



SBORNÍK KONFERENCE

ISSS 2017 let

DOPROVODNÁ MEZINÁRODNÍ KONFERENCE V4DIS

3.-4. DUBNA 2017 HRADEC KRÁLOVÉ

issSS
LOCAL AND REGIONAL INFORMATION SOCIETY
V4DIS

Obsah

Úvodní slovo	3
<i>Ing. Tomáš Salomon, generální ředitel a předseda představenstva České spořitelny, a. s.</i>	
Úvodní slovo	4
<i>RNDr. Tomáš Renčín, výkonný ředitel konference</i>	

Informace

Seznam vystavovatelů a partnerů konference	6
Orientační plán kongresového centra Aldis	7
Informace pro účastníky konference	10

Dokumenty

Konference V4DIS již počtrnácté	13
Český zavináč 2017 – ocenění za zásadní přínos k rozvoji a modernizaci IZS a tísňových linek	14
Zlatý erb 2017	16
Prezentace tchajwanských dodavatelů	17

Přednášky

Mobile Device Management – hromadná správa a zabezpečení mobilních zařízení.....	19
<i>Petra Holubcová, Ondřej Kubeček, System4u, s.r.o.</i>	
Elektronické skartační řízení v praxi.....	21
<i>Mgr. Věra Hottmarová, Město Smiřice, Ing. Pavel Jirásek, Městská část Praha 16, Bc. Irina Rálišová, Město Sezemice, Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
Objevte svět internetu věcí – chytrá řešení pro moderní vedení města.....	33
<i>Ing. Ján Jacina, business development manager pro IoT, České Radiokomunikace a.s.</i>	
Moderní API již není jen pro startupy	37
<i>Vítězslav Košina, IBA CZ</i>	
Evidence smluv a registr smluv naostro.....	39
<i>Ing. Petra Kubíková, Kamila Kolbová, Městská část Praha-Zličín; Mgr. Petr Wohanka, Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)	45
<i>Mgr. Tomáš Lechner, Ph.D., Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva</i>	
GDPR – nové nařízení zasáhne celou veřejnou správu.....	54
<i>Mgr. Bc. Tomáš Mudra, UEPA advokáti, s. r. o.; Mgr. Vladimíra Hloušková, d-eye CZECHIA, s. r. o.</i>	
Smart Cities? Města, kde je radost žít	57
<i>Václav Pávek, ředitel odboru Smart Cities&Regions, GORDIC spol s r. o.</i>	
Elektronický zdravotní záznam jako základní stavební kámen e-health řešení – pohled praktický i legislativní	58
<i>Jan Petřík, Institut pro elektronizaci zdravotnictví, z. ú.</i>	
CZ.PEPS: základ infrastruktury pro vzájemné uznávání eID	65
<i>Mgr. Jiří Průša, CZ.NIC, z. s. p. o.</i>	
NetMetr: harmonizace otevřených dat napříč Evropou	68
<i>Mgr. Jiří Průša; CZ.NIC, z. s. p. o.</i>	
KYBEZ – platforma kybernetické bezpečnosti.....	70
<i>Michal Řezáč, výkonný ředitel platformy KYBEZ, GORDIC spol s r. o.</i>	

Koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury	72
<i>Ing. Jiří Sedláček, CEO, Network Security Monitoring Cluster, družstvo</i>	
Města a regiony budoucnosti.....	77
<i>Karel Skokan, Managing Consultant, Czech Republic, Slovakia and Eastern Europe, CGI IT Czech Republic s.r.o.</i>	
Rok a půl otevřených dat ČSSZ – zkušenosti a poznatky z každodenní praxe	79
<i>Ing. Jiří Šunka, vedoucí oddělení metodiky a správy dat ČSSZ</i>	
Jak dosáhnout transparentnosti obce	84
<i>Mgr. Dana Ullwerová, Obec Vrané nad Vltavou; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.</i>	
Elektronizace procesů a digitalizace dat úřadu	91
<i>Miroslav Wolf, obchodní ředitel Praha, GORDIC spol s r. o.</i>	
Routery Turrus Omnia – do internetu bezpečně	92
<i>Patrick Zandl, CZ.NIC, z. s. p. o.</i>	

Katalog

Generální partner konference	95
Hlavní partneři konference.....	96
Partneři konference	99
Partneři odborných bloků.....	102
Spolupracující instituce a sdružení.....	103
Kraje a města.....	104
Ministerstva.....	105
Prezentace firem.....	106
Prezentace tchajwanských dodavatelů	115
Pořadatelé.....	118
Programový výbor a realizační tým konference ISSS/V4DIS 2017	119

Úvodní slovo Ing. Tomáše Salomona, generálního ředitele a předsedy představenstva České spořitelny, a. s., generálního partnera konference ISSS 2017

Vážené dámy a pánové,

žijeme v digitálním světě. Digitalizace znamená komfort, rychlost, efektivitu a prosperitu nás všech. To jsou hodnoty, ke kterým se hlásí i Česká spořitelna. Je nám ctí být 17 let partnerem konference.

Česká spořitelna pomáhá rozvíjet naše města a obce, regiony a kraje. Společenská odpovědnost vždy patřila a patří ke genetické výbavě naší banky. Jsme úspěšnou bankou a jednou z největších firem v zemi. Usilovat o lepší Česko a jeho prosperitu považujeme za naši povinnost.

Procházíme dobou exponenciálních změn, technologie pronikají do všech oborů. Z pohledu budoucí prosperity Česka je důležité „být u toho“. S nástupem digitálních technologií už nemusí stačit naše dlouhodobé konkurenční výhody, ať již se jedná o kvalifikovanou pracovní sílu, anebo geografickou blízkost k Německu coby lídru evropské ekonomiky.

Podpora zavádění moderních technologií, inovací a technické vzdělanosti patří mezi priority České spořitelny. Kromě významných sponzorských aktivit a financování konkrétních projektů nabízíme i poradenství a pomáháme zprostředkovat spolupráci mezi dodavateli technologií a jejich zákazníky. Úspěšným příkladem je působení České spořitelny na nově vznikajícím trhu „chytrých“ měst. Již více než rok pomáháme našim městům v rámci našeho programu „Chytré město“ zavádět „chytré“ systémy v dopravě, veřejné správě, odpadovém hospodářství a dalších oblastech, díky kterým mohou šetřit jak finance, tak životní prostředí, a být zároveň skvělým místem pro život.

Na naší cestě k lepšímu Česku se moderním technologiím nevyhneme. Pojďme z nich udělat naši konkurenční výhodu! Věřím, že tato konference tomu může velmi pomoci.

*Ing. Tomáš Salomon,
generální ředitel a předseda představenstva
České spořitelny, a. s.*

Úvodní slovo RNDr. Tomáše Renčina, výkonného ředitele konference

Dámy a pánové, milí hosté a vážení kolegové,

konference ISSS dospěla do svého jubilejního 20. ročníku – je až neuvěřitelné, že v tak dynamickém a stále se měnícím prostředí, jakým je oblast ICT technologií ve veřejné správě, trvá něco tak dlouho. Akce, která je už počtrnácté doprovázena visehradskou konferencí V4DIS, se navíc neustále rozvíjí a získává větší renomé.

V královéhradeckém Aldisu se opět scházejí prakticky všichni, kdo se zabývají informatizací veřejné správy. Rád bych na tomto místě poděkoval všem spolupracovníkům a partnerům, kteří se každoročně podílejí na úspěšné realizaci konference, ať už jde o hostitelské město Hradec Králové, Královéhradecký kraj nebo Kraj Vysočina, který se v posledních letech výrazně podílí na organizaci celé akce, a samozřejmě i všem partnerům v čele s Českou spořitelnou. Nesmím zapomenout ani na ty, kdo této akci poskytli osobní záštitu – ať už to jsou členové vlády ČR, Parlamentu ČR nebo Asociace krajů ČR.

Během dvou dnů konferenčního programu se společně ohlédneme za vším podstatným, co se v průběhu uplynulého roku v tuzemském e-governmentu událo, probereme klíčové projekty a jejich další rozvoj a samozřejmě se budeme zabývat budoucností. Věřím, že se jako obvykle podaří prodiskutovat řadu klíčových úkolů, které musí v následujících měsících a letech veřejná správa ČR řešit, včetně dalšího rozvoje digitálního trhu a sdílených služeb nebo třeba nového nařízení EU o ochraně osobních údajů známého pod zkratkou GDPR.

Celý organizační tým nesmírně těší, že o účast na hradeckém setkání je stále velký zájem, a to jak mezi politiky, zástupci státních institucí i samospráv a odborníky na danou problematiku, tak mezi dodavateli služeb a technologií do tohoto segmentu. Velice si vážíme také toho, že program konference doplňuje řada důležitých setkání a jednání, jako jsou například jednání komisí AK ČR a SMO ČR s poslanci Parlamentu ČR, setkání Sdružení tajemníků obecních a městských úřadů a řada dalších akcí včetně vyhlášení vítězů populárních soutěží Zlatý erb a Český zavináč.

Jsem přesvědčen o tom, že jubilejní dvacátý ročník konference ISSS všem přinese novou inspiraci a důležité impulzy pro další práci. Budeme se snažit poskytnout maximum informací a zároveň zajistit, aby všechny důležité podklady, prezentace a záznamy byly dobře dostupné i po skončení akce. Těší nás vaše důvěra a doufám, že ji ani letos nezklameme.

Přeji příjemné a inspirativní prožití dvacátého ročníku ISSS.

*RNDr. Tomáš Renčín,
výkonný ředitel konference*

20

INFORMACE



SEZNAM VYSTAVOVATELŮ

PARTNEŘI KONFERENCE

GENERÁLNÍ PARTNER / GENERAL PARTNER	UMÍSTĚNÍ	STÁNEK
Česká spořitelna, a. s.	1. p / 1 st	26

HLAVNÍ PARTNEŘI / MAIN PARTNERS	UMÍSTĚNÍ	STÁNEK
Cisco Systems (Czech Republic) s.r.o.		
Česká pošta, s. p.	1. p	18
ICZ a.s.	1. p	25
Microsoft s.r.o.	1. p	31, Salonek 2
Oracle Czech, s.r.o.		
Taipei Economic and Cultural Office	přízemí	52
VITA software, s.r.o.	1. p	22

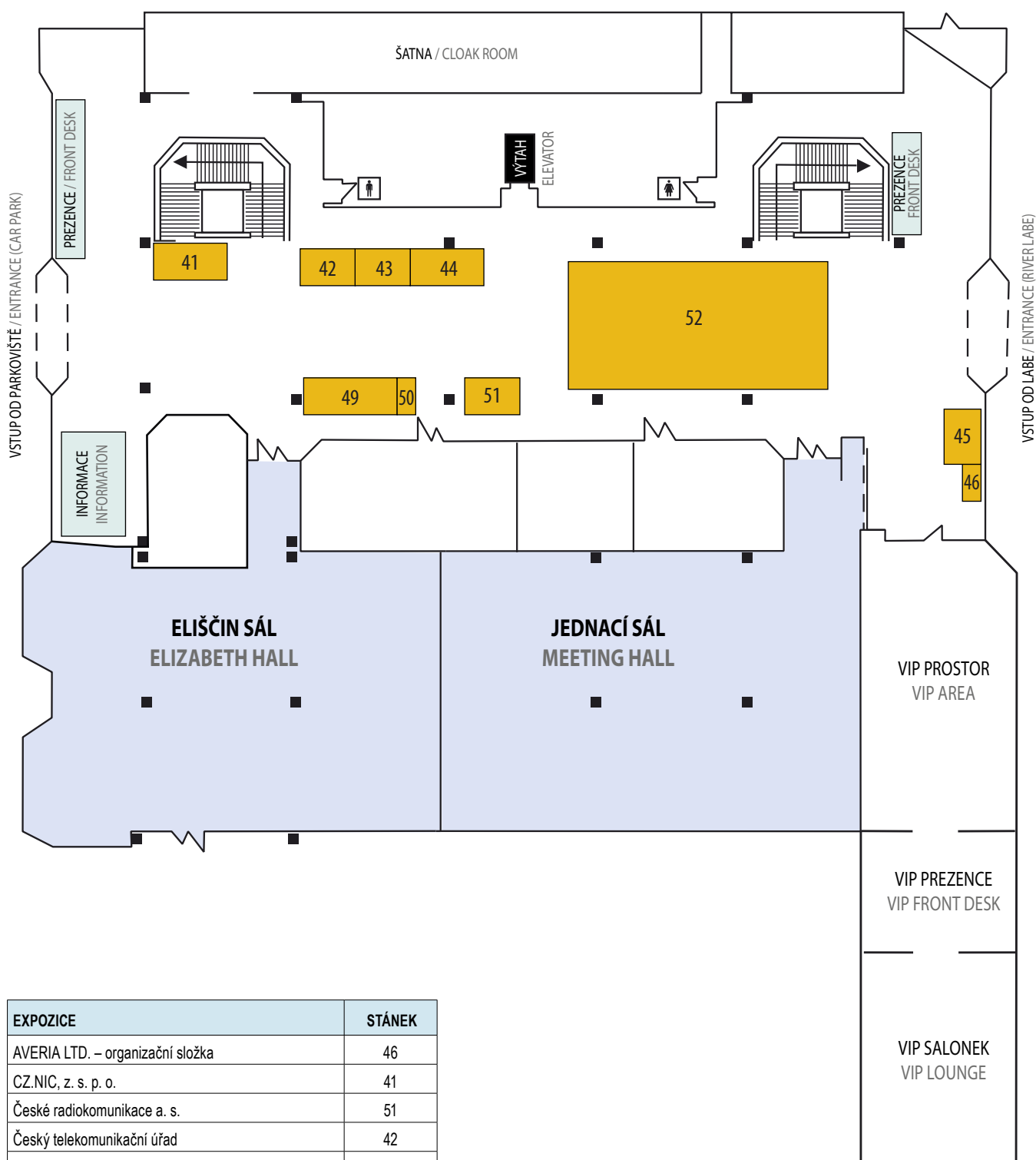
PARTNEŘI / PARTNERS	UMÍSTĚNÍ	STÁNEK
ALEF NULA, a.s.		
Asseco Central Europe, a. s.	1. p	10
AutoCont CZ a.s.		
AV MEDIA, a. s.	1. p	11
Citrix Systems Czech Republic s.r.o.	1. p	4
České Radiokomunikace a. s.	přízemí	51
FORTINET		
Fujitsu Technology Solutions s.r.o.	1. p	Salonek 1
GORDIC spol. s r. o.	1. p	29

ABECEDNÍ SEZNAM EXPOZIC

EXPOZICE	UMÍSTĚNÍ	STÁNEK
ALEF NULA, a.s.	1. p	36
ARCDATA PRAHA, s.r.o.	1. p	20
Asseco Central Europe, a. s.	1. p	10
ATLAS software a.s.	1. p	35
AV MEDIA, a. s.	1. p	11
AVERIA LTD. – organizační složka	přízemí	46
CEVRO Institut, z.ú.	1. p	16
Citrix Systems Czech Republic s.r.o.	1. p	4
CZ.NIC, z. s. p. o.	přízemí	41
ČD - Telematika a.s.	1. p	8
Česká pošta, s. p.	1. p	18
Česká spořitelna, a.s.	1. p	26
České radiokomunikace a. s.	přízemí	51
Český telekomunikační úřad	přízemí	42
DAIN, s.r.o.	1. p	23
DATRON, a.s.	1. p	6
Flowmon Networks a.s.	1. p	5
Fujitsu Technology Solutions, s.r.o.	1. p	Salonek 1
GEOVAP, spol. s r.o.	1. p	9
GEPRO spol. s r.o.	1. p	3
GORDIC spol. s r.o.	1. p	29
HP Inc. Czech Republic s.r.o.	přízemí	44
IBR Consulting, s. r. o.	1. p	30
ICZ a.s.	1. p	25
Kraj Vysočina	1. p	33, 34

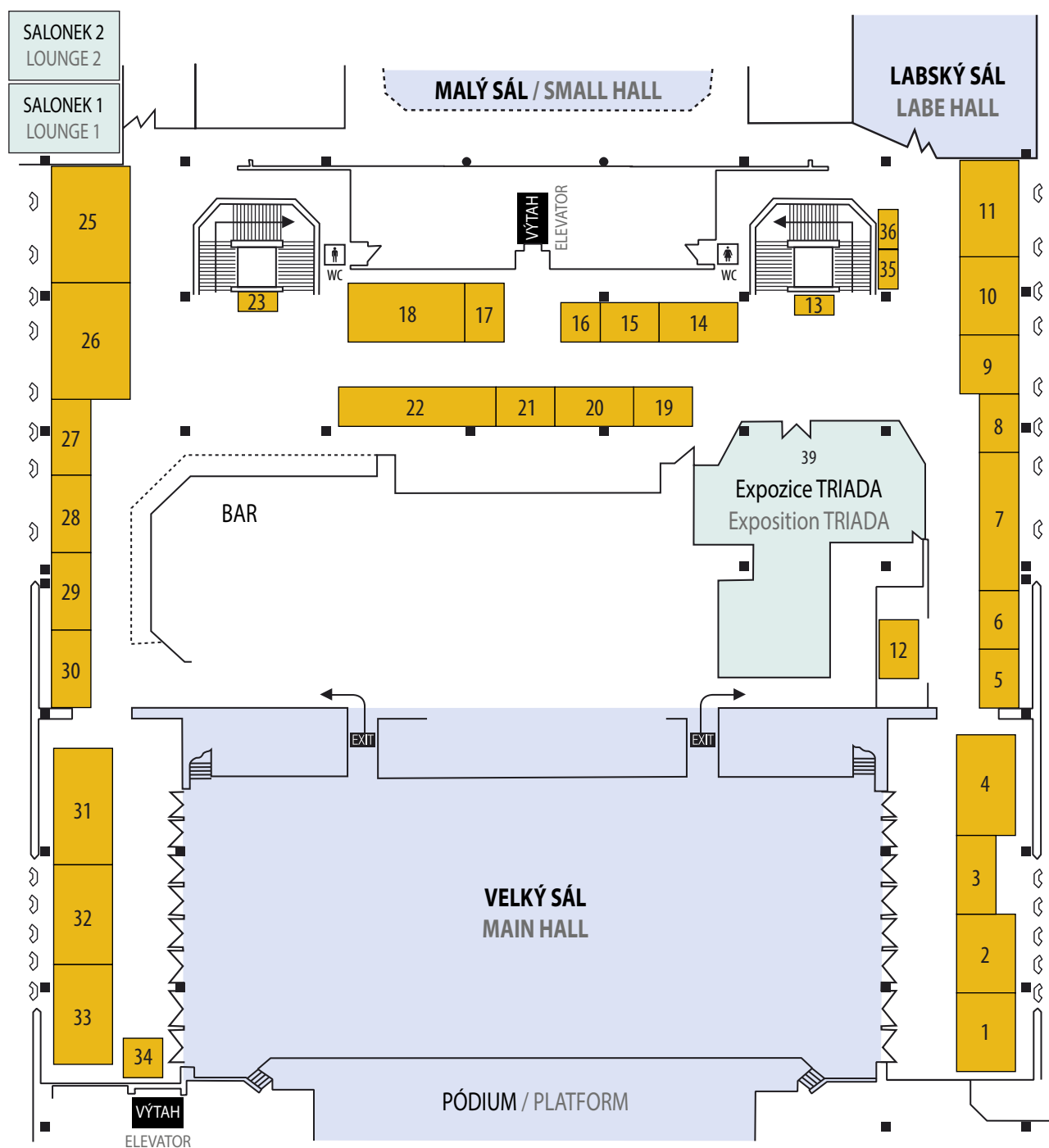
EXPOZICE	UMÍSTĚNÍ	STÁNEK
MARBES CONSULTING s.r.o.	1. p	17
MICROSOFT s.r.o.	1. p	31, Salonek 2
Ministerstvo pro místní rozvoj ČR	1. p	1
Ministerstvo vnitra ČR	2. p	61
Network Security Monitoring Cluster, družstvo	přízemí	49
OKI Systems (Czech and Slovak), s.r.o.	2. p	63
OKsystem a.s.	1. p	27
QCM, s.r.o.	1. p	28
Software602 a.s.	1. p	7
Státní fond životního prostředí české republiky	1. p	13
Státní tiskárna cenin, státní podnik	1. p	32
STYRAX, a.s.	přízemí	43
System4u, s.r.o.	přízemí	50
T - MAPY spol. s r.o.	1. p	21
Taipei Economic and Cultural Office	přízemí	52
Tender systems s.r.o.	přízemí	45
TRIADA, spol. s r. o.	1. p	39
VARS Brno a.s.	1. p	15
Vema, a. s.	1. p	19
VERA, spol. s r.o.	1. p	14
VITA software, s.r.o.	1. p	22
WEBHOUSE, s. r. o.	2. p	62
Wolters Kluwer ČR, a. s.	1. p	12
Zeměměřický úřad, Český úřad zeměměřický a katastrální	1. p	2

ORIENTAČNÍ PLÁN EXPOZIC – PŘÍZEMÍ

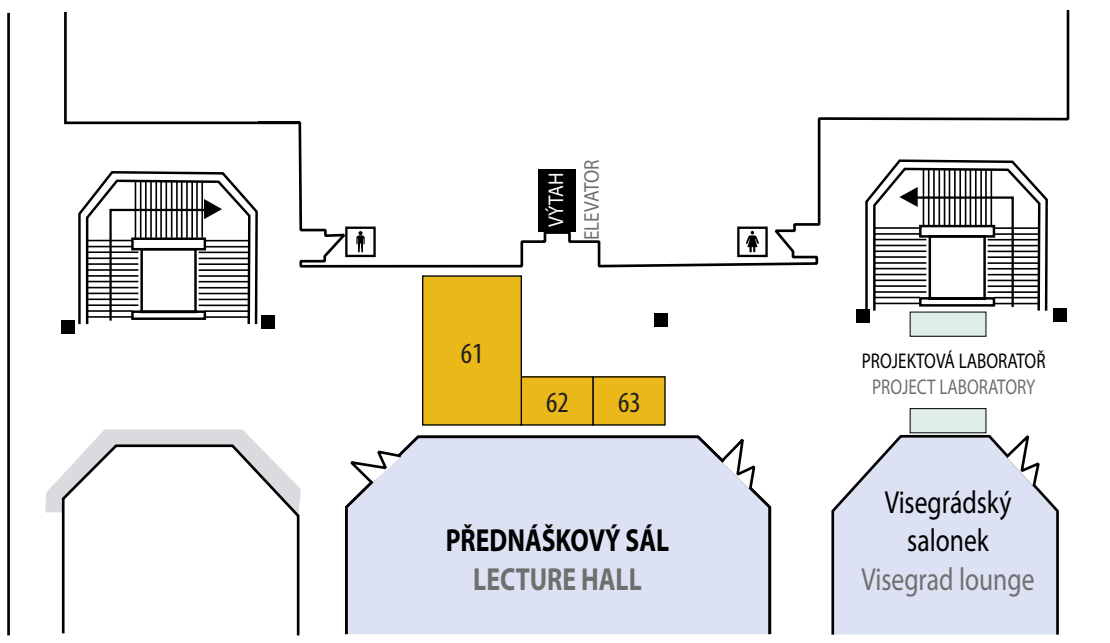


EXPOZICE	STÁNEK
AVERIA LTD. – organizační složka	46
CZ.NIC, z. s. p. o.	41
České radiokomunikace a. s.	51
Český telekomunikační úřad	42
HP Inc. Czech Republic s.r.o.	44
Network Security Monitoring Cluster, družstvo	49
STYRAX, a.s.	43
System4u, s.r.o.	50
Taipei Economic and Cultural Office	52
Tender systems s.r.o.	45

ORIENTAČNÍ PLÁN EXPOZIC – 1. PATRO



ORIENTAČNÍ PLÁN EXPOZIC – 2. PATRO



EXPOZICE	STÁNEK
Ministerstvo vnitra ČR	61
OKI Systems (Czech and Slovak), s.r.o.	63
WEBHOUSE, s. r. o.	62

Seznam expozic 1. patra

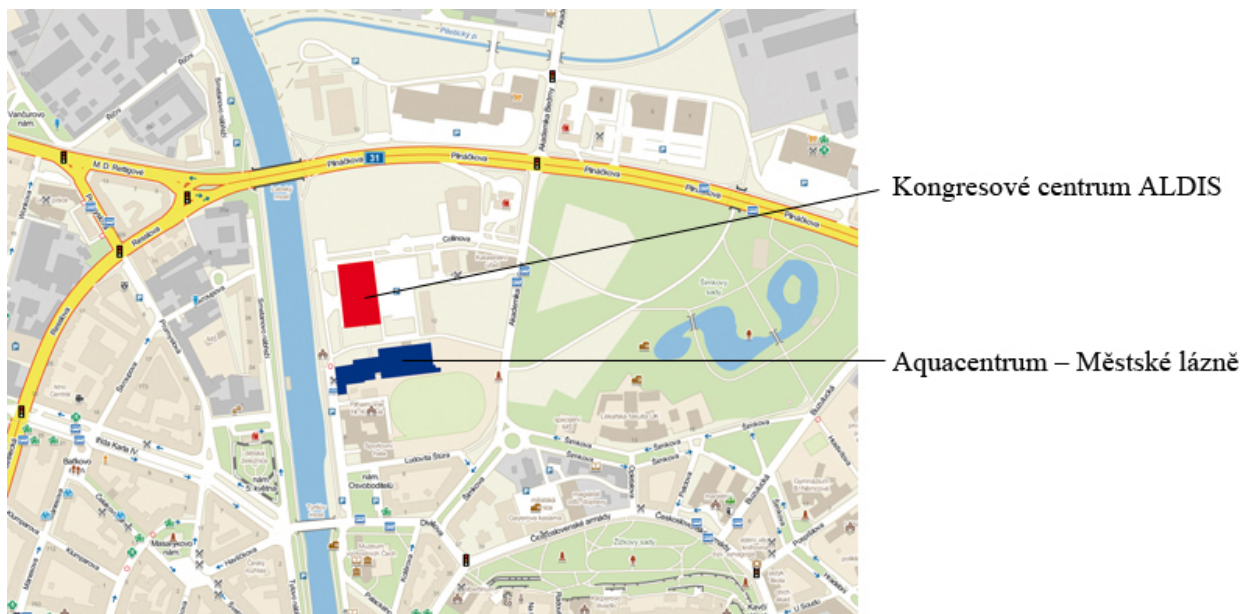
EXPOZICE	STÁNEK
ALEF NULA, a.s.	36
ARCDATA PRAHA, s.r.o.	20
Asseco Central Europe, a. s.	10
ATLAS software a.s.	35
AV MEDIA, a. s.	11
CEVRO Institut, z.ú.	16
Citrix Systems Czech Republic s.r.o.	4
ČD - Telematika a.s.	8
Česká pošta, s. p.	18
Česká spořitelna, a.s.	26
DAIN, s.r.o.	23
DATRON, a.s.	6
Flowmon Networks a.s.	5
Fujitsu Technology Solutions, s.r.o.	Salonek 1
GEOVAP, spol. s r.o.	9
GEPRO spol. s r.o.	3
GORDIC spol. s r.o.	29
IBR Consulting, s. r. o.	30

EXPOZICE	STÁNEK
ICZ a.s.	25
Kraj Vysočina	33, 34
MARBES CONSULTING s.r.o.	17
MICROSOFT s.r.o.	31, Salonek 2
Ministerstvo pro místní rozvoj ČR	1
OKsystem a.s.	27
QCM, s.r.o.	28
Software602 a.s.	7
Státní fond životního prostředí české republiky	13
Státní tiskárna cenin, státní podnik	32
T - MAPY spol. s r.o.	21
TRIADA, spol. s r. o.	39
VARS Brno a.s.	15
Vema, a. s.	19
VERA, spol. s r.o.	14
VITA software, s.r.o.	22
Wolters Kluwer ČR, a. s.	12
Zeměměřický úřad, Český úřad zeměměřický a katastrální	2

Informace pro účastníky konference

Místo konání konference

Kongresové centrum ALDIS
 Eliščíno nábřeží 375, 500 02 Hradec Králové
 GPS souřadnice: 15,83272°, 50,21572



Městská hromadná doprava

- Pro účastníky konference je ve spolupráci s Dopravním podnikem města Hradec Králové zajištěna **ZDARMA**
- Účastníci se prokazují konferenční kartičkou, kterou obdrží při prezenci
- Nejbližší zastávka přímo před kongresovým centrem – „Aldis“
- Zastávky MHD do 500 m – „Muzeum“, „Adalbertinum“
- Pro více informací navštivte www.dpmhk.cz

Aquacentrum – Městské lázně

- Účastníci konference mohou po náročném konferenčním programu relaxovat v Městských lázních, které se nacházejí v těsném sousedství Kongresového centra Aldis
- Vstup je **ZDARMA** na základě vstupenky, kterou účastníci konference obdrží při prezenci
- Provozní doba:

neděle	2. 4. 2017	10.00–20.00 hod.
pondělí	3. 4. 2017	10.00–21.00 hod.
úterý	4. 4. 2017	10.00–21.00 hod.

Pondělní společenský večer

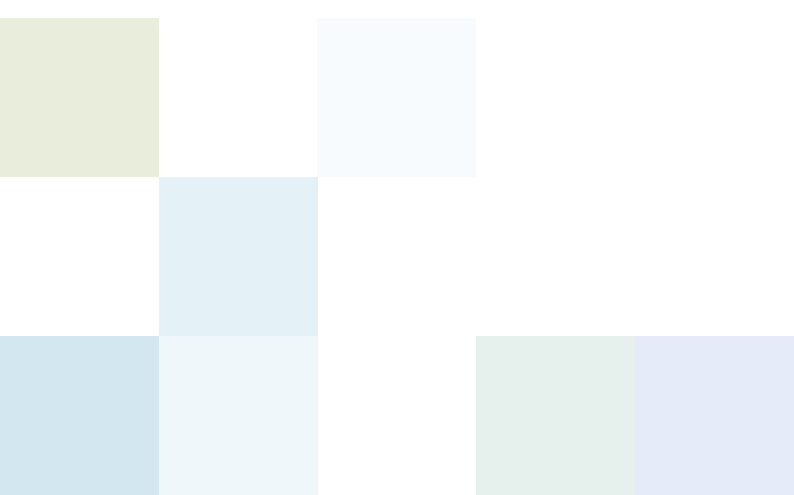
- **3. dubna 2017 od 20.00 hodin** v prostorách Kongresového centra Aldis
- Vyhlášení soutěží Zlatý Erb, Biblioweb a Cena ministra vnitra
- Občerstvení formou rautu, hudba k poslechu i tanci
- **Vstup s platnou vstupenkou**

Přehled dalších doprovodných akcí

- Setkání KI SMO a KR AKČR pro informační technologie ve veřejné správě s poslanci PSP ČR a zástupci centrálních orgánů
- Setkání Sdružení tajemníků městských a obecních úřadů (STMOÚ)
- Setkání účastníků soutěže JuniorErb
- Seminář Právní dopady GDPR
- Panelová diskuse k Národní strategii cloudcomputingu

20

DOKUMENTY



Konference V4DIS již počtrnácté

Současně s renomovanou národní konferencí ISSS se ve dnech 3.–4. dubna 2017 uskuteční již počtrnácté i tradiční mezinárodní konference V4DIS (Visegrad Four for Developing Information Society). Setkání zástupců veřejné správy zemí Visegrádské čtyřky i letos přivítá řadu významných hostů nejen z visegrádského regionu, ale i z dalších evropských zemí. Akce se jako obvykle zúčastní desítky zástupců veřejné správy ze zemí V4 a řada tuzemských i zahraničních odborníků věnujících se problematice informatizace společnosti a reformě veřejné správy. Mezi vzácnými hosty konference ISSS/V4DIS 2017 nebudou chybět ani premiér ČR Bohuslav Sobotka, vicepremiéři Pavel Bělobrádek a Andrej Babiš, ministryně pro místní rozvoj Karla Šlechtová a řada dalších osobností tuzemského politického života.

Hlavními tématy konference bude tradiční hodnocení rozvoje e-governmentu v zemích Visegrádu, stejně jako informace o klíčových projektech, které se v uplynulém roce podařilo rozpracovat nebo dokončit. Prostor v programu obvykle dostávají i projekty týkající se dalšího rozvoje přeshraniční spolupráce, zkušenosti z implementace moderních technologií v širokém spektru oblastí souvisejících s veřejnou správou a ukázky best practices.

Hlavním organizátorem konference V4DIS je spolek Český zavináč, spoluorganizátorem již poněkolidkrát Kraj Vysočina a na celkové koncepci akce se významně podílejí i hostitelské město Hradec Králové a hlavní město Praha. Součástí programu V4DIS 2017 bude vedle obvyklých doprovodných akcí konference ISSS i tradiční nedělní VIP večer v Klicperově divadle, vyhlášení ceny Český zavináč či ocenění účastníků soutěže mladých talentů JuniorErb.

Více informací o konferenci V4DIS 2017 i o předchozích ročnících lze najít na www.v4dis.eu nebo www.issc.cz.

Český zavináč 2017 – ocenění za zásadní přínos k rozvoji a modernizaci IZS a tísňových linek

V rámci programu slavnostního setkání v předvečer zahájení jubilejního 20. ročníku konference ISSS/V4DIS v královéhradeckém Klicperově divadle byly vyhlášeny výsledky soutěže Český zavináč. Aktuálním držitelem tradiční ceny se stal Integrovaný záchranný systém ČR, a to za průběžné zvyšování úrovně ochrany obyvatel ČR a moderní řešení spolupráce a koordinace záchranných a bezpečnostních složek, orgánů státní správy a samosprávy i fyzických a právnických osob při společném provádění záchranných a likvidačních prací a přípravě na mimořádné události.

„Porota ocenila především úspěšné dokončení realizace více než čtyřicítky souvisejících projektů, které vytvářejí ucelený a funkční systém příjmu tísňového volání všech základních složek integrovaného záchranného systému,“ poznamenává RNDr. Tomáš Renčín, předseda spolku Český zavináč. „Vnímáme to jako velký přínos v rozvoji informační společnosti a výrazné zrychlení spolupráce záchranných složek i zkrácení času mezi oznámením a zásahem na místě události.“

Převážná část projektu nazvaného „Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému“ byla dokončena již koncem roku 2015, v letošním roce bude ještě dopracován ZZS hl. m. Prahy. Garantem je MV-generální ředitelství HZS ČR, věcným gestorem pak plk. Ing. Luděk Prudil, nyní ředitel HZS Libereckého kraje.

V průběhu celého projektu byla řešena modernizace technologií operačních středisek, zlepšení a standardizace interoperability, zavedení jednotného GIS, dokončení integrace operačního řízení z okresních operačních středisek do krajských. Bližší informace na: <http://is-izs.izscr.cz/>.

Soutěž se poprvé uskutečnila v roce **1999**. Prvním vítězem se stal tehdejší ministr spravedlnosti **Otakar Motejl**, a to za zpřístupnění Obchodního rejstříku (www.justice.cz) a za dlouhodobě otevřený přístup nositele tohoto ocenění k potřebám široké veřejnosti.

O rok později, v roce **2000**, zvítězila **Kancelář Poslanecké sněmovny Parlamentu ČR**. Porota ocenila společný projekt Parlamentní knihovny a odboru informatiky Kanceláře Poslanecké sněmovny Parlamentu ČR, nazvaný Digitální knihovna Český parlament (www.psp.cz/eknih). Digitální knihovnu tvoří archiv digitalizovaných tísňových zpráv z jednání našeho parlamentu od roku 1918 do současnosti.

Na třetím ročníku soutěže bylo Českým zavináčem **2001** oceněno **Ministerstvo vnitra České republiky** za projekty zaměřené na praktickou pomoc občanům. Projekty „Pátrání po vozidlech“, „Neplatné doklady“ a „Úřad není labyrint“ se setkaly s mimořádným ohlasem veřejnosti a mají dlouhodobě vysokou sledovanost.

V roce **2002** se laureátem stalo **Ministerstvo financí**. Porota tak podpořila nejen internetový „Registr plátců DPH“ a „Registr plátců spotřební daně“, ale také aktivitu a koncepčnost, s níž ministerstvo přistoupilo k řešení komplexního využití moderních technologií v oblasti daňové správy jako celku.

Držitelem Českého zavináče **2003** se stal bilaterální projekt „**Společná česko-slovenská digitální parlamentní knihovna**“. Jednalo se o zcela mimořádný počín v rozvoji informační společnosti v obou zemích, který znamenal průlom ve vzájemné informovanosti zákonodárných sborů a široké české a slovenské veřejnosti.

V roce **2004** si za nepřetržitou a bezplatnou službu „Nahlížení do katastru nemovitostí“ dostupnou všem uživatelům internetu, odnesl ocenění **Český úřad zeměměřický a katastrální**. Aplikace umožnila získávat některé vybrané údaje týkající se parcel a budov evidovaných v katastru nemovitostí, a dále pak informace o stavu jednotlivých řízení založených na příslušném katastrálním pracovišti, a to jak pro účely zápisu vlastnických a jiných práv, tak pro účely potvrzování geometrických plánů.

V roce **2005** se neudělovala hlavní cena, ale **dvě čestná uznání**, a to projektu **České spořitelny, a. s.**, – „Ověřování vlastnictví nemovitosti pomocí dálkového přístupu ke katastru nemovitostí pro potřeby posuzování hypotečních úvěrů“ a projektu **Úřadu MČ Praha 6** – „Ověřování vlastnictví nemovitosti pomocí dálkového přístupu ke katastru nemovitostí“.

V roce **2006** se držitelé ceny společně staly dva subjekty veřejné správy – „**Podvýbor pro informační systémy ve veřejné správě Výboru pro veřejnou správu, regionální rozvoj a životní prostředí Poslanecké sněmovny Parlamentu ČR**“ a „**Ministerstvo informatiky ČR**“, a to za úspěšné prosazení zásadního rozšíření okruhů míst, která jsou oprávněná k vydávání ověřených výpisů z úředních rejstříků a databází, do návrhu novely zákona o informačních systémech veřejné správy.

U příležitosti jubilejního desátého ročníku konference ISSS v roce **2007** získal prestižní ocenění prezident Nejvyššího kontrolního úřadu ČR **Ing. František Dohnal** za dlouholeté úsilí o rozvoj informační společnosti a významný podíl na elektronizaci veřejné správy na místní i regionální úrovni.

V roce **2008** vybrala porota jako vítěze novou službu **Dopravního podniku hl. m. Prahy** – možnost nákupu jízdenky prostřednictvím zaslání krátké textové zprávy z jakékoli stávající sítě GSM, která byla spuštěna v listopadu 2007.

V roce **2009** získaly toto prestižní ocenění dvě osobnosti, které se v posledních letech výrazným způsobem podílely na rozvoji informační společnosti v České republice – **Zdeněk Zajíček** (náměstek ministra vnitra ČR) a **Jaroslav Winter** (zakladatel sdružení BMI – Březen – měsíc internetu).

V roce **2010** bylo oceněno dlouhodobé úsilí **Kraje Vysočina** při rozvoji informatiky na úrovni kraje. Ocenění bylo předáno do rukou současného hejtmána MUDr. Jiřího Běhounka a jeho předchůdců na tomto postu Ing. Františka Dohnala a RNDr. Miloše Vystrčila.

V roce **2011** porota udělila cenu oblíbené celostátní soutěži o nejlepší webové stránky měst a obcí „**Zlatý erb**“, která byla podle slov odborné poroty v minulých letech nesmírně důležitá pro zprůhlednění procesů probíhajících na úřadech měst a obcí. Přispěla zásadním způsobem k prosazení webových stránek jako důležitého informačního kanálu a rovněž k posunu vnímání webů obcí a měst od pouhé prezentace k efektivní komunikaci s občany.

V roce **2012** byl Českým zavináčem oceněn **Ondřej Felix**, a to za zásadní přínos pro elektronizaci veřejné správy v ČR, který sehrál v roli hlavního architekta e-governmentu, a za dotažení řady klíčových projektů do fáze konečné realizace.

V roce **2013** získala tradiční cenu **ICT Unie**. Porota ocenila především celkový přínos k dalšímu rozvoji informatizace veřejné správy a trvalé úsilí o smysluplný dialog mezi světem ICT a veřejnou sférou přinášející benefity celé společnosti.

V roce **2014** porota ocenila velice potřebnou osvětovou činnost v oblasti internetu a elektronických služeb a rozhodla se udělit cenu sdružení **CZ.NIC**. Při rozhodování přihléda i k dalším aktivitám sdružení, které přispívají k rozvoji informační společnosti, jako jsou podpora open-source projektů, provoz národního bezpečnostního týmu CSIRT.CZ či implementace nových technologií (IPv6, DNSSEC).

V roce **2015** zaměřila porota svoji pozornost na důležité momenty informatizace veřejné správy v celé dosavadní historii rozvoje e-governmentu a shodla se na tom, že jedním z nejvýraznějších impulzů v posledních dvou dekádách bylo populární roadshow „**Internet mění svět**“ z roku 2001, které iniciovalo sdružení SPIS a vedle jeho prezidentky Jitky Pavlonové se na něm podíleli politici Ivan Langer, Karel Březina a Vladimír Mlynář.

V roce **2016** byl oceněn pedagog, publicista a současný radní ČTÚ **Jiří Peterka**, a to především za dlouhodobou publicistickou a analytickou činnost v oblasti elektronických komunikací a zároveň za odvahu přejít na druhou stranu barikády a měnit tento segment z pozice radního Českého telekomunikačního úřadu.

Více informací včetně kompletního archivu minulých ročníků lze najít na www.issc.cz.

Zlatý erb 2017

Devatenáctý ročník oblíbené soutěže o nejlepší webové stránky a elektronické služby měst a obcí je v plném proudu. Soutěže se aktivně zúčastnily obce a města z celé ČR. Celkově se letos zapojilo 504 přihlášených projektů obcí a měst včetně elektronických služeb, ve srovnání s minulým ročníkem se počet soutěžících navýšil o více než 50 %. Do kategorie Cena ministryně pro místní rozvoj, která se uděluje v rámci celostátního kola soutěže za nejlepší turistickou prezentaci, se přihlásilo 75 projektů.

Smysl soutěže Zlatý erb spočívá nejen ve vlastním srovnání webů měst a obcí, ale jejich webmasterům a provozovatelům poskytuje také užitečné informace a hodnocení pro další zlepšování. Vítězové jednotlivých kategorií krajských kol mají zajištěn vstup zdarma na konferenci ISSS v Hradci Králové a na odborné semináře zaměřené na hodnocení webů a s tím spojenou problematiku.

Hlavní ceny jsou v krajských kolech i celostátním kole udělovány v kategoriích **nejlepší webové stránky města**, **nejlepší webová stránka obce** a **Smart City** a **nejlepší elektronická služba**. V celostátním kole bude udělena také **cena ministryně pro místní rozvoj za nejlepší turistickou prezentaci**, mimo měst a obcí mohou soutěžit i kraje, regiony a turistické destinace.

Vyhlašovatelem a hlavním organizátorem soutěže Zlatý erb je od roku 2017 spolek **Český zavináč**. Všechny potřebné informace včetně přihlašovacího formuláře jsou k dispozici na www.zlatyerb.cz.

Prezentace tchajwanských dodavatelů

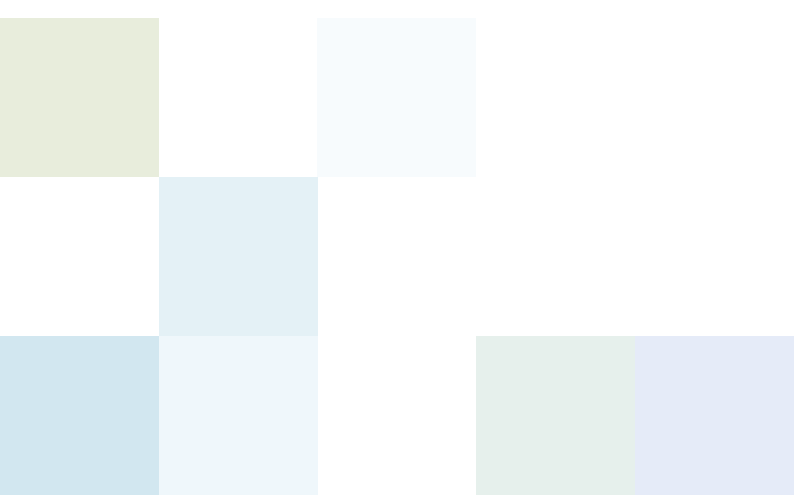
Dlouhodobá spolupráce Tchaj-wanu a Kraje Vysočina v oblasti digitalizace veřejné správy a dalších oblastí, jako je například zdravotnictví, přinesla další plody. Odstartovalo to pozvání ředitele Ekonomické divize Tchajpejské hospodářské a kulturní kanceláře, která v České republice vykonává funkci zastupitelského úřadu Tchaj-wanu, ze strany hejtmána Jiřího Běhounka na předloňský ročník konference. Ředitel Ben Wu seznámil v rámci své prezentace účastníky s výsledky, jichž dosáhla tchajwanská vláda v oblasti e-governmentu a e-health v posledních letech.

V roce 2016 pak Tchajwanský Úřad pro zahraniční obchod, který podléhá ministerstvu hospodářství, pověřil státní agenturu pro podporu podnikání a investic TAITRA, aby zorganizovala delegaci nejvýznamnějších společností v oblasti digitalizace veřejné správy a dalších oblastí a zajistila prezentaci na konferenci ISSS/V4DIS 2016. Na konferenci poté prezentovalo devět tchajwanských společností produkty ze svého portfolia, ať už formou živých ukázek ve velké národní expozici nebo během vystoupení v přednáškové části akce. Účastníci se společností se zaměřují zejména na vývoj a realizaci řešení v oblasti elektronického mýta, softwarových a hardwarových řešení IVS, AMI, inteligentních sítí a systémů řízení spotřeby energií či elektronických zdravotnických systémů. Během slavnostního zahájení celé konference ISSS/V4DIS 2017 pak vystoupil i tehdejší ředitel kanceláře, pan Ron Sheau-Jung Lu.

K únoru 2017 došlo v Tchajpejské hospodářské a kulturní kanceláři k obměně vedení, ovšem spolupráce s konferencí ISSS pokračuje a také návštěvníci ISSS/V4DIS 2017 budou moci zavítat do tchajwanského pavilónu v přízemí královéhradeckého Kongresového cen-tra Aldis nebo navštívit přednášky některých z technologicky vyspělých tchajwanských dodavatelů.

20

PŘEDNÁŠKY



Mobile Device Management – hromadná správa a zabezpečení mobilních zařízení

Petra Holubcová, Ondřej Kubeček, System4u, s.r.o.

Přístupy do firemní sítě z mobilních zařízení jako jsou chytré telefony a tablety přináší firmám i zaměstnancům mnoho výhod. Zaměstnanci mohou pracovat a vzdáleně se připojovat do firemního virtuálního prostředí kdykoli a odkudkoli. Tím se zvyšuje jejich produktivita, ale zároveň vzrůstají obavy o bezpečí citlivých firemních dat, a to zejména v dnešní době, kdy je kybernetická bezpečnost na prvním místě.

Zaměstnanci pro svou práci používají nejen firemní telefony a tablety, ale i svá vlastní zařízení (BYOD) a IT oddělení si nemůže dovolit ztratit nad těmito zařízeními kontrolu.

Proto začíná být pro firmy nezbytným řešením hromadná správa firemních mobilních zařízení – Mobile Device Management (MDM) nebo také jinak Enterprise Mobility Management (EMM). Pomocí EMM nástrojů dochází k integraci mobilních zařízení do firemní infrastruktury a zaměstnanci tak mohou snadno a efektivně pracovat na svém zařízení z kanceláře, služební cesty či z domova a citlivá firemní data zůstávají stále v bezpečí a pod kontrolou.

VMware AirWatch je přední světová technologie pro hromadnou správu a zabezpečení firemních mobilních zařízení. Tuto technologii používají firmy ve více než 150 zemích světa a její řešení je překládáno do 18 jazyků včetně češtiny.

VMware AirWatch Enterprise Mobility Management zahrnuje tři oblasti práce s mobilními zařízeními, každá oblast slouží k řešení specifických potřeb.

1. **Mobile Device Management (MDM)** – správa firemních zařízení. Řeší autorizovaný/neautorizovaný přístup do sítě, připojení či vymazání zařízení nebo přidělení práv uživateli. Jediná řídicí konzole poskytuje přehled o všech registrovaných zařízeních. Pomocí organizačních skupin administrátoři efektivně spravují všechny uživatele i všechna zařízení. Ovládací panely poskytují administrátorům rychlý pohled na informace o zařízení v reálném čase.
2. **Mobile Application Management (MAM)** – správa mobilních aplikací. Řeší problém získávání, distribuce, zabezpečování a sledování mobilních aplikací, a to na zařízeních firemních, soukromých (BYOD) či sdílených. Administrátorům se z centrální konzole zobrazují dostupné a nainstalované veřejné a interní aplikace. Mohou vytvářet whitelisty a blacklisty, konfigurovat zásady konformity a omezovat nativní aplikace.
3. **Mobile Content Management (MCM)** – správa dokumentů. Chrání citlivá firemní data, přístup k jejich úložišti či přístup k intranetu. Pomocí softwarového šifrovaného kontejneru odděluje v mobilních zařízeních firemní data od soukromých a poskytuje zabezpečený tunel pro přístup k firemní síti (micro VPN).

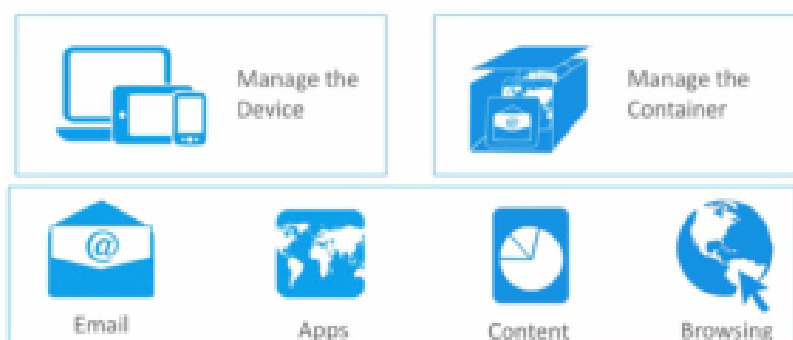
BYOD a firemní zařízení pod kontrolou

Rostoucím fenoménem ve firmách je tzv. BYOD (Bring Your Own Device). Jedná se o soukromá mobilní zařízení, které zaměstnanci používají jak pro své osobní účely, tak i pro svou práci. EMM technologie VMware AirWatch podporuje všechny hlavní mobilní platformy a dokáže v mobilním zařízení oddělit soukromá data od pracovních a citlivé firemní dokumenty tak zůstanou v bezpečí. Pokud uživatel takového zařízení opustí firmu, administrátoři mu vzdáleně odstraní přístup do firemní sítě a smažou pouze firemní data. Jeho soukromá data v telefonu stále zůstávají.

Výhody technologie VMware AirWatch:

- snadné ovládání pro uživatele i administrátory
- uživatelská i administrátorská část je v českém jazyce
- velmi široká funkcionalita systému
- technologie pro oddělení firemních a soukromých dat (šifrovaný kontejner)
- nástroje pro zabezpečení vlastních aplikací
- propracovaný reporting

What is AirWatch?



Díky zavedení EMM technologie se firma stane produktivnější. Zaměstnanci získají potřebnou flexibilitu pro práci a IT pracovníci zase požadovaný dohled nad všemi aplikacemi a dokumenty. Spokojení uživatelé mohou používat jak soukromé, tak firemní mobilní zařízení pro práci, a to vše v zabezpečeném prostředí, kde jsou jasně definovaná všechna pravidla.

Společnost System4u – partner pro MDM řešení

Společnost System4u, s.r.o. se na poli Mobile Device Managementu pohybuje již více než deset let a za tuto dobu se stala partnerem mnoha významných českých, ale i zahraničních firem. Poskytuje komplexní služby v oblasti, tedy vše od zpracování analýzy současné situace mobility ve firmě až po implementaci EMM technologií a následnou správu a podporu.

Podrobněji na www.system4u.cz

Elektronické skartační řízení v praxi

Mgr. Věra Hottmarová, Město Smiřice, Ing. Pavel Jirásek, Městská část Praha 16, Bc. Irina Rálišová, Město Sezemice, Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Skartační řízení je jedním z možných posledních kroků životního cyklu dokumentu u původce [4]. Pokud je pro podporu odborné správy dokumentů používán elektronický systém spisové služby, pak je dána zákonná povinnost i skartační řízení realizovat v elektronické podobě. Rozhodující tedy není to, zda konkrétní dokumenty, jež do skartačního řízení vstupují, jsou v listinné či elektronické podobě, ale jaká je forma primární evidence. To platí nejen pro spisovou službu, ale také pro samostatné evidence dokumentů. Jsou-li například daňové doklady a další účetní dokumenty evidovány v elektronickém systému, pak také proces jejich následné skartace musí být veden v elektronické podobě.

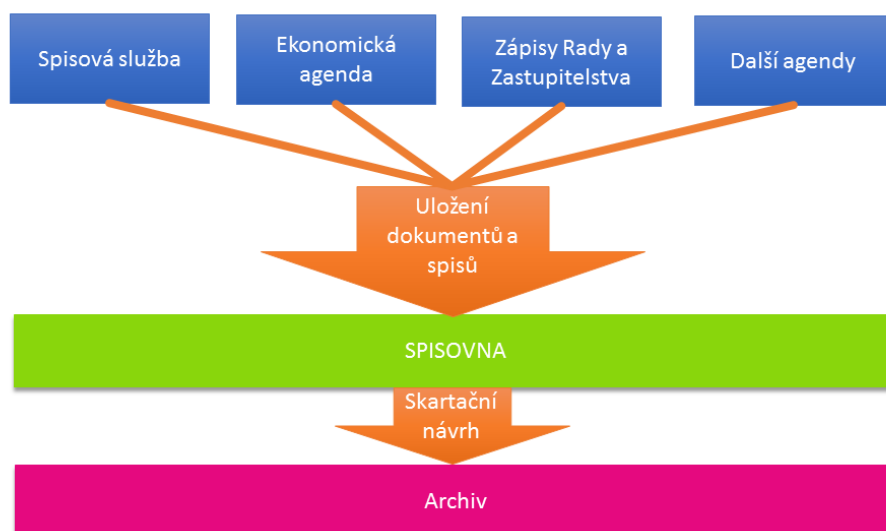
Protože se z hlediska oblasti archivnictví a spisové služby jedná o poměrně nový proces, je zkušeností s jeho praktickou realizací ještě poměrně málo. Tento příspěvek se snaží představit tři případové studie tří původců, kteří se na elektronické skartační řízení aktivně připravovali a postupně jej realizují.

Spisová služba a skartační řízení

Základními předpisy, které procesy týkající se skartačního řízení v elektronické podobě popisují, jsou zákon č. 499/2004 Sb., o archivnictví a spisové službě, vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, a v neposlední řadě Národní standard pro elektronické systémy spisové služby. Jak již bylo zmíněno, je skartační řízení jedním z možných posledních kroků životního cyklu dokumentu u původce. A právě podporu celého životního cyklu dokumentu má pokrývat spisová služba, která je citovaným zákonem předurčena k zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností [viz § 2 písm. l) cit. zákona]. Blíže k výkonu spisové služby viz kniha [4].

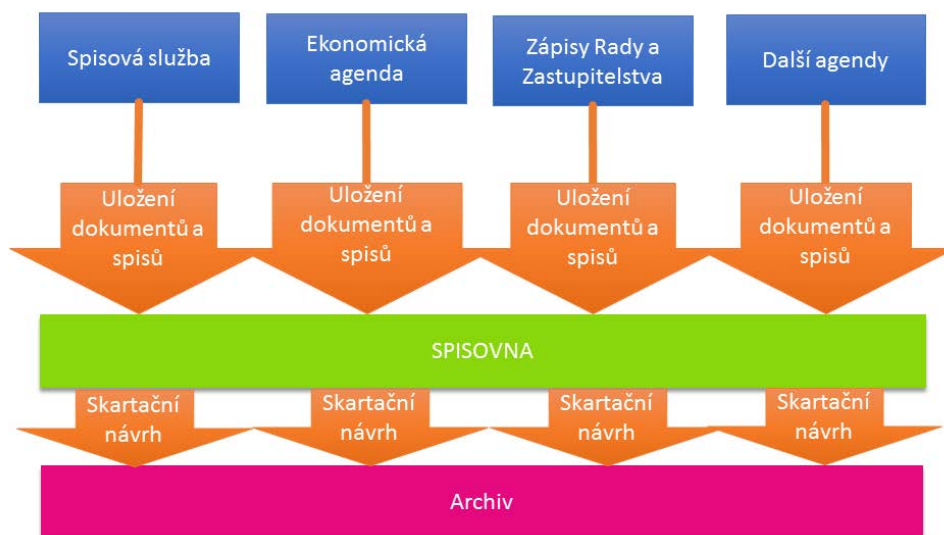
Pokud probíhalo skartační řízení v klasické podobě, bylo v praxi většinou zcela odděleno od přímého výkonu spisové služby. Jinými slovy, výkon spisové služby prakticky končil uložením dokumentů ve spisovně, pak následoval předěl v podobě skartační lhůty, po jejímž uplynutí byl sestavován skartační návrh na základě podkladů uvedených v evidenčních pomůckách spisovny. Tedy zcela odděleně od předchozí evidence dokumentů ve spisové službě, přičemž hloubka oddělující propasti mezi spisovou službou a skartačním řízením se zvyšovala se zvyšující se délkou skartační lhůty. Schematicky je uvedený stav ilustrován na Obr. 1.

Podklady pro skartační řízení v elektronické podobě nelze jednoduše získat jinak, než přímou návazností na předchozí životní cyklus dokumentu a jeho evidenci v elektronickém systému spisové služby. Proto také nejsou v zákoně o archivnictví a spisové službě definovány elektronické spisovny, neboť ty jsou vlastně integrální součástí spisové služby. Je třeba stejným způsobem však začít přistupovat i k evidenci dokumentů a spisů uložených v klasické spisovně. Vzhledem k tomu, že zde máme různé dlouhé skartační lhůty a k tomu ještě různé spouštěcí události, jež je iniciují, požadujeme vlastně nyní při realizaci skartačního řízení v elektronické podobě návaznost na něco, co už dávno bylo. I s ohledem na tento fakt vydal Národní archiv metodický pokyn [5], který říká, že komponenty, metadata a postup skartačního řízení všech dokumentů, spisů a typových spisů vyřizovaných nebo uzavřených po 31. červenci 2012 musí odpovídat všem požadavkům platných právních předpisů, avšak pro spisy a dokumenty uzavřené, resp. vyřizené do 31. července 2012 včetně jsou minimalizována povinná metadata nutná k vytvoření SIP balíčku a dále platí, že jejich komponenty není nutné převádět do výstupních datových formátů.

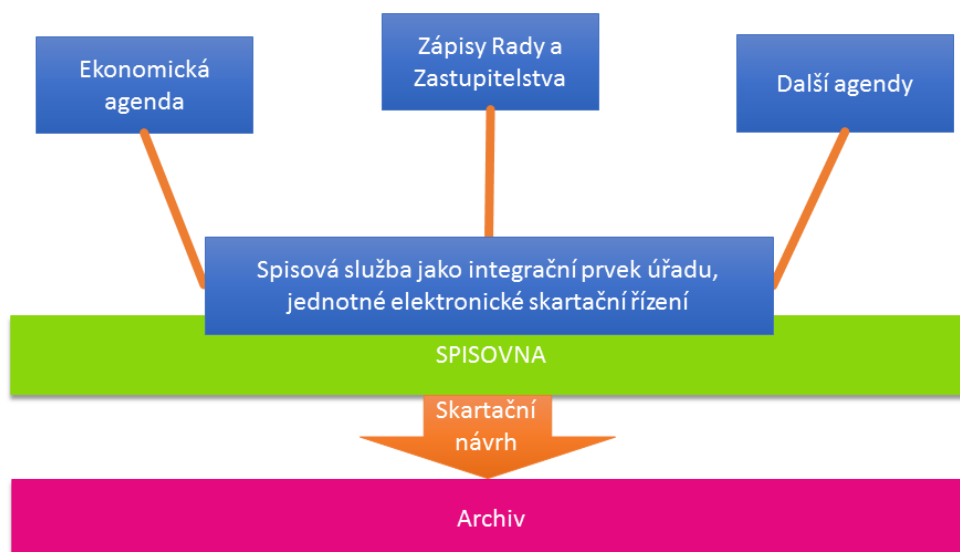


Obr. 1: Schéma procesů typické pro klasické skartační řízení.

Výše zmíněné předpisy požadují po každé elektronické evidenci dokumentů, ať se jedná o spisovou službu, nebo o speciální evidenci dokumentů v elektronické podobě, aby zajišťovala podporu pro celý životní cyklus dokumentu u původce, tedy včetně evidence spisovny, zajištění důvěryhodného uložení elektronických dokumentů po dobu plynutí skartační lhůty a podporu pro elektronické skartační řízení. Schematicky je tedy požadovaný stav znázorněn na Obr. 2. Nicméně v praxi se jeví tento přístup jako neefektivní a náročný. Proto se zvyšuje důraz na provázanost všech systémů pro evidenci dokumentů provozovaných původcem na páteřní agendu spisové služby, která pak zajistí poslední fáze životního cyklu dokumentu centralizovaně, jak ukazuje schéma na Obr. 3



Obr. 2: Schéma požadavků na provádění skartačního řízení v elektronické podobě vyplývající z aktuálních právních předpisů.



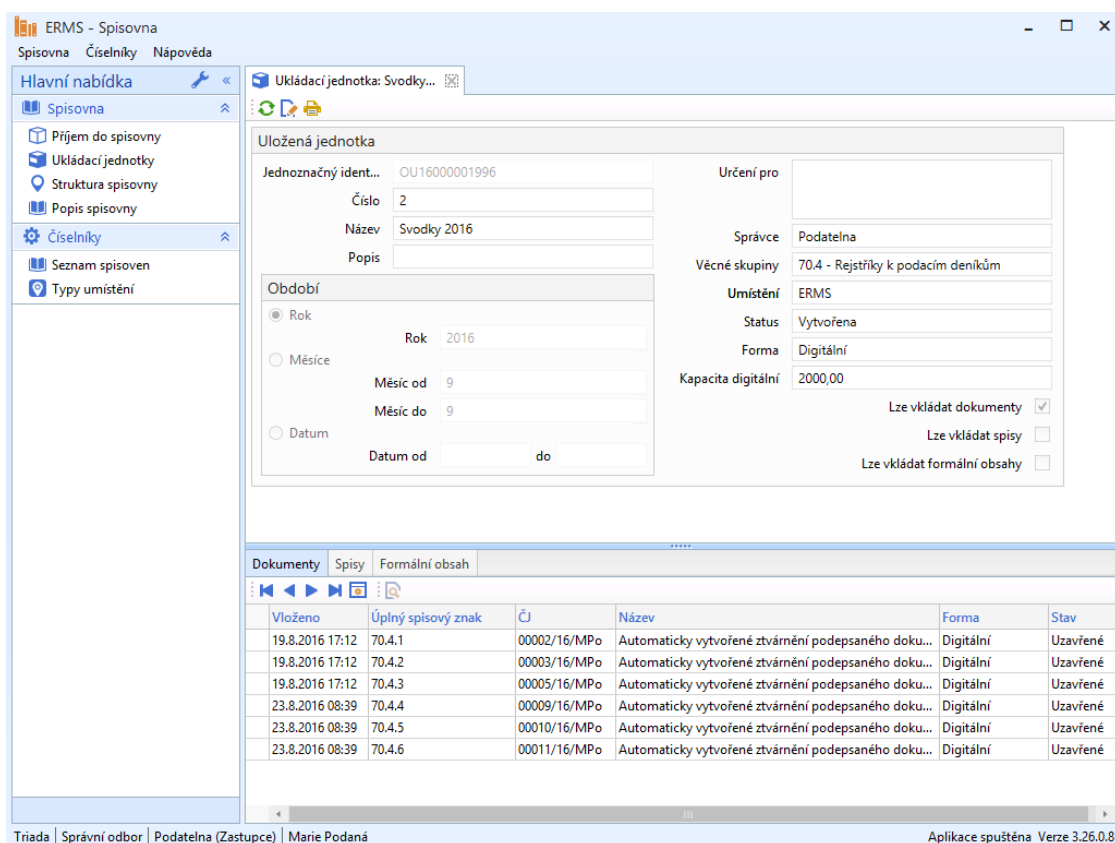
Obr. 3: Provázanost evidencí dokumentů na páteřní agendu spisové služby zajišťující podporu pro skartační řízení.

Příprava na skartační řízení v elektronické podobě

Jak jednoznačně plyne z předchozího textu, je příprava na elektronické skartační řízení dlouhodobý systematický proces, který musí zahrnovat správné vedení spisové služby a dále napojování samostatných evidencí dokumentů v elektronické podobě na páteřní agendu spisové služby. Je potřeba zdůraznit zejména onu dlouhodobost, která je spjata s během skartační lhůty. Jak plyne z výše citovaného metodického pokynu, musíme mít přesnou evidenci nejméně těch dokumentů a spisů, které byly vyřízeny resp. uzavřeny od 31. července 2012. Nicméně do skartačního návrhu v elektronické podobě musíme být schopni zařadit i mnohem starší dokumenty a spisy. S největší pravděpodobností je nebudeme mít přímo v elektronické spisové službě, když byly vyřízeny či uzavřeny třeba před 20 lety (např. tedy v době konání prvního ročníku konference ISSS). Nastupuje zde významná role vhodného elektronického nástroje, který dokáže zajistit zpětné naplnění celkové evidence.

Tvůrci informačního systému Munis na tyto potřeby myslí a upravují modul Spisovna, který je součástí elektronické spisové služby Munis ERMS tak, aby umožňoval různé vstupy, nejen ty, které přímočarě plynou z vlastní evidence této spisové služby. Základem evidence v aplikaci Spisovna je ukládací jednotka, která může obsahovat dokumenty, spisy a tzv. formální obsah (viz Obr. 4). Dokumenty, které nejsou součástí spisů, a spisy včetně všech do nich vložených dokumentů vstupují do spisovny výhradně z primární evidence vedené v elektronickém systému spisové služby. Pokud v rámci IS Munis vznikají anebo jsou evidovány další dokumenty, jsou různými vazbami přímo zaevidovány také v Munis ERMS, odkud se pak dostávají do spisovny.

Naopak výše zmíněný tzv. formální obsah je evidován právě až na úrovni spisovny. Jde o mocný nástroj umožňující popisovat nejen jednotlivosti (jednotlivé dokumenty či spisy), ale též jejich soubory pomocí jednoho generického popisu. V případě rozříštěnosti informačních systémů původce a různých neprovázaných (a neprovázatelných) samostatných elektronických evidencí dokumentů lze tak snadno doplnit evidenci spisovny o výstupy z těchto systémů. Stejně tak lze doplnit i historické dokumenty a spisy, které byly vyřízeny či uzavřeny před tím, než na úřadě byl elektronický systém spisové služby veden. Samozřejmě se v těchto případech jedná vesměs o metadata o analogových dokumentech a nikoliv o digitální dokumenty. Musíme však mít stále na paměti, že forma dokumentu není pro způsob realizace skartačního řízení rozhodující.



Obr. 4: Detail ukládací jednotky v aplikaci Spisovna, který je součástí Munis ERMS.

Zbývá tedy zdůraznit poslední věc, a tou je vyjasnění si toho, co to znamená správné vedení spisové služby v elektronické podobě. Základem je samozřejmě implementovaný vhodný elektronický nástroj, např. Munis ERMS. Ale ten sám o sobě nestačí. Pokud jej uživatelé nebudou používat, pokud úředníci nebudou označovat vyřízení dokumentů, pokud nebudou uzavírat spisy, pak výsledná evidence nikdy nebude úplná a správná.

Kromě potřebných procesů, které mají být ve spisové službě realizovány, je třeba věnovat pozornost také správnému vyplňování metadat. Elektronický systém spisové služby může mít implementovány různé kontroly, ale zda je věc dokumentu popsána tak dobře, aby následně mohl podle ní archivář rozhodnout, zda přijme dokument jako archiválii, nebo zda vydá souhlas se skartací, to už žádný systém do důsledku ohlídat nemůže, to závisí jen na správném přístupu úředníka.

Připomeňme, že podle § 10 odst. 1 a 2 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, musí být dobře popsán zejména (uveden výběr toho, kde se často chybuje):

- stručný obsah dokumentu – písm. f),
- údaje o kvantitě dokumentu – písm. e), čímž se rozumí počet listů, jde-li o dokument v listinné podobě, počet listů nebo počet svazků příloh v listinné podobě, počet a druh příloh v nelistinné podobě včetně příloh v digitální podobě, přičemž u dokumentu v digitální podobě se počet a druh příloh uvádí pouze v případě, že je povaha dokumentu umožňuje určit,
- údaje o vyřízení dokumentu – písm. h), které zahrnují způsob vyřízení, popř. identifikace adresáta, datum odeslání, počet a druh odeslaných příloh, přičemž opět u dokumentu v digitální podobě se počet a druh příloh uvádí pouze v případě, že je povaha dokumentu umožňuje určit.

Minimálně toto vše dohromady tedy znamená správné vedené spisové služby. Pojdme se nyní podívat na několik příkladů dobré praxe, které uvedené podmínky plně naplňují.

Případová studie města Smiřice

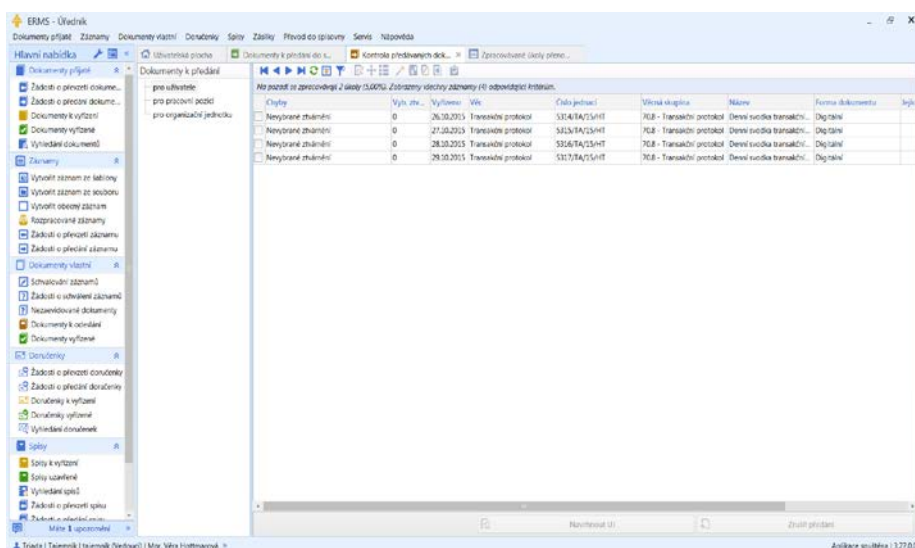
Město Smiřice leží přibližně 15 km od Hradce Králové směrem na Jaroměř a je součástí mikroregionu Smiřicko. Město má 3 tisíce obyvatel. Smiřice se pyšní dvěma národními kulturními památkami, a to barokní kaplí Zjevení Páně (obr. 1) a v ní umístěným Brandlovým obrazem Klanění Tří králů. Více informací viz [1].

Městský úřad Smiřice je pověřeným obecním úřadem, jehož správní obvod tvoří 12 obcí s více než 8 tisíci obyvateli. Úřad je členěn na odbory: správní odbor vč. matriky, ekonomický odbor, odbor správy majetku a životního prostředí a odbor výstavby. Pracuje zde celkem 29 zaměstnanců, přičemž elektronickou spisovou službu využívá sedmnáct z nich a starosta.



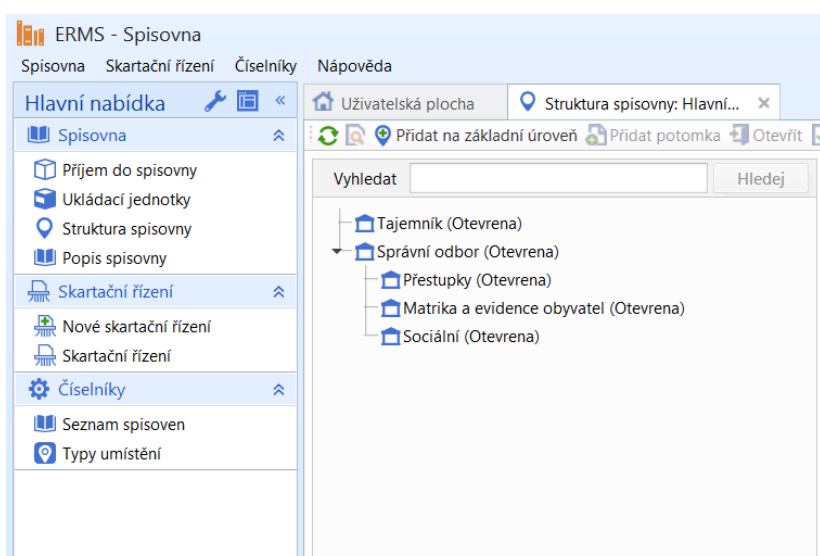
Obr. 5: Interiér kaple Zjevení Páně – zdroj [1].

Úřad vede spisovou službu od začátku ledna 2007, přičemž implementace probíhala již během podzimních měsíců roku 2006. Všichni pracovníci úřadu tak byli zvyklí na elektronickou evidenci dokumentů ještě dříve, než se stala více méně praktickou nutností vyvolanou nástupem informačního systému datových schránek v červenci 2009. Od roku 2011 probíhá na úřadě další elektronizace dokumentů předem určených a vybraných typů. Dlouhodobým používáním spisové služby realizované prostřednictvím modulu Kancelář a dalších modulů informačního systému Munis si uživatelé zvykli na systematický a metodický přístup k evidenci dokumentů i k jejich digitalizaci. V roce 2016 jsme přešli na technologického nástupce původních modulů – elektronickou spisovou službu Munis ERMS. Převod proběhl během měsíce května a došlo při něm také k převodu všech dokumentů a spisů. Evidence je tedy stále kontinuální a úplná. Sžívání se s novým systémem bylo samozřejmě spojeno s mnohými školeními, dotazy a potřebnými konzultacemi, nicméně nakonec jsme vše zvládli a pustili jsme se do přípravy podkladů pro naše první skartační řízení v elektronické podobě.



Obr. 6: Kontroly dokumentů při přenosu do spisovny.

V aplikaci Spisovna, která je nedílnou součástí elektronické spisové služby Munis ERMS, jsme si připravili strukturu spisovny čítající prozatím dvě základní uložení, tedy místa kde jsou pak uchovávány ukládací jednotky s dokumenty a spisy (viz Obr. 7). Následně jsme začali uzavřené spisy přesouvat do této evidence. Šlo vlastně o převod existující evidence spisovny (archivní knihy) do elektronické podoby evidence v aplikaci Spisovna. Při tomto formálním přesunu dochází také k řadě formálních i technických kontrol. Jejich příklad pro dokumenty je uveden na Obr. 6, kde jsou zobrazeny dokumenty s více ztvárněními, přičemž program dává na výběr, která ztvárnění budou zachována pro uložení ve spisovně. Asi největším problémem tohoto přesunu jsou starší digitální dokumenty, které byly přijaty prostřednictvím elektronické podatelny, tedy ve formátu EML. Jeho převod do výstupního formátu podle zákona o archivnictví a spisové službě a příslušné vyhlášky není jednoznačně vyřešen. Naštěstí se v našem případě jedná vesměs o dokumenty vyřízené před 31. červencem 2012, a proto převod nebude zřejmě nutný (viz [5]). Ovšem vidíme v tom jeden ze zásadních problémů, který by mohl být lépe řešen na úrovni centrálního archivního portálu, než na úrovni jednotlivých původců.



Obr. 7: Iniciační struktura spisovny MěÚ Smiřice.

V současné době máme připraveno 10 kompletních spisů z roku 2010, které budeme zařazovat do skartačního návrhu našeho prvního skartačního řízení v elektronické podobě. Přidáme k nim ještě denní souhrny transakčního protokolu, což jsou dokumenty se skartačním režimem A/1. U všech přesunutých dokumentů a spisů do spisovny umožňuje Munis ERMS okamžité vygenerování SIP balíčku bez nutnosti vytvářet celý skartační návrh. Díky tomu si lze ověřit výsledné SIP balíčky ve validátoru dostupném na webových stránkách národního archivu. Podařilo se nám tak odhalit několik drobných formálních chyb, které byly odstraněny ještě dříve, než jsme se pustili do přímé komunikace s archivem v rámci skartačního řízení. Nyní jsme tedy na první skartační řízení v elektronické podobě plně připraveni. Na základě získaných zkušeností budeme převádět do spisovny složitější spisy, např. stavební agendy apod.

Vlastní skartační řízení je obsaženo v aplikaci Spisovna, kde z navržených dokumentů a spisů podle skartačních lhůt sestavíme seznam pro skartační návrh. Aplikace k němu vygeneruje automaticky průvodní dopis a vše pošle jako dokument přes elektronickou spisovou službu. Reakce archivu je zapsána na podatelně jako standardní podání a dále v rámci vyřizování v aplikaci Úředník spárována s daným skartačním řízením. Výsledek je pak zobrazen opět v aplikaci Spisovna. Následuje pak vygenerování tří dalších dokumentů:

- podkladů pro skartaci analogových dokumentů,
- podkladů pro přenos analogových archiválií do archivu,
- seznamu kompletních SIP balíčků s průvodním dopisem pro přenos digitálních archiválií do digitálního archivu.

Skartace digitálních dokumentů je provedena přímo v elektronické spisové službě Munis ERMS. Výsledek tohoto našeho prvního skartačního řízení v elektronické podobě bychom rádi prezentovali na konferenci.

Případová studie městské části Praha 16

Hlavní město Praha je členěno na 22 správních obvodů a 57 městských částí. Městská část Praha 16 (ilustrační fotografie viz Obr 8) je jednou z těchto částí ležící na jihozápadním okraji města. Současně je sídlem správního obvodu, který zahrnuje území městských částí Praha 16 (katastrální území Radotín), Praha-Lipence, Praha-Lochkov, Praha-Velká Chuchle (katastrální území Velká Chuchle a Malá Chuchle) a Praha-Zbraslav (katastrální území Zbraslav a Lahovice). Celý správní obvod měl k 1. lednu 2017 celkem 20 818 obyvatel (z toho v Radotíně 8 026) při rozloze 3 616 ha (z toho Radotín 931 ha). Další informace o městské části lze najít na webových stránkách [2].

Úřad městské části Praha 16 je členěn na odbory, jejichž úkolem je vykonávat státní správu (u většiny agend pro celý správní obvod) a samosprávu (pouze pro Radotín) dle Organizačního řádu úřadu, případně dle pověření Rady městské části tak, aby byla zajištěna činnost úřadu jako orgánu městské části. Aktuální podobu organizační struktury představuje schéma na Obr. 9.

Úřad vede spisovou službu pomocí elektronických nástrojů již od roku 2002, tedy delší dobu, než platí zákon o archivnictví a spisové službě. Samozřejmě že vývoj legislativy významně ovlivnil konkrétní podobu jednotlivých kroků spisové služby a též funkcionality příslušných modulů informačního systému Munis, který po celou dobu pro výkon spisové služby využíváme. Nejprve se jednalo o modul Kancelář a další přidružené moduly. Následně, v roce 2015, jsme přešli na technologické nástupce původního řešení v podobě elektronické spisové služby Munis ERMS. Využili jsme toto nasazení pro celkovou revizi procesů spojených s evidencí dokumentů od jejich přijetí, až po jejich odeslání a uložení ve spisovně. Významnou změnou bylo též zavedení striktních pravidel do schvalovacích procesů. Zároveň jsme postupně provedli přenos všech dokumentů a spisů ze starého systému do nového. Celkem bylo přeneseno více než 260 tisíc dokumentů včetně mnoha desítek návazných spisů.



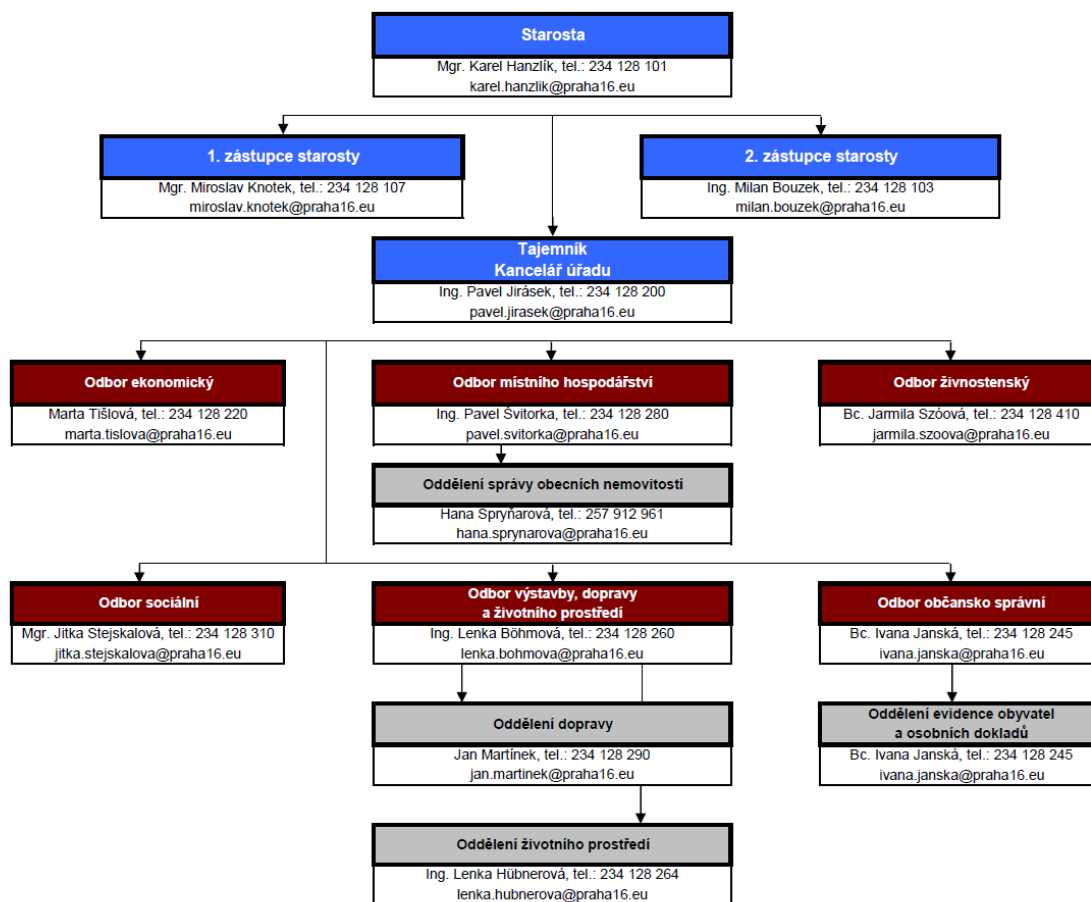
Obr. 8: Letecký snímek Prahy 16 – autor Ing. Pavel Jirásek.

Dalším přímočarě navazujícím krokem rozvoje implementace elektronické spisové služby bylo zavedení elektronické evidence spisovny, jejíž struktura je poměrně složitá. Každý odbor úřadu má svou vlastní spisovnu, nad níž má dohled příslušný vedoucí. Z hlediska nastavení v modulu Munis ERMS tedy nešlo jen o přenesení vlastní struktury, ale též nastavení příslušných přístupových práv k jednotlivým spisovnám. Každá z nich má samozřejmě svou specifickou vnitřní strukturu, která také byla do aplikace Spisovna přenesena. Ačkoliv má každý odbor svou vlastní spisovnu, úřad sestavuje jeden skartační návrh za všechny tyto spisovny. I s tím si příslušná aplikace Spisovna modulu Munis ERMS poradí.

Nyní jsme tedy ve fázi, kdy převádíme současnou listinnou evidenci spisovny do elektronické podoby s tím, že tam primárně vkládáme vyřízené dokumenty a uzavřené spisy vedené přímo ve spisové službě. Jde tedy o jakési formální rozřazování podle struktury spisovny a zároveň formální kontrolu úplnosti popisných dat k jednotlivým entitám. Také jsme za každý odbor vytipovali několik dokumentů a spisů, u nichž právě uplynula skartační lhůta, a můžeme je zařadit do skartačního návrhu, který bude poprvé připraven v elektronické podobě a předán Archivu hlavního města Prahy. Celý návrh sestávající se s balíčku SIP podle přílohy č. 2 a 3 Národního standardu pro elektronické systémy spisové služby automaticky vygeneruje aplikace Spisovna jako nedílná součást elektronické spisové služby Munis ERMS.

Nezbytnou podmínkou, abychom k tomu všemu mohli přistoupit, je dlouhodobé precizní vedení spisové služby v elektronické podobě postihující celý životní cyklus dokumentů a spisů na úřadě. Každý úředník musí chápat spisovou službu jako nedílnou součást výkonu své činnosti a rozumět jednotlivým krokům tak, aby zvládnul zaznamenat správně všechny procesní kroky a nezbytné údaje včetně začlenění spisů i samostatných dokumentů do spisového a skartačního plánu úřadu, jež je základem pro členění výsledného skartačního návrhu. Výsledek našeho prvního skartačního řízení v elektronické podobě bychom rádi prezentovali na konferenci.

Organizační struktura Úřadu městské části Praha 16
ke dni 31. 1. 2017



Obr. 9: Organizační schéma ÚMČ Praha 16.

Případová studie města Sezemice

Město Sezemice, které leží při řece Loučné nedaleko polabské dominanty, Kunětické hory. Patří k nejstarším sídlištím Pardubického kraje. Nejstarší zaznamenaná písemná zpráva o Sezemících pochází z roku 1227. Zatímco na počátku druhé poloviny 17. století bydlelo v Sezemících pouhých 339 obyvatel, v dnešní době žije v Sezemících, včetně připojených obcí Dražkova, Kladiny, Lukovny, Počapel, Velkých Kolodějů a Veské, celkem 3818 obyvatel.

Město Sezemice je obcí I. typu, avšak vykonává také přenesenou působnost na úseku stavebního úřadu a na úseku matriky a evidence obyvatel. Městský úřad (ilustrativní foto viz Obr. 10) se člení na úseky – matriku a evidenci obyvatel a na odbory – kancelář vedení úřadu, finanční odbor, odbor stavebního úřadu a územního plánování a odbor správy majetku a životního prostředí. Celkový počet pracovníků v městském úřadu je 35, z nichž je 16 úředníků, kteří v současné době využívají elektronickou spisovou službu. Dále elektronickou spisovou službu využívá starosta a místostarosta.



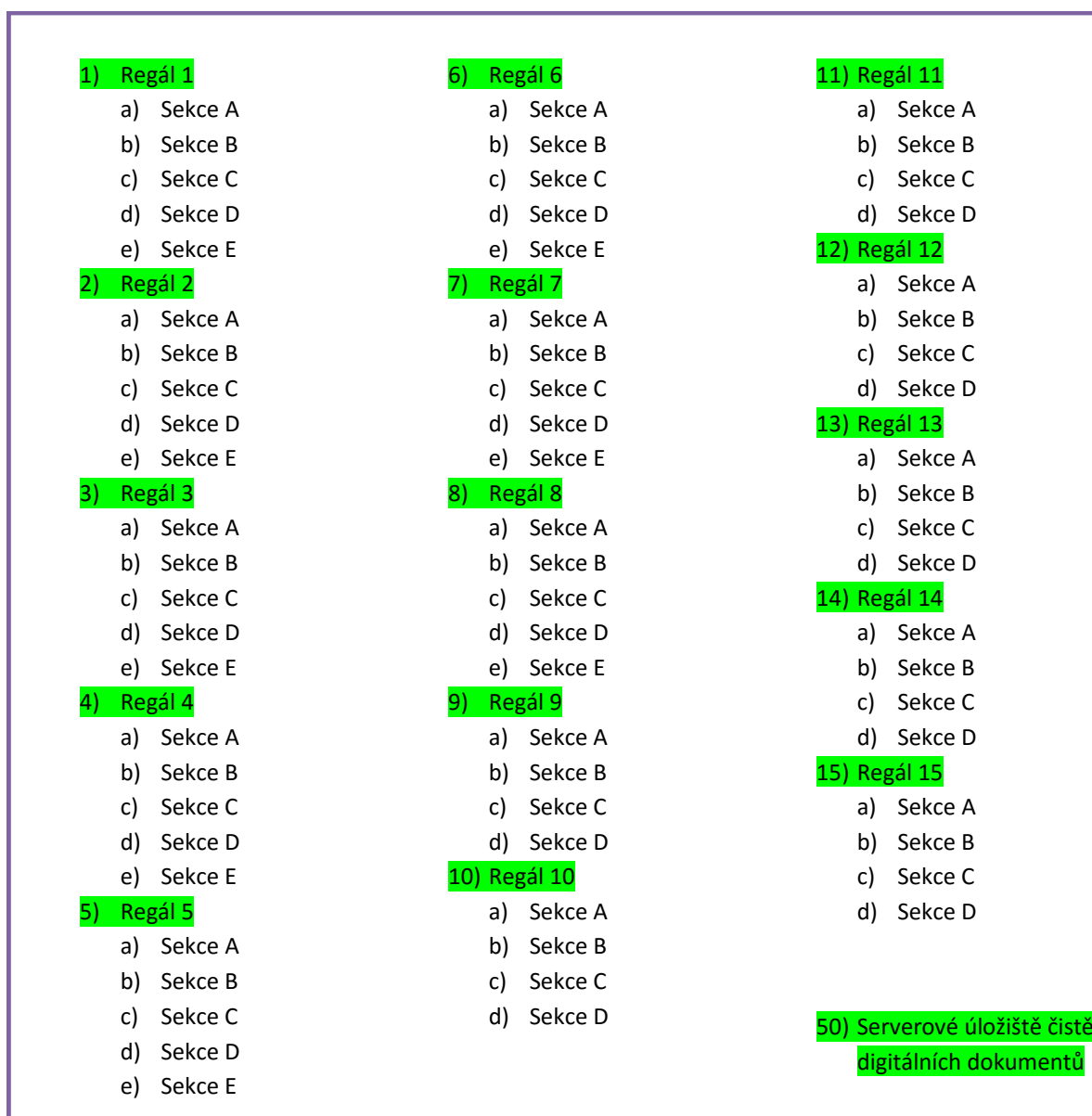
Obr. 10: Pohled na městský úřad Sezemice – zdroj [3].

Úřad vede spisovou službu pomocí elektronických nástrojů od začátku roku 2005. Implementace systému probíhala v roce 2004. Tehdy se jednalo o modul Kancelář informačního systému Munis a další související moduly. Primární motivací bylo řešení nástroje pro realizaci elektronické podatelny, ale nakonec byla do elektronické podoby převedena celá evidenci podatelny. Došlo tím ke sjednocení pravidel pro příjem listinných i elektronických dokumentů.

Lze tedy říci, že historie vedení spisové služby pomocí elektronický nástrojů na úřadě je stejně dlouhá jako historie aktuálního právního předpisu regulujícího tuto oblast, tedy zákona č. 499/2004 Sb., o archivnictví a spisové službě. Stejně jako tento zákon byl za dobu své existence několikrát novelizován, docházelo ke změnám i v příslušných elektronických nástrojích využívaných městským úřadem. K modulu Kancelář přibývaly další specifické moduly pro nové vazby na nástroje e-Governmentu, jako např. datové schránky nebo CzechPOINT, i pro vazbu na agendové informační systémy, jako např. pro agendu stavebního úřadu. Poslední z těchto změn byl přechod na technologického nástupce uvedených modulů, tedy na elektronickou spisovou službu Munis ERMS. K tomu došlo na podzim roku 2014. V rámci převodu byly přeneseny ze starého do nového systému také všechny dokumenty a spisy.

Jak v případě prvotní implementace v roce 2004, tak při nasazení elektronické spisové služby Munis ERMS v roce 2014 se nám velmi osvědčilo školení uživatelů přímo na počítačích. Pronajali jsme si od místní školy počítačovou učebnu, kde společnost Triada dočasně nainstalovala stejnou verzi spisové služby jako na úřadě, a naši pracovníci si mohli rovnou probírané postupy zkusit na počítačích. V obou případech se nám tento postup velmi vyplatil, protože uživatelé následně zvládali práci se spisovou službou velmi dobře, a to hned od samého počátku.

V loňském roce jsme se dále začali aktivně připravovat na skartační řízení v elektronické podobě. Protože elektronickou evidenci dokumentů a spisů máme vedenou dlouhodobě a do všech detailů, znamenalo to pouze doplnění popisu struktury spisovny (viz Obr. 10) a naplnění daty formálním převodem vyřízených dokumentů a uzavřených spisů, tedy rozčleněním do jednotlivých ukládacích jednotek podle věcných skupin a roku vyřízení či uzavření.

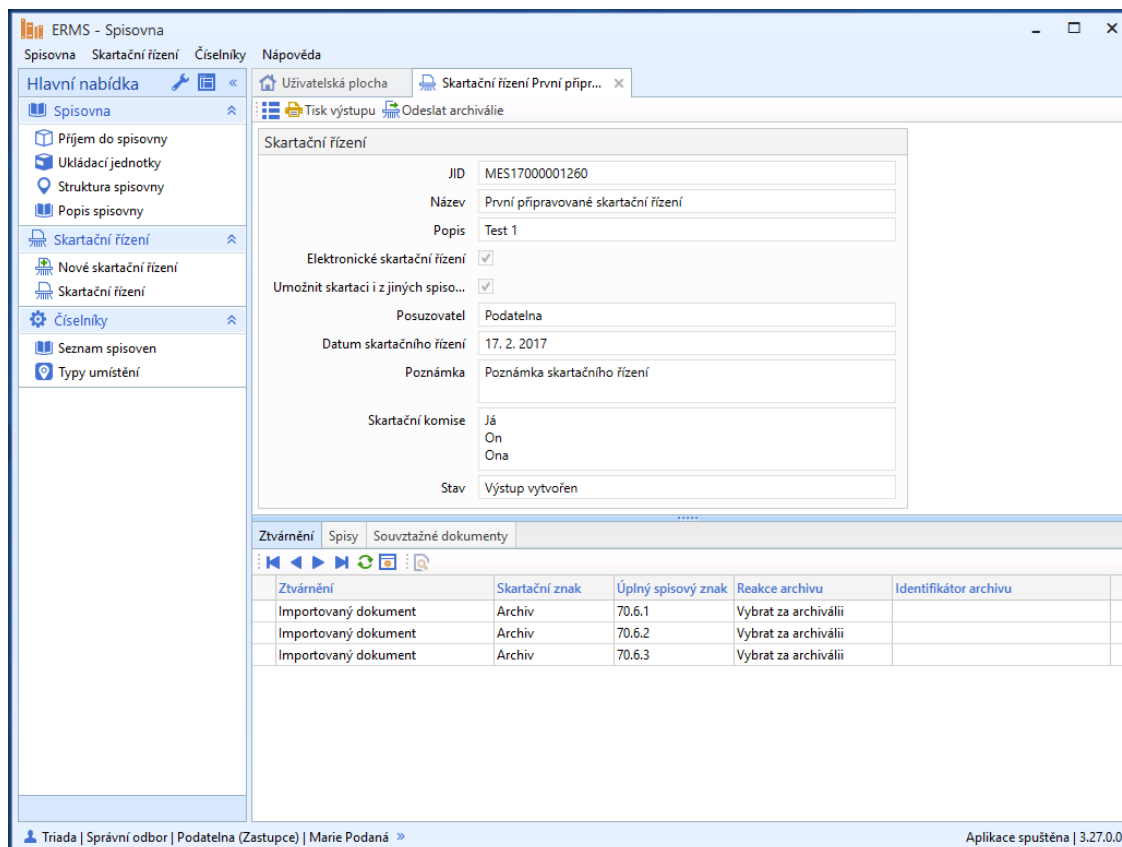


Obr. 11: Struktura spisovny na MěÚ Sezemice.

Pro naše první skartační řízení v elektronické podobě jsme se rozhodli použít denní souhrny transakčních protokolů, které mají přiřazen skartační režim A/1. Půjde tedy o čistě digitální dokumenty, a tím bude ověřen nejen skartační návrh se seznamem dokumentů a balíčky SIP podle přílohy č. 2 a 3 Národního standardu pro elektronické systémy spisové služby, načtení odpovědi archivu podle přílohy č. 4 téhož standardu, ale také následný přenos digitálních dokumentů do archivu. Všechny části procesu přípravy spisovny i skartačního řízení v elektronické podobě aktivně konzultujeme s pracovníky dodavatele elektronického systému spisové služby i s příslušným oblastním archivem. Protože jsme se oblasti spisové služby věnovali opravdu důkladně, vyplynula z toho přímočaře potřeba úpravy spisového řádu úřadu a také jsme při tom provedli důkladnou revizi spisového a skartačního plánu. Výsledek našeho prvního skartačního řízení v elektronické podobě bychom rádi prezentovali na konferenci.

Shrnutí

Skartační řízení v elektronické podobě je kvalitativně nový proces, který staví na mnoha zkušenostech z původního skartačního procesu, ale také přidává mnoho nového. Bez pečlivě vedené spisové služby a dlouhodobé podpory precizního výkonu spisové služby, zejména ze strany vedení organizace, jej nelze realizovat. Na druhou stranu, pokud má úřad kvalitně vedenou spisovou službu, není příprava a provedení skartačního řízení v elektronické podobě v žádném případě nepřekonatelnou překážkou.



Obr. 12: Detail skartačního řízení v aplikaci Spisovna v elektronické spisové službě Munis ERMS

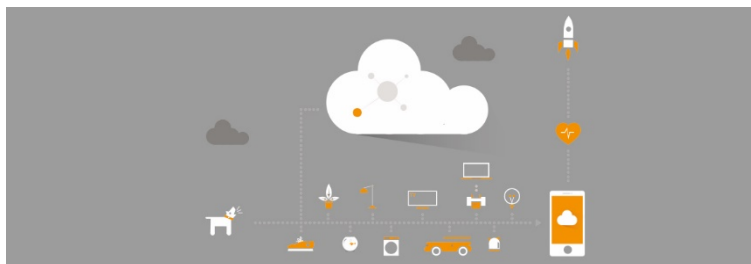
Literatura

- [1] Oficiální webové stránky Města Smiřice dostupné na adrese <<http://www.mestosmirice.cz>>.
- [2] Oficiální webové stránky Městské části Praha 16 dostupné na adrese <<http://www.praha16.eu>>.
- [3] Oficiální webové stránky Města Sezemice dostupné na adrese <<http://www.sezemice.cz>>.
- [4] M. Kunt, T. Lechner. *Spisová služba*. Praha: Leges, 2015.
- [5] Metodický pokyn Národního archivu dostupný na adrese <http://digi.nacr.cz/wp-content/uploads/2014/10/prechodnaObdobi_cistopis.pdf>.

Objevte svět internetu věcí – chytrá řešení pro moderní vedení města

Přínosy IoT sítě LoRa od Českých Radiokomunikací pro platformu chytrých měst

Ing. Ján Jacina, business development manager pro IoT, České Radiokomunikace a.s.



Česká republika je už čtvrt století připojena k internetu. To, co se v současné době zdá jako naprosto běžná a nedílná součást našeho života, bylo ještě před pětadvaceti lety téměř sci-fi. Na internet se tehdy připojovaly jen důležité státní orgány, vědecká centra a mezinárodní firmy. Nyní přichází nový trend v internetové éře – velmi masivně se rozvíjí technologie a sítě, kde spolu komunikují „věci“ – přesněji řečeno senzory, čidla a zařízení – jejich komunikace spočívá ve využití speciálního datového protokolu určeného právě pro komunikaci věcí kolem nás.

Technologicky orientované společnosti se zaměřují na vývoj koncových zařízení pro široké využití. Hledají prostor pro výrobu milionů koncových zařízení a pokoušejí se vyvolat poptávku po svých výrobcích v dosud neobsazených oblastech lidské činnosti. Díky tomu vznikají spousty konkrétních projektů. Kromě chytré výroby a potenciálu oblasti průmyslu 4.0 se v současné době velmi rychle rozvíjí sféra tzv. chytrých měst.

Internet věcí (IoT) zahrnuje čtyři základní kategorie ekosystému:

- vlastní zařízení – široké spektrum čidel a senzorů,
- komunikační síť – firmy se soustředí na rozvoj a využití stávající technologické infrastruktury,
- platformu pro uložení a zpracování získaných dat,
- software pro koncové uživatele – možnost řízení cílových procesů na dálku (např. řízení dopravy, optimalizace energetické soustavy, optimalizace svozu odpadu apod.).

IoT infrastruktura a role Českých Radiokomunikací

České Radiokomunikace (CRA) sledují technologické trendy a chtějí v internetu věcí sehrát svou roli. Je zřejmé, že ji chtějí sehrát tím způsobem, který je jim nejbližší – tedy telekomunikační a IT částí. Cílem je **vybudovat telekomunikační infrastrukturu**, která zajistí přenos dat formou zpráv přenášených bezdrátovou komunikací od jednotlivých zařízení. Dalším cílem je vybudovat **platformu**, na které ve spolupráci s vhodnými obchodními partnery zajistí komplexní řešení pro co nejširší spektrum projektů internetu věcí – platformu, která mimo jiné nabízí i řešení pro efektivní řízení fungování a chodu měst a obcí.

CRA jsou si plně vědomy toho, že pro plnění své role mají v České republice **vynikající předpoklady**:

- disponují řádově stovkami věží, které byly původně budovány s cílem pokrýt co největší území analogovým televizním signálem,
- disponují telekomunikační sítí mezi výše uvedenými věžemi. Tím mají vybudovanou nosnou infrastrukturu pro rozmístění radiových koncentrátorů pro IoT technologie,

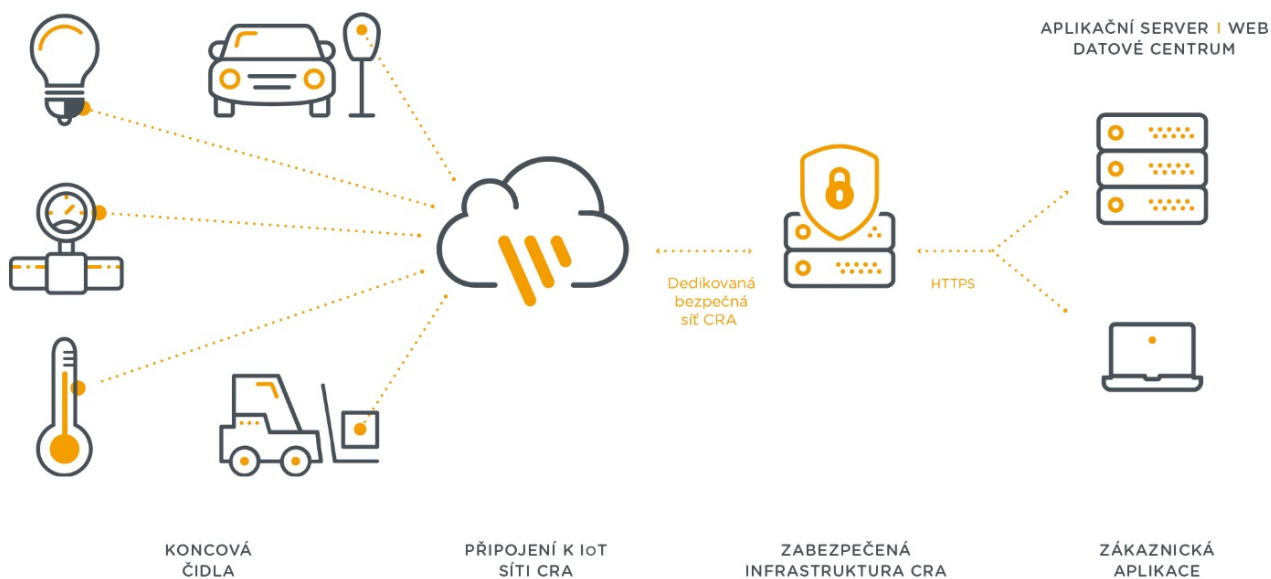
- disponují datovými centry s maximálním možným zabezpečením jak po stránce fyzické, tak i kybernetické bezpečnosti. Díky tomu poskytují optimální prostor pro umístění centrální jednotky pro síť internetu věcí nejen z hlediska spolehlivosti, ale také z hlediska garance, že s daty bude nakládáno s vědomím, že se jedná o „privátní“ data a zejména s garancí, že data neopustí hranice České republiky.

Výběr vhodné technologie pro české prostředí

Pro síť IoT existuje celá řada technologií. CRA věnovaly značné úsilí jejich analýze a výběru té nejvhodnější technologie pro specifické podmínky fungování Internetu věcí. Nejdůležitější požadavky pro výběr vhodné technologie jsou uvedeny v následujícím výčtu:

- dostupnost kmitočtového pásma a vysoká spolehlivost technologie,
- široká kompatibilita – otevřený standard s možností růstu počtu spolupracujících firem a mezinárodní pokrytí,
- odolnost proti rušení, komunikace na velkou vzdálenost,
- optimální pokrytí s využitím objektů CRA,
- možnost dokrytí specifických objektů na projektové bázi,
- cenově dostupná technologie umožňující poskytovat komunikační služby za konkurenceschopné ceny,
- nízkoenergetický provoz s použitím baterií s dlouhou životností – bez nutnosti údržby na straně zákazníka,
- oboustranná komunikace umožňující nejen sběr dat, ale také ovládací povely umožňující dálkové ovládání některých strojů a zařízení,
- síť umožňující snadno a s nízkými náklady monitorovat provozní stav celé sítě včetně koncových čidel.

S ohledem na tyto požadavky se na základě podrobných testů jako plně odpovídající prokázala **technologie LoRa (LoRaWAN – Long Range Wide Area Network)**. Jde o otevřený standard, na kterém participují stovky firem po celém světě. Tato bezdrátová technologie umožňuje za minimální vstupní a provozní náklady připojit obrovské množství zařízení do celonárodní vyhrazené datové sítě, a tím umožňuje připojení tam, kde není k dispozici internet (popř. připojení k internetu by bylo příliš nákladné). Současně je to zcela nezávislá síť. **CRA si tedy pro svou IoT síť vybraly technologie LoRa** z důvodů dostupnosti, dosahu, obousměrného zabezpečeného přenosu dat a stability.



Možnosti využití

Přestože IoT je velmi mladá technologie, nejen ve světě, ale i nás, již můžeme poukázat na řadu příkladů využití. Výše uvedené vlastnosti IoT sítě na platformě LoRa umožňují využití internetu věcí v oblastech jako je energetika (vzdálené odečty – Smart Metering), chytrá výroba a průmysl (velký potenciál v projektech průmyslu 4.0), doprava a logistika a velký praktický potenciál je v oblasti správy měst a obcí a městských služeb (městské dopravy a parkování, svoz odpadu, monitoring kvality ovzduší ve městě).

V zahraničí nemusíme pro příklady chodit daleko. Ve Francii využívají přenosu dat na LoRa s celonárodním pokrytím např. projekty chytrého parkování nebo projekty pro monitoring zaplněnosti veřejných kontejnerů s odpadem. V Belgii – konkrétně na bruselském letišti prostřednictvím LoRa sítě monitorují pohyb 600 vozidel, zajišťujících převoz nákladu v areálu letiště.

I v České republice již vznikají první projekty v rámci chytrých měst (Smart Cities):

- **Chytré parkování** – magnetické senzory sledují naplněnost parkovacích míst. Data jsou sdílena s parkovacími systémy, navigačními panely a navigačními aplikacemi v mobilních zařízeních.
- **Chytrý svoz odpadu** – ultrazvukové senzory jsou umístěny do kontejnerů na komunální a tříděný odpad. Systém v reálném čase přenáší informace a upozornění při vyšší naplněnosti.
- **Sledování kvality ovzduší** – sledování hladiny emisí CO₂ v továrnách, znečištění vzduchu automobilovou dopravou a toxických plynů vznikajících zemědělskou produkcí.

Městská platforma – portál pro správu chytrých technologií města

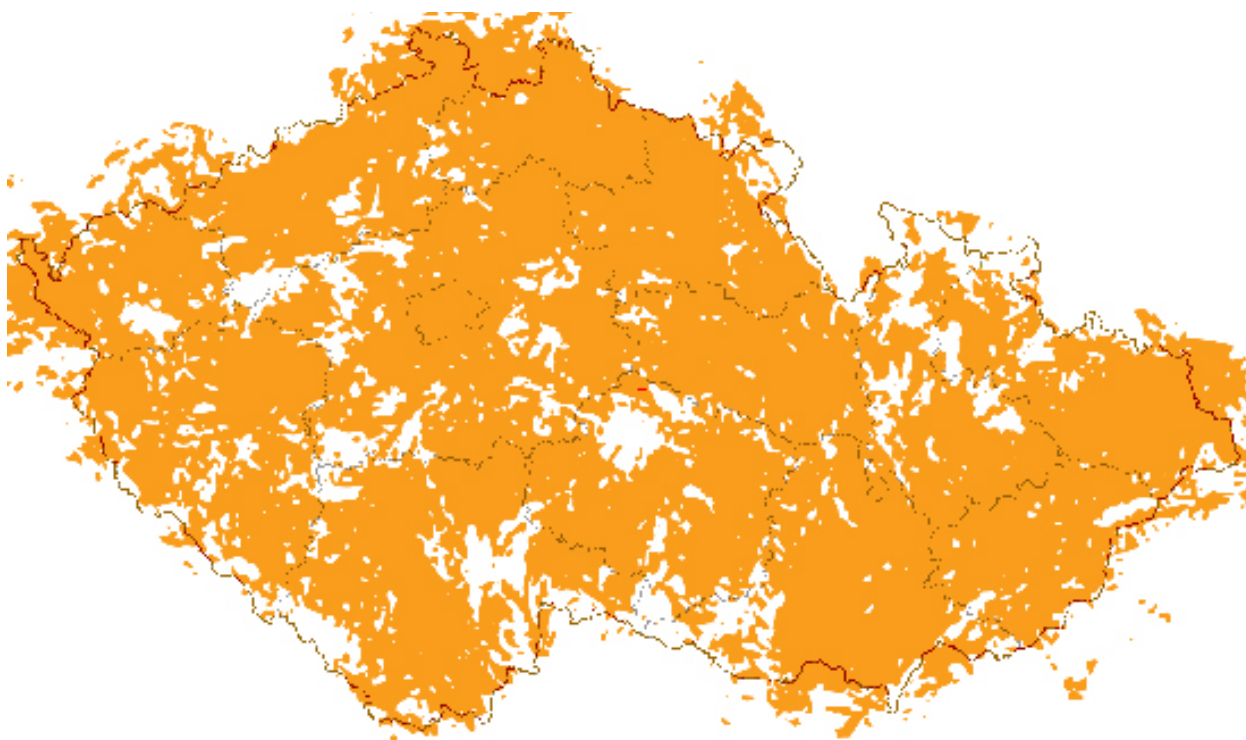
Kromě spolupráce na realizaci projektů pro chytrá města připravují CRA i **portál pro správu chytrých měst**. Cílem je **integrace** čidel, chytrých tabulí pro MHD, chytrých zařízení, měřáků energií, která města už dnes používají, **do jednoho místa**. Města a obce budou mít k dispozici mapu lokální infrastruktury, která bude snímat a vizualizovat data z jednotlivých chytrých řešení, ale do níž mohou i občané přímo přispívat (hlásit chyby, nefunkční zařízení apod.). Bude to tedy **jeden městský portál pro chytré řešení celé obce a města**.

Zabezpečení dat

Přestože se v internetu věcí typicky jedná o krátké zprávy o stavu dotyčných zařízení, případně o spotřebě energie, lze data, pokud se k nim dostane někdo neoprávněně, zneužít. Např. by mohlo dojít ke zneužití informací o spotřebě energií – informace o přítomnosti obyvatel v domácnosti, podle kterých by organizované skupiny mohly například plánovat vloupání a krádeže. Z toho důvodu se při návrhu protokolu LoRaWAN věnovalo značné úsilí **zabezpečení celého systému**. Kromě ochrany na úrovni čidel připojených do sítě a typů kódování zpráv, kterou tato čidla vysílají, je také každá vysílaná informace zabezpečena prostřednictvím dvou na sobě nezávislých šifrovacích klíčů.

Pokrytí sítě LoRa

V současné době pokrývá IoT síť CRA všechna krajská města v ČR a jejich okolí a probíhá spouštění sítě na úrovni okresních měst – aktivní je již síť v okolí měst Mladá Boleslav, Kolín, Frýdek-Místek a v následujícím období budou pokryta i další města. Do konce roku 2017 by LoRa měla dosáhnout celostátního pokrytí pro 70 % procent populace.



Podpora technologie LoRa, budování ekosystému partnerů

CRA kromě robustní infrastrukturní části a aplikačního rozhraní pro využití internetu věcí v rámci municipalit nabízí i prostor a zázemí pro data, která s využitím internetu věcí bezprostředně souvisejí. Pro tuto oblast zpřístupnily CRA IoT Cloud, který umožňuje hostování IoT aplikace, ukládání velkého množství dat z IoT zařízení a rovněž správu dat – pro jejich další využití.

Současně se CRA aktivně podílejí na **budování ekosystému partnerů sítě LoRa v ČR**, a to nejen na úrovni výrobců, dodavatelů hardwaru a koncových čidel a uživatelských aplikací, ale také na úrovni zákazníků a projektů, které se již zrealizovaly a mohou spolu sdílet zkušenosti, jež přispějí k dalšímu rozvoji této technologie u nás.

V rámci budování partnerského prostředí s možností navázání další spolupráce CRA organizují softwarově i hardwarově zaměřené akce a počátkem roku 2017 otevřely unikátní prostor pro spolupráci v oblasti internetu věcí – CRA IoT Hub.

Další informace naleznete na stránkách www.cra.cz a webu projektů prijoj.me.

Moderní API již není jen pro startupy

Vítězslav Košina, IBA CZ

Existuje stále větší množství služeb více či méně sbírajících různé druhy dat, které následně otevřeně nebo i skrytě monetizují. Prakticky je spíše nelehký úkol najít aplikaci, která o nás něco nesbírá. Znamená to tedy, že technologie, jež relativně neinvazivně sesbírají data i v rámci různých zařízení, existují a jsou plošně rozšířené i běžně používané. A pak tu máme jeden velmi zajímavý paradox. Pokud se pro sběr dat rozhodne jakákoliv instituce, je takové rozhodnutí provázáno mediální kanonádou a výsledný „produkt“ ve většině případů bývá poměrně obskurní. Rozebírat u takového řešení něco, jako je uživatelská přívětivost, je již většinou mimo jakýkoliv rámec.

Jak je tedy možné, že existují dva extrémů? Na jedné straně jsou tu komerční subjekty, které dokážou v řádu jednotek týdnů připravit a nasadit funkční řešení pro sběr dat. A na druhé straně pak mediální humbuk v řádu měsíců okolo každého sběru dat v nějaké instituci, jehož výsledkem bývá různě funkční řešení. Ale vždy ho předchází nelichotivé PR a téměř výhradně negativní reakce uživatelů. Důvod je nasnadě.

V myšlení mnoha lidí stále přetrvává rigidní uvažování. S jakoukoliv institucí se přece komunikuje přes formulář a zároveň formulář musí být dostatečně složitý na to, aby v uživateli nebudil dojem, že se jedná jen o nějakou drobnost. Současně se sbírají informace, o kterých se uživatel může oprávněně domnívat, že se sbírají opakovaně nebo mohou být případně zneužity. Můžete namítat, že někdy je potřeba více informací, nicméně toto je pohled z praxe. Kolik údajů, které jsou v rámci formuláře sebrány, představuje skutečnou datovou podstatu formuláře? Pokud si na tuto otázku odpovíte, zjistíte, že v mnoha případech to není většina.

A to jsem stále na straně uživatelů. Větší zábava nastane, když se do toho vloží IT specialista, protože pak se kromě „formulářového“ rozměru, který vnímá běžný uživatel, dostaneme do rozměru technologií. A zde se kreativité meze nekladou. Typické rozhraní pro sběr dat má v zásadě umět především čtyři základní operace s daty, a to založení, změnu, načtení a zrušení. Velmi často se setkáváme s tím, že jsou publikovány další zajímavé funkcionality, ale výše zmíněné základní funkce jsou implementovány jen částečně nebo některé vůbec.

Ale pryč z abstraktní roviny. Vezměme jednoduchý a velmi rozšířený příklad, kdy zákon ukládá povinnost sbírat vybraná data pro provádění dozorové činnosti. Pro začátek si vystačíme s tím, že si položky, které nás opravdu zajímají, tzn. jsou podstatné pro výkon zmiňované povinnosti, sepíšeme do oblíbeného nástroje, jako je například Excel nebo podobný tabulkový procesor. Velmi důležité je rozlišit (např. barvou), které položky jsou ty zásadní, tzn. nejde je vzít z již existujícího zdroje, a ty, které jsou pomocné. Uveďme příklad. Mám identifikovat firmu a opravdu mi bude stačit IČO nebo jiný podobný identifikátor a jistě není potřeba si pro jistotu ještě nechat poslat adresu a další údaje. Budete překvapeni, kolik skutečně relevantních údajů nakonec budete sbírat.

Vzápětí je potřeba si určit formát dat. Přijde mi až úsměvné, že specifikace různých rozhraní např. u čísel vyžaduje povinně dvě desetinná místa, přestože většina údajů v této položce přijde téměř jistě vždy jako celé číslo. Stejně tak o kvalitě návrhu nesvědčí časté opakování datového pole, kam lze napsat libovolný text, který více specifikuje detail. Nevěřím tomu, že to snad někdo v budoucnu bude dále zpracovávat. A dalo by se pokračovat. Pokud máme návrh, co tedy chceme sebrat, je potřeba se vždy oprostít od uvažování ve stylu „a ještě přidáme nepovinnou položku“. Nepovinná položka je to samé jako žádná položka a pouze to ukazuje na další lidovou tvořivost.

A teď už přichází na řadu technologie. Již několik let jsou zde predikce od renomovaných agentur, jako je Gartner, o tom, že mobilní zařízení v použití předeženou desktopy. Ačkoliv se tyto předpovědi naplňují, v implementaci mnoha rozšíření se to příliš neodráží. Máme zde dvě roviny. Jednak rovinu uživatelskou a zde se stačí podívat, kolik existuje uživatelských rozhraní, která jsou udělána dle filozofie „Mobile first“ nebo ještě lépe „Offline first“ nebo jsou alespoň použitelná na mobilních zařízeních. To je klíčové pro formuláře, které jsou interaktivní. A pak tu máme automatizovaná rozhraní pro sběr dat, tedy API. Zde je situace malinko

odlišná. Podstatné je, zda se jedná o rozhraní pro sběr dat, nebo spíše interní integrační rozhraní, protože každé je něco jiného a jistě bude vhodné i podle toho volit technologie.

Tento příspěvek se týká API, tedy rozhraní určených primárně pro sběr dat. Obsah každé takové zprávy má v zásadě dvě části, z nichž povinná je část týkající se vlastních dat a nepovinná pak část, která data zabezpečuje např. pomocí elektronického podpisu. Je maximálně výhodné, pokud máte data v takovém tvaru, že vám je dokáže vytvářet i interpretovat jak mobilní nebo webová aplikace, tak i program ve většině programovacích jazyků bez přidání významné pracnosti. A současně se nejedná o proprietární technologii, která vás sváže s konkrétním výrobcem a jeho postupy.

Zmínil jsem mobilní zařízení, ale platí to obecně. Méně je více, tzn. nepřenášíme, co není nezbytně nutné, a to, co přenášíme, pak v základním tvaru (tzn. bez formátování apod.). U rozhraní většinou potřebujeme výše uvedené čtyři základní operace a můžeme směle přejít k technologii.

Technologie zvolíme tak, aby jedna byla samodokumentující se, tzn. už z definice je i ne-IT specialistovi jasné, jaká data se budou sbírat, a současně vznikne něco jako referenční klient. Situace, kdy se publikuje PDF dokument a k tomu definiční soubor, kterému rozumí pouze IT specialisté, je stále velmi oblíbený vzor specifikace rozhraní. Nicméně krom toho, že nahrává softwarovým firmám, konečnému uživateli nic nepřináší. V roce 2017 bych spíše očekával rozhraní, které má implementovaného referenčního klienta s otevřeným zdrojovým kódem nebo ještě lépe je celé implementováno jako otevřená technologie. Nicméně to by znamenalo, že technologie se vybírá podle požadavků rozhraní a uživatelů, a nikoliv že rozhraní a uživatelé se ohýbají do konkrétní, již dříve vysoutěžené technologie, kterou je potřeba z různých důvodů použít.

A tak se dostáváme k praktické realizaci. Ukázkové rozhraní je typicky REST API, které přenáší data zabezpečeným tunelem, přičemž je možné současně u dat ověřit autenticitu a integritu např. pomocí elektronického podpisu. Zároveň je možno použít již lepší metody zabezpečení než zadávat jméno a heslo. Takové rozhraní je schopno data konzumovat jak z webové formulářové aplikace, tak i programově ze služeb běžících na serveru. A samozřejmě bude škálovatelné třeba i na desítky tisíc požadavků za vteřinu bez „enterprise“ licencí a věci jako vysoká dostupnost a opensource implementace jsou samozřejmost bez dalších dodatečných nákladů. Přijďte se tedy podívat na naši ukázkou...

Evidence smluv a registr smluv naostro

Ing. Petra Kubíková, Kamila Kolbová, Městská část Praha-Zličín;
Mgr. Petr Wohanka, Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

V roce 2015 byl po mnoha dohadech a dřívějších neúspěšných pokusech schválen zákon upravující povinnosti zveřejňování smluv, v nichž jako jedna ze smluvních stran vystupuje určitý subjekt veřejného sektoru. Nejedná se v této oblasti o úplnou novinku, neboť již dříve bylo třeba zveřejňovat smlouvy podle zákona o veřejných zakázkách, zákona o rozpočtových pravidlech územních rozpočtů, zákona o podpoře výzkumu, experimentálního vývoje a inovací, koncesního zákona a také zákona o kolektivním vyjednávání. Nicméně průlomová je jistě širší záběr různých smluv, které této povinnosti podléhají. Od 1. července 2016, kdy zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále jen „zákon o registru smluv“), nabyl účinnosti, nebylo nesplnění povinnosti zveřejnění nijak sankcionováno. Situace se změnila až k 1. červenci 2017, kdy začne platit, že pokud smlouva měla být dle daného zákona zveřejněna, ale nestalo se tak, a to ani do tří měsíců ode dne, kdy byla uzavřena, platí, že je zrušena od počátku. To je velmi silná sankce, která znamená, že je třeba velmi pečlivě zvažovat, zda má či nemá být smlouva zveřejněna. V případě, že si nejsme jisti, je vždy vhodnější smlouvu zveřejnit než se vystavit nebezpečí jejího automatického zrušení od počátku.

Tento příspěvek popisuje praktické zkušenosti se zveřejňováním v registru smluv realizovaným z modulu Evidence smluv, který je součástí informačního systému Munis. Jako příklad dobré praxe je představena situace městské části Praha-Zličín.

Městská část Praha-Zličín

Městská část Praha-Zličín je jednou z 57 městských částí hlavního města Prahy. Leží na západním okraji Prahy. Městská část je utvořena ze dvou původně samostatných obcí-Zličína a Sobína. Centra těchto původních vsí dodnes dokumentuje zástavba statků a zemědělských usedlostí, která tvořila jejich historická jádra. Městská část Praha-Zličín se skládá z katastrálního území Zličín, katastrálního území Sobín a severní části katastrálního území Třebonice, která je omezena severním okrajem komunikace Rozvadovské spojky. Celková rozloha území městské části činí 682 ha. Nejvýše položený bod v území, lokalita Za hospodou v kat. území Sobín, 399,22 m n. m., je zároveň i nejvyšším bodem na území hl. m. Prahy. Aktuálně ke konci roku 2016 bylo v městské části k trvalému pobytu hlášeno 6802 obyvatel.



Obr. 1: Ilustrační fotografie sídliště Zličín – zdroj [1].

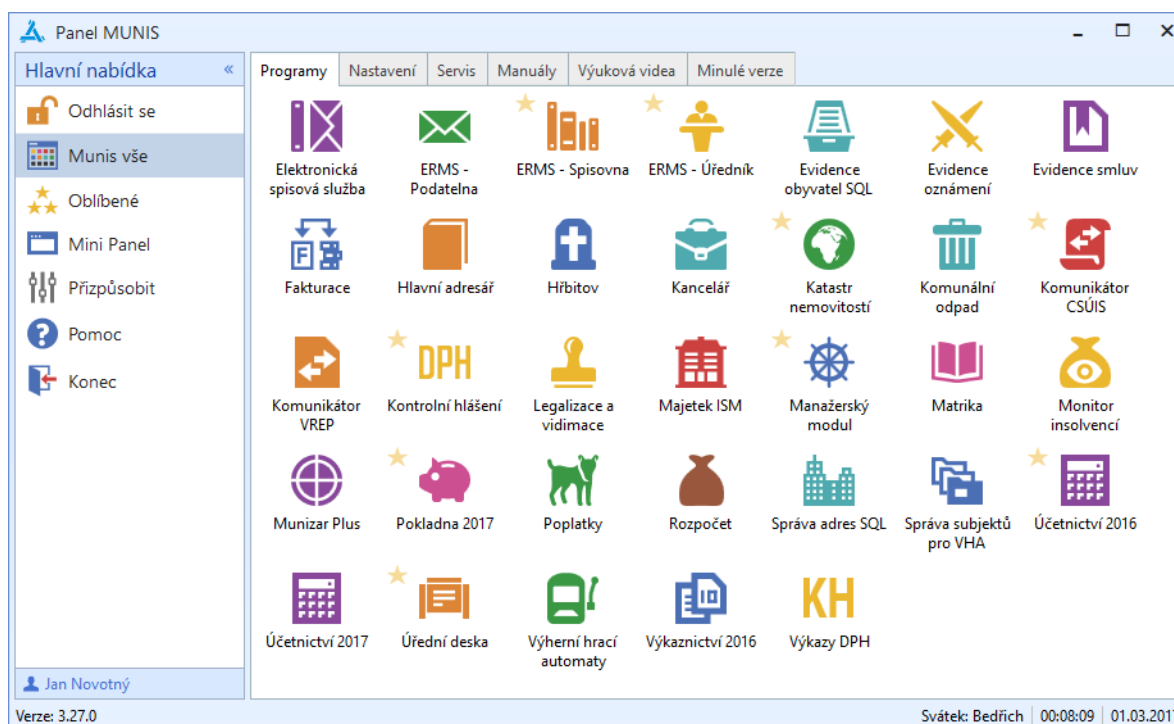
Úřad městské části Praha-Zličín se sestává ze tří odborů:

- Kanceláře úřadu – 6 pracovníků, včetně tajemnice úřadu,
- Odbor ochrany prostředí, rozvoje a investic – 3 pracovníci,
- Odbor občanskosprávní, vnitřních věcí a majetku – 4 pracovníci.

V čele městské části stojí patnáctičlenné Zastupitelstvo MČ a pětičlenná Rada MČ. Dále je zřízeno 7 komisí a dva výbory zastupitelstva.

Modul Evidence smluv

Informační systém Munis je komplexní informační systém pro města, městské části a obce, který svými moduly zahrnuje většinu agend vedených příslušnými municipalitami (blíže viz též [2]). Přehled zahrnutých modulů je patrný z Obr. 2. Modul Evidence smluv je jednou z aplikací, která může pracovat jak samostatně, tak ve výhodné kooperaci s dalšími moduly. Asi nejvýznamnější z hlediska zveřejňování smluv je vazba na elektronický systém spisové služby Munis ERMS. Nicméně modul umožňuje zveřejňování smluv do registru smluv také prostřednictvím jiných spisových služeb.



Obr. 2: Nabídka modulů informačního systému Munis.

Modul Evidence smluv neslouží pouze ke zveřejňování, ale umožňuje přehledně ukládat popisné informace o smlouvách a hlídat související termíny jednorázových i opakujících se událostí, např. výročních dní pomocí systému tzv. milníků. Velkou výhodou je též přehledné vyhledávání podle mnoha kritérií. Evidované smlouvy je navíc možné přiřazovat k jednotlivým projektům, grantům a veřejným zakázkám, čímž uživatel získá opravdu výkonný a přehledný nástroj a udělá si jednou pro vždy pořádek ve svých smlouvách.

Základem modulu Evidence smluv je číselník typů smluv, který je nadstavbou pro jednotlivé kategorie smluv a zároveň slouží jako zdroj šablon zjednodušující následné zadávání. Při zaevidování konkrétní smlouvy jsou díky těmto šablonám nejen předvyplňovány opakující se údaje včetně dynamických vazeb určujících prostřednictvím pracovních pozic jednotlivé vztahy konkrétních osob ke smlouvě, ale jsou též určena základní pravidla vyplňovaných údajů, např. způsoby plnění. Do evidence se samozřejmě také vkládají elektronické podoby smluv a jejich příloh, přičemž každá z těchto komponent může být až ve třech variantách:

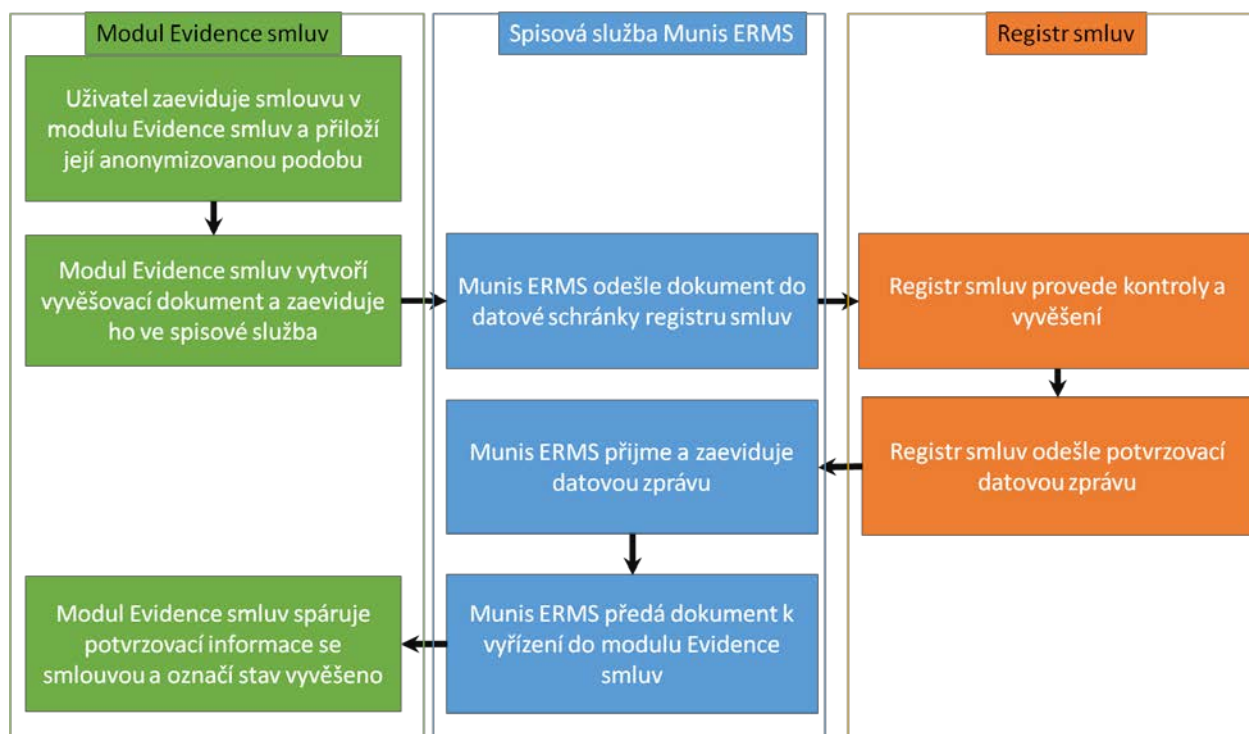
- textová podoba plného textu smlouvy,
- anonymizovaná textová podoba určená ke zveřejňování,
- skenovaná podoba včetně případných vlastnoručních podpisů a dalších atributů (např. razítek).

Anonymizovaná podoba a primární textová podoba se mohou shodovat. Nicméně u zveřejňovaných smluv je to asi spíše výjimečná situace, neboť proces anonymizace je nezbytný téměř v každém případě. A to nejen pro textovou podobu smlouvy, ale také pro popisná data, jak o předmětu smlouvy, tak o smluvních stranách. V modulu Evidence smluv je anonymizace řešena v rámci prvního kroku kompletního vyvěšovacího procesu – viz Obr. 3.

Obr. 3: Iniciační formulář vyvěšovacího procesu, který v sobě zahrnuje různé možnosti anonymizace.

Po založení vyvěšovacího procesu má uživatel možnost volby dalšího postupu v závislosti na nastavené vazbě. V případě spisové služby Kancelář nebo jiné spisové služby mimo informační systém Munis volí vyvěšení souborem, kdy program vytvoří potřebné podklady (XML a přílohy) a uloží je do přednastaveného adresáře. Následné odeslání do datové schránky registru smluv je pak úkolem spisové služby. V případě elektronické spisové služby Munis ERMS je tato vazba automatizována. Rovnou je vytvořen příslušný dokument a zaslán, kterou spisová služba vypraví v rámci hromadného procesu výpravny. Odpověď s potvrzením od registru smluv se opět páruje buď ručně – výběrem souborů z adresáře, kam je uložila spisová služba, nebo přímou vazbou z aplikace Úředník elektronické spisové služby Munis ERMS. Těsná vazba mezi moduly informačního systému Munis a schematické vyjádření procesu vyvěšení je znázorněno na Obr. 4.

Modul Evidence smluv obecně neomezuje uživatele v žádných úpravách a opravách smluv, dokud nedojde k jejich vyvěšení. Je-li třeba následné úpravy (po vyvěšení), je automaticky generován nový vyvěšovací proces tak, aby publikovaná data i textové podoby smluv byly vždy aktuální. Stejně tak je to s dodatky smluv. Zajištění povinností plynoucích zákona o registru smluv je tedy pomocí tohoto nástroje poměrně jednoduché a hlavně spolehlivé, což s ohledem na sankci neplatnosti smlouvy při nezveřejnění je velmi podstatné.



Obr. 4: Schematická vazba mezi modulem Evidence smluv a Registrem smluv.

Praktické zkušenosti

Modul Evidence smluv si městská část Praha-Zličín pořídila v polovině roku 2016 jako další z modulů informačního systému Munis, jehož služby využívá již od září roku 1998. Městská část tak využívá výhody plynoucí z celkové provázanosti modulů tohoto informačního systému, i když z pohledu Evidence smluv a zveřejňování ne dosud v plné míře, neboť přechod na technologického nástupce modulu Kancelář – elektronickou spisovou službu Munis ERMS – je naplánován až na letošní rok.

V Evidenci smluv byl primárně naplněn číselník typů smluv, který nyní zahrnuje 20 typů plus 1 univerzální pro umožnění zaevidování „historické“ smlouvy (smlouva staršího data, kterou v registru potřebujeme z nějakého důvodu mít). Městská část má v celkové evidenci zapsáno již 95 smluv. Z toho jsme ve veřejném registru publikovali 25 smluv – viz Obr. 5.

Zkušenosti s modulem jsou dobré. Líbí se nám rozsah údajů, které je možné u smluv evidovat a následně dle nich smlouvy vyhledat. Práce v Evidenci smluv není složitá, spíše jednoduchá a intuitivní. Velkou výhodou vidíme v možnosti ukládání smlouvy ve třech typech – naskenovaná smlouva s podpisem i razítkem v PDF, smlouva ve formátu Word a anonymizovaná smlouva. Tyto výhody již byly mnohokrát využity – jak k tisku smlouvy s razítkem a podpisem v PDF, tak možnost smlouvu ve formátu Word dále upravit a použít ji např. jako předlohu k jiné podobné smlouvě. Mnohokrát stačilo jen do smlouvy nahlédnout bez zbytečného hledání v šanonech.

Odesílání smluv z Evidence smluv do veřejného registru přes datové schránky v Kanceláři je vcelku jednoduché, ale vyžaduje více úkonů, což je ale nevýhoda dočasná a přechodem na Munis ERMS se vyvěšování ještě zjednoduší. Proces zpracování odpovědi z veřejného registru (potvrzení) přes datové schránky zpět do Evidence smluv probíhá hladce.

Co se týká Evidence smluv, nedostatek aktuálně sledujeme v nemožnosti filtrovat smlouvy dle zakladatele (pracovníka), který smlouvu do Evidence smluv vkládal a dle provedení zveřejnění. Jedná se o připomínky, jejichž potřeba vyvstala až po nějaké době provozu systému, a předpokládáme jejich postupné zapracování.



Podrobné vyhledávání

Datum zveřejnění (od - do)	ID smlouvy	ID verze
<input type="text"/> - <input type="text"/>	<input type="text"/>	<input type="text"/>
Název publikujícího subjektu praha - zličín	⁽¹⁾ Název smluvní strany	⁽¹⁾ Číslo smlouvy / č.j.
<input type="text"/>	<input type="text"/>	<input type="text"/>
Dot. schránka publikujícího subjektu	⁽¹⁾ Dot. schránka smluvní strany	⁽¹⁾ Datum uzavření smlouvy (od - do)
<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>
IČO publikujícího subjektu	⁽¹⁾ IČO smluvní strany	⁽¹⁾ Textové označení smlouvy
<input type="text"/>	<input type="text"/>	<input type="text"/>
Adresa publikujícího subjektu	⁽¹⁾ Adresa smluvní strany	⁽¹⁾ Podepisující osoba
<input type="text"/>	<input type="text"/>	<input type="text"/>
Hodnota v ruzí měně (od - do)	⁽¹⁾ Hodnota bez DPH v CZK (od - do)	⁽¹⁾ Hodnota vč. DPH v CZK (od - do)
<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>
Označení měny	⁽¹⁾ Text ve smlouvě	⁽²⁾ Rozsah vyhledávání
<input type="text"/>	<input type="text"/>	jen platné verze

[Vyhledat](#) [Exportovat do XLSX](#)

¹⁾ Vyhledávání podle označovacího pole nemusí poskytnout úplné výsledky, protože jeho vyplnění není při zveřejňování smlouvy povinné.

²⁾ Přehledné dokumenty, které byly zveřejněny bez textové smlouvy, nebudou prohledány.

Vyhledané smlouvy na základě kritérií

Změna kritérií

Počet nalezených záznamů 21

Publikující smluvní strana	Textové označení smlouvy	Platná verze	Publikováno	Hodnota smlouvy	Smluvní stranami	
MČ Praha - Zličín	Opravy komunikací a chodníků	ano	21.12.2016	Neuváděno	Autostar, spol. s r.o.	Detail
Městská část Praha - Zličín	Dodatek č. 1 k smlouvě	ano	20.12.2016	Neuváděno	Laděk Sekyra	Detail
Městská část Praha - Zličín	oprava přemostění	ano	04.10.2016	Neuváděno	SKS Czech Republic, s.r.o.	Detail
Úřad MČ Praha - Zličín	Správa, údržba a opravy nemovitostí	ano	07.02.2017	Neuváděno	Kulářova Katerina	Detail
Městská část Praha - Zličín	pozemek par.č. 105 k.ú. Zličín	ano	06.02.2017	Neuváděno	Maruška V.	Detail
MČ Praha - Zličín	žmínové listy	ano	14.12.2016	Neuváděno	PHS slaby a.s.	Detail
MČ Praha - Zličín	dodávka nábytku MŠ v Hvelínské	ano	01.12.2016	Neuváděno	První chráněná dílna s.r.o.	Detail
MČ Praha - Zličín	žmínové listy č.5, ul 9	ano	05.12.2016	Neuváděno	PHS slaby a.s.	Detail
MČ Praha - Zličín	Požizení	ano	30.11.2016	Neuváděno	AUTO STYX a.s.	Detail
MČ Praha - Zličín	Dodávka nábytku MŠ Hvelínská	ano	08.12.2016	Neuváděno	První chráněná dílna s.r.o.	Detail
MČ Praha - Zličín	Kupní smlouva - tuzemské	ano	01.12.2016	Neuváděno	LUMINEXIA GROUP, a.s.	Detail
MČ Praha - Zličín	žmínové listy	ano	25.11.2016	54 000 CZK	BDP (OUR) ILLUMINATION s.r.o.	Detail
MČ Praha - Zličín	Dodatek č. 5 ke smlouvě o dílo S84/2011	ano	21.11.2016	Neuváděno	Laděk Sekyra	Detail
Městská část Praha - Zličín	Oprava elektroinstalace veškerý Městských	ano	16.02.2017	Neuváděno	AQUACONSULT spol. s r.o.	Detail
MČ Praha - Zličín	Dodatek č. 2	ano	31.01.2017	Neuváděno	Kulářova Katerina	Detail
Městská část Praha - Zličín	zpracování strategického plánu	ano	04.01.2017	175 450 CZK	Finanční paradenise, s.r.o.	Detail
MČ Praha - Zličín	Dodatek č. 4 ke smlouvě o dílo na stavbu MŠ v Hvelínské	ano	22.12.2016	Neuváděno	PHS slaby a.s.	Detail
MČ Praha - Zličín	Dle č. zúčín na území fotbalového klubu	ano	13.12.2016	230 000 CZK	FC Zličín	Detail
MČ Praha - Zličín	Dodatek č. 12 ke smlouvě o dílo S 92/2007	ano	14.11.2016	Neuváděno	Laděk Sekyra	Detail
MČ Praha - Zličín	Dopravní opravy hrušického auta	ano	26.10.2016	135 000 CZK	Scania Czech Republic, s.r.o.	Detail
MČ Praha - Zličín	Zajištění administrativního zápisu pro senátory	ano	06.08.2016	Neuváděno	Centroví kancelář s.r.o.	Detail

Obr. 5: Aktuální pohled na registr smluv se smlouvami zveřejněnými městskou částí Praha-Zličín – zdroj [3].

Literatura

- [1] Oficiální webové stránky městské části Praha-Zličín dostupné na adrese <<http://www.mczlicin.cz>>.
- [2] Webové stránky o informačním systému Munis dostupné na adrese <<http://www.munis.cz>>.
- [3] Registr smluv dostupný na adrese <<https://smlouvy.gov.cz>>.

Základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR)

Mgr. Tomáš Lechner, Ph.D., Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva

Úvod

Nařízení Evropského parlamentu a Rady EU 2016/679, 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), pro které se často používá zkratka GDPR z anglického označení „General Data Protection Regulation“, bylo publikováno v Úředním věstníku Evropské unie dne 4. května 2016, v platnost vstoupilo 24. května 2016 a účinnosti nabude až 25. května 2018. Tato poměrně dlouhá doba mezi nabytím platnosti a účinností již naznačuje, že rozsah regulované oblasti je poměrně značný a příprava jednotlivých členských států EU na aplikování této normy bude vyžadovat nemálo úsilí.

Z čistě právního pohledu jde o předpis, který je přímo účinný ve všech členských státech a netřeba jej transponovat do národních právních systémů. Avšak je třeba dát do souladu národní právní předpisy s tímto nařízením, což v případě České republiky bude minimálně znamenat změnu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Zda bude harmonizace řešena novelizací tohoto právního předpisu nebo jeho zrušením a schválením nového zákona či zákonů, jako tomu bylo v případě nařízení eIDAS [1], to vše teprve ukáže čas. Nicméně je jistě vhodné zmínit v této souvislosti ještě potřebu transpozice související směrnice Evropského parlamentu a Rady EU 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Tato směrnice byla publikována ve stejném Úředním věstníku jako GDPR a nabyla platnosti 5. května 2016. Povinnost transponovat ji do vnitrostátních právních systémů mají všechny členské státy EU do 6. května 2018, což poměrně koresponduje (měsícem) s GDPR. Lze tedy předpokládat, že řešení obou potřeb změn právních předpisů bude řešeno souběžně.

Jedním z cílů GDPR je zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci EU prostřednictvím sjednocení úrovně ochrany práv a svobod fyzických osob v souvislosti se zpracováním těchto údajů (odst. 10 preambule GDPR). I toto nařízení, stejně jako nařízení eIDAS, lze zasadit do kontextu plánů budování jednotného digitálního trhu [5].

Tento příspěvek se dále bude věnovat základnímu rozboru GDPR s tím, že si neklade za cíl identifikovat všechny možné dopady, ale spíše být úvodem do této problematiky a poukázat na některé významné změny, které v souvislosti s nabytím účinnosti GDPR nastanou v oblasti ochrany osobních údajů.

Ochrana osobních údajů

Jak je napsáno hned v prvním bodě preambule GDPR, patří ochrana fyzických osob v souvislosti se zpracováním osobních údajů mezi základní práva. Na evropské úrovni je toto právo formulováno v čl. 8 odst. 1 Listiny základních práv Evropské unie a v čl. 16 odst. 1 Smlouvy o fungování Evropské unie. Na úrovni České republiky vychází z čl. 10 odst. 2 a 3 Listiny základních práv a svobod (zákon č. 2/1992 Sb.), kde se stanoví, že:

- Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
- Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Nejen v souvislosti s rozvojem informační společnosti a elektronizací veřejné správy [2] je ochrana osobních údajů stále obsáhlejší téma, které má celou řadu souvislostí a aspektů (viz např. [2], [3] a [4]). Právo na ochranu osobních údajů se někdy nesprávně zaměňuje s ochranou osobnosti. Je třeba si uvědomit, že právo na

ochranu osobních údajů se týká pouze informací, které můžeme jako osobní údaj kvalifikovat [3]. Toto právo, není právem absolutním (viz odst. 4 preambule GDPR), tedy jak uvádí citovaný odstavec, musí být toto právo vždy posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality a musí být v rovnováze s dalšími základními právy. Je však jednoznačné, že jakékoliv zpracování osobních údajů by mělo být prováděno zákonným a spravedlivým způsobem (odst. 39 preambule GDPR).

Struktura nařízení

GDPR má poměrně obsáhlou preambuli čítající 173 bodů. Dále je rozdělena na 11 kapitol:

- I – Obecná ustanovení
- II – Zásady
- III – Práva subjektu údajů
- IV – Správce a zpracovatel
- V – Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím
- VI – Nezávislé dozorové úřady
- VII – Spolupráce a jednotnost
- VIII – Právní ochrana, odpovědnost a sankce
- IX – Ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování
- X – Akty v přenesené pravomoci a prováděcí akty
- XI – Závěrečná ustanovení

V první kapitole GDPR (čl. 1–4) je definován základní předmět nařízení, věcná a místní působnost a pojmy. V druhé kapitole (čl. 5–11) jsou definovány základní zásady zpracování osobních údajů a specifikovány podmínky vyjádření souhlasu, včetně pro české prostředí nové problematiky týkající se souhlasu dítěte. Již zde se také setkáváme se specifickým případem zpracování osobních údajů, a to zpracováním osobních údajů týkajících se rozsudků v trestních věcech a trestných činů (čl. 10), což má též souvislost s výše zmíněnou směrnicí Evropského parlamentu a Rady EU 2016/680. Dále je v této kapitole zmíněno zpracování, které nevyžaduje identifikaci. Další specifické případy zpracování osobních údajů jsou pak předmětem kapitoly IX.

Třetí kapitola GDPR (čl. 12–23) se vnitřně člení na 5 oddílů. Souhrnně se kapitola věnuje právům subjektu údajů. V prvním oddíle (čl. 12) je specifikované právo na stručná, transparentní, srozumitelná a snadno přístupná sdělení týkající se postupů pro výkon práv subjektu údajů. V druhém oddíle (čl. 13–15) je popisováno právo na přístup subjektu údajů k informacím o zpracovávaných osobních údajích o své osobě, na které se samozřejmě vztahují pravidla z čl. 12. Poskytované informace se liší podle toho, zda osobní údaje jsou získány od subjektu údajů (čl. 13), nebo zda osobní údaje nebyly získány od subjektu údajů (čl. 14). Ve třetím oddíle (čl. 16–20) je specifikováno právo na opravu (čl. 16), právo být zapomenut (čl. 17), právo na omezení zpracování (čl. 18) a právo na přenositelnost údajů (čl. 20). Posledně jmenované patří opět mezi novinky tohoto nařízení. Zatímco poměrně často uváděné jako nové „právo být zapomenut“ mezi zcela nová práva nepatří, neboť navazuje na předchozí „právo na výmaz“, které zná i stávající zákon č. 101/2000 Sb. (viz § 21 odst. 1 cit. zákona). Čtvrtý oddíl (čl. 21 a 22) přidává právo vznést námitku a právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Poslední pátý oddíl třetí kapitoly obsahuje v čl. 23 možnost omezit rozsah práv definovaných touto kapitolou, tedy čl. 12 až 22, a také čl. 5, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit zejména národní bezpečnost, obranu, ochranu nezávislosti soudnictví a soudních řízení a v dalších taxativně uvedených případech.

Čtvrtá kapitola GDPR (čl. 24–43) se opět člení na 5 oddílů a věnuje se zejména povinnostem správce a zpracovatele osobních údajů. Právě oddíl jedna (čl. 24–31) stanoví obecné povinnosti. Druhý oddíl (čl. 32–34) popisuje zejména zabezpečení osobních údajů při jejich zpracování a ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu i subjektu údajů. Třetí oddíl (čl. 35 a 36) specifikuje pravidla

pro posouzení vlivu na ochranu osobních údajů (čl. 35) a povinnosti předchozí konzultace zpracování s dozorovým úřadem (čl. 36). Čtvrtý oddíl (čl. 37–39) popisuje roli pověřence pro ochranu osobních údajů. V České republice jde o zcela nový institut, který má poměrně zásadní úkoly. Pátý oddíl (čl. 40–43) se věnuje kodexům chování, které mají přispět k řádnému uplatňování GDPR, a také zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečeti a známek dokládajících ochranu údajů pro účely prokázání souladu s GDPR v případě operací zpracování prováděných správci a zpracovateli.

Pátá kapitola GDPR (čl. 44–50) specifikuje postupy a pravidla pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím. Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená GDPR nebyla znehodnocena.

Šestá kapitola GDPR (čl. 51–59) se dělí na dva oddíly a celá se týká nezávislých dozorových úřadů v jednotlivých členských státech. První oddíl (čl. 51–54) specifikuje základní postavení dozorových úřadů, jeho nezávislost, obecné podmínky pro členy dozorového úřadu a pravidla a postupy pro jeho zřízení. Druhý oddíl (čl. 55–59) se pak věnuje příslušnosti těchto úřadů, jak na vnitrostátní úrovni, tak v případě přeshraničního zpracování osobních údajů. Článek 57 stanoví konkrétní úkoly dozorových úřadů, následující článek pak jejich pravomoci. Každý dozorový úřad má povinnost vypracovávat výroční zprávu o své činnosti (viz čl. 59).

Sedmá kapitola GDPR (čl. 60–76) dále navazuje na předchozí kapitolu a rozvíjí oblast spolupráce mezi dozorovými úřady navzájem i mezi dozorovými úřady a Evropským sborem pro ochranu osobních údajů. Tato kapitola s názvem „Spolupráce a jednotnost“ se dělí na tři oddíly. První z nich (čl. 60–61) se blíže věnuje právě oblasti spolupráce, vzájemné pomoci a společných postupů dozorových úřadů. Druhý oddíl (čl. 63–67) popisuje princip jednotnosti a vztahy mezi dozorovými úřady a Evropským sborem pro ochranu osobních údajů, jehož postavení, nezávislost, úkoly a další atributy specifikuje oddíl třetí (čl. 68–76). Mimo jiné je také stanovena povinnost vypracovávat výroční zprávy.

Osmá kapitola GDPR (čl. 77–84) stanoví další práva a dále se věnuje odpovědnosti a sankcím. Stanovená práva jsou: právo podat stížnost u dozorového úřadu, právo na účinnou soudní ochranu vůči dozorovému úřadu, právo na účinnou soudní ochranu vůči správci nebo zpracovateli a právo na náhradu újmy, v souvislosti s nímž je v čl. 82 definována též odpovědnost. V této kapitole jsou také popsány obecné podmínky pro ukládání správních pokut, a to včetně jejich výše (čl. 83). Pokud bychom zmínili opět srovnání s nařízením eIDAS, u kterého je definice pokut ponechána na národních předpisech a jejich výše tak může být upravena v závislosti na místních podmínkách, pak zde zákonodárce zvolil ryze centralizovaný přístup s nastavením pokut odpovídající ekonomicky silným státům EU. Protože konkrétní výše pokuty vždy závisí na posouzení příslušným dozorovým úřadem, je zřejmé, že jejich rozhodovací pravomoc je tímto, zejména pro případ České republiky a dalších méně ekonomicky silných států EU, značně posílena.

Devátá kapitola GDPR (čl. 85–91) se věnuje zvláštním situacím, při nichž dochází ke zpracování osobních údajů. Jde o různé specifické souvislosti týkající se svobody projevu a informací (čl. 85), úředním dokumentům (čl. 86), národních identifikačních čísel (čl. 87), zpracování v souvislosti se zaměstnáním (čl. 88), zpracování pro účely archivace, vědeckého či historického výzkumu anebo pro statistické účely (čl. 89) a dále pravidel uplatňovaných církvemi a náboženskými sdruženími (čl. 91). Součástí této kapitoly je též definice povinnosti mlčenlivosti, kterou ale blíže budou upřesňovat národní právní předpisy, jenž má každý členský stát povinnost přijmout do 25. května 2018, tedy do nabytí účinnosti GDPR.

Desátá kapitola GDPR (čl. 92 a 93) se týká prováděcích právních předpisů, které má Komise EU připravit a vydat. Poslední jedenáctá kapitola (čl. 94–99) obsahuje závěrečná ustanovení včetně vztahu ke směrnici 2002/58/ES a definici účinnosti, která, jak již bylo několikrát zmíněno, je stanovena na 25. května 2018.

Působnost nařízení

GDPR se primárně vztahuje na automatizované zpracování osobních údajů. Vzhledem k postupující elektronizaci veřejné správy tedy do jeho působnosti spadá vedení všech registrů a informačních systémů veřejné správy obsahujících osobní údaje. Samozřejmě, že toto nařízení se nevztahuje jen na veřejnou správu, ale na

všechny subjekty, které takové evidence vedou, s tím, že vyňaty jsou pouze fyzické osoby, které by takové evidence vedly v průběhu výlučně osobních či domácích činností [viz čl. 2 odst. 2 písm. c)], což je v podstatě obdobná situace jako v případě stávajícího zákona o ochraně osobních údajů (viz § 3 odst. 3 zákona č. 101/2000 Sb.). Kromě uvedené výjimky je vhodné ještě připomenout, že GDPR se nevztahuje na zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Na něj se vztahuje výše zmíněná směrnice Evropského parlamentu a Rady EU 2016/680.

GDPR se vztahuje na zpracování všech osobních údajů správcem nebo zpracovatelem usazeným v Evropské unii bez ohledu na to, kde toto zpracování probíhá. Dále se vztahuje na osobní údaje všech subjektů údajů, tedy např. občanů, ať jsou zpracovány subjektem usazeným v Unii nebo mimo ni s tím, že na správce a zpracovatele mimo Unii se vztahuje jen, pokud činnosti zpracování souvisejí s nabídkou zboží anebo monitorováním chování. Z hlediska občanů členských států Evropské unie je má toto nařízení chránit, ať zpracování jejich osobních údajů probíhá kdekoli a kýmoli.

Pojmosloví

Z definovaných pojmů si zde povšimneme osobních údajů, genetických údajů, biometrických údajů, údajů o zdravotním stavu, profilování, pseudonymizace, správce a zpracovatele. Ve všech případech vyjdeme primárně z ustanovení čl. 4 GDPR, přičemž budeme provádět srovnání se stávajícím aktuálním zněním zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „OOUZ“).

Osobními údaji se dle GDPR rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě, která se pak nazývá subjekt údajů, přičemž identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Podle stávajícího OOUZ se osobním údajem rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. GDPR tedy pracuje s informacemi o osobách, zatímco OOUZ s informacemi týkajícími se osob. Byť jsou tyto formulace rozdílné, jedná se dle mého názoru pouze o formální rozdílnost, nikoliv obsahovou. Proto lze obě definice primárně považovat za totožné, neboť tyto informace se týkají osoby, jež lze pomocí těchto údajů přímo či nepřímo identifikovat. Znamená to, že z hlediska toho, co chápeme jako osobní údaj, nepřináší GDPR oproti OOUZ nic nového.

To, v čem se původní a nový přístup liší, jsou příklady daných možností identifikace, kdy OOUZ se více věnuje příkladům, které spíše jako osobní údaje chápeme, zatímco GDPR přidává i lokační údaje nebo síťový identifikátor, ale samozřejmě pouze za podmínky, že jím lze fyzickou osobu identifikovat. Je tedy zcela nesporné domnívat se, že GDPR obecně považuje IP adresu vašeho počítače za osobní údaj. Stejně jako jméno a město trvalého bydliště mohou být vašimi osobními údaji, pokud se v daném městě nevyskytuje jiná osoba stejného jména, ale nejsou jimi, pokud je v daném městě jmenovců více, tak IP adresa se může osobním údajem stát, pokud pomocí ní lze v rámci daného procesu konkrétní osobu identifikovat. Vždy je tedy třeba posuzovat okolnosti a procesy, které v daném případě zpracování jsou implementovány, abychom mohli rozhodnout, zda určitá množina údajů odpovídá či neodpovídá definici osobních údajů.

Hned za osobními údaji definuje OOUZ zcela obecně citlivé osobní údaje, jako takové osobní údaje, které vypovídají o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a také genetický údaj subjektu údajů a biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. GDPR žádnou takovou obecnou definici nemá, přestože se tento pojem zmiňuje v odst. 10 preambule, kde se říká, že se citlivým osobním údajem rozumí zvláštní kategorie osobních

údajů. GDPR tyto kategorie taxativně uvádí. Konkrétně definuje genetické údaje, biometrické údaje a údaje o zdravotním stavu. Další citlivé osobní údaje jako např. údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, explicitně neuvádí v definici, přestože s nimi pracuje a dokonce primárně zakazuje jejich zpracování až na konkrétně jmenované speciální případy (viz čl. 9 GDPR). Z hlediska konstrukce pojmů se mi v tomto ohledu zdá OOUZ jednodušší a pojmově čistší. Na druhou stranu vyjádření o jejich zpracování je stanoveno jasněji než v případě OOUZ, který sice také uvádí podmínky, za kterých je možné tyto údaje zpracovávat, ale jasně nedeclaruje, že jiné případy jejich zpracování jsou nepřijatelné. V tomto ohledu hovoří GDPR jasněji.

Zcela nový pojem, který GDPR zavádí, je pseudonymizace. Tou se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě. Pseudonymizace patří mezi technická a organizační opatření zvyšující ochranu osobních údajů v případech, kdy je to z hlediska posouzeného rizika třeba (viz např. čl. 32 odst. 1 GDPR).

Profilování je další nový pojem, který GDPR zavádí. Podle definice jde o jakoukoli formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

Následující tabulka (Tab. 1) ukazuje srovnání posledních dvou pojmů, tedy správce a zpracovatel, kterým zde budu věnovat pozornost, tak, jak jsou uvedeny v OOUZ a GDPR. Z tabulky je zřejmé, že obě definice jsou velmi podobné a zahrnují stejné subjekty.

Pojem	Zákon č. 101/2000 Sb. (OOUZ)	GDPR
Správce	Správce se rozumí každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj.	Správce se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.
Zpracovatel	Zpracovatelem se rozumí každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.	Zpracovatelem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Tab. 1: Srovnání vybraných pojmů mezi OOUZ a GDPR.

Zásady zpracování osobních údajů

GDPR zavádí (a pojmenovává) konkrétní zásady zpracování osobních údajů. Ve většině případů se nejedná ve srovnání s OOUZ o novinky, avšak jejich systematizace je nová a zcela jistě přínosná. V rámci tohoto základního rozboru se omezím jen na vyjmenování těchto zásad s jejich stručnou charakteristikou. Většina formulací vychází z ustanovení čl. 5 GDPR, pokud není dále uvedeno jinak.

Základní zásady zpracování osobních údajů jsou:

- **Zákonnost** – podmínky zákonnosti zpracování osobních údajů jsou dány čl. 6 GDPR, patří mezi ně zejména udělení souhlasu subjektem údajů, nebo nezbytnost pro splnění právních povinností, anebo nezbytnost pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
- **Korektnost** – jde o obecnou vlastnost způsobu zpracování osobních údajů.
- **Transparentnost** – ta se týká nejen obecného způsobu zpracování, ale též poskytování informací subjektu údajů dle čl. 12, 13 a 14 GDPR. Musí být též zakotvena v kodexech chování dle čl. 40. Zásada transparentnosti je uplatňována také v dalších případech, jako jsou procesy vydávání osvědčení nebo jmenování členů dozorových orgánů.
- **Účelové omezení** – osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.
- **Minimalizace údajů** – osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- **Přesnost** – zpracovávané osobní údaje musí být přesné, což znamená také případnou povinnou aktualizaci a přijetí opatření zajišťující, aby nepřesné údaje byly vymazány nebo opraveny. Pokud provedeme srovnání s pravidly pro základní registry veřejné správy v České republice, tak zde je ještě povinnost před opravou tyto údaje ihned po zjištění případných nesrovnalostí označit jako zpochybněné. Stejně tak postupuje stávající OOUZ. Je překvapivé, že GDPR takové vyznačení přímo nepožaduje.
- **Omezení uložení** – to znamená uložení na dobu nezbytnou pro účel jejich zpracování.
- **Integrita a důvěrnost** – osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.
- **Odpovědnost** – primární odpovědnost má správce, přičemž podle čl. 5 odst. 2 musí být schopen dodržení souladu zpracování osobních údajů se základními zásadami doložit. Další pravidla pro odpovědnost jsou definována v čl. 24 a čl. 82 GDPR.

Práva subjektu údajů

V rámci základního rozboru GDPR se opět omezím pouze na vyjmenování, popř. stručné komentáře k jednotlivým právům subjektu údajů. Než k tomu přistoupím, rád bych připomněl slova z čl. 4 preambule, že právo na ochranu osobních údajů není právem absolutním a že musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality a že musí být v rovnováze s dalšími základními právy. Aplikování níže uvedených práv je tedy vždy třeba posuzovat v kontextu konkrétních situací, při kterých ke zpracování osobních údajů dochází.

GDPR tedy přiznává subjektu údajů následující právo:

- **Právo na stručná, transparentní, srozumitelná a snadno přístupná sdělení** týkající se postupů pro výkon práv subjektu údajů (viz čl. 12).
- **Právo na přístup subjektu údajů k informacím o zpracovávaných osobních údajích o své osobě.** Poskytované informace se liší podle toho, zda osobní údaje jsou získány od subjektu údajů, nebo zda osobní údaje nebyly získány od subjektu údajů (viz čl. 13, 14 a 15).
- **Právo na opravu** znamená, že subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení (viz čl. 16).
- **Právo „být zapomenut“** je rozšířením dřívějšího práva na výmaz v taxativně určených případech, např. pokud subjekt údajů odvolal souhlas se zpracováním svých osobních údajů. GDPR uvádí pro výmaz bez zbytečného odkladu zejména následující důvody (čl. 17):
 - osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,

- subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně.
- Právo na omezení zpracování v konkrétních případech stanovených v čl. 18 GDPR.
- Právo na přenositelnost údajů je v této podobě novým přístupem, který má zjednodušit pohyb osobních údajů se souhlasem subjektu údajů. Podle čl. 20 GDPR má subjekt údajů právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Velice podstatné je, že toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen (viz čl. 20 odst. 3 GDPR), protože jinak by se orgány veřejné moci vedoucí různé registry, zejména evidenci obyvatel, staly zcela jistě terčem obrovského množství požadavků na tyto údaje.
- Právo vznést námitku znamená, že subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají (detailně viz čl. 21).
- Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně týká (čl. 22).
- Právo podat stížnost u dozorového úřadu definuje čl. 77.
- Právo na účinnou soudní ochranu vůči dozorovému úřadu je popsáno v čl. 78.
- Právo na účinnou soudní ochranu vůči správci nebo zpracovateli definuje čl. 79.
- Právo na náhradu újmy je posledním z pojmenovaných vymezených kategorizovaných práv subjektu údajů. Toto právo znamená, že kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy (čl. 82 odst. 1 a další).

Povinnosti správců a zpracovatelů

Jak již bylo zmíněno dříve, jsou povinnosti správců a zpracovatelů osobních údajů definovány zejména v člancích 24 až 43 cit. nařízení. Nicméně při řešení otázek zpracování osobních údajů z pohledu správců a zpracovatelů se nelze omezovat jen na tato ustanovení a je třeba si pročíst celé nařízení. Obecnou základní povinností správců a zpracovatelů je třeba dodržovat základní zásady zpracování osobních údajů, jak je stanoví čl. 6 a další. Další obecnou poznámkou je v podstatě nemožnost připravit univerzální návody. Při každém zpracování osobních údajů se přihlíží k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob. Podle toho jsou pak aplikována příslušná opatření. Mezi základní opatření patří pseudonymizace, minimalizace údajů a šifrování osobních údajů. Neznamena to však, že pseudonymizace musí být provedena vždy, když se osobní údaje zpracovávají.

Již několikrát byla zmíněna a v čl. 30 je konkrétně specifikována povinnost vést záznamy o činnostech zpracování. Účelem je zejména doložitelnost souladu s GDPR.

Z obecných povinností uveďme ještě ustanovení čl. 31, které říká, že správce a zpracovatel a případný zástupce správce nebo zpracovatele spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů.

Pokud dojde k porušení zabezpečení osobních údajů, správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí tuto událost dozorovému úřadu. Uvedenou povinnost lze velmi dobře srovnat s povinností ohlašování incidentů podle zákona o kybernetické bezpečnosti [4]. Navíc pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu také subjektu údajů.

Mezi zásadní postupy pro správce patří povinnost provést posouzení vlivu na ochranu osobních údajů pro každý konkrétní případ zpracování, který může být spojen s vysokým rizikem pro práva a svobody fyzických osob (viz čl. 35). Je pravděpodobné, že v tomto případě mohou vzniknout určité typizované postupy týkajících se opakovaných případů, např. zpracování osobních údajů orgány veřejné moci vyplývajících ze speciálních zákonů. V případě, že z posouzení vyplyne, že správce musí přijmout určitá opatření a tato přesahují jeho možnosti, nebo i po jejich aplikování stále hrozí vysoké riziko, je stanovena povinnost předchozí konzultace s dozorovým úřadem (čl. 36). Uvedené podmínky vedoucí k povinné konzultaci jsou jen jedním z přístupů a názorů na ustanovení GDPR, přičemž lze očekávat, že bližší pokyny případně bude publikovat sám dozorový úřad, tedy v případě České republiky Úřad pro ochranu osobních údajů.

Pověřenec pro ochranu osobních údajů

Mezi povinnosti správce a zpracovatele patří jmenování pověřence pro ochranu osobních údajů. Protože se jedná o zcela nový institut, který je navíc povinný pro všechny orgány veřejné moci, věnuji se mu zde v samostatné kapitole. Pověřenec musí být tedy jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů (čl. 37 odst. 5 GDPR). Z hlediska orgánů veřejné moci, které si z principu nekonkurují, není problém ve „sdílení“ pověřence mezi více organizacemi, což připouští i GDPR za podmínky, že bude z každé organizace snadno dosažitelný (čl. 37 odst. 2 GDPR). Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů (čl. 38 odst. 1 GDPR). Protože se pověřenec v rámci plnění svých úkolů podle čl. 39 GDPR dostává k interním informacím organizace, je v souvislosti s výkonem svých úkolů vázán tajemstvím (čl. 38 odst. 5 GDPR). Pověřenec pro ochranu osobních údajů může plnit pro organizaci i jiné úkoly a povinnosti, ale z hlediska jeho postavení je velmi důležité, ba přímo zásadní, aby žádný z jeho úkolů a povinností nevedl ke střetu zájmů (čl. 38 odst. 6 GDPR). Znamená to, že to nemůže být např. vedoucí IT oddělení apod. Postavení pověřence pro ochranu osobních údajů v organizační struktuře správce či zpracovatele musí být velmi specifické, aby měl příslušné pravomoci a nedostával se do střetu zájmů.

Mezi základní úkoly pověřence pro ochranu osobních údajů patří zejména (čl. 38 a 39 GDPR):

- poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle GDPR,
- monitorování souladu s GDPR v oblasti ochrany údajů,
- monitorování souladu s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů,
- spolupráce s dozorovým úřadem,
- působení jako kontaktní místo pro dozorový úřad,
- působení jako kontaktní místo pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR.

Stanovení deliktů a sankcí

Jak již bylo zmíněno výše, jsou postupy týkající se ukládání správních pokut a jejich výše stanoveny přímo GDPR. Posouzení každého jednotlivého případu však závisí na dozorovém úřadě. Ustanovení čl. 83 odst. 1 a 2 k tomu říká, že

- každý dozorový úřad zajistí, aby ukládání správních pokut ohledně porušení tohoto nařízení bylo v každém jednotlivém případě účinné, přiměřené a odrazující,
- správní pokuty se ukládají podle okolností každého jednotlivého případu.

Podle čl. 83 GDPR platí, že za porušení určených povinností správce či zpracovatele a za porušení určených povinností subjektu pro vydávání osvědčení lze uložit pokutu až do výše 10 mil. EUR (nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší). Za porušení základních zásad pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9, nebo za porušení určených práv subjektu údajů, dále v případě nesplnění příkazu dozorového úřadu a za neposkytnutí přístupu dozorovému úřadu i v dalších taxativně určených případech lze uložit pokutu až do výše 20 mil. EUR (nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší). Výše těchto pokut významně přesahuje dosavadní praxi a jasně naznačuje, že ochranou osobních údajů je třeba se vážně a důkladně zabývat.

Kromě uvedených sankcí stanoví členské státy EU pravidla pro jiné sankce, jež se mají ukládat za porušení tohoto nařízení, zejména za porušení, na něž se nevztahují správní pokuty podle čl. 83, a učiní veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující.

Shrnutí

Tento základní rozbor nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, si rozhodně nekládá za cíl být úplným a komplexním, ale chtěl poukázat na základní rysy a obsah nařízení jako celku. Zároveň z něj jasně plyne, že ochranu osobních údajů nelze podceňovat, což ale platilo už od 1. června 2000, kdy nabyl účinnosti původní český zákon č. 101/2000 Sb., o ochraně osobních údajů. Vybraná srovnání GDPR s tímto zákonem ukázala, že v základních principech se toho zas až tolik nemění. Z hlediska orgánů veřejné moci je nejvýraznější novinkou povinnost jmenovat pověřence pro ochranu osobních údajů. Z hlediska i dalších subjektů pak povinnost poskytnou osobní údaje subjektu údajů pro jejich přenos jinému správci a zpracovateli. Konkrétní další praktické dopady GDPR bude možné detailně posoudit, až bude známo znění adaptačního zákona (či zákonů).

Literatura

- [1] LECHNER, Tomáš. Nebude nařízení eIDAS jen další promarněnou příležitostí? *IT Systems*. 2016, roč. 18, č. 7–8, s. 6–7. ISSN 1802-002X.
- [2] MATES, P., SMEJKAL, V. *E-government v České republice: Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání, Praha: Leges, 2012.
- [3] FIALOVÁ, E. *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges, 2016.
- [4] SMEJKAL, V. *Kybernetická kriminalita*. Aleš Čeněk, 2015.
- [5] EVROPSKA KOMISE. *The Digital Single Market strategy* [online]. [cit. 2015-06-06]. Dostupné z: <<https://ec.europa.eu/digital-agenda/en/digital-single-market>>.

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/65/2017 „Změny v úkolech obcí v důsledku změn českých a evropských právních předpisů“.

GDPR – nové nařízení zasáhne celou veřejnou správu

Mgr. Bc. Tomáš Mudra, UEPA advokáti, s. r. o.; Mgr. Vladimíra Hloušková, d-eye CZECHIA, s. r. o.

Přestože se již od začátku loňského roku začaly objevovat první články na téma nové evropské úpravy ochrany osobních údajů (např. článek z března loňského roku „Nové nařízení EU o ochraně osobních údajů. Jak se dotkne České republiky?“), je vhodné se k tomuto tématu znovu vrátit, a to nikoliv naposledy.

Důvodem je skutečnost, že nové evropské **Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů EU 2016/679** (dále jen „Nařízení“) schválené v dubnu 2016, je i na evropské předpisy neobyčejně obsáhlým dokumentem, který má ale naprosto zásadní dopady do každodenního života mnoha subjektů – obce jako součást veřejné správy nevyjímaje. Přestože se jedná o téma zásadní, je dosud k dispozici jen minimum metodických materiálů a zdá se, že vláda nemá koncepci, jak zajistit splnění povinností dle nařízení napříč veřejným sektorem. Protože tak hrozí, že obce se budou muset přizpůsobovat novým povinnostem „na poslední chvíli“, pojďme se podívat, co může být z jejich pohledu zásadní.

Co to je GDPR čili Nařízení?

Nařízení je evropský předpis srovnatelný svojí vahou a postavením s českým zákonem. Zároveň je to méně obvyklý druh evropského právního předpisu, který na rozdíl od tzv. směrnic ukládá povinnosti přímo všem občanům EU a společnostem podnikajícím v EU. **Práva a povinnosti obsažená v nařízení tak platí pro všechny bez ohledu na národní předpisy** (které nesmějí být s Nařízením v rozporu) **od okamžiku účinnosti Nařízení, tj. od 25. 5. 2018.**

Jaký dopad má Nařízení na činnost obcí?

Jelikož Nařízení upravuje zpracování osobních údajů fyzických osob, je jeho dopad na obce zásadní. Jako orgán samosprávy a orgán veřejné moci obce při plnění většiny svých úkolů osobní údaje zpracovávají (tzn. shromažďují, zaznamenávají, strukturují nebo pozměňují údaje schopné přímo či nepřímo identifikovat subjekt údajů – fyzickou osobu), čímž se ocitají v roli správce, popř. zpracovatele dle Nařízení.

Obce přitom v rámci své vlastní i přenesené státní působnosti zpracovávají i speciální kategorie osobních údajů jako jsou např. osobní údaje dětí (úsek školství), popř. o zdravotním stavu fyzických osob (zajišťování poskytování sociálních služeb), pro které platí ještě speciální právní úprava.

Ačkoli orgány veřejné moci mohou být od některých povinností dle Nařízení za daných okolností na základě speciálních národních předpisů osvobozeny, obce se zejména na některých úsecích svých činností **musí připravit:**

- na realizaci informační povinnosti vůči fyzickým osobám,
- na nová či rozšířená práva fyzických osob (např. právo na omezení zpracování, právo na přenositelnost osobních údajů, právo na opravu osobních údajů) a
- na povinnost vést záznamy o činnostech zpracování.

Tato příprava zahrnuje nejenom vypracování příslušné dokumentace, ale i úpravu informačních systémů, a to tak, aby byly dle Nařízení bezpečné a schopné poskytnout dostatečnou technickou podporu pro plnění povinností obce jako správce dle Nařízení.

Nařízení dále zavádí pro většinu případů zpracování tzv. **posouzení dopadu na ochranu osobních údajů**, což je interní analýza správce (v tomto případě obce), která obsahuje rozbor rizik, která dané zamýšlené zpracování či proces přináší fyzickým osobám a způsoby jejich systematického ošetření.

Obce jako orgány veřejné moci jsou též povinny jmenovat **pověřence pro ochranu osobních údajů**, tj. nového úředníka, který bude dohlížet na zpracování osobních údajů obcí v souladu s Nařízením (dále jen

„pověřenec“) a poskytovat v této oblasti odborné poradenství. Pověřenec musí být nezávislý (tzn. nemůže se jednat o nikoho, kdo v obci rozhoduje o účelech a prostředcích zpracování) a odborně způsobilý (viz dále). Zavedení této funkce může obcím pomoci i při samotné přípravě na zavedení Nařízení.

Jaká rizika vyplývají z nezahájení včasné přípravy na Nařízení?

Jelikož na zavedení potřebných postupů a procesů je nyní jen o něco více než rok (povinnost zpracovávat v souladu s Nařízením bude od 25. 5. 2018), přináší případná pozdní příprava na zavedení Nařízení tato **rizika**:

4. Obec nebude mít v termínu určeny odpovědné osoby do rolí pověřence a zpracovatele posouzení vlivu na ochranu osobních údajů.
5. Obec nebude mít včas zpracováno a schváleno Posouzení vlivu na ochranu osobních údajů.
6. Obec nebude mít nastaven proces a vyčleněny prostředky pro přenos údajů jinému správci na základě žádosti dotčené osoby (právo na přenositelnost údajů).
7. Obec nebude mít nastaven proces a vyčleněny prostředky na poskytování informací o zpracování osobních údajů na žádost dotčené osoby a nebude mít zpracovanou související dokumentaci
8. Obec nebude mít nastaven proces archivace dat a dokumentů (včetně skartace) tak, aby odpovídal Nařízením.
9. Obec nebude mít nastaven proces komunikace s dozorovým orgánem.
10. Obec nestihne včas určit odpovědné osoby, zpracovat a schválit potřebnou dokumentaci a nastavit procesy u všech svých podřízených organizací, u nichž je zřizovatelem.

Výše uvedená rizika pak mohou vyústit v **postih** ze strany dozorového orgánu, který může určit pokutu za porušení pravidel obsažených v Nařízením. Výše sankcí pro orgán veřejné moci ještě sice v naší zemi nebyla stanovena, ale obecně může dle Nařízení dosáhnout až 20 milionů EUR. Nadto se v rámci porušení povinnosti poškozené mohou fyzické osoby domáhat i odškodnění.

Jak rizika spojená se zaváděním Nařízení eliminovat či zmenšit?

Za prvé, **na nic nečekat a začít jednat**. Času je málu a povinnosti ukládané Nařízením jsou velmi dobře známy.

Za druhé, je třeba **zajistit odborníky**, kteří zpracují potřebnou dokumentaci a budou komunikovat s odpovědnými orgány. Pokud se obec rozhodně řešit vše **vlastními silami**, musí nejprve určit pracovníky, kteří budou mít agendu ve svém popisu práce, přičemž je potřeba zohlednit v případě pověřence požadavek na jeho nezávislost a zákaz konfliktu zájmů. Je přitom vysoce pravděpodobné, že takové pověření zaměstnanci budou potřebovat školení, aby mohli tuto činnost vykonávat. Obce pak do doby přípravy musí započítat také dobu na výběrové řízení pro školení, zpracování vlastní dokumentace a dobu na její schválení. Je potřeba zároveň nezapomínat, že v rámci činnosti obcí existuje několik z pohledu osobních údajů velmi odlišných oblastí.

Další možností je **využití služeb komerčních poskytovatelů**. Výhodou je, že tento poskytovatel má smluvní odpovědnost za poskytované služby (na rozdíl od zaměstnance, kdy výše náhrady škody je zastropována), je pojištěný a má k dispozici proškolený personál. Nevýhodou je, že správce musí nechat třetí osoby nahlédnout do procesů zpracování dat, datových modelů, datových a dokumentových úložišť i interní dokumentace jako je například skartační řád. Využití služeb komerčních poskytovatelů dále komplikuje skutečnost, že těchto poskytovatelů je na současném českém trhu málo (dle provedených odhadů výrazně méně, než bude v souvislosti s Nařízením zapotřebí).

S předchozím bodem pak tedy přímo souvisí nutnost **začít neprodleně připravovat výběrová řízení**, a to buď na školení zaměstnanců nebo na dodávku služeb GDPR komerčními poskytovateli.

Je nutné mít vlastní zaměstnance či je vhodnější zakoupit si externě poskytované služby?

Pro mnohé obce již nyní vyvstává otázka, zda je **vhodnější** výše uvedené povinnosti řešit vlastními silami nebo využít komerčně nabízených služeb.

Uvedenou otázku je nutno řešit především s ohledem na výši nákladů, které zákonem vyvolaná povinnost obcím přinese. Obce v závislosti na metodických pokynech Ministerstva vnitra ČR budou muset a již nyní mohou jmenovat pověřence pro ochranu osobních údajů. Pověřenec může být jak zaměstnanec obce, tak může své úkoly plnit i na základě smlouvy o poskytování služeb, vždy ale musí být jmenován na základě svých profesních kvalit, zejména na základě svých **odborných znalostí** práva ochrany osobních údajů, Nařízení a praxe v oblasti ochrany osobních údajů. Velkou výhodou je pak **znalost prostředí**, kde ke zpracování osobních údajů dochází.

Zaměstnávat vlastního pověřence a svěřit mu dohled nad osobními daty má své výhody i nevýhody. Pozitivním faktem je, že lidé zevnitř přesně znají firemní procesy a kdykoli je potřeba, mohou být „přímo u zdroje“. Naopak nevýhodou je paradoxně fakt, že jsou svázáni konvencemi obce. Často je třeba pohled externího odborníka, aby dokázal přemýšlet nestranně. Sporným bodem je pak finanční úspora při zaměstnávání vlastního pověřence. Zde velice záleží na velikosti obce. Nejde jen o výplatu jednomu pověřenci, ale také o nutnost mít i další vlastní profesionály na správu a zpracování osobních dat a provádění doporučení pověřence. Upozorňuje přitom např. na skutečnost, že pověřenec díky konfliktu zájmů, nemůže zpracovat posouzení dopadu na ochranu osobních údajů.

Vlastní pověřenec zná chod a procesy u obce a může si vypěstovat „čich“ na případné problémy. Naproti tomu ale nemá nadhled a přináší obci poměrně vysoké mzdové náklady.

V případě **smluvní spolupráce** s externím pověřencem nebude potřeba navyšovat počet pracovních míst uvnitř obce a tento externí pověřenec bude mít větší nadhled na způsob a zabezpečení ochrany osobních dat realizovaných obcí.

Rozhodně se však vyplatí sednout si s tužkou a papírem a počítat.

Jak vypsát zakázku na služby?

Pro výběr externího pověřence bude potřeba obcí realizovat zadávací řízení. Dle interních pokynů obce se ale bude vždy jednat o veřejnou zakázku malého rozsahu, tj. o VZ mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Její předpokládaná hodnota bude dle velikosti obce realizována především přímým poptáním, případně uzavřenou nebo otevřenou výzvou uveřejněnou prostřednictvím profilu zadavatele obce.

Závěr

Nařízení bude mít výrazný dopad do fungování obcí, s nímž není možné se vyrovnat ze dne na den. Ačkoli je jasné, že reakce státní správy a samosprávy na Nařízení bude muset být centrálně koordinována, rozsah povinností je již nyní plně znám a nic nebrání tomu, aby se obce začaly na tyto povinnosti připravovat již nyní. Je to dokonce zcela žádoucí, jelikož tato včasná příprava jim ušetří mnohé náklady spojené s případným „ostrým“ startem na jaře příštího roku a také jim umožní přesněji identifikovat skutečné potřeby obce a náklady s plněním povinností s Nařízením spojené.

Smart Cities? Města, kde je radost žít

Václav Pávek, ředitel odboru Smart Cities&Regions, GORDIC spol s r. o.

Pojem Smart je v dnešních dnech jedním z nejskloňovanějších termínů nejen ve světě informačních a komunikačních technologií. Smart City je především chytré využití moderních technologií tak, aby byl život v obcích kvalitnější, hospodárnější a bezpečnější. Zásadní je, aby se občanům žilo příjemněji a pohodlněji v kvalitním prostředí. Celý koncept bude zbytečný a kontraproduktivní, pokud nebude svým účelem směřovat efektivně a ekonomicky na život spoluobčanů v obci s ohledem na udržitelný rozvoj.

Život v chytrém městě

V chytrém městě si pomocí mobilní aplikace můžete zjistit například volné místo k parkování, díky senzorům umístěným na lampách veřejného osvětlení. Navigace v autě Vám ukazuje trasu nejen vzhledem ke vzdálenosti a rychlosti, ale také vzhledem k aktuální dopravní situaci, neboť je online zásobována informacemi z dopravního centra města. Ve stavebnictví a v energetice se realizují chytré budovy, které umožňují chytrě řídit a plánovat spotřebu energií. Občané si nemusí vybírat dovolenou a běhat po úřadech, protože si vše vyřídili po internetu, popř. si zarezervovali čas úředníka.

Vídeň: blízká inspirace

Jeden příklad za všechny je město, které je dlouhodobě na špičce kvality života a nemusíme jezdit nikam daleko – jedná se o Vídeň. Vídeň letos v hodnocení kvality života obhájila v konkurenci 230 světových měst první příčku, a to poosmé za sebou! Praha je pro zajímavost až na 69. místě, i když z měst bývalého východního bloku opět zvítězila. U Vídně se inspirovalo také řešení GORDIC ve tvorbě a publikace OpenDat.

Čeští lídři

V České republice je již mnoho míst s prvními pilotními smart realizacemi. Za jednu z úplně prvních realizací se považuje Smart region Vrchlabí. V Praze je se smart řešeními nejdále městské části Praha 1 a Praha 3. Na Praze 1 např. zaujme realizace chytrých prvků v odpadovém hospodářství. Na Praze 3 je nutné ocenit organizační ustanovení oddělení Smart City s hlavním architektem a koncepční práci ve spolupráci s ČVUT UCEEB s plánem a s cíli v horizontech let 2020, 2030 a 2050 – velmi podobně, jako zmíněná Vídeň.

Ruku v ruce s bezpečností

Bezpečnost je zásadní vlastností, kterou musí systém naprosto splňovat. Klíčový je aktuálně zákon o kybernetické bezpečnosti, ovšem bylo by chybou myslet pouze na něj. Velmi důležité je také vzdělávání veřejnosti, neboť ve výsledku to je uživatel, který systém ovládá, a jehož data a nejen data jsou v ohrožení. I u těchto technologií platí „dobrý sluha, ale zlý pán“. A kdo na nebezpečí zneužití nebude myslet hned od začátku architektury, zadělává si na problémy do budoucna.

GORDIC a Smart Cities

Vedle jednotlivých smart projektů jako je Smart Administration nebo realizace energicky efektivních budov je to především schopnost bezpečné integrace chytrých technologií. V oblasti nabídky produktů GORDIC se protínají tři platformy: GINIS (veřejná správa), KYBEZ (kybernetická bezpečnosti) a GYBER (internet věcí). Díky propojení těchto platforem a technologií třetích stran jsme schopni nabídnout plně integrovaný produkt. A to navíc s vysokým stupněm znalosti prostředí a specifik veřejné správy.

Elektronický zdravotní záznam jako základní stavební kámen e-health řešení – pohled praktický i legislativní

Jan Petřík, Institut pro elektronizaci zdravotnictví, z. ú.

1. Úvod

Dnešní svět se vyznačuje silným tlakem na regulaci všech možných oblastí lidské činnosti zdravotnictví nevyjímaje. Všechny státy Evropské unie, včetně České republiky, zažily během posledních let exponenciální nárůst právních předpisů všech úrovní. Právní předpisy se dnes snaží popsat a regulovat všechny aktivity a činnosti, kterými se člověk, resp. společnost zabývá. Touto snahou byrokraticky popsat a zaznamenat všechno graduje ve společnosti i dějinný konflikt státní moci a občanů daného státu. Růstem právní agendy totiž adekvátně roste i ingerence státu do soukromí občanů. V článku 2 odst. 3 Ústavy ČR je totiž stanoveno, že státní moc slouží všem občanům a lze ji uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Pokud tedy není určitá pravomoc pro stát ukotvena zákonem, státní moc v této oblasti nemá co pohledávat. V této oblasti pak mohou naopak občané činit všechno, co jim zákon nezakazuje. Jde o spojené nádoby dvou právních zásad, které se v právu neustále vývojem společnosti kontrolují a regulují. Takzvané zásady enumerativnosti veřejnoprávních pretenzí a zásady legální licence. Zásada enumerativnosti veřejnoprávních pretenzí vyjadřuje, že veřejnou moc lze uplatňovat jen v případech, mezích a způsoby, které stanoví zákon. Zásada legální licence, jež je opakem zásady enumerativnosti veřejnoprávních pretenzí, pak vyjadřuje, že každý může činit vše, co zákon nezakazuje, a naopak není povinen činit nic, co mu zákon neukládá.

Jinými slovy, vznikne-li ve společnosti jakákoliv nová oblast činnosti, stát, aby co nejrychleji vyrovnal hladiny těchto spojených nádob, reaguje obvykle legislativní změnou a doplněním zákonů tak, že takovou činnost zreguluje, vytvoří na ni kolonku, statistické označení, definuje úředníka, jeho pravomoci, možnosti kontrol a samozřejmě i sankcí. Tím ovšem vzniká dosti kazuistická změt' zákonných a podzákonných norem, které jenom v závěsu reagují na lidskou činnost a kreativitu, navzájem spolu nekomunikují a mnohdy jsou ve své snaze regulovat a kontrolovat vše ve vzájemném konfliktu. Velmi trefně toto vystihl v nedávné době v rozhovoru pro Aktuálně.tv předseda Nejvyššího správního soudu ČR JUDr. Josef Baxa, který dokonce tvrdí, že s růstem právní regulace ubývá svoboda. Doslova k tomu uvedl, že: „**Přibývá právní regulace, všechny předpisy, které přibývají a mění se, tak ukrájí kousek svobody, je to byrokratická setrvačnost, které bychom se měli bránit.**“ Podle JUDr. Baxy společnost navíc příliš spoléhá na to, že stát se o ni postará. Nejenže se stát o společnost automaticky ve všem nepostará, ale dokonce lze pochybovat, že se stát postará o společnost dobře, pokud tak učiní. V devadesátých letech se v ČR dokonce ustálilo rčení, že stát je nejhorší hospodář. To pak bylo hlavní silou ekonomické privatizace, kdy stát otevřeně přiznával, že nemusí a ani nechce kontrolovat všechno. Je tomu nyní jinak? Zjistil stát, že je pro něj naopak lepší a vhodnější kontrolovat a dohlížet na všechny oblasti lidské činnosti a kreativity? A nyní i zásadní otázka pro oblast elektronizace zdravotnictví. Je eHealth třeba nejdříve detailně popsat, dostat jej do legislativy a také regulovat? Je třeba s vývojem a implementací eHealth čekat na zákonodárce a byrokratický státní aparát? Autor tohoto článku je bytostně přesvědčen, že nikoli.

2. Elektronický zdravotní záznam neboli EHR podle Národní strategie elektronického zdravotnictví

EHR je ve schválené Národní strategii elektronizace zdravotnictví (NSEZ) popsán na mnoha místech. Jedna ze základních definic je pak následující: „**Osobní elektronický zdravotní záznam (EHR/PHR) bude obsahovat vybrané zdravotní údaje, lékové záznamy a výsledky vybraných vyšetření. Záznamy budou prostřednictvím indexu okamžitě dostupné oprávněným poskytovatelům zdravotních služeb i pacientovi. Minimální rozsah sdílených zdravotních údajů (elektronického zdravotního záznamu), povinnosti poskytovatelů**

zdravotních služeb a pravidla přístupu k nim, práva a povinnosti správců, budou stanoveny legislativně. Osobní zdravotní záznam umožní trvale ukládat vybrané zdravotní údaje, lékové záznamy a výsledky vybraných vyšetření. Záznamy budou prostřednictvím indexu zdravotnické dokumentace okamžitě dostupné oprávněným poskytovatelům zdravotních služeb i pacientovi a popř. dalším subjektům (lékaři lékařské posudkové služby pracující v resortu práce a sociálních věcí, lékárníci, nebo revizní lékaři zdravotních pojišťoven). Záznamy budou dostupné jak z prostředí webového rozhraní, tak pro přímý přístup z informačních systémů poskytovatelů zdravotních služeb (pokud dodavatelé tento přístup do svých systémů implementují). Minimální rozsah sdílených zdravotních údajů (elektronického zdravotního záznamu), povinnosti poskytovatelů zdravotních služeb a pravidla přístupu k nim, práva a povinnosti správců, budou vycházet z platné legislativy a budou realizovány v souladu s cíli národní strategie elektronického zdravotnictví. Systém umožní také zápisy informací pacientem v pro něj vyhrazené části seznamu. S dostatečným předstihem je vhodné reagovat na potřebu sdílet vybrané informace i pro sociální služby, což je mj. budoucnost v podobě integrace služeb.

Integrované zdravotní a sociální služby nelze ve velkém měřítku efektivně zavádět bez sdíleného PHR (nebo EHR) se sociálními službami. Toto budoucí sdílení však musí mít legislativní oporu.“ Výše uvedený popis je komplexní a vyčerpávající. Shrnutí:

- (a) EHR je dlouhodobým záznamem o zdravotních údajích a zdravotní péči jednoho konkrétního pacienta.**
- (b) Do EHR zapisuje data zdravotnický pracovník a případně i pacient.**
- (c) EHR je dostupný on-line oprávněným poskytovatelům zdravotních služeb i pacientovi.**
- (d) Z kontextu NSEZ je zřejmé, že EHR není zdravotnickou dokumentací pacienta, ale spíše jejím souhrnem.**
- (e) Na několika místech se objevuje volání po potřebě legislativních změn.**

NSEZ zároveň obsahuje velmi zajímavé kapitoly pojednávající o EHR v jiných zemích a využití tohoto systému. Studie Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services (Milieu Ltd – time.lex) sledovala specifická pravidla pro výslovný souhlas pacienta s ukládáním a zpracováním jeho dat v rámci elektronických zdravotních záznamů. V Německu, Francii, Chorvatsku a Itálii je uplatněn princip opt-in; zatímco v Rakousku, Lucembursku, Švédsku a Anglii je pak možné implicitní souhlas s vedením EHR odvolat (princip opt-out). Česká republika patří mezi země, kde pacient musí výslovně souhlasit s vedením a zpracováním dat mimo poskytovatele zdravotních služeb, Národní strategie elektronického zdravotnictví prosazuje princip opt-out.

Ve 14 zemích je pro identifikaci pacientů pro eHealth využívána ID karta; ve 13 zemích je to pak číslo zdravotního pojištění. Specifický identifikační kód pro eHealth není zaveden v žádné zemi. Ve 13 zemích je zakotveno právo pacienta nahlížet / kopírovat data ze sdíleného elektronického zdravotního záznamu; v 11 zemích jsou implementovány mechanismy auditovaného přístupu, které umožňují pacientovi zjistit údaje o přístupech k jeho záznamům. V 5 zemích je pacientovi dána možnost modifikovat / vymazat data ze svého zdravotního záznamu, která byla vložena jiným subjektem. Jakkoliv je tedy ve většině zemí zřejmé, že data patří pacientovi, nesmí se ve většině z nich k datům chovat jako skutečný vlastník s právem je měnit a mazat. To je samozřejmě z hlediska ochrany zdraví a efektivity systému vhodné a logické. Národní strategie elektronického zdravotnictví příliš nehovoří o výhodách EHR a sdílení. Je to logické. Jde o strategický dokument, který nemá sloužit jako promotérská aktivita v rámci elektronizace, ale nastavovat základní klíčové cíle a metody jejich dosažení. Zároveň je zřejmé, že výhody EHR jsou jasně čitelné a logické i bez jejich výslovného shrnutí. Dají se shrnout do dvou základních pilířů. Mnohé z nich lze zároveň označit za výhody elektronického zdravotnictví obecně.

Základní výhody:

(a) **Zapojení pacienta**

- **Prevence, zvyšování zdravotní gramotnosti.** Jde o notorietu, která je již obecně akceptována. Prevence je v důsledku pro systém levnější než následná péče. Pomáhá odhalovat nemoc v raném a často léčitelném stádiu. Zdravotní gramotnost oproti tomu vede k prodloužení zdravé fáze života. Zdravotní gramotnost jako nástroj příznivě ovlivňuje schopnost lidí ovlivňovat svůj životní a zdravotní osud. Bývá nepříjemné si přiznat, že je statisticky prokázáno, že skupiny s nízkou zdravotní gramotností nejvíce čerpají zdravotní služby, nevyužívají prevenci a systém nejvíce zatěžují.
- **Technologické trendy.** Lidé obecně nyní tíhnou k čím dál většímu používání technologických novinek. Nástup mobilních telefonů, internetu, počítačů a chytré (smart) technologie je čím dál rozšířenější. Systémy jsou jednodušší, rychlejší a srozumitelnější.
- **Elektronická identita.** Lidé jsou v rámci dobrého elektronického systému identifikovatelní. Mohou jeho prostřednictvím činit úkony, včetně úkonů právních a mohou systém využívat k jednodušší komunikaci.
- **Efektivní a levná komunikace.** Komunikace prostřednictvím elektronických systémů je rychlá, levná a má všechny předpoklady, aby byla i efektivní.
- **Pacient určuje přístup a sdílení.** Občan (pacient) je osobou, která si v systému opt-in nebo opt-out určí, zda chce být jeho součástí a jakým způsobem se mají jeho zdravotní data sdílet. Osoby s respektem k sdílení mohou nebýt v systému, nebo limitovat sdílení svých dat. Je statisticky prokázáno i v rámci ČR, že většina osob nemá problém se sdílením svých zdravotních záznamů¹.

(b) **Zlepšení zdravotní péče**

- **Přístup odkudkoliv.** Přístup k EHR má být realizován z jakéhokoli externího prostředí, kde je k záznamu potřeba přistoupit (např. ordinace, terén).
- **Podpora pro rozhodování.** EHR je jako základní informace o pacientovi nejrychlejší možnou podporou pro rozhodování lékaře. V současné době je zdrojem dat pacient, což v případě EHR zůstává, ale tento zdroj je doplněn informacemi z EHR, na které již pacient mohl zapomenout. EHR může být zdrojem informací i v případě, že pacient nekomunikuje (např. bezvědomí).
- **Rychlost.** V případě on-line sdílení jde zatím o nepřekonanou a asi i těžko překonatelnou rychlost posunu informací mezi jednotlivými body.
- **Koordinace péče.** Sdílením základních informací v rámci EHR mezi jednotlivými profesemi může dojít k zásadnímu zvýšení efektivity koordinace péče. Nejzákladnějším příkladem, který by potřeboval efektivní komunikaci prostřednictvím EHR je řetězec praktik – specialista – laborať – lékárna.
- **Nadstavbové systémy.** Nad systémem EHR lze budovat takřka nekonečné množství nadstavbových modulů a využívat jejich funkcí. Příkladem jsou moduly snižující administrativu, telemedicína, disease management, umělá inteligence atd.

Lze shrnout, že NSEZ popisuje základní strategii ohledně EHR vhodným způsobem, ačkoliv nedefinuje katalog jeho přínosů. NSEZ ovšem volá po zásadních legislativních změnách, které by definovaly jednak obsah EHR a zároveň parametry jeho sdílení. Otázka je opět nasnadě. Jsou tyto legislativní změny nutné? Je třeba s rozjezdem EHR systému vyčkávat a implementovat je až svou práci odvede zákonodárský sbor?

3. Práva občana (pacienta)

Odpověď lze částečně nalézt v legislativě ohledně práv pacienta, jak tato existuje nyní. Postavení pacienta je nyní v legislativě v zásadě rovnocenné (rovné, svobodné a občanskoprávní) s postavením zdravotnického

¹ Například v systému Elektronické zdravotní knížky EZK souhlasilo s nejšířší možností sdílení osobních zdravotních záznamů 83 % osob.

pracovníka. Úprava dvou zásadních kodexů regulujících vztahy, tj. občanského zákoníku a zákona o poskytování zdravotních služeb tento rovnocenný vztah jenom podtrhuje. V praxi je pacient často označován za klienta lékaře, jakkoliv tento termín může být zavádějící. Důležité je ovšem to, že pacient má podstatným způsobem definováno právo na informace o svém zdravotním stavu již nyní. Základní definici tohoto práva lze rozdělit na právo ústavní neboli právo „jednoduché“ a právo dané zákonem a podzákonnými předpisy.

3.1 Ústavní předpisy ČR a mezinárodní smlouvy

Listina základních práv a svobod Článek 31 Listiny stanoví, že: „**Každý má právo na ochranu zdraví.** Občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon.“ Článek 17, který je v části politických práv, pak pojednává o právu na informace tak, že právo na informace jsou zaručeny a každý má právo svobodně vyhledávat informace. Jde o práva politická, a tak je jejich propojení s článkem 31 sporné, ale nikoli nemožné. **Úmluva o lidských právech a biomedicíně, kterou ČR ratifikovala a vyhlásila ve sbírce č. 96/2001** Tato úmluva o právu na informace hovoří už zcela jasně. Dle čl. 10 této mezinárodní smlouvy má každý právo na ochranu soukromí ve vztahu k informacím o svém zdraví s tím, že **každý je oprávněn znát veškeré informace shromažďované o jeho zdravotním stavu.** Nicméně přání každého nebýt takto informován je nutno respektovat. Pokud je to v zájmu pacienta, může ve výjimečných případech zákon omezit uplatnění práv pacienta na informace. Uvedené „jednoduché“ právo tak stanoví jasný rozsah toho, co má každý právo po systému požadovat. Slova jako „veškeré informace shromažďované o jeho zdravotním stavu“ a „ochrana zdraví“ nedovolují jiný výklad než ten, že **každý občan ČR má nárok na to, aby:**

- (a) dostal informace o svém zdravotním stavu a zároveň
- (b) dostal informace, které o jeho zdravotním stavu „systém“ shromažďuje.

3.2 Zákon o zdravotních službách

Ještě zajímavější je popis informací, které má právo pacient znát podle zákona č. 372/2011 Sb., o zdravotních službách. Tento zákon je v popisu práv již detailnější, což může svádět k tomu, že platí pouze to, co je v něm definováno, ovšem pravda to není. Pokud zákon nepopisuje detailně právo stanovené ústavním předpisem, či na takové právo zapomíná, je nutné použít úpravu jednoduchého – ústavního práva a práva pacienta čist jeho optikou.

Práva pacienta ve vztahu k informacím

Ustanovení § 28 zákona stanoví: (1) Zdravotní služby lze pacientovi poskytnout pouze s jeho svobodným a **informovaným souhlasem**, nestanoví-li tento zákon jinak. (...) (3) Pacient má při poskytování zdravotních služeb dále právo (...) b) zvolit si poskytovatele oprávněného k poskytnutí zdravotních služeb, které odpovídají zdravotním potřebám pacienta, a zdravotnické zařízení (...), c) vyžádat si konzultační služby (...), d) být seznámen s vnitřním řádem zdravotnického zařízení (...).

Informace o zdravotním stavu pacienta a o navržených zdravotních službách

Ustanovení § 31 zákona shrnuje informace, které má pacient dostat při přijetí do péče a jindy, je-li to účelné. Jakkoli ustanovení směřuje k situaci, kdy je pacient už „pacientem“, první část jasně hovoří ještě o zdravotním stavu a pokrývá samozřejmě i situace, kdy zdravotní stav nevyžaduje detailní informace dle odst. 2 tohoto ustanovení nebo vyžaduje jenom jejich část. Poskytovatel je podle tohoto ustanovení povinen zejména zajistit, aby byl **pacient srozumitelným způsobem v dostatečném rozsahu informován o svém zdravotním stavu** a o navrženém individuálním léčebném postupu a všech jeho změnách. Informace o zdravotním stavu pak obsahuje zejména údaje o: (a) příčině a původu nemoci (...), (b) informace k navrhovaným zdravotním službám (obsah, přínosy, rizika atd.), (c) jiných možnostech zdravotních služeb, (d) další potřebné léčbě, (e) omezeních a doporučeních ve způsobu života a (f) možnosti vzdát se podání informace o zdravotním stavu, určit jiné osoby nebo vyslovit zákaz o podávání informací o zdravotním stavu.

Nahlížení do zdravotnické dokumentace, pořizování jejích výpisů nebo kopií

Ustanovení § 65 zákona pak komplexním způsobem upravuje možnost nahlížení do zdravotnické dokumentace a možností pořizovat si z ní kopie nebo výpisy. Do zdravotnické dokumentace vedené o pacientovi mohou v přítomnosti zaměstnance pověřeného poskytovatelem nahlížet, pořizovat si její výpisy nebo kopie samozřejmě pacient, zákonný zástupce nebo opatrovník pacienta, ale i osoby určené pacientem. Postupy nahlížení nesmí narušit poskytování zdravotních služeb. Bez souhlasu pacienta pak mohou nahlížet do zdravotnické dokumentace třetí osoby jenom za přesně určených podmínek. Musí to být v zájmu pacienta nebo potřebné pro účely vyplývající ze zákona nebo jiných právních předpisů.

Nahlížení musí proběhnout jenom v nezbytném rozsahu. Nahlížení pak může provést jenom přesně definovaný okruh osob, kdy se jedná zejména o osoby se způsobilostí k výkonu zdravotnického povolání a jiní odborní pracovníci v přímé souvislosti s poskytováním zdravotních služeb nebo osoby podílející se na výkonu působnosti příslušného správního orgánu.

V ustanovení § 66 pak zákon definuje způsob pořízení kopie a výpisu, lhůty a další parametry této již velmi podrobně popisované činnosti. Zajímavé je, že je-li zdravotnická dokumentace vedena pouze v elektronické podobě, má pacient nebo jiná osoba oprávněná podle § 65 zákona právo nahlížet dálkovým přístupem nebo na pořízení její kopie na technickém nosiči dat, který si určí, nebrání-li tomu technické možnosti poskytovatele. Zákon zde již hovoří jasně o elektronizaci nahlížení do zdravotnické dokumentace. Mohlo by se zdát, že slova jako „pouze“ a „technické možnosti“ limitují tento postup. Pravda je taková, že má-li k nahlédnutí nebo pořízení kopie dojít, jeví se elektronická cesta opět jasně jako nejvhodnější a nejefektivnější. Uvedená práva jsou pak detailně popisována i podzákonnými předpisy a dále na různých informačních webech ministerstva zdravotnictví (viz. http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html), na stránkách Ministerstva práce a sociálních věcí (viz. <http://www.mpsv.cz/cs/840>), <http://www.pravnilinka.cz/bezplatna-pravni-poradna-zdarma/prava-pacienta.html>, <http://ferovanemocnice.cz>, webech nemocnic, poliklinik atd. Zdrojů je skutečně dost.

4 Od zákonů k EHR a k pacientovi

Pacient a občan má ve světle výše uvedeného již poměrně dost široká práva na informace o svém zdravotním stavu. Připomeneme-li si ještě charakter postavení pacienta a lékaře, který má být v zásadě rovnocenný, lze dojít k možnosti, že si tyto subjekty mohou nad rámec zákona ještě mnohé dohodnout smluvně, a to jak ústně, tak písemnou formou.

Čím nižší právní předpis v tomto směru zkoumáme, tím složitější úpravu najdeme a větší komplikace si tím způsobíme.

Zajímavé vodítko v tomto směru definuje **zákon č. 101/2000 Sb., o ochraně osobních údajů**. Osobní údaj vypovídající o zdravotním stavu patří mezi citlivé osobní údaje subjektu údajů a jeho zpracování se řídí podmínkami upravenými zejména v § 9 zákona o ochraně osobních údajů. V citovaném ustanovení zákon o ochraně osobních údajů očekává, že ke zpracovávání citlivých osobních údajů správcem nebo zpracovatelem může docházet za podmínky, že subjekt údajů dal ke zpracování výslovný souhlas. Souhlas subjektu údajů musí být dán subjektem údajů a musí z něho být zřejmé, k jakým údajům je dáván, jakému správci údajů, k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může subjekt údajů kdykoliv odvolat. Správce je povinen předem subjekt údajů o jeho právech poučit. V návaznosti na uvedené lze tedy učinit několik závěrů:

- (a) Občan má právo na informace o svém zdravotním stavu**
- (b) Občan má právo dostat informace, které o jeho zdravotním stavu systém shromažďuje**
- (c) Občan má uvedená práva bez ohledu na to, zda je nemocný či zdravý**
- (d) Občan má právo dát souhlas se správou a zpracováním informací o jeho zdravotním stavu**
- (e) Občan má právo určit k jakým účelům lze jeho zdravotní informace zpracovávat.**

Skutečně zásadní otázka tedy nyní zní: „Je podle stávajících právních předpisů možné, aby občan souhlasil se shromažďováním, správou a zpracováváním informací o svém zdravotním stavu za účelem realizace databáze EHR a jsou poskytovatelé zdravotních služeb povinni mu takovou možnost shromažďování a zpracovávání informací umožnit?“ Podle všeho ano.

5 Existující databáze EHR v ČR

Výše uvedené právní shrnutí není v českém prostředí úplnou novinkou. Databáze zdravotních záznamů již v ČR existují a jsou pořizovány v rámci stejné nebo podobné právní úvahy, jako je uvedena shora. Zatím největší stopu na trhu v ČR zanechal projekt IZIP Elektronická zdravotní knížka, který byl provozován stejnojmennou společností již od roku 2001 převážně pro klienty Všeobecné zdravotní pojišťovny. Projekt zažil některé vrcholy i útlumy. V českém i evropském kontextu však šlo o projekt zcela jedinečný, který možná tak trochu předběhl svou dobu. Stávající stav projektu je takový, že společnost IZIP se přejmenovala na společnost ZDRAVEL, a.s., která je nyní v soukromých rukou investiční skupiny, jež provoz EZK zafinancovala z vlastních zdrojů a provoz databáze znovu obnovila. V přehledné tabulce lze shrnout stav projektu IZIP/ZDRAVEL následovně: V přehledové tabulce jsou vidět základní údaje ke stavu databáze ZDRAVEL.

Počet uživatelů demonstruje počet fyzických osob, které se do systému registrovaly. Podepsaly souhlas se shromažďováním, zpracováním a sdílením svých zdravotních záznamů ve smyslu kapitoly 3 výše. Podpis tohoto souhlasu byl ověřen buď oficiálně dle právních předpisů (notář, Czech Point atd.) nebo lékařem, který měl s IZIP, a.s. uzavřenou smlouvu a který za přihlášku pacienta dostával odměnu od VZP. Historicky největší podíl registrovaných osob do systému ZDRAVEL zajistili právě lékaři. Lze konstatovat, že v ČR neexistuje databáze sdílení zdravotních informací s větší základnou, než je právě ZDRAVEL. Registrovaná zdravotní zařízení a zdravotničtí pracovníci jsou pak profesionálové, kteří mají se ZDRAVEL, a.s. uzavřenou smlouvu o zpracování osobních údajů v systému.

Aktuální stav systému ZDRAVEL	
Počet uživatelů:	2 556 668
Počet zdravotnických pracovníků v systému ZDRAVEL:	20 968
Počet zdravotnických zařízení v systému ZDRAVEL:	8 631
Vykázané léky:	163 685 111
Předepsané léky:	11 302 797
Vydané léky:	21 290 350
Ambulantní vyšetření:	13 643 938
Laboratorní vyšetření:	7 252 002
Anamnézy:	641 695
Hospitalizace:	137 913
Očkování:	370 024
Diagnózy:	12 387 157
Celkem zdravotních záznamů:	230 710 990

Obrázek 1 – Přehledová tabulka stavu systému ZDRAVEL, zdroj www.zdravel.cz

Smlouva upravuje způsob nakládání s daty ze strany zdravotnických profesionálů, jejich vkládání, nahlížení do nich a další parametry spolupráce. I v tomto směru jde o největší smluvní agendu v rámci sdílení patientských dat. Poslední jsou pak v tabulce uvedena jednotlivá data ve strukturované podobě. Systém obsahuje cca 230 mil. zdravotních záznamů v různé podobě. Jsou zde anamnézy, laboratorní výsledky, předepsané i vydané léky a další informace. I v tomto směru jde o jednu z největších evropských databází sdílených patientských dat typu EHR. NSEZ obsahuje ve svém textu následující klíčovou deklaraci: „Stát nebude vytvářet žádný megalomanský centralistický projekt, ale zajistí základní stavební kameny elektronizace, které umožní postupný vznik a realizaci účelných dílčích projektů, sladěných se strategickými záměry a stanovenými principy uvedenými v této strategii.“ V dalším textu pak NSEZ uvádí: „**Prioritním záměrem strategie je maximální využití existujících informačních systémů** za podmínky, že splní kvalitativní, bezpečnostní a další požadavky na interoperabilní systémy elektronického zdravotnictví, tedy zejména požadavky na vstupní/výstupní formát dat a modularitu, tj. jednotlivé informační systémy mohou vznikat nezávisle na sobě, ale budou si schopné předávat data, protože bude definována jejich struktura. Dosažení vzájemné interoperability dosavadních řešení elektronického zdravotnictví je i ochranou investic a využitím současného potenciálu fungujících aplikací.“ Jedná se o velmi prozíravé řešení. Vždyť je zjevné, že například výše uvedená databáze ZDRAVEL je velkou historickou investicí připravena na to, aby se některé náklady nemusely utrácet znovu. **Má-li pak databáze ZDRAVEL nějaké parametry, jsou to tyto:**

- Je postavena na bázi právních předpisů popsaných výše a **je tedy plně legální.**
- Díky vysoké historické investici do Elektronické zdravotní knížky EZK **reprezentuje EHR databáze ZDRAVEL cca 1/4 obyvatel České republiky** s 230 mil. zdravotních záznamů.
- Databáze **nabízí extrémní možnost úspor v nákladech.** Jeden registrovaný člověk stál v nákladech IZIP 200 až 300 Kč. Je tedy možné hovořit o úsporách v řádech stovek milionů korun a dosahujících až tři čtvrtě miliardy Kč.
- Projekt byl neregionální a je tedy rozšířen po celé ČR a díky migraci pojištěnců již nyní **nezahrnuje jenom pojištěnce VZP**, ale i dalších pojištěnoven.

6 Závěr

Na základě výše uvedeného lze konstatovat, že již dnešní právní předpisy umožňují vznik EHR databází, jak je definuje Národní strategie elektronického zdravotnictví. Zákony sice nyní ještě nedefinují přesný obsah EHR, strukturu a parametry sdílení, ale umožňují, aby občané dávali souhlas se sdílením svých základních zdravotních informací za účelem dosažení výhod EHR. Databáze EHR tedy mohou vznikat a působit v ČR a následně regulaci a legislativním změnám, které Národní strategie elektronického zdravotnictví předpokládá se postupně přizpůsobovat. Národní strategie elektronického zdravotnictví je zároveň vizionářská a lze ji chválit v tom, že její prioritou je využití stávajících řešení v elektronickém zdravotnictví. Proto a díky tomu lze realizovat mnohé úspory, které by v případě využití stávajících projektů mohly dosahovat stovek milionů korun, případně i řádů miliard Kč.

Literatura

- [1.] Ústavní systém České republiky, 5. Vydání, Gerloch Aleš, Hřebejk Jiří, Zoubek Vladimír, vydavatel Aleš Čeněk, s.r.o. <https://video.aktualne.cz/josef-baxa/1~i:keyword:31293/>
- [2.] Národní strategie elektronického zdravotnictví ČR, 11. 10. 2016 schváleno ministrem zdravotnictví ČR, 28. 11. 2016 schváleno vládou ČR, www.nsez.cz
- [3.] Prof. MUDr. Jan Holčík, Role zdravotní gramotnosti v péči o zdraví, 2009
- [4.] Šustek P., Holčápek T. a kol., Zdravotnické právo, Praha: Wolters Kluwer ČR, 2016 852 str.

CZ.PEPS: základ infrastruktury pro vzájemné uznávání eID

Mgr. Jiří Průša, CZ.NIC, z. s. p. o.

Jednu z nejvýznamnějších novinek, kterou eIDAS přináší, představuje vzájemné uznávání elektronické identifikace (eID). Hlavní myšlenkou eIDAS v oblasti elektronické identifikace je v souladu se snahou o vybudování tzv. jednotného digitálního trhu umožnit vzájemné uznávání eID prostředků (typicky, ale nejen elektronické občanky). Velmi zjednodušeně řečeno, aby se např. Estonec, který má v České republice firmu, mohl se svojí elektronickou občankou přihlásit do datové schránky.

Zatímco většina ustanovení nařízení eIDAS již vstoupila v platnost a v České republice i v ostatních zemích Evropy s nimi žijeme již 9 měsíců, **povinnost umožnit vzájemné uznávání eID** vznikne členským státům od **29. září 2018**. Do tohoto data bude muset mít každý členský stát svůj funkční národní eIDAS uzel, zajišťující propojení s dalšími uzly v Evropě. Český národní uzel pod názvem CZ.PEPS buduje na základě smlouvy s Evropskou komisí v rámci Nástroje pro propojení Evropy (CEF) sdružení CZ.NIC.



Filosofie a fungování eIDAS uzlů

Zatímco u elektronických podpisů vychází eIDAS především z dnes již neplatné Směrnice č. 99/93/ES, regulace eID představuje značné rozšíření oblasti regulace, byť ani zde Komise nestavěla na „zelené louce“ a navázala na výsledky především tzv. rozsáhlých pilotních projektů (LSP), zejm. projektu STORK 2.0 a e-SENS.

Již v roce 2008, kdy začínal projekt STORK, se přitom ukázalo, že jednotlivé národní systémy a jejich legislativa jsou natolik odlišné, že řešení jednotné či společné občanky nejsou pro členské státy přijatelné a cesta vede přes propojení skrze národní brány². Ústřední role těchto uzlů pro propojení systémů elektronické identifikace členských států je zdůrazněna rovněž v prováděcím Nařízení č. 2015/1501³, které upravuje požadavky na tyto uzly. Jedním z hlavních požadavků je zajištění bezpečnostních standardů dle mezinárodní normy ISO/IEC 27001.

Tyto národní uzly jsou prostřednictvím SAML 2.0 vzájemně propojeny systémem „každý s každým“. Úkolem jednotlivých provozovatelů PEPS je pak zajistit napojení těchto bran na národní eID prostředky, přičemž eIDAS podporuje využití více typů prostředků (i od různých vydavatelů – identity providerů) tak, aby uživatel měl možnost volby. Rozhodnutí o tom, zda členský stát umožní svým občanům přihlašování i k zahraničním službám (tj. oznámí svůj národní systém), záleží pouze na jeho rozhodnutí a na rozdíl od uznávání cizích eID se nejedná o povinnost dané země.

Elektronické občanky i mojeID

V České republice bude provoz národní brány integrován do Národní identitní autority (NIA), kterou v rámci projektu MORIS 2.0 buduje Správa základních registrů. V rámci NIA, resp. portálu eIdentita.cz, si pak každý občan bude moci zvolit ten eID nástroj, který mu nejvíce vyhovuje, resp. odpovídá tzv. úrovni důvěry vyžadované provozovatelem dané služby. Stejně jako v klasickém světě by i v tom elektronickém měly základní identifikační a autentizační prostředky představovat občanské průkazy. Ty však dle novely zákona o **občanských průkazech**, která je stále v legislativním procesu, nebudou vydávány dříve než v létě 2018.

² Ve STORKu nazývané jako Pan European Proxy Services – PEPS, odkud též název CZ.PEPS.

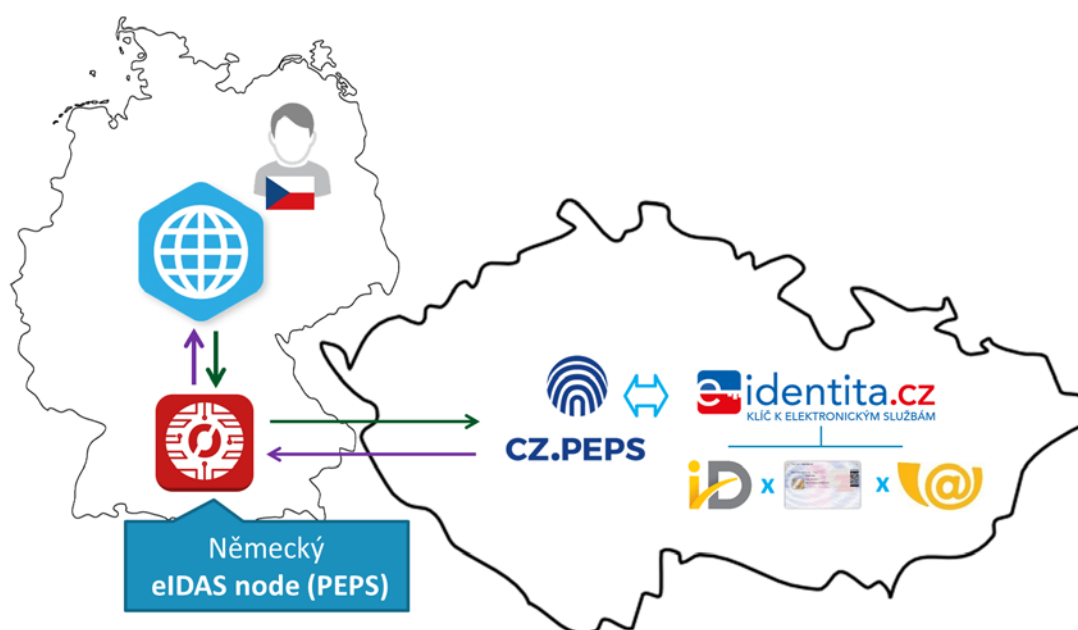
³ Prováděcí nařízení Komise 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. CELEX: 32015R1501. Dostupné na <http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015R1501&from=CS>.

Dalším vážným kandidátem na získání statusu národního eID nástroje, v souladu s eIDAS, je služba jednotných identit **mojeID**⁴, kterou již nyní využívá pro přihlášení na své stránky přes 150 městských a obecních úřadů a další instituce veřejné správy. Díky projektu STORK 2.0 pak mojeID funguje i pro vybrané zahraniční služby. Tou nejviditelnější je EU Login – autentizační služba Evropské komise⁵, kterou využívají např. úředníci pro přístup k dokumentům na jednání v Bruselu či je možné přes ni přistupovat k systémům na podávání grantů. Další zahraniční využití mojeID by mělo být již brzy možné v Holandsku pro přihlašování na portály tamějších měst.

Vedle mojeID se jako soukromoprávní poskytovatelé identit celkem logicky nabízejí i banky či telekomunikační operátoři. V úvahu přichází i informační systém datových schránek, který dnes neslouží již jen jako nástroj elektronického doručování, ale též jako autentizační nástroj pro přihlašování k vybraným službám e-Governmentu, např. daňový portál.

Zjednodušené schéma fungování přes-hraničního uznávání eID je znázorněno v následujícím Schématu č. 1 – Přes-hraniční uznávání eID.

Přes-hraniční uznávání eID

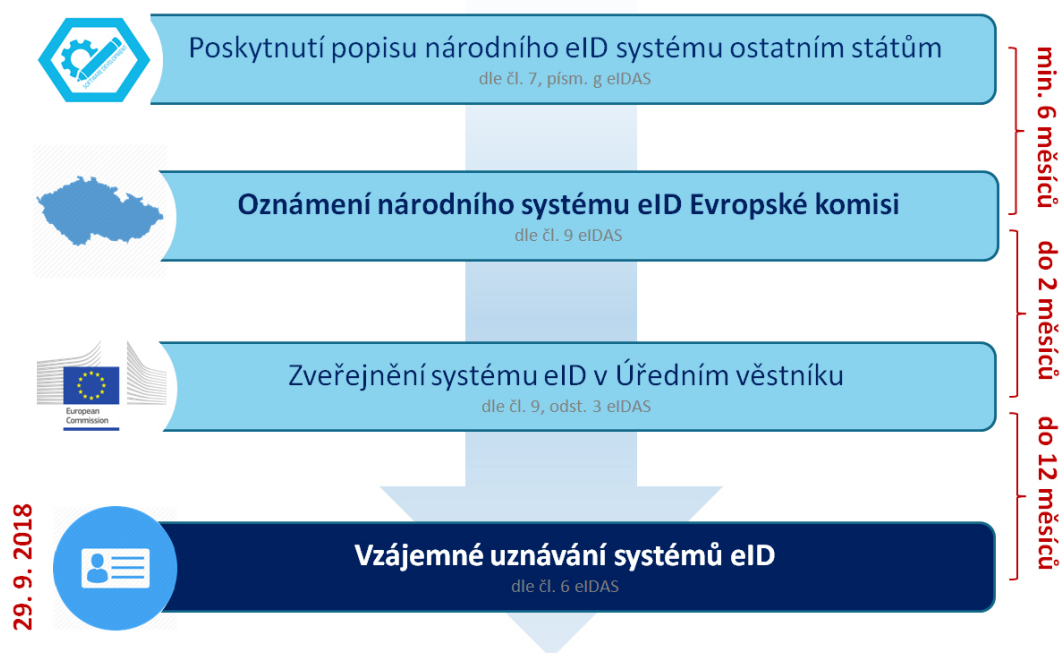


Z legislativního pohledu je však třeba si uvědomit, že od prvního oznámení národního eID nástroje vede ke vzájemnému uznávání napříč Evropu cesta dlouhá min. 18 až 20 měsíců (viz. Schéma č. 2 – Časový rámec vzájemného uznávání eID).

⁴ www.mojeid.cz

⁵ <https://webgate.ec.europa.eu/cas>

Časový rámec vzájemného uznávání eID



První krok v tomto ohledu učinilo zatím Německo, které popis svého systému založeného na elektronických občanských průkazech oznámilo 20. února 2017. Dalším vážným zájemcem je Estonsko, které již cizincům vydává tzv. e-Residency průkazy⁶. Ty dnes vlastní již více než 16 000 lidí ze 137 zemí světa, mezi nimi i více než 100 Čechů.

Ideální scénář pro Českou republiku?

Díky aktivitám sdružení CZ.NIC je Česká republika na vzájemné uznávání eID dle eIDAS z technického pohledu připravena již nyní. Díky projektu CZ.PEPS má Česká republika vybudovaný funkční eIDAS uzel a mojeID je připraveno stát se národním nástrojem se značnou úrovní důvěry. K tomuto kroku je však nutná politická vůle a uznání ze strany Ministerstva vnitra.

S ohledem na aktivity jiných členských států, zejm. Německa a Estonska, není důvod příliš vyčkávat. Pokud totiž budeme čekat až na schválení zákona o elektronické identitě, jehož účinnost nenastane dříve než od 1. ledna 2018, prvního českého eID nástroje umožňujícího dle eIDAS přihlášení k zahraničním službám e-Governmentu se dočkáme nejdříve ve druhé polovině roku 2019. A v té době se již může stát, že čeští občané budou využívat např. estonské e-Residency.

Oddalování oznámení národních eID zároveň oslabí konkurenceschopnost České republiky na jednotném digitálním trhu a je jasné, že s takovýmto přístupem cíl iniciativy 202020, tj. stát se 20. zemí s nejrozvinutějším e-Governmentem do roku 2020, nenaplníme.



Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

⁶ <https://e-estonia.com/e-residents/about/>

NetMetr: harmonizace otevřených dat napříč Evropou

Mgr. Jiří Průša; CZ.NIC, z. s. p. o.

Mezi jasné trendy posledních let v oblasti e-Governmentu patří bezesporu zpřístupňování dat veřejné správy. Za téměř 5 let, kdy se zmínka o otevřených datech poprvé objevila ve vládních dokumentech, zpřístupnily svá data již desítky českých úřadů a v loňském roce Evropská komise označila Českou republiku spolu se Slovenskem a Irskem mezi země rozvíjející svá data nejdynamičtěji v celé Evropě. Pokud si však chce Česká republika svoji pozici udržet a potenciál otevřených dat dále rozvíjet, je nutné, aby se jednotlivé iniciativy neomezovaly pouze na národní úroveň, ale byly propojeny napříč Evropou. Úspěšným příkladem je projekt „Open crowdsourcing data related to the quality of service of high-speed Internet“, jehož koordinátorem je sdružení CZ.NIC a který patří mezi pouhé dva mezinárodní projekty na otevřená data, které Evropská komise podpořila v rámci Nástroje pro propojení Evropy (CEF).

Základem byla aplikace na národní úrovni

Základy současného evropského projektu byly položeny v roce 2015, kdy sdružení CZ.NIC v úzké spolupráci s Českým telekomunikačním úřadem (ČTÚ) spustilo projekt NetMetr, který vychází ze zkušeností rakouského regulátora RTR⁷ v oblasti uživatelského měření tzv. kvality služeb (QoS) mobilního broadbandu, tj. možnosti si jako koncový uživatel ověřit, jaká je rychlost mého připojení k Internetu a zda můj operátor dodržuje např. zásady tzv. síťové neutrality definované především Nařízením Evropského parlamentu a Rady (EU) č. 2015/2120 ze dne 25. listopadu 2015 a souvisejícím doporučením „BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules“ (BoR (16) 127) ze dne 30. srpna 2016⁸.

Aplikaci NetMetr mohou zdarma⁹ získat jak uživatelé mobilních zařízení na platformě Android, tak na platformě iOS pro iPhone a iPad. Především pro zjištění kvality a rychlosti připojení na osobních počítačích je možné využít též webového rozhraní NetMetru. Veřejně přístupná část na www.netmetr.cz pak umožňuje anonymní zobrazení jednotlivých měření a publikaci výsledků ve formě otevřených dat. Díky vizualizaci ve formě mapy je pak možné ověřit např. reálně dosahovanou rychlost připojení od daného operátora v konkrétním místě.

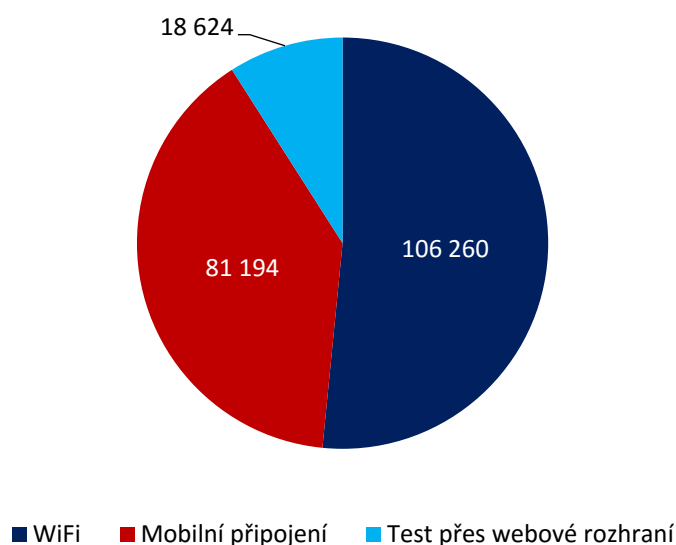
V současné době aplikaci NetMetr používají již tisíce uživatelů a za rok 2016 bylo realizováno přes 200 000 testů (viz graf).

⁷ Rundfunk und Telekom Regulierungs-GmbH

⁸ Dostupné on-line na http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

⁹ Aplikace lze získat přes odkaz na stránkách <https://www.netmetr.cz/cs/aplikace.html>

Podíl měření v NetMetru v roce 2016



Od národního projektu ke spolupráci napříč Evropou

Sdílení českých zkušeností s ostatními telekomunikačními regulátory v Evropě ukázalo, že podobné problémy – tj. především možnost ověření reálné rychlosti Internetu – řeší i v dalších zemích Evropy, což vedlo Český telekomunikační úřad k inicializaci užší spolupráce potvrzené v roce 2015 podpisem Memoranda o spolupráci¹⁰, jehož zakládajícími členy je vedle České republiky též Slovensko, Slovinsko a Chorvatsko a následně se k memorandu připojilo též Rumunsko.

V rámci této užší spolupráce realizované na základě čl. 20, 42(6), 46 Smlouvy o Evropské unii a čl. 326–334 Smlouvy u fungování Evropské unie pak byl v rámci výzvy v Nástroji pro propojení Evropy (CEF) zaměřené na oblast telekomunikací¹¹ předložen návrh společného projektu, jehož cílem je nejen rozvoj a sjednocení jednotlivých uživatelských aplikací, ale především vypracování celoevropské metodologie měření tak, aby data publikovaná na evropském portálu otevřených dat¹² vznikla na základě stejných kritérií bez ohledu na to, zda byla získána prostřednictvím české nebo slovenské aplikace.

Inspirace pro další české projekty

V oblasti otevřených dat se Česká republika rozhodně nemá za co stydět a i díky aktivitám Fondu Otakara Motejla u nás začaly úřady nejen otevírat svá data, ale vzniklo i mnoho užitečných aplikací. Projekt „Open crowdsourcing data related to the quality of service of high-speed Internet“ pak ukazuje, jakým směrem mohou vést další aktivity úspěšných českých iniciativ i to, že financování projektů e-Governmentu nemusí být realizováno pouze prostřednictvím strukturálních fondů.



Spolufinancováno Evropskou unií

Nástroj pro propojení Evropy

¹⁰ Celým názvem „Memorandum of Cooperation in the field of QoS and spectrum management“

¹¹ 2015-CEF-TC-2015-1

¹² <https://data.europa.eu/euodp/en/data/>

KYBEZ – platforma kybernetické bezpečnosti

Michal Řezáč, výkonný ředitel platformy KYBEZ, GORDIC spol s r. o.

KYBEZ je platforma pro efektivní spolupráci akademických institucí a komerčních firem zabývajících se osvětou, systematickým vzděláváním, managementem, službami a technologiemi v oblasti bezpečnosti informací, a to včetně kybernetické bezpečnosti a obrany.

Systematické vzdělávání, osvěta a efektivní kooperace akademických institucí a firem je tím nejdůležitějším úkolem platformy KYBEZ. Není to jen o kurzech, školeních, auditech a seminářích, cílem je prosadit bezpečnost informací do všech stupňů vzdělávání od základního až po doktorandské. Dále se platforma snaží spolupracovat s partnery a připravovat pro širokou veřejnost co nejzajímavější a zároveň nejdůležitější kurzy a školení. Jakmile totiž neexistuje povědomí o riziku, nebezpečí, tak lidé ani netuší, co všechno je ohrožuje. Bezpečnost informací a zdravotní hygiena jsou si v mnohém podobné, každý by si měl uvědomit a dodržovat běžná pravidla, aby neohrožoval sebe ani ostatní.

Partneři projektu KYBEZ jsou připraveni pomoci organizacím veřejné správy (veřejné moci), dalším zainteresovaným subjektům, jež to myslí s bezpečností informací vážně, a to nejenom ve splnění požadavků, které na ně zákon o kybernetické bezpečnosti klade. KYBEZ tedy není pouze sdružení firem, je to komunikační platforma spolupracujících firem. A to i takových, které si navzájem konkurují.

S příchodem etapy informační evoluce, jako je Internet všeho (IoE), Internet věcí (IoT), Smart Home, Smart Buildings, Smart Factories, Smart Cities, Smart Administration, „revoluční“ výzvy Průmysl 4.0 a eGovernment 4.0 nelze řešit kybernetickou bezpečnost bez přiměřené bezpečnosti informací. Kybernetickou bezpečnost proto považuje platforma KYBEZ nikoli pouze jen jako zákonnou povinnost, ale především za existenční nutnost.

KYBEZ - BEAN (bezpečnostní analytický nástroj)

Nově vzniklý analytický nástroj KYBEZ - BEAN byl navržen za účelem jednoduché a rychlé analýzy bezpečnosti informací. Na základě výsledků této analýzy můžete předejít potenciálním bezpečnostním hrozbám.

Analytický nástroj KYBEZ - BEAN poskytuje dvě varianty úrovní bezpečnosti informací, přičemž obě varianty budou umístěny na portálu KYBEZ a návštěvník si mezi nimi bude moci libovolně vybrat. U první varianty se jedná o odlehčenou verzi, která bude obsahovat obecnější otázky. Druhá varianta v sobě bude zahrnovat komplexnější otázky zasahující více oblastí bezpečnosti informací. Je cílena na specialisty IT, bezpečnostní pracovníky organizací a další relevantní osoby.

Odpovědný zájemce, zejména ten kdo bezpečnost informací dosud nijak neřešil, si vyzkouší strukturovaný test a může si uvědomit, jaké hrozby mu hrozí a jak zranitelné jsou systémy, se kterými pracuje. Cílem je, aby lidé zjistili, jaká rizika je ohrožují, a na základě toho se pak logicky budou chtít dozvědět, jak k těm rizikům přistupovat. A pro ně připravujeme opět v rámci KYBEZ náměty na vzdělávání a specializovaná školení.

Jak analýza funguje?

Po volně jedné z variant se uživateli zobrazí formulář, který obsahuje otázky různých oblastí bezpečnosti s různými typy odpovědí. Po vyplnění formulářového dotazníku probíhá vypočtení „score“, tedy jaké úrovně bezpečnosti daná organizace dosahuje. Dále analýza nabídne doporučení ke zlepšení, hrozby, které se jich mohou týkat s ohledem na výše uvedené normy, zákony a vyhlášky.

Přínosy tohoto nástroje spočívají v rychlosti ověření bezpečnosti informací, relevantních výsledcích, podkladech pro audit, doporučení k řešení problematických oblastí, nabídce konzultací zdarma nebo otázkách postavených na ZoKB, ISO a vyhláškách NBÚ.

Partnerský program

Do partnerského programu platformy KYBEZ v současnosti spadají instituce z oblasti veřejné správy, soukromého sektoru, dále to jsou auditorské firmy, certifikační autority, vzdělávací a akademické instituce či mediální organizace.

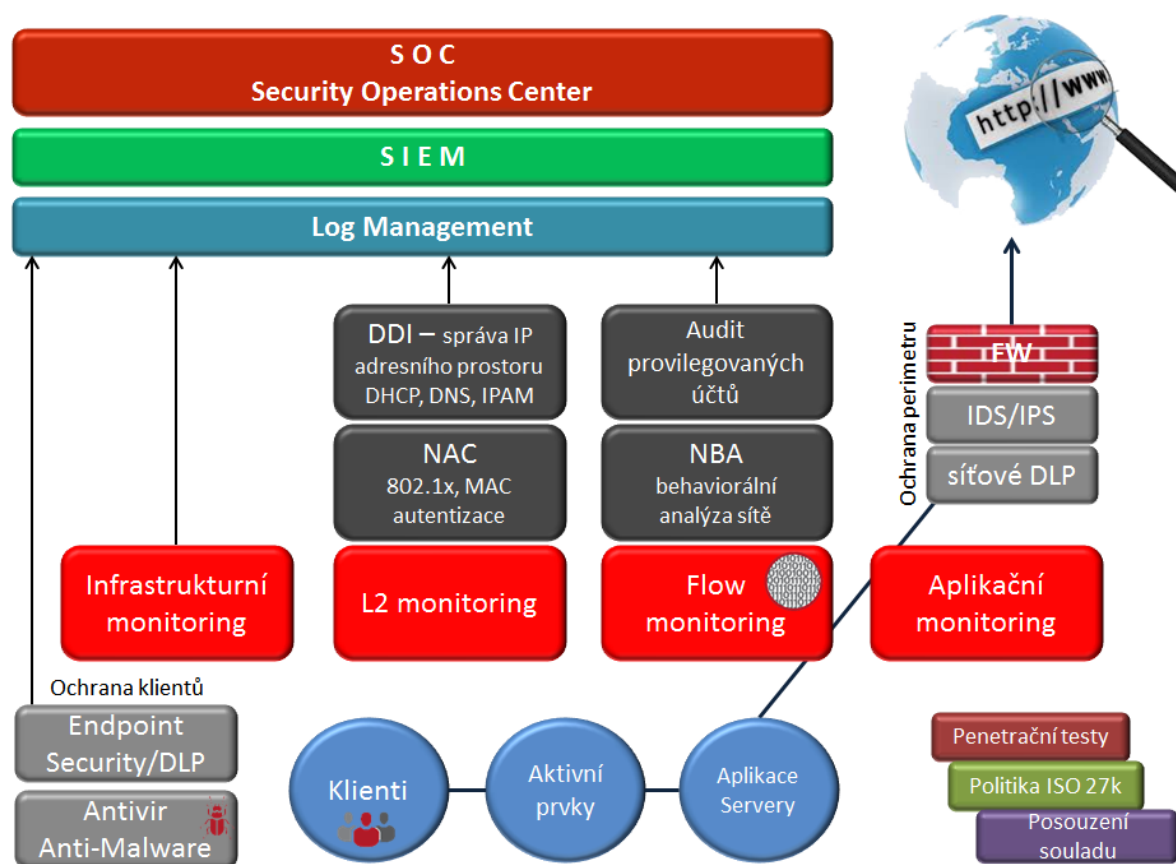


Koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury

Ing. Jiří Sedláček, CEO, Network Security Monitoring Cluster, družstvo

Úvod

Každá organizace využívající nástroje a technologie ICT řeší problematiku bezpečnosti a zajištění kontinuity svých procesů. To, že se jedná o téma nanejvýš aktuální, dokládá i vývoj v oblasti legislativní, tedy existence zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB) a zřízení Národního centra kybernetické bezpečnosti v rámci NBÚ. Tento článek představuje koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury (dále Koncept) vycházející jak z reálných potřeb, tak i z požadavků ZoKB.



Obrázek 1: Schéma NSMC konceptu aktivní bezpečnosti a spolehlivosti IT infrastruktury

Představovaný Koncept respektuje běžné fungování a zvyklosti organizací v oblasti informačních technologií a při práci s daty. Rovněž reaguje na nové požadavky, které na tuto oblast klade platná i připravovaná česká a evropská legislativa.

Do běžné infrastruktury organizace přidává sofistikované monitorovací nástroje a metody. Ty jsou dále rozšířeny o integrované nástroje pokročilé analýzy provozu datové sítě (NBA – Network Behavior Analysis) společně s nástroji pro komplexní správu IP adresního prostoru a řízením přístupů pevných i mobilních zařízení do sítě (IPAM/DDI/NAC). Tyto nástroje mohou být vhodně doplněny prostředky komplexní ochrany klientů (End Point Security). Samozřejmostí je koexistence s běžnými komponentami ochrany perimetru (Firewall, IDS/IPS, DLP apod.) a klientů (Antivir, Anti-Malware, Antispam apod.). Nasazení uvedených komponent v praxi znamená, že bezpečnost a spolehlivost se stává přímo vlastností IT infrastruktury a jako takovou ji není možné obejít, případně narušit.

Klíčovými a integrovanými komponentami Konceptu jsou:

- **Monitoring** (napříč všemi vrstvami datové sítě – L2 monitoring, L3/L4 monitoring datového provozu, L7 monitoring aplikací).
- **Behaviorální analýza sítě** (automatická detekce bezpečnostních i provozních incidentů).
- **Řízení přístupu do sítě** (omezení přístupu pouze pro povolená zařízení).
- **SIEM** (komplexní vyhodnocování a řízení informační bezpečnosti).

Prvním krokem pro aplikaci Konceptu v organizaci je vždy bezpečnostní analýza, která umožňuje zmapovat stávající stav a navrhnout konkrétní řešení.

Bezpečnostní analýza

Bezpečnostní analýzy jsou jednou ze specializovaných činností zabývajících se dekompozicí bezpečnostního problému z pohledu procesu, organizace zdrojů a technického řešení. Bezpečnostní analýza se zabývá evidencí aktiv, což je soubor procesních či datových vstupů a výstupů a soubor všech komponent technických řešení k zajištění vykonávaných procesních workflow.

V rámci zajištěné evidence aktiv lze v dalším kroku bezpečnostní analýzy postoupit k analýze vztahů aktiv vůči procesům společnosti – analýza rizik. Jejím cílem je identifikace slabých míst ve společnosti a doporučení k jejich minimalizaci či eliminaci. Synergickým efektem je identifikace kritických workflow a procesů společnosti či identifikace skutečných vlastníků workflow a procesů.

Hlavním výstupem bezpečnostní analýzy je dokumentace stávajícího IS/IT systému označovaná často jako tzv. Configuration Management Database (CMDB). V praxi jde o seznam komponent IS/IT a jejich vzájemných vztahů, na základě kterého mohou teprve zodpovědět otázku, co a jakým způsobem chráním.

Bezpečný perimetr – podmínka nutná, nikoliv postačující

Tradiční firewall pracující pouze na úrovni třetí a čtvrté síťové vrstvy je dnes již překonaným řešením. Moderní řešení pro ochranu perimetru musí být v reálném čase schopno rozpoznat a blokovat desetitisíce verzí škodlivého kódu při neustálé aktualizaci databáze známých hrozeb tak, aby byly schopny zachytit co nejvíce nových hrozeb a snížit riziko úniku citlivých dat organizace. Moderní firewally často integrují systémy označované jako Intrusion Detection/Prevention System (IDS/IPS) schopné v reálném čase vyhodnocovat rizika spojená s běžnými zranitelnostmi, jako je např. virem infikovaná příloha e-mailové zprávy nebo útok využívající známou zranitelnost operačního systému. V případě systému IPS je možné detekovaný útok přímo zablokovat.

Dalším logickým krokem je monitorování provozu lokální/vnitřní datové sítě tak, aby bylo možné reagovat na útoky, které perimetr překonají nebo jsou způsobeny přímo zaměstnanci organizace a na perimetru tyto útoky není možné zachytit.

Monitoring a analýza provozu datové sítě

Monitorování provozu (Flow Monitoring) a jeho následná analýza (NBA - Network Behavior Analysis) představuje moderní prostředek pro správu a bezpečnost IT infrastruktury označovaný jako tzv. next-generation monitoring. Na rozdíl od tradičního sledování dostupnosti aktivních prvků, serverů a služeb přináší úplný přehled o provozu datové sítě, jeho struktury, využívaných aplikací, chování uživatelů, provozních problémech a bezpečnostních incidentech.

Hlavní výhodou tohoto přístupu je v provozní oblasti kompletní viditelnost do sítě a rychlé vyhledávání skutečných příčin provozních problémů, v oblasti bezpečnosti pak automatická detekce pokročilých hrozeb,

útoků a malware bez použití signatur. Efektivně tak doplňuje tradiční řešení, jako jsou firewally, antiviry a systémy detekce/prevence průniků. Oproti řešením na straně klienta (tzv. host-based) přináší kompletní pokrytí IT infrastruktury bez nutnosti cokoli instalovat na jednotlivé stanice, vysokou škálovatelnost a nezávislost na platformě nebo operačním systému.

Důležitým předpokladem pro zajištění bezpečnosti sítě je také její náležitá řádná správa. Ta se v dnešní době neobejde bez řízení přístupu do datové sítě.

Řízení přístupu a adresní plánování

Centrální správa IP adresního prostoru (IPAM) formou vedení IP adresního plánu a vynucování IP adresní politiky (DDI) - kombinací integrovaného L2 monitoringu a řízením základních síťových služeb DHCP a DNS, je pro rozsáhlé datové sítě nezbytností. Integrované řízení přístupu do sítě (NAC), díky podpoře standardu 802.1x pro autentizaci a autorizaci oprávněných zařízení formou prokázání se suplikantem nebo MAC adresou s kontrolou proti podvržení, umožňuje efektivně řídit přístup do datové sítě vč. automatického vynucování politik (např. zařazení zařízení do VLAN) a to až na úrovni koncového bodu pro připojení k síti. Velkou výhodou je možnost využití rovněž dalších částí integrovaného DDI/NAC řešení, jako jsou L2 monitoring nebo správa BYOD zařízení pro dosažení vysoce efektivní správy sítě, zvýšení provozní spolehlivosti a bezpečnosti interní sítě. V kombinaci s dalšími integrovanými nástroji Konceptu (NBA, SIEM), rovněž zkrácení doby odpojení nežádoucích síťových zařízení.

Výše uvedené prostředky zajišťují bezpečnost napříč datovou infrastrukturou od perimetru datové sítě přes centrální prvky až po přístupové switche. Dalším úkolem IT oddělení je bezproblémový a spolehlivý provoz systémů a aplikací.

Provozní monitoring

Hlavním účelem provozního monitoringu je aktivní sledování dostupnosti klíčových prvků IT infrastruktury (serverů, tiskáren, aktivních prvků) a jejich systémových prostředků (zatížení procesoru, volné místo na disku, množství toneru, apod.). Podobně je možné simulovat a kontrolovat komplexní procesy jako je funkčnost e-mailového systému nebo měřit dobu pravidelného testovacího průchodu webovou aplikací. Na všechny výše uvedené metriky je možné definovat a následně vyhodnocovat SLA, tedy dosaženou kvalitu služby. Provozní monitoring tak snižuje kapacitní nároky na IT podporu, riziko pozdržení nebo neprovedení procesních operací, dále zvyšuje produktivitu práce uživatelů a umožňuje detekovat výskyt, identifikovat původce a lokalizovat místo problému.

Provozní monitoring pracuje na principu simulování chování uživatele, z čehož vyplývá zásadní omezení. Poskytované informace mohou být zkreslené, neboť odezva skutečných uživatelů v různých částech IT infrastruktury se může významně odlišovat od hodnot získaných syntetickým testem. Řešením je monitoring aplikací a jejich odezvy vůči skutečným uživatelům.

Monitoring aplikací

Monitoring aplikací v reálném čase sleduje, jak se aplikace „chová“ ke všem svým uživatelům, signalizuje celkové zdraví systému a určuje zdroje zhoršené výkonnosti, umožňuje odstranění úzkých míst v komplexních systémech a poskytuje reporting z pohledu business procesů i technologie. V ideálním případě by měl být založen na neinvazivní analýze síťového provozu, neboť instalace agentů na jednotlivé systémy může představovat ohrožení stability a funkčnosti monitorovaných aplikací.

Mezi monitorované metriky patří doba odezvy centrálního systému pro jednotlivé části aplikace, latence transportní vrstvy (uživatel – centrální systém), velikost přenesených dat nebo počet uživatelů a transakcí.

Téměř každá komponenta informačního systému je schopna generovat záznam o svém provozu, tzv. log záznam, ve kterém je uveden čas záznamu, identifikace komponenty a vlastní provozní status či detekovaný bezpečnostní stav. Sběr log záznamů a práce s nimi je procesně řízená činnost, která spadá pod proces Log management.

Log management

Log management představuje základní nástroj pro zajištění ochrany informací a bezpečnosti provozu ICT centralizací provozních a bezpečnostních informací z prostředí informačního systému organizace. Protože k rozsáhlé instalaci síťových serverů, pracovních stanic, mobilních zařízení se navíc přidává i rostoucí počet hrozeb z datových sítí i provozovaných systémů, tak počet log záznamů i výsledný datový objem výrazně narostl. Tím se vytváří aktuální potřeba řízeného procesu Log managementu, což je proces o vytváření, přenosu, uchování, analýzy a odstranění nepotřebných log záznamů. V případě potřeby, např. vyšetřování bezpečnostního incidentu, jsou tak všechny záznamy na jednom místě s možností provést např. jejich audit. Proces log managementu je možné dále automatizovat prostřednictvím tzv. SIEM systému.

SIEM – Bezpečnostní dohled informačního systému

SIEM (Security Information and Event Management) je management bezpečnostních informací a událostí, který vychází z dlouhodobého ukládání událostí (logů), jejich analýzy, hlášení problémů, monitoringu infrastruktury, korelací událostí a alertování v reálném čase. Obsluhu přehledným způsobem prezentuje informace o zaznamenaných anomáliích a předkládá návrhy na potřebné reakce.

Mezi hlavní funkcionality SIEM patří automatická archivace logů a událostí na zabezpečené platformě, event management, převod logových záznamů do událostí s flexibilním filtrováním, analýza událostí v reálném čase s jejich automatickou klasifikací, korelací, detekcí anomálií a identifikací příčiny problému, dále automatické generování a prioritizace alertů z korelovaných událostí ve vztahu k důležitým systémům a komplexní reporty pokrývající regulačními požadavky jako SOX, PCI, FISMA, GLBA, HIPAA, ISO 27 00X, s možností jejich pravidelného doručování uživatelům SIEM systému.

Naplnění Konceptu aktivní bezpečnosti a spolehlivosti IT infrastruktury

Problematikou monitorování IT systémů a aplikací, dohledovými nástroji a řízením informační bezpečnosti se v České republice zabývá celá řada subjektů. Najdeme zde i specializované výrobce, jejichž technologie umožňují představený Koncept efektivně realizovat. Jedná se o následující produkty, služby a řešení:

- **Analýza stavu bezpečnosti IT (NSMC):** analýza stavu kyberbezpečnosti v dané organizaci vč. ohodnocení aktiv a klíčových procesů a vč. návrhů na zlepšení. Možno doplnit školením kyberbezpečnosti pro zaměstnance i management.
- **Log Management (AXENTA):** nástroj pro sběr, archivaci a vyhledávání nad logy z IT infrastruktury. Logy jsou uchovávány v nezměněné podobě.
- **MoNet (NOVICOM):** nástroj pro pokročilý provozní monitoring IT infrastruktury přes všechny vrstvy s průběžným vyhodnocováním SLA.
- **AddNet (NOVICOM):** nástroj pro adresní plánování a řízení přístupu do sítě s integrovanými síťovými službami DHCP, DNS, Radius.
- **SIEM (Axenta):** nástroj pro vyhodnocení logů a pro alerting událostí v souladu s interními procesy dle požadavků ZoKB.
- **SOC (Axenta):** špičkové dohledové pracoviště s integrovanými nejmodernějšími kyberbezpečnostními technologiemi obsluhované vysoce kvalifikovaným týmem expertů v režimu 24/7/365. Připojené organizaci umožňuje sledovat kybernetickou bezpečnost v reálném čase s možností neprodlené reakce na

kybernetické bezpečnostní incidenty. Toto pracoviště má význam jak v oblasti prevence, tak i analýzy a reakce.

Nespornou výhodou českých výrobců a dodavatelů řešení je mimo ceny i vzájemná provázanost a kompatibilita jednotlivých systémů. Díky vzájemné integraci je tak např. možné indikovat bezpečnostní incident na dashboardu MoNet a příslušné zařízení přímo odpojit pomocí AddNet.

Závěr

Koncept aktivní bezpečnosti a spolehlivosti IT infrastruktury je příkladem, jak zabezpečit ICT v organizaci v souladu se současnými právními normami a s vysokou účinností. Koncept je pouze doporučeným přístupem. Samotnou aplikaci jednotlivých komponentů do konkrétního počítačového systému organizace je nutné řešit vždy individuálně podle požadavků TOP managementu organizace a nároků dané sítě.

Města a regiony budoucnosti

*Karel Skokan, Managing Consultant, Czech Republic, Slovakia and Eastern Europe,
CGI IT Czech Republic s.r.o.*

Snahou představitelů měst je poskytnout obyvatelům i turistům co nejpříjemnější podmínky života ve městě. Ale jiné potřeby má pracující, důchodce, dítě, student nebo rodič na mateřské dovolené. Přesto lze nalézt několik pohledů na život ve městě zajímaví občany:

- Příležitost uspokojit své požadavky na vzdělání, kulturu, zábavu, sportovní vyžití, zdravotní a sociální péči, bydlení, pracovní uplatnění, atd.;
- Komfort, rychlost a bezpečnost pobytu a pohybu po městě;
- Být součástí příjemného prostředí, přátelské komunity, mít příležitost setkávání s ostatními lidmi;
- Obklopovat se hezkými věci (tradice i moderna);
- Nežít v hlučném, prašném nebo jinak zdravotně závadném prostředí.

Není prakticky možné uspokojit výše uvedené požadavky, natož všechny a hned. Zároveň městské rozpočty nejsou bezedné. Proto je nutné k dané problematice přistupovat chytrě, tj. SMART. Důležité je realizovat jen projekty, které splňují následující kritéria:

- S Specific – specifické, konkrétní cíle;
- M Measurable – měřitelné cíle;
- A Achievable/Acceptable – dosažitelné/přijatelné;
- R Realistic/Relevant – realistické/relevantní (vzhledem ke zdrojům);
- T Time Specific/Trackable – časově specifické/sledovatelné.

Ale ani to nestačí. Velmi důležitá je schopnost využívat inovativních technologií pro zvýšení efektivity obsluhy potřeb občanů. Právě tyto technologie umožní zvládnout dosud neřešitelné komplikace, přičemž hybnou silou jsou velmi často informační a komunikační technologie ve spojení s digitalizací provozních technologií. Jedním z příkladů může být průběžné měření aktuální hustoty dopravy v uzlových bodech pomocí senzorových sítí, predikce vývoje dopravy pro nejbližší hodiny na základě historických měření a aktuálních klimatických podmínkách. Tyto informace mohou být podkladem pro přijetí opatření na regulaci dopravy na nejbližší hodiny včetně včasného informování řidičů o plánovaných změnách pro ně co nejpohodlnějším způsobem. Obdobných příkladů existuje mnoho.

Jistě i ve vašem městě či regionu máte řadu podnětů, co lze dělat jinak a lépe. Těmito podněty se chcete zabývat, ale který z nich má větší prioritu? Jak vůbec definovat prioritu? Odpovědi na tento typ otázek nejsou lehké, zejména pokud se hledají poprvé. Naštěstí máme pro místní samosprávu dobrou zprávu. Nabízíme osvědčenou metodiku jak se vypořádat s počátečním chaosem a nastavit systematický přístup jak:

- Společně revidovat vize a cíle města, resp. regionu;
- Nastavit měřítka a prahové hodnoty pro evaluaci projektových záměrů;
- Vyhodnotit přínos konkrétních projektových záměrů pro naplnění vizí města;
- Odhalit závislosti mezi jednotlivými projekty;
- Identifikovat rizika a navrhnout opatření na snížení rizik.

Výstupem konzultačních prací je snadno pochopitelná cestovní mapa realizačních projektů SMART CITY podložená shromážděnými fakty. Tato mapa se tvoří postupně na workshopech s jednotlivými pracovními skupinami, které ve městě, resp. v regionu zodpovídají za SMART CITY. Nesmírně důležitá je právě moderovaná diskuze zástupců jednotlivých skupin a hledání společného konsensu, aby byla zachována sociální, ekonomická a environmentální rovnováha. Diskuzi napomáhá použití interaktivního nástroje, kde

jsou evidovány všechny nápady, rozpracované projekty, projekty určené k realizaci, či projekty právě realizované nebo již dokončené. Všechny zainteresované osoby vidí vzájemné souvislosti mezi projekty, časovou souslednost a v neposlední řadě soulad očekávaných přínosů konkrétních projektů s nadefinovanými SMART CITY vizemi a cíli.

Rok a půl otevřených dat ČSSZ – zkušenosti a poznatky z každodenní praxe

Ing. Jiří Šunka, vedoucí oddělení metodiky a správy dat ČSSZ

1. Úvodem

V loňském roce se ČSSZ na konferenci ISSS zabývala historií a principy otevřených dat a způsobem jejich implementace ve svých podmínkách. Během uplynulého roku se ČSSZ podařilo dopracovat celý proces publikace otevřených dat do téměř finální podoby jak po stránce provozní, tak i po stránce realizační.

Připomeňme si úvodem alespoň základní definici otevřených dat a jejich historii v podmínkách ČSSZ. Definice zní: „*Otevřená data jsou úplná, snadno dostupná, strojově čitelná, používající standardy s volně dostupnou specifikací, zpřístupněná za jasně definovaných podmínek s minimem omezení a dostupná uživateli při vynaložení minima nákladů.*“

Historie v podmínkách ČSSZ

Základním krokem bylo rozhodnutí vedení ČSSZ o zveřejňování otevřených dat na vlastních webových stránkách. Byly přijaty tyto zásady:

- a) data budou publikována v maximální otevřenosti,
- b) bude vytvořeno vlastní řešení pro publikaci dat,
- c) kromě samotných dat bude ČSSZ zveřejňovat i jejich vizualizace ve formě interaktivních grafů pro snazší interpretaci.

ČSSZ svůj portál otevřených dat zveřejnila spolu s prvními datovými sadami 2. listopadu 2015 a najdete jej na adrese <https://data.cssz.cz>. Další publikace nových datových sad proběhly v dubnu, listopadu a prosinci následujícího roku. Současně od poloviny roku 2016 probíhají pravidelné aktualizace zveřejněných datových sad podle publikačního plánu a stanovené periodicity.

V současné době je **publikováno** celkem **63 datových sad** z různých oblastí – důchodového a nemocenského pojištění, lékařské posudkové služby, osob samostatně výdělečně činných (OSVČ), správního řízení, statistických ročenek, personalistiky a dalších.

ČSSZ nezůstala pouze u publikace samotných dat, ale připravila také interaktivní vizualizace vybraných datových sad v podobě grafů (sloupcových, spojnicových, koláčových) nebo mapových vizualizací na úrovni států, krajů a okresů. U většiny vizualizací lze interaktivně měnit parametry výběru dat pro zvolený graf (například rok, druh důchodu, pohlaví apod.) a získané výstupy uložit formou tabulky ve formátu CSV pro další zpracování nebo jako obrázek grafu ve formátu PNG nebo PDF, včetně uložení informace o nastavených výběrových podmínkách. Celkem je nyní **publikováno 75 vizualizací**.

2. Portál Otevřená data ČSSZ

Portál *Otevřená data ČSSZ* je přístupný komukoliv na adrese <https://data.cssz.cz>. Na úvodní stránce se nachází základní informace o možnostech portálu, podmínkách užití a jeho registraci v Národním katalogu otevřených dat. V pravé části je umístěn panel novinek, který obsahuje průběžné časově seřazené informace o provedených publikacích nových datových sad, jejich aktualizacích a úpravách portálu. V dolní části jsou odkazy na Nejčastější dotazy, Prohlášení o přístupnosti, Technickou pomoc a webové stránky provozovatele portálu ČSSZ.

Nejdůležitější záložkou v menu portálu je Katalog otevřených dat. Po jeho výběru se zobrazí formulář, který v horní části obsahuje seznam klíčových slov, podle nichž se dají v seznamu vyhledávat datové sady. U každého klíčového slova je uveden počet datových sad, ke kterým je přiřazeno. Zcela vpravo nahoře je

umístěno pole pro fulltextové vyhledávání, které umožní vybrat záznamy, obsahující uvedený text v názvu nebo popisu datové sady. Hlavní část (dvousloupcová tabulka) obsahuje v prvním sloupci abecedně seřazený seznam datových sad a ve druhém seznam vizualizací příslušné datové sady s ikonou informující o typu vizualizace (spojnicový, sloupcový nebo koláčový graf, mapa, tabulka).

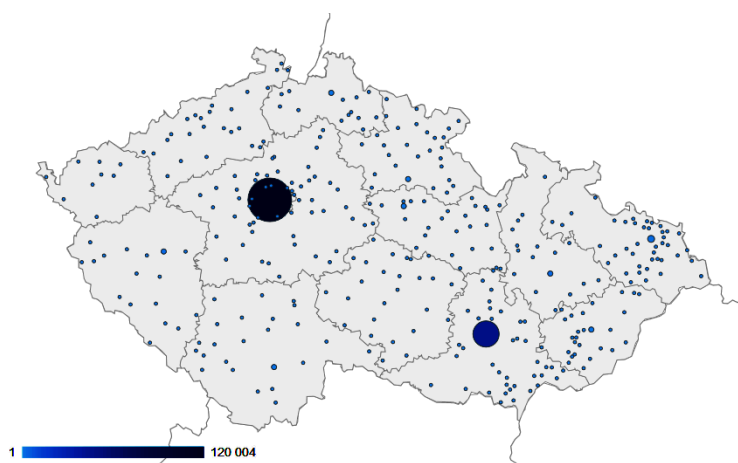
Kliknutím na požadovanou datovou sadu se zobrazí stránka s jejím katalogizačním záznamem, který v první části obsahuje její název, popis, periodicitu aktualizace, související geografické území (tj. zda jsou data kumulována na úrovni státu, kraje nebo okresu), mezinárodní klasifikaci oblasti dat podle EuroVoc, odkaz na dokumentaci vybrané datové sady a dotčené časové období (tj. časový interval publikovaných dat). Druhá část – Datové zdroje – v jednotlivých řádcích uvádí odkazy na soubory, které obsahují publikovaná data ke stažení v uvedeném formátu (typicky RDF/Trig a CSV). Kromě toho obsahuje každý řádek i odkaz na technický popis struktury dat (typicky RDF/Trig a JSON). V poslední části stránky je uveden seznam vizualizací.

Interaktivní vizualizace umožňuje ve většině případů volbu výběrových podmínek pro prezentaci dat. Po nastavení požadovaného filtru (výběrem z hodnot v rozbalovacím seznamu) se po stisknutí tlačítka Zobrazit graf vykreslí data pro zadanou podmínku. Pomocí tlačítka Zobrazit tabulku se zobrazí zdrojová data grafu odpovídající výběrové podmínce. Poslední tlačítko Export umožňuje exportovat vybraná data ve formátu CSV nebo uložit aktuálně zobrazený graf ve formátu PNG nebo PDF, včetně uložené informace o nastavených výběrových podmínkách.

3. Získané zkušenosti a poznatky

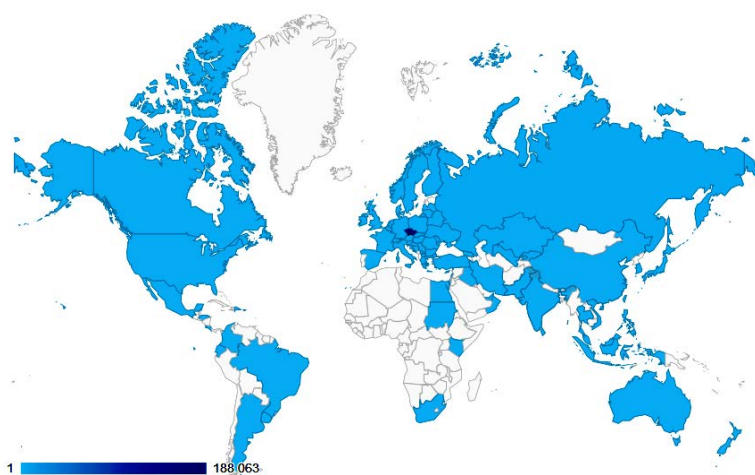
Zkušenosti a poznatky získané z více než ročního provozování portálu *Otevřených dat ČSSZ* lze shrnout do následujících bodů:

- a) Poskytovaná data ČSSZ mají specifický charakter vyplývající ze základních činností, které ČSSZ zajišťuje. Určitě jsou přitažlivá pro uživatele z řad členů akademické obce, výzkumníků v sociální a demografické oblasti, statistiků, datových analytiků, novinářů apod.
- b) Podle měření přístupů na stránky portálu můžeme konstatovat, že i přes specifickou dat se průměrný počet přístupů pohybuje v rozmezí 2 500 až 3 000 měsíčně, a to z celé České republiky (viz Obrázek 1).



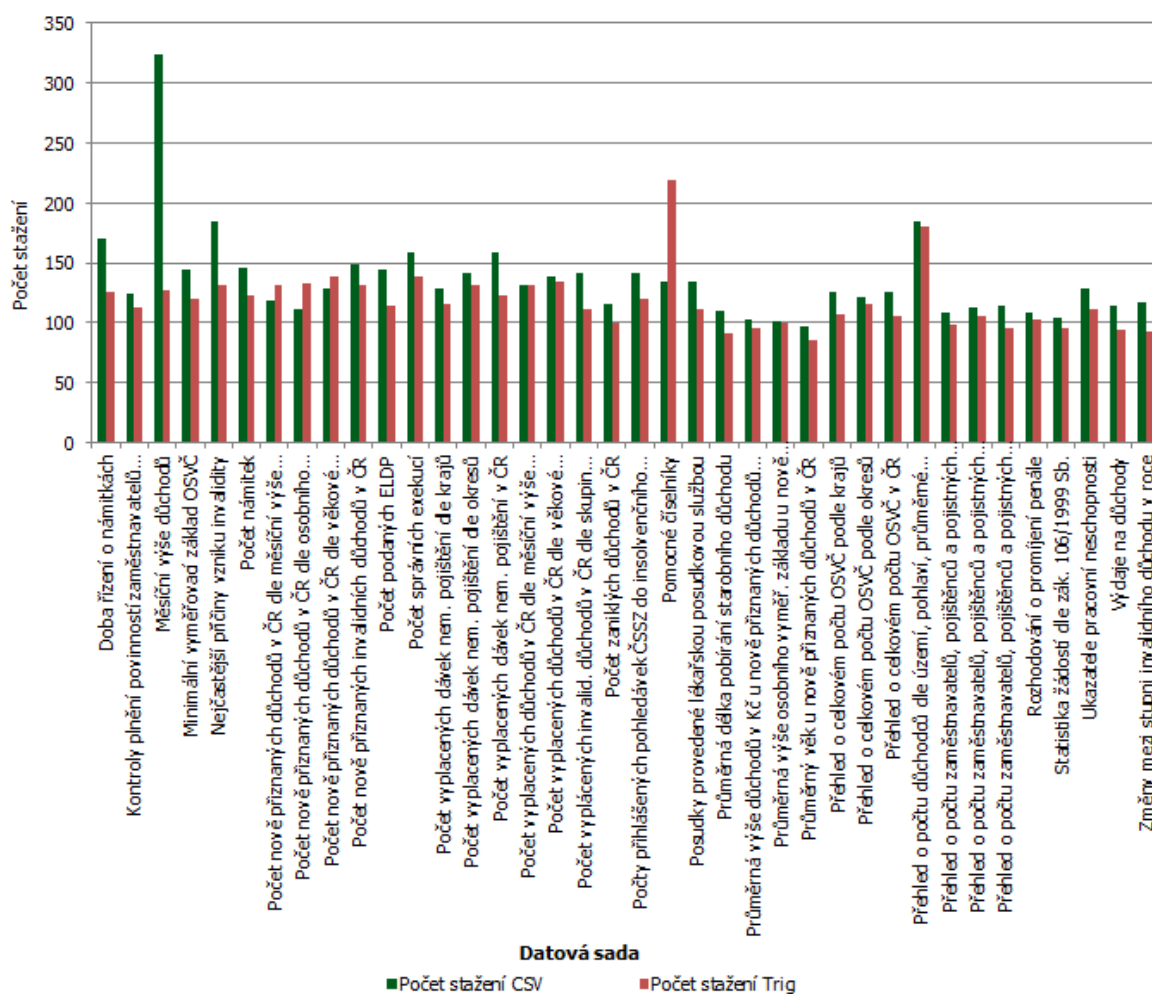
Obrázek 1: Přístupy na portál z ČR

- c) Pro zajímavost lze uvést, že v jednotkách až desítkách eviduje ČSSZ přístupy z celého světa (viz Obrázek 2).



Obrázek 2 Přístupy na portál celosvětově

- d) Uživatelé rovněž projevují zájem o samotné datové soubory, které jsou stahovány z portálu v počtu cca 200 až 300 zaznamenaných aktivit stažení měsíčně. Zajímavostí je, že poměrně vyrovnaný je zájem jak o data ve formátu RDF (usnadňuje propojování dat z různých zdrojů), tak i o data ve formátu CSV (viz Obrázek 3).



Obrázek 3: Statistika stahování CSV × Trig za rok 2016

- e) V každodenní praxi se ukázala nezbytná potřeba vypracování a naprogramování důkladné evidence, která výraznou měrou zjednodušuje proces publikace otevřených dat, jeho vyhodnocování a poskytuje statistické přehledy o publikovaných datech. Reagovali jsme na ni vytvořením evidenční pomůcky v MS Access, která umožňuje zpracovat veškerá metadata o datové sadě, evidovat jednotlivá měření a metriky, poskytnout informace o publikovaných vizualizacích včetně jejich filtrů. Velmi ceněnou se stala podpora v procesu aktualizace datových sad, kdy tento nástroj umožňuje sledovat plánované aktualizace, generovat e-maily vlastníkům/zpracovatelům dat se žádostí o aktualizace. Poskytuje rovněž detailní přehled o stavu zpracování. Nezanedbatelnou součástí je i poskytování statistik za zvolené období (počet nových publikací a vizualizací, počet aktualizací a přehled o aktuálním stavu portálu Otevřených dat ČSSZ). Samozřejmostí je generování reportů podle široce nastavitelných výběrových podmínek.
- f) Zaznamenali jsme několik doplňujících dotazů a požadavků na publikovaná data. Jejich počet je výrazně nižší, než bychom předpokládali, což může svědčit o dostatečné srozumitelnosti publikovaných dat nebo o určité omezené atraktivnosti těchto dat pro běžného uživatele. Proto, abychom od uživatelů získali zpětnou vazbu o využití našich dat, jsme na portál umístili výzvu ke spolupráci a poskytování zpětné vazby z využití otevřených dat ČSSZ.
- g) Informace o otevřených datech ČSSZ sdílíme s veřejností rovněž prostřednictvím sociálních sítí, zejména Twitter, kde zaznamenáváme příznivé reakce.

4. Využití otevřených dat ČSSZ

Nejjednodušší formou použití otevřených dat ČSSZ je přímý přístup na portál. Od svého spuštění do konce března 2017 zaznamenal již kolem 30 tisíc návštěv.

Technicky náročnější je práce s propojenými daty ve formátu RDF. V obecné rovině použitý formát RDF usnadňuje propojování dat z různých zdrojů, a tím i analýzu možných souvislostí mezi jevy, které tato data popisují. Jako příklad lze uvést možnost propojení dat o počtu a struktuře důchodců v jednotlivých okresech a letech, které zveřejňuje ČSSZ, s daty o počtu obyvatel a jejich věkové struktuře v okresech, které zveřejňuje Český statistický úřad. Výsledkem takového propojení je možnost výpočtu ukazatelů typu počet důchodců na počet obyvatel v okrese, počet invalidních důchodců ve věkových pásmech na počet obyvatel apod., které lze použít pro demografické studie nebo pro rozhodování o aktivitách orgánů veřejné moci v sociální oblasti. Protože jsou data zveřejněna v časových řadách, lze zpracovávat prognózy a odhady dalšího vývoje, které mohou být jedním z podkladů pro řízení či strategické cíle. Z principu otevřenosti publikovaných dat (a to nejen dat ČSSZ, ale i jiných institucí a orgánů státní správy) vyplývá, že zajisté lze najít další nepřehledné množství nápadů a námětů, jak a s kterými daty propojení realizovat, a jak takto získané informace využít.

5. Budoucnost

Otevřená data jsou vnímána jako jeden z nástrojů podporujících myšlenku tzv. otevřeného vládnutí. Otevřené vládnutí představuje snahu o posílení transparentnosti, demokracie a spolupráce mezi politiky, veřejnou správou, zástupci podnikatelské sféry a občany. Otevřené vládnutí je i jedním z témat strategie Digitální agenda pro Evropu. Aby se občané a další subjekty mohli efektivně podílet na politické diskusi, potřebují relevantní data a informace. Zvyšování dostupnosti otevřených dat tak otevírá cestu k informacím a pomáhá naplnit tento předpoklad pro vyšší zapojení občanů a dalších subjektů do politické a celospolečenské diskuse.

ČSSZ nezůstane pouze u dat zveřejněných v uplynulém období, ale již nyní pracuje na přípravě aktualizace publikačního plánu, který bude zahrnovat nejen nové datové sady, ale i další rozšiřování počtu vizualizací již zveřejněných otevřených datových sad, aby usnadnila přístup široké veřejnosti k těmto datům. Samozřejmostí zůstává zajištění průběžné aktualizace již publikovaných datových sad v příštím období.

6. Závěrem

Mnohá data ve veřejné správě a samosprávě jsou většinou výsledkem činnosti hrazené z veřejných prostředků, a proto by měla být rovněž veřejně k dispozici. Publikace otevřených dat plně respektuje a podporuje tuto myšlenku. Tlak veřejnosti (laické i odborné) by měl směřovat k tomu, aby bylo tímto způsobem publikováno maximum dat a informací ze všech oblastí života (při současném zajištění všech zákonných požadavků na ochranu dat), která jsou využitelná jak pro účinnou kontrolu správní moci, tak i pro vytváření nových aplikací a řešení zjednodušujících každodenní život. Snažme se všichni o to, abychom mohli v oblasti otevřených dat co nejdříve každému jenom doporučit: **„Nežádejte o data, vezměte si je!“**

Jak dosáhnout transparentnosti obce

Mgr. Dana Ullwerová, Obec Vrané nad Vltavou; Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Transparentnost veřejné správy je dlouhodobý cíl, kterého lze dosahovat snad jen postupnými kroky. Praktické příklady těchto kroků z prostředí obcí budou představeny v tomto příspěvku, a to na konkrétním příkladu obce Vrané nad Vltavou.

Obec Vrané nad Vltavou

Obec Vrané nad Vltavou se nachází ve Středočeském kraji v těsném sousedství jihozápadního okraje hlavního města Prahy. Obec leží na pravém břehu řeky Vltavy a skládá se ze dvou historických osad, Skochovice a Vraného. Je zde přibližně 650 domů a 2488 trvale bydlících obyvatel. Obec je aktivně využívána i k rekreaci, což dokladuje i množství chat, který je zde 568. Další informace o obci lze najít na webových stránkách [1].

Z hlediska výkonu přenesené působnosti státní správy se jedná o obec prvního typu, která ale navíc vykonává působnost na úseku matrik. Obecní úřad tvoří starostka, místostarosta a tři úřednice. Obec má patnáctičlenné zastupitelstvo. Zřízeny jsou následující komise a výbory: kontrolní výbor, finanční výbor, komise životního prostředí, komise sociální a pro občanské záležitosti, komise kultury, komise rozvoje obce a plánování, komise pro projednávání přestupků a povodňová komise.



Obr. 1: Pozdrav z obce Vrané nad Vltavou – zdroj [1].

Rozklikávací rozpočet

Každá obec má podle zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů, povinnost zveřejnit návrh rozpočtu, a to nejméně po dobu 15 dnů přede dnem jeho projednání v zastupitelstvu. Dále obec zveřejňuje tzv. závěrečný účet, tedy přehled o hospodaření za uplynulý rok. Kromě těchto jasně daných povinností, může obec přistoupit ještě k dalšímu zveřejňování svého hospodaření, a to průběžně během roku, čímž významně přispěje ke zvýšení své transparentnosti a otevřenosti. Velmi elegantním řešením je služba Rozklikávací rozpočet, kterou nabízí společnost Triada jako nadstavbu nejen vlastního účetnictví.

Jde o sdílenou službu portálu iMunis.cz, jehož kompletní aktuální nabídka služeb je ilustrována na Obr. 2. Služby tohoto portálu jsou koncipovány tak, že zachovávají maximální bezpečnost ukládaných dat vzhledem k jednotlivým uživatelům. Portál je provozován v režimu 7x24. Velmi podstatný je také fakt, že vlastní datové centrum leží v České republice a jeho provoz tedy plně podléhá českému právnímu řádu. Uživatelé se tak v žádném případě nemusí bát o svá data, jejichž zabezpečení je na velmi vysoké úrovni, což je velmi podstatné s blížící se účinností Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

The screenshot shows the iMunis.cz website interface. At the top, there is a navigation bar with links: Triada | Munis | iMunis | ISSS | DMO | Obec a finance | DVS | Solón. Below this is the iMunis logo and the text 'Centrum sdílených služeb'. A row of service icons includes: Úřední deska, SMIS, Evidence oznámení, Webináře, HelpDesk, and Rozklikávací rozpočet. The main content area is divided into three columns: 'Hlavní nabídka' with links like 'O iMunis', 'Přihlásit', and 'Kontakt'; 'iMunis – Úvod' with a detailed description of the portal and a list of services including 'Úřední deska', 'SMIS', 'Evidence oznámení', 'Webináře', 'HelpDesk Munis', and 'Rozklikávací rozpočet'; and 'ISSS' with news items like 'ISSS 2017 – premiér Sobotka' and 'IS Munis'. The footer contains the Triada logo, contact information, and copyright notice: © 2017 Triada, spol. s r. o., Praha, webmaster@imunis.cz.

Obr. 2: Nabídka sdílených služeb portálu iMunis.cz – zdroj [2].

Služba Rozklikávací rozpočet funguje na principu datového skladu, do kterého jsou nahrávány měsíční výstupy z účetnictví obce. Vzhledem ke zvolenému obecnému formátu pro přenášená data jej lze napojit na účetnictví více dodavatelů, nejen na vlastní modul Účetnictví, jenž je součástí informačního systému Munis vytvářeného a dodávaného společností Triada. Jednoduchý přenos dat nezatěžuje významně vlastní zpracování na straně účetní obce a díky datovému skladu není náročný ani na infrastrukturu obce, což je samozřejmě obecnou vlastností sdílených služeb.

3 Služby pro obyvatelstvo

Rozpočtové informace

	Rozpočet	z celého rozpočtu	Skutečnost	z celého plnění/čerpaní	plnění čerpání
Příjmy	2 315 834 Kč	5,5 %	509 428 Kč	12,4 %	22,0 %
Výdaje	13 584 000 Kč	30,6 %	2 208 089 Kč	58,8 %	16,3 %

Další členění		Vývoj po měsících		Meziroční vývoj	
Oddíl	dle druhu	Tabulka	Graf	Tabulka	Graf
		Příjmy		Výdaje	
Kód	Název	rozpočet	skutečnost	rozpočet	skutečnost
31	Vzdělávání a školské služby	6 000	0	4 487 000	629 774
32	Vzdělávání a školské služby	0	0	20 000	20 000
33	Kultura, církev a sdělovací prostředky	16 000	3 934	562 000	65 288
34	Tělovýchova a zájmová činnost	15 000	15 000	1 020 000	409 352
35	Zdravotnictví	360 834	66 148	184 000	33 518
36	Bydlení, komunální služby a územní rozvoj	1 361 000	251 911	4 403 000	512 221
37	Ochrana životního prostředí	557 000	172 435	2 908 000	537 936

ROZKLÍKÁVACÍ ROZPOČET

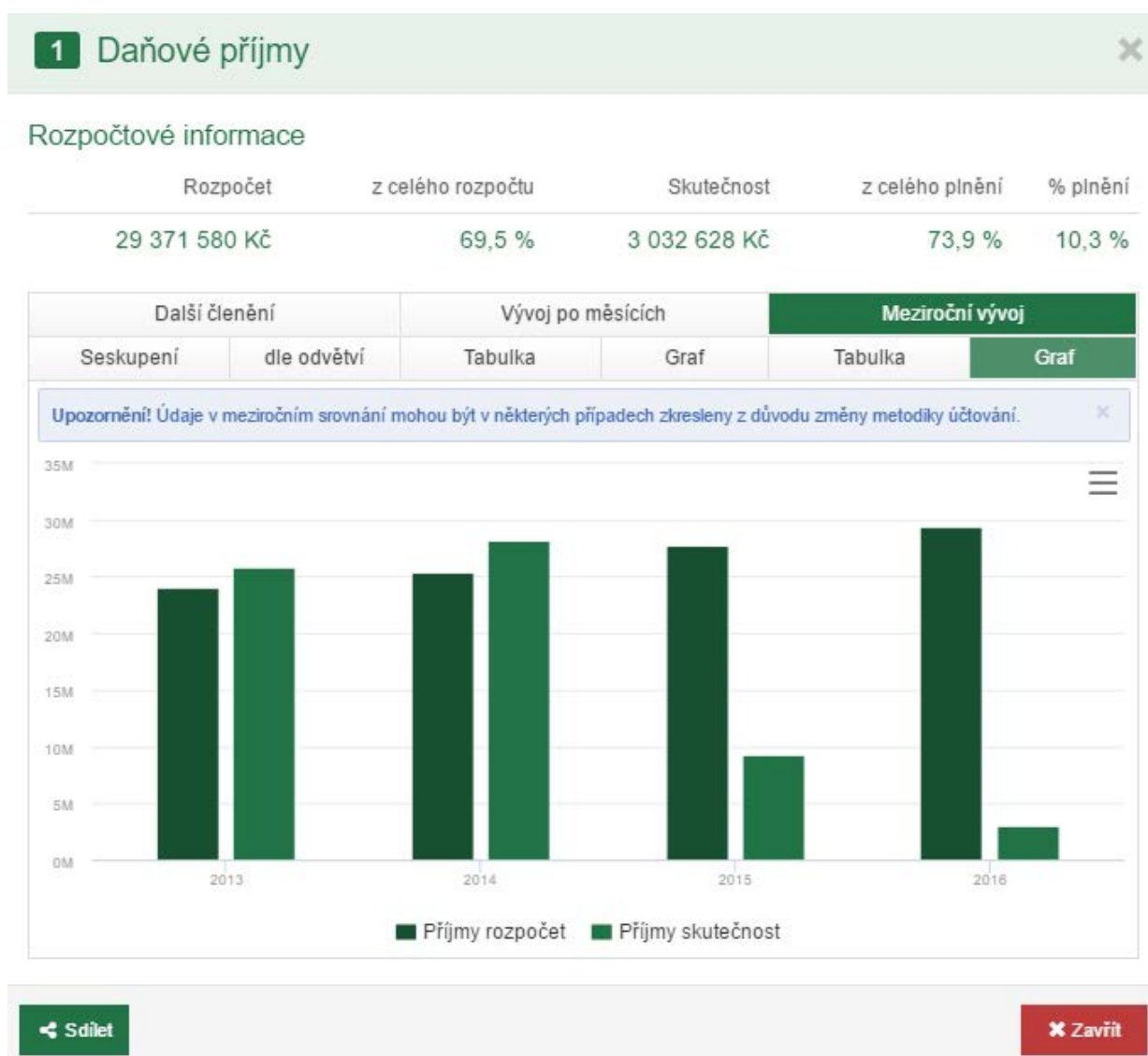
Odvětvový rozpočet	Příjmy		Výdaje			
	členění dle odvětví	členění dle druhu	členění dle odvětví	členění dle druhu		
Skupina / Oddíl / Pododdíl / Paragraf	Příjmy rozpočet	Příjmy skutečnost	Výdaje rozpočet	Výdaje skutečnost		
- Rozklikávací rozpočet	42 269 214	4 102 803	9,7 %	44 444 700	3 757 206	8,5 %
+ 000000 Pro příjmy (technický záznam)	35 917 780	3 190 328	8,9 %	0	0	
+ 2 Průmyslová a ostatní odvětví hospodářství	3 067 000	286 798	9,4 %	23 694 700	750 043	3,2 %
+ 3 Služby pro obyvatelstvo	2 315 834	509 428	22,0 %	13 584 000	2 208 089	16,3 %
+ 4 Sociální věci a politika zaměstnanosti	0	0		10 000	0	0,0 %
+ 5 Bezpečnost státu a právní ochrana	0	0		180 000	56 896	31,6 %
+ 8 Všeobecná veřejná správa a služby	968 600	116 250	12,0 %	6 976 000	742 178	10,6 %

Obr. 3: Příklad odvětvového rozpočtu obce včetně „rozkliknutého“ náhledu na detail části „Služby pro obyvatelstvo“ – zdroj [4].

Při realizaci Rozklikávacího rozpočtu se tvůrci soustředili zejména na jednoduchost, srozumitelnost, přehlednost a úplnost výsledného produktu. Jedině s těmito vlastnostmi může být skutečným přínosem ke zvýšení transparentnosti hospodaření obce. Srozumitelnost je v rámci iMunis Rozklikávacího rozpočtu zajištěna

zejména prostřednictvím tzv. Odvětvového náhledu na čerpání a plnění rozpočtu (příklad je zobrazen na Obr. 3). Ten je členěný dle oblastí s přehledným zobrazením příjmů a výdajů na jednom místě. Samozřejmě, že rozpočet lze zobrazit též v zákonem daném členění dle rozpočtové skladby, která obsahuje položky (druhové členění) a paragrafy (odvětvové členění). Aby i pro tyto pohledy byla zajištěna srozumitelnost pro občany, jsou všechny pohledy i části druhového a odvětvového členění komentovány, aby občané lépe rozuměli jejich významu.

Kromě čerpání a plnění rozpočtu dokáže vytvářet Rozklikávací rozpočet také meziroční srovnání, a to jak v tabulkové, tak v grafické podobě. Ukázka meziročního srovnání daňových příjmů je na Obr. 4. Míra otevřenosti obce po nasazení tohoto produktu tedy významně roste, přičemž díky tomu, že se jedná o sdílenou službu, jsou náklady na vlastní realizaci minimální. Přidaná hodnota takového postupu je tedy vysoká. Samozřejmě že nejdůležitější je následná zpětná vazba od občanů, kteří takovou míru otevřenosti oceňují. Každý může detailně vidět, kolik má obec od státu peněz, kolik vybere na daních a poplatcích, kam obec investuje a co všechno platí, a to přímým proklikem z webových stránek obce.



Obr. 4: Meziroční srovnání pro daňové příjmy obce Vrané nad Vltavou – zdroj [4].

Úřední deska

Přestože je zveřejnění obsahu úřední desky způsobem umožňujícím dálkový přístup povinnost podle § 26 správního řádu, lze i v této oblasti diskutovat o různé míře transparentnosti plynoucí ze zvoleného způsobu realizace. Kladně lze v této souvislosti posuzovat různé možnosti vyhledávání včetně plno-textového, možnost zobrazení stavu úřední desky k určitému historickému datu, popř. implementaci RSS. Všechny tyto atributy splňuje prezentace úřední desky nabízená portálem iMunis.cz v rámci sdílených služeb. Ukázka ilustrující historický pohled na úřední desku obce Vrané nad Vltavou tak, jak vypadala na Vánoce 2016, je na Obr. 5.

Historický pohled k okamžiku 24. 12. 2016 18:00:00

Obec Vrané nad Vltavou

Úřední deska – Historický pohled k okamžiku 24. 12. 2016 18:00:00

Aktuální úřední deska, Vyhledávání, Stav k datu, Domácí stránka

Datum (+čas) 24.12.2016 18:00 Nastavit

Nalezeno 12 záznamů.

Název	Značka	Typ	Přivodce	Zveřejněno od:	Zveřejnit do	Rozh. dat. od	Dokumenty
Oznámení o uložení písemnosti - Josef Zamrazil	2357/2016	uložení písemnosti	MěÚ Jilové	23.12.2016	9.1.2017	23.12.2016	dokument PDF (100 kB) ↓
Plán financování obnovy kanalizací v obci Vrané nad Vltavou	2016	Informace	Obecní úřad	7.12.2016	7.1.2017	7.12.2016	dokument PDF (0.7 MB) ↓
Plán financování obnovy vodovodů v obci Vrané nad Vltavou	2016	Informace	Obecní úřad	7.12.2016	7.1.2017	7.12.2016	dokument PDF (78 kB) ↓
Výzva k podání nabídek ve výběrovém řízení "Nájem nebytových prostor v č. p. 148"	2016	Výběrové řízení	Obecní úřad	7.12.2016	5.1.2017	7.12.2016	dokument PDF (269 kB) ↓
Vyměření místního poplatku - hromadný předpisný seznam zpřístupněn k nahlédnutí	2123/2016	Veřejná vyhláška	Magistrát města Kladna	29.11.2016	30.12.2016	29.11.2016	dokument PDF (65 kB) ↓
Agenda nedostatečně určitě zapsaných osob v katastru nemovitosti	1934/2016	oznámení	Úřad pro zastupování	29.11.2016	29.12.2016	29.11.2016	2 dokumenty
doručení písemnosti Josef Brož	1050/2009	Veřejná vyhláška	MěÚ Benešov	20.7.2009		20.7.2009	obrázek JPG (201 kB) ↓
Rozhodnutí Havlíčkovi pokračování	800/08/SÚ/GRo	rozhodnutí	MěÚ Jilové	14.7.2008		14.7.2008	3 dokumenty
Rozhodnutí Havlíčkovi stav povolení	800/08/SÚ/GRo	rozhodnutí	MěÚ Jilové	14.7.2008		14.7.2008	obrázek JPG (193 kB) ↓
záměr odprodat 219/1	219/1	Prodej	Obecní úřad	11.7.2008		11.7.2008	obrázek JPG (84 kB) ↓
Záměr odprodat pozemek 219/48	219/48	Prodej	Obecní úřad	11.7.2008		11.7.2008	obrázek JPG (86 kB) ↓
Ozn o uložení pís Bernat	0891/2008	oznámení	Celní úřad	4.7.2008		4.7.2008	

Poznámka: Při zadání data včetně časového údaje je zobrazen historický pohled na úřední desku tak, jak se zobrazovala v zadaný okamžik. Pokud je zadáno pouze datum, jsou zobrazeny všechny záznamy, které se na úřední desce objevily v době od 0 do 24 hod. Pokud bylo v zadaný den nějaké vyřízení opravováno, zobrazí se více jeho verzí.

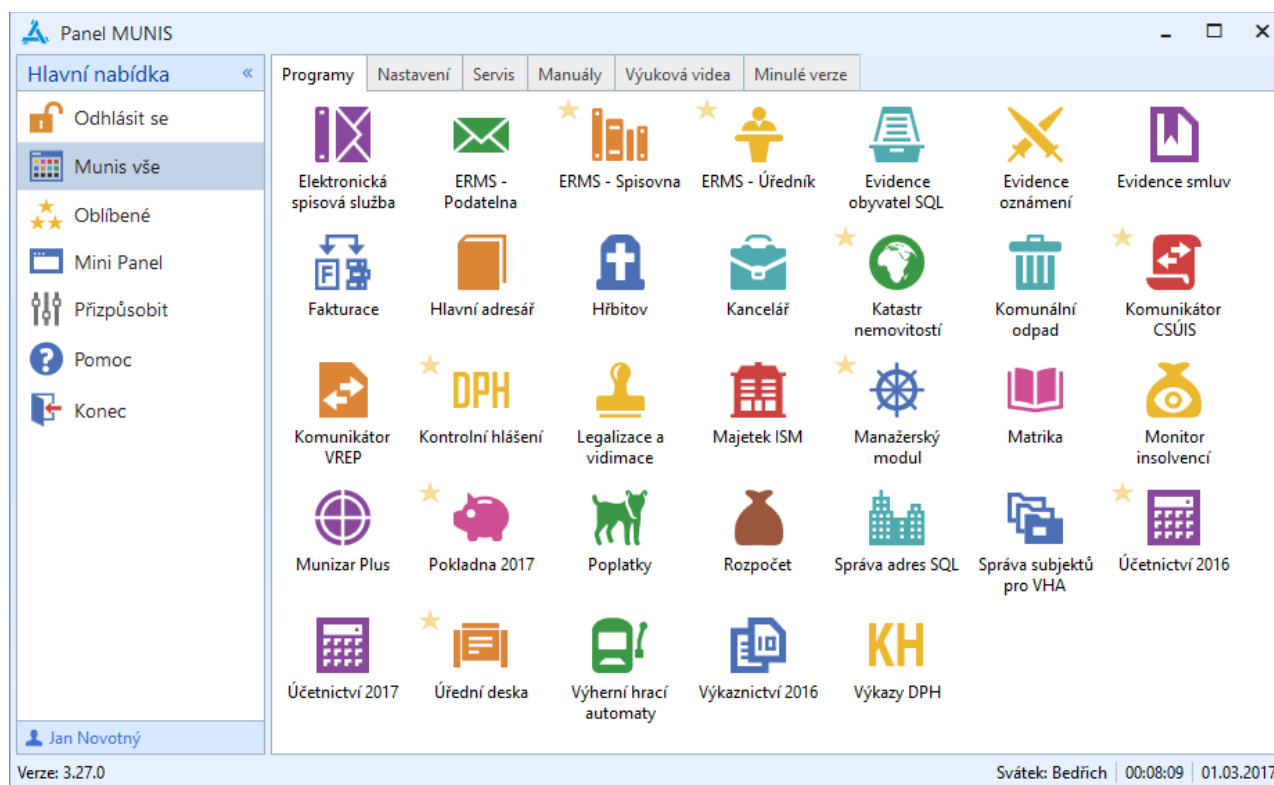
Upozornění: Zveřejněna jsou pouze vyvěšení od 1. 1. 2008, tj. od účinnosti zákona č. 500/2004 Sb. (správní řád). [Prohlášení o přístupnosti](#)

Munis eDeska © 2008 Triada, spol. s r. o.

Obr. 5: Ilustrace historického zobrazení úřední desky k 24. 12. 2016 – zdroj [3].

Dokladování určitého stavu úřední desky k danému datu může být velmi podstatné při řešení sporů, zda byl či nebyl daný dokument řádně vyvěšen. Navíc zpětná přístupnost je také vhodným přínosem k vyšší transparentnosti obce. Jak dokladuje Obr. 3, jsou zveřejněné dokumenty ve výstupních formátech dle vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby. To, spolu s faktem, že webové stránky úřední desky jsou vytvořeny s ohledem na přístupnost a bezbariérovost tak, aby splňovaly všechny důležité zásady přístupnosti podle metodického pokynu k vyhlášce č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti), je dalším pozitivem zvyšujícím hodnotu právě této zvolené cesty k prezentování obsahu úřední desky způsobem umožňujícím dálkový přístup prostřednictvím sdílené služby portálu iMunis.cz.

Všechny podklady pro zveřejňování na úřední desce lze jednoduše připravit v modulech informačního systému Munis (nabídka modulů komplexní IS Munis je na Obr. 6) a následně integrovaným nástrojem převést do výstupního datového formátu PDF/A a kromě publikování na elektronické úřední desce také vytisknout, aby byly synchronizovány informace na klasické úřední desce i na internetu. Stejně postupy pro obě formy úřední desky zjednodušují práci a minimalizují riziko vzniku chyb.



Obr. 6: Nabídka modulů IS Munis.

Evidence smluv

Poslední dobou často diskutovaným tématem je též zveřejňování smluv. Ačkoliv obce, které nevykonávají rozšířenou působnost, jsou vyňaty z povinností daných zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), mnoho z nich přistupuje k dobrovolnému zveřejňování. Základem k tomu je však vnitřní proces uspořádání smluv, který lze nejlépe realizovat samozřejmě pomocí příslušného softwarového nástroje. Jedním z těchto výkonných je modul Evidence smluv informačního systému Munis. Právě tento modul si obec Vrané nad Vltavou pořídila jako další rozšíření již dlouhá léta provozovaného IS Munis, který svými moduly pokrývá všechny potřeby obce v oblastech vykonávaných agend, včetně matričního úřadu (kompletní nabídka modulů – viz Obr. 6).

Základem modulu Evidence smluv je číselník typů smluv, který je nadstavbou pro jednotlivé kategorie smluv a zároveň slouží jako zdroj šablon zjednodušující následné zadávání. Při běžné práci zaevidování konkrétní smlouvy jsou díky těmto šablonám nejen předvyplňovány opakující se údaje včetně dynamických vazeb určujících prostřednictvím pracovních pozic jednotlivé vztahy konkrétních osob ke smlouvě, ale jsou též určena základní pravidla vyplňovaných údajů, např. způsoby plnění. Kromě popisných údajů lze k zaevidované smlouvě doplnit také její elektronickou podobu, a to celkem ve třech variantách:

- textová podoba plného textu určená pro indexování plnotextového vyhledávání a uložení celého textu smlouvy,
- anonymizovaná textová podoba určená pro zveřejňování,
- skenovaná podoba včetně případných vlastnoručních podpisů a dalších atributů (např. razítek).

Popisná data o smlouvě

Číslo smlouvy JID Ext. číslo smlouvy Zvláštní číslo Anonymizovat předmět smlouvy

MES17000001313 Předmět smlouvy Energie

Datum podpisu 31.12.2016

Schválil 10 ... Jakub Novák

Zveřejnění ceny Zveřejnit celk. částku jako cenu s DPH Měna CZK

Celk. částka bez DPH 0,00 Celk. částka vč. DPH 1500000,00

Subjekt	Platící	Datová schr...	Název	Adresa	Název souboru	Anon...
Publikující smluvní strana	Ne		První energetická	Éčková 1, 11000 Pra	8695237-16109-10060116...	Ne
Smluvní strana	Ano	Su6agt5	Město Spisovkářov	Podaciho deniku 28		

Uložit Neukládat

Triada | Vedení úřadu | Asistent starosty (Zastupce) | Jakub Novák » Aplikace spuštěna | 3.27.0.0

Obr. 7: Inicializace zveřejňovacího procesu v modulu Evidence smluv IS Munis.

Zveřejňování smluv je možné buď v Registru smluv, nebo prostřednictvím sdílených služeb portálu iMunis.cz. V případě první možnosti lze využít přímé vazby s elektronickou spisovou službou Munis ERMS, díky níž je odeslání dat do Registru smluv velmi jednoduché, stejně jako následný příjem potvrzení o vyvěšení. V případě druhé možnosti je vazba realizována přes úřední desku, o níž už bylo v tomto příspěvku pojednáno.

Zveřejňování smluv je jistě dalším dobrým přínosem ke zvýšení transparentnosti obce, avšak už to, že si obec udělá pořádek ve svých smlouvách, je velmi pozitivní a samozřejmě je to nutný předpoklad dalšího rozvoje.

Shrnutí

Říká se, že nástroje e-Governmentu mají potenciál zvyšovat transparentnost veřejné správy. Uvedený potenciál mohou využít města a obce, jak bylo ukázáno v tomto příspěvku na příkladu dobré praxe obce Vrané nad Vltavou.

Jako starostka obce chci ještě zdůraznit, že využíváním sdílených služeb portálu iMunis.cz – Úřední deska a Rozklikávací rozpočet šetříme významně náklady na zajištění těchto služeb. A dále nově nasazením modulu Evidence smluv se ještě dále dostáváme do oblasti zveřejňování, která není vynucena zákonem, ale je významným přínosem k posílení transparentnosti obce.

Literatura

- [1] Oficiální webové stránky obce Vrané nad Vltavou dostupné na adrese <http://www.vranenadvltavou.cz>.
- [2] Portál iMunis.cz dostupný na adrese <http://www.imunis.cz>
- [3] Úřední deska obce Vrané nad Vltavou dostupná na adrese <http://vranenadvltavou.imunis.cz/edeska/>
- [4] Rozklikávací rozpočet obce Vrané nad Vltavou dostupné na adrese <http://vranenadvltavou.imunis.cz/rr/>

Elektronizace procesů a digitalizace dat úřadu

Miroslav Wolf, obchodní ředitel Praha, GORDIC spol s r. o.

Moderní trend, který se snaží efektivně využívat dostupné moderní technologie s hlavním cílem optimalizace interních procesů, integraci informačních systémů a důrazem na maximální správnost a dostupnost digitálních dat. Správně nastavené elektronicky řízené interní procesy úřadu zajistí nejen časovou úsporu úředníkům, ale i lépe fungující úřad. Jako příklad je možné uvést finanční kontrolu, která je vyžadována platnou legislativou ČR. V případě, že je realizována prostřednictvím elektronizovaných procesů a využitím digitálních dat dodavatelských faktur a všech souvisejících digitálních dokumentů, zajistí úřadu přehledný schvalovací proces, který je možné kontrolovat s ohledem na nastavená interní pravidla, legislativní správnost a dodržování závazků úřadu.

Na podobném principu, je možné zavést jakékoliv schvalování úřadu, které je prováděné na základě legislativního požadavku nebo interní směrnice (cestovní příkazy, hotovostní zálohy, rozpočtové úpravy, apod.). Pro využití plného potenciálu elektronizace procesů je nutné neopomenout ani oblast integrace informačních systémů, které jsou na úřadu provozovány.

Jestliže hovoříme o elektronizaci úřadu a digitalizaci dat, nemůžeme opomenout elektronické formuláře, které mohou automaticky vytěžovat data informační systémy. Elektronické formuláře jsou používány pro interní procesy úřadu, ale i jako nástroj efektivní komunikace občana s úřadem. V oblasti komunikace občana s úřadem, jsou nejčastěji řešeny vybrané životní situace.

Nedílnou součástí je i oblast manažerských pohledů, kterou je zajištěn aktuální přehled vybraných pohledů na ověřená data v informačním systému. Na základě takto zpracovaných výstupů je managementu úřadu umožněno efektivnější rozhodování a aktuální přehled s možností plánování změn za účelem optimalizace chodu úřadu.

Routery Turrís Omnia – do internetu bezpečně

Patrick Zandl, CZ.NIC, z. s. p. o.

Routery jsou pro většinu uživatelů internetu neviditelné krabičky, o jejichž existenci běžný uživatel internetu nic netuší a vlastně ani tušit nemusí. Jsou to ale nakonec ony, kdo se stará o provoz na internetu a na jejich kvalitách závisí, jaká bude uživatelská spokojenost s lokální sítí, internetovým připojením a především, jak bezpečné prostředí vytvoří. A to je ten problém. Hon za nejnižší cenu byl v posledních letech na úkor kvality: levné routery nenabízejí ani potřebnou bezpečnost, ani výkon, který by byl schopen obsloužit sítě i jen menších firem, natož institucí se stovkami účastníků. Stále častěji se setkáváme s tím, že do sítí pronikají nezvaní hosté a útočníci, zatímco samotní uživatelé si stěžují na problémy s připojením. To klade vysoké požadavky na administrátory sítí, kteří se na běžně dostupném hardware snaží odvést co nejlepší práci, nebo musí sahat po drahých řešeních, která kromě ceny kladou i zbytečně vysoké nároky na údržbu a administraci.

Z tohoto dilematu se zrodil projekt Turrís Omnia. Jde o router obstarávající připojení do internetu přes až gigabitovou ethernetovou nebo optickou přípojku a obsluhující libovolný počet uživatelů s možností připojení přes ethernet (5 LAN portů, další přes switch) nebo WiFi (2,4 a 5GHz až 802.11ac).

Turrís Omnia je router zaměřený na bezobslužnost, vysoký výkon a především bezpečnost. To nejsou jen prázdná slova, která se tak rády a snadno objevují na barevných přebalech produktů. Turrís Omnia monitoruje pomocí speciálních technik (adaptivních firewallů a honeypotů, pastí na hackery) pokusy o průnik do vnitřní sítě, vyhodnocuje je a mohou je sdílet s ostatními routery Turrís. Routery se tak na nebezpečí připraví ještě dříve, než hacker zabuší na vaše vrátka. To výrazně zjednodušuje administrativu a bezpečnostní správu routerů.

Bezobslužnost: Zapoj a zapomeň

Turrís Omnia je router vytvořený s předpokladem „zapoj a zapomeň“. Po prvotním nastavení sítě se o všechno podstatné stará router sám. Zaktualizuje se proti bezpečnostním hrozbám, nastaví pravidla firewallu, stáhne si automaticky aktualizace software v momentě, kdy se objeví. To je první výhoda. Je připravený na všechno běžné, co v síti potřebujete.

Otevřenost: open source se vším všudy

Druhou výhodou je jeho otevřenost, protože každá síť je přeci jen trochu jiná. Její administrátoři mají své potřeby a požadavky. Do routeru lze doinstalovat rozšiřující balíčky zpřístupňující další funkce, a protože jde o distribuci populárního open source OpenWRT, lze si i vlastní balíčky snadno vytvářet a na routeru je nasadit. Administrátor se zkušeností s Linuxem si může router přizpůsobit zcela podle svého a provozovat jej například jako server pro sdílení vnitřních dat.

Výkon bez kompromisů

Třetí výhodou je výkon. Turrís Omnia má výkonný dvoujádrový procesor ARM a až 2 GB paměti postačí pro provoz všeho myslitelného software pro místní síť i odbavování provozu do internetu. Připojení navíc můžete zálohovat pomocí LTE modemu (samostatné příslušenství) pro případ výpadku. Router se tak pohybuje svými parametry ve zcela jiné kategorii, než běžně používané routery.

Turrís Omnia je ideálním řešením dilematu, jak zabezpečit vlastní síť, nabídnout v ní dobrý výkon a zároveň pomoci chránit i ostatní. Právě tato funkce je totiž unikátní vlastností projektu Turrís, kdy jednotlivá zařízení detekují pokusy o útok a přesměrovávají je do specializovaných honeypotů provozovaných CZ.NIC. Honeypoty se tváří jako „zranitelné oběti“ a postupně se snaží z útočníka vylákat všechny možné informace a postupy, které by k útoku uměl použít. Specialisté CZ.NIC tyto útoky analyzují, kategorizují a varují před nimi

ostatní uživatele internetu v pravidelně vydávaných sadách dat. Uživatelé Turrisu na žádná varování samozřejmě čekat nemusí, systém si sám stáhne a aplikuje upravené postupy ochrany routerů.

Poslední, dnes nikoliv samozřejmou výhodou, je zázemí routerů Turrisu. Stojí za nimi firma, která je bytostně spjata s českým internetem, s dvacetiletou zkušeností s internetovým prostředím, stabilním zázemím a hlubokou technologickou znalostí. To umožňuje kontinuální vývoj produktu a především důsledné dbání na bezpečnosti produktu a jeho otevřenosti všem. Routery se navíc vyrábějí v České republice a i to začíná být pro mnoho zákazníků z důvodů bezpečnosti podstatné.

Mimochodem, z webu Turriscz si můžete stáhnout zdrojové kódy veškerého software i hardware a nejenom si router sami sestavit a rozchodit, ale především se přesvědčit, že dělá to, co má. A jenom to, co má. Protože špioni do vašich sítí nepřicházejí jen z Dálného Východu, ale v podstatě odkudkoliv. Nedejte jim šanci.

Parametry

Turrisc Omnia je dostupný v provedení s nebo bez WiFi a 1 či 2GB paměti RAM

CPU 1.6 GHz dvoujádrový ARM RAM 1 GB DDR3 (volitelně 2 GB) Úložiště 8 GB flash LAN 5× Gbit port WAN 1× Gbit port SFP USB 2× USB 3.0 Mini PCI Express 2× mSATA / mini PCI Express 1× Wi-Fi (mini PCIe) 3×3 MIMO 802.11ac 2×2 MIMO 802.11b/g/n Kromě toho má Turrisc Omnia slot pro SIM kartu, hodiny reálného času (RTC) zálohované baterií, kryptočip pro bezpečné generování náhodných čísel, stmívatelné RGB diody, pin-headery s GPIO, I²C, SPI a další.

20

KATALOG FIREM



GENERÁLNÍ PARTNER KONFERENCE

Česká spořitelna, a. s.

Centrála České spořitelny
Olbrachtova 1929/62, 140 00 Praha 4
info linka: +420 800 207 207
e-mail: csas@csas.cz
www.csas.cz



Česká spořitelna je moderní banka orientovaná na drobné klienty, malé a střední firmy a na města a obce. Nezastupitelnou roli hraje také ve financování velkých korporací a v poskytování služeb v oblasti finančních trhů.

HLAVNÍ PARTNEŘI KONFERENCE

Cisco Systems (Czech Republic) s.r.o.

V Celnici 10, 117 21 Praha 1
tel.: +420 221 435 111
www.cisco.com/cz



Cisco je vedoucí firmou v oblasti síťových služeb. Mění způsob, jakým se lidé propojují, komunikují mezi sebou a spolupracují. Pomáhá svým zákazníkům řešit výzvy, které před ně klade digitální ekonomika. Výzvy, které se dotýkají nejenom firem, ale i zdravotnictví, veřejného sektoru, vzdělávání nebo pracovního trhu – tedy celé společnosti.

V digitální ekonomice se strategickým aktivem každé firmy, země i regionu stávají data. Pro budoucí úspěch je klíčová schopnost vyhodnocovat data, dodávat na jejich základě nové služby a především je vždy bezpečně ochránit. Cisco vytváří páteř pro celý digitální svět. Spojuje smysluplně a bezpečně lidi, procesy, data a věci. Dodává řešení, IT kapacity a odborníky pro internet věcí, analýzu a cloud, které přinášejí okamžitý užitek díky správnému využití dat a propojení. Cisco je leaderem v bezpečnosti a svým zákazníkům je partnerem v boji proti kybernetickému zločinu.

Cisco spolupracuje s jednotlivými zeměmi na vybudování technologických dovedností a nástrojů nezbytných k řízení globálního ekonomického růstu.

Česká pošta, s. p.

Politických vězňů 909/4, 110 00 Praha 1
tel.: +420 221 131 111 (ústředna)
zákaznická linka: 840 111 244
www.ceskaposta.cz



Česká pošta je dlouhodobým garantem služeb tzv. eGovernmentu v České republice. Jde o služby zajišťující rychlou, důvěryhodnou a efektivní komunikaci občanů, živnostníků i velkých korporací se státní správou, úřady, soudy, policií atp.

Stěžejními produkty České pošty v oblasti eGovernmentu jsou Czech POINT, datové schránky (a s nimi spojené užitečné služby jako Datový trezor nebo Poštovní datová zpráva) či certifikáty pro elektronické podepisování a elektronická časová razítka.

Právě s elektronickými podpisy je spojená nová zákonná povinnost týkající se orgánů veřejné moci. Ty musí podle nového zákona používat pro podepisování elektronických dokumentů pouze kvalifikovaný elektronický podpis opatřený časovým razítkem. Vytvoření kvalifikovaného elektronického podpisu v souladu s novým zákonem Vám zajistí prostředky z nabídky certifikační autority PostSignum České pošty.

HLAVNÍ PARTNEŘI KONFERENCE

ICZ a.s.

Na hřebenech II 1718/10, 140 00 Praha 4-Nusle
 tel.: +420 222 271 111
 fax: +420 222 271 112
 e-mail: marketing@i.cz
 www.i.cz



ICZ a.s. (člen Skupiny ICZ) – dodavatel IT a systémový integrátor pro veřejnou správu, zdravotnictví, obranu, dopravu, výrobu, logistiku, finance a další.

Disponuje ucelenou a vzájemně provázanou nabídkou řešení a služeb a svým záběrem pokrývá oblasti specifického aplikačního programového vybavení, bezpečnosti, komunikace a infrastruktury.

Působí v ČR i zahraničí.

Microsoft s.r.o.

Vyskočilova 1561/4a, 140 00 Praha 4
 www.microsoft.cz



Microsoft je přední výrobce technologií pro svět, ve kterém jsou mobilita a cloud na prvním místě. Naší misí je umožnit každému člověku a každé organizaci na světě dokázat více. Microsoft Corporation vznikla před více než 40 lety - v dubnu roku 1975. Česká pobočka zahájila činnost v roce 1992. Na podzim 2015 jsme se spolu s pražskou divizí Skype přestěhovali do nového světa práce – kanceláře vytvořené pro svět práce odkudkoli. V červenci 2016 spojila česká pobočka síly se slovenskou a vznikl Microsoft Česká republika a Slovensko. Na podzim 2016 bylo v Praze otevřeno vývojové centrum Microsoft Dynamics. **Naší vizí je inspirovat naše zákazníky, jednotlivce i organizace v České republice i na Slovensku, aby pomocí digitálních technologií dokázali měnit svět.**

Oracle Czech, s.r.o.

U Trezorky 921/2, 158 00 Praha 5
 tel.: +420 221 438 150
 e-mail: info_cz@oracle.com
 www.oracle.com/cz



Společnost Oracle Corporation byla založena v roce 1977 a dnes zaměstnává ve 145 zemích světa přes 136 tisíc lidí. Svým více než 400 tisícům zákazníků – včetně 100 firem z žebříčku Fortune 100 – nabízí kompletní a plně integrovaný soubor cloudových aplikací, platformových služeb a integrovaných systémů.

Datová centra i cloud řešení společnosti Oracle snižují složitost IT prostředí, které bývá překážkou obchodních inovací. Zajišťují vyšší rychlost, spolehlivost, zabezpečení i lepší možnosti správy. Oracle poskytuje kompletní portfolio cloudových řešení přes všechny tři vrstvy cloudu – IaaS, PaaS a SaaS.

Česká pobočka Oracle byla založena v roce 1994 a sídlí v Praze nově na adrese U Trezorky 2, Praha 5-Jinonice. Od okamžiku, kdy společnost Oracle vstoupila na český trh, bylo jejím hlavním cílem přiblížit technologii Oracle co nejširšímu spektru firem i státním institucím.

HLAVNÍ PARTNEŘI KONFERENCE

Taipei Economic and Cultural Office

Evropská 33c, 160 00 Prague 6
tel.: +420 233 322 415
www.taiwanembassy.org/cz_cs

TAIWAN

駐捷克台北經濟文化辦事處
Taipei Economic and Cultural Office, Prague
Tchajpejská hospodářská a kulturní kancelář v Praze

Tchajpejská hospodářská a kulturní kancelář vznikla v Praze roku 1991. Kancelář funguje jako nejvyšší zastupitelský úřad vlády Tchaj-wanu (ROC) v České republice. Jejím hlavním posláním je podporovat oboustranné mezivládní a meziparlamentní vztahy a přispívat k rozvoji vzájemných vztahů mezi Českou republikou a Tchaj-wanem prostřednictvím kulturních výměn, vědecké spolupráce, turistiky, obchodní činnosti a investic, jakož i poskytovat konzulární služby mezi Tchaj-wanem a Českou republikou.

Toto je podruhé, co se tchajwanská delegace podílí na konferenci ISSS, a zároveň podruhé, co Rada pro rozvoj zahraničního obchodu Tchaj-wanu na veletrhu představuje tchajwanský pavilon. Tchajwanská delegace se skládá ze zastupitelů předních tchajwanských značek, které poskytují služby a produkty související s datovými centry, inteligentními systémy v domácnostech, inteligentními systémy pro vzdělávání a úsporou energie. Tchaj-wan je celosvětově uznávaný pro své enormní výrobní kapacity v oboru ICT a prokazatelné úspěchy ve vývoji ICT aplikací a je schopen poskytnout inteligentní integrovaná řešení, která nejlépe vyhovují vašim potřebám. Vše, co musíte udělat, je sdělit nám vaše potřeby a naše kancelář vám najde nejlepšího partnera i řešení.

VITA software, s.r.o

Na Beránce 57/2, 160 00 Praha 6
tel.: +420 212 241 549
e-mail: vita@vitasw.cz
www.vitasw.cz



VITA vytváří software pro správní orgány, zejména pro městské a krajské úřady a ministerstva. VITA je dominantním dodavatelem softwaru pro stavební úřady, úřady územního plánování, silniční správní úřady, vodoprávní úřady, vyvlastňovací úřady, orgány na úseku ochrany památek a velmi významným dodavatelem pro správní orgány řešící přestupky a jiné správní delikty, životní prostředí, dopravní agendy, koordinované stanovisko a poskytování informací. Dodávaný software je integrován se spisovou službou, ekonomickým systémem, geografickým informačním systémem, identity managementem, portálem občana i portálem úředníka. Samozřejmě je integrován s celostátními informačními systémy ISZR, ISDS, ISKN, ČSÚ atd. Dodávaný software je v souladu s legislativou, vyniká vysokou kvalitou a je významným pomocníkem úředníků.

PARTNEŘI KONFERENCE

Alef Nula

U Plynárny 1002/97, 101 00 Praha 10
<http://training.alef.com>



V ALEF NULA řešíme 5 základních dynamických rozvojových oblastí – Security, Smart City, Datacenter, Collaboration a Training Center. Navrhujeme konkrétní řešení dle potřeby na míru. Pomůžeme s nalezením vhodných forem financování pro Vaše investice. Specializujeme se na kvalitní poradenské a vzdělávací služby. Teoretické znalosti jsme podložili zkušenostmi z implementací. Ověřitelné reference jsou samozřejmostí. Kontaktujte nás. www.alef.com.

Asseco Central Europe, a. s.

Budějovická 778/3a, 140 00 Praha 4
 tel.: +420-234 292 500
 fax: +420-234 292 502
 email: sales@asseco-ce.com
www.asseco.com/ce



Asseco Central Europe (Asseco CE) je jedním z nejsilnějších softwarových domů ve střední a východní Evropě. Působí v České republice, Slovensku, Maďarsku, Německu, Rakousku, Švýcarsku a Bělorusku. Patří mezi nejvýznamnější poskytovatele komplexních řešení a služeb v oblasti informačních technologií. Realizuje náročné projekty jak pro komerční sféru, tak pro státní správu a samosprávu a má dlouholeté zkušenosti s rozsáhlými projekty, které podporují strategické záměry klientů. Asseco Central Europe je součástí mezinárodní skupiny Asseco, která působí ve více než 54 zemích světa a zaměstnává přes 21 500 lidí.

AutoCont CZ a.s.

Hornopolní 3322/34, 702 00 Ostrava
 tel.: +420 910 971 111
 fax: +420 910 970 100
 e-mail: obchod@autocont.cz
www.autocont.cz

AutoCont je česká soukromá společnost, která přes 25 let na českém a slovenském trhu úspěšně zavádí a provozuje užitečné informační technologie. Zaměřuje se na poskytování komplexních IT řešení a služeb pro firemní klientelu a státní správu.

AV MEDIA, a. s.

Pražská 63, 102 00 Praha 10
 tel.: +420 261 260 218
 fax: +420 261 227 648
 e-mail: paha@avmedia.cz
www.avmedia.cz



Společnost AV MEDIA je leaderem na poli prezentační, projekční a audiovizuální techniky v České republice. Prostřednictvím návrhů a realizací řešení pro sdílení obrazu a zvuku přinášíme svým zákazníkům inspiraci, užitek i radost. Poskytujeme profesionální služby od projektového návrhu řešení až po zaškolení a následný servis a vždy sledujeme nejnovější trendy, které pak přinášíme do ČR jako první. AV technika a další produkty společnosti jsou využívány v konferenčních a zasedacích místnostech, na dispečerských pracovištích s nepřetržitým provozem, v učebnách a školicích místnostech, u speciálních simulačních a 3D aplikací, v kinosálech, v muzejních expozicích, na veletrzích a na mnoha dalších místech. Našimi zákazníky jsou školy, vysoké školy, kulturní instituce, firmy, veřejná správa, hotely i domácnosti. Vedle realizací řešení zajišťujeme i pronájem a obsluhu špičkové audiovizuální techniky pro širokou škálu různorodých akcí, od firemních školení přes korporátní kongresy, společenské akce a veletržní expozice až po venkovní projekci na budovy.

PARTNEŘI KONFERENCE

Citrix Systems Czech Republic s.r.o.

Na Pankráci 1724/129, 140 00 Praha 4
e-mail: tomas.poslusny@citrix.com
www.citrix.cz



Aplikace, Data, Síť – klíčové komponenty digitálního světa. Ve společnosti Citrix se řídíme jedním hlavním principem: zajistit zabezpečený a snadný přístup ke všem aplikacím a datům na světě. Všude. Kdykoli. Z jakéhokoli zařízení nebo sítě. Řešení Citrix používá více než 400 000 organizací a více než 100 milionů uživatelů po celém světě. Více na www.citrix.cz.

České Radiokomunikace a. s.

Skokanská 2117/1, 169 00 Praha 6
tel.: +420 242 411 111
e-mail: info@cra.cz
www.cra.cz



České Radiokomunikace a.s. (CRA) jsou leaderem v poskytování digitální infrastruktury. Kromě vysílacích služeb se firma zaměřuje na propojování světa televize, rádia a internetu. Provozuje vlastní datová centra a svým zákazníkům poskytuje špičkový výpočetní výkon s maximálním možným zabezpečením. CRA disponují vlastní optickou páteří sítě a díky silné vysílací infrastruktuře mohou nabídnout zákazníkům i bezdrátové řešení, případně připojení blízkých lokalit pomocí optických vláken. Díky této unikátní infrastruktuře budují robustní IoT síť na technologii LoRaWAN, která umožňuje bezdrátovou komunikaci pro chytrá řešení a propojuje tato řešení do CRA IoT Cloudu. V průběhu roku 2017 plánují do rozvoje v této oblasti investovat desítky milionů korun a počítají, že by pokrytí IoT sítě mělo zasáhnout 90 % populace v ČR. Zároveň se CRA aktivně podílejí na budování ekosystému partnerů sítě LoRa v ČR, budují prostředí pro spolupráci v oblasti IoT a organizují SW i HW orientované akce pro širší odbornou veřejnost.

Více informací o společnosti a jejich službách naleznete na www.cra.cz.

FORTINET

Pekařská 10A, 155 00 Praha 5
tel.: +420 773 788 788
e-mail: fortinet.czechrepublic@fortinet.com
www.fortinet.com



Společnost Fortinet (NASDAQ: FTNT) chrání nejcennější majetek firem, poskytovatelů služeb i vládních organizací po celém světě. Rychlá, bezpečná a globální řešení Fortinet pro kybernetickou bezpečnost poskytují širokou a vysoce výkonnou ochranu proti dynamickým bezpečnostním hrozbám, a zároveň zjednodušují IT infrastrukturu.

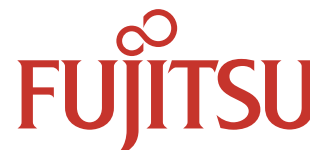
Řešení jsou vyvíjena na základě řady výzkumů, analýz a monitoringu aktuálních hrozeb. Díky tomu se Fortinet dokáže vypořádat s nejdůležitějšími bezpečnostními požadavky firem, ať už v oblasti sítě, aplikací nebo mobility, bez ohledu na to, zda se jedná o virtualizované, cloudové či fyzické prostředí. Více než 210 000 zákazníků po celém světě, včetně těch největších a nejsložitějších organizací, spoléhá na Fortinet při ochraně svého prostředí.

Společnost Fortinet vyvíjí, vyrábí a prodává portfolio produktů a služeb, které tvoří nejmodernější a nejvýkonnější síťovou bezpečnostní platformu, s jejíž pomocí mohou zákazníci bezpečně budovat a rozvíjet své IT infrastruktury, a to jednodušeji a s nižšími náklady. Díky integraci širokého spektra bezpečnostních služeb v jednom zařízení pomáhá Fortinet zjednodušit celou síťovou infrastrukturu a zajistit pohodlnou centralizovanou správu, lepší kontrolu a ucelený pohled na bezpečnostní situaci v reálném čase.

PARTNEŘI KONFERENCE

FUJITSU

Fujitsu Technology Solutions s.r.o.
V Parku 2336/22, 148 00 Praha 4
tel.: +420 233 034 007
e-mail: info.cz@ts.fujitsu.com
www.fujitsu.cz



Fujitsu Technology Solutions nabízí kompletní portfolio IT produktů, řešení a služeb – od klientského portfolia až po řešení datových center, spravovanou infrastrukturu a infrastrukturu poskytovanou jako služba (IaaS). Zákazníkům poskytuje služby od poradenství a návrhu systému, dodávky systému a jeho implementaci až po následný provoz, údržbu a servis.

Fujitsu má bezkonkurenční znalosti a zkušenosti s nasazením výpočetních systémů v podnikové a státní sféře, včetně dodávek prvotřídních serverů na bázi platform Intel a UNIX, mainframů či zařízení pro ukládání dat. Patří též mezi přední dodavatele profesionálních PC, notebooků, ultrabooků, tabletů a pracovních stanic pro firmy i domácnosti. V posledních letech byla nabídka rozšířena i o scannery a tiskárny a také o unikátní biometrickou metodu PalmSecure™ – bezdotykové jednoznačné rozpoznávání uživatelů vhodné například pro banky, zdravotnická zařízení nebo sportovní utkání.

Na český trh vstoupila společnost Fujitsu v roce 1999, kdy vytvořila společný podnik se společností Siemens AG pod názvem Fujitsu-Siemens. V dubnu roku 2009 po odkoupení 50% podílu od Siemensu vznikla společnost **Fujitsu Technology Solutions s.r.o.** V současné době je tato společnost zodpovědná za rozvíjení obchodních aktivit nejen v ČR, ale i na Slovensku.

GORDIC spol. s r. o.

Erbenova 4, 586 01 Jihlava
tel.: +420 567 309 136
e-mail: gordic@gordic.cz
www.gordic.cz



GORDIC spol. s r.o. je předním českým tvůrcem a dodavatelem informačních systémů. V její činnosti se protíná oblast komplexních softwarových řešení pro veřejný sektor a bankovníctví, kybernetické bezpečnosti a Internetu věcí. GORDIC více než 6000 zákazníkům veřejné správy pomáhá s vedením ekonomiky, spisové služby nebo správních agend. Spolupracuje s městy a regiony při naplňování jejich vizí Smart Cities&Regions. V oblasti kybernetické bezpečnosti buduje platformu KYBEZ, která je založená na spolupráci odborných akademických, veřejných i komerčních institucí. Součástí jejího portfolia jsou také technologie HDL pro chytré budovy.

PARTNEŘI ODBORNÝCH BLOKŮ

Český telekomunikační úřad

Sokolovská 219, 190 03 Praha 9
 adresa pro doručování: P.O. BOX 02, 225 02 Praha 025
 tel.: +420 224 004 111, fax: +420 224 004 830
 e-mail: podatelna@ctu.cz
www.ctu.cz



Český telekomunikační úřad

Český telekomunikační úřad je ústředním orgánem státní správy. Vykonává působnost státu ve věcech stanovených zákonem, včetně regulace trhu a stanovování podmínek pro podnikání v oblasti elektronických komunikací a poštovních služeb.

Software602 a.s.

Hornokrčská 15, 142 00 Praha 4
 tel.: +420 222 011 602
 e-mail: info@602.cz
www.602.cz



Jsme tradiční česká společnost. Digitalizací procesů, dokumentů a dlouhodobou archivací pomáháme efektivněji dosáhnout provozních i obchodních cílů.

CZ.NIC, z. s. p. o.

Milešovská 5, 130 00 Praha 3
 tel.: +420 222 745 111
 e-mail: podpora@nic.cz, podpora@mojeid.cz
www.nic.cz, www.mojeid.cz



Službu mojeiD vyvíjí a provozuje sdružení CZ.NIC, jehož hlavní činností je provoz registru doménových jmen .CZ, zabezpečení provozu domény nejvyšší úrovně .CZ a osvěta v oblasti doménových jmen.

Network Security Monitoring Cluster, družstvo

CERIT Science Park, Botanická 554/68a, 602 00, Brno
 tel.: +420 549 49 2286
 e-mail: info@nsmcluster.com
www.nsmcluster.com



NSMC je sdružení českých firem a expertů z oblasti KB. Věnuje se evangelizaci problematiky počítačové bezpečnosti, vzdělávání, vědě a výzkumu.

SPOLUPRACUJÍCÍ INSTITUCE A SDRUŽENÍ

Asociace krajů ČR

Zborovská 11, 150 21 Praha 5
tel.: +420 236 003 481
ID datové schránky: 77x5zix
www.asociacekrajů.cz



Český úřad zeměměřický a katastrální

Pod Sídlištěm 1800/9, 182 11 Praha 8
tel.: +420 284 041 111
e-mail: cuzk@cuzk.cz
ID datové schránky: uuaaatg
www.cuzk.cz



ICT UNIE z.s.

K Červenému dvoru 25a/3269, 130 00 Praha 3
ID datové schránky: zjbsfas
www.ictu.cz



IDC CEMA s.r.o.

Malé náměstí 13, 110 00 Praha 1
tel.: +420 221 423 140, fax: +420 221 423 150
www.idc-czech.cz



Iniciativa 202020

K Červenému dvoru 25a/3269, 130 00 Praha 3
tel.: +420 222 582 880
e-mail: Iniciativa@202020.cz



Sdružení tajemníků městských a obecních úřadů ČR, z. s.

Dlážděná 1004/6, 110 00 Praha 1-Nové Město
tel.: +420 481 312 276, +420 606 882 187
e-mail: stmou@mmdecin.cz
ID datové schránky: bbd8nn3
www.tajemnici.cz



Svaz měst a obcí ČR

5. května 1640/65, 140 00 Praha 4
tel.: +420 234 709 711, fax: +420 234 709 786
e-mail: smocr@smocr.cz
ID datové schránky: 5fkgwn3
www.smocr.cz



Zeměměřický úřad

Pod sídlištěm 1800/9, 182 11 Praha 8
tel.: +420 284 041 111
ID datové schránky: 6yvadsa
e-mail: zu-praha@cuzk.cz
www.cuzk.cz, http://geoportal.cuzk.cz



KRAJE A MĚSTA

Kraj Vysočina

Žižkova 57, 587 33 Jihlava
 tel.: +420 564 602 111, +420 564 602 100
 fax: +420 564 602 420
 e-mail: posta@kr-vysocina.cz
 ID datové schránky: ksab3eu
www.kr-vysocina.cz



Královéhradecký kraj

Krajský úřad Královéhradeckého kraje
 Regiocentrum Nový pivovar
 Pivovarské náměstí 1245, 500 03 Hradec Králové
 tel.: +420 495 817 111
 fax: +420 495 817 336
 e-mail: posta@kr-kralovehradecky.cz
 ID datové schránky: gcgbp3q
www.kr-kralovehradecky.cz



Statutární město Hradec Králové

Magistrát města Hradec Králové
 Československé armády 408, 502 00 Hradec Králové
 tel.: +420 495 707 111
 fax: +420 495 707 100
 e-mail: posta@mmhk.cz
 ID datové schránky: bebb2in
www.hradeckralove.org



Hlavní město Praha

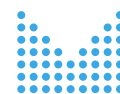
Magistrát hlavního města Prahy
 Mariánské nám. 2, 110 01 Praha 1
 tel.: +420 12 444
 e-mail: info@praha.eu
 ID datové schránky: 48ia97h
www.praha.eu



MINISTERSTVA

Ministerstvo vnitra ČR

Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7
tel.: +420 974 811 111
e-mail: posta@mvcz.cz
ID datové schránky: 6bnaawp
www.mvcz.cz



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo pro místní rozvoj ČR

Staroměstské náměstí 6, 110 15 Praha 1
tel.: +420 224 861 111
e-mail: info@mmr.cz
ID datové schránky: 26iaava
www.mmr.cz



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

Ministerstvo spravedlnosti ČR

Vyšehradská 16, 128 10 Praha 2
tel.: +420 221 997 111
e-mail: posta@mzp.justice.cz
www.justice.cz



Ministerstvo spravedlnosti České republiky

Ministerstvo práce a sociálních věcí ČR

Na Poříčním právu 1/376, 128 01 Praha 2
tel.: +420 221 921 111
e-mail: posta@mpsv.cz
ID datové schránky: sc9aavg
www.mpsv.cz



Ministerstvo zdravotnictví ČR

Palackého nám. 4, 128 01 Praha 2
tel.: +420 224 971 111
e-mail: mzcr@mzcr.cz
ID datové schránky: pv8aaxd
www.mzcr.cz



MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Ministerstvo životního prostředí

Vršovická 1442/65, 100 10 Praha 10
tel.: +420 267 121 111
e-mail: info@mzp.cz
ID datové schránky: 9gsaax4
www.mzp.cz

Ministerstvo životního prostředí

PREZENTACE FIREM

ADUCID s.r.o.

Vídeňská 204/125, 619 00 Brno-Průzřenice
tel.: +420 271 100 100
e-mail: sales@aducid.com
www.aducid.com

Zajišťujeme silnou autentizaci pro zákazníky eID řešení v oblasti elektronické veřejné správy a eBanking.



AION CS, s.r.o.

Nám. T. G. Masaryka 1280, 760 01 Zlín
tel.: +420 577 217 811
e-mail: info@aion.cz
www.aion.cz; www.zakonyprolidi.cz

Hlavní naší aktivitou jsou právní informační systémy – zakázkové projekty pro naše klienty (www.epi.sk) i služby pro koncové uživatele (www.zakonyprolidi.cz).

Zákony pro lidi.cz

ANECT a.s.

Vídeňská 204/125, Průzřenice, 619 00 Brno
tel. Praha: +420 547 100 100
e-mail: anect@anect.com
www.anect.com

Přední dodavatel profesionálních řešení z oblasti informačních a komunikačních technologií. Jsme integrátorem služeb ICT, které přinášejí každodenní užitek.



ARCDATA PRAHA, s.r.o.

Hybernská 24, 110 00 Praha 1
tel.: +420 224 190 511, fax: +420 224 190 567
e-mail: office@arcdata.cz
www.arcdata.cz

Distributor geografických informačních systémů Esri a dodavatel komplexních GIS řešení s řadou referencí ve veřejném i privátním sektoru.



ATLAS consulting spol. s r.o. / CODEXIS®

Výstavní 292/13, 702 00 Ostrava
tel.: +420 596 613 333, fax: +420 596 613 330
e-mail: klientske.centrum@atlasconsulting.cz
www.atlasconsulting.cz

CODEXIS® – komplexní právní informační systém pro všechny, kteří při výkonu své profese přicházejí do styku s právní problematikou.



Atos IT Solutions and Services, s.r.o

Doudlebská 1699/5, Praha 4, 140 00

e-mail: cz.info@atos.netwww.cz.atos.net

Atos SE (Societas Europaea) je lídrem v digitálních službách, který dosáhl za rok 2015 ročního výnosu ve výši 12 miliard EUR a který zaměstnává 100 tisíc pracovníků v 72 zemích.

Akvizicí společnosti Siemens IT Solutions and Services v říjnu 2010 začal Atos působit v České republice pod jménem Atos IT Solutions and Services, s.r.o. Atos v České republice dosáhl v roce 2015 čistého obrátu firmy 39 697,- tis. EUR a zaměstnává 300 zaměstnanců v Praze, Brně, Ostravě a Vysokém Mýtě

Atos přináší poradenství a systémovou integraci, řízené služby a outsourcing business procesů, cloudové operace, Big Data a řešení pro kybernetickou bezpečnost, stejně tak jako i transakční služby prostřednictvím společnosti Worldline, evropského lídra v oblasti platebních a transakčních služeb.

Díky vysoké technologické odbornosti a znalostem průmyslových odvětví společnost Atos pracuje s klienty z různých obchodních sektorů jako jsou: finanční služby, zdravotnictví, výrobní průmysl, média, telekomunikace, energetika, veřejný sektor, doprava, obrana a retailové podniky.

Atos se zaměřuje na technologie, které přinášejí pokrok a pomáhají organizacím vytvářet firmu budoucnosti.

Společnost Atos je celosvětovým technologickým partnerem Olympijských a Paralympijských her a je kotovaná na pařížské burze NYSE Euronext Paris. Společnost Atos působí pod značkami Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify a Worldline.

AXENTA a.s.

Mlýnská 326/13, 602 00 Brno

tel.: +420 549 492 289

e-mail: info@axenta.czwww.axenta.cz

AXENTA a. s. je integrátor bezpečnosti ICT = bezpečnosti IT, ochrany informací a fyzické bezpečnosti. Je zkušeným dodavatelem Log Managementu, SIEM a Security Operation Center řešení v ČR, SR.

CENIA, česká informační agentura životního prostředí

Vršovická 1442/65, 100 10 Praha 10

tel.: +420 267 125 226

e-mail: info@cenia.czwww.cenia.cz

CENIA je příspěvkovou organizací MŽP. Posláním CENIA je shromažďování, hodnocení, interpretace a distribuce informací o životním prostředí.

CEVRO Institut, z.ú.

Jungmannova 28/17, 110 00 Praha 1

tel.: +420 221 506 777

e-mail: info@vsci.czwww.cevroinstitut.cz

CEVRO Institut je soukromou vysokou školou práva, politologie, mezinárodních vztahů, ekonomie a bezpečnostních studií, která na českém vysokoškolském trhu působí více než deset let.

CGI IT Czech Republic s.r.o.

Laurinova 2800/4, 155 00 Praha 5
tel.: +420 284 020 111
cz.cgi.com



CGI je přední globální firma v oblasti IT konzultací a služeb založená v r. 1976 v Kanadě od r. 1993 působí i v ČR. Nabízí komplexní portfolio služeb a řešení.

Česká správa sociálního zabezpečení

Křížová 25, 225 08 Praha 5
tel.: +420 257 061 111, fax: +420 257 063 360
e-mail: posta@cssz.cz
www.cssz.cz



ČESKÁ SPRÁVA
SOCIÁLNÍHO ZABEZPEČENÍ

ČSSZ spravuje sociální zabezpečení pro 8,7 mil. klientů. Je klientsky orientovaným úřadem a podporuje elektronizaci: ePortál ČSSZ ...naše služby jsou vám blíže.

ČD - Telematika a.s.

Pernerova 2819/2a, 130 00 Praha 3
www.cdt.cz



ČD - Telematika a.s. – telekomunikační služby, služby výstavby a servisu infrastruktury, druhá největší optická síť v ČR, vysoce zabezpečená datacentra a IoT chytrá řešení řešení pro města i firmy.

DAIN, s.r.o.

Na Hrázi 176/17, 180 00 Praha 8
tel.: +420 284 683 592
e-mail: info@dain.cz
www.dain.cz



Specializovaný poskytovatel řešení a služeb v oboru ICT, procesního řízení, znalostního managementu a enterprise architektury – ARCHIREPO (www.archirepo.com/cz).

DATASYS s.r.o.

Jeseniova 2829/20, 130 00 Praha 3
tel.: +420 225 308 111
fax: +420 225 308 110
e-mail: datasys@datasys.cz
www.datasys.cz



DATASYS je dynamická, ryze česká soukromá společnost. Od roku 1994 poskytuje komplexní implementační a integrační služby v oblasti IT, telekomunikací a vývoje na zakázku. Jejimi zákazníky jsou významné české společnosti z oblasti utilit, financí, průmyslu, telekomunikací, zdravotnictví či obchodu a služeb a instituce státní správy a samosprávy.

DATRON, a.s.

Vachkova 3008, 470 01 Česká Lípa
tel.: +420 483 030 411
e-mail: info@datron.cz
www.datron.cz



Společnost DATRON se ve veřejné správě specializuje na dodávky portálových řešení. Nabízíme i řešení pro Dashboardy, OpenData a řízení rozvojových potřeb.

Elektrotechnický zkušební ústav, s.p.

Pod Lisem 129, 171 02 Praha 8-Troja
 tel.: +420 266 104 111
 e-mail: info@ezu.cz
 www.ezu.cz



EZÚ, s.p. jako první akreditovaný subjekt nabízí certifikaci dle nařízení eIDAS. Dále pak mezi jeho služby patří zajištění kybernetické bezpečnosti, audity systémů řízení, školení v oblasti IT služeb.

Flowmon Networks a.s.

U Vodárny 2965/2, 616 00 Brno
 tel.: +420 511 205 250
 e-mail: info@flowmon.com
 www.flowmon.com



Flowmon Networks pomáhá spravovat a zabezpečovat síťovou infrastrukturu firem prostřednictvím monitorování a analýzy chování poč. sítí na bázi datových toků.

GEOVAP, spol. s r.o.

Čechovo nábřeží 1790, 530 03 Pardubice
 tel.: +420 466 024 111, fax: +420 466 657 314
 e-mail: info@geovap.cz
 www.geovap.cz



Informační systémy pro města a obce, spisová služba a systémy pro správu dokumentů, GIS a mapové portály.

GEPRO spol. s r.o.

Štefánikova 52, 150 00 Praha
 tel.: +420 257 089 811, fax: +420 257 089 838
 e-mail: gepro@gepro.cz
 www.gepro.cz



Geoportál GEPRO i GIS systém MISYS používají zaměstnanci více než 1800 úřadů měst i obcí a občané celé ČR. VYZKOUŠEJTE: http://geoportal.gepro.cz/obce/nazev_obce

HP Inc Czech Republic s.r.o.

Za Brumlovkou 1559/5, 140 00 Praha 4
 tel.: +420 225 439 636
 e-mail: info.cz@hp.com
 www.hp.com



HP vytváří technologie, které usnadňují život lidem po celém světě. Díky našemu portfoliu tiskáren, počítačů, řešení a služeb vytváříme zážitky, které ohromí.

IBA CZ, s.r.o.

Petržilkova 2565/23, 158 00 Praha 5
 tel.: +420 251 050 150
 e-mail: info@ibacz.eu
 www.ibacz.eu



IBA CZ, člen nadnárodní IBA Group, je technologická společnost poskytující IT služby a vývoj software v oblasti portálů, ECM, mobilních aplikací, CRM, Identity Managementu a BI & BigData.

IBR Consulting, s. r. o.

Sokolovská 352/215, 190 00 Praha 9
 tel.: +420 234 256 212
 e-mail: info@ibrconsulting.cz
 www.ibrconsulting.cz, www.aspe.cz



IBR Consulting, s. r. o. působí na trhu v oblasti přípravy a realizace staveb. Zajišťujeme TDS, cenové expertizy, administraci projektů a specializované SW pro investory, projektanty a stavitele.

Institut pro elektronizaci zdravotnictví, z. ú.

Českomoravská 2408/1a, 190 00, Praha 9-Libeň
 e-mail: info@zdravel.cz
 www.zdravel.cz



Nezbytným základním kamenem pro elektronizaci zdravotnictví je tzv. Electronic health record (el. zdrav. záznam), nad kterým mohou vznikat nadstavbová řešení.

Intergraph CS s.r.o., divize Hexagon Safety & Infrastructure

Prosek Point - budova A, Prosecká 851/64, 190 00 Praha 9
 tel.: +420 234 707 820
 e-mail: info-cz@intergraph.com
 www.hexagonsafetyinfrastructure.com



Hexagon je světový lídr v oblasti informačních technologií. Naše řešení pomáhají efektivně propojit krizová a podniková data a dodat zákazníkovi včas maximum přesných informací.

MARBES CONSULTING s.r.o.

Brojova 2113/16, 326 00 Plzeň
 tel.: +420 378 121 500, fax: +420 378 121 501
 e-mail: marbes@marbes.cz; obchod@marbes.cz
 www.marbes.cz



Konzultační, vývojová a vzdělávací společnost působící v oblasti informačních technologií jako systémový integrátor a dodavatel ucelených SW řešení zejména pro státní správu a samosprávu.

Novicom, s.r.o.

Koněvova 67a, 130 00 Praha 3
 tel.: +420 271 777 231
 e-mail: info@novicom.cz
 www.novicom.cz



Český výrobce nástrojů pro monitoring, správu a bezpečnost ICT. Přináší integrované DDI/NAC řešení AddNet pro efektivní, spolehlivé a bezpečné fungování sítí.

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví

Roškotova 1225/1, 140 21 Praha 4
 tel.: +420 261 105 555, fax: +420 261 105 300
 e-mail: ozp@ozp.cz
 www.ozp.cz



OZP je první zdravotní pojišťovna v ČR nabízející plně funkční a bezpečné online komunikační nástroje nejen pro web, ale rovněž pro mobilní telefony a tablety.

OKI Systems (Czech and Slovak), s.r.o.

Futura business park, Sokolovská 668/136d, 186 00 Praha 8
 tel.: +420 737 282 645
 e-mail: jiri.sojka@oki.cz
 www.oki.cz

Specialista v oboru tištěné podnikové komunikace. Hlavní sortimentní skupiny jsou počítačové tiskárny, multifunkční zařízení včetně tiskových řešení.

OKsystem a.s.

Na Pankráci 125, 140 21 Praha 4
 tel.: +420 236 072 111
 e-mail: info@oksystem.cz
 www.oksystem.cz

Vývoj rozsáhlých informačních systémů na zakázku, vývoj mobilních aplikací, správa dokumentů, bezpečnost dat ve světě IT a mobilních zařízení.

QCM, s.r.o.

Heršpická 5, 639 00 Brno
 tel.: +420 538 702 702
 e-mail: obchod@qcm.cz
 www.qcm.cz

QCM je leader v elektronizaci veřejných zakázek. Spolehlivě dodává pro zadavatele z řad státní správy a samosprávy individuální elektronický nástroj E-ZAK, e-tržišť Gemin, systém centralizovaného zadávání RSCZ, e-aukční portál eAUKCE, poskytuje profil zadavatele na Portálu pro vhodné uveřejnění. Vzdělává zadavatele a dodavatele v oblasti elektronizace, veřejných zakázek, registru smluv a dalších zákonů. Dále nabízí právní služby a administraci veřejných zakázek.

SEFIRA spol. s r.o.

Antala Staška 2027/77, 140 00 Praha
 tel.: +420 222 558 111
 e-mail: sales@sefira.cz
 www.sefira.cz

Společnost SEFIRA je dodavatelem IT produktů a služeb se zaměřením na dodávky moderních řešení pro důvěryhodné vytváření, ověřování a dlouhodobé uchovávání elektronických dokumentů a poskytování služeb v oblastech digitální transformace.

Sirwisa a.s.

Zubatého 295/5, 150 00 Praha 5
 tel.: +420 257 211 849
 e-mail: obchodnici@logmanager.cz
 www.logmanager.cz

LOGmanager – český systém pro sběr, správu a analýzu logů z operačních systémů, aplikací, síťových a bezpečnostních zařízení a dalších.

LOGmanager se stal vítězem soutěže „IT produkt roku 2016“ v kategorii Bezpečnostní zařízení.

Státní fond životního prostředí České republiky

Kaplanova 1931/1, 148 00 Praha 11
tel.: +420 267 994 300
fax: +420 272 936 597
e-mail: dotazy@sfzp.cz
www.sfpz.cz



STÁTNÍ FOND
ŽIVOTNÍHO PROSTŘEDÍ
ČESKÉ REPUBLIKY

Státní fond životního prostředí ČR je specificky zaměřenou institucí, která zásadním způsobem přispívá na investice do ochrany a zlepšování životního prostředí.

Státní pokladna Centrum sdílených služeb, s.p.

Na Vápence 915/14, 130 00 Praha 3-Žižkov
tel.: +420 225 515 111
e-mail: info@spcss.cz
www.spcss.cz



Státní pokladna
Centrum sdílených služeb

Hlavní předmět činnosti SPCSS s.p. je zaměřen na poskytování služeb provozu IT a kybernetické bezpečnosti primárně pro resort ministerstva financí.

STÁTNÍ TISKÁRNA CENIN, státní podnik

Růžová 6, č. p. 943, 110 00 Praha 1
tel.: +420 236 031 111, fax: +420 236 031 400
e-mail: obchod@stc.cz
www.stc.cz



Od roku 1928 jsme dodavatelem komplexního technologického know-how v oblasti tisku produktů ceninového charakteru, vyžadujících vysoký stupeň zabezpečení výroby.

STYRAX, a.s.

Zelený pruh 95/97, 140 00 Praha 4
tel.: +420 227 027 324
e-mail: info@styrax.cz
www.styrax.cz



STYRAX, a.s. se orientuje především na vývoj a implementaci proprietárních informačních systémů a na poskytování konzultačních a analytických služeb. STYRAX úspěšně realizoval rozsáhlé projekty, zejména v oblasti finančního a kapitálového trhu a také v oblasti zdravotnictví.

System4u, s.r.o.

Křížová 18, 603 00 Brno
tel.: +420 543 210 522
e-mail: info@system4u.com
www.system4u.cz



System4u, s.r.o. – technologie a služby pro hromadnou správu a zabezpečení podnikových mobilních zařízení – Mobile Device Management.

T-MAPY spol. s r.o.

Špitálská 150, 500 03 Hradec Králové
tel.: +420 498 511 111
e-mail: info@tmapy.cz
www.tmapy.cz



Nabízíme webové technologie pro geografické i základní informační systémy, softwarové prostředky pro desktopový GIS a geografická data pro všestranné využití.

Tender systems s.r.o.

nám. Před Bateriemi 18, 162 00 Praha
 tel.: +420 212 241 545
 e-mail: info@tendersystems.cz
 www.tendersystems.cz



Společnost Tender systems s.r.o. se zabývá výrobou a provozováním informačních systémů pro elektronické zadávání veřejných zakázek. Nabízí řadu doplňkových produktů a služeb, včetně vzdělávání a odborného poradenství v oblasti elektronizace veřejného investování.

TRIADA, spol. s r. o.

U Svobodárny 1110/12, 190 00 Praha 9
 tel.: +420 284 001 284, fax: +420 284 818 027
 e-mail: info@triada.cz
 www.triada.cz



Společnost TRIADA patří k předním dodavatelům software (IS MUNIS) a služeb pro sféru veřejné správy ČR. Kromě této činnosti pořádá konferenci ISSS, organizuje setkání starostů Den malých obcí a vydává odborný časopis OBEC & finance.

VARs BRNO a.s.

Kroftova 80c, 612 00 Brno
 tel.: +420 515 514 111
 e-mail: info@vars.cz
 www.vars.cz



VARs BRNO a.s. je technologická firma nabízející inovativní a chytrá řešení pro dopravní telematiku, správu majetku a GIS. Naše řešení pro Smart City akcentuje především oblast mobility, hospodaření na pozemních komunikacích a komunikaci s obyvateli. Zajišťujeme dohled nad dopravou i její ovlivňování. Poskytujeme dopravní informace pro veřejnost a statistická dopravní data pro dopravní odborníky.

Vyvinuli jsme komplexní systém CleveRA pro diagnostiku komunikací a tvorbu plánů údržby a oprav, jsme experty v oblasti hospodaření na pozemních komunikacích.

V portálu SMARTiC CITY kombinujeme data o mobilitě a komunikacích s daty o hospodaření, životním prostředím a dalších oblastech života města, abychom poskytli lepší podklady pro rozhodování managementu města a zlepšili informovanost občanů a zájem o jejich město.

Vema, a. s.

Okružní 871/3a, 638 00 Brno
 tel.: +420 530 500 000
 e-mail: vema@vema.cz
 www.vema.cz



Přední český dodavatel informačních systémů pro řízení lidských zdrojů. Vyvíjí a implementuje vlastní softwarové řešení v oblastech zpracování mezd, evidence personálních údajů, docházky, hodnocení, systemizace, vzdělávání, výběrových řízení, plánování dovolené, pracovních cest atd.

Lídr na poli cloudových řešení HR systémů.

VERA, spol. s r.o.

Sídlo: Lužná 2, 160 00 Praha 6
 Kontaktní adresa: Klicperovo nám. 39/I, 503 51 Chlumeck nad Cidlinou
 tel.: +420 495 703 211
 e-mail: obchod@vera.cz, info@vera.cz
 www.vera.cz



VERA Radnice, VERA Dimenze – Kompletní řešení IS pro veřejnou správu.

Komplexní systémy zahrnují mj. ekonomiku, majetek, agendy, podporu interních procesů, vč. mobilních řešení, manažerských nadstaveb, systému pro městskou policii, portálových řešení pro občany a možnosti integrace na okolí.

ERP systém pro organizace s vlastnickým podílem obcí, krajů a státu.

WEBHOUSE, s. r. o.

Masarykovo nám. 47, 586 01 Jihlava
 tel.: +420 561 207 247
 e-mail: obchod@webhouse.cz
 www.webhouse.cz



Tvoříme weby nejen pro veřejnou správu. Naše stránky jsou bezbariérově přístupné a splňují zákonné požadavky kladené na města a obce. Vyvíjíme redakční systém vismo Online s unikátním principem „Edituj, co vidíš“.

Wolters Kluwer ČR, a. s.

U Nákladového nádraží 6, 130 00 Praha 3
 tel.: +420 246 040 4003
 e-mail: obchod@wolterskluwer.cz
 www.wolterskluwer.cz



Wolters Kluwer patří k předním světovým vydavatelům a poskytovatelům informačních produktů a služeb. Jedním z nejznámějších produktů je znalostní systém ASPI.

Zeměměřický úřad

Pod sídlištěm 1800/9, 182 11 Praha 8
 tel.: +420 284 041 111
 ID datové schránky: 6yvadsa
 e-mail: ZU-praha@cuzk.cz
 www.cuzk.cz, www.geoportal.cuzk.cz



Zeměměřický úřad je správním úřadem zeměměřictví s celostátní působností. Ve své odborné působnosti vykonává správu geodetických základů ČR, včetně ochrany státních geodetických bodových polí, spravuje státní mapové a tematické dílo, vykonává správu ZABAGED®, zabezpečuje správu geografického názvosloví, vede Ústřední archiv zeměměřictví a katastru a provádí zeměměřické činnosti.

Český úřad zeměměřický a katastrální

Pod sídlištěm 1800/9, 182 11 Praha 8
 tel.: +420 284 041 111
 e-mail: cuzk@cuzk.cz
 ID datové schránky: uuaaatg
 www.cuzk.cz



PREZENTACE TCHAJWANSKÝCH DODAVATELŮ

Aten International Co., Ltd.

Address: 3F, No.125, Sec. 2, Datung Road, Sijhih District, New Taipei City 221, Taiwan
 tel.: +886-2-8692-6789
 fax: +886-2-8692-6767
 e-mail: marketing@aten.com
www.aten.com



ATEN, is specialized in connectivity and management solutions in accessing and sharing technologies. ATEN's SOHO and SMB solutions offer a series of cable KVM, desktop KVM, and LCD KVM products. The Enterprise solutions offer a series of Over IP solutions that allow customers to effectively manage IT infrastructure from anywhere in the world. The Professional Audio / Video line offers integrated video solutions for home and professional use for a variety of uses including corporate, education, hospitality, and commercial and home theater applications. The recently developed Green Energy line offers energy-saving solutions for the data center with a range of intelligent PDUs that provide real-time energy management and performance indicators locally and remotely. ATEN specializes in connectivity and management solutions. We distribute our products through a global sales network to meet a broad range of customer needs.

Foxconn CZ

U Zamecku 27, 530 03 Pardubice, CZECH REPUBLIC
www.foxconn.cz



Foxconn CZ was founded in 1974 in Taiwan and is a part of Hon Hai / Foxconn Technology Group. The company is a global leading provider of complex solutions in the field of IT and consumer electronics. The company has been operating on the Czech market since 2000 as a regional base for EMEA region. Its branches are situated in Pardubice, Kutna Hora and Prague. Foxconn is one of the key exporters in the Czech Republic. In 2014, it became the second largest exporter of goods worth almost 120 billion CZK. In 2015 and 2016, the company was awarded as the best employer of its region and is one of the top 3 employers in the Czech Republic. Please find more information on www.foxconn.cz.

Foxconn DRC

K Zizkovu 851, 190 00 Prague 9, CZECH REPUBLIC
www.foxconndrc.com



Foxconn DRC – Development and Research Center located in Prague with branches in Kutna Hora and Munich. The company offers digital transformation to businesses and suppliers via first-rate customer services, business effectiveness and know-how, using the latest technologies like the Internet of Things, Big Data, cloud computing, mobility, safety, united communication, etc. Foxconn DRC provides customer oriented solutions combining its skills with professional knowledge in the field of product engineering, IT services, infrastructure, management and safety. Foxconn DRC is a subsidiary of Foxconn CZ whose owner is Hon Hai / Foxconn Technology Group, Taiwan. More information on www.foxconndrc.com.

Foxconn 4Tech

Praha office: K Zizkovu 851, 190 00 Prague 9, CZECH REPUBLIC
 Pardubice office: U Zamecku 27, 530 03 Pardubice, CZECH REPUBLIC
www.foxconn.cz



Foxconn 4Tech was founded in 2015 and works on the Industry 4.0 projects. Company's vision is an absolute synergy of all industrial and cyber-physical systems, people, Internet of Things and Advanced Data Analytics. It focuses on development of smart industrial solutions in the field of automation and robotics. Internally, Foxconn 4Tech introduced an advanced industrial IoT platform which interconnects all physical and corporate devices via cloud software. Foxconn 4Tech is a subsidiary of Foxconn CZ whose owner is Hon Hai / Foxconn Technology Group, Taiwan.

Institute for Information Industry

address: 2F., No.133, Sec. 4, Minsheng E. Rd.,
 Taipei City 105, Taiwan
 tel.: +886-2-66072023, fax: +886-2-66072026
 www.iii.org.tw



Auto Fare Collection System, Hospital e-Registration System, Energy Management System

K-Jump Health Co., Ltd.

Address: No.56, Wu Kung 5th Rd., New Taipei Industrial Park, New Taipei City 24890, Taiwan
 tel.: +886-2-22991378
 fax: +886-2-22991386
 e-mail:sales@kjump.com.tw
 www.kjump.com.tw

Established in 1983, K-jump is one of the first digital human body thermometer manufacturers in Taiwan. Following years of continuous development and innovation, we have grown into a diverse biomedical electronic company and manufactured a full range of physiological monitoring devices meeting the needs of our customers. Today, our product lines include devices in body temperature care, respiratory care and cardiovascular care. We offer our customers professional service, reasonable price, reliable quality and timely delivery.

Ogreen Co., Ltd.

Address: 8F., No.32-1, Songjiang Rd., Zhongshan Dist., Taipei City 104, Taiwan (R.O.C.)
 tel.: +886-2-25673382
 e-mail.: service@ogreen.com.tw
 www.ogreen.com.tw



Ogreen provides IoT platform with high expandability, security and reliability. It provides a total solution from modules to cloud computation applications. This platform supports various devices with agile connecting to cloud, transforms into a smart device which only spends one month for remote monitoring, data collection, statistical analysis, intelligent control, and many more services. Ogreen offers hundreds of IoT products and applications in capable of creating extra-value services for your business. In our solutions, includes smart home management (In-Family), enterprise energy management (In-EMS), intelligent lighting management (In-Light) and renewable energy management (In-Solar). We hope to help and counsel enterprises to boost their product values as well as their competitiveness on the market by providing them with a comprehensive energy service.

SafeDX

K Zizkovu 813/2, 190 00 Prague 9, CZECH REPUBLIC
 www.safedx.eu



Innovative data center SafeDX was launched in 2016 by Foxconn and the international investment group KKCG. Each company owns a 50 % share. Data center SafeDX is strategically located in Prague. The company offers not only hardware, but also complex IT solutions focused mostly on foreign companies. New data center provides clients with full services, high availability and premium operational effectiveness including international connectivity. More information on www.safedx.eu.

TAITRA

address: 5-7 Fl., 333 Keelung Rd., Section 1, Taipei 11012, Taiwan ROC
 tel: +886 (2) 2725-5200, fax: +886 (2) 2757-6245
 e-mail: taitra@taitra.org.tw
www.taitra.com.tw



Rada pro rozvoj zahraničního obchodu (TAITRA), přední nezisková organizace na Tchaj-wanu propagující obchodování, byla založena v roce 1970 za účelem podporování obchodu s cizími zeměmi. Organizace TAITRA je sponzorována vládou, svazy průmyslu a několika komerčními organizacemi a pomáhá tchajwanským podnikům a výrobcům s posílením jejich mezinárodní konkurenceschopnosti a při vyrovnávání se s výzvami, kterým čelí na cizích trzích.

Od svého založení vyvinula TAITRA dobře koordinovanou informační a propagační síť složenou z více než 1200 vyškolených specialistů nacházejících se v sídle v Tchajpeji, ve čtyřech místních pobočkách v Hsinchu, Taichungu, Tainanu a Kaohsiungu, a ve více než 60 zastupitelských úřadech po celém světě.

Ve spolupráci se svými sesterskými organizacemi – Taiwan Trade Center (TTC), s.r.o., a Taipei World Trade Center (TWTC) – dělá TAITRA dále vše proto, aby přizpůsobila své strategie pro podporu obchodu měnícím se mezinárodním trendům a podmínkám. Mezi hlavní funkce a oblasti aktivit organizace patří rozvoj trhu, strategický marketing, obchodní informační služby, výstavy, kongresové služby, vzdělávání a TaiwanTrade (služba virtuálního centra obchodování).

V dynamické ekonomice Tchaj-wanu lze nalézt obrovské obchodní příležitosti. Strategická poloha, infrastruktura a kapitál dělají z ostrova ideální odrazový můstek pro obchodní aktivity v Asii a okrajové části Tichomoří. Organizace TAITRA je spolu se svými zkušenými obchodními specialisty připravena vám pomoci obchodovat s Tchaj-wanem.

TATUNG CO.

Address: 22, Chungshan N. Rd., 3rd Sec., 10435 Taipei, Taiwan
 tel.: +886-2-25925252 ext. 2813
 e-mail: astley1@tatung.com
www.tatung.com



Tatung Company established in 1918 headquartered in Taipei, evolved into a conglomerate from its substantial heritage. Tatung is also a leading brand for energy saving and related system in Taiwan. Our specialized smart solutions can be easily applied to smart community, smart energy.

POŘADATELÉ

TRIADA, spol. s r. o.

U Svobodárny 1110/12, 190 00 Praha 9-Libeň
tel.: +420 284 001 284, fax: +420 284 818 027
e-mail: info@triada.cz
www.triada.cz



Pobočka Brno:
Cejl 72, 602 00 Brno
tel.: +420 545 210 549, fax: +420 545 210 549



Vzdělávací instituce akreditovaná MV ČR; www.triada.cz



Munis – informační systémy pro města a obce; www.munis.cz
iMunis SMiS – portál obce pro komunikaci s občany; www.imunis.cz



OBEC & finance – odborné periodikum pro ekonomické otázky měst a obcí
Veřejná správa online – příloha zaměřená na ICT technologie ve veřejné správě
www.obecafinance.cz



Den malých obcí – pravidelné setkání starostů malých obcí s představiteli
státní správy a dalšími odborníky nad aktuálními problémy
www.denmalychobci.cz



Deník veřejné správy – konference, semináře a školení pro pracovníky ve veřejné správě
www.dvs.cz



Solon – legislativní a metodická podpora pracovníků veřejné správy
www.solon.cz

Český zavináč z.s.

U Svobodárny 1110/12, 190 00 Praha 9
tel.: +420 284 001 284, fax: +420 284 818 027
www.ceskyzavinac.cz



PONCA spol. s r. o.

Drahobejlva 1142/34, 190 00 Praha 9
www.ponca.eu



PROGRAMOVÝ VÝBOR A REALIZAČNÍ TÝM KONFERENCE ISSS/V4DIS 2017

PROGRAMOVÝ ŘEDITEL

Mgr. Vojtěch Dvořáček

PROGRAMOVÝ VÝBOR

RNDr. Tomáš Renčín

předseda programového výboru

Mgr. Zdeněk Zajíček

ICT UNIE, o. s.

Ing. Petr Pavlínek

Krajský úřad kraje Vysočina

Ing. Ivo Bělonohý

Sdružení tajemníků městských a obecních úřadů

Ing. Pavel Rous

Magistrát města Kladna

Ing. Cyril Čapka

Komise pro informatiku Svazu měst a obcí ČR

Mgr. Tomáš Lechner, Ph.D.

Vysoká škola ekonomická v Praze

REALIZAČNÍ TÝM

RNDr. Tomáš Renčín

výkonný ředitel konference

Mgr. Vojtěch Dvořáček

programový ředitel konference

Marek Zubr

asistent

Blanka Brychtová

manažer konference, organizační zajištění

PhDr. Prokop Konopa

manažer komunikace

Kateřina Pánková

manažer pro VIP hosty, redakce sborníku

Mgr. Jan Brychta

technické zabezpečení

Simona Češková

registrace účastníků, doprava

Ing. Arnošt Hanzl

organizační zajištění

Roman Falhar, DiS.

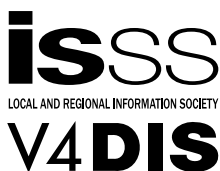
soutěže, ubytování

Ing. Petr Palisa

webmaster, PPT prezentace,

JUDr. Ing. Antonín Eliáš

časopis OBEC & finance



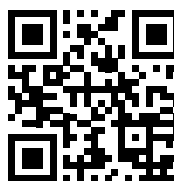
SEKRETARIÁT KONFERENCE

U Svobodárny 1110/12, 190 00 Praha 9

tel.: +420 284 001 284

e-mail: sekretariat@issc.cz

www.issc.cz



M.ISSC.CZ



WWW.V4DIS.EU