Egovernment

elektronizace veřejné správy

„Žijem si jak na zámku, ať to trvá věčně.“

KONFERENCE MIKULOV e-government

GDPR: nová pravidla ochrany osobních dat

www.egovernment.cz

č. 3/2017

Pořádná ochrana je skutečně důležitá

Ano, přesně to si zřejmě myslí i Evropská unie, a proto zatížila dodržování ochrany osobních údajů pokutami zdánlivě až astronomickými. Ale upřímně, není se co divit. Data jsou dnes vysoce atraktivní zboží, a jsou-li těmi daty osobní údaje, pak se jejich atraktivita násobí. Z osobních údajů se totiž dá vyčíst kdeco. I to, co čteme, co si myslíme, kolik vyděláváme, koho máme či nemáme rádi, vlastně obecně, jací jsme. Z osobních údajů se dokonce dá leckdy vyčíst i to, o čem my, „subjekty těchto údajů", nemáme ani ponětí.

Nejde tady ale primárně pouze o ochranu údajů samotnou, takříkajíc jen pro to, abychom si mohli říci, že naše data jsou v bezpečí. Už totiž skutečně „přestává sranda" a „jde do tuhého". I přes naše, někdy možná až rozpačité přešlapování, které dokládá pozice České republiky v rámci světových i evropských žebříčků s tématem e-governmentu, jsme nyní nuceni udělat řadu kroků, které, doufejme, budou znamenat definitivní naplnění hesla „obíhat mají data, nikoli občané ". Na spadnutí je totiž úplné elektronické podání, tedy situace, kdy skutečně budeme, a doufejme že technicky bez komplikací, moci realizovat svá podání vůči veřejné správě jednoduše, intuitivně, a to tak, že se identifikujeme elektronicky. Veřejná správa si elektronicky „natáhne" všechna potřebná data, která o nás vlastní a k danému podání je potřebuje, a podání následně zpracuje. Zbytečné dodávat, že i ono zpracování bude elektronicky a elektronicky budeme následně o jeho zpracování vyrozuměni. To bude krása. A to největší kouzlo spočívá v tom, že tak budeme moci činit nejen směrem k naší veřejné správě, ale vlastně ke všem úřadům v rámci EU. Tedy do celkem 28 zemí a všude budou muset stejně reagovat.

Podstatou fungování je ale skutečnost, že budou k dispozici všechna potřebná data (o nás). A to jsou právě ony osobní údaje. A my, jakožto subjekty těchto údajů, bychom zase byli rádi, kdyby v žádné z těch 28 zemí, tedy nejen tady u nás, nedošlo k jejich zneužití, pozměnění, nebo snad i vymazání. Když se na to podíváme tak, že jde o celkem 510 milionů obyvatel EU a uvedená pokuta by měla tak nějak vyjadřovat hodnotu jejich osobních údajů, pak vězte, že osobní data každého z nás stojí 51 euro, tedy nějakých 1500 Kč. To je vlastně za babku.

Ing. Michal Jirkovský
šéfredaktor

Obsah

V rámci České a Slovenské republiky vydává:

info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
ISSN 1801-9420

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Patricie Stránská

Grafika: PROPAGANDA, Malá Štupartská 7, Praha 1
Tiskárna: A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
Registrační číslo: MK ČR E 11364

Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**. Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **100 Kč (4 EUR)** bez DPH**/výtisk, tj. 400 Kč (16 EUR)** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

Magazín Egovernment pořádal letos už po deváté konferenci e-government 20:10 aneb žijem si jak na zámku, ať to trvá věčně, která se každoročně věnuje aktuální situaci v oblasti elektronizace veřejné správy v ČR. I letos jsme se sešli na zámku Mikulov a po dva dny prezentovali a diskutovali o všem, co je z pohledu e-governmentu podstatné.

Téměř 800 účastníků mělo možnost sledovat vystoupení plenárního bloku, kde převažovaly informace z Ministerstva vnitra, odpolední sekce, které daly prostor pro představení konkrétních projektů, i workshop druhého dne, který byl zaměřen na oblast GDPR a elektronickou identifikaci. Tato dvě témata však z pochopitelných důvodů přesáhla rozměr workshopu a prolínala se všemi částmi odborného programu. Vystoupení hlavní části konference bylo možné sledovat přímo v hlavním sále, nebo s ohledem na zájem, který převyšoval kapacitu sálu, na velkoplošných obrazovkách v Grolově sále v horní části zámku. Pauzy mezi jednotlivými částmi programu pak bylo možné prožít na prosluněné terase s občerstvením a nádherným výhledem na Svatý kopeček.

Na následujících stránkách naleznete pasáž, která je věnována právě vystoupením v úvodním, plenárním bloku konference. Část GDPR, tedy hlavní vystoupení druhého dne konference, je popsána od strany 24.

Konferenci, která se tradičně koná pod záštitou ministra vnitra, hejtmana Jihomoravského kraje a starosty města Mikulov zahájil **náměstek ministra vnitra pro řízení sekce ICT JUDr. Jaroslav Strouhal**. Ve svém vystoupení se snažil poukázat především na kroky, které se podařilo realizovat, ať již samotnému MV ČR, nebo ve spolupráci s Asociací krajů ČR. Jednalo se především o jednotlivé legislativní kroky, které jsou podstatné především s ohledem na realizaci elektronické identifikace. Ta se v současné době stává vysoce aktuální a i díky ní se blíží naplnění heslo: "obíhat mají data, nikoli občané", čemuž by měl napomoci Portál občana, který rovněž náměstek Strouhal zmínil.

Hejtman Kraje Vysočina MUDr. Jiří Běhounek tentokráte reprezentoval především **komisi rady AK ČR pro informační technologie ve veřejné správě**. Velké poděkování vyslovil právě informatikům jednotlivých krajů a prezentoval několik zásadních projektů i momentů v rámci krajské informatiky, na kterých se KI podílela, stejně jako nejbližší plánované aktivity. Ve svém projevu ale upozornil na leckdy velmi špatnou vzájemnou komunikaci mezi jednotlivými institucemi v oblasti e-governmentu a pozici MV ČR vůči ostatním resortům, kterou není možné nazvat vůdčí.

Další z náměstků MV ČR **JUDr. PhDr. Petr Mlsna, náměstek pro řízení sekce legislativy, práva, archivnictví a správních agend**, referoval nejprve o završení téměř desetiletého období práce na elektronické Sbírce zákonů a elektronické legislativě, které jak se zdá, se podařilo dovést úspěšně ke konci. Obsáhleji se pak věnoval tématu GDPR a podrobně především novému zákonu, respektive novele zákona č. 101/2000 Sb., o ochraně osobních údajů. V souvislosti s návrhem GDPR upozornil na skutečnost, že zřejmě největší novinkou bude tzv. výkladová praxe, neboť samotné nařízení, dle jeho mínění, neposkytuje odpovědi na řadu otázek, bylo tedy nutné ustanovit pracovní skupinu, která bude poskytovat odpovědi v podobě vlastních výkladů.

Ředitel odboru e-governmentu MV ČR Ing. Roman Vrba se věnoval tématu Procesního modelování agend, a to mimo jiné proto, že se jedná o projekt, který by měl popsat veřejnou správu. To je podle Romana Vrby velice důležité pro další vývoj elektronizace veřejné správy. Aby se skutečně ubíral přívětivě směrem k občanovi, je velice nutné sestavit tzv. Katalog služeb, který může být následně

podporou Portálu občana či aplikací typu Co dělat když?, kterou rovněž svojí prezentací představil. Jako druhé prezentované téma si Roman Vrba vybral informační registr smluv, a především pak náměty na jeho změny a úpravy. Obojí je totiž podle něj podstatné pro posun v rámci e-governmentu, ke kterému se schyluje.

Hlavní architekt e-governmentu Ing. Petr Kuchař a ředitel Správy základních registrů Ing. Michal Pešek si připravili společné vystoupení, které každému z nich dalo prostor pro prezentaci „jeho" půlky tématu. Petr Kuchař tedy především připomněl historii a princip fungování Útvaru hlavního architekta s tím, že stěžejní téma bylo schvalování projektů ICT ve veřejné správě. Z uvedeného vyplynulo, že se vlastně jedná o určitou konzultantskou činnost, kdy je dobré, aby žadatel byl s ÚHA v kontaktu už před podáním žádosti tak, aby mohl konkrétní detaily dolaďovat. Podání žádosti je totiž z pohledu Petra Kuchaře vlastně již finálním krokem. Michal Pešek na doklad řečeného prezentoval projekt Základní registry 2.0, který takovouto popsanou spoluprací prošel i s ohledem na očekávanou zvýšenou zátěž například díky Národní identitě.

Ředitel odboru kybernetické bezpečnosti a koordinace ICT MV ČR Ing. Miroslav Tůma se, především na základě požadavků, které jeho odbor obdržel, jal vysvětlovat dopady novely zákona o kyberbezpečnosti. Hovořil jak o změnovém zákonu č. 104/2017 Sb., tak o zákonu č. 205/2017 Sb. Hovořil konkrétně o tom, co tyto zákony zavádějí a blíže vysvětloval, co je přesně základní služba, co digitální služba, jaké jsou povinnosti správců a provozovatelů a na jakých principech by se měla vytvářet bezpečnostní dokumentace, přičemž prezentoval všech 21 bezpečnostních politik definovaných zákonem. Pro všechny tyto účely přítomným zobrazil návodné tabulky, které by jim při řešení této problematiky měly být nápomocné. Na závěr ještě upozornil na e-learnignový kurz s tématem kybernetické bezpečnosti, který společně realizuje NÚKIB, MV ČR, Úřad vlády ČR a Institut pro veřejnou správu ČR.

Prezident ICT Unie Mgr. Zdeněk Zajíček si na podporu svého vystoupení vzal nedávné, nijak povzbudivé výsledky porovnání ČR v oblasti elektronizace veřejné správy se světem i s Evropou. Jak řekl, domnívá se, že v zásadě bychom mohli být v čele těchto žebříčků a jediné, co tomu brání, je jisté legislativní vězení, v němž se nacházíme. Důležité je podle jeho slov, začít se dívat na celou oblast očima klienta veřejné správy a jeho potřeb, respektive práv. Následně poukazoval na některá práva, na která už v současné době občan v souvislosti s elektronizací má nárok a která nejsou k dispozici buď proto, že pro to nejsou legislativní podmínky, nebo i proto, že není chuť takto téma vnímat.

Prezentace a fotogalerie z konference v Mikulově k dispozici na **www.egovernment.cz sekce MIKULOV**.

e-government 20:10
aneb žijem si jak na zámku, ať to trvá věčně
MIKULOV • 5. - 6. 9. 2017

Co se podařilo

Náměstek pro ICT JUDr. Jaroslav Strouhal připomněl v úvodu svého vystoupení, že předešlý rok, kdy se v Mikulově obsáhle diskutovalo o nařízení eIDAS, zde hovořil o tom, že k jeho naplnění bude nutné vytvořit právní rámec, který by umožňoval občanům zprostředkovat elektronické transakce vůči veřejné správě prostřednictvím jakési elektronické samoobsluhy. Dnes může potvrdit, že bylo skutečně nutné přijmout řadu zákonů reflektujících nařízení Evropské komise o elektronické identifikaci a službách vytvářejících důvěru a rád referuje o tom, že se to vše podařilo.

Jednalo se především o:

1. **Zákon o službách vytvářejících důvěru v rámci elektronických transakcí**, který nabyl účinnosti v průběhu loňského roku. Jak náměstek Strouhal uvedl, jedná se o zákon, který upravuje elektronický podpis a otázky kolem pečetě elektronických dokumentů a je pro realizaci elektronických transakcí vůči veřejné správě nezbytným;
2. **Zákon o elektronické identifikaci**, jenž je druhou, relativně čerstvou právní normou, která je pro eIDAS důležitá. Podle Jaroslava Strouhala zde taková právní norma doposud skutečně chyběla. Pozitivně hodnotní především skutečnost, že vznikla ve velice krátké době, neboť se o záměru takového zákona začalo hovořit přesně před rokem, tedy v průběhu loňského září. Za pomoc a spolupráci v tomto směru poděkoval především hejtmanovi Kraje Vysočina Jiřímu Běhounkovi a iniciativě 202020;
3. **Novelu zákona o elektronických průkazech**, která je podle náměstka Jaroslava Strouhala posledním legislativním příspěvkem MV ČR ke zdárnému fungování elektronické identifikace. Tato norma nabude účinnosti 1. 7. 2018 a bude umožňovat výměnu současných občanských průkazů za nové elektronické s čipem, a to zdarma.

I když jsou toto vše velice důležité legislativní kroky, samy o sobě by nestačily k tomu, aby řádně fungovaly uvedené instituty elektronické identifikace a komunikace s veřejnou správou. I proto v rámci odboru e-governmentu probíhají intenzivní práce na přípravě portálu občana. MV ČR jej plánuje spustit v rámci testovacího provozu na konci letošního roku a mělo by se jednat o určitý rozcestník, nebo „samoobsluhu", jejímž prostřednictvím bude moci občan obsluhovat agendy veřejné správy z pohodlí svého domova.

V souvislosti s backoffice českého e-governmentu je podle Jaroslava Strouhala dobré zmínit **Útvar hlavního architekta**. Vznikl před dvěma a půl roky a i díky jeho práci postupně došlo k masivnímu nárůstu vyřízených žádostí v souvislosti s IT projekty. Náměstek Strouhal vidí přidanou hodnotu Útvaru hlavního architekta především v tom, že poprvé se dá v rámci IT projektů ČR hovořit o tom, že jsou v pořádku, schvalovány podle jednotného architektonického plánu a jednotných pravidel. Zdůraznil ještě, že se postupně daří zbavovat IT projekty jejich negativní nálepky, kterou získaly v průběhu předchozích období v souvislosti s nejasnými průběhy některých výběrových řízení. Zároveň došlo, podle jeho slov, k úspoře 100 mil. Kč, a to v rámci podaných žádostí díky odhalování duplicit IS u stejného úřadu.

Jaroslav Strouhal považuje ještě za důležité zmínit i téma **Open Dat**, neboť se tuto problematiku podařilo ukotvit do českého právního řádu, a to v rámci **zákona o svobodném přístupu k informacím**. V současné době funguje v ČR národní katalog Open Dat, a to jako součást portálu MV ČR, ve kterém je zveřejněno několik tisíc datových sad.

Pohled krajů

Hejtman Kraje Vysočina a předseda komise rady AKČR pro informační technologie ve veřejné správě MUDr. Jiří Běhounek v úvodu svého vystoupení poděkoval především všem pracovníkům IT v krajích za jejich podíl na dosavadním vývoji krajské informatiky. Zároveň upozornil, že zdaleka ne všichni z nich mají pro svoji práci ideální podmínky a zdaleka ne ve všech krajích je oblasti IT věnována dostatečná pozornost.

V rámci stručné historie krajské informatiky uvedl několik zásadních momentů a projektů, na kterých se KI podílela. Jednalo se například o:

2014

- CMS – krajské konektory, registr sítí, memorandum o spolupráci s MV ČR,
- krajské digitální spisovny, projekt krajských videokonferencí;

2015

- DTM – digitálně technické mapy krajů,
- NAP – národně architektonický plán (MV ČR),
- NGA sítě (MPO).
- vznik projektu Kraje pro bezpečný internet (KBI),
- NIS IZS;

2016

- rejstřík přestupků,
- CMS 2.0 a služby samosprávy,
- výzvy IROP,
- eHEALTH (MZd),
- NIX.ZD.

Jiří Běhounek připomněl, že v roce 2013 zpracovala KI AKČR vlastní Strategii rozvoje informačních a komunikačních technologií regionů na období 2013–2020, která definovala společnou vizi krajů v této oblasti: **„Udržitelný rozvoj ICT zvyšující kvalitu a efektivitu výkonu veřejné správy a podporující rozvoj, spolupráci a konkurenceschopnost regionů."** V této souvislosti upozornil především na skutečnost, že sice probíhá intenzivní spolupráce s ostatními složkami státní a veřejné správy, ale rozhodně není vyrovnaná a stejně intenzivní a vstřícná se všemi.

Ve vztahu k roku 2017 a 2018 je z pohledu jejího předsedy pro krajskou informatiku důležité vyřešit tyto aktivity:

- NGA jednání s MPO po zapojení samospráv do OPPIK – výstavba NGA;

MUDr. Jiří Běhounek

- BEZPEČNOST – GDPR, KPBI, ZKB – VIS provozované kraji, organizacemi krajů;
- CMS 2.0 a KIVS – využití služeb CMS 2.0, KIVS zakázky – respektování memoranda o sdílení sítí veřejné správy (nefunguje ani s MV ani s MPSV);
- eGOV služby – portál občana, NIA, eOP, eHEALTH (ve všech těchto oblastech především očekávají, jaké budou další kroky odpovědných institucí).

Ve všech uvedených oblastech je, jak Jiří Běhounek zdůraznil, nutné vést další jednání a především zjistit, jaké jsou představy konkrétních odpovědných institucí. Pravdou je, že řadu věcí se už podařilo realizovat, ale je důležité, aby obce a úřady dostávaly do rukou, místo obecných proklamací, jasnou představu o tom, co a jak mají dělat, co kdy bude spuštěno atp.

Za zcela zásadní problém Jiří Běhounek označil komunikaci, respektive žádnou komunikaci mezi jednotlivými institucemi v oblasti e-governmentu a jeho projektů. Nejen, že nejsou schopny se shodnout navzájem, ale problém je podle něj především v tom, že u nás neexistuje jednotící směr, jasné stanovisko, a především, že MV ČR nemůže takový jednotící směr ostatním resortům nařídit. I proto se posouváme v oblasti elektronizace veřejné správy kupředu daleko pomaleji, než by bylo skutečně možné.

Jiří Běhounek doufá, že bez ohledu na výsledek voleb se i nadále budou všichni zainteresovaní do rozvoje e-governmentu snažit posunout jej dál. Jak zdůraznil, byl by rád, kdybychom k tomu všichni nalezli chuť i sílu.

Elektronická sbírka zákonů a GDPR

Vzhledem k tomu, že v minulém roce musel náměstek JUDr. PhDr. Petr Mlsna své plánované vystoupení na konferenci v Mikulově na poslední chvíli zrušit, vrátil se nejprve k tématu, které chtěl tehdy prezentovat, a to elektronické sbírce zákonů a elektronické legislativy.

Jak uvedl, sliby a představy v této oblasti se podařilo dotáhnout do konce, když byl přijat zákon o elektronické sbírce zákonů a elektronické legislativě a především byla vypsána veřejná zakázka na implementaci projektů legislativy a e-sbírky a na verifikaci datové báze.

Podle jeho slov poběží tato zakázka až do poloviny listopadu a domnívá se, že tímto krokem se skutečně podařilo splnit sliby, s nimiž Ministerstvo vnitra vstupovalo do právě končícího funkčního období. Je to podle jeho mínění uzavření jakéhosi desetiletého období, neboť poprvé byla tato idea otevřena v roce 2007. Nyní se tedy podařilo dokončit mimořádně složitý projekt nejen z pohledu kyberbezpečnosti, ale například i množství modalit, které mohou v rámci legislativního procesu České republiky nastat.

GDPR

Po tomto návratu ke svému tématu loňského roku se věnoval aktuální problematice GDPR, tedy legislativě na ochranu osobních údajů a volnému pohybu těchto údajů v rámci EU. Jak zdůraznil, nejedná se o zásadní téma pouze z pohledu veřejné správy, ale rovněž soukromého sektoru. Evropská unie tímto nařízením zcela změnila koncepci ochrany osobních údajů oproti modelu, který obsahovala norma z roku 1998. Uvedl, že je to logické, neboť takto stará norma nemohla reflektovat některé aktuální požadavky typově, jako např. právo být zapomenut v digitálním prostředí atp.

GDPR je podle slov náměstka Mlsny vnímáno, možná poněkud neprávem, trochu odtažitě. Přitom ale pouze zahrnuje to, co zde už reálně existuje a co vnímáme jako dané, i když nikoli doposud legislativně upravené. Evropská unie schválila nařízení č. 679 v dubnu 2016 poněkud ve skrytu ostatních velkých témat, kterými byla migrace a bezpečnost. Implementační lhůta nařízení je poměrně krátká, protože 25. 5. 2018 musí být toto nařízení promítnuto v právních řádech členských zemí. Pro nás je to podle náměstka Mlsny o to obtížnější, že se nacházíme na přelomu legislativních period, tedy v období voleb do

JUDr. PhDr. Petr Mlsna, PhD., *náměstek ministra vnitra pro řízení sekce legislativy, práva, archivnictví a správních agend, pověřený řízením sekce veřejné správy*

Poslanecké sněmovny. A tak, byť MV ČR má připraven nový zákon o zpracování osobních údajů, který by měl ten stávající nahradit, nemáme, kdo by jej schválil.

NÁVRH MVČR

V souvislosti s novým návrhem zákona náměstek Mlsna uvedl, že byla zvolena nová koncepce odlišná od stávajícího zákona č. 101/2000 Sb. Především nový zákon o ochraně osobních údajů by měl rozpracovávat pouze to, co není přímo upraveno daným evropským nařízením. Jak uvedl, nařízení EU je přímo použitelné a vykonavatelné, a tedy není nutné jej popisovat duplicitně. Nový zákon se tak bude věnovat především úpravě ochrany osobních údajů v situacích, na které obecné nařízení EU přímo nedopadá:

- činnosti, které nejsou evropským právem regulovány a jsou výhradně v působnosti jednotlivých členských států;
- společná zahraniční a bezpečnostní politika na ochranu osobních údajů, kde se budou jednotlivé státy nadále řídit vlastními pravidly;
- předcházení, odhalování a stíhání trestných činů;
- evidence cestujících (primárně v letecké dopravě).

Pokud bude návrh zákona schválen novou sněmovnou, měl by obsahovat především tyto zásady:

- zákonnitosti – osobní údaje by měly být zpracovány na základě zákonného titulu, korektně a transparentně;

- účelové omezení - osobní údaje by měly být shromažďovány pouze pro jasně a legitimně a dopředu definované účely;
- minimalizace údajů – shromažďovat pouze množství údajů omezené na nutné minimum ve vztahu k definovanému účelu.

Jak dále náměstek MIsna uvedl, veškeré osobní údaje by měly přesné, aktuální, uloženy tak, aby bylo možné identifikovat subjekty údajů pouze po dobu nezbytně nutnou pro daný účel. Zabezpečena musí být rovněž integrita důvěrnosti, tedy zajištěna jejich náležitá ochrana. Správce osobních údajů musí pak vycházet z tzv. zásady odpovědnosti a musí zajistit, aby všechny uvedené principy byly skutečně v praxi dodržovány.

VÝKLAD ZÁKONA

V souvislosti s nařízením EU náměstek MIsna uvedl, že patrně největší novinou bude tzv. výkladová praxe. Samotné nařízení totiž podle něj neposkytuje odpovědi na řadu otázek, proto byla ustavena pracovní skupina 29 (WP29). Jedná se o evropský sbor pro ochranu osobních údajů, který by měl jednotlivé problematické oblasti rozpracovávat svými právními výklady. Náměstek MIsna se domnívá, že toto bude klást zvýšené nároky především na ustavení a výkon pověřenců na ochranu osobních údajů, především pak na jejich znalosti.

Jako určitý doprovodný prvek přípravy nového zákona by podle slov náměstka pro legislativu byla vhodná rovněž diskuze na téma struktury ÚOOÚ jakožto dozorového orgánu. Pojetí úřadu v současné podobě považuje za zastaralé, především pak skutečnost, že dozorovou činnost má napříč nejrůznějšími segmenty vykonávat jen několik málo osob, jejichž výběr navíc podléhá politickému mechanismu, neboť inspektoři jsou jmenováni prezidentem ČR na návrh senátu. Ministerstvo vnitra se tedy podle jeho slov snaží navrhnout koncepci úřadu jako klasického správního úřadu, v němž jsou úředníci vykonávající dozorovou činnost jmenováni podle zákona o státní službě s příslušnými zákonnými kritérii.

SPRÁVCE

Nařízení GDPR definuje správce jako fyzickou, nebo právnickou osobu, jako OVM, agenturu či jiný subjekt, který sám či společně s jinými určuje účel i prostředky zpracování údajů. Na základě této definice vzniká správci řada povinností, jako vést záznamy o činnostech, které ve vztahu ke zpracování osobních údajů činil, posuzovat vliv těchto kroků na ochranu osobních údajů, vést konzultace (například s ÚOOÚ), ohlašovat případy porušení zabezpečení ochrany osobních údajů a také ustanovit pověřence na ochranu osobních údajů. To je podle náměstka MIsny zcela zásadní moment. Ke zřízení této funkce musí podle jeho slov dojít v okamžiku, kdy:

1. zpracování osobních údajů provádí orgán veřejné moci, nebo veřejný subjekt;
2. hlavní činnost správce nebo zpracovatele OÚ spočívá v rozsáhlém systematickém monitorování;
3. správci zpracovávají citlivé OÚ

POVĚŘENEC

Zcela novou funkcí, kterou nařízení GDPR přináší, je pověřenec na ochranu osobních údajů. Odpovědět přesně na otázku, co by měl dělat **pověřenec na ochranu osobních údajů**, není podle náměstka MIsny úplně jednoduché. MV ČR v tomto směru komunikuje s ÚOOÚ, který čeká na výklad z EU, jenž by podle všeho měl nyní přijít díky WP29. Jak náměstek MIsna uvedl, není úplně optimální, když pro takto důležitou a náročnou funkci přijdou pokyny až na poslední chvíli, ale přesná metodika bohužel k dispozici v tomto směru skutečně není. Obecně platí, že pověřenec by měl poskytovat určité poradenství směrem ke správci, zpracovateli i samotným zaměstnancům, kteří s osobními údaji nakládají. Zároveň by měl monitorovat, zda nakládání s osobními údaji a jejich zpracování v rámci daného správce odpovídá zákonem stanoveným kritériím a podmínkám. Pokud by měl najít nějaké přirovnání, pak je v případě pověřence možné hovořit o určité formě vnitřního auditu.

PODKLADY

I když v případě pověřence není ještě informací dostatek, obecně platí, že metodické pokyny je možno dohledat na stránkách ÚOOÚ (www.uoou.cz sekce GDPR), a to v českých překladech. MV ČR vydalo vlastní pokyny, které jsou určeny především samosprávě. Jak zdůraznil, vyplývá z nich především to, že není nutné, aby každá obec měla svého vlastního pověřence. Samozřejmě záleží na velikosti a rozsahu agendy, ale bezpochyby je možné, aby v případě menších obcí mělo deset až patnáct obcí jednoho společného (externího) pověřence. Náměstek MIsna považoval za důležité upozornit, že i v případě nejmenších obcí dochází k nakládání s osobními údaji (rybářské lístky, spolkové činnosti ...). I proto je nutné, aby i ty nejmenší obce věnovaly tématu dostatečnou pozornost.

Multiagendový přístup

Roman Vrba zahájil své vystoupení v Mikulově výčtem toho, o čem všem by mohl mluvit, protože, zajímavých témat je v oblasti elektronizace veřejné správy skutečně hodně. Vybral nakonec jen několik aktuálních.

PROCESNÍ MODELOVÁNÍ AGEND

Projekt PMA je podle Romana Vrby historicky jedním z nejlepších projektů elektronizace veřejné správy. I když obecně není možná příliš pozitivně vnímán, je velice důležitým a dává v sobě určitou naději, že se podaří popsat, jak funguje veřejná správa. Výsledky tohoto projektu tedy považuje Roman Vrba za velice důležité pro další vývoj e-governmentu.

Podstatou, či podnětem pro procesní modelování je skutečnost, že občan je vnímán jako klient veřejné správy, kterému se snažíme usnadnit jeho běžné problémy. Každý občan průběžně řeší různé životní situace, životní události, a právě jejich prostřednictvím je velice důležité se na veřejnou správu dívat. Občané podle Romana Vrby takto na problém nahlížejí, zajímají je události, které potřebují řešit, nikoli agendy, které jsou uvnitř veřejné správy. Naproti tomu úředník, sevřený legislativou, vnímá především „svoji" vlastní agendu a příliš se nestará o to, jak funguje jiná agenda a jestli k ní má nějaký vztah či nikoliv. Podstatný je tedy pohled prostřednictvím konkrétní události, která bývá většinou multiagendová. Roman Vrba připustil, že tento multiagendový přístup byl již v minulosti popsán, ale fakticky nebyl nikdy dopracován tak, aby existovala „mapa" veřejné správy.

Jako určitý příklad události, která k vyřešení potřebuje řadu agend, je tedy multiagendovou událostí, uvedl narození dítěte. V souvislosti s touto událostí je nutné řešit sociální dávky, matriku, zdravotní pojišťovnu atp. To nejsou jednoduché úkony. Je však nutné si uvědomit, že i v případě, kdy každou tuto agendu elektronizujeme tak, že ji vybavíme elektronickým formulářem, občanovi jeho situaci příliš neulehčíme, stále bude stejně ztracen. Je nutné mu popsat životní událost a služby, které jsou v jejím rámci k dispozici a dále jaké agendy jsou na tyto služby navázány. Z pohledu veřejné správy je nutné identifikovat jakési pojítko (službu) mezi konkrétní agendou a konkrétní životní situací. Služby, které jsou tím pojítkem, by měly být agregované, a jak Roman Vrba připustil, identifikovat vztah mezi jednotlivými agendami nebude v některých případech zdaleka jednoduché.

Roman Vrba, ředitel odboru eGovernmentu MV ČR

Jako důkaz uvedl životní situaci, kdy žena díky sňatku změní příjmení. Je zřejmé, že následně musí vyměnit své doklady - OP, řidičský průkaz, pokud je vlastníkem vozidla, pak i jeho TP, cestovní pas atp. Roman Vrba uvedl, že tento proces máme popsán na základě vlastních zkušeností, nikoliv však systémově. Skutečně platí, že nemáme systémově popsány jednotlivé životní situace. Proto je cílem MV ČR tento popis dokončit a následně služby a agendy propojit a některé procesy, je-li to možné, automatizovat. Právě uvedená výměna průkazů v případě sňatku by mohla například startovat automaticky, neboť je zřejmé, že nastala tato životní situace, veškeré potřebné údaje (včetně fotografie) jsou veřejné správě k dispozici, a tak by si nevěsta mohla přijít už jen vyzvednout doklady, pokud možno všechny na jedno místo. To je ideální představa, a jak Roman Vrba upozornil, nikoli nereálná.

KATALOG SLUŽEB

Z uvedených důvodů MV ČR sestavuje Katalog služeb, který by měl být nástrojem poznání výkonu veřejné správy. Zároveň je podle Romana Vrby důležité na něj nahlížet jako na informační zdroj pro návrhy optimalizací služeb a rovněž jako databázový zdroj pro Portál veřejné správy a Portál občana. V této souvislosti je důležité, že je vytvářen z centra MV ČR. Zároveň je ale tvořen ve spolupráci s obcemi, tedy i zespodu, a ve spolupráci s gestory agend, tedy i horizontálně. Jedině tímto způsobem je podle Romana Vrby možné popsat fungování výkonu agend v území.

Výsledkem by měla být jakási karta služby, na jejímž vyplňování se pracuje, a výsledek by měl být uložen v RPP.
Jako určitou možnost výstupu směrem k občanům ukázal Roman Vrba aplikaci CO DĚLAT KDYŽ? Na příkladu životní situace ZMĚNA BYDLIŠTĚ demonstroval celkem jednoduchý a návodný způsob, jakým aplikace s uživatelem komunikuje a přivede jej ke způsobu řešení jeho situace. Připustil, že není vše ještě odladěno, nicméně aplikace je již k dispozici jak na GOOGLE STORE, tak na APP STORE. MV ČR očekává reakce, na jejichž základě bude aplikaci postupně odlaďovat, tedy doporučení, co změnit, o co aplikaci obohatit atp. Podle Romana Vrby pouze takováto „komunitní" spolupráce může vést ke skutečně funkčnímu modelu, který občanovi pomůže v konkrétní situaci. Nejde tedy o vytvoření obrovského množství údajů, úkonů a agend v elektronické podobě, ale jejich funkční propojení a vytvoření snadné a srozumitelné nabídky.

INFORMAČNÍ SYSTÉM REGISTR SMLUV

Druhé téma, které si Roman Vrba pro své vystoupení na konferenci v Mikulově vybral, byl Informační systém registru smluv. Jak uvedl, celkově bylo zveřejněno 700 000 smluv, a proto graficky demonstroval zkušenosti z provozu.

Pravým důvodem pro prezentaci ISRS jsou podle něj ale náměty na jeho změny. Jak připustil, sešlo se jich je docela velké množství. V Mikulově prezentoval jen některé z nich, například:

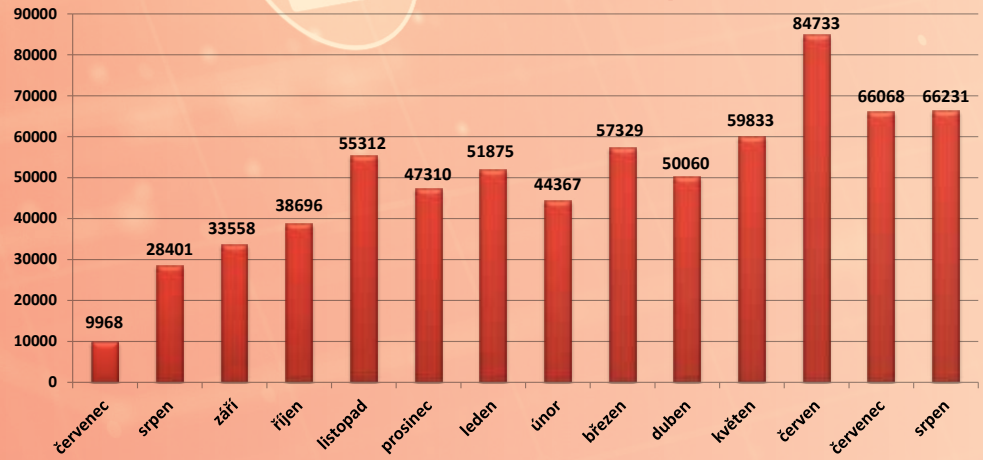
- umožnit znepřístupnit zveřejněnou přílohu, pokud obsahuje osobní údaje, obchodní tajemství apod., případně ji nahradit jinou verzí;
- změna formátu potvrzení na PDF/A tak, aby byl v souladu s § 23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, v důsledku nařízení eIDAS by to mělo být konkrétně ve formátu PDF/A 2b;
- zjednodušení pravidel zveřejňování

– názvy souborů,

– vyhodnocování pokynů podle obsahu;

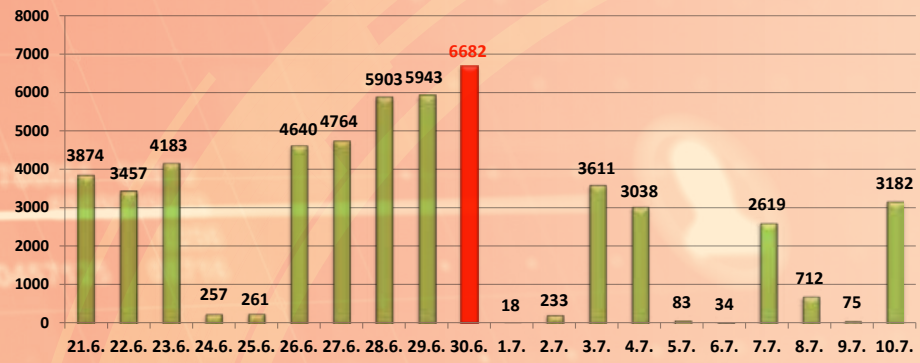
- třídění výsledků vyhledávání podle různých kritérií (např. datum zveřejnění, název subjektu apod.), tedy podle všech sloupců;
- oboustranné provázání záznamů (např. smlouva a dodatek);
- rozšíření statistických přehledů (souhrny hodnot smluv, statistiky stahování open dat);
- nerozlišitelné „skryté údaje", fyzická osoba, zahraniční subjekt - řešení = dodatečný subjekt;
- nejednoznačná identifikace smluvních stran tam, kde je to možné; nepřesná metodika identifikace smluvní strany – řešení = MV metodiku doplní o doporučení/povinnost zadat IČO u českých právnických osob, které mají IČO, nebo možné napojení na ARES, vyžadovalo by další analýzu;
- nejednoznačný, resp. neuvedený plátce a příjemce – řešení= povinné uvedení;
- nerozlišené ceny s DPH a bez DPH – řešení = povinnost zadat obě ceny jako povinný atribut;
- metodika (jaká cena u dodatků – platná či rozdílová?) - řešení = upravení, vyjasnění metodiky, nyní chybí úplně;
- příznak cena neuvedena/skryta, případně uvést důvod (nyní je řešeno jako hodnota atributu = 0) – řešení = dodatečný atribut;

Počty publikovaných smluv v Registru smluv za období červenec 2016 – srpen 2017



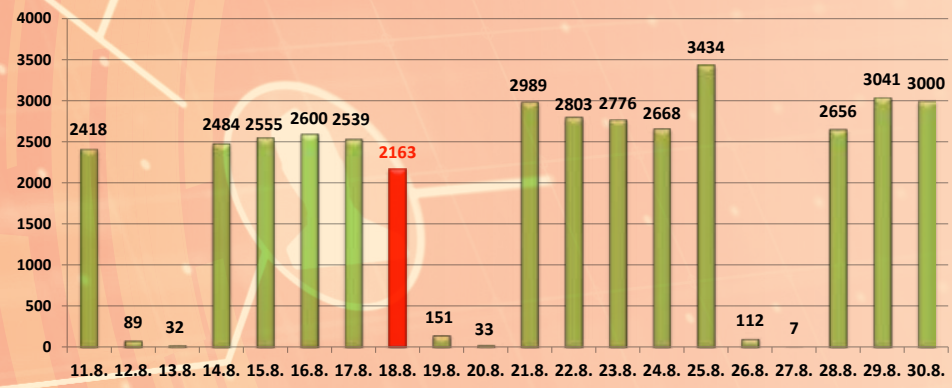
- ***celkem zveřejněno:*** *693 741*
- ***smluv zveřejňovalo:*** *6 949 publikujících subjektů*

Počty zveřejňovaných smluv na přelomu června a července 2017 – vliv nabytí účinnosti § 6 a § 7 zákona o RS od 1. 7. 2017



- *trvalý nárůst zveřejňovaných smluv v pracovních dnech od 21. 6. do 30. 6. 2017*
- *velký pokles zveřejňovaných smluv v pracovních dnech od 1. 7. 2017*
- *je nutné uvažovat i vliv svátků 5. a 6. 7.*

Počty zveřejňovaných smluv od 11. 8. do 30. 8. 2017 – vliv nabytí účinnosti novely zákona o RS od 18. 8. 2017



- *není patrný pokles počtu zveřejňovaných smluv po nabytí účinnosti novely*

- dodatečné údaje ke smlouvě, typ smlouvy (nová, dodatek). Nyní je chaos zejména v dodatcích – řešení = možnost přidat ke smlouvě informaci o charakteru záznamu (nová smlouva, dodatek ke smlouvě s uvedenou vazbou na smlouvu, modifikace smlouvy, zneplatnění);
- denní změny - řešení = možné řešení, že bude k dispozici XML s daty za daný den (analogie s měsíčními dumpy), nutné rozhodnout, jak dlouhou „denní historii“ držet;
- chybějící URL příloh v XML pro 1 smlouvu – řešení = u XML pro 1 smlouvu doplnit URL příloh (v dump XML je, v XML pro záznam není).

Roman Vrba upozornil, že není záměrem MV ČR rozhodovat o těchto změnách, jejich rozsahu a množství samostatně. Byl by rád, aby se uskutečnilo setkání, jakési „veřejné slyšení“ či workshop, kde by se diskutovalo o tom, zda má smysl registr smluv měnit, pokud přidávat, tak jaké atributy, a celkově tak směřovat k usnadnění práce s tímto registrem.

ZÁVĚR

Veškeré popsané snažení směřuje podle Romana Vrby k realizaci a naplnění Portálu občana, na kterém se intenzivně pracuje. Jak Katalog služeb, tak rozvoj ISRS je potřebný pro to, aby si občan mohl v prostředí Portálu veřejné správy (Portálu občana) vyhledat konkrétní službu. Roman Vrba zdůraznil, že pokud bychom neměli k dispozici takové databáze a elektronickou identifikaci, pak nic z toho nebude fungovat. Záměr je dlouhodobě deklarován, legislativa nachystána a měli bychom tedy být připraveni na to, že od 1. 7. 2018 bude v tomto směru cosi funkční.

INFORMAČNÍ SYSTÉMY ICZ VÁS DRŽÍ UŽ 20 LET NA ŠPICI

ISVS a sdílené služby v roce 2017

Ředitel ÚHA Ing. Petr Kuchař a ředitel SZR Ing. Michal Pešek pojali své společné vystoupení v Mikulově jako dialog. A nejprve byl jejich rozhovor zaměřen na práci Útvaru hlavního architekta. Petr Kuchař připomněl, že veškerou práci Útvaru hlavního architekta odstartovalo usnesení vlády č. 889 z roku 2015. Podle něj přineslo dva důležité dokumenty – Strategii rozvoje služeb ICT veřejné správy a Základní zásady schvalování projektů. A právě podle druhého dokumentu postupuje Útvar hlavního architekta při schvalování veškerých projektů ICT ve veřejné správě, především projektů od OVM a jejich podřízených organizací. ÚHA tak tedy počínaje 1. 1. 2016 začal činit, a jak Petr Kuchař uvedl, k dnešnímu dni schválil 250 projektů, zhruba 90 jich nyní má rozpracováno. S ohledem na vrcholící výzvy SF EU je nyní v ÚHA situace taková, že každý, kdo může, se věnuje schvalování projektů.

Petr Kuchař upozornil, že ÚHA v zásadě nepoužívá institut zamítnutí projektu. Převážně využívá institut pozastavení s tím, že následně probíhají s žadatelem jednání a konzultace tak, aby byl projekt přizpůsoben architektonickým požadavkům. Většinou se takto skutečně společně doberou ke zdárnému výsledku, neboť za uvedenou dobu schvalování projektů byly ze strany ÚHA skutečně zamítnuty pouze dva. Ten první vykazoval známky čisté duplicity systému, který již existoval a byl již realizován jako samostatný projekt, a v druhém případě se jednalo o projekt, který zásadně neodpovídal výzvě, na kterou byl podáván. Petr Kuchař v této souvislosti upozornil, že ÚHA zcela běžně poskytuje konzultace, a to ještě před tím, než mu je oficiálně žádost o schválení projektu doručena. Útvaru jde totiž o to, aby působil na žadatele tak, aby žádosti byly v souladu s architektonickou představou. Jde tedy v určitém směru o koordinační činnost. Svým způsobem je zaslání projektu už finální záležitostí, které předchází období spolupráce a vylaďování.

Projekty jsou rozděleny do tří skupin podle velikosti a zaměření:

A. kategorie velkých projektů – jedná se většinou o nově stavěné systémy;
B. rámcové smlouvy, v nichž na začátku není zcela jasné, o co přesně se žádá, ale je znám objem;
C. komodity typu počítače, tiskárny atp.

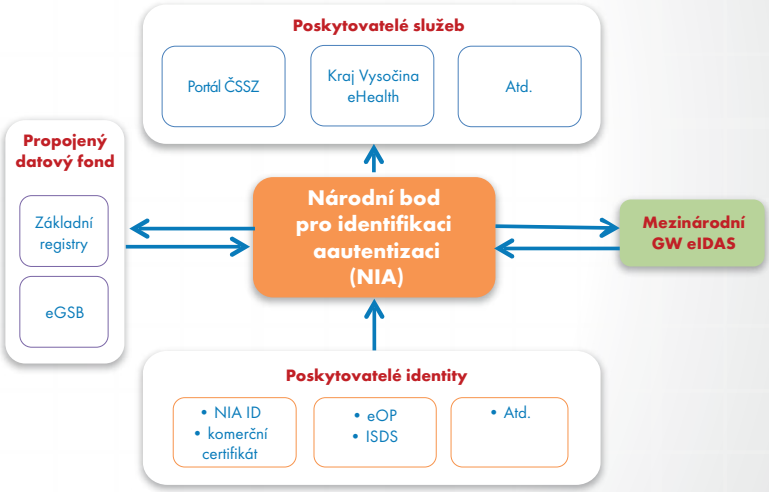
Složitosti každé kategorie tak odpovídá i rozsah a složitost formuláře, který musí žadatel vyplnit. Část těchto kritérií, podle nichž se projekty posuzují, je podle slov Petra Kuchaře obsažena ve zmiňovaném usnesení vlády č. 889/2015. Jako další definoval ÚHA určité komponenty sdílených služeb české veřejné správy, tedy tzv. architektonická schémata. A třetí kriteriální fáze souvisí s novelou zákona č. 365/2000, která MV ČR dala pravomoc definovat informační koncepci České republiky. Na tomto dokumentu se nyní pracuje, bude hotov do konce roku 2017.

Protože Správa základních registrů a projekt Základní registry 2.0 je zdárným příkladem takové spolupráce, dostal ve druhé části vystoupení více prostoru Michal Pešek, aby vysvětlil, že v podstatě jsou dva zásadní momenty, proč se začali zabývat projektem Základní registry 2.0. Ten prozaičtější je, že se jednalo o projekt financovaný ze SF, kterému končí tzv. doba udržitelnosti. Druhým je skutečnost, že narůstá počet propojených agendových informačních systémů (AIS). Jak zdůraznil, zhruba před pěti lety začali s propojováním datového fondu. Tehdy se jednalo o pár desítek či stovek AIS. Dnes toto číslo dosáhlo zhruba 5000. Jedná se pouze o referenční data a je, jak upozornil, nutno vzít v úvahu i data nereferenční (fotografie...). Vlastně dalším motivem je rovněž obsah horní vrstvy ICT a e-governmentu. Spodní vrstvou je infrastruktura, nad ní databáze, nad tím jsou aplikace a horní vrstva jsou potřeby veřejné správy, případně komerční oblasti. A právě potřeby, respektive požadavky veřejné správy nutí SZR zabývat se propojeným datovým fondem a uvažovat o tom, jaké konkrétní služby veřejná a státní správa potřebuje.

Jako příklad takového požadavku, který podle jeho mínění rozhodně zvýší zátěž základních registrů, je Národní identita. Zejména v oblasti registrů obyvatel je možné po zavedení elektronické identity počítat se zvýšením transakční zátěže. Každé přihlášení na jakémkoliv portálu bude znamenat volání základního registru obyvatel. Musíme být připraveni a to je tedy důvod pro Základní registry 2.0.,

samozřejmě vedle například legislativních změn (zákon č. 250/2017 Sb., doprovodný zákon č. 215 a zákon č. 365). V této souvislosti ale upozornil právě na zákon č. 365, který zavádí termín přístup se zaručenou identitou a dovoluje tak občanům obstarat si výstup z Informačního systému veřejné správy. Právě tady čeká Michal Pešek skutečně velkou zátěž, a proto je třeba jednotlivé systémy významně upravit. Protože se jedná o technickou realizaci, je potřeba testovat. Michal Pešek uvedl, že už jsou s projektem ve fázi, kdy je testování možné. V této souvislosti poděkoval všem, kdo se na testovacím procesu podíleli, a zároveň uvedl, že bude probíhat až do 30. 6. 2018.

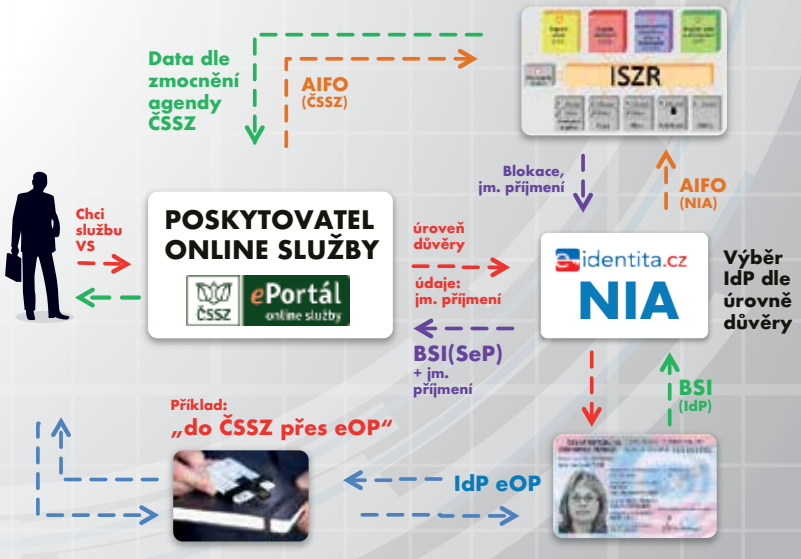
Pro nástin funkčnosti ukázal schémata, nejprve personifikováno na jeden portál a použití OP a obecnější schéma, kde je vidět, že poskytovatel služby portál potřebuje identifikaci, tlačítkem přihlásit se obrátí na Národní bod, který uživateli umožní výběr identifikačního prostředku (kromě



eOP mohou být i další). Vybraný identifikační prostředek zavolá konkrétního poskytovatele identity, vůči němuž je uživatel identifikován. Na základě této identifikace se Národní bod podívá do datového fondu a „zjistí" o uživateli vše potřebné. To složí do datové struktury a odešle tazateli. Podstatné je, že takto by to skutečně mělo fungovat v celé Evropě v září 2018. Na evropské úrovni proto pracuje Cooperation Network, orgán složený ze zástupců členských států EU, který řeší, jak přesně toto propojení realizovat v praxi. Zřejmě dojde k tomu, že každá země bude mít vlastní Gateway a nebude žádná centrální propojovací. Národní brány se pak budou v případě potřeby spojovat 1:1 pro vzájemnou komunikaci.

Pro celou záležitost je samozřejmě podstatná i notifikace jednotlivých národních identitních systémů. V současné době je Německo prvním státem, který započal (v dubnu) tuto notifikaci. Nyní běží osmnáctiměsíční lhůta, kdy jsou ostatní členské státy povinny akceptovat tuto národní identifikaci, tedy akceptovat volání (prostřednictvím německé eOP, případně kartou povolení k pobytu) uvnitř německého prostoru. Ostatní státy budou bezpochyby následovat. Česká republika předpokládá tento krok zhruba v polovině roku 2018, v souvislosti s účinností zákona o elektronické identifikaci. To bude správný moment pro nahlášení českého národního identitního prostoru, který bude reprezentován eOP, ale možná i dalšími prostředky.

V závěru vystoupení pak už jen oba pánové představili možnost správy profilu, který by měl umožňovat mimo jiné podat žádost pro ověření pomocí CzP Home, připojit další prostředky identity (například zpřístupnit možnost přihlášení komerčním certifikátem) nebo profil zrušit atp. Pro vytvoření tohoto profilu je samozřejmě nutná návštěva občana na CZECH Pointu. Následně je pak práce obdobná jako v případě internetového bankovnictví a podobných systémů. Nyní probíhá testování Ministerstvem zdravotnictví, Státním ústavem pro kontrolu léčiv ČSO a CZ.NIC.



Dopady novely zákona o kyberbezpečnosti – aplikace v ISMS resortu MV

Ing. Miroslav Tůma, PhD. prezentaci zahájil tím, že při výběru tématu se řídil požadavky, s nimiž se obrací řada lidí na odbor kybernetické bezpečnosti, a to vyjasnit otázky dopadu novely zákona o kyberbezpečnosti. Vzhledem k tomu, že letošní rok poznamenaly oblast kyberbezpečnosti dvě novely – zákon č. 104/2017 Sb. a novela zákona o kybernetické bezpečnosti č. 205/2017 Sb., je evidentní, že pro řadu lidí je důležité, aby MV ČR dalo k dispozici vzory, šablony, případně návody, jak nastavit dopady těchto novel.

Změnový zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy, přináší nové role. Především je to provozovatel systému. Jedná se o nový subjekt, kterému se stejně, jako správci, ukládají povinnosti. Povinným subjektem se provozovatel stává v případě naplnění definičních znaků. Zákon dále ukotvuje vztah mezi správcem a provozovatelem a stanovuje bezpečnostní opatření, která k 1. 1. 2018 musí provozovatel zavést. Podle tohoto zákona provozovatel:

- předává správci data a informace, které má k dispozici v souvislosti s provozováním tohoto systému na vyžádání a bezodkladně, případně po ukončení provozování systému, kdy kopie těchto dat a informací zlikviduje;
- má nárok na úhradu účelně vynaložených nákladů souvisejících s předáním;
- má povinnost hlásit kybernetické bezpečnostní incidenty NÚKIB (týká se i provozovatele);
- byly zostřeny sankce za nedodržování požadavků zákona (až 1 000 000 Kč).

Zákon rovněž zavádí shodné povinnosti pro správce i provozovatele:

- zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti systému a vést o nich bezpečnostní dokumentaci;
- zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro systém;
- detekovat kybernetické bezpečnostní události v systému;
- hlásit kybernetické bezpečnostní incidenty NÚKIB.

Miroslav Tůma se dále věnoval **zákonu č. 205/2017 Sb.**, který rovněž novelizoval zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a navíc do tohoto zákona implementoval evropskou směrnici NIS (směrnice EU č. 2016/1148). Zákon mimo jiné definoval **nový úřad pro kybernetickou informační bezpečnost** se sídlem v Brně (NÚKIB) a vymezil nové povinné subjekty a typy služeb.

Miroslav Tůma, PhD., ředitel odboru kybernetické bezpečnosti a koordinace ICT MV ČR

Novými subjekty podle tohoto zákona jsou:

- poskytovatel digitální služby;
- provozovatel základní služby;
- správce a provozovatel informačního systému základní služby.

Nově definovaným typy služeb jsou:

- základní služba;
- digitální služba.

ZÁKLADNÍ SLUŽBA

je podle tohoto zákona služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:

- energetika;
- doprava;
- bankovnictví;
- infrastruktura finančních trhů;

- zdravotnictví;
- dodávky a rozvody pitné vody;
- digitální infrastruktura;
- chemický průmysl.

DIGITÁLNÍ SLUŽBA

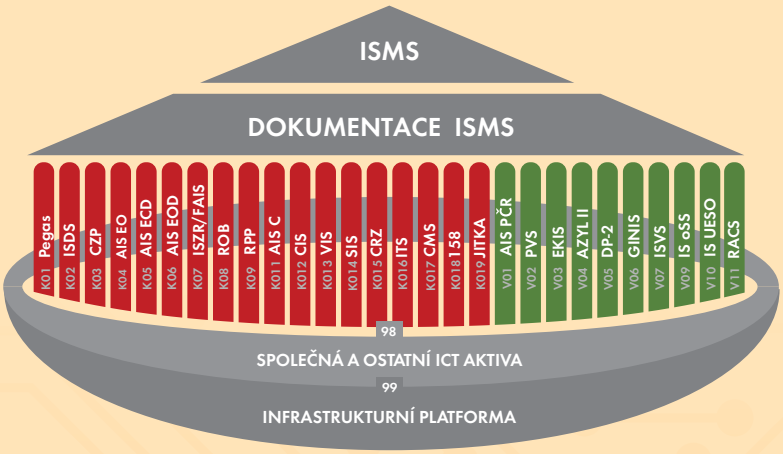
Podle tohoto zákona se jedná o službu informační společnosti, tedy jakoukoliv službu poskytovanou elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, která je většinou poskytována za úplatu. Služba spočívá v provozování on-line tržiště, internetového vyhledávače nebo Cloud Computingu. Jak Miroslav Tůma uvedl, zákon vymezuje vzájemné provázání, tedy vzájemnou informační povinnost. Informovat je třeba nejen v rámci organizace, ale nutné je informovat i NÚKIB například o jednotlivých incidentech a následně je v kooperaci s tímto úřadem řešit.

Náročný je rovněž dopad zákona na smluvní vztahy. Smlouvy s poskytovatelem Cloud Computingu v případě OVM musí obsahovat:

- zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb;
- stanovení úrovně poskytovaných služeb;
- systém schvalování subdodavatelů služby Cloud Computingu;
- podmínky ukončení smluvního vztahu z pohledu bezpečnosti;
- řízení kontinuity činností v souvislosti s poskytovanou službou Cloud Computingu;
- určení vlastníka uchovávaných dat;
- dohodu o důvěrnosti smluvního vztahu;
- stanovení úrovně ochrany dat z ohledu důvěrnosti, dostupnosti a integrity;
- pravidla zákaznického auditu.

ZABEZPEČENÍ KII A VIS V RESORTU MV – ÚPRAVA POVINNOSTÍ SPRÁVCŮ A PROVOZOVATELŮ

Jak Miroslav Tůma dále uvedl, v rámci resortu MV ČR je celý systém řízení kyberbezpečnosti postaven na třech základních pilířích. Jsou to základní pravidla a základní dokumentace. Z toho vyplývá rozdělení jednotlivých rolí, jejich činností a odpovědností. K těmto rolím jsou pak definovány systémy, které spadají pod KII a VIS. Těchto systémů je, jak Miroslav Tůma zdůraznil, celkem 28, což je bezkonkurenčně největší číslo v rámci ČR. Všech těchto 28 systémů je nutno zabezpečit, a to jak příslušnou bezpečnostní dokumentací, tak organizačními i technickými opatřeními. Nad tím vším bdí dohledové centrum e-governmentu. Všechny uvedené systémy jsou tedy dohledovány a vyhodnocovány z pohledu incidentů.



Vlastní systém řízení bezpečnosti informací tedy stojí na těchto 28 systémech a zastřešuje jej ISMS s vlastní dokumentací. Ta je platná celoresortně, a proto je i k dispozici na sjednoceném informačním prostředí. Tento pantheon definuje základní strukturu a umístění jednotlivých systémů. Je jasně vymezena odpovědnost pro správce ISMS, věcného správce, správce systému, stejně tak jsou definované role, především odboru KB, který garantuje celý systém, a základní schéma odpovědnosti.

<table>
<tr><th>Odpovědnost</th><th colspan="2">Plnění požadavků ZoKB</th><th>Realizace</th></tr>
<tr><td>Správce systému (Ministerstvo vnitra)</td><td colspan="2">ISMS resortu MV</td><td>Odbor kybernetické bezpečnosti</td></tr>
<tr><td>Věcný správce</td><td rowspan="3">Zabezpečení KII a VIS</td><td>Dokumentace KII a VIS</td><td>Garant primárních aktiv</td></tr>
<tr><td rowspan="2">Provozovatel</td><td>Organizační opatření</td><td rowspan="2">Garant podpůrných aktiv</td></tr>
<tr><td>Technická opatření</td></tr>
</table>

Pro zabezpečení systémů KII a VIS platí podle slov Miroslava Tůmy čtyři kroky – PDCA (plánuj, dělej, kontroluj, jednej).

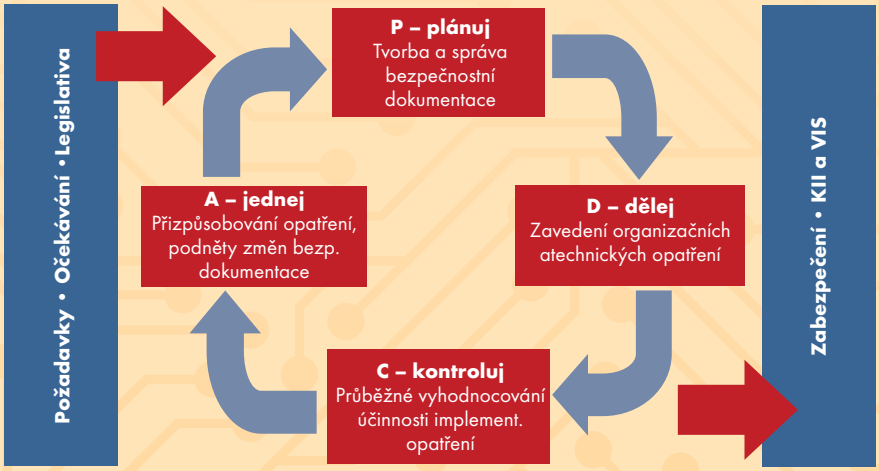
Nadřízená role	Činnost	Činnost	Podřízená role	Osoba
Správce systému	Ministr vnitra	Jmenuje	Manažer kybernetické bezpečnosti	Fyzická osoba
Věcný správce	Ředitel odboru	Určuje	Garant primárních aktiv	Fyzická osoba
			Technický správce	Útvar MV
			Administrátor aplikace	Fyzická osoba
Provozovatel	Ředitel odboru nebo externí poskytovatel	Určuje	Garant podpůrných aktiv	Fyzická osoba
			Administrátor systému	Fyzická osoba

Role	Osoba	Kontakt pro
Správce systému	Odpovídá za plnění požadavků ZoKB na systémy KII a VIS resortu MV.	
Manažer KB	Odpovídá za systém řízení bezpečnosti informací a zastává tuto roli za všechny KII a VIS resortu MV.	
Věcný správce	Určuje garanty podpůrných aktiv,odpovídá za plnění požadavků ISMS pro příslušný systém KII nebo VIS.	OKB, NÚKIB
Provozovatel	Určuje garanty podpůrných aktiv, odpovídá za plnění požadavků ISMS pro příslušný systém KII nebo VIS	OKB, NÚKIB
Garant primárních aktiv	Plní požadavky ISMS pro příslušný systém KI I nebo VIS, zejména v oblas t i organizačních opatření	OKB
Garant podpůrných aktiv	Plní požadavky ISMS pro příslušný systém KII nebo VIS, zejména v oblasti technických opatření	OKB
Technický správce	Realizuje rozvoj a vývoj příslušného KII nebo VIS, a to i v oblasti KB. Současně stanovuje technické parametry provozu systémů, jež naplňuje provozovatel.	OKB
Administátor aplikace	Zajišťuje bezpečnostní aspekty správy systému KII nebo VIS na funkční, resp.uživatelské úrovni.	
Administátor systému	Na technické úrovni zajišťuje bezpečnostní aspekty správy systému KII nebo VIS.	OKB, NÚKIB

PRINCIPY TVORBY BEZPEČNOSTNÍ DOKUMENTACE

V této souvislosti upřesnil, že dokumentaci každého ze systémů KII a VIS resortu MV spravuje osoba určená věcným správcem, tzv. správce bezpečnostní dokumentace ISMS. Principiálně lze ale samotnou tvorbu rozdělit a přidělit dle příslušných věcných kompetencí: garant primárních aktiv – organizační témata, garant podpůrných aktiv – technická témata. Dále podle Miroslava Tůmy platí, že individuální bezpečnostní dokumentace systémů KII a VIS nesmí být v rozporu se schválenou podobou resortní dokumentace ISMS. A zpracovatelé se musí řídit principy řízení bezpečnostní dokumentace ISMS v resortu MV (ISMS 02.03 řízená dokumentace). Tyto principy mimo jiné vyžadují použití schválených šablon pro programy Microsoft Word a Microsoft Excel a publikaci dokumentů v sekci KB sdíleného informačního prostředí resortu MV.

Čtyři kroky zabezpečení systémů KII a VIS



Struktura bezpečnostní dokumentace se v souladu s VyKB dělí na bezpečnostní politiky a ostatní bezpečnostní dokumentaci. Zpracovatelé mohou ve spolupráci s OKB při tvorbě bezpečnostních politik postupovat následujícími způsoby:

- převzít plné znění centrálního dokumentu z resortní dokumentace ISMS, na který se v rámci připravených šablon odvolají;
- převzít znění centrálního dokumentu formou odkazu a současně popsat modifikace, tj. zpřesnění a specifika konkrétního systému;
- v odůvodněných případech vytvořit nový vlastní dokument.

Jak dále Miroslav Tůma upřesnil, zpracování většiny dokumentů z části ostatní bezpečnostní dokumentace centrálně zajišťuje OKB. Určení garanti primárních a podpůrných aktiv spolupracují na jejich přípravě a aktualizaci.

Následně Miroslav Tůma prezentoval všech 21 bezpečnostních politik definovaných zákonem, a jak uvedl, ke všem těmto politikám jsou vytvořeny jednotlivé dokumenty v rámci DISMS. Je tedy jasně definováno, které dokumenty na úrovni kterého garanta je možné měnit či doplňovat, kdo je má v gesci, kdo na nich spolupracoval atp. Tento přehled prezentoval ve formě tabulek, které jsou podle jeho slovy těmi, o které jej mnozí ve svých dotazech žádali. Je z nich patrno, „kam má kdo sáhnout", co je konkrétně v gesci určitého provozovatele a co jak onen provozovatel, tak samotní garanti mají nově dotvářet v rámci specifik informačních systémů. Následně k tomu ještě vychází jednotlivá organizační bezpečnostní opatření, tedy opět návodná tabulka, kdo má co dělat a kdo za co odpovídá. Následně pak zbývá v rámci implementace povinnost informovat vůči NÚKIB a vůči OKB, protože jak uvedl na začátku, spravují celkově 28 systémů pro 56 organizací, tedy jednota v tomto rozsahu musí být zajištěna.

V závěru svého vystoupení Miroslav Tůma upozornil na e-learnignový kurz kybernetické bezpečnosti. Ten podle jeho slov vychází z:

- akčního plánu pro rozvoj digitálního trhu;
- akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období 2015-2020.

Kurz je realizován ve spolupráci Národního úřadu pro kybernetickou bezpečnost, Ministerstva vnitra, Úřadu vlády ČR a Institutu pro veřejnou správu, který realizaci kurzu zajišťuje. Pilotní test kurzu zahajuje MV ČR v říjnu tohoto roku.

Občan má právo, aneb Digitální revoluce.

Prezident ICT Unie Mgr. Zdeněk Zajíček se ve svém, poněkud emotivním, projevu odkazoval především na skutečnost, že v několika posledních mezinárodních srovnáních vychází český e-government dosti nelichotivě, protože například v loňském roce jsme se umístili podle správy OSN až na 50. místě (hodnoceno více kritérii) na světě. Přitom, kdyby se hodnotila jen samotná kapitola e-governmentu, posadila by nás až na 92. světovou příčku. Poněkud optimističtěji to vypadá v rámci evropského žebříčku – index DESI, kde jsme letos skončili na 18. místě (z 28 hodnocených zemí).

Jak Zdeněk Zajíček uvedl, dokáže si představit, že bychom mohli být v oblasti e-governmentu nejlepší, nebo minimálně na stejné úrovni jako vyspělí Estonci či Britové. Ptal se proto, co je tou bariérou, která nám v dosažení takového výsledku brání? Jak uvedl, domnívá se, že potřebujeme digitální revoluci. Musíme se totiž naučit myslet trochu jinak, mimo zavedené hranice a nesmíme se bát zkoušet nové možnosti. I když připouští, že veřejná správa se skutečně snaží realizovat leccos zajímavého a nového, je podle jeho mínění v určitém směru v legislativním vězení. Jsme totiž svázáni zákony, které nám v některých momentech skutečně brání v dalším postupu. Je tedy nutné zvážit, zda jsme schopni při současném legislativním rámci činit další kroky, nebo zda jako ten nejbližší musíme změnit právě onen legislativní rámec. A není přitom nutné, podle Zdeňka Zajíčka, vždy hned hovořit o novém paragrafu či dokonce zákonu, jako spíše o novém výkladu odpovídajícím více reálné situaci a době, v níž se nacházíme.
Zdeněk Zajíček připustil, že sám, jako dlouholetý úředník, byl uzavřen uvnitř těchto legislativních bariér. Nyní, kdy se na ně dívá z druhé strany, zastává názor, že je skutečně nutné, abychom na realizaci legislativních norem změnili náhled a dívali se na tento problém z pozice klienta veřejné správy – občana. Musíme si uvědomit, že občan má na něco právo – právo na poskytnutí konkrétní služby veřejné správy elektronickou formou, samozřejmě za předpokladu, že takové realizaci nebrání nějaké technologické omezení.

Prezident ICT Unie Mgr. Zdeněk Zajíček

OBČAN MÁ PRÁVO

Podle Zdeňka Zajíčka má občan právo například na:

- to, aby cokoliv mohl poslat veřejné správě v elektronické podobě (podání, fakturu, podklady...). Pokud v konkrétním případě neexistuje přesně stanovený postup, který by elektronickou cestu vylučoval, má skutečně takovou možnost a právo vyžadovat od veřejné správy akceptaci tohoto jeho rozhodnutí;
- doručování a vyplácení finančních prostředků ze strany státu v elektronické podobě - pokud si nepřeje vybírat hotovost, je to cesta, kterou si může zvolit;
- to, aby nemusel dokládat státu stále stejné údaje - sdílení dat je už nyní obsaženo v zákoně o registrech;
- to, aby elektronické údaje dokládal elektronicky, tedy aby nemusel nosit množství papírových dokladů atp.

Zdeněk Zajíček upřesnil, že toto jsou jen některá z práv, která jako občané máme a možná o nich nevíme. Dalším je například právo na přístup ke své zdravotnické dokumentaci v elektronické podobě. To je sice oblast, kde se podle jeho slov leccos za poslední roky zvládlo udělat, přesto není možné například zařídit, aby tyto údaje sdíleli rodinní příslušníci.

Obecně je zřejmé, že veřejná správa má zatím potíž s poskytnutím dat, která o nás „vlastní", dále. Není například možné, i v případě, že si to občan přeje, aby banky či operátoři sdíleli jeho data, která jsou uložena v základních registrech. Tyto subjekty však k základním registrům nemohou přistupovat, protože, jak Zdeněk Zajíček zdůraznil, nikdo není ochoten postavit informační systém, který by to umožňoval, přitom je to právo občanů.

ZÁKONNÝ PŘEHLED

Zdeněk Zajíček uvedl, že podle toho, o čem referoval náměstek MIsna, to vypadá, že projekt elektronické Sbírky zákonů je ve své závěrečné fázi a snad jej tedy do roku 2020 budeme skutečně mít k dispozici. Ale Zdeněk Zajíček by rád upozornil na skutečnost, že to je pouze část cesty.

Následně je potřeba zpřehlednit náš právní řád a udělat jakýsi seznam povinností, které ze zákona vyplývají. Bylo by podle něj dobré nabídnout občanům takovou službu, která v příloze zákona bude mít přehled povinností uvedený tak, že i občanům bez právního vzdělání bude zřejmé, co přesně a v jakých lhůtách se musí splnit, případně jaká sankce hrozí v případě nesplnění.

Zdeněk Zajíček na závěr ještě jednou zopakoval, že je nutné si uvědomit, jak moc máme zažitá schémata, která jsme si zde historicky nastavili, a v případě, že chceme posunout e-government, měli bychom zvažovat, která z těchto schémat je možné a vhodné změnit.

Umělá inteligence: neúnavný spolupracovník i strážce citlivých dat

Kyberútoky se neustále zdokonalují a počítačovou síť už lze napadnout i prostřednictvím termostatu. Zvyšují se i zisky hackerů. Jen v loňském roce vydělali kyberzločinci využívající vyděračský software, tzv. ransomware, podle FBI zhruba 1 miliardu dolarů. Hackeři, kteří se specializují na podvržené firemní e-maily, jsou na tom dokonce ještě lépe. Za tři roky si takto podle odhadů amerického týmu Internet Crime Complaint Center přišli na 5,3 miliardy dolarů. V ohrožení ale nejsou pouze firmy. Útoky dnes cílí i na systémy obcí a institucí veřejné správy. Technologická firma Cisco řeší aktuální bezpečnostní výzvy originálně: pomocí sítě, která bude mít vlastní inteligenci.

„Hackeři si dokážou zjistit vnitřní strukturu organizace a identifikovat osoby, na které je vhodné zaútočit. Následně připraví podvržený e-mail, který vypadá jako zpráva od ředitele a obsahuje například dokument, který je nutné urgentně zkontrolovat a poslat zpátky. Falešný e-mail vypadá například tak, že přijde z adresy jan.novak@quallcart.cz, namísto ze správné jan.novak@qualicart.cz. Zbytek e-mailu je zcela totožný s oficiálním – podpis, logo i písmo. Rozdílu si nikdo nevšimne, nebezpečný malware se nainstaluje do systému. Následně může hackerům odesílat citlivá data organizace," varuje Tomáš Kupka, expert společnosti Cisco na architekturu podnikových sítí.

Jsou dva druhy organizací: napadené („hacknuté") a ty, které o tom ještě neví

Rychlost a účinnost dnešních kyberútoků ukázaly nedávné vlny ransomwarů WannaCry a Nyetya. Ty se šířily tak účinně, neboť využívaly stejnou techniku jako virus typu červ. Dokázaly totiž z jednoho napadeného zařízení infikovat všechna ostatní, která byla připojena do stejné sítě.

„Každou organizaci lze „hacknout". Bezpečnostní experti se proto nemohou zaměřovat jen na prevenci útoku, ale musí počítat s tím, že útočníci už do systému organizace mohli proniknout. Našim úkolem je jejich rychlé odhalení a eliminace," popisuje Tomáš Kupka. *Klíčem k úspěchu je podle něj to, aby se bezpečnostním senzorem organizace stala celá její síť. „Využíváme umělou inteligenci, která odhalí tzv. zero-day útoky v průměru za 3,5 hodiny, zatímco tradičním řešením to trvá kolem 100 dní,"* dodává.

Kyberútok a jeho následky

Jedna malá nepozornost či překlik mohou organizaci stát podstatnou část zákazníků i zisků. Podle bezpečnostní studie Cisco téměř čtvrtina organizací (22 %), na které byl veden úspěšný útok, ztratila své zákazníky a 40 % z nich přišlo o více než pětinu své zákaznické základny. Podobně se snížily i jejich tržby. *„Celých 29 % úspěšně napadených organizací zaznamenalo nižší příjmy, 38 % z nich pak ztratilo více než 20 % objemu tržeb,"* popisuje Tomáš Kupka.

Jaké změny čekají sítě?

S obrovským nárůstem počtu zařízení v síti už nebudou tradiční přístupy dostačovat – už v roce 2020 se totiž každou hodinu připojí k síti 1 milion nových zařízení. Proto se počítačové sítě musí změnit. Tato proměna bude postavena na 3 pilířích, a to na: potřebě automatizace, důrazu na bezpečnost a pokročilé analytice.

Trend č. 1: Potřeba automatizace

Automatizace bude základním stavebním kamenem moderních sítí v celém rozsahu jejich životního cyklu – počínaje návrhem přes nasazení a implementaci až po správu provozu, dohled a optimalizaci. Automatizované nástroje dovolí navrhovat sítě, které budou od počátku přizpůsobené charakteru firmy a její organizační struktuře. Automatický provisioning je obecně velkým tématem v oblasti sítí a bude se velmi rychle vyvíjet. Mimo jiné i proto, že se v posledních letech výrazně snižovala doba nutná k nasazení serverů v datových centrech. Narůstal tak postupně rozdíl mezi dobou nutnou k nasazení serverů a aplikací a dobou nutnou k nasazení sítí. Že se tento rozdíl setře úplně, asi nelze čekat z důvodu větší složitosti a distribuo-

vané povahy sítě. Ale zcela jistě se bude postupně snižovat. A automatizace či výrazné zjednodušení dříve zbytečně zdlouhavých, ale zároveň nutných manuálních kroků to umožní. Nová softwarová řešení se přitom přizpůsobí stávající infrastruktuře.

Trend č. 2: Důraz na bezpečnost

Organizace a jejich sítě jsou tak dnes pod větším tlakem než kdy dříve. Útoky jsou totiž stále propracovanější a dokážou měnit svoji podobu v řádu hodin. Zároveň se neustále zpřísňuje legislativa – již v květnu příštího roku přibudou organizacím nové povinnosti vyplývající z nařízení GDPR. Navíc prudce roste počet zařízení připojených do sítě. *„Pokud se naplní předpovědi, zvýší se počet internetových zařízení do 4 let třikrát. A kybernetický útok se může skrývat v každém z nich – v bezpečnostní kameře, v senzoru výrobního stroje nebo i v termostatu na zdi. To prakticky vylučuje, aby se o bezpečnost těchto zařízení starali jednotliví IT specialisté,"* vysvětluje Tomáš Kupka.

Automatizace a bezpečnost se proto musí stále výrazněji prolínat. Automatické zapojení systému do definice a aplikace firemních bezpečnostních politik totiž výrazně zrychluje nejenom reakci na případné bezpečnostní incidenty, ale zároveň snižuje riziko chyby způsobené lidským faktorem. Tento přístup zajišťuje nejenom efektivnější minimalizaci škod po úspěšném průniku, ale hraje také velmi důležitou roli ve fázi prevence. Jinými slovy, dokáže v mnoha případech rozpoznat příznaky napadení ještě před hlavním útokem.

Lze také očekávat, že organizace budou stále častěji využívat sítí, které nabídnou automatickou segmentaci, tedy vzájemné oddělení částí sítě s různými charakteristikami a nároky. Dnes se totiž často setkáváme s její nedostatečnou úrovní, která snižuje celkovou bezpečnost sítě. Nízká nebo žádná segmentace totiž v konečném důsledku znamená, že se případný škodlivý software může z jednoho zařízení rozšířit do celé sítě nebo do její velké části. Tento efekt je dobře známý, nicméně podrobná a dynamická segmentace bývá časově i finančně velmi náročná. Proto se o tuto práci bude muset postarat software.

Trend č. 3: Pokročilá analytika

Data se stávají klíčovým „majetkem" a konkurenční výhodou organizací i jednotlivých zemí. Samozřejmě pokud je dokážou zpracovat a analyzovat. Navíc analytika neslouží pouze k vyhodnocení událostí v minulosti. Díky ní budou moci organizace (nebo i města či státy) lépe předvídat budoucí vývoj a mnohem lépe se tak připravit na situace nebo problémy, které mohou nastat.

Analytika využívající síťovou telemetrii se samozřejmě dá využít i v jiných oblastech, například pro zlepšení zdravotnické péče, pro optimalizaci dopravy, pro efektivnější hospodaření s energiemi, vodou, odpady a podobně. Do podoby analytických nástrojů bude stále častěji promlouvat umělá inteligence a strojové učení. Algoritmy, které se od sebe budou navzájem učit v open-source prostředí, výrazně zvýší pravděpodobnost predikcí.

Umělá inteligence: strážce i pracovník

Všechny tyto trendy zosobňuje koncept The Network.Intuitive., síť s umělou inteligencí, se kterou přichází společnost Cisco. Automatizuje rutinní činnost IT specialistů, kteří budou do budoucna podle názoru Cisco nastavovat všeobecná pravidla pro fungování infrastruktury. O jejich aplikaci se postará samotná síť. *„Dramaticky se zmenší pravděpodobnost lidské chyby, bude zajištěn prokazatelný soulad s legislativními pravidly. V tom tkví přelomová inovace našeho přístupu. Jsme přesvědčeni, že člověk má určit pravidla a síť je má automaticky aplikovat. Pokud budete firemní síť spravovat postaru a počet zařízení v ní se za pár let zdesetinásobí, jednoduše vám dojdou IT specialisté,"* uzavírá Tomáš Kupka. Síť s umělou inteligencí se tak stává nejenom strážcem citlivých dat, ale zároveň i spolupracovníkem, který neúnavně zvládá příval rutinních úkolů.

Milan Habrcetl, Cisco

GDPR a elektronická identifikace

Zařazení samostatného workshopu s tématem GDPR a elektronické identifikace do programu konference v Mikulově bylo jen zcela logickým krokem, který reagoval na současný zvýšený zájem o tato témata.

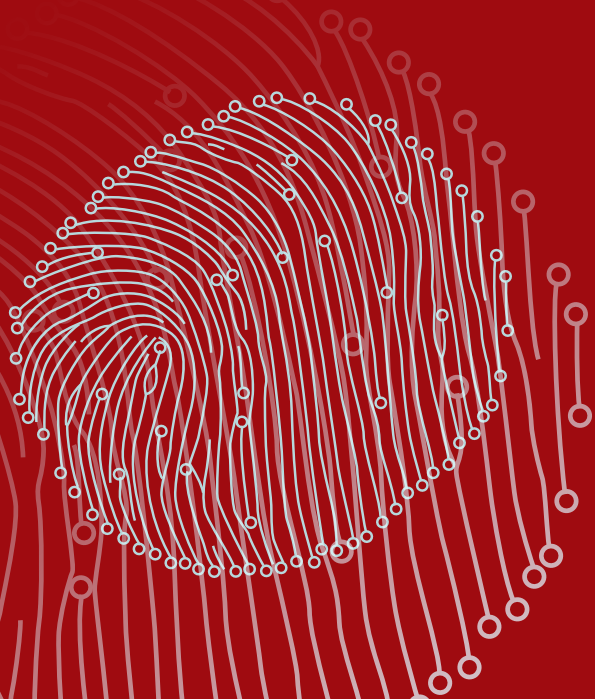
Proč se ale najednou všichni zajímají o problematiku ochrany osobních údajů, když dosavadní zákon č. 101/200 Sb., zákon na ochranu osobních údajů, zde platil téměř 17 let, a jak se z následujících příspěvků dozvíte, nikdo si s jeho naplňováním vlastně hlavu moc nelámal? Je to jen tím, že nyní se bavíme nikoli pouze o národní legislativě, ale o nařízení na úrovni EU. Vždyť navíc nařízení GDPR, o němž je řeč, zase tak revoluční není, neboť v zásadě nepřináší ani tak mnoho nového, co bychom doposud naší legislativou nepostihovali. Možná je kouzlo v tom, že to málo navíc, co přináší, si umí docela nekompromisně vynutit. Pokuta 10 mil. euro pro veřejnou správu (20 mil. euro pro soukromý sektor) už není úplně zanedbatelná. Navíc o účinnosti tohoto nařízení není vůbec žádná diskuze. Jedná se o nařízení EU, a tak bude od 25. 5. 2018 účinné ve všech členských zemích, a tedy i u nás.

Co to tedy znamená? Najednou skutečně všichni řeší, jak správně zpracovávat a ochraňovat osobní údaje. A protože jich veřejná správa má skutečně hodně a často v řadě různých souvislostí, je v tom trochu zmatek. Kdy, na jak dlouho, za jakým účelem, jak a proč? To jsou jen některé z otázek, které si veřejná správa začíná klást a učit se hledat na ně odpovědi.
Hledat musí také odborníky. Nařízení zavádí zcela novou funkci a najít lidi do jejího obsazení nebude úplně jednoduchá záležitost. Pověřenec na ochranu osobních údajů je vlastně, alespoň podle toho, jak působí první definice, jakýmsi vnitřním auditorem, který bude dohlížet na to, zda organizace správně s osobními údaji nakládá, radit zaměstnancům, organizaci a komunikovat s ÚOOÚ. Kromě samotného nalezení takové vhodné osoby se zdá, že druhým zásadním problémem bude, jak přesně takového odborníka zaplatit.

V současné době, pokud jste tak ještě neučinili, doporučujeme prostudovat nařízení EU č. 2016/679 a sledovat vývoj novely zákona č. 101/2000 Sb. Ta možná přinese veřejné správě i určité úlevy v této oblasti, jen ještě není úplně jasné, kdy přesně, protože nyní prošla připomínkami a tiše čeká na sestavení nové Poslanecké sněmovny, aby mohla být odhlasována. Doufejme, že se tak stane a nebude to dlouho trvat.

Elektronická identifikace v podstatě s problematikou ochrany osobních údajů přímo souvisí. Je zřejmé, že veřejná správa bude muset zpracovávat čím dále větší množství elektronických dokumentů, a to takových, které bezesporu ponesou množství osobních údajů. Díky nařízení eIDAS č. 910/2014 směřujeme k tomu, že se občané budou moci elektronicky identifikovat. Zároveň lze očekávat, že díky službám vytvářejícím důvěru elektronickým transakcím získají k těmto službám skutečně důvěru a budou je vůči veřejné správě čím dál tím více využívat.
Aby toho nebylo málo, směřujeme ještě k tomu, že díky jednotné digitální bráně bude možné, aby se občané elektronicky identifikovali a častovali elektronickými dokumenty veřejnou správu napříč Evropskou unií. Doufejme tedy jen, že tzv. úplné elektronické podání významně usnadní život občanů a přitom úplně nezahltí přístupové kanály k veřejné správě.

Kromě uvedených evropských norem je vhodné v tomto směru mít načtené české zákony o službách vytvářejících důvěru a zákon o elektronické identifikaci.



FORTINET®

– víme jak vás ochránit

Vyžadujte bezpečnostní řešení, které pokryje celé spektrum vašich požadavků jak z pohledu výkonnosti, univerzálnosti, tak zároveň z pohledu na budoucí požadavky.

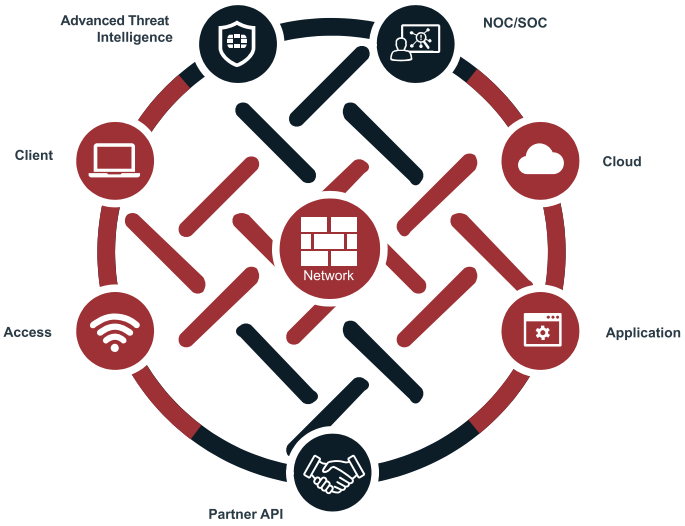
Buďte připraveni na budoucí hrozby. **www.fortinet.com**

První krok…

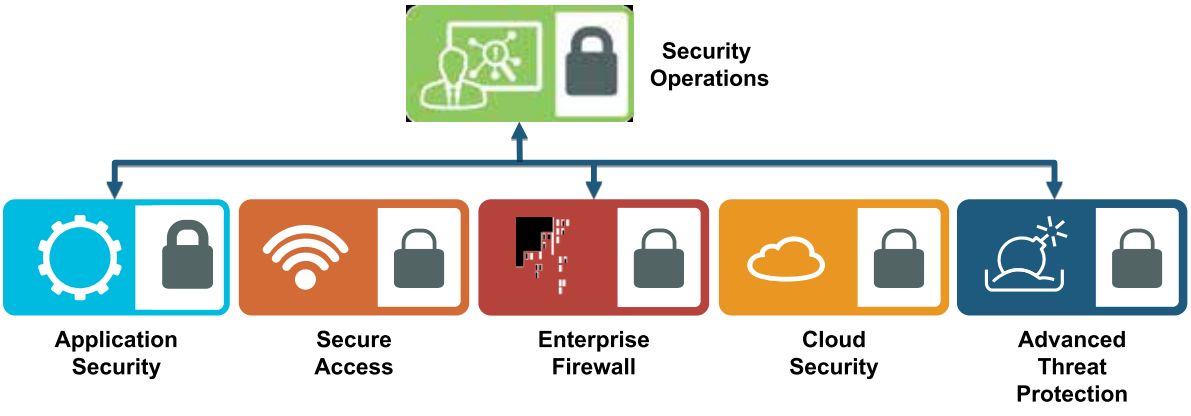
…k souladu s GDPR

FORTINET SECURITY FABRIC

Broad
Powerful
AUTOMATed



Fortinet Security Fabric a jeho stavební prvky



Dopady nové legislativy

Ing. Robert Piffl, poradce náměstka ministra vnitra pro ICT se ve svém vystoupení věnoval dopadům evropské i české legislativy na elektronické dokumenty a procesy e-governmentu. Proto v úvodu vystoupení připomenul, o jaké předpisy, opatření a nařízení se jedná:

V RÁMCI eIDAS

Nová evropská legislativa:

- nařízení eIDAS (nařízení č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce)+ jednotná digitální brána;

Nové české zákony:

- zákon o službách vytvářejících důvěru pro elektronické transakce (č. 297/2016 Sb.) + doplňující zákon č. 298/2016 Sb.) – účinnost 19. 9. 2016,
- zákon o elektronické identifikaci (č. 250/2017 Sb. + doplňující zákon č. 251/2017 Sb.);

Opatření na centrální úrovni jsou:

- usnesení vlády č. 889/2015 k ICT projektům,
- usnesení vlády č. 265/2016 k eOP a ÚeP,
- usnesení vlády č. 347/2017 k eFA a ÚeP;

Dále pak:

- novela zákona o OP (č. 328/1999 Sb., vyhlášeno 10. 7. 2017),
- novela zákona základních registrech (č. 11/2009 Sb., účinnost 1. 1. 2017),
- novela zákona o ISVS (č. 365/2000 Sb., účinnost 1. 7. 2017),
- nový standard pro elektronické spisové služby (4. 7. 2017);

V RÁMCI GDPR

Nová evropská legislativa:

- nařízení o ochraně osobních údajů (nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, účinnost od 25. 5. 2018);

České zákony

- MV ČR připravuje komplexní změnu zákona o ochraně osobních údajů (nahradí zákon č. 101/2000 Sb.).

Pro celkový rozvoj a „hladký" chod e-governmentu Robert Piffl vidí jako stěžejní dvě věci – **elektronický dokument** a **úplné elektronické podání**.

ÚPLNÉ ELEKTRONICKÉ PODÁNÍ

Cílem úplného elektronického podání je situace, kdy občané budou při svých podáních vůči veřejné správě dokládat (doplňovat) skutečně pouze minimum údajů. Stát tedy bude veškerá potřebná data čerpat především z těch, která již vlastní, a občan dodá pouze to, co chybí, co stát ještě nemá v držení.

Díky IS VS, on-line službám, portálům atp. bude moci občan vytvořit jakýsi formalizovaný dokument, který následně podá vůči úřadu, a to v elektronické podobě. Je ovšem nutné zajistit nejen skutečnost, že úřad bude schopen takový dokument přijmout a zpracovat, ale je především nutné zajistit, aby touto cestou nevznikal digitální balast, který bude zbytečně (kapacitně, finančně, energeticky) zatěžovat. Směřujeme tedy k využití elektronických inteligentních dokumentů (definovaný kontejner obsahující vizualizovaný dokument, textovou vrstvu a strukturované údaje), které nám nabízejí možnost automatizovaného zpracování a zároveň minimalizování jejich velikosti.

Jako určitou zajímavost v této souvislosti prezentoval projekt utajovaných dokumentů v digitální podobě. Podle Roberta Piffla se bude jednat o speciální digitální dokument, který bude možné zpracovat standardními systémy elektronické spisové služby, i když bude obsahovat důvěrné informace. A samostatnou kapitolou pak je připravované automatizované zpracování elektronických faktur.

Pokud tedy v rámci informačního systému veřejné správy realizujeme nějaké podání, zcela jistě tak vzniká elektronický dokument, který je nutné náležitě zpracovat. Ať už se jedná o úplné elektronické podání, nebo o elektronickou fakturu, vždy to budou strukturovaná data, která musí plnit požadavky dalších právních předpisů, aby se dokumenty skutečně dobře zpracovávaly. V rámci těchto předpisů došlo podle Roberta Piffla za posledních 13 let k jediné zásadnější změně, a to novelizaci Národního standardu spisových služeb. Došlo vlastně ke zjednodušení tohoto standardu, ale v zásadě se dá říci, že základní principy jsou celých třináct let stejné a většina systémů elektronických spisových služeb by si měla být schopna vyměňovat informace o dokumentech právě podle těchto standardů.

PRÁVNÍ PŘEDPISY

V souvislosti s právními předpisy upozornil Robert Piffl na skutečnost, že daleko častěji jsou shledány nedostatky v plnění předpisů již dávno zavedených než v těch aktuálně nových. Kromě samotného nařízení eIDAS (nařízení č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce) byl v ČR přijat zákon o službách vytvářejících důvěru pro elektronické transakce (č. 297/2016 Sb.) a vznikl návrh zákona o elektronické identifikaci (č. 250/2017 Sb.). Výsledkem toho všeho je skutečnost, že máme k dispozici právní předpisy, které určují, jak přesně můžeme nakládat s elektronickými dokumenty, máme nástroje k zajištění důvěryhodnosti původu takových dokumentů a velice důležité právní východisko pro vzdálenou identifikaci fyzických (zatím pouze fyzických) osob s určitou vyhovující mírou jistoty.

Ve velmi krátké budoucnosti by měla být schválena a přijata nařízení, která se týkají tzv. digitální brány EU. Bude zpracována ve všech jazycích EU a bude se jednat o jakýsi evropský portál občana. Budou zde nabídnuta řešení agend základních životních situací (narození, stěhování, úmrtí...). Všechny tyto životní situace budou v návaznosti na realizaci Evropské brány muset jednotlivé evropské země upravit tak, aby byly realizovatelné elektronicky. I v tomto případě platí dvouleté adaptační období. Kromě uvedených agend bude brána rovněž sloužit jako bod, kam budou moci občané zasílat podněty na konkrétní služby e-governmentu jednotlivých států, pokud jim budou připadat nedořešené, komplikované, případně špatně nastavené.

GDPR

Jakmile budeme pracovat s elektronickými dokumenty, je podle Roberta Piffla velice pravděpodobné, že v rámci jejich životního cyklu budeme pracovat s určitými osobními údaji, což bude mít od 25. 5. 2018 zásadní dopad. Je tedy důležité si uvědomit, že osobní údaj je velice široký pojem a skutečně se dá vystopovat ve většině dokumentů, s nimiž veřejná správa pracuje. Proto je velice zásadní analyzovat, jak organizace s elektronickými dokumenty skutečně nakládá a na základě jakého účelu. V této souvislosti Robert Piffl upozornil na skutečnost, že pokud nějaký úřad shromažďuje data, která obsahují osobní údaje na základě nařízení určitého zákona, jedná se o podmínku nutnou. Požadavek zákona však není možné považovat za účel, ten je nutné definovat. Jak Robert Piffl upozornil, podobných momentů, kterým se bude nutné podrobněji věnovat, je docela dost (právo na výmaz, právo na přenostitelnost údajů atp.), proto doporučuje například webové stránky ÚOOÚ (především převodní tabulku k zákonu č. 101/2000 Sb.), případně i web Evropské komise (www.uoou.cz, https://ec.europa.eu).

Obecně se k GDPR podle Roberta Piffla dá říci, že zákon č. 101 existuje 17 let, a pokud jej úřad či instituce dodržovala, nemůže mít s přechodem na GDPR žádný problém.

EIDAS

Robert Piffl upozornil na skutečnost, že v souvislosti s nařízením eIDAS se převážně hovoří pouze o službách vytvářejících důvěru a elektronické identifikaci. Nařízení však zavádí, v rámci zajištění fungování vnitřního trhu na území EU, normativně pojmy podstatné pro práci s elektronickým dokumentem (časová razítka, pečetě, podpisy), ale i samotný elektronický dokument. Elektronickým dokumentem je zde definován jakýkoliv obsah v elektronické podobě, zejména text, audio či video nahrávka. Máme tedy v rámci EU jasně definován elektronický dokument, stejně tak i jsou jasně stanoveny právní účinky, které mimo jiné říkají, že elektronický dokument nesmí být odmítán

pro správní či soudní řízení jen proto, že je elektronický. Pokud navíc bude tento elektronický dokument opatřen kvalifikovaným podpisem, je na stejné úrovni jako listina s vlastnoručním podpisem. V návaznosti na toto s e velice často diskutuje o tom, co a kdy je dokumentem. Pro jednoduchost je podle Roberta Piffla vhodné vycházet z toho, že ve veřejné správě platí:

„Pokud mám něco ve své moci (vytvořil jsem, nebo mi někdo poslal), jedná se nepochybně o dokument dle zákona č. 499/2004 Sb., a je tedy elektronickým dokumentem dle nařízení eIDAS.“

Jak Robet Piffl upozornil, je velice důležité správně evidovat dokumenty. Zásadní evidenční pomůckou je podle jeho slov spisová služba, což bývá často opomíjeno. Řada institucí si totiž průběžně vytvářela vlastní evidenční agendy. Stejně tak je důležité, v souvislosti se zákonem o službách vytvářejících důvěru, si uvědomit, že nejpozději od konce přechodného období (19. 9. 2018) není možno, aby ve veřejné správě byl vytvořen dokument bez kvalifikovaného elektronického podpisu a časového razítka, případě elektronické pečetě a časového razítka.
MV ČR tedy připravilo všechny potřebné zákony a normy tak, abychom se mohli přihlásit ke službám veřejné správy na dálku a identifikovat se, a to v režimu 365 dní v roce. Potřebné nástroje jsou k dispozici, nyní je pouze nutné, aby veřejná správa splnila požadované. Jako jeden z bezpečných prostředků pro elektronickou identifikaci bude možné použít eOP. Jak ale Robert Piffl zdůraznil, bude to jeden z mnoha možných prostředků. Vydávat eOP se začne od 1. 7. 2018, nicméně vzhledem k tomu, že ročně se vydá zhruba 1,3 mil. občanských průkazů, je velice pravděpodobné, že budou využívány rovněž jiné identitní prostředky (pokud se některý ze soukromých poskytovatelů stane kvalifikovaným poskytovatelem).
V souvislosti s elektronickou identitou a jejím prokazováním vyslovil Robert Piffl obavu, že doposud byl kladen malý důraz na osvětu. Existuje tak řada lidí s nízkou „gramotností“ v tomto směru. Hrozí, že si nebudou uvědomovat nebezpečí, která jim plynou z vyzrazení, případně zcizení jejich elektronické identity.

ČASOVÝ RÁMEC

Na závěr svého vystoupení poradce náměstka ministra vnitra pro ICT ještě jednou zopakoval časový rámec:

2016 – služby vytvářející důvěru v praxi,

2017 – právní předpisy a nástroje připravené MV -
novela zákona o elektronických občanských průkazech,
zákon o elektronické identifikaci,
do 31. 12. 2017 úprava vnitřních směrnic a pravidel pro úplné elektronické podání;

2018 25. 5. 2018 nařízení GDPR v účinnosti,
1/2 2018 – první elektronické občanské průkazy s čipem,
1. 7. 2018 účinnost zákona o elektronické identifikaci,
29. 9. 2018 účinnost nařízení eIDAS – oznámené systémy Eid,
31. 12. 2018 povinný příjem elektronických faktur v evropském formátu a ISDOC 5.2 a vyšší.

Ještě jednou připomněl, že elektronický dokument je možné považovat za základní stavební kámen e-governemntu, a proto je vhodné si uvědomit, že mám-li s ním pracovat ve veřejné správě při respektování definic eIDAS a zákona o archivnictví a spisové službě, je nutné zajistit věrohodnost jeho původu, neporušitelnost jeho obsahu a čitelnosti, tvorbu a správu metadat náležejících k těmto dokumentům atd.
V závěru pak ještě informoval o skutečnosti, že na jaře letošního roku byla zřízena dočasná pracovní skupina pro elektronické standardy spisových služeb při Radě vlády pro informační společnost. Skupina připravila kompletní metodiku (Problematika zpracování elektronické faktury u veřejnoprávních původců), která je zároveň jakousi rekapitulací právního stavu v této oblasti za posledních 17 let (s ohledem na zákon č. 101/2000 Sb.), respektive 13 let (zákon č. 499/2004 Sb.). Krok po kroku by zde mělo být popsáno, jak se má zpracovat elektronická faktura v systému veřejné správy, jak má procházet spisovou službou atp.
Podobně pracovní skupina projednává dokument Úplné elektronické podání a rovněž vypracovala doporučení k úplnému elektronickému podání a pracuje na návrhu inteligentního elektronického dokumentu, protože jak Robert Piffl uvedl, podle jejich názoru budoucnost patří elektronickým inteligentním dokumentům, které vznikají asistovanými on-line službami.

vmware.com/cz/company/customers

vmware®

„Zajištění spolehlivého a trvalého zabezpečení citlivých informací je pro nás klíčové.

Platforma NSX nám přináší bezprecedentní možnosti.“

Miroslav Prokeš
Ředitel odboru technického rozvoje a provozu
Burza cenných papírů Praha

PRAGUE STOCK EXCHANGE
BURZA CENNÝCH PAPÍRŮ PRAHA

GDPR – co se dá stihnout včas?

Místo avizovaného Josefa Donáta nakonec v Mikulově vystupoval jeho kolega Mgr. Michal Nulíček, LL.M. ze společnosti Rowan Legal. A podle vlastních slov poněkud optimističtěji ladil nejen název, ale i celkové vyznění prezentace. Josef Donát si totiž připravoval vystoupení na téma GDPR aneb Co se zase nestihne včas? Michal Nulíček ovšem raději pohlíží na problematiku pozitivněji, a tak zvolil GDPR aneb Co se dá stihnout včas? Přece jen, podle jeho slov, zbývá do účinnosti tohoto nařízení ještě téměř devět měsíců, tedy dostatek času na to, ledacos v této oblasti stihnout ať už na úrovni obcí či větších orgánů veřejné správy. Mluvit bude o dopadech GDPR na veřejnou správu, ale také o českém zákonu, který má nahradit dosavadní zákon č. 101/2000 Sb. a který je v současné době v připomínkovém řízení (pro veřejnou správu přináší některé úlevy z povinností GDPR).

Mgr. Michal Nulíček, LL.M.

ZÁKLADNÍ DOPADY NAŘÍZENÍ GDPR

Michal Nulíček uvedl, že tématu ochrany osobních údajů se věnuje už dvanáct let. Ze zkušenosti tedy může říci, že prvních deset let registroval skutečně jen velice málo, a to spíše dceřiných firem velkých nadnárodních společností, které se skutečně zabývaly ochranou osobních údajů. Ve většině ostatních případů se jednalo o určité pokrytí souhlasu se zpracováním, nikoliv však o systémové řešení bezpečnosti. Podle jeho slov je to v podstatě logické, protože sankce za porušování zákona v této oblasti byly vlastně mizivé. Například v případě, že se jednalo o porušení při zpracování osobních údajů v rozsahu 10 až 100 tisíc osob, byla v minulosti uložena pokuta v řádu desítek korun. Lakonicky se to dá vyjádřit tak, že cena soukromí každého z nás činila jen několik haléřů. To se nyní výrazně mění, neboť sankce pro veřejnou správu v oblasti ochrany osobních údajů může dosáhnout až 10 mil. euro. Najednou je, podle slov Michala Nulíčka, o zabezpečení procesu zpracování osobních údajů výrazný zájem.

Kromě sankcí přináší nová úprava i změny v oblasti práv subjektu údajů. Sice řadu těchto práv, která upravuje nařízení GDPR, už v dnešním zákoně č. 101/2000 Sb. máme, ale nyní jsou upravena detailněji a dopadají na širší okruh případů. Některá z těchto práv jsou ale skutečně úplně nová, například právo na přenositelnost osobních údajů od jednoho správce k jinému, to zde skutečně doposud nebylo.

Michal Nulíček upozornil, že pro každého správce se tato práva upravují různě, především dle toho, na základě jakého titulu osobní údaje zpracovává. Poslední a velice důležitá oblast dopadů nařízení GDPR je v oblasti vnitřní kontroly souladu s právními předpisy. Především se jedná o zabezpečení osobních údajů, evidenci jejich zpracování, hlášení bezpečnostních incidentů atp.

HLAVNÍ PRINCIPY

Michal Nulíček upozornil, že dopady nařízení GDPR se skutečně netýkají VS pouze v momentě výkonu veřejné moci, ale velmi významně se budou projevovat například v rámci zaměstnaneckých vztahů. I proto zdůraznil tři základní principy tohoto zákona:

- **Zákonnost** – to je vlastně povinnost identifikovat v rámci GDPR určitý právní titul pro zpracování osobních údajů. Podle Michala Nulíčka se může jednat o zákonnou povinnost, nebo plnění smlouvy, či například o tzv. oprávněný zájem. Zavedení kamerových systémů může být tímto oprávněným zájmem. Je tedy vhodné právní titul činnosti, kterou organizace vykonává, stanovit a neustále ověřovat, zda pořád platí;

- **Účel** – to je rovněž klíčový prvek pro ochranu osobních údajů. Je nutné velice pečlivě na začátku stanovit, za jakým účelem organizace zpracovává dané údaje, neboť od toho se odvíjí další povinnosti. Tedy stanovit, k čemu osobní údaje potřebuje a jak je plánuje využívat, přičemž je nutné oddělit od sebe údaje potřebné pro odlišné účely;
- **Minimalizace** – je nutné zpracovávat pouze údaje v rozsahu a po dobu nezbytnou pro konkrétní identifikovaný účel. Neustále je tedy nutné si klást otázku, zda nezpracováváme údaje ve větším než nezbytném rozsahu, či je neuchováme delší dobu, než je nutná.

Tyto tři jsou řekněme těmi naprosto nejdůležitějšími principy, ale jsou zde ještě další:

- **Transparentnost** – je to otázka určitého férového přístupu, kdy organizace poskytuje informace subjektu údajů. GDPR vyžaduje, aby nyní bylo těchto informací poskytováno více a aby tyto informace byly srozumitelné a jasné;
- **Integrita a důvěrnost** – je nutné zajistit zabezpečení údajů i procesu jejich zpracování a vědět přesně, co dělat v momentě incidentu;
- **Odpovědnosti** – organizace musí být schopna dokumentovat, že skutečně své povinnosti dodržuje. To znamená, že musí vlastně dokumentovat každé své rozhodnutí v této oblasti. Pokud se například organizace rozhodne nehlásit bezpečnostní incident, protože se domnívá, že riziko pro subjekty údajů je nepatrné, musí toto své rozhodnutí zdůvodnit a dokumentovat. Pokud se organizace naopak rozhodne implementovat určitá technická opatření, musí jejich volbu odůvodnit a opět dokumentovat atp. Tedy dodržovat nařízení, dokumentovat všechny kroky a prokazovat dodržování.

POVINNOSTI

Michal Nulíček v uvedeném smyslu definoval několik základních povinností, neboť je podle něj velice důležité nepodceňovat bezpečnostní rizika a vhodná opatření začlenit do každého procesu:

- **Privacy by design** – je vhodné při návrhu zpracování a při zpracování samotném určit opatření ochrany, která jsou přiměřená stavu techniky a nákladům na provedení, povaze a riziku;
- **Privacy by default** – zajistit, že budou zpracovávány pouze nezbytné údaje, po nezbytnou dobu s přístupem pouze určených osob;
- **Compliance systém** –definujte politiku ochrany, procesy, povinnosti pracovníků a jejich plnění monitorujte a hodnoťte;
- **Zabezečení zpracování** – přijměte vhodná opatření ochrany, která jsou přiměřená stavu techniky, nákladům na provedení a povaze a riziku zpracování.

Zavedení a dodržování není podle Michala Nulíčka jen pouhým splněním určitých povinností. Je možné je chápat rovněž jako určitý štít, který chrání samotnou organizaci. Pokud bude schopna prokázat, že jako správce udělala skutečně vše, co bylo v jejích silách, aby nedošlo k porušení práv subjektů údajů, a že měla komplexní systém technických a organizačních opatření, a je možné určit, že došlo k individuálnímu selhání jednotlivce, pak se může tato organizace pokutě skutečně vyhnout.

OUTSOURCING

Další oblast, které je podle Michala Nulíčka potřeba věnovat pozornost, je jakýkoliv outsourcing v oblasti zpracování osobních údajů – ukládání osobních údajů u třetí strany, zpracování jakýchkoliv výstupů z osobních údajů třetí stranou, zpracování osobních údajů. To jsou všechno momenty, kdy použití třetí stranou nesnímá její odpovědnost za zacházení s těmito daty. Je tedy, v případě takovéto spolupráce, vždy vhodné realizovat určitou „miniprověrku", do jaké míry vybraný zpracovatel splňuje požadavky GDPR. Nové povinnosti podle něj jsou tedy především:

- **výběr zpracovatele** – vybrat důvěryhodného zpracovatele, uzavřít s ním smlouvy s nezbytnými náležitostmi a kontrolovat zpracování;
- **POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ (DPIA)** – provést posouzení vlivu u rizikových zpracování a v případě vysokého rizika konzultovat s ÚOOÚ;
- **POVĚŘENEC NA OCHRANU OSOBNÍCH ÚDAJŮ – DPO** – zajistit nezávislého a kvalifikovaného pověřence pro ochranu osobních údajů;
- **incidenty** – monitorovat, evidovat a ohlašovat rizikové incidenty ÚOOÚ a vysoce rizikové incidenty pak i subjektům údajů.

NOVELA č. 101

Vedle samotného nařízení GDPR je vhodné věnovat rovněž pozornost samotné novele zákona č. 101/2000 Sb., neboť například v oblasti posuzováni vlivu přináší pro veřejnou správu určitou úlevu. Pokud ke zpracování osobních údajů dochází na základě zákonné povinnosti, pak titulem je ona povinnost stanovená zákonem a není nutné provádět posouzení vlivu (pokud bylo provedeno zákonodárcem při přijímání tohoto zákona).

Jak bylo již řečeno, legislativní proces této novely je v současné době v plném proudu, ale jestli se jej podaří dokončit do účinnosti nařízení GDPR, není zatím zřejmé. Novela prochází sice připomínkovým řízením, ale její schvalování se trefilo na konec volebního období. Je tedy nutné počkat na výsledky voleb a sestavení nové Poslanecké sněmovny. Ovlivnit proces schvalování mohou samozřejmě i prezidentské volby. Kdy tedy nastane její účinnost, není zatím zřejmé.

POVĚŘENEC

Vedle sankcí za neplnění je funkce pověřence druhým nejviditelnějším prvkem nařízení GDPR. Důležité je si uvědomit, že se musí jednat o dostatečně kvalifikovanou osobu, která se vyzná v oblasti ochrany osobních údajů, případně v oblasti veřejné správy samotné. Bude se jednat o člověka, který bude dohlížet na dodržování požadavků nařízení GDPR v dané organizaci. Zároveň to bude jakýsi primární kontaktní bod pro subjekty údajů i pro ÚOOÚ. Michal Nulíček zdůraznil, že není skutečně vždy nutné hledat a najímat zcela nového zaměstnance. Naopak, v případě větších organizací by doporučoval zvážit, zda není vhodné zainteresovat osobu zevnitř, která zná interní procesy organizace. V případě nutnosti se pak dá outsourcovat určitá podpora tohoto pověřence. Ale mít plně outsourcovánu funkci pověřence nepovažuje pro velké organizace za vhodné a prospěšné. Naopak, smysluplný outsourcing této funkce vidí například u malých obcí, kde je možné, aby několik obcí „sdílelo" stejného pověřence, který je vybaven potřebným know how.

ZÁVĚR

Závěrem Michal Nulíček shrnul, že pokud konkrétní organizace s přípravami doposud nezačala, je ta pravá chvíle rozhodnout se, zda bude projekt řešit externě, interně, či nějakou kombinací. Ve všech případech však platí, že se nejedná o proces, který by vyřešila veřejná správa v rámci několika dní. Rozhodně je podle něj dobré začít zmapováním toho, jaké údaje a proč vlastně organizace zpracovává a na základě jakých titulů. A především je nutné si uvědomit, že se toto týká nejen osobních údajů v rámci výkonu veřejné správy, ale rovněž v rámci zaměstnaneckých vztahů. U všech těchto položek (zpracování uchazečů o zaměstnání, zpracování osobních údajů zaměstnanců pro účely plnění smluvního vztahu, zpracování osobních údajů kamerovými systémy atp.) je nutné posoudit soulad a nesoulad s plněním nařízení GDPR. V případě identifikace nesouladu pak zvolit a navrhnout způsob jeho odstranění. A především je potřeba umět stanovit priority, neboť je zřejmé, především u větších organizací, že se ne zcela vše podaří nastavit do účinnosti nařízení GDPR. Podle Michala Nulíčka je možné za prioritní považovat vnější dokumentaci, informace pro subjekty údajů, jmenování pověřence atp.

Ani ti, kteří se spoléhají na služby zpracovatele, by neměli vyčkávat, ale měli by se začít ptát, jak tito zpracovatelé mají své vnitřní normy a postupy v souladu s legislativou, jak zajišťují technické a organizační opatření a případně upravit nyní platné smlouvy tak, aby v dlouholetém horizontu odpovídaly požadavkům nařízení GDPR.

GDPR má tedy rozhodně zásadní dopady na veřejnou správu. Připravovaná novela zákona pro ni přináší určitou úlevu, ale neznamená komplexní vynětí z jeho nároků. Proto je potřeba i nadále sledovat legislativní proces v této oblasti.

INTRODUCING

CHECK POINT
INFINITY

THE CYBER SECURITY ARCHITECTURE
OF THE FUTURE

CLOUD MOBILE THREAT PREVENTION

Check Point®
SOFTWARE TECHNOLOGIES LTD

Snadná navigace světem úřadů

Konference, která má usnadnit navigaci světem úřadů. Konference, která je určena nejvyšším státním úředníkům, starostům a tajemníkům obcí. Konference, která osvětlí koncepce a strategie, směřování e-governmentu a spolupráci napříč resorty. To je akce, kterou pořádá NAKIT ve spolupráci s Úřadem vlády a Ministerstvy vnitra, financí, průmyslu, místního rozvoje, práce a zemědělství. To je akce, která proběhne 2. listopadu od 9:30 hod. na pražském Žofíně. Jejím moderátorem bude Martin Veselovský. O konferenci jsme si povídali s Romanem Vrbou, ředitelem odboru e-governmentu MV ČR.

„Na unikátní listopadové konferenci nabídneme úřadům zásadní informace o novinkách z e-governmentu,“ říká Roman Vrba z Ministerstva vnitra.

Tématem, které zcela jistě zaujme mnoho posluchačů, bude GDPR. Informace o konferenci – tématech i řečnících – budeme průběžně aktualizovat na stránkách **www.eKonference.eu**.

- **Co se na konferenci její účastníci dozví?**
  Cílem je představit zástupcům úřadů z celé republiky nové trendy, koncepce a strategie v oblasti e-governmentu na jednom místě. Detailně představíme nový portál občana. Budeme mluvit samozřejmě o chystaném zavedení využívání elektronické identity. Kolegové ze zahraničí, například z Velké Británie nebo z Estonska, také popíší jejich vlastní zkušenosti s implementací e-governmentu.
  V odpoledním bloku se také chceme věnovat novým e-službám, které jsou ve většině těsně před spuštěním, například e-neschopenka, e-recept nebo e-fakturace.

- **Kolik bude poplatek a kde se mohou zájemci registrovat?**
  Zájemcům z veřejné správy nabízíme účast na konferenci zdarma. Právě pro ně je tato akce určena. Mohou se registrovat na webových stránkách konference. Ostatní zájemci si mohou na stejném místě vstupenky koupit. Jako u jiných podobných akcí i tady platí otřepané pravidlo, kdo dřív přijde, ten dřív mele. Zaprvé bude mít šanci se vůbec ještě na akci dostat kvůli omezenému množství vstupenek, které zbývají, zadruhé budou vstupenky čím dál blíže k datu konference dražší.

- **Je ještě nějaká jiná možnost, jak konferenci sledovat?**
  Ano, právě proto, že očekáváme o konferenci velký zájem, rozhodli jsme se, že ji budeme živě přenášet na internetu, na webových stránkách konference včas zveřejníme detaily, kde přenos naleznete.

Konference, která je určena nejvyšším státním úředníkům, starostům a tajemníkům obcí.

2. listopadu 2017 od 9.30 hod. na pražském Žofíně

- **Proč jste se vlastně rozhodli pro uspořádání takové konference?**
  Žádná konference, kterou by si napříč resorty organizovala veřejná správa sama pro sebe tu není a cítíme ze strany úřadů oprávněný hlad po informacích. Nemůže to být tak, že my v ústředních orgánech státní správy budeme něco vymýšlet, zpracovávat k tomu příslušné legislativní procesy a následně necháme úřady – samosprávu – na holičkách. Jen při úzké spolupráci s nimi máme šanci na to, aby se u nás e-government rozvíjel tak, aby to odpovídalo moderním trendům v komunikaci občanů s úřady.

  Zároveň chceme, a to je podle mého názoru výjimečné, na konferenci dát velký prostor posluchačům, aby se z nich vlastně stali spolutvůrci konference – v každém bloku budou mít velký prostor pro diskusi, kde budou moct zástupcům jednotlivých ministerstev, náměstkům a ředitelům odborů, příslušným expertům a dalším osobnostem pokládat otázky na témata, která je nejvíc zajímají.

„GINIS bude na GDPR připraven," informoval GORDIC v Mikulově

GDPR bylo na mikulovské konferenci tématem číslo jedna. Cílem Obecného nařízení o ochraně osobních údajů (General Data Protection Regulation neboli GDPR) je výrazně zvýšit ochranu osobních dat občanů. Jedná se o dosud nejucelenější soubor pravidel na ochranu dat na světě. Nařízení nabývá účinnosti už 25. května 2018 a role informačního systému zpracovavatele pro zvládnutí všech požadavků bude velmi podstatná.

GDPR nařízení vzniklo za účelem dát občanovi větší kontrolu nad tím, jak je s jeho osobními údaji nakládáno a co se s nimi děje. Dává mu například právo „být zapomenut", tedy zrušit souhlas se zpracováním svých osobních údajů a nechat je vymazat nebo vzít si bezplatně své osobní údaje a přenést je jinam.

Pro zpracovatele údajů naopak znamená nová legislativní norma řadu povinností. Navíc GDPR přichází až s astronomickými pokutami. Nařizuje také větším zpracovatelům dat zřídit nezávislou kontrolu -funkci pověřence pro ochranu osobních údajů, tzv. DPO. Ten má za úkol dohlížet na řádné zacházení s osobními daty a hlásit kontrolnímu orgánu daného státu úniky dat a porušení nařízení.

Víte, jaké osobní údaje eviduje Váš systém?

Zkrátka není toho málo, co se na firmy a úřady valí. Navíc výklad některých ustanovení nařízení není jednotný. Z důvodu existence řady nejasností bylo rozhodnuto, že v průběhu přechodné doby před platností nařízení GDPR budou upřesněny výklady, kterých se vzniklé nejasnosti dotýkají. V rovině EU poskytne potřebná vysvětlení skupina WP29, v národním prostředí tuto funkci zajistí Úřad pro ochranu osobních údajů (ÚOOÚ). Oběma subjektům byl tento úkol svěřen na základě rozhodnutí Evropské komise.

Jasný ale zůstává fakt, že klíčovou roli pro zvládnutí požadavků GDPR bude představovat nastavení interních procesů v každé organizaci. Ta by se měla věnovat identifikaci výskytu osobních údajů a nechat si zpracovat analýzu shody nakládání s osobními údaji s výše uvedeným nařízením. Následovat by mělo zpracování popisu rizik s doporučeným řešením.

V čem může pomoct samotný informační systém organizace? Bezpochyby právě v identifikaci osobních údajů a jejich uložení. Prostřednictvím systému je dále možné vyhledat a předat požadované údaje (popřípadě je měnit a mazat), zaznamenávat zpracování údajů, včetně důvodu a autora, řídit přístup k datům pouze pro oprávněné uživatele nebo zajistit dostupnost logů. A nezapomínejme na zabezpečení. „Provozovatel systému chce mít (oprávněně) nejen jistotu, že bude mít potřebné informace během celého životního cyklu údaje, ale i že jeho data jsou potřebným způsobem chráněna například díky pseudonymizaci nebo šifrování," říká analytik David Brychta, který je supervizorem implementace nařízení GDPR do systému GINIS.

GINIS: 4 oblasti GDPR podpory

Platforma GINIS byla navržena tak, že již v základech tohoto informačního systému jsou položeny klíčové stavební kameny GDPR. Jedná se například o zmíněnou pseudonymizaci dat nebo možnost jejich šifrování. *„Na tomto základě jsme vybudovali komplexní řešení podpory GDPR, které se primárně soustředí na řízenou práci s osobními údaji subjektu údajů (externích subjektů), se kterými uživatelé pracují,"* vysvětluje David Brychta.

Čtyři oblasti podpory GDPR v rámci platformy GINIS: logování, výmaz osobních údajů, analytické nástroje a náhledy na data.

Další základní funkcionalitou, kterou systém disponuje, je řízení přístupu k osobním údajům mezi agendami. Obdobně jako v případě základních registrů (SZR) tak bude možné pracovat s osobními údaji pouze v rámci dané agendy. Systém lze konfigurovat tak, aby práce s osobními údaji byla prováděna pouze v rámci dané agendy.

Aby bylo možné využívat připravovaných nových funkcionalit, je nutné, aby daná organizace měla přehled o legislativních důvodech evidence osobních údajů. Proto byla do systému GINIS implementována evidence těchto legislativních důvodů.

Důslednou analýzou nařízení a všech dostupných zdrojů informací stanovil GORDIC několik základních oblastí, které jsou řešeny v rámci vývoje platformy GINIS: logování, výmaz osobních údajů, analytické nástroje a náhledy na data.

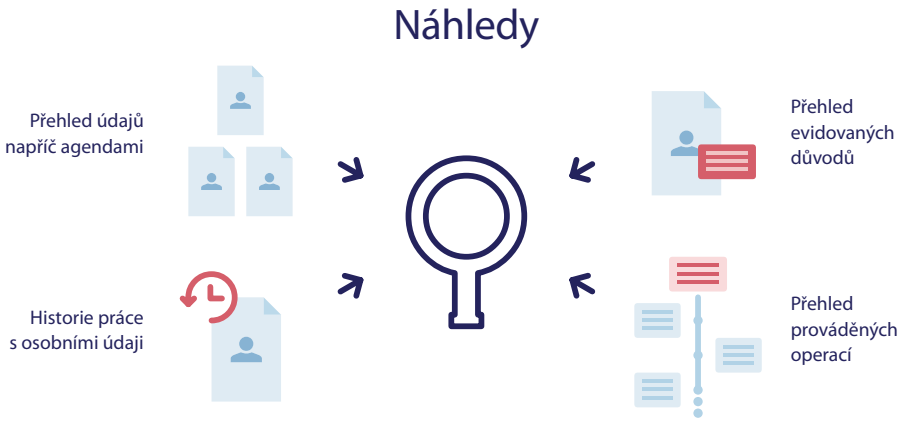
Občan se zeptá, Vy budete připraveni

Logování odpoví na otázku, „kdo a co dělal s mými osobními údaji." GINIS® je rozšířen o podrobné logování práce s externími subjekty v souladu s evropským nařízením a jím definovaných operací. Ve všech částech systému budou požadované operace s osobními údaji sledovány. Výsledkem logování bude snadné a průkazné dohledání všech přístupů a operací v celém systému GINIS.

Výmaz osobních údajů umožnuje reagovat na požadavek, „vymažte všechny mé osobní údaje!" Je však potřeba si uvědomit, že výmaz osobních údajů není absolutní právo a podléhá určitým pravidlům, za jakých je možné provést odstranění dat z organizace či systémů. Výmaz osobních údajů, evidovaných ze zákona, bude možný až po úspěšné realizaci skartačního řízení navázaného dokumentu.

Máte přehled, co se z pohledu ochrany osobních údajů v systému děje? Ano, uživatel ho bude mít. Do GINISu jsou zaváděny **nové analytické a integrační nástroje**, které umožňují provádění kontrol osobních údajů, zpracování pravidelných analýz i monitoring stavu celé kartotéky externích subjektů. Praktické využití analytických nástrojů lze využít např. pro provádění konsolidace kartotéky externích subjektů. Jedním z možných výstupů je informace o tom, které osobní údaje nejsou používané, jaké osobní údaje jsou evidovány duplicitně nebo z jakých externích systémů případně vznikají.

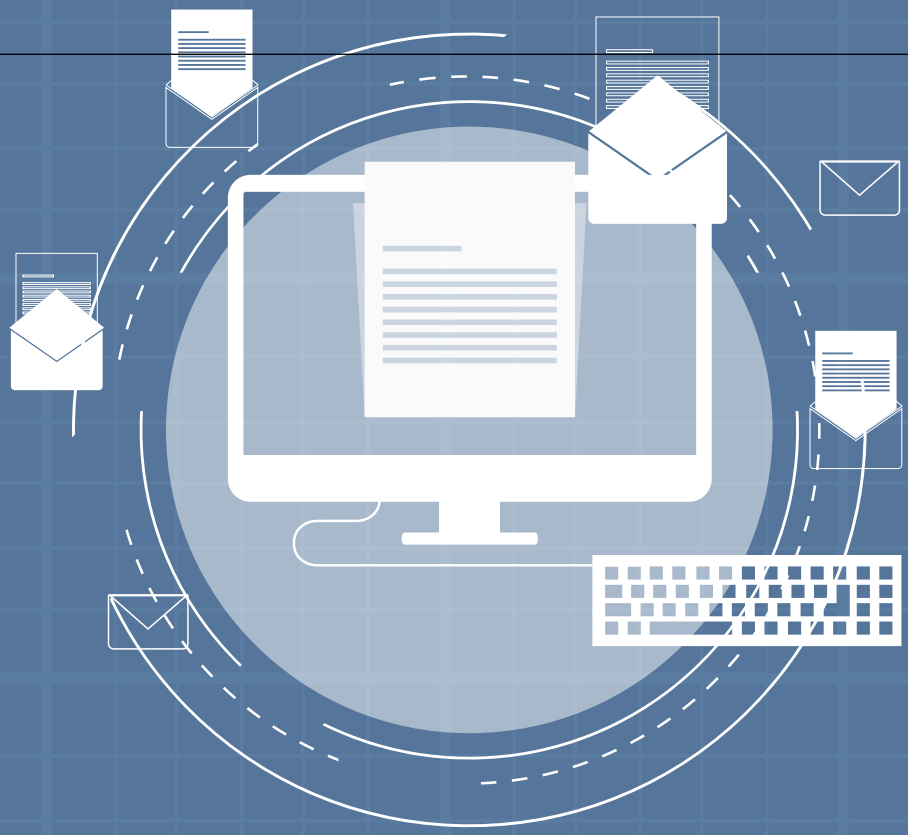
Náhledy „Co o mně evidujete? A k jakému účelu?" Odpověď na tyto otázky usnadní náhledy na sledované operace s daným externím subjektem. Tiskové výstupy přehledně zobrazí jak nakládání s daty, tak dohledání navázaných objektů, ke kterým se externí subjekt váže. Součástí je též podpora portability.



Díky analytickým nástrojům umožní GINIS pravidelné kontroly osobních údajů i monitoring stavu kartotéky externích subjektů

Bc. Radka Šustrová
marketingová specialistka

GORDIC®



Kvalifikovaná služba pro spisové služby a úložiště dokumentů

V celé Evropské unii se díky nařízení eIDAS spustil nezvratný proces digitalizace, Česko nevyjímaje. Všichni, kdo pracují s internetovým bankovnictvím a již nechtějí platit za papírové výpisy, chodit na poštu a do banky, jsou první, kdo jsou již dnes připraveni na digitální komunikaci jak s úřady, tak s velkými korporacemi v oblasti utilit, operátorů bank apod. Nařízení eIDAS jim všem dává jednotná evropská pravidla, jak takovou digitální komunikaci realizovat, aniž by hrozilo, že adresát digitálního podání může toto podání odmítnout.

V současné době běží přechodné období, které přináší povinnost vyznat se například v různých druzích elektronických podpisů – uznávaný podpis, kvalifikovaný podpis nebo třeba zaručený podpis. Víte, kdy a kdo má který podpis použít a za jakých podmínek? Víte to jistě? A víte, jak správně pracovat s elektronickými dokumenty, jak elektronické dokumenty archivovat a mít jistotu, že uchováte platnost jejich elektronických podpisů, pečetí nebo razítek v čase třeba pro soudní jednání někdy v budoucnu? Je nutné si uvědomit, že pokud dostanete správně odbavený elektronický dokument, je pro danou věc tím jediným důkazem a je nutné se o něj starat, aby bylo stále ověřitelné, že takový dokument je stále elektronickým originálem. Je to stejné jako u papírových originálů, které si dáváte do svého trezoru.

Proč tedy využívat kvalifikované služby vytvářející důvěru

Všichni ti, kteří mají chuť digitálně komunikovat, ale nemají čas nebo schopnosti vše sledovat, by měli raději využívat kvalifikované služby vytvářející důvěru. Jejich používáním získají jistotu, že jejich práce s elektronickými dokumenty bude správná a bude odpovídat všem legislativním požadavkům, včetně nařízení eIDAS. Především však klienti těchto služeb získají bezpečný nástroj pro svoji práci. Poskytovatel služby vytvářející důvěru ručí za správnou funkci služeb podle zákona, a je tudíž odpovědný za případné vzniklé škody. S určitou mírou zjednodušení se dá říct, že klient využíváním kvalifikované služby získává pojistku pro práci s elektronickými dokumenty – pokud se „něco pokazí při ověřování“, odpovědnost za vzniklou škodu nese poskytovatel kvalifikované služby a klient je ochráněn. Dobrým příkladem je nová služba SecuSign od Software602, která poskytuje kvalifikované služby vytvářející důvěru pro ověřo-

vání platnosti podpisů, pečetí a razítek a uchovávání důvěryhodnosti podpisů a pečetí, a to pro všechny kvalifikované poskytovatele v Evropě. Software602 se tak stal prvním a zatím jediným poskytovatelem obou těchto služeb v celé Evropské unii. S touto službou získáte jasný přehled o úrovních použitých elektronických podpisů, včetně dopadu na jejich právní váhu.

Kvalifikovaná služba je však úplně nejdůležitější v oblasti dlouhodobého uchování elektronických originálů. Nařízení eIDAS v této oblasti stanovuje způsob, jak takové dlouhodobé uchovávání provádět. Jedná se o to, že vše má být optimálně součástí původního dokumentu. Jedině tak si zajistíte fakt, že digitální dokument je pouze na jednom místě, můžete kdykoliv změnit způsob jeho uchovávání v čase a nejste tak závislí na některém poskytovateli nekvalifikovaných služeb vytvářejících důvěru. Zároveň máte jistotu škodní odpovědnosti poskytovatele kvalifikovaného uchovávání v případě, že by zajištění dlouhodobé ověřitelnosti Vašeho cenného digitálního originálu nebylo provedeno správně a Vy jste o svůj elektronický originál defacto přišli.

K dlouhodobé ověřitelnosti digitálních dokumentů totiž jistě patří i dlouhodobá čitelnost těchto dokumentů. S tím souvisí i další podpůrné služby SecuSign pro správné vytváření elektronicky podepsaných dokumentů, zajištění dlouhodobé čitelnosti PDF dokumentů konverzí do PDF/A, zajištění autorizované konverze z moci úřední přímo z Vašeho informačního systému a celá řada praktických nástrojů pro snadnou práci s elektronickými dokumenty.

Dalším důležitým důvodem použití kvalifikované služby je nezávislost na dodavateli. Kvalifikované služby jsou popsány prováděcími rozhodnutími, a proto máte možnost čerpat kvalifikované služby od libovolného poskytovatele těchto služeb. Kromě toho jsou poskytovatelé kvalifikovaných služeb pravidelně kontrolováni orgánem dohledu a je tedy zaručeno, že jejich služby musí být technicky trvale aktuální.

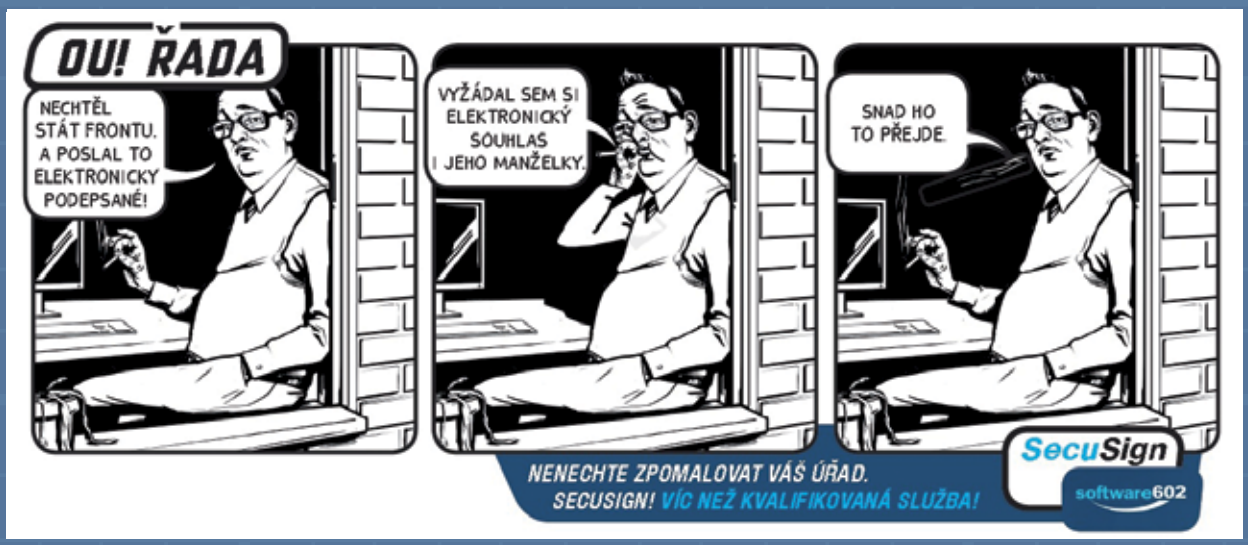
Nařízení eIDAS a elektronické dokumenty

Nařízení eIDAS přineslo rovnost mezi papírovými a elektronickými dokumenty. To je věc důležitá a pro digitalizaci státní správy nezbytná. S rostoucím množstvím digitálních dokumentů však také roste riziko chybného rozhodnutí na základě neověřeného (nebo špatně ověřeného) digitálního dokumentu. Aby se právě toto nestávalo, existují kvalifikované služby vytvářející důvěru. Ty jsou uživatelům, kteří digitální dokumenty vytvářejí či přijímají, v mnoha ohledech nezbytným pomocníkem. Koneckonců každý z nás ví, proč je dobré mít pojistku na vlastní zdraví či majetek. A doba, kdy je dobré „mít pojištěné" i digitální dokumenty, již nastala.

Na první pohled se zdá, že použití elektronických podpisů, značek, pečetí a časových razítek je složité a nemotorné. V odborné terminologii se často používají termíny, které běžným lidem nic neříkají: PAdES, XAdES, CAdES, ASiC, CRL, OCSP, Rozhodný okamžik, Identifikátor zásad=2.23.134.1.4.1.18.100, Trust List... Tak použijte kvalifikovanou službu, abyste nemuseli klikovat před digitálními dokumenty jako pan OU! ŘADA na obrázku...

Ing. Pavel Nemrava, ředitel divize Public

software602



Investiční mapa poskytuje občanům města Blanska dokonalý přehled o městských investicích

V loňském roce řešil Městský úřad Blansko požadavek investičního odboru na srozumitelnou formu prezentace vynakládání prostředků z rozpočtu města – znázornění investičních akcí a větších oprav a rekonstrukcí majetku města, které by nabízelo umístění jednotlivých akcí na území města i jeho částí. Hlavním cílem bylo zajistit občanům přehledné informace o tom, kolik prostředků je investováno právě v jejich zájmové oblasti v jednotlivých letech.

Bez ručního zadávání

Jako řešení byla zvolena investiční mapa firmy GORDIC. Jedním z hlavních důvodů výběru této varianty byla i jednoduchost celé implementace a fakt, že realizace nevyžadovala ruční zadávání informací. Modul investiční mapy plně spolupracuje s moduly systému GINIS a plynule navazuje na vlastní zpracování přípravy návrhu rozpočtu, jeho schválení i následné úpravy rozpočtu. Správci rozpočtu následně stačí pouze označit investiční akce, které chce na mapě zveřejnit, a systém data bez dalšího přebírá.

Jedná se o transparentní a srozumitelnou formu prezentace ekonomických dat ze systému GINIS (přímá integrace s aplikacemi plán akcí a balancování rozpočtu), která umožňuje sdělovat informace o aktuálních nebo zamýšlených investicích, zejména z oblastí rozpočtu a účetnictví. Díky aplikaci, která využívá podkladových map společnosti Google, mohou občané získávat přehledné informace o městských investicích i jejich rozmístění.

Pomoc i pro zastupitele

Kromě zajímavé formy mapy je výhodou i snadné a intuitivní ovládání. Občané vyhledají nejen místo, ve kterém jednotlivé projekty probíhají, ale i jejich cenu, zdroje financování a stav čerpání investic z městského rozpočtu. Navíc si mohou jednoduše rozčlenit projekty a vyobrazené akce podle kategorií. V mapě lze prezentovat i další informace ze smluv nebo faktur, popř. připojovat fotografie.

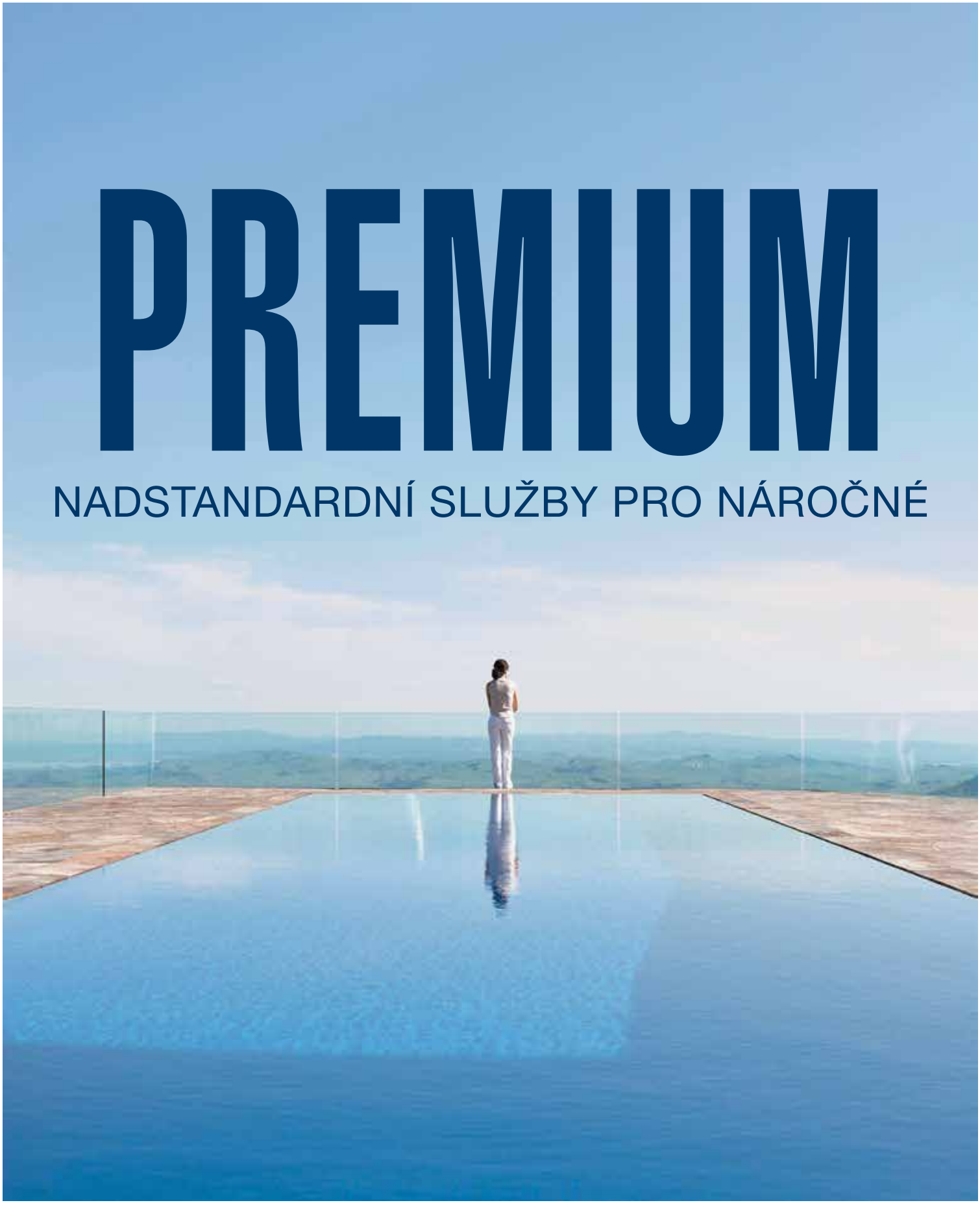
Město Blansko využívá mapu nejen pro zveřejňování investičních akcí, ale i vybrané akce neinvestiční povahy, jako je větší údržba a rekonstrukce apod. Tato forma zveřejňování akcí rozpočtu se ukázala prospěšná i při projednávání návrhu rozpočtu města. V interní verzi je možno odprezentovat územní rozložení plánovaného akcí na jednání zastupitelům, kteří tak přehlednou formou získávají informace o proporcionálním rozmístění prostředků rozpočtu a mohou tak snadněji návrh připomínkovat.

Co občany zajímá? Cena nebo termín dokončení

Pro občany i interní využití městem je důležitá i okolnost, že mapa umí zobrazovat čerpání prostředků za jednotlivé roky a je možno takto lehce získat přehled i v dlouhodobějším horizontu. Údaje na jednotlivé položce uvádějí název akce, rozpočet schválený upravený i stav čerpání. Informace mohou být doplněny i o termín vlastní realizace, případně doprovodnou poznámku. Mapa řeší kromě akcí umístěných na konkrétní adrese i akce zahrnující celou ulici, křižovatku, most apod. Adresu lze nahradit i přiřazením souřadnic umístění akce.

Na vlastní realizaci projektu se podílel především odbor finanční ve spolupráci s oddělením informatiky. Při řešení vycházeli z požadavků a podkladů dalších odborů města. Po zhodnocení projektu investiční mapy na Městě Blansku je patrné, že došlo k vyřešení původního požadavku. Z původního záměru prezentace pro veřejnost byl projekt rozšířen i pro interní využití. Zařadil se plnohodnotně mezi další využívané komponenty Interaktivního úřadu firmy GORDIC využívaných městem, jako je Rozklikávací rozpočet, Rozklikávací smlouvy nebo Portál občana.

Ing. Michal Tausch
marketingový specialista
Gordic, spol. s r. o.



ČSOB Premium

Získejte to nejlepší z bankovních služeb a produktů a poznejte prvotřídní péči.

Dejte prostor svým přáním a požadavkům a dovolte nám spolu s vámi najít cestu, jak je naplnit. Jsme připraveni splnit vaše nároky na osobní péči, diskrétnost, prestižní služby i nadstandardně výhodné produkty. Díky bezkonkurenčnímu zázemí dokáže ČSOB Premium poskytnout svým klientům zcela unikátní řešení pro každou životní situaci.

800 370 370 | www.csobpremium.cz

ČTÚ předal dokumenty do Národního digitálního archivu

Český telekomunikační úřad jako jeden z prvních provedl rutinní skartační řízení v systému GINIS a předal vybrané elektronické dokumenty, zatím fakticky pouze metadata, k uložení do Národního digitálního archivu (NDA). Pro tvorbu skartačních návrhů, tvorbu SIP balíčků, automatickou komunikaci s NDA a celkově pro řádné ukončení životního cyklu dokumentů ČTÚ využil nástroj Elektronické skartační řízení (ESR) systému GINIS s podporou dalších modulů. Se svými zkušenostmi při realizaci řešení v prostředí úřadu, který je z hlediska počtu podání jedním z nejvytíženějších v zemi, se s námi podělili Milan Mičienka, odborný referent ČTÚ, a Ing. Miroslav Kunt, archivní inspektor Národního archivu."

Český telekomunikační úřad je jedním z prvních v zemi, který řádným způsobem předal ze svého elektronického systému spisové služby elektronické dokumenty k archivaci. Čemu vděčíte za to, že jste byli tak rychlí a stali se v tomto směru jedním z průkopníků?

Elektronický systém spisové služby byl v ČTÚ zaveden v roce 2004, ale řádný výkon spisové služby zde má svoji tradici, dbáme na řádnou evidenci a správu dokumentů v průběhu jejich celého životního cyklu. To je komplikováno enormním množstvím podání, které ČTÚ ročně – většinou ve správním řízení – zpracovává. Když k tomu připočteme dlouhé skartační lhůty (obvykle přes 10 let), musíme zajistit řádné vyřazení nejen dokumentů, ale i jejich metadat. Mimochodem i metadata v systému obsahují osobní údaje, takže řádné zakončení životního cyklu dokumentů v systému je s ohledem na nařízení GDPR nutností. Proto jsme včas konzultovali problematiku jak s dodavatelem, firmou GORDIC, tak s Národním digitálním archivem.

Jak moc byla příprava elektronických dokumentů k archivaci časově či procesně náročná?

Tím, že jsme, jak říkáte průkopníky, příprava samozřejmě časově náročná byla a neobešla se bez problémů. Ty se postupně podařilo odstraňovat, ale zároveň se objevovaly

další. Je to způsobeno také tím, že pracujeme s daty, které byly pořízeny ještě před účinností dnes platné legislativy. To je daň za to „průkopnictví". Zatím všechny dokumenty nebo jejich metadata, které byly zařazeny do elektronického skartačního řízení, podléhají úlevám stanoveným Národním archivem. Jsou například minimalizována povinná metadata nutná k vytvoření SIP balíčku, komponenty není nutné převádět do výstupních datových formátů. Týká se to jen dokumentů vyřízených a uzavřených do 31. 7. 2012. Proto bude důležité při vyřízení a uzavření spisů, aby byly nastaveny veškeré kontroly dle národního standardu pro elektronické systémy spisové služby a vyhlášky č. 259/2012 Sb. a elektronické dokumenty byly již ve výstupním formátu. V současné době již máme ve spisovně kolem 5200 dokumentů s rokem zařazení do skartačního řízení 2017, které musí být uvedeny do souladu s legislativou. Jsou upravovány v modulu SUD, RAK a PAR. Samotné elektronické skartační řízení se pak provádí v modulech ESR.

V aktuálním skartačním řízení jsme vyřadili 1905 SIP. Z nich bylo pět nástroji Národního digitálního archivu odmítnuto jako nevalidní a byla nutná jejich oprava. Národnímu archivu jsme předali celkem 103 písemností v listinné podobě a jejich metadata v podobě digitální.

Má Váš úřad z hlediska práce s elektronickými dokumenty nějaká specifika?

Specifikum spatřuji ve skladbě dokumentů. Převážná většina dokumentů obsahuje povinnost k finančnímu plnění, vlastně jde o rozhodování účastnických sporů v elektronických komunikacích. Navíc po vyřízení a uzavření spisů, a tedy i po předání do spisovny, jsou spisy vyžadovány k nahlédnutí nebo k předložení soudům – někdy se značným odstupem od jejich vzniku (některé kauzy to dotáhly až k Ústavnímu soudu). Spisy je tak nutno vyjímat z balíků a zapůjčení evidovat v systému GINIS.

Jaké dokumenty budete jako ČTÚ předávat k archivaci?

Skartační návrh oblastních odborů zahrnuje průměrně kolem 120 běžných metrů ročně (zde se jedná především o uvedená finanční plnění). Z „centrály", resp. ostatních odborů, je navrhováno kolem 15 bm ročně. Co bude předáno Národnímu archivu záleží na jeho rozhodnutí, ale jsou to až na výjimky dokumenty „centrály" – zde vybírá vždy i z dokumentů skartačního znaku „S" a naopak, některé „A" přeřadí ke zničení. Kromě běžného „úřadu" (výroční zprávy, zápisy z porad vedení) jde o velmi odbornou agendu, např. koordinace frekvencí, měření radiového spektra, certifikace telekomunikačních zařízení, řízení ohledně propojovacích smluv a cen telekomunikačních operátorů.

Co byste doporučili úřadům, které se na archivaci dokumentů teprve chystají?

Co nejdříve provést se „svým" archivem zkušební skartační řízení, co nejrychleji nastavit kontroly metadat k vytvoření SIP balíčku a převod do výstupního datového formátu již na vstupu nebo při vyřízení a uzavření spisů. Jinak se budou hromadit ve spisovně dokumenty, které nebude v silách zaměstnanců zvládnout. Bez potřebné úpravy nebudou moci být zařazeny do elektronického skartačního řízení. „Náš" Národní archiv podle svého stanoviska předpokládá u nepřipravených dokumentů a spisů vyřízených nebo uzavřených po 31. 7. 2012 zastavení skartačních řízení a zahájení řízení správních pro neplnění povinností vyplývajících ze zákona.

Bc. Lucie Pišlová
marketingová specialistka
Gordic, spol. s r. o.

MISS EGOVERNMENT 2017

Robert Piffl se ve svém vystoupení věnoval dopadům evropské i české legislativy na elektronické dokumenty a procesy e-governmentu. Proto v úvodu vystoupení připomenul, o jaké předpisy, opatření a nařízení se jedná.

CO JE MISS EGOVERNMENT

Jedná se o soutěž, kterou každoročně (od roku 2009) vyhlašuje magazín Egovernment a která je určena VŠEM sympatickým dámám, které pracují ve veřejné správě. Vzhledem k postupující elektronizaci veřejné správy jsou vlastně všichni pracovníci veřejné správy účastníky e-governmentu (elektronické veřejné správy).

Přihlásit do soutěže se tedy mohou skutečně všechny dámy, které v ní pracují. Může se jednat od referentky, vedoucí odborů, tiskové mluvčí, obsluhu Czech POINTu, pracovnice spisové služby, starostky, tajemnice, náměstkyně ..., které jsou zaměstnány na ministerstvu, magistrátu, MěÚ, OÚ či v rámci organizace zřizované některým z těchto úřadů, případně na kontaktních místech České pošty nebo Hospodářské komory atp.

Soutěž je zároveň určitým poděkováním všem, kteří se věnují výkonu elektronické veřejné správy. Zároveň chceme představit sympatické dámy, neboť převážně ony ve veřejné správě pracují, a také trochu navodit příjemnou a zábavnou atmosféru jako poděkování za jejich práci.

JAK SOUTĚŽ PROBÍHÁ?

Soutěžící dámy posílají své profily, které magazín Egovernment umisťuje na své webové stránky, kde mohou čtenáři pro jednotlivé soutěžící hlasovat. To znamená, že návštěvníci tohoto webu mají možnost přidělovat své hlasy jednotlivým dámám. Deset dam, které vždy do konce července nasbírají největší počet hlasů, automaticky postupuje do finálového večera na zámku Mikulov.

Společenský večer na zámku je součástí výroční konference e-government 20:10, aneb žijem si jak na zámku, ať to trvá věčně. Soutěž Miss Egovernment je jednou z jeho součástí, jejímž cílem je pobavit přítomné a ocenit ty, kteří realizují veřejnou správu v první „linii".

Dámy se zde tradičně v krátkém rozhovoru s moderátorem představí. Dále mají možnost předvést svoji volnou disciplínu (tanec, zpěv...) a rovněž jim bývá zadána nějaká „povinná" disciplína, kterou musí zvládnout všechny.

Na vítězky čekají hodnotné ceny, které jim sice nezmění život, ale rozhodně jsou příjemné (v minulých ročnících se jednalo například o zájezd do italského Milána, wellness pobyt v Mikulově, tablet – iPad atp.). Krom toho podzimní číslo magazínu Egovernment vždy přináší rozhovory a fotografie prvních tří dam, což právě plníme.

SOUTĚŽNÍ CENY

Sympatické dámy soutěží nejen o přízeň publika a poroty, ale rovněž o zajímavé ceny, které věnují partneři soutěže. V roce 2017 si vítězka odvezla:

- tablet iPad od společnosti Apple;
- možnost ubytování v hotelu Galant v Mikulově spojenou s víkendovým wellness pobytem pro dvě osoby;
- zapůjčení vozu SEAT na víkend a
- hodnotné ceny od MV ČR.

Obdobně byly obdarovány rovněž dámy na druhé a třetí pozici.

Samozřejmě, že v příštím ročníku, který je jubilejním desátým, bychom rádi nabídli ještě poutavější ocenění pro jednotlivé soutěžící.Kromě cen je rovněž velice důležité, aby vítězky byly skutečně pečlivě vybrány. Proto dáváme velký důraz na složení poroty. Letos v ní usedli:

- RNDr. Josef Postránecký, náměstek ministra vnitra pro státní službu;
- Květoslav Štrunc, CISCO;
- Jakub Fiala, GORDIC;
- Karolína Doskočilová, Miss Egovernment 2016;
- a v pozici předsedkyně poroty Mgr. Jana Vildumetzová, hejtmanka Karlovarského kraje a předsedkyně Rady AK ČR.

Pozor, již nyní je možné se hlásit do jubilejního desátého ročníku soutěže MISS EGOVERNMENT 2018.

Další informace najdete na www.egovernment.cz v sekci MISS.

Porota pak na základě předvedených výkonů určila toto pořadí:

MISS EGOVERNMENT 2017

Michaela Vyšehradová

Věk: 33 let

Pracoviště: Česká pošta Blansko 1

Zaměstnancem České pošty je již 12 let. Začínala jako administrátorka pošt, pracovnice přepážky, dále vedoucí na malé poště a nyní pracuje 3. rokem na poště Blansko 1, kde je na přepážce Czech POINTu a občas zaskakuje za kolegyně na speciální přepážce České pojišťovny. Je velice energická a téměř žádný sport jí není cizí. Miluje cyklistiku, in-line bruslení, lyžování, plavání, pěší turistiku po krásách naší malebné krajiny a velice ráda také cestuje. Jelikož má doma budoucího prvňáčka, všechen volný čas chce trávit s ním a plně se mu věnovat.

V kolektivu je velice oblíbená možná také proto, že ráda peče a vaří zdravá jídla a svoje výrobky testuje v práci na kolegyních.

1. VICEMISS EGOVERNMENT

Mgr. Lenka Feberová

Věk: 27 let

Pracoviště: Magistrát města Karviné

Narodila se a žije v Karviné.Ve veřejné správě pracuje již třetím rokem na odboru organizačním, oddělení právním a kontrolním na pozici právník. V současné době také lektoruje interní školení pro celý MMK – ASPI (právní systém) a registr smluv.

V kolektivu se stala velmi brzy oblíbenou pro svoje bezprostřední přátelské chování i ochotu kdykoli poradit a podat pomocnou ruku.

Lenka je neustále v pohybu. V dětství hrála házenou a v současnosti se závodně věnuje sportovní střelbě a biatlonu. Ráda si vyjede na kolečkových bruslích nebo se proběhne se svým psem Coudym. Při nepřízni počasí si zahraje badminton či navštíví fitness studio. Každopádně je to člověk, který má rád nové výzvy, a tak se s nadšením vrhla do oblasti výtvarného umění (pro ni prozatím neprozkoumané) a vytváří keramické mozaiky.

Velmi ráda cestuje a poznává nové země, jejich tradice a kulturu. Je společenská, komunikativní, přátelská...

Další informace najdete na www.egovernment.cz v sekci MISS.

2. VICEMISS EGOVERNMENT

Lucie Mahdalová

Věk: 27 let
Pracoviště: MÚ Zábřeh
Bydlí v Zábřeze, kde je také součástí skvělého týmu odboru vnitřních věcí městského úřadu. Popsala by se jako společenská, komunikativní, pracovitá, flexibilní, ochotná, empatická, ráda poznává a učí se nové věci.
Ve veřejné správě pracuje 5 let, v současné době na pozici tisková mluvčí. Hlavní náplní její práce je tolik důležitá komunikace, a to ať už s médii nebo občany prostřednictvím sdělovacích prostředků.
Snaží se město propagovat, podílí se na obsahu městského webu, zpravodaje, sociálních sítí a spolupracuje s různými místními organizacemi. V rámci jejich odboru pořádají různé akce, například Radniční noc, Rozsvícení vánočního stromu apod.
Svou práci považuje také za svůj koníček. Mimo ni má ale i další záliby, jelikož je velmi aktivní člověk. Několik let se věnovala společenskému a latinsko-americkému tanci, dva roky ho také vyučovala v místním DDM Krasohled.
Její největší zálibou je jednoznačně rodina, manžel a dvě dcery. Pokud si najde chvilku jen pro sebe, ráda čte knihy o rozvoji osobnosti, miluje cestování, pěší turistiku, dobré jídlo a jako každá správná žena i nakupování.

Přítomní diváci vybrali Miss Sympatie, kterou se stala:

Lenka Witturová

Věk: 40 let
Pracoviště: Česká pošta Nový Bor
Pochází ze sklářské oblasti, tudíž její původní profesí je malířka skla.
Na České poště pracuje 5 let, z toho jeden rok na Czech POINTu.
Začínala na malé poštičce v Polevsku, kde také bydlí. V současné době pracuje na poště Nový Bor.
Práce s lidmi ji baví. Poštěstilo se jí pracovat ve skvělém kolektivu, kterým její novoborské kolegyňky a kolega jsou. To, jaká je, mohou nejlépe posoudit lidé, kteří ji obklopují a znají. Myslí si, že je veselá, spolehlivá, pracovitá a ráda se učí novým věcem.
Na koníčky jí moc času nezbývá, má dvě dcery, kterým se snaží maximálně věnovat. Když už si nějaký čas vyšetří, renovuje starožitnosti, které sbírá.
Má ráda historii, výlety po hradech a zámcích. Také ráda jezdí na koloběžce. Nejdůležitější je pro ni rodina a především děti.

Na následující stránce najdete rozhovory s vítězkami.

Museli jsme využít práva organizátorů a oslovili jsme naše sympatické vítězky s několika dotazy k samotné soutěži. Odpovědi berte tak trochu jako pozvánku k příštímu ročníku soutěže. Bude se totiž jednat o jubilejní desátý ročník, a tak na jeho přípravách začínáme pracovat už letos. Každopádně, jestli Vás účast v soutěži Miss Egovernment jen trochu láká, přečtěte si následující rozhovory a určitě do Mikulova přijedete.

Michaela Vyšehradová – Miss Egovernment 2017

• S jakými pocity jste šla do soutěže?

Pocity jsem měla velice smíšené, moc se mi do Mikulova nechtělo, jenže jsem si řekla, že když už jsem se dala na vojnu, musím bojovat.

• Co Vás vedlo k tomu přihlásit se?

V podstatě mě přihlásila paní vedoucí.

• A jaké jste měla představy o zámeckém finále?

Pár stručných informací jsem měla od loňské vítězky Karolíny Doskočilové.

• Jak na Vás působilo finálové klání na nádvoří mikulovského zámku?

Velice pozitivně, až na trému to byl velice příjemný večer.

• Měla jste za sebou nějakou „speciální" přípravu, nebo jste do toho šla rovnou?

Speciální přípravu jsem určitě neměla (pokud se nepočítá návštěva kadeřnice a podobné ženské zkrášlující záležitosti).

• Vnímala jste v průběhu večera podporu diváků?

Na rozdíl od mých spolusoutěžících kolegyněk jsem neměla tak silnou podporu v hledišti, ale jak je vidět, nijak zvlášť mi to nevadilo.

• Co na Vaši účast v soutěži a výsledek říkala rodina, případně kolegové?

Rodina, blízké okolí, přátelé i kolegyně mi fandili a byli velice příjemně překvapeni z mé výhry.

• Jak zpětně hodnotíte tento zážitek?

Určitě kladně, byl to velice zajímavý večer a výhry jsou moc krásné a určitě si je užiju.

• Nyní připravujeme pro příští rok jubilejní desátý ročník soutěže, doporučila byste kolegyním a kamarádkám, aby se přihlásily?

Rozhodně bych to doporučila všem, koho to láká, a přitom mají na druhou stranu nějaké pochybnosti, jestli to zvládnou atd. Je třeba to vyzkoušet a třeba se na ni usměje štěstí a vyhraje.

• Na co máte největší vzpomínku v rámci celé soutěže?

Vyhlášení vítězky, všechny ostatní kolegyně už byly oceněny a já jsem tam stála a čekala, co bude, jestli budu vyhlášena i já, nebo pojedu s prázdnou domů…

• Pokud byste měla možnost rozhodnout se znovu, po těch zkušenost, přihlásila byste se?

100% ano.

Lenka Feberová, 1. vicemiss Egovernment 2017

• S jakými pocity jste šla do soutěže?

Pocity byly smíšené, nevěděla jsem, co od toho čekat, ale ráda překonávám nové výzvy, takže jsem se těšila i bála.

• Co Vás vedlo k tomu přihlásit se?

Jak jsem uvedla již při soutěži, přihlásili mě moji kolegové a já už jen pak kývla. Co k tomu vedlo je, to nevím :).

• A jaké jste měla představy o zámeckém finále?

Čekala jsem trochu větší prostor a pódium, ale jinak to naplnilo mé představy, zejména krásného prostředí a skvělé atmosféry.

• Jak na Vás působilo finálové klání na nádvoří mikulovského zámku?

Prostředí nádvoří je úžasné a komorní, a navíc kdy jindy můžete zapařit na takovém místě :).



• Měla jste za sebou nějakou „speciální" přípravu, nebo jste do toho šla rovnou?

Přípravy samozřejmě nějaké proběhly, bohužel byly dost ovlivněné mým zraněním týden před soutěží, kdy se muselo měnit všechno - od outfitu po volnou disciplínu.

• Vnímala jste v průběhu večera podporu diváků?

Podporu jsem určitě vnímala, publikum bylo skvělé a navíc mě mile překvapil můj support team, který dovezl velký transparent. To mě při prvním pohledu na něj hodně dojalo a potěšilo a dodalo odvahu v průběhu soutěže.

• Co na Vaši účast v soutěži a výsledek říkala rodina, případně kolegové?

Kolegové mi všichni gratulovali a paní vedoucí mi dokonce koupila korunku, aby mi nebylo líto, že jsem nevyhrála... a co se týče rodičů, tak ti to celé prožívali a poté samozřejmě byli hrdí, nebo to aspoň tvrdili.

• Jak zpětně hodnotíte tento zážitek?

Zážitek byla určitě zajímavý, pozitivní a nezapomenutelný.

• Nyní připravujeme pro příští rok jubilejní desátý ročník soutěže, doporučila byste kolegyním a kamarádkám, aby se přihlásily?

Určitě bych to doporučila těm, které si chtějí zkusit něco nového, nebojí se vystoupit před lidmi a chtějí zažít tu atmosféru na zámku :).

• Na co máte největší vzpomínku v rámci celé soutěže?

Největší vzpomínka jde těžko určit, jak jsem říkala, nejvíc mě dojala podpora mých kolegů, kteří si pro mě připravili překvapení ve formě transparentu, pocit úlevy po slavnostním vyhlášení a samozřejmě nezapomenutelná tancovačka uprostřed nádvoří... řekla bych, že celý večer se stal nezapomenutelným zážitkem od začátku do konce.

• Pokud byste měla možnost rozhodnout se znovu, po těch zkušenost, přihlásila byste se?

Jsem ráda, že jsem do toho šla, ale nevím, jestli bych se do toho nechala znova přemluvit.

Lucie Mahdalová, 2. vicemiss Egovernment 2017

• S jakými pocity jste šla do soutěže?

S obavami i nadšením. Ráda přijímám nové výzvy a jsem vděčná za každou zkušenost.

• Co Vás vedlo k tomu přihlásit se?

S touto iniciativou přišli moji skvělí kolegové z odboru informatiky a paní tajemnice. Popravdě jsem si jejich nominace velmi vážila.


• A jaké jste měla představy o zámeckém finále?

Naštěstí byl průběh večera přiblížený na internetových stránkách pořadatele. Dokázala jsem si tedy finálový večer představit, neočekávala jsem ale tak výbornou atmosféru a tak perfektně připravené zázemí.

• Jak na Vás působilo finálové klání na nádvoří mikulovského zámku?

Naprosto to předčilo mé očekávání. Mikulov vnímám jako jedno z nejkrásnějších měst a atmosféra na nádvoří zámku byla pro mne nepopsatelná.

• Měla jste za sebou nějakou „speciální" přípravu, nebo jste do toho šla rovnou?

Několik dlouhých večerů jsem trápila dlouholetého kamaráda přípravou volné disciplíny. Z původně naplánované ukázky společenských tanců se ale nakonec stala spíše „ukázka výuky společenských tanců". Potom už jsem se snažila být jen přirozená.

• Vnímala jste v průběhu večera podporu diváků?

Ano, a ráda bych jim za to moc poděkovala. Tou obrovskou podporou jsem byla chvílemi opravdu dojatá. Diváci i kolegové mi ji projevovali i mezi jednotlivými body programu a po finálovém vyhlášení. Velmi mne to překvapilo a moc jsem si toho vážila.

• Co na Vaši účast v soutěži a výsledek říkala rodina, případně kolegové?

Podporovali mě. Nejvíce můj manžel. Nejenže hlídal dcery v době tréninků na volnou disciplínu, ale je také mým nejupřímnějším kritikem. Měla jsem velkou radost i z pozitivní odezvy na Facebooku.

• Jak zpětně hodnotíte tento zážitek?

Jako skvělou zkušenost a příležitost reprezentovat město Zábřeh a městský úřad. Mimo to jsem ráda, že jsem poznala nové sympatické kolegyně z veřejné správy.

• Nyní připravujeme pro příští rok jubilejní desátý ročník soutěže, doporučila byste kolegyním a kamarádkám, aby se přihlásily?

Určitě ano. Neváhejte!

• Na co máte největší vzpomínku v rámci celé soutěže?

Celý finálový večer je pro mě nezapomenutelnou vzpomínkou. Nejraději asi vzpomínám na pozitivní reakce diváků po finálovém vyhlášení a příjemně strávený zbytek večera s kolegy.

• Pokud byste měla možnost rozhodnout se znovu, po těch zkušenostech, přihlásila byste se?

Bez váhání...

Lenka Witturová – Miss Sympatie

• S jakými pocity jste šla do soutěže?

Jelikož jsem docela trémistka a nerada vystupuji před publikem, měla jsem docela obavy. Ale na druhou stranu mě lákalo, poznat a vyzkoušet něco nového.

• Co Vás vedlo k tomu přihlásit se?

Do soutěžě jsem se nepřihlásila sama, na to nemám dostatek odvahy. Přihlásila mě moje paní vedoucí. Konečné rozhodnutí ale bylo na mně.

• A jaké jste měla představy o zámeckém finále? Jak na Vás působilo finálové klání na nádvoří mikulovského zámku?

Musím se přiznat, že jsem trošičku pátrala, jak probíhaly minulé ročníky miss, abych měla alespoň nějakou představu. A byla jsem i zvědavá na loňské, předloňské a další finalistky. Takže jsem podle fotografii zhruba tušila, jak bude finálový večer probíhat. Myslím, že žádná fotografie nemůže vystihnout kouzelné prostředí mikulovského zámku a atmosféru, která panovala na nádvoří. Celý finálový večer předčil mé očekávání, byl to nezapomenutelný zážitek.

• Měla jste za sebou nějakou „speciální" přípravu, nebo jste do toho šla rovnou?

Připravovala jsem se na volnou disciplínu. Jinak na rozhovor a jakékoliv vyprávění se v mém případě opravdu připravit nejde, tréma za mě udělá vše.

• Vnímala jste v průběhu večera podporu diváků?

Potlesk a reakce diváků jsem vnímala, pouze u ostatních finalistek. Já osobně, když jsem měla vystupovat, jsem nevnímala vůbec nic. Ale rodina, kterou jsem měla v publiku, mě ujistila, že ohlasy pozitivní byly.

• **Co na Vaši účast v soutěži a výsledek říkala rodina, případně kolegové?**
Největší podporu jsem měla od rodiny, dětí, manžela... Mladší dcera Leontýnka se mnou vystupovala ve volné disciplíně a starší Violka celou taneční choreografii vymyslela, za to jim velice děkuji a jsem ráda, že je mám. Nesmím zapomenout na své kolegyňky, kolegu, paní vedoucí, těm velice děkuji navíc za milé přivítání po návratu z finále.

• **Jak zpětně hodnotíte tento zážitek?**
Mně osobně celý večer neuvěřitelně rychle utekl. Tím, že se o nás starali a obklopovali nás pohodoví lidé, celý večer proběhl ve skvělé atmosféře a náladě.

• **Nyní připravujeme pro příští rok jubilejní desátý ročník soutěže, doporučila byste kolegyním a kamarádkám, aby se přihlásily?**
Všem budoucím soutěžícím a finalistkám mohu jen doporučit. Pokud bude někdo, kdo bude stejně jako já váhat a rozmýšlet se – jděte do toho, nebudete litovat. Je to skvělý zážitek a zkušenost.

• **Na co máte největší vzpomínku v rámci celé soutěže?**
Velice mě potešilo a je můj nejlepší zážitek určitě vyhlášení. To, že jsem se v tak skvělé konkurenci umístila. Jinak celá soutěž se mi moc líbila.

• **Pokud byste měla možnost rozhodnout se znovu, po těch zkušenostech, přihlásila byste se?**
Tím, že už vím, co a jak probíhá, by moje rozhodování bylo jednoznačné. Ano, přihlásila bych se znovu. Také vím, že bych si celý večer užila klidněji a byla víc v pohodě.

Všechny tyto dámy prožívaly letošní večer v Mikulově dosti nervozně, neboť byly svázány soutěžní atmosférou. Karolína Doskočilová, která soutěž vyhrála v roce 2016, byla letos členem poroty a vítězce předávala křišťálovou korunku. Netrpěla tedy soutěžní nervozitou a dívala se na večer úplně jinýma očima. Zajímal nás tedy i její názor:

Karolína Doskočilová – Miss Egovernment 2016

Soutěž jsem si užila opravdu na všech frontách. I jako soutěžící, vítězka a předávající. Tuto soutěž vnímám jako poděkování nám, pracovnicím Czech POINTu, což je milé zpříjemnění mezi celodenním papírováním. Mikulov je nádherné místo a dodává na krásné a příjemné atmosféře. Vše na mě působí a působilo jednoznačně pozitivně.

S předáváním titulu už jsem nepociťovala tu nervozitu jako v loňském roce, tudíž jsem si celý večer opravdu užívala se vším všudy. Ale z loňska můžu potvrdit, že pocity rozhodně nejsou pro soutěžící v žádném ohledu negativní. Osobně svoje kolegyně z práce povzbuzuji, aby se přihlásily. Myslím, že každá z nás, pracovnic, které poskytují služby Czech POINT, by si měla večer v Mikulově užít minimálně tak, jako jsem si užila já.

Do soutěže bych se přihlásila rozhodně znovu. Organizace je opravdu skvělá a celý večer se nese ve velmi přátelském duchu. Jak jsem již zmínila, Mikulov je krásný a věřím, že příští, tedy 10. ročník bude minimálně tak skvělý jako dva ročníky, kterých jsem se mohla zúčastnit.

Tak tedy, chcete se účastnit soutěže Miss Egovernment 2018 – jubilejního desátého ročníku? Už nyní nám můžete zasílat své přihlášky (nebo přihlášky svých kolegyň), které najdete na www.egovernment.cz v sekci MISS. Nyní sbíráme přihlášky, od ledna pak budeme postupně vystavovat profily soutěžících a sbírat hlasy čtenářů.

Pro jubilejní ročník samozřejmě plánujeme několik vylepšení:

- delší čas na internetové hlasování (od ledna 2018);
- delší čas na přihlašování do soutěže (od listopadu 2017);
- více zajímavých cen pro vítězky;
- větší komfort pro finalistky (proplacené ubytování atp.)
- a řadu dalších.

Přihlaste se a soutěžte o jubilejní desátý titul Miss Egovernment www.egovernment.cz.

KYBEZ Platforma kybernetické bezpečnosti

Chcete zjistit, jak jste na tom s GDPR a kybernetickou bezpečností?

Analytický nástroj BEAN vám na tuto otázku odpoví.

Základní

- Analýza stavu bezpečnosti
- Seznámení s bezpečností informací
- Ohodnocení stavu
- Dodržení legislativy ČR

GDPR

- Analýza stavu ochrany osobních údajů
- Zvýšení ochrany osobních údajů
- Příprava na implementaci
- Ohodnocení stavu připravenosti

Pokročilá

- Podrobná analýza stavu bezpečnosti
- Selekce dle oblastí bezpečnosti
- Ohodnocení stavu
- Porovnání s legislativou ČR

www.kybez.cz