

eGovernment bezpečně



Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude **trestně stíháno**.

Používání elektronické verze knihy je umožněno jen osobě, která ji legálně nabyla a jen pro její osobní a vnitřní potřeby v rozsahu stanoveném autorským zákonem. Elektronická kniha je datový soubor, který lze užívat pouze v takové formě, v jaké jej lze stáhnout s portálu. Jakékoliv neoprávněné užití elektronické knihy nebo její části, spočívající např. v kopírování, úpravách, prodeji, pronajímání, půjčování, sdělování veřejnosti nebo jakémkoliv druhu obchodování nebo neobchodního šíření je zakázáno! Zejména je zakázána jakákoliv konverze datového souboru nebo extrakce části nebo celého textu, umístování textu na servery, ze kterých je možno tento soubor dále stahovat, přitom není rozhodující, kdo takovéto sdílení umožnil. Je zakázáno sdělování údajů o uživatelském účtu jiným osobám, zasahování do technických prostředků, které chrání elektronickou knihu, případně omezují rozsah jejího užití. Uživatel také není oprávněn jakkoliv testovat, zkoušet či obcházet technické zabezpečení elektronické knihy.





Copyright © Grada Publishing, a.s.



Copyright © Grada Publishing, a.s.

Obsah

Úvodem	7
1. Informační systémy veřejné správy (ISVS).....	11
1.1 Možnost užití open source produktů v ISVS ve státní správě	22
2. Elektronické komunikace.....	27
3. Ochrana osobních údajů, implementace biometrických údajů v praxi.....	31
4. Elektronický podpis, elektronická značka, časové razítko	37
4.1 Certifikační autorita, certifikáty a časová razítka	40
5. Elektronická správní řízení, e-podatelný, e-volby	47
6. Dlouhodobé uchování elektronických dokumentů	55
7. Konverze dokumentů, zrovnoprávnění elektronické a papírové formy komunikace	71
8. Registry veřejné správy, potřeba sjednocení vládních informačních zdrojů	75
9. Informační audit a jeho principy.....	79
9.1 Základní okruhy auditu	81
9.2 Audit a bezpečnost	87
9.3 Audit pro eBusiness	93
10. Bezpečnost – ochrana utajovaných informací.....	97
11. Bezpečnost – komplexní zabezpečení informačních systémů	103
12. eCommerce, elektronická fakturace.....	109
13. Elektronické veřejné zakázky	113
14. Zahraniční zajímavosti v oblasti eGovernmentu.....	119
14.1 eGovernment v USA	122
14.2 eGovernment ve Velké Británii.....	123
14.3 eGovernment ve Francii.....	124
14.4 eGovernment v Belgii.....	127
14.5 eGovernment v Německu.....	128
14.6 eGovernment ve Finsku.....	128
14.7 eGovernment ve Švédsku	131
14.8 eGovernment v Nizozemí	132
14.9 eGovernment v Dánsku.....	133
15. eGovernment pro každého aneb „co bude dál“?.....	135
Použitá literatura.....	140
Obrázky	141
Tabulky	141
Kolektiv autorů	142
Seznam zkratk.....	144

Úvodem

Slovo eGovernment v České republice zdomácnělo, a tak se nikdo nediví, že ho slýchá téměř denně v politických debatách, laických i odborných diskuzích, na seminářích nebo ve školách. Jeho přesné vymezení a chápání je ovšem různé. I přesto, že vyhledavač Google nabídne na dotaz „eGovernment“ přes 400 tisíc odkazů, nalézt definici, která plně vystihuje rozsah eGovernmentu, není jednoduché. Uvádíme proto několik definic, které podle názoru autorského kolektivu nejlépe vystihují jeho podstatu.

Definice OSN

Trvalá povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a efektivních služeb, informací a znalostí. Praktická realizace toho nejlepšího, co může veřejná správa nabídnout.

Definice MVČR

eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy.

Pro potřeby této publikace je eGovernment třeba vymezit širěji než uvedené definice, a proto uvádíme **definici vlastní**:

eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.

Pod pojem eGovernment je zapotřebí zahrnout také legislativní prostředí, které umožňuje výměnu informací mezi orgány veřejné správy, občany a komerčními subjekty ve všech možných komunikačních směrech.

Pro lepší vysvětlení významu eGovernmentu uvádíme výčet oblastí a činností, jež jsou součástí eGovernmentu v České republice a které si dále podrobně představíme:

- informační systémy veřejné správy, open source,
- elektronická komunikace,
- ochrana osobních údajů, implementace biometrických údajů,
- elektronický podpis, elektronická značka,

- elektronická správní řízení, elektronická podání, e-podatelný, e-volby,
- dlouhodobé uchovávání elektronických dokumentů,
- konverze dokumentů,
- registry veřejné správy,
- informační audit,
- bezpečnost a ochrana utajovaných informací,
- bezpečnost – komplexní zabezpečení informačního systému,
- eCommerce,
- elektronické veřejné zakázky,
- zahraniční zajímavosti v oblasti eGovernmentu a
- novinky v oblasti eGovernmentu aneb co bude dál?

eGovernment je v současné době zakotven zákonnými a podzákonnými předpisy. Jejich velká složitost a rychlá proměnlivost však znesnadňuje uživateli rychle pochopit jejich význam a orientovat se v problematice. Cílem této publikace je podat přehled o současném stavu a budoucím vývoji eGovernmentu, podrobně vysvětlit související zákony a technologické možnosti. Pro lepší přehlednost a srozumitelnost textu je na konci každé kapitoly uveden zákonný rámec dané problematiky v legislativním okénku a následně technologický rámec v technologickém okénku. Problematika je vždy vysvětlena a jsou uvedeny praktické příklady jejího řešení, případně popis dostupných produktů.

Tato publikace podává přehled základních povinností a možností v oblasti eGovernmentu pro pracovníky v orgánech veřejné správy. Má také sloužit jako pomůcka pro studenty vysokých i středních škol zejména v akreditovaných oborech „Informatika“, „Veřejná správa“ nebo „Veřejná správa a regionální rozvoj“, které jsou orientovány na vzdělávání kvalifikovaných odborníků pro státní správu.

eGovernment se týká rovněž dodavatelů služeb veřejnoprávním institucím, zejména firem z oblasti informatiky. Tam, kde komerční subjekty vystačí pro svůj provoz s běžně dostupnými „balíčkovými softwary“, případně je provedena customizace SAPu nebo jiného podnikového softwaru, mají veřejnoprávní subjekty nároky na vývoj nových aplikací. Tyto aplikace se specializovanými funkcionalitami, které hradí a „konzumuje“ výhradně veřejná správa (specializovaný software pro ochranu utajovaných informací, registry, rejstříky či metainformační systémy) a které se vymykají běžně dodávanému softwaru, musí být vytvořeny v souladu s pravidly eGovernmentu.

Proto tuto publikaci mohou dobře využít pracovníci komerčních společností podnikajících v oblasti informačních technologií, vedoucí projektů, ekonomové

a další odborníci, kteří potřebují dobře porozumět legislativě a procesům uvnitř veřejné správy, aby zvládali zpracovat produkty vyhovující složitým zákonným podmínkám. Na základě praktických zkušeností autorů můžeme říci, že při akceptaci softwaru pro státní správu mnohdy dojde na „lámání chleba“ právě při porovnání souladu s legislativou. Přestože je aplikace rychlá, funkční a moderní, nemusí být pro orgán veřejné správy přijatelná z legislativního hlediska. Tato publikace se snaží představit požadavky na produkty pro státní správu tak, aby se dodavatelé problémům s akceptací mohli spolehlivě vyhnout.



**Informační systémy
veřejné správy (ISVS)**

1

1. Informační systémy veřejné správy (ISVS)

ISVS jsou informační systémy, které jsou definovány zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. § 3 odst. 1 výše uvedeného zákona vymezuje ISVS jako „soubor informačních systémů, které slouží pro výkon veřejné správy“.

Pokud bychom chtěli rozdíl mezi informačním systémem a ISVS vysvětlit, mohli bychom jej přirovnat k automatické pračce. Pračku si koupíte a necháte přivést. Potom nastávají další činnosti. Chcete, aby pračka fungovala přesně tak, jak si představujete, a požadujete český návod, abyste náhodou své oblíbené červené tričko neobarvili. O pračku se staráte, změkčujete vodu a dbáte na to, aby vše fungovalo, jak má. Podobné je to i s informačním systémem.

Cílem zákona je takový stav, kdy bude informační systém opatřen patřičným návodem, budou se o něj starat zkušení odborníci, bude mít patřičný servis a bude dělat jen to, co má. Jak ale takový ISVS poznáte? I pro pracovníky minulého gestora předpisu (Ministerstvo informatiky) bylo mnohdy velmi obtížné odpovědět na otázku, zda ten či onen informační systém je či není ISVS, a proto vznikl počátkem roku 2007 metodický pokyn „Co je a co není ISVS“.

Dříve, než se dostaneme k podstatě toho, co je a co není ISVS, je zapotřebí říci, proč je rozdíl mezi informačním systémem a ISVS tak důležitý. Rozdíl spočívá pouze v tom, zda konkrétní informační systém bude spadat pod zákon č. 365/2000 Sb. či ne. Vzhledem k zákonným požadavkům na ISVS je zde rozdíl v dokumentaci, komunikaci a správě informačního systému. Zákon č. 365/2000 Sb. je často používán i jako podmínka veřejných zakázek právě z toho důvodu, že definuje náležitosti komunikace ISVS a jeho dokumentace, přičemž příslušný úřad se těmito technickými náležitostmi dále nezabývá.

Za ISVS můžeme u orgánu veřejné správy označit následující informační systémy:

- informační systém, o kterém zákon (který stanovuje požadavky na vznik informačního systému) stanoví, že se jedná o ISVS podle zákona č. 365/2000 Sb. (například § 137 odst. 1 zákona č. 262/2006 Sb., zákoník práce),
- informační systém, který je zákonem označen jako registr, rejstřík nebo evidence (například § 21 zákona č. 76/2002 Sb., o integrované prevenci, omezování znečišťování, o integrovaném registru znečišťování),

- informační systém, u kterého je v zákoně uvedeno, že se jedná o ISVS, ale odkaz na zákon č. 365/2000 Sb. není uveden (například § 419 odst. 1 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení),
- informační systém, který je zákonem stanoven bez označení, že se jedná o ISVS (například § 4 odst. 1 písm. i) a j) zákona č. 365/2000 Sb.),
- informační systémy, které nejsou upraveny zákonem, ale prostřednictvím nichž orgán veřejné správy vykonává svěřené činnosti (např. informační systém o poplatcích za psy, pokud je tento informační systém provozován obcí, která tuto činnost vykonává ze zákona č. 565/1990 Sb., o místních poplatcích).

ISVS je informační systém, který spravuje konkrétní orgán veřejné správy. Je potřeba popsat, jaké požadavky jsou na něj a na orgán veřejné správy kladeny.

1. Orgán veřejné správy musí uveřejňovat číselníky, pokud je jejich správcem.

Číselník je seznam přípustných hodnot datového prvku ve formě dvojic – kódu a hodnoty. Datový prvek je pro potřeby ISVS dále nedělitelná část reálného světa, která je v ISVS spravována. Datovými prvky v registru obyvatel mohou být například „jméno“, „příjmení“, „pohlaví“ nebo „telefonní číslo“. Standardizace těchto datových prvků, která je zákonem č. 365/2000 Sb. prováděna, je nutná z následujících důvodů. V případě výměny dat a při rozdílných datových definicích jednotlivých datových prvků mohou být vyměněná data nečitelná, nebo je nutné je náročně převádět.

Například pokud jsou v ISVS „A“ uložena telefonní čísla jako 00420 a dalších devět číslic, je položka v databázi pro toto telefonní číslo dlouhá 14 znaků a její formát je číslicový. V ISVS „B“ jsou uložena telefonní čísla jako +420 a devět číslic, položka pro toto telefonní číslo je v databázi dlouhá 13 znaků a alespoň 1 znak není typu číslice. Při výměně dat mezi ISVS „A“ a „B“ vyměněná data samozřejmě nemohou souhlasit v délce a datových položkách. Proto je tímto zákonem zavedena standardizace datových prvků pro všechny ISVS orgánů veřejné správy.

Ke standardizaci číselníků dochází opět z důvodu výměny informací. Pro zjednodušení má například datový prvek „pohlaví“ k dispozici tři přípustné hodnoty a k nim přiřazen číselník (jeden z nejméně rozsáhlých číselníků ve veřejné správě): 1 – „muž“, 2 – „žena“, 3 – „neurčeno“. Pokud by čtenáře zajímalo, proč je pod označením 1 veden muž a žena pod označením 2, je nutné se dotázat správce tohoto datového prvku (AA0211), jímž je MVČR. Tento datový prvek je veden podle zákona č. 301/2000 Sb., o matkách, jménu a příjmení, ve znění

pozdějších předpisů. Číselníky jsou standardně tvořeny pro seznamy čítající několik desítek, stovek i tisíc záznamů.

Činnost správy datových prvků a číselníků se až na výjimky týká pouze ústředních orgánů veřejné správy. Správce číselníků je obvykle stanoven zvláštním právním předpisem. Pro správu datových prvků a číselníků, jejich změny, zrušení a založení je zřízen ISVS MVČR v souladu s § 4 odst. 1 písm. i) zákona č. 365/2000 Sb. informační systém o datových prvcích. Tento ISVS obsahuje veřejnou část, kde jsou uvedeny všechny standardizované číselníky a datové prvky, vstup do této části není omezen.

2. Orgán veřejné správy musí MVČR v elektronické podobě a bez zbytečného odkladu (tzn. okamžitě s výjimkou záchrany lidských životů, hašení požáru, poskytování první pomoci atp.) zpřístupňovat informace o jím provozovaných informačních systémech.

V příslušné pasáži zákona by pro dokonalou právní úpravu mělo sice stát „jím spravovaným“, protože se zde nepočítá s outsourcingem, ale schopní právníci to jistě zvládnou překlenout výkladem příslušného ustanovení. Zpřístupnění informací zde probíhá do informačního systému o ISVS (někdy též IS o ISVS), kde jsou požadované informace volně přístupné. IS o ISVS vznikl s jasným cílem pomoci informatikům při tvorbě a vytváření komunikujících informačních systémů.

Přestože je nutné do IS o ISVS zadávat informace o všech ISVS provozovaných orgánem veřejné správy, není celá agenda příliš rozsáhlá. Z více než 95 % totiž orgány veřejné správy provozují ISVS, které nekomunikují s jinými ISVS.

Pro potřeby této knihy i příslušného zákona si pojďme vymezit **komunikaci**. Komunikace, jak o ní budeme hovořit dále:

- probíhá mezi ISVS a jiným informačním systémem,
- probíhá mezi informačními systémy různých správců (orgánů veřejné správy),
- probíhá automatizovaným způsobem,
- probíhá mezi separátními informačními systémy.

Tento model relativně přesně vymezuje komunikaci na systém přenosu dat (například ve formátu XML mezi ISVS), který je veřejně dostupný a poskytuje služby jiným informačním systémům. Z praktického hlediska se jedná například o ISVS ARES (správce Ministerstvo financí), který poskytuje data o ekonomických subjektech z několika ISVS, které integruje.

Ale zpět k IS o ISVS. Pokud ISVS nekomunikuje podle výše uvedených požadavků, jsou předávané informace omezeny (jméno ISVS, právní základ, cena, správce atp.). Formulář pro vyplnění neobsahuje více než 20 povinných položek. Pokud ovšem ISVS komunikaci provádí, je situace dosti odlišná. Do popředí se dostává pravý účel IS o ISVS, kterým je poskytnutí informací o možnostech připojení a získání volně dostupných dat z ISVS. Pro tyto účely je nutné do ISVS předat datový formát včetně jeho specifikace, model přenosu, údaje o portech jednotlivých služeb a další nezbytné údaje, aby programátoři ostatních ISVS byly schopni s příslušným ISVS realizovat komunikaci.

3. Orgán veřejné správy musí zajistit, aby komunikace všech jeho ISVS probíhala přes referenční rozhraní a s využitím vyhlášených datových prvků. Tento požadavek je kladen pouze na komunikující ISVS, ostatních se netýká.

Pojem referenční rozhraní byl ve veřejné správě využíván dlouho. Jeho definice je následující.

„Referenční, bezpečné a sdílené rozhraní je soubor právních, technických, organizačních a jiných opatření, vytvářejících jednotné integrační prostředí ISVS, které poskytuje kvalitní soustavu společných služeb...“

Jak je vidět, referenční rozhraní by mohlo být vlastně téměř všechno, nebo nic.

Prvotní představy o referenčním rozhraní byly takové, že nad komunikační infrastrukturou veřejné správy (KIVS) bude vytvořena společná aplikační část, která bude všem orgánům veřejné správy poskytovat služby. Definovat tyto společné služby není jednoduché. Pro orgány veřejné správy by jako společné služby mohly sloužit webhosting, hosting nebo služba poskytování časových razítek, případně společné autentizační služby.

Projekt společných služeb pro celou veřejnou správu nebyl realizován a pravděpodobně ani realizován nebude. Proto bylo upraveno právními předpisy referenční rozhraní do varianty „light“, která nepřináší nové služby nebo informace, na druhou stranu neomezuje implementaci různých ISVS, jejich technologií, komunikací apod. Nepředepisuje standardy, datové typy a jiné součásti ISVS a tím zvyšuje flexibilitu řešení.

Pro komunikaci ISVS platí následující pravidla:

- komunikující ISVS musí být zapsán v IS o ISVS,
- při komunikaci musí být použity výhradně vyhlášené datové prvky (v informačním systému o datových prvcích),

- komunikace musí být logována (kdo žádal o informaci, kdy to bylo, výsledek žádosti – zda informace byla nebo nebyla poskytnuta).

Komunikace ISVS podléhá atestaci. Organizace provádějící atestaci musí být pro tuto činnost akreditována Českým institutem pro akreditaci a pověřena výkonem atestací MVČR. Při atestaci referenčního rozhraní je ověřován soulad s legislativou a následně prakticky vyzkoušena funkčnost a dostupnost komunikujícího ISVS s údaji uvedenými jeho správcem v IS o ISVS.

4. Orgán veřejné správy musí dlouhodobě řídit své ISVS. To znamená, že musí zpracovat informační koncepci orgánu veřejné správy, ve které uvede:

- charakteristiku všech spravovaných ISVS,
- způsob financování těchto ISVS,
- způsob a odpovědnosti při správě ISVS,
- dlouhodobé cíle v oblasti řízení kvality ISVS,
- dlouhodobé cíle v oblasti řízení bezpečnosti ISVS.

Cíl vytvoření informační koncepce je jednoduchý, je zpracována pro všechny ISVS souhrnně. Praktická realizace někdy naráží na nezajištěné financování a chybějící dlouhodobý výhled. Orgány veřejné správy mají pro procesní a funkční řízení někdy zavedeno zbytečně mnoho agend a s nimi spojených ISVS, které jsou pak logicky duplicitní.

Informační koncepce orgánu veřejné správy musí být pro kontrolu atestována. Při atestaci je informační koncepce ověřována proti současnému stavu, vývoji technologií a legislativě.

5. Orgán veřejné správy musí ke všem svým ISVS (zvláště) vést provozní dokumentaci. Tato provozní dokumentace se skládá z následujících dokumentů:

- bezpečnostní politika ISVS,
- bezpečnostní směrnice pro činnost bezpečnostního správce,
- uživatelská příručka,
- systémová příručka,
- případně jiné důležité provozní dokumenty podle povahy a rozsahu ISVS.

Pro potřeby atestace provozní dokumentace je v souladu s legislativou předkládána pouze bezpečnostní politika příslušného ISVS. V případě malých ISVS je možné provozní dokumentaci sloučit, případně ji vypracovat pouze v minimalistické verzi.

6. Jen málokdo ještě neslyšel o další součásti eGovernmentu, zvané Czech POINT.

Czech POINT je právně zakotven v zákoně č. 365/2000 Sb., o ISVS, a proto se o něm zmíníme v této části textu.

Český podací ověřovací informační národní terminál, tedy Czech POINT je projektem, který redukuje přílišnou byrokracii ve vztahu občan-veřejná správa. V současnosti musí občan navštívit několik úřadů k vyřízení jedné agendy. Czech POINT slouží jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby „obíhala data, ne občan“.

Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho univerzálního místa, kde je možné získat a ověřit data z veřejných i neveřejných ISVS, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů.

Celý postup probíhá následovně: Občan se dostaví na pobočku České pošty, vybrané zastupitelské úřady, případně další instituce stanovené prováděcími vyhláškami. Na přepážce příslušný pracovník Czech POINT získá údaje o žadateli a údaje o předmětu jeho zájmu. Je nutno podotknout, že kontaktní místa neslouží k nahlížení do ISVS nebo registrů – to znamená, že je nutné znát údaje o subjektu nebo předmětu svého zájmu. Například při vyhledávání společnosti je nutné znát IČO nebo jméno, při hledání domu číslo popisné apod. Pracovník Czech POINT se zabezpečeným kanálem připojí k centrále Czech POINT, prostřednictvím které zadá dotaz a přijme odpověď. Elektronickou odpověď vytiskne, orazítkuje a podepíše. Takto vytvořený ověřený výpis má charakter veřejné listiny. V současné době lze na kontaktních místech Czech POINT získat výpisy z rejstříku trestů, katastru nemovitostí, výpis z obchodního rejstříku nebo výpis z živnostenského rejstříku.

V konečné fázi projektu bude občan své záležitosti vyřizovat i z domova prostřednictvím internetu.