovanými správci.

Z předchozích základních pojmů a pravidel vyplývá opakující se pojem elektronické identifikace, která ale není řešena jen v zákoně č. 250/2017 Sb., o elektronické identifikaci, ale i v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy, a dává uživatelům

informačních systémů veřejné správy možnost využívat jejich služeb tzv. přístupem se zaručenou identitou.

Přístupem se zaručenou identitou se myslí přístup do informačního systému veřejné správy nebo elektronické aplikace s využitím prostředku pro elektronickou identifikaci, při jehož vydání nebo v souvislosti s ním anebo v souvislosti s umožněním jeho využití byla totožnost osoby ověřena státním orgánem, orgánem územního samosprávného celku nebo orgánem veřejné moci, který není státním orgánem ani orgánem územního samosprávného celku, nebo který byl vydán v rámci kvalifikovaného systému elektronické identifikace.

Možnost daná zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, tedy dává teoreticky širší pole působnosti pro správce informačních systémů veřejné správy, jak umožnit uživatelům elektronickou identifikaci s tím, že jde použít pro předem stanovené úkony:

- Úkon, jehož náležitostí má být podpis toho, kdo jej činí, učiněný prostřednictvím informačního systému veřejné správy se považuje za podepsaný, umožňuje-li informační systém veřejné správy prokázání totožnosti toho, kdo úkon činí, s využitím elektronické identifikace, autorizaci úkonu tím, kdo úkon činí, a zpětné prokázání projevu vůle toho, kdo úkon činí.
- Osoba, která je držitelem prostředku pro elektronickou identifikaci, který umožňuje přístup se zaručenou identitou, je oprávněna obstarat si s využitím tohoto prostředku výstup z informačního systému veřejné správy, který je neveřejnou evidencí, rejstříkem nebo seznamem, který se jí přímo týká, nebo údaje vedené o ní v tomto informačním systému veřejné správy, a to i prostřednictvím portálu veřejné správy nebo s využitím národního bodu pro identifikaci a autentizaci. Správce portálu veřejné správy zveřejní na portálu veřejné správy informační systémy veřejné správy, z nichž lze výstup z informačního systému veřejné správy nebo údaje takto obstarat.
- Osoba, která je držitelem prostředku pro elektronickou identifikaci, který umožňuje přístup se zaručenou identitou, je oprávněna umožnit s využitím tohoto prostředku poskytnutí výstupu z informačního systému veřejné správy, který se jí přímo týká, nebo údajů vedených o ní v informačním systému veřejné správy jiné osobě anebo veřejnému orgánu.

Ač by tedy čistě z pohledu právních předpisů bylo možné pro definované situace v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy, využívat pro elektronickou identifikaci i jiné prostředky než ty, kterou jsou kvalifikovaným systémem dle zákona č. 250/2017 Sb., o elektronické identifikaci, nedává to pro využívání ve veřejné správě smysl. Pokud se má veřejná správa chovat hospodárně a efektivně, dává smysl využívat pouze kvalifikované systémy a národní bod pro identifikaci a autentizaci. Kvalifikovaných systémů je již dostatečné množství a uživatelé očekávají od veřejné správy jednotnost v jejich používání.

3 Právo na elektronickou identifikaci

3.1 Využívání elektronické identifikace v digitálních službách

Uživatel má právo na to, aby digitální služba, která vyžaduje ověřenou totožnost, využívala elektronickou identifikaci popsanou v předchozí kapitole. Správce dané služby má v tomto případě povinnost ohlásit do katalogu služeb, jakou úroveň důvěry od uživatele požaduje, aby ji mohl poskytnout. Pokud tak neučiní, považuje se za dostatečnou úroveň důvěry úroveň „značná“, tedy střední. Více o úrovních a poskytovaných prostředích je zde https://archi.gov.cz/nap:nia#seznam_poskytovatelu_identity_identity_provideridp

3.2 Ověření identity třetí osoby

Uživatel má právo, pokud zná identifikační údaje třetí osoby, aby si ověřil její identitu u Národního bodu pro identifikaci a autentizaci. Aby uživatel mohl tuto službu využít musí znát jméno a příjmení dané osoby v kombinaci buďto s adresou místa pobytu, datem narození nebo číslem a druhem identifikačního dokladu.

Pokud uživatel zadá takovou kombinaci údajů, která neodpovídá právě jedné osobě, bude mu poskytnuta odpověď, že na danou kombinaci existuje více osob a musí zadat další údaj. Teprve až kombinace údajů bude odpovídat právě jedné osobě, poskytne se uživateli výpis aktuálních údajů vedených v registru obyvatel k dané osobě ve stejné sadě, jaká byla poskytnuta pro ověření, a navíc mu bude sdělen tzv. bezvýznamový směrový identifikátor.

Tento identifikátor slouží pro budoucí jednoznačné ztotožnění, pokud se například změní původně známé údaje o osobě.

Pro veřejnou správu z tohoto ustanovení neplynou žádné implementační povinnosti, kromě informace, že se jedná o obecný způsob, jak nahrazovat a utlumovat využívání rodného čísla jako jedinečného identifikátoru pro systémovou i uživatelskou komunikaci https://archi.gov.cz/znalostni_baze:utlum_rc.

4 Fyzická identifikace

Mimo elektronickou identifikaci jsou zákonem uživateli dána i práva v případě fyzické identifikace (osobní provedení úkonu). Uživatel má právo pro ty úkony, u kterých je to v katalogu služeb uvedeno, aby se při jejich osobním provedení vyžadoval tzv. BOK (bezpečnostní osobní kód), který si může každý uživatel zvolit při vyzvedávání občanského průkazu.

Orgán veřejné moci, který toto chce toto právo uživateli umožnit, tedy nejprve musí označit dané úkony v katalogu služeb jako způsobilé pro doplnění prokázání totožnosti o BOK. Následně musí technicky zajistit propojení technické propojení s aplikací spravovanou Digitální a informační agenturou (Mobilní klíč eGovernmentu), který uživatel bude používat pro zadání BOK.

Uživateli se prostřednictvím formuláře na Portálu občana dává možnost udělit generální souhlas či nesouhlas s vynucováním BOK pro ty úkony, u kterých je v katalogu služeb uvedena možnosti využití BOK při osobním provedení.

Potvrzení o autentizaci, které má se vystavuje na žádosti uživatele při využití BOK pro osobní provedení úkonu nemá stanoven formát ani strukturu. Subjekty povinné vystavovat potvrzení po žádosti od uživatele by na něj měli minimálně uvést identifikaci uživatele, vystavovatele, datum provedení a identifikaci služby. Za vzor se může použít i předpis pro osvědčení podle § 5.

5 Technologická neutralita

Orgány veřejné moci nesmí své digitální služby vázat na konkrétní platformu či technologii, která by následně omezovala či nutila uživatele využívat tyto technologie a platformy. V ustanovení jsou dány výjimky z pohledu kybernetické bezpečnosti a nepřiměřené ekonomické náročnosti či dokonce veřejný zájem.

Výjimky jsou tedy dány jednak poměrně široce a velmi neurčitě. Samotná technologická a platformová neutralita je v celkové šíři prakticky nemožná bez toho, aniž by si celý technologický a platformový ekosystém nenavrhla veřejná správa sama. To by jednak byla ekonomicky velmi náročné a výsledek by nemusel znamenat stejnou či lepší uživatelskou spokojenost.

Hlavním cílem by tedy neměla být zcela platformová a technologická neutralita, ale využívání takových platforem a technologií, které se dají považovat za „de facto“ standardy, a které uživatelé znají či očekávají. Pokud například existuje uživatel, který využívá málo rozšířený operační systém a internetový prohlížeč nepodporující potřebné webové standardy pro zobrazení a vyplnění elektronické formuláře, nemůže se odvolávat na zajištění technologické a platformové neutrality, protože přizpůsobení se tomuto případu by bylo velmi ekonomicky náročné a mohlo by to ohrozit kybernetickou bezpečnost.

Naopak by se orgány veřejné správy měly vyvarovat nucenému využívání i „de facto“ standardů tam, kde nejsou nezbytné. Příkladem může být povinné připojení přílohy, která je ve formátu tabulkového procesoru s makry vytvořeném v programu Microsoft Excel. Tím, že orgán veřejné moci vyžaduje po uživateli, aby tuto přílohu připojil, porušil technologickou a platformovou neutralitu, protože i bez velkých ekonomických dopadů a bez ohrožení kybernetické bezpečnosti, lze tuto povinnost zpracovat jako elektronický formulář, který je součástí digitální služby.

Veškeré výstupy z digitální služby by následně měly být v otevřeném a strojově čitelném formátu. Tato povinnost se dá sloučit i do jednoho dokumentu, kdy očekáváme, že většina výstupů bude formou dokumentu ve formátu PDF, do kterého může být ve verzi 3A vložena příloha obsahující datovou strukturu ve formátu XML. Celý tento kontejner by tedy obsahoval jak lidsky čitelnou podobu výstupu digitální služby, tak strojově čitelný obsah, a zároveň by celý kontejner byl otevřeném formátu.

6 Návrhy na novelizaci ZoPDS

Bez návrhů na novelizaci.

7 Odlišné stanovisko členů meziresortní pracovní skupiny

Bez odlišného stanoviska.