Přehled aktuálních kroků v prioritních oblastech digitální agendy

- k tématům ochrany osobních údajů, kybernetické bezpečnosti a rozvoje eGovernmentu

Zpracoval koordinátor digitální agendy ČR Úřadu vlády ve spolupráci s Ministerstvem vnitra, Úřadem pro ochranu osobních údajů, Národním bezpečnostním úřadem a dalšími resorty.

**Obsah**

Úvod 3

Shrnutí 4

1. Ochrana osobních údajů 6

2. Kybernetická bezpečnost 8

3. Rozvoj eGovernmentu 12

3.1. Shrnutí uplynulého období v bodech 12

3.2. Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ICT služeb 13

3.3. Národní architektonický plán a jeho naplňování - proces schvalování veřejných zakázek na ICT ve veřejné správě v odboru Hlavního architekta MV ČR 14

3.4. Řešení situace v nečerpání evropských prostředků na rozvoj eGovernmentu ze strany resortů i územních samospráv 14

3.5. Aktuální stav příprav Strategického rámce Národního cloud computingu – eGovernment cloud ČR 18

3.6. Úplné elektronické podání 20

3.7. Elektronická identifikace 21

3.8. Elektronický občanský průkaz 22

3.9. Služby CzechPOINT 23

3.10. Iniciativa 202020 23

3.11. Otevřená data 24

3.12. Elektronická faktura 25

3.13. Dohledové centrum eGovernmentu 25

3.14. Elektronické zdravotnictví 26

3.15. eJustice 30

3.16. Databáze strategií 31

3.17. Aplikace k operačním programům a elektronické zadávání veřejných zakázek 31

3.18. Portál eAGRI a elektronizace agend Ministerstva zemědělství 32

3.19. Informační systém Registru živnostenského podnikání 33

3.20. Elektronizace finanční správy 34

3.21. ePortál České správy sociálního zabezpečení 34

3.22. Infrastruktura pro dopravně správní agendy 35

Úvod

Plenární schůze Rady hospodářské a sociální dohody ČR, která se konala dne 12. září 2016, uložila koordinátorovi digitální agendy v závěru bodu 1.3 Akční plán pro rozvoj digitálního trhu mimo jiné, aby ve spolupráci s Ministerstvem vnitra (MV), Úřadem pro ochranu osobních údajů (ÚOOÚ) a Národním bezpečnostním úřadem (NBÚ) předložil přehled aktuálních kroků v prioritních oblastech digitální agendy, a to konkrétně k tématům ochrany osobních údajů, kybernetické bezpečnosti a rozvoje eGovernmentu se zřetelem k:

* urychlenému řešení aktuální situace v nečerpání evropských prostředků na rozvoj eGovernmentu ze strany resortů i územních samospráv;
* urychlení a zefektivnění procesu schvalování veřejných zakázek na ICT ve veřejné správě v odboru hlavního architekta MV ČR;
* dokončení Národní strategie cloud computingu jako dílčího strategického materiálu pro podporu využívání nových technologií ve veřejné správě;

a aby tuto informaci o způsobu plnění stanovených úkolů předložil na listopadovou Plenární schůzi RHSD ČR.

Akční plán pro rozvoj digitálního trhu, jehož aktualizovaná verze byla schválena vládou dne 17. října 2016, identifikuje eGovernment a e-bezpečnost, do které spadá oblast ochrany osobních dat a kybernetická bezpečnost, jako dvě z pěti hlavních prioritních oblastí koordinace digitální agendy. V Akčním plánu jsou ke každé oblasti popsána konkrétní plánovaná nebo již probíhající opatření s termíny jejich plnění. Rozvoj elektronické veřejné správy má nicméně i svou sektorovou strategii s názvem Strategický rámec rozvoje veřejné správy pro období 2014 – 2020 a implementační plány pro její naplnění. Primárním gestorem je Ministerstvo vnitra ČR. Plán na zajištění kybernetické bezpečnosti a vize, které v této oblasti Česká republika má, jsou obsaženy v Národní strategii kybernetické bezpečnosti na období let 2015 – 2020 a v navazujícím Akčním plánu. Gestorem této sektorové strategie je Národní bezpečnostní úřad ČR. Prioritou v oblasti ochrany osobních dat je aktuálně implementace Obecného nařízení o ochraně osobních údajů, které vstoupilo v platnost v květnu tohoto roku a použije se od 25. května roku 2018. Gestorem implementace Obecného nařízení do českého právního řádu je Ministerstvo vnitra.

Shrnutí

V oblasti ochrany osobních údajů je aktuální prioritou příprava na implementaci Obecného nařízení o ochraně osobních údajů, které nabude účinnosti v květnu 2018, do českého právního řádu a praxe. Ministerstvo vnitra navrhlo zařadit do Legislativního plánu prací vlády na rok 2017 reakci na jeho přijetí, tj. zejména novelu zákona 101/2000 Sb., o ochraně osobních údajů. Celkovou koncepci novelizovaného zákona o ochraně osobních údajů a dalších legislativních požadavcích unijních předpisů o ochraně osobních údajů podrobně konzultuje MV s Úřadem pro ochranu osobních údajů. Jejich zástupci se také účastní pracovních skupin a jednání na evropské úrovni. Vnitrostátní konzultace probíhají i s podnikatelským sektorem. Při Výboru pro digitální ekonomiku byla zřízena Pracovní skupina k legislativě v oblasti ochrany osobních údajů. Je koordinována Úřadem vlády a skládá se ze zástupců ministerstev, ÚOOÚ a sociálních a hospodářských partnerů. Jejím smyslem je připravit se na národní implementaci a poskytnout sektoru výklad nařízení v nejasných otázkách. MV využije výstupy z této skupiny také pro meziresortní koordinaci, při které se připraví novelizace dotčených právních předpisů.

Legislativa v oblasti kybernetické bezpečnosti v roce 2017 dozná změn z důvodu transpozice evropské směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS) a s ohledem na praxí identifikované nedostatky stávající právní úpravy. Po faktickém ukončení vyjednávání o směrnici NIS zřídil NBÚ v březnu 2016 dvě pracovní skupiny za účelem přípravy transpoziční novely zákona o kybernetické bezpečnosti, sdružující relevantní resorty, zástupce dotčených odvětví a další odborné veřejnosti. Dne 19. července 2016 byl návrh transpoziční novely společně s tezemi prováděcího právního předpisu předložen do mezirezortního připomínkového řízení. V návaznosti na vypořádání připomínek, které proběhlo v září 2016, byl dne 30. září návrh novely předložen Legislativní radě vlády. Na základě předložené novely má ZKB být rozšířen o nové kategorie povinných osob, jmenovitě provozovatelů základních služeb, správců a provozovatelů informačních systémů základních služeb a poskytovatelů výše uvedených digitálních služeb. V říjnu 2016 svolal NBÚ pracovní skupinu k přípravě prováděcí vyhlášky týkající se určujících kritérií pro provozovatele základních služeb.

S cílem vyřešit situaci nečerpání evropských prostředků na rozvoj eGovernmentu a dalších oblastí v rámci SC 3.2 IROP proběhly k 9. září 2016 revize pravidel výzev č. 4, 10, 23, 26 a 28, a to konkrétně: zjednodušení způsobu stanovení rozpočtových cen, zrušení povinné přílohy „průzkum trhu“, možnost přiložení souhlasného stanoviska podle Usnesení vlády ČR č. 889/2015 tak, aby žadatel nemusel dokládat dva velice podobné dokumenty, úprava většiny obecných a specifických hodnotících kritérií přijatelnosti, zařazení koncových HW zařízení mezi vedlejší způsobilé výdaje projektu, zařazení výdajů na služby odborné konzultace a dozoru implementace pořizovaného IS mezi vedlejší způsobilé výdaje projektu, zařazení výdaje na stavební práce vyžadující stavební povolení (kromě liniových staveb) mezi vedlejší způsobilé výdaje projektu, upřesnění celoplošného dopadu včetně uvedené příkladů a rozšíření výzvy č. 26 o projektové okruhy „opendata“, „geodata“ a „eProcurement“.

V dokumentu je přiložena tabulka mapující aktuální výzvy a zaregistrované projekty v dotčené oblasti.

Ministerstvo vnitra v rámci své koordinační úlohy v oblasti ICT prostřednictvím odboru Hlavního architekta eGovernmentu posuzuje dva typy IT projektů, a) projekty spolufinancované z Integrovaného regionálního operačního programu ve vybraných výzvách a b) IT záměry podléhající usnesení vlády č. 889 ze dne 2. listopadu 2015. Ministerstvo vnitra zpracovalo zprávu k posuzování projektů, která byla předložena pro informaci členům vlády dne 7. listopadu 2016 a je přílohou tohoto materiálu. V období od ledna do září roku 2016 bylo posuzováno 71 žádostí o stanovisko OHA a jejich souhrnná hodnota činila 13,8 miliardy Kč bez DPH. Průměrná doba pro vydání stanoviska je 25 kalendářních dnů. Stanovisko k většině projektů je však vydáno dříve, delší lhůta pro vyřízení je u projektů, které je nutné upravit do souladu s architektonickými principy a vzory, především na využívání propojeného datového fondu a na využívání sdílených služeb eGovernmentu. Společně s architektonickým posouzením probíhá i posouzení bezpečnostních aspektů, které provádí jednotlivé bezpečnostní složky státu, ty sdělují své závěry do 20 kalendářních dnů a odbor Hlavního architekta eGovernmentu je zohlední ve svém konečném stanovisku.

Vizí „Strategického rámce Národního cloud computingu – eGovernment cloud ČR“ je otevřít dveře cloudovým řešením v České republice a umožnit tak lepší a efektivnější způsoby využití ICT ve veřejné správě plynoucí z využívání sdílených služeb vytvořením tzv. eGovernment cloudu neboli eGC. Princip rozvoje sdílených služeb cloud computingu je podporován na úrovni vlády a je vnímán jako společný úkol všech zainteresovaných subjektů, kteří budou služby eGovernment cloudu využívat. Vládě bude materiál předložen ke schválení s největší pravděpodobností do konce listopadu tohoto roku. Pokud bude schválen, plánovaný časový rozklad následných prací je následující. První přípravná fáze se plánuje na roky 2016-2017. Během ní budou definovány konkrétní podmínky fungování eGovernment cloudu z hlediska provozního, legislativního, organizačního, technického, ekonomického, bezpečnostního, lokalizačního a řady dalších. Druhá realizační fáze a vybudování eGovernment cloudu jsou plánovány na 2018-2019 a třetí standardizační fáze na 2019-2020. Časový plán může nicméně během přípravné fáze podlehnout dalším změnám.

Materiál dále obsahuje informace o stavu eGovernmentu v dalších oblastech, které spadají do gesce jednotlivých ministerstev.

1. Ochrana osobních údajů

Obecné nařízení o ochraně osobních údajů (2016/679/EU), které nabude účinnosti v květnu 2018, představuje zásadní reformu ochrany osobních údajů v rámci Evropské unie. Obecné nařízení zasáhne většinu oblastí života státu a hospodářství, které podléhají právu EU (v podstatě s výjimkou činnosti policie a dalších orgánů činných v trestním řízení).

Ochranu osobních údajů upravuje v ČR primárně zákon 101/2000 Sb., který implementuje směrnici o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (1995/46/ES). Z této směrnice koncepčně vychází i nové Obecné nařízení, takže jejich základní struktura a klíčové instituty jsou do značné míry podobné. Nové nařízení je ovšem daleko ambicióznější, jeho rozsah je zhruba trojnásobný. Některé povinnosti jsou zcela nové, navíc se kromě principů a základních práv na evropské úrovni sjednocují i některé detaily. Mezi hlavní rozdíly náleží posílení ochrany dětí (podmínky souhlasu se zpracováním, podmínky výmazu dat), posílení informačních povinností správců (bezplatnost, lhůty), právo „být zapomenut“ (čl. 17), právo na přenositelnost osobních údajů (čl. 20), podrobná úprava vztahu správce a zpracovatele, posílení kontroly nad správci mimo území EU, posílení řady požadavků na správce a zpracovatele, včetně hodnocení dopadů na soukromí a předběžných konzultací s dozorovým orgánem, upuštění od notifikace všech nových zpracování osobních údajů dozorovému orgánu, posílení pravidel o zabezpečení dat (zejm. technické) a hlášení narušení bezpečnosti osobních dat, pro veřejnou správu a pro část podniků povinný pověřenec ochrany dat, zásadní sjednocení pravomocí dozorových úřadů (pro ochranu osobních údajů), podrobná úprava jejich spolupráce, zcela nová a principiálně nevyzkoušená úprava společného rozhodování dozorových úřadů v různých typech přeshraničních případů, zavedení rozhodovací pravomoci pro Evropský sbor dozorových úřadů v konkrétních věcech a také sjednocení a zásadní zvýšení sankcí formou 2% nebo dokonce 4% podílu z ročního globálního obratu podnikatele.

Pro soukromý sektor Obecné nařízení o ochraně osobních údajů znamená na jednu stranu značnou, byť nikoli úplnou, harmonizaci předpisů v celé EU a jistou úlevu v podobě odstranění obecné notifikační povinnosti, na druhou stranu to nepochybně přinese nové povinnosti navíc. Kromě velmi obecně formulovaných a diskutabilních nových práv (zejm. práva na přenositelnost) řadě podniků a organizací vznikne například povinnost ustanovit pověřence ochrany osobních údajů nebo povinnost ohlašovat narušení zabezpečení dat. Za nesplnění posílených povinností navíc hrozí podstatně vyšší sankce.

Při adaptaci českého právního řádu na Obecné nařízení pro ochranu osobních údajů se postupuje podle následujících principiálních vodítek. Kromě solidní ochrany soukromí bude nutné vyhnout se zbytečnému zvyšování administrativní zátěže správců a zpracovatelů, které by mohlo poškodit nejen ta odvětví hospodářství, která se opírají o informační technologie. Součástí tohoto přístupu je zásadní legislativní zdrženlivost v oblastech, ve kterých by sice bylo možno povinnosti unijní legislativy zpřísnit nebo rozšířit, ale zatím není ani známo, jaký dopad budou mít takové nové požadavky v praxi ani v těch oblastech, kde budou povinné. V rámci volnosti dané pro určité oblasti (média, pracovní nebo zdravotní předpisy a další) bude klíčové nalézt správnou rovnováhu mezi ochranu subjektu údajů a dalšími relevantními hodnotami nebo společenskými potřebami. V neposlední řadě se usiluje, tam, kde je to přípustné, předcházet některým situacím, ve kterých by nejasný či více výkladů připouštějící text Obecného nařízení vnášel do probíhajících zpracování zbytečnou právní nejistotu.

MV se účastní expertní skupiny Evropské komise pro podporu implementace Obecného nařízení pro ochranu osobních údajů i tzv. Trestněprávní směrnice, kde si členské státy vyměňují informace a zkušenosti týkající se vnitrostátních legislativních kroků. Dosud proběhla tři jednání.

MV navrhlo zařadit do Legislativního plánu prací vlády na rok 2017 reakci na přijetí balíčku pro ochranu údajů, tj. zejména novelu zákona 101/2000 Sb., o ochraně osobních údajů. Celkovou koncepci novelizovaného zákona o ochraně osobních údajů a dalších legislativních požadavcích unijních předpisů o ochraně osobních údajů podrobně konzultuje MV a ÚOOÚ.

MV připravilo informační dopis pro resorty a další ústřední orgány státní správy s cílem zajistit řádnou přípravu na Obecné nařízení o ochraně osobních údajů. Meziresortní jednání o způsobu adaptace právního řádu proběhne během listopadu.

Při Výboru pro digitální ekonomiku byla zřízena Pracovní skupiny k legislativě v oblasti ochrany osobních údajů, čímž bylo splněno opatření 5.1 Akčního plánu pro rozvoj digitálního trhu. Pracovní skupina je koordinována Úřadem vlády a skládá se ze zástupců ministerstev, ÚOOÚ a sociálních a hospodářských partnerů. Jejím smyslem je připravit se na národní implementaci a poskytnout sektoru výklad nařízení v nejasných otázkách. Její první jednání dne 30. září se věnovalo představení Obecného nařízení a představení činnosti Pracovní skupiny dle čl. 29, v rámci které se scházejí dozorové úřady z jednotlivých členských států EU. Diskutováno bylo i stanovení témat další práce. Druhé jednání v polovině října se blíže věnovalo problematice pověřenců ochrany osobních údajů a souvisejícím otázkám. MV vznese nejzávažnější podněty a dotazy ze strany členů i v rámci expertní skupiny Evropské komise. MV využije výstupy z této skupiny také pro meziresortní koordinaci, při které se připraví novelizace dotčených právních předpisů. Další jednání pracovní skupiny, které proběhlo 9. listopadu, se zaměřilo na dvě témata, která byla vybrána na základě podnětů od soukromého sektoru: právo na přenositelnost osobních údajů a povinnost provádět hodnocení dopadů. Další jednání této pracovní skupiny proběhne během prosince.

1. Kybernetická bezpečnost

Kybernetická bezpečnost je nedílnou součástí digitální agendy a předpokladem rozvoje digitálního trhu jak ostatně vyplývá z relevantních dokumentů na vnitrostátní i evropské úrovni.

Gestorem problematiky kybernetické bezpečnosti v České republice je Národní bezpečnostní úřad, jemuž tato kompetence byla usnesením vlády svěřena v roce 2011. V rámci výkonu své role NBÚ vybudoval Národní centrum kybernetické bezpečnosti, které plní dvě funkce. První je funkce technická, tzv. vládního CERT (Computer Emergency Response Team), neboli bezpečnostního týmu pro koordinaci řešení kybernetických bezpečnostních incidentů v systémech kritické informační infrastruktury a významných informačních systémů (systémy spravované orgány veřejné moci). Druhou funkcí, kterou plní oddělení teoretické podpory, vzdělávání a výzkumu, je určování prvků kritické informační infrastruktury, metodická podpora při výkladu a provádění legislativy kybernetické bezpečnosti, implementace národní strategie kybernetické bezpečnosti, vzdělávání a osvětová činnost, rozvíjení mezinárodní spolupráce a zajišťování zastoupení České republiky na mezinárodní úrovni.

**Současné aktivity**

**Transpozice evropské směrnice o bezpečnosti sítí a informačních systémů (tzv. směrnice NIS)**

Ke dni 1. ledna 2015 vešel v účinnost zákon o kybernetické bezpečnosti, který společně s prováděcími předpisy s cílem zajistit danou společnou úroveň kybernetické bezpečnosti ukládá specifikovaným kategoriím adresátů povinností v oblasti bezpečnostních opatření, detekce a hlášení kybernetických událostí a incidentů a svěřuje NBÚ příslušné kompetence včetně kontroly plnění povinností a mezinárodní spolupráce v oblasti kybernetické bezpečnosti. Adresáty zákona jsou primárně správci informačních a komunikačních systémů kritické informační infastruktury a významných informačních systémů.

Legislativa kybernetické bezpečnosti v roce 2017 dozná změn z důvodu transpozice evropské směrnice o bezpečnosti sítí a informačních systémů (směrnice NIS) a s ohledem na praxí identifikované nedostatky stávající právní úpravy.

Směrnice NIS zavádí povinnost pro členské státy vytvořit Národní strategie bezpečnosti sítí a informačních systémů, ustavit vnitrostátní příslušné orgány odpovědné za naplňování směrnice, jednotná kontaktní místa pro přeshraniční spolupráci a týmy CSIRT, přičemž tyto orgány musí mít dostatečné zdroje pro efektivní vykonávání své činnosti. Věcná působnost se vztahuje na provozovatele základních služeb a na poskytovatele tzv. digitálních služeb, jmenovitě internetových vyhledávačů, online tržišť a služeb cloud computingu.

S cílem zajistit kontinuitu jimi poskytovaných služeb budou tyto subjekty muset zavádět přiměřená technická a organizační opatření pro zvládnutí rizik hrozících bezpečnosti sítí a informačních systémů, které používají. Zároveň budou muset přijmout i přiměřená opatření pro prevenci, případně minimalizaci dopadů incidentů postihujících bezpečnost sítí a informačních systémů používaných při poskytování základních služeb. Členské státy rovněž budou povinny zajistit, že provozovatelé oznamují incidenty s významnými dopady na kontinuitu poskytované základní služby příslušným orgánům nebo týmům CSIRT. Pro zlepšení přeshraniční spolupráce informuje příslušný orgán nebo tým CSIRT ostatní postižené členské státy o takovýchto významných dopadech. Zároveň může po konzultaci s provozovatelem rovněž příslušný orgán nebo tým CSIRT informovat veřejnost. V oblasti vynucování těchto povinností musí členské státy zajistit příslušným orgánům nezbytné pravomoci a prostředky pro zajištění plnění těchto povinností provozovateli, které spočívají zejména v možnosti požadovat příslušné informace od provozovatelů.

Po faktickém ukončení vyjednávání o směrnici NIS, která byla formálně přijata dne 6. července 2016, zřídil NBÚ v březnu 2016 dvě pracovní skupiny za účelem přípravy transpoziční novely zákona o kybernetické bezpečnosti, sdružující relevantní resorty, zástupce dotčených odvětví a další odborné veřejnosti. Dne 19. července 2016 byl návrh transpoziční novely společně s tezemi prováděcího právního předpisu předložen do mezirezortního připomínkového řízení. V návaznosti na vypořádání připomínek, které proběhlo v září 2016, byl dne 30. září návrh novely předložen Legislativní radě vlády.

Na základě předložené novely má ZKB být rozšířen o nové kategorie povinných osob, jmenovitě provozovatelů základních služeb, správců a provozovatelů informačních systémů základních služeb a poskytovatelů výše uvedených digitálních služeb. Základní služby budou identifikovány v oblastech, které se částečně kryjí s odvětvími uvedenými v nařízení vlády č. 432/2010 o kritériích pro určení prvku kritické infrastruktury, prováděcím předpisem k ZKB však budou formulována jiná určující kritéria a doplněna některé jiné služby, např. v oblasti digitální infrastruktury. Správci informačních systémů základních služeb budou plnit povinnosti podle ZKB ve stejném rozsahu jako správci KII, nebudou však na ně dopadat povinnosti podle zákona č. 240/2000, o krizovém řízení. Obecně lze k základním službám a kritické informační infrastruktuře (KII) poznamenat, že budou ve vztahu hierarchie, přičemž naplnění kritérií pro určení prvku KII bude mít prioritu.

V návaznosti na předložení návrhu novely ZKB vládě svolal v říjnu 2016 NBÚ pracovní skupinu k přípravě prováděcí vyhlášky týkající se určujících kritérií pro provozovatele základních služeb.

Lze konstatovat, že legislativní práce zatím probíhají podle připraveného harmonogramu.

**Mechanismus spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR**

Byla vytvořena mezirezortní platforma k implementaci akčního plánu k Národní strategii kybernetické bezpečnosti a dvě pracovní skupiny Rady pro kybernetickou bezpečnost (RKB) pro harmonizaci pozic v oblasti kybernetické bezpečnosti na vnitrostátní a mezinárodní úrovni. Zpráva o plnění akčního plánu byla předložena Bezpečnostní radě státu v dubnu 2016 společně se Zprávou o stavu kybernetické bezpečnosti za rok 2015. Pracovní skupina RKB pro harmonizaci pozic na vnitrostátní úrovni, která zároveň projednává plnění Akčního plánu k Národní strategii kybernetické bezpečnosti 2015-2020, se sejde na konci října 2016.

Průběžně probíhá určovací proces subjektů kritické informační infrastruktury (KII) a významných informačních systémů (VIS). K dnešnímu dni je určeno 98 prvků KII a identifikováno přes 150 VIS.

Na operační úrovni probíhají pravidelně cvičení kybernetické bezpečnosti, pomocí nichž je testována účinnost spolupráce mezi jednotlivými subjekty při zajišťování kybernetické bezpečnosti. Ve dnech 13. a 14. října 2016 se ČR zúčastnila cvičení Cyber Europe, ve dnech 18. a 19. října 2016 NBÚ ve spolupráci s Masarykovou univerzitou uspořádal další vydání národního cvičení Cyber Czech. Na konci listopadu 2016 se ČR zúčastní mezinárodního cvičení NATO Cyber Coalition.

**Navyšování integrity sítí kritické informační infrastruktury (KII)**

NBÚ pokračuje v průběžné analýze a kontinuálním sledování zabezpečení systémů a sítí KII v ČR a všem subjektům KII poskytuje technickou, metodickou, právní a jinou podporu.

Průběžně se navyšují i samotné kapacity a schopnosti GovCERT.CZ pro předcházení a zvládání bezpečnostních incidentů v informačních a komunikačních systémech KII. Mezi ně patří schopnosti forenzní analýzy, provozování laboratoře pro detekci a analýzu malware, rozvoj expertízy na zabezpečení průmyslových řídicích systémů a další. GovCERT.CZ zároveň vede evidenci incidentů a pravidelně je vyhodnocuje.

V průběhu roku pokračovaly kontroly plnění povinností podle zákona o kybernetické bezpečnosti u správců kritické informační infrastruktury, se kterými NBÚ začal v prvním kvartálu roku 2016.

**Osvěta široké veřejnosti a rozvoj lidského kapitálu**

NBÚ pokračuje v publikační a přednáškové činnosti, mj. zajišťuje výuku dvou předmětů na Masarykově univerzitě v Brně a na Univerzitě Palackého v Olomouci.

Stále pokračují aktivity pro veřejnost zaměřené na kybernetickou bezpečnost jako prevenci proti kybernetické kriminalitě, v létě 2016 byla uzavřena smlouva o spolupráci mezi NBÚ a Národním centrem bezpečnějšího internetu. Probíhají osvětové přednášky na základních školách (nejvíce je žádané téma kyberšikany a bezpečnostního desatera pro žáky). Pokračuje příprava e-learningové platformy pro vzdělávání širší a odborné veřejnosti, která se bohužel z technických důvodů zpozdila, její spuštění se očekává začátkem roku 2017.

Ohledně vytvoření metodických materiálů a doporučení pro školy pro zapracování kybernetické bezpečnosti do školních vzdělávacích programů byla provedena analýza současných rámcových vzdělávacích programů. V oblasti podpory studijních programů pro výchovu expertů na kybernetickou bezpečnost podporuje NBÚ studenty Pedagogické fakulty Masarykovy univerzity (poskytování stáží a konzultací k diplomové práci). Dále poskytuje NBÚ metodickou a odbornou podporu vznikajícího středoškolského oboru „Kybernetická bezpečnost“, jehož vytváření je nyní ještě v samotných počátcích.

NBÚ rovněž zpřístupnil na svých webových stránkách výsledky mapování relevantních předmětů a oborů na vysokých školách. Obdobnou iniciativu na mezinárodní úrovni realizovala agentura ENISA, NBÚ její výstupy využije.

NBÚ jedná se dvěma odbornými středními školami o přípravě vzdělávacího oboru Kybernetická bezpečnost. Současně je členem pracovní platformy při Národním ústavu vzdělávání ustavené s cílem připravit příslušný rámcový vzdělávací program. V rámci prosazování prvku kybernetické bezpečnosti jako nezbytné součásti digitálního vzdělávání a digitální gramotnosti pak NBÚ pokračuje v realizaci projektu Digistopa na základních školách.

**Edukace státních zaměstnanců v oblasti kybernetické bezpečnosti**

S koordinátorem pro digitální agendu a Ministerstvem vnitra probíhá spolupráce s cílem zvyšovat bezpečnostní povědomí v oblasti kybernetické bezpečnosti u zaměstnanců státní správy. Školení již na několika úřadech (Úřad vlády, Ministerstvo pro místní rozvoj) proběhlo, s dalšími probíhají v této věci jednání. Probíhá tvorba základních standardů kybernetické bezpečnosti a vzniká pilotní projekt e-learningového programu pro státní zaměstnance.

1. Rozvoj eGovernmentu
	1. Shrnutí uplynulého období v bodech

Rok 2016 znamenal v mnoha ohledech zlom ve struktuře a nabídce elektronických služeb veřejné správy nejen díky zdokonalení systému kontroly.

Rada vlády pro informační společnost (RVIS) navrhla a vláda schválila Strategii rozvoje ICT služeb ve veřejné správě a její opatření na zefektivnění ICT služeb.

Práce na Národním architektonickém plánu (NAP) pokračují pomocí publikování a revidování architektonických vzorů, tvorby lokálních architektur samospráv a pilotních projektů. V případě NAP se jedná o soustavný proces tvorby architektur ve stavech AS-IS (současnost), TO-BE (budoucnost) a přechodové architektury mezi těmito stavy. Cílem pro rok 2017 je zprovoznění centrálního repozitáře. Národní architektonický plán má za cíl zavést jednotný strukturovaný popis služeb veřejné správy prostřednictvím architektonických nástrojů IT, dále popsat výsledky jednotlivých již realizovaných projektů ve státní správě a vytvořit tím informační základ pro správu sdílených služeb pomocí architektury a vytvořit strukturovaný popis cílů jednotlivých strategií upravujících oblast eGovernmentu a veřejné správy tak, jak je popsáno ve Strategickém rámci rozvoje veřejné správy České republiky pro období 2014 – 2020. Do této aktivity bude zapojena také samospráva.

Odboru Hlavního architekta eGovernmentu byly v rámci Ministerstva vnitra svěřeny silné pravomoci pro koordinaci a řízení rozvoje ICT ve státní správě České republiky. Tyto pravomoci vyplývají z usnesení vlády č. 889 z 2. listopadu 2015 a ukládají povinnost nechat si schválit každý záměr vynaložit prostředky na ICT, který přesáhne hranici 6 mil. Kč/rok nebo 30 mil. Kč/5 let, na soulad s principy a pravidly NAP. Ministerstvo vnitra tak v rámci své koordinační úlohy v oblasti ICT prostřednictvím odboru Hlavního architekta eGovernmentu posuzuje dva typy IT projektů, a) projekty spolufinancované z Integrovaného regionálního operačního programu a b) IT záměry podléhající usnesení vlády č. 889 z 2. listopadu 2015.

Bylo dokončeno Centrální místo služeb, jehož funkcí je poskytnout orgánům veřejné moci řízené, bezpečné, efektivní a monitorované komunikační prostředí pro všechny jejich běžné potřeby.Uživatelé, orgány státní správy, krajské úřady či místní samosprávy tedy budou mít snadný a bezpečný přístup k informačním systémům a informacím, které potřebují k výkonu své činnosti, resp. na které mají dle platné právní úpravy nárok. Projekt Centrální místo služeb 2.0 byl dokončen a jeho výstupy akceptovány v roce 2015. Informace o aktuálním provozním stavu CMS 2.0 spravuje provozovatel, NAKIT s.p. Další rozvoj CMS 2.0 je v současné době připravován v součinnosti MV a provozovatele.

V rámci RVIS vznikla pracovní skupina pro komunikaci za účelem dosažení efektivní spolupráce se zástupci krajů a obcí a zástupci ICT firem.

Nadále se pokračuje v publikaci architektonických vzorů sdílených služeb a prosazování základních principů Národního architektonického plánu a principů efektivního využívání sdílených služeb.

Díky rámcové smlouvě na produkty Microsoft stát ušetřil 600 milionů korun za dva roky.

Na základě realizace 377 veřejných zakázek na datové a hlasové služby Komunikační infrastruktury veřejné správy (KIVS) realizovaných od října 2014 do října 2016 se podařilo dosáhnout úspory 299,4 mil. Kč včetně DPH oproti původním cenám výše uvedených datových a hlasových služeb KIVS.

Proběhla první fáze výstavby dohledového centra eGovernmentu – SOCCR (Security Operational Centre for Cyber Reliability). SOCCR svými nástroji zajišťuje kybernetickou bezpečnost, bezpečnostní dohledy a monitoring pro komunikační a informační systémy kritické informační infrastruktury a významné informační systémy resortu Ministerstva vnitra (dále jen „KII“ a „VIS“). Dále mimo jiné zabezpečuje hlášení kybernetických bezpečnostních incidentů na Národní centrum kybernetické bezpečnosti (dále jen „NCKB“) včetně zprostředkování potřebné komunikace.

* 1. Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ICT služeb

Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ICT služeb byla vypracována v návaznosti na Strategický rámec veřejné správy pro období 2014-2020 a představuje jeho bližší rozpracování. Naplňování této strategie jednotlivými cílenými opatřeními a aktivitami probíhá průběžně, většina z nich je zmíněna dále v tomto dokumentu. Je však nutné zmínit, že v rámci reformy investic do ICT bylo zahájeno a probíhá schvalování ICT nákupních záměrů a jejich architektur dle usnesení vlády č. 889 z 2. 11. 2015. Byly vytvořeny základní architektonické vzory a realizovány pilotní projekty Národní architektury (MPO, MsK, MZ (KSRZIS[[1]](#footnote-1))). Z dalších kroků jmenujme například budování Národní architektury, tj. architektury služeb veřejné správy a navazujících ICT služeb na principech Enterprise architektury a pokračování v modelování centrálních prvků eGovernmentu, vyjadřování nejlepší praxe v podobě architektonických vzorů a budování lokálních modelů NAP na jednotlivých úřadech.

* 1. Národní architektonický plán a jeho naplňování - proces schvalování veřejných zakázek na ICT ve veřejné správě v odboru Hlavního architekta MV ČR

Ministerstvo vnitra v rámci své koordinační úlohy v oblasti ICT prostřednictvím odboru Hlavního architekta eGovernmentu posuzuje dva typy IT projektů, a) projekty spolufinancované z Integrovaného regionálního operačního programu ve vybraných výzvách a b) IT záměry podléhající usnesení vlády č. 889 ze dne 2. listopadu 2015. Ministerstvo vnitra zpracovalo zprávu k posuzování projektů, která byla předložena pro informaci členům vlády dne 7. listopadu 2016 a je přílohou tohoto materiálu.

V období od ledna do září roku 2016 bylo posuzováno 71 žádostí o stanovisko OHA a jejich souhrnná hodnota činila 13,8 miliardy Kč bez DPH. Tato částka je však výrazně vychýlena projektem Systému elektronického mýta ve výši 6,6 miliardy Kč na období 3 let, kdy projekt elektronického mýta ve svém objemu zahrnuje navíc i výraznou část výdajů nesouvisejících s informačními a komunikačními technologiemi. Pomineme-li tedy ze souhrnu tento vybočující projekt, tak OHA posoudilo za 9 měsíců 70 projektů v souhrnné hodnotě 7,2 miliardy Kč. To znamená přibližně dva projekty týdně, kdy průměrná hodnota každého z nich byla 102,9 mil Kč. Nelze určit objem finančních prostředků, který se ušetřil díky procesu posuzování projektů. Jednotlivá řešení a funkcionality musí korelovat s NAP a zapadat do jeho koncepce, přičemž nelze v současné době říci, o jakou částku jsou schválená řešení finančně výhodnější než ostatní či alternativní řešení.

Průměrná doba pro vydání stanoviska je 25 kalendářních dnů. Stanovisko k většině projektů je však vydáno dříve, delší lhůta pro vyřízení je u projektů, které je nutné upravit do souladu s architektonickými principy a vzory, především na využívání propojeného datového fondu a na využívání sdílených služeb eGovernmentu. Společně s architektonickým posouzením probíhá i posouzení bezpečnostních aspektů, které provádí jednotlivé bezpečnostní složky státu, ty sdělují své závěry do 20 kalendářních dnů a odbor Hlavního architekta eGovernmentu je zohlední ve svém konečném stanovisku.

* 1. Řešení situace v nečerpání evropských prostředků na rozvoj eGovernmentu ze strany resortů i územních samospráv

Na podporu projektů z oblasti eGovernmentu a informačních a komunikačních systémů a projektů ke zvýšení kybernetické bezpečnosti ČR je v rámci Prioritní osy 3 „Dobrá správa území a zefektivnění veřejných institucí“ Integrovaného regionálního operačního programu (IROP) vyčleněn specifický cíl 3.2 „Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů“ (SC 3.2 IROP), kde je alokováno 330 mil. EUR (cca 8,9 mld. Kč). V rámci SC 3.2 IROP bylo od září 2015 do dubna 2016 vyhlášeno celkem 6 průběžných výzev (č. 4, 10, 17, 23, 26 a 28).

V létě 2016 proběhlo dotazníkové šetření k problematice čerpání evropských prostředků ve specifickém cíli 3.2 IROP, který se dlouhodobě potýká s nízkým nebo nulovým předkládáním projektových žádostí o podporu[[2]](#footnote-2). V rámci šetření se podařilo shromáždit odpovědi a poznatky z 38 obcí, 6 krajů a 6 organizačních složek státu, na základě kterých byly identifikovány hlavní bariéry přípravy projektu do výzev ve specifickém cíli 3.2 IROP. Jako hlavní bariéru přípravy projektu respondenti nejčastěji uváděli nedostatečnou personální kapacitu na straně žadatele (projektoví manažeři, IT odborníci). Ta byla zmíněna v 60 % odpovědí. Náročnost přípravy studie proveditelnosti projektu pak byla jako významná bariéra označena v 54 % všech odpovědí. Ve více než 20 % odpovědí byly jako bariéry přípravy projektů označeny nemožnost financování koncových zařízení, získání souhlasného stanoviska odboru Hlavního architekta eGovernmentu MV ČR, nepřipravená legislativa, nedostatečné řízení Strategického rámce rozvoje veřejné správy (SRRVS) a obecně eGovernmentu na národní úrovni, chybějící zastřešující strategie v případě výzvy č. 26 (eGovernment I, Investiční priorita: Posilování aplikací v oblasti IKT určených pro elektronickou veřejnou správu, elektronické učení, začlenění do informační společnosti, elektronickou kulturu a elektronické zdravotnictví) a „ostatní“ (přílišné svázání tématy/úzká specifikace, pozdní poskytování informací žadatelům, úmyslně složitá legislativa, spodní limit celkových způsobilých výdajů projektu[[3]](#footnote-3), časová náročnost). Ve více než nebo v 10 % odpovědí byl uveden minimální limit způsobilých výdajů na projekt, pomalý proces schvalování projektové žádosti na straně žadatele, nezajištěné předfinancování projektu na straně žadatele, nedostatečná komunikace ze strany Centra pro regionální rozvoj ČR a ŘO IROP ohledně konzultace projektových záměrů, nepotřebnost nových nebo modernizovaných informační systémy nebo nezajištěné kofinancování projektu na straně žadatele. Pouze jedna z odpovědí jako bariéru přípravy projektu identifikovala nedostatečnou podporu vedení instituce žadatele. Nikdo pak jako hlavní překážku neoznačil maximální limit způsobilých výdajů na projekt.

V odpovědi na otázku „Jaké konkrétní změny v konkrétní výzvě by Vám usnadnily podání projektu do některé z výzev ve specifickém cíli 3.2 IROP?“ byly identifikovány následující (seřazeny podle důležitosti):

* obecné zjednodušení administrativy a pravidel,
* snížení minimální výše způsobilých výdajů,
* intenzivnější pořádání seminářů pro žadatele a prezentace jednotlivých výzev,
* možnost financování koncových zařízení (28. výzva),
* zrušení povinnosti získání stanoviska hlavního architekta,
* možnost obnovy bez nutnosti vázání na nové systémy, méně výzev a prodloužení doby na přípravu,
* uvolnění výčtu podporovaných funkcionalit.

S cílem vyřešit situaci nečerpání evropských prostředků na rozvoj eGovernmentu a dalších oblastí v rámci SC 3.2 IROP proběhly na základě obdržených informací k 9. září 2016 revize pravidel výzev č. 4, 10, 23, 26 a 28, a to konkrétně:

* zjednodušení způsobu stanovení rozpočtových cen,
* zrušení povinné přílohy „průzkum trhu“,
* možnost přiložení souhlasného stanoviska podle Usnesení vlády ČR č. 889/2015 - pro předložení projektu je možné jak souhlasné stanovisko podle přílohy specifických pravidel SC 3.2, tak souhlasné stanovisko podle usnesení – žadatel tak nemusí dokládat dva velice obdobné dokumenty,
* úprava většiny obecných a specifických hodnotících kritérií přijatelnosti na tzv. napravitelná kritéria - jedná se o změnu, kterou umožnila změna Jednotného metodického prostředí, kdy již není nutné vyřazovat projekty ihned po nesplnění nejméně jednoho kritéria přijatelnosti, ale je možné žadatele vyzvat k opravě v projektu, a to až dvakrát,
* zařazení koncových HW zařízení mezi vedlejší způsobilé výdaje projektu,
* zařazení výdajů na služby odborné konzultace a dozoru implementace pořizovaného IS mezi vedlejší způsobilé výdaje projektu,
* zařazení výdaje na stavební práce vyžadující stavební povolení (kromě liniových staveb) mezi vedlejší způsobilé výdaje projektu,
* upřesnění celoplošného dopadu včetně uvedené příkladů,
* rozšíření výzvy č. 26 o projektové okruhy „opendata“, „geodata“ a „eProcurement“.

Kromě výše uvedeného se prozatím žádné další změny ve výzvách neplánují a rovněž se prozatím neplánuje vyhlašování dalších výzev, protože běžící průběžné výzvy SC 3.2 pokrývají všechny jeho aktivity a je možné je kdykoliv prodloužit. Zároveň se pozitivně projevily provedené revize a k 31. říjnu 2016 bylo do všech průběžných výzev předloženo 16 projektů kumulativně za cca 0,75 mld. Kč. Další projekty, mimo jiné v rámci výzev č. 23 a 26, v objemu několika miliard Kč jsou těsně před podáním žádosti nebo v procesu konzultace s odborem Hlavního architekta eGovernmentu MV ČR ohledně vydání souhlasného stanoviska, které je u většiny projektů SC 3.2 povinnou přílohou.

**Tabulka k přehledu relevantních výzev:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Název výzvy** | **Alokace výzvy (EFRR, Kč)** | **Ukončení výzvy** | **Počet zaregistrovaných žádostí** | **Objem zaregistrovaných žádostí (EFRR, Kč)** |
| Výzva č. 4 Aktivity vedoucí k úplnému elektronickému podání | 400 000 000,00 Kč | 30. 6. 2017 | 4 | 110 839 034 |
| Výzva č. 10 Kybernetická bezpečnost | 1 200 000 000,00 Kč | 30. 6. 2017 | 2 | 97 139 848 |
| Výzva č. 17 eLegislativa, eSbírka, NDA | 600 000 000,00 Kč | 31. 12. 2016 | 2 | 432 796 802 |
| Výzva č. 23 Specifické informační a komunikační systémy a infrastruktura I. | 1 332 500 000,00 Kč | 29. 9. 2017 | 0 | 0 |
| Výzva č. 26 eGovernment I. | 1 860 000 000,00 Kč | 29. 9. 2017 | 0 | 0 |
| Výzva č. 28 Specifické informační a komunikační systémy a infrastruktura II. | 878 849 850,00 Kč | 29. 9. 2017 | 13 | 110 757 971 |

**Přehled zaregistrovaných projektů v rámci SC 3.2 IROP (k 15. 11. 2016)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Název projektu** | **Právní forma žadatele/příjemce** | **Číslo výzvy** | **Příspěvek EU (EFRR, Kč)** | **Datum ukončení realizace** |
| Celní kodex Unie - elektronizace celního řízení | Organizační složka státu | 4 | 74 391 200,00 | 30.6.2019 |
| Portál občana a komunikace s úřadem přes internet | Obec | 4 | 13 597 453,40 | 31.12.2017 |
| Vybudování systému řízení přístupů do základních registrů | Organizační složka státu | 4 | 15 433 748,20 | 30.9.2018 |
| Úřad podporující eGovernment | Obec | 4 | 7 416 632,50 | 31.12.2018 |
| Realizace bezpečnostních opatření podle zákona o kybernetické bezpečnosti | Kraj | 10 | 10 327 500,00 | 31.10.2018 |
| Systém detekce kybernetických bezpečnostních incidentů ve vybraných informačních systémech veřejné správy | Organizační složka státu | 10 | 86 812 348,79 | 31.12.2018 |
| Národní digitální archiv II | Organizační složka státu | 17 | 42 945 190,72 | 30.9.2019 |
| Elektronická sbírka zákonů a mezinárodních smluv (e-Sbírka) a elektronická tvorba právních předpisů (e-Legislativa) | Organizační složka státu | 17 | 389 851 611,75 | 31.12.2019 |
| Rozvoj Architektury ICT Moravskoslezského kraje | Kraj | 28 | 41 485 950,00 | 31.8.2018 |
| Efektivní a transparentní úřad | Obec | 28 | 4 223 752,85 | 31.12.2018 |
| Vytvoření nového a modernizace stávajícího IS ve městě Sezemice | Obec | 28 | 4 149 666,00 | 30.6.2018 |
| ICT systém Městského úřadu Františkovy Lázně | Obec | 28 | 8 430 614,50 | 30.6.2018 |
| Informační systém pro řízení organizace USKK | Akciová společnost | 28 | 10 535 750,00 | 30.6.2018 |
| Moderní systémy pro využití dat DP | Akciová společnost | 28 | 10 533 200,00 | 30.6.2018 |
| Zajištění dostupnosti a bezpečnosti ICT a rozšíření stávajících IS | Akciová společnost | 28 | 6 670 800,00 | 31.3.2018 |
| Nové funkce IS Města Kralupy nad Vltavou | Obec | 28 | 4 601 458,85 | 31.8.2017 |
| Efektivní digitální úřad Votice | Obec | 28 | 3 696 502,95 | 31.12.2018 |
| Efektivní řízení organizací města | Obec | 28 | 4 305 037,50 | 31.12.2018 |
| Moderní elektronický úřad Svitávka | Obec | 28 | 3 080 461,20 | 31.12.2018 |
| Moderní a efektivně řízený úřad | Obec | 28 | 4 598 160,39 | 31.12.2018 |
| Nové funkce IS města Říčany | Obec | 28 | 4 446 616,90 | 31.8.2017 |

* 1. Aktuální stav příprav Strategického rámce Národního cloud computingu – eGovernment cloud ČR

Na základě úkolu uloženého Akčním plánem k Národní strategii kybernetické bezpečnosti ČR na období let 2015–2020 „Vytvořit a vládě předložit Národní strategii cloud computingu“ vznikl ve spolupráci Ministerstva vnitra, Národního bezpečnostního úřadu a Ministerstva financí dokument s názvem Národní strategie cloud computingu, který byl na žádost vlády předložen do meziresortního připomínkového řízení. Vzhledem k velkému počtu připomínek byla podoba materiálu opakovaně projednávána jak se zástupci státní správy, tak se zástupci odborných svazů a odborné veřejnosti.

Po řadě diskusí bylo původní znění materiálu přepracováno a vznikl dokument s názvem „Strategický rámec Národního cloud computingu – eGovernment cloud ČR“ (dále jen „Strategický rámec“), který byl opětovně předložen do meziresortního připomínkového řízení spolu s návrhem na aktualizaci vybraných úkolů Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020.

Vizí tohoto Strategického rámce je otevřít dveře cloudovým řešením v České republice a umožnit tak lepší a efektivnější způsoby využití ICT ve veřejné správě plynoucí z využívání sdílených služeb vytvořením tzv. eGovernment cloudu neboli eGC. Účelem Strategického rámce je dosažení základní shody (napříč resorty i se zástupci odborné veřejnosti) na zásadních principech fungování eGovernment cloudu (eGC) a nastavení kroků nezbytných k jeho vybudování a využívání v prostředí ČR.

Hlavními cíli vybudování eGovernment cloudu jsou vytvoření sdíleného infrastrukturního a následně také aplikačního prostředí, centralizace a standardizace provozního prostředí vybraných aplikací a služeb veřejné správy při současném zajištění potřebné úrovně bezpečnosti, důvěrnosti, dostupnosti a spolehlivosti takto provozovaných systémů. Očekávaným přínosem je zefektivnění a optimalizace provozu, podpory a souvisejících doprovodných služeb pro informační systémy a aplikace (ICT) využívané ve veřejné správě a optimalizace nákladů na provoz informačních systémů a aplikací poskytujících standardní ICT služby.

Základním předpokladem eGovernment cloudu je vytvoření dvou částí:

* státní část, kterou tvoří služby datových center, které jsou ve výhradním vlastnictví státu a výhradně používané pro potřeby státu za podmínek a v rozsahu definovaném právním řádem ČR. Majetek je svěřen do užívání výhradně organizačním složkám státu, popř. je provozován prostřednictvím státních podniků. Podmínkou využívání služeb státní části eGC je připojení datových center ke garantované komunikační infrastruktuře státu (KIVS, ITS a CMS); dále se předpokládá využití tzv. technologických center krajských úřadů jako nedílné součásti státní části eGC;
* komerční část je tvořena službami datových center komerčních subjektů včetně připojení na privátní komunikační infrastrukturu (popř. i vč. připojení na garantovanou komunikační infrastrukturu státu), poskytující cloudové služby dle definovaných a schválených standardů.

Konkrétní podmínky fungování eGovernment cloudu z hlediska provozního, legislativního, organizačního, technického, ekonomického, bezpečnostního, lokalizačního a řady dalších určí projekt „Příprava vybudování eGovernment cloudu“, na jehož zpracování se bude podílet meziresortní pracovní skupina Rady vlády pro informační společnost se zapojením rovněž zástupců odborné veřejnosti.

Výstupy tohoto projektu v podobě komplexní analytické zprávy budou předloženy vládě k rozhodnutí o dalším postupu implementace eGovernment cloudu v České republice.

V rámci probíhajícího vypořádání obdržených připomínek meziresortního připomínkového řízení panuje shoda na výše uvedených základních předpokladech a zásadách možného fungování eGovernment cloudu. Tento princip rozvoje sdílených služeb cloud computingu je podporován také na úrovni vlády a je vnímán jako společný úkol všech zainteresovaných subjektů, kteří budou služby eGovernment cloudu využívat. Vládě bude materiál předložen ke schválení s největší pravděpodobností v polovině listopadu tohoto roku. Pokud bude schválen, plánovaný časový rozklad následných prací je následující. První přípravná fáze se plánuje na roky 2016-2017, druhá realizační fáze a vybudování eGovernment cloudu na 2018-2019 a třetí standardizační fáze na 2019-2020. Časový plán může nicméně během přípravné fáze podlehnout dalším změnám.

* 1. Úplné elektronické podání

V průběhu měsíce září došlo k úpravě strategie realizace úplného elektronického podání (dále jen ÚEP), a to v rámci specifikace předmětu plnění a rozdělení práce mezi projekt („Vytvoření metodického rámce pro úplné elektronické podání“) a dílčí veřejnou zakázku. Veřejná zakázka do konce roku 2016 přinese koncepci zavádění ÚEP především na základě zmapování potřeb a požadavků zákazníků vzhledem k ÚEP a legislativních bariér zavádění ÚEP. Dalším z jejích výstupů bude koncept napojení na stávající aktivity Ministerstva vnitra (procesní modelování agend, plánovaný Portál Občana, projekt „Vytvoření metodického rámce“).

V současnosti, konkrétně v průběhu měsíců října a listopadu, probíhá příprava projektové žádosti projektu „Vytvoření metodického rámce pro úplné elektronické podání“, který v návaznosti na výstupy veřejné zakázky přinese metodický, koncepční a architektonický rámec pro zavádění principu ÚEP pro podporu další implementace úplného elektronického podání ve veřejné správě ČR. Ještě předtím v měsíci září proběhlo doplnění a stylistická úprava projektového záměru. Projekt se bude realizovat v letech 2017 – 2021.

Souběžně s výše zmíněným projektem bude probíhat projekt tvrdý pro implementaci ÚEP (především elektronických formulářů), přičemž žádost o finanční podporu musí být předložena ke schválení řídícímu orgánu v první polovině roku 2017. Počítá se s realizací projektu v letech 2018 – 2021, přesné termíny zatím k dispozici nejsou.

Dalším krokem v rámci implementace ÚEP pro následující roky (odhadem 2018 – 2021) bude příprava a implementace Portálu Občana. Bude se jednat o webovou aplikaci zajišťující komunikaci občana s veřejnou správou z jednoho místa. V současné koncepci by měl obsahovat několik základních modulů. Nabídne přehledné rozhraní mimo jiné s popisy konkrétních životních situací s odkazy na potřebné elektronické formuláře, které bude možné přímo stáhnout či vyplnit a následně odeslat. Aby mohl uživatel plně využít nabízeného potenciálu, vytvoří si vlastní profil, v němž bude po identifikaci moci sledovat historii realizovaných aktivit. Z principu se tedy jedná o plně interaktivní a intuitivní prostředí, jež bude uživateli vycházet vstříc. Portál Občana navazuje na předchozí aktivity a projekty realizované v rámci budování eGovernmentu, v první řadě CzechPOINT. Kombinuje výhody a funkční principy elektronického kontaktního místa CzechPOINT@home a úplného elektronického podání (předpokládaná souběžná organizace s projektem Metodický rámec úplného elektronického podání), přičemž bude zároveň navazovat na závěry a výstupy projektu Optimalizace životních situací ve vztahu k Registru práv a povinností. Předpokládá se, že Portál Občana bude využívat autentizaci prostřednictvím elektronických občanských průkazů (viz níže).

Portál Občana je v současnosti ve fázi počátků práce na studii proveditelnosti, její velká část by měla být připravena do konce roku 2016 a projektová žádost zaslána na řídící orgán Integrovaného regionálního operačního programu v prvním kvartálu roku 2017.

* 1. Elektronická identifikace

Předpokladem úplného elektronického podání je elektronická identita klienta veřejné správy a dodržování zásad kybernetické bezpečnosti. Vzájemně propojené elektronické služby mohou fungovat, je-li bezpečně nastavena elektronická identifikace, autentizace a autorizace. Vzájemné uznávání oznámených prostředků pro elektronickou identifikaci řeší evropské nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), které se nyní implementuje do právních řádů členských států. Díky němu bude rozvoj eGovernmentu v ČR zaměřen i na možnost využití on-line služeb veřejné správy také přeshraničně.

Nařízení eIDAS stanoví právní rámec služeb vytvářejících důvěru, mezi které se řadí zejména elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování, certifikační služby pro autentizaci internetových stránek a elektronickou identifikaci.

Dne 19. září 2016 nabyl účinnosti zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. V zákoně je upraveno pouze to, co nařízení výslovně nechává na úpravu vnitrostátním právním řádem.

Úprava obsažená v zákoně proto zejména stanoví některé postupy poskytovatelů služeb vytvářejících důvěru a požadavky na služby vytvářející důvěru a pravidla elektronického podepisování, elektronického pečetění a opatřování dokumentů elektronickými časovými razítky. Zákon rovněž stanovuje Ministerstvo vnitra jako orgán dohledu nad poskytovateli služeb vytvářejících důvěru. V zákoně není upravena elektronická identifikace, která bude řešena samostatně v připravovaném zákoně o elektronické identifikaci. Tímto zákonem byla zrušena věcná materie zákona o elektronickém podpisu, neboť tuto oblast zcela upravuje nařízení eIDAS a výše zmíněný zákon o službách.

V současné době je vytvářen systém státem garantované elektronické identity vyhovující požadavkům eIDAS. Nosičem elektronické identity, která bude dostupná pro každého a zdarma, bude eObčanka jako univerzální klíč k elektronickým službám. Zároveň se připravuje novela zákona o občanských průkazech. Co se týče návrhu zákona o elektronické identifikaci, aktuálně se nachází v meziresortním připomínkovém řízení. Do připomínkového řízení byl zákon odeslán 19. října 2016, konec připomínkového řízení by měl nastat 18. listopadu 2016. Zatím je navrhovaná účinnost zákona k 1. lednu 2018.

Pilotní projekt pro využití elektronické identity bude realizován společně s ČSSZ, GFŘ a Krajem Vysočina a na PVS, konkrétně na CzechPOINT@home. Ověření uživatele služby proběhne na identifikační bráně eIdentita.cz, která bude součástí Národní identitní autority. eObčanka nabídne i možnost elektronického podepisování.

* 1. Elektronický občanský průkaz

Již stávající zákon č. 328/1999 Sb., ve znění pozdějších předpisů, umožňuje do kontaktního elektronického čipu stávajícího elektronického občanského průkazu zapisovat kryptografické klíče spolu s certifikátem sloužícím k autentizaci držitele občanského průkazu vůči informačním systémům, vydaným důvěryhodným poskytovatelem certifikačních služeb (dále jen „autentizační certifikát“) odpovídajícím těmto klíčům. Autentizační certifikát může sloužit ke vzdálené identifikaci občana vůči portálům veřejné správy i vůči jiným informačním systémům. K zápisu kryptografických klíčů a autentizačního certifikátu je oprávněn pouze držitel občanského průkazu. Poskytovatelé tento typ certifikátu nabízejí pod názvem „komerční certifikát“.

Dále se připravuje vydávání „nového“ elektronického občanského průkazu, který bude vždy vybaven kontaktním elektronickým čipem, na kterém bude již při výrobě nahrán identifikační certifikát občanského průkazu. Nebude se již vybírat správní poplatek za umístění kontaktního elektronického čipu na občanském průkazu. Zmiňovaný „nový“ občanský průkaz se stane základním nástrojem sloužícím občanům pro prezenční i vzdálené prokázání totožnosti s nejvyšší úrovní důvěry zaštítěné ČR.

S využitím elektronického občanského průkazu se občanům například naskytne možnost získat své údaje z registru obyvatel, daňového portálu a dalších úředních systémů a zároveň vznikne jednodušší možnost elektronické komunikace se státem. Ověřování totožnosti by mělo být jednodušší a šlo by provést nejen na úřadě ale i na dálku (on-line). Občané by také mohli dokumenty podávat přímo z domova a nemuseli by se dostavovat osobně na úřad. Stát tím nabídne automaticky každému držiteli občanského průkazu možnost elektronické identifikace na nejvyšším stupni důvěry podle nařízení eIDAS.

Vládní návrh zákona, kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a další související zákony, byl dne 26. září 2016 schválen vládou. Účinnost tohoto zákona je stanovena prvním dnem dvanáctého kalendářního měsíce následujícího po jeho vyhlášení, předběžně se kalkuluje s účinností od roku 2018.

* 1. Služby CzechPOINT

V rámci rozšiřování nabídky služeb CzechPOINT byl ve spolupráci s Českým úřadem zeměměřickým a katastrálním zpřístupněn výpis z katastru nemovitostí z moci úřední pro obce a kraje (v rámci CzechPOINT@office) v dubnu 2015, dále výpis ze snímku KN mapy pro občany (v rámci kontaktních míst veřejné správy) v srpnu 2015 a výpis ze snímku KN mapy z moci úřední pro obce a kraje (v rámci CzechPOINT@office) v říjnu 2015. Od září 2015 je k dispozici on-line výpis z bodového výpisu řidiče a od listopadu 2015 je možné odeslat výstup z autorizované konverze do vybrané datové schránky (pro FO, PFO i PO). V lednu 2016 byl ve spolupráci s Policejním prezidiem zpřístupněn registr zbraní (pro FO i PO), a to pro všechny exekutory. V současné době se pracuje na formuláři pro CzechPoint@office v součinnosti s Policií ČR (konkrétně v rámci agend pátrání po vozidlech a pátrání po osobách), dále na formuláři pro báňské úřady s přístupem do registru zbraní a na mobilním formuláři pro smartphony a tablety pro zpřístupnění výpisu z evidence přestupků.

* 1. Iniciativa 202020

Cílem Iniciativy je podpořit a urychlit vývoj ČR v oblasti eGovernmentu. Název Iniciativy je odvozen od ambice, aby se ČR do roku 2020 posunula ve světových žebříčcích hodnotících úroveň a využívání služeb eGovernmentu dopředu a ocitla se tak mezi prvními dvaceti hodnocenými zeměmi v Evropě podle indexu OSN. Iniciativa 202020 si klade za cíl aktivně přispívat k nalezení shody napříč politickým spektrem a veřejnou správou na odstranění legislativních, organizačních, případně dalších bariér bránících většímu rozšíření on-line služeb veřejné správy, které mohou usnadnit život a podnikání v ČR. Iniciativa 202020 se chce zejména podílet na propagaci funkčních digitálních služeb státu a zvyšovat tím povědomí veřejnosti o jejich nabídce a využitelnosti pro život a podnikání.

Zároveň je jejím smyslem sdružovat a propojovat odborníky na oblast eGovernmentu, politické reprezentanty, představitele exekutivy a akademické a podnikatelské sféry a tím podněcovat veřejnou debatu, která by měla vést k tlaku na poskytování širší škály služeb státu elektronickou cestou. Za vznikem Iniciativy stojí ICT Unie spolu s krajem Vysočina, Ministerstvem vnitra a koordinátorem digitální agendy ČR. Iniciativa je koncipována jako otevřená platforma, do které se může zapojit každý, kdo považuje téma eGovernmentu za důležité pro budoucnost ČR. Iniciativu zastřešuje politická deklarace, která vysvětluje klíčový význam služeb e-Governmentu pro efektivní řízení státu a udržení konkurenceschopnosti ČR.

Hlavním nástrojem Inciativy v současnosti je webová stránka www.202020.cz, která sdružuje existující online služby poskytované státem. Zároveň obsahuje výčet některých plánovaných služeb a umožňuje zasílat podněty k tvorbě nových online služeb. Webová stránka bude průběžně aktualizována. Na dalším rozvoji Iniciativy se dále pracuje.

* 1. **Otevřená** data

Vybraná data veřejné správy jsou nyní k dispozici prostřednictvím formátu otevřených dat za pomoci Národního katalogu otevřených dat a s využitím vzorových publikačních plánů. Implementace otevřených dat v ČR ve sledovaném období výrazně pokročila dopředu. Otevřená data byla zakotvena do českého legislativního systému v září 2016, kdy byl vydán zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce. Tato novela upravuje zákon č. 106/1999 Sb., o svobodném přístupu k informacím. V rámci ní je nově definován pojem otevřená data, Národní katalog otevřených dat je veden jako informační systém veřejné správy a slouží jako centrální místo systému otevřených dat VS ČR. V souvislosti s novelou je také připraven návrh Nařízení vlády o stanovení seznamu informací povinně zveřejňovaných jako otevřená data, který je v současné době v mezirezortním připomínkovacím řízení. Národní katalog otevřených dat byl spuštěn v dubnu 2015 a v současné době je v Národním katalogu otevřených dat (NKOD) registrováno přes 44 871 datových sad. V roce 2015 vznikla metodologie Standardy publikace a katalogizace otevřených dat veřejné správy ČR.

MV průběžně pořádalo bezplatná školení ke standardům otevřených dat. Např. v deseti školeních (září – listopad 2015) 415 osob z celkem 206 subjektů. Závazky v oblasti otevřených dat byly nově vloženy do aktualizovaného Akčního plánu pro rozvoj digitálního trhu a staly se jednou z hlavních priorit nově ustanoveného koordinátora digitální agendy. V roce 2016 byly nové závazky ČR v oblasti otevřených dat součástí Akčního plánu České republiky Partnerství pro otevřené vládnutí na období let 2016 až 2018. Koordinátor digitální agendy spolu s Ministerstvem vnitra také chystá spustit webový formulář pro veřejnost, který bude sbírat podněty k nejžádanějším datům k otevření.

* 1. Elektronická faktura

S ohledem na rozsáhlé legislativní úpravy v souvislosti se směrnicí 2014/55/EU o elektronické fakturaci při zadávání veřejných zakázek jsou připravována opatření na implementaci přijímání elektronických faktur v rámci veřejné správy. Směrnice byla transponována do právního řádu ČR zákonem č. 134/2016 Sb., o zadávání veřejných zakázek. Nyní probíhá vyhodnocení připravenosti veřejné správy na povinnou elektronickou fakturaci v souladu s evropskými projekty, úprava metodických postupů a návrh typové architektury řešení, případně návrh změn v odpovídající legislativě, a ekonomická analýza dopadů na povinnou elektronickou fakturaci v rámci B2G. V následujících letech bude se směrnicí zavedena povinná e-fakturace v B2G. Standardy pro evropskou elektronickou fakturu jsou nyní předmětem jednání na evropské úrovni, proto není v současné době možno plně státní správu začít na elektronickou fakturaci ve společných formátech připravovat. Standardy by měly být zveřejněny do května 2017.

* 1. Dohledové centrum eGovernmentu

Jako hlavní přínosy budování Dohledového centra eGovernmentu (zkráceně DCeGOV) Ministerstvo vnitra vnímá zejména:

* Vybudování jednotného dohledového centra bezpečnostních a provozních dohledů zastřešující informační systémy celého resortu MV;
* zajištění nepřetržitého bezpečnostního dohledu a monitoringu komunikačních a informačních systémů KII a VIS resortu Ministerstva vnitra a popřípadě dalších informačních systémů resortu MV;
* navržení dostatečně variabilní architektury se snadnou možností dalšího rozvoje;
* realizace vybraných technických a organizačních opatření vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejících právních předpisů;
* zajištění nákladově efektivní centralizace bezpečnostních technologií a zajištění jednotného řízení kybernetické bezpečnosti v rámci resortu MV.

DCeGOV je implementováno jako otevřený systém, který lze kdykoliv rozšířit pro libovolný počet systémů. Budováním bezpečnostně-provozního dohledového centra, které nabízí pokrytí celé České republiky díky svým 14 krajským sběrným místům, postupně dochází k centralizaci provozních a bezpečnostních nástrojů, které mohou využívat plošně všechny systémy resortu MV (včetně krajských ředitelství Hasičského záchranného sboru, Policie ČR a dalších).

Připojované systémy využívají již nastavenou technologickou platformu, kde dochází ke korelaci a agregaci logů a dat a následnému vyhodnocení zjištěných událostí a incidentů za využití jednotných procesních principů řízení incidentů a událostí včetně hlášení na NCKB. Tím dochází ke sjednocení bezpečnostních, provozních a rozvojových úloh a díky tomu i k centralizaci správy a nákupů informačních technologií, následně pak k úsporám času, financí i lidských zdrojů.

* 1. Elektronické zdravotnictví

Ministerstvo zdravotnictví (dále jen MZd) bylo určeno gestorem v klíčové prioritní oblasti 4. Rozvoj elektronické veřejné správy – části **Elektronické zdravotnictví**. V Akčním plánu pro rozvoj digitálního trhuje zařazeno elektronické zdravotnictví v gesci MZd s těmito opatřeními:

* Dokončit Národní strategii elektronického zdravotnictví.
* Vytvořit koordinační centrum pro řízení rozvoje elektronizace.
* Vytvořit architekturu stávajícího a budoucího stavu klíčových projektů pro rozvoj elektronizace.
* Realizovat klíčové projekty/stavební prvky elektronizace.
* Připravit opatření k eliminaci bariér.

V roce 2016 Ministerstvo zdravotnictví dokončilo první znění Národní strategie elektronického zdravotnictví ČR na období 2016 – 2020 v souladu s Metodikou přípravy veřejných strategií, která reaguje na vývoj za poslední roky a opírá se o Zdraví 2020 - Národní strategii ochrany a podpory zdraví a prevence nemocí, schválenou vládou 8. ledna 2014 a vychází z jejího Akčního plánu elektronizace zdravotnictví, přijatého vládou dne 20. srpna 2015.

Primární zdroje finančních prostředků pro zajištění a podporu implementačních projektů Národní strategie elektronického zdravotnictví budou zabezpečeny v rámci rozpočtovaných výdajů kapitoly MZd a střednědobých výdajových limitů této kapitoly, případně rozpočty krajů. Důležitým zdrojem budou zároveň Evropské strukturální a investiční fondy. Dalším zdrojem financování budou případně jiné finanční mechanismy podpory - Norské fondy, nástroj pro propojení Evropy CEF, zdroje WHO (Smlouva o spolupráci mezi MZd a Regionální úřadovnou WHO pro Evropu).

K plánovaným opatřením pro oblast elektronického zdravotnictví byly Ministerstvu vnitra předloženy projektové listy pro financování z ESI fondů. S řídícími orgány operačních programů a MV proběhla jednání o uznatelnosti předkládaných projektů. Plánovaná opatření pro oblast elektronického zdravotnictví jsou v souladu s postupem naplňování Strategického rámce rozvoje veřejné správy České republiky pro období 2014 – 2020, který zahrnuje v rámci implementačního plánu pro cíl 3 projektový okruh 3.7 eHealth, pokrývající oblast elektronizace zdravotnictví. Všechna plánovaná opatření uvedená v AP pro oblast elektronického zdravotnictví jsou postupně zpřesňována s cílem stanovit časový rámec plnění úkolů.

Ministerstvo zdravotnictví definovalo pro nejbližší období, tj. do roku 2020 následující priority:

* Vytvoření / úprava autoritativních registrů Národního registru zdravotnických pracovníků, Národního registru poskytovatelů zdravotních služeb, které budou obdobou základních registrů eGovernmentu a budou autoritativním zdrojem údajů pro identifikaci subjektů a zdravotnických pracovníků.
* Vybudování základní resortní infrastruktury pro řešení elektronické identity v resortu zdravotnictví a k tomu příslušející datová rozhraní pro sdílení informací. Tato infrastruktura zajistí a posílí právní a organizační jistoty zdravotnických pracovníků a zavede možnost kontinuity při práci s elektronickými písemnostmi a zdravotnickou dokumentací. Tento projekt bude v souladu s řešením eID realizovaným MV a bude řešit i autorizaci, autentizaci a správu přístupů a souhlasů.
* Zajištění jednotného přístupu ke službám elektronického zdravotnictví v souladu s principy eGovernmentu. Průřezová priorita, která má za cíl uzpůsobit procesy ve zdravotnictví, a to zejména správního charakteru tak, aby v maximální míře využívaly postupy a služby eGovernmentu, se kterými je občan srozuměn a naučil se je využívat při řešení životních situací.
* ePreskripce – připravit postupný náběh plnohodnotné elektronické preskripce včetně vedení lékového záznamu pacienta, přístupného oprávněným lékařům, lékárníkům a pacientovi, s možnostmi kontroly interakcí a duplicit. Tento úkol bude vyžadovat legislativní úpravy.
* Ustavit / vytvořit Národní centrum elektronického zdravotnictví, které bude mít za úkol programově a hospodárně koordinovat a podporovat rozvoj digitalizace, udržovat a rozvíjet koncepci národního systému elektronického zdravotnictví.

Rámcový harmonogram realizace jednotlivých cílů a opatření Národní strategie elektronického zdravotnictví rozděluje implementaci do tří kategorií: zadání prioritní, jejichž realizace byla či bezprostředně bude zahájena; střednědobé, kde má být dosaženo měřitelného pokroku do roku 2020; a ostatní, nastavující dlouhodobé směřování bez nutného stanovení priorit do roku 2020. Zároveň zachycuje takto kategorizované cíle a opatření ve vazbě na projektové okruhy, popř. projektové záměry, podrobněji specifikované ve strategii. V neposlední řadě předložené schéma podává rámcovou představu o vzájemné závislosti (podmíněnosti) priorit, cílů, opatření a projektových okruhů či záměrů v čase.

Pro všechny jednotlivé cíle explicitně musí být stanoveny implementační kroky zahrnující přípravu potřebných legislativních změn. V návaznosti na to také kroky týkající se legislativního procesu těchto změn, jinak není předložený harmonogram realistický.

Pomalý postup potřebných legislativních kroků může vést k posunu realizace cílů strategie do delšího časového období a celá strategie musí být tedy z tohoto hlediska kontinuálně přehodnocována a aktualizována s důrazem na aktuální vývoj priorit elektronizace zdravotnictví.



Legenda k obrázku Harmonogram realizace prioritních oblastí Národní strategie elektronického zdravotnictví:

* Aktivity označené šedivě znázorňují přípravnou fázi na implementaci – tvorbu implementačního plánu.
* Kroužkem jsou označeny odkazy na projektové záměry definované ve strategii. Harmonogram takto uvádí spojitost na zdroje financování.
* Bílé šipky bez popisu označují, že aktivita nekončí realizací projektového záměru a dosažením stanovených identifikátorů, ale potřeba ji dále udržovat, rozvíjet a modifikovat dle aktuálních požadavků.
* SC 3 - Průběh a rozsah realizace jednotlivých opatření tohoto strategického cíle bude určen dle analytických závěrů a studií.
* SC 4.3 - Úspěšná realizace strategie podmiňuje implementaci řady dalších opatření, zejména potřebu personálních a odborných expertních kapacit ke specifikaci jednotlivých záměrů.

Harmonogram bude průběžně aktualizován, aby odrážel skutečný vývoj elektronizace a vzal do úvahy i rozvoj dalších služeb resortu zdravotnictví, eGovernmentu a také technologický pokrok.

* 1. eJustice

Klíčová pro další rozvoj eGovernmentu je Resortní strategie pro rozvoj eJustice, jejímž cílem je posílit efektivitu a rychlost činností organizačních složek resortu justice a zvýšit transparentnost rozhodování, a to mimo jiné prostřednictvím dalšího rozvoje elektronizace justice (eJustice). V říjnu 2016 byla odevzdána první žádost o schválení projektu eJustice 2020 - část insolvenční řízení. V současnosti spadají do zmíněné strategie následujících opatření:

* Podpořit podmínky pro spravedlivé, zákonné a rychlé rozhodování organizačních složek resortu justice a jejich výkon;
* Umožnit snadnou a přívětivou komunikaci s účastníky řízení, veřejností a jinými orgány veřejné moci včetně zkvalitnění a rozšíření rozsahu poskytovaných informací;
* Úprava a optimalizace systému technické infrastruktury, financování a údržby informačních a systémů a technologií v justici.

Dotčené organizace a jejich role v rámci rozvoje:

Ministerstvo spravedlnosti: Ministerstvo kromě výkonu správy v oblasti ICT pro ostatní organizační složky resortu justice samo vykonává určité činnosti, které lze zařadit pod pojem eJustice. Kromě obecných povinností vedení spisové služby v elektronické podobě a přijímání a doručování elektronických podání, lze např. uvést vedení evidence insolvenčních správců, registru pomoci obětem trestné činnosti, seznamu rozhodců, seznamu mediátorů, které se zveřejnují na internetových stránkách.

Vězeňská služba: Z hlediska eJustice je významná povinnost Vězeňské služby vést evidenci osob ve výkonu zabezpečovací detence, vazby a trestu odnětí svobody, ze které čerpají údaje orgány činné v trestním řízení a další osoby a orgány, kterým to zákon umožňuje. Tato evidence se označuje jako Centrální evidence vězněných osob (CEVO).

Probační a mediační služba: Z hlediska eJustice je významná možnost provádění elektronického monitoringu osob, který umožňuje účinnou a bezprostřední kontrolu výkonu vhodných alternativních trestů a opatření. Dále je významné poskytování informací a potřebné podpory orgánům činným v trestním řízení. Rovněž poskytuje ostatním složkám důležité seznamy, např. přehledy poskytovatelů obecně prospěšných prací, registr osob odsouzených k alternativním trestům, atd.

Justiční akademie: Z hlediska eJustice je významné zajišťování vzdělávání prostřednictvím tzv. e-learningu spočívajícího jak v přenosu přednášek do dalších sálů pracovišť Justiční akademie, tak v zajištění interaktivních učebních textů pro pracovníky justice.

Rejstřík trestů: Nově vede Rejstřík trestů evidenci přestupků, ve kterém se evidují údaje o pravomocných rozhodnutích o vybraných přestupcích.

Institut pro kriminologii a sociální prevenci: Dopady eJustice na toto pracoviště a dopady činnosti pracoviště na eJustici jsou zejména v oblasti práce s datovými vzory a jejich evaluace pro vědecké účely.

* 1. Databáze strategií

Jedním z důležitých nástrojů rozvoje strategické práce v ČR je elektronický systém **Databáze strategií**. Databáze strategií je celostátním informačním systémem dokumentů strategického charakteru, který umožňuje jejich přehledné zobrazení, vč. zobrazení cílů a opatření, odpovědností za plnění, indikátorů úspěšnosti. Zároveň je zde možné tyto dokumenty interaktivně vytvářet či je zobrazovat ve strategických mapách. Na jednom místě tak lze nabízet pestrá data k relevantním dokumentům na mezinárodní, národní, oblastní, regionální i místní úrovni, které zde mohou být rozpracovávány co do jejich obsahu a následně s nimi dále pracovat.

Nástroj je dostupný jak pro veřejnost (webové rozhraní), tak i pro zástupce relevantních institucí, kteří jej ve spolupráci s MMR naplňují strategickými dokumenty a souvisejícími materiály. Databáze se průběžně aktualizuje a doplňuje o nové funkcionality, což je plánováno i v následujících letech.

* 1. Aplikace k operačním programům a elektronické zadávání veřejných zakázek

V provozu a stále aktualizována je **aplikace MS2014+**. Umožňuje přípravu, plánování, řízení, monitorování, podávání zpráv a vyhodnocování plnění Dohody o partnerství a jednotlivých operačních programů až do úrovně operací. Jejím prostřednictvím lze vyhlašovat výzvy k podávání žádostí o podporu, předkládat a vybírat žádosti o podporu a spravovat projekty v rámci životního cyklu a v době udržitelnosti, např. podávat žádosti o platbu, změnová hlášení a další obdobné dokumenty. MS2014+ přináší jeden společný monitorovací systém a jedinou databázi pro ukládání všech dat. Procesy jsou realizovány dle jednotné metodiky. Zároveň přináší tři uživatelské portály: IS KP14+ pro externí uživatele, CSSF 14+ pro interní uživatele a Service Desk neboli servisní portál. Do konce roku proběhnou úpravy a optimalizace základních procesních funkcionalit.

Více než rok provozovaný **Národní elektronický nástroj** je IT aplikace volně dostupná z internetu (https://nen.nipez.cz). Je určen pro elektronické zadávání veřejných zakázek a koncesních řízení a všechny zainteresované subjekty (veřejnost, zadavatel, dodavatel, externí administrátor). Funkčnost je poskytována všem subjektům zdarma. Jeho využívání je v současné době dobrovolné.

* 1. Portál eAGRI a elektronizace agend Ministerstva zemědělství

Rezort zpřístupňuje opatření v rámci eGovernmentu především prostřednictvím **portálu eAGRI**. V poslední době připravil řadu výstupů definujících **procesy a standardy**, přičemž na dalších dále pracuje. V průběhu roku 2016 jsou jednotlivé procesy a standardy postupně implementovány na úrovni MZe, dále jsou v přípravě a postupné realizaci primárně procesy obsluhy jednotlivých dotačních titulů.

V rámci IT architektury dosáhlo ministerstvo zprovoznění **Centrálního repositáře architektonických modelů** v ArchiMate notaci a publikace související dokumentace (HP Enterprise Maps). Repositář podporuje životní cyklus architektonických návrhů, umožňuje sdílet a vyhledávat komponenty a podporuje řízení ICT.

V rámci tohoto řešení je dále možnost udržovat a sdílet agendové a podpůrné procesy v přehledných, exportovatelných schématech vhodných pro využití zadávacích dokumentacích nových systému, nebo při jejich nahrazováních.

**Dokumentační nástroj** (Sparx Systems Enterprise Architect) je aplikace pro modelování a dokumentaci architektury a centrální repositář detailních technických modelů. Systém je primárně určen k zajištění standardů dokumentace všech systémů MZe – pro využití interních uživatelů (systémoví inženýři a architekti) a externí dodavatele.

V průběhu roku 2015 bylo vyhlášeno výběrové řízení na realizaci **IS Národní dotace** dle nových standardů a metodiky. Tento modulární informační systém je využíván pro administraci a nábor národních dotačních titulů z oblastí v působnosti resortu MZe. Dodavatel v rámci návrhu architektury musel pouze částečně modifikovat a doplňovat architektonický návrh (výrazné zkrácení analýzy).

**AgriGIS** – v průběhu roku 2017 a 2018 bude vytvořen GIS nástroj pro práci s daty resortu MZe. Nástroj bude přístupný jako resortní geoportál s pokročilými možnostmi práce jak pro zemědělskou tak širokou veřejnost. Díky univerzálnímu konceptu budou přístupná data v režimu konceptu OpanData tak kde to bude možné. Jako podkladové snímky budou použity jak podklady z dálkového průzkumu země, ortofoto, 4D snímky apod. Systém bude propojen s jednotlivými resortními GIS platformami s možností konzumace jejich dat a tím získá systém mnoho zajímavých dat pro následné dopadové analýzy a strategie resortu a vědeckých institucí. V neposlední řadě bude systém disponovat daty, která jsou důležitá pro výkon precizního zemědělství. V rámci nasazení a provozu je uvažováno s dalšími efekty, jako je rozvoj startup projektů a podpory inovativních aktivit komerčních subjektů.

**Projektový program pro zajištění kybernetické bezpečnosti –** projektový program pro zajištění pokročilých funkcí bezpečnostního monitoringu a to nejenom v návaznosti na kybernetický zákon. V roce 2016 budou dokončeny projekty pro přístup privilegovaných uživatelů a pokročilého monitoringu Netflow a detekce anomálií v aplikacích, v průběhu roku 2017 bude doimplementován bezpečnostní monitorování na úrovni centrálních IS resortu MZe. V průběhu dalších let budou implementovány systémy správy identit, přístupového Portálu farmáře a další.

* 1. Informační systém Registru živnostenského podnikání

Informační systém Registru živnostenského podnikání (IS RŽP) zajišťuje jednotný výkon státní správy na úseku živnostenského podnikání v celé České republice;

* zpřístupňuje informace z veřejné části živnostenského rejstříku prostřednictvím internetu (včetně možnosti pořízení elektronicky podepsaného výpisu);
* zajišťuje funkci Centrálního registračního místa – podnikatel může prostřednictvím obecních živnostenských úřadů činit podání i vůči jiným orgánům veřejné správy (např. finanční úřady, správa sociálního zabezpečení, zdravotní pojišťovny);
* předává centrálně elektronicky data z IS RŽP oprávněným orgánům veřejné moci;
* umožňuje elektronické podání (ohlášení živnosti, žádost o koncesi);
* je editorem registru osob.

V roce 2016 byl realizován projekt k zajištění infrastruktury IS RŽP se zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy. V rámci projektu byl zaveden proces identifikace, vyhodnocování a zvládání jednotlivých bezpečnostních událostí a incidentů pro celý IS RŽP a byla zavedena zvýšená ochrana integrity komunikačních sítí IS RŽP, včetně služby Security Operation Centre, SW a HW vybavení.

V legislativním procesu je novela živnostenského zákona, která, mimo jiné, umožní na základě žádosti fyzických či právnických osob vydávání sestav v listinné nebo elektronické podobě z veřejné části živnostenského rejstříku (jedná se o sestavy podnikatelů podle adresy sídla, umístění provozovny a podle živností). Účinnost novely se předpokládá od 1. července 2017.

* 1. Elektronizace finanční správy

Ministerstvo financí pracuje na novém zákonu o příjmových daních. Příprava je navázána na zjednodušení daňového systému a rozšiřování **elektronizace finanční správy** (termín: čtvrtý kvartál 2019). Finanční správa v rámci resortního projektu Ministerstva financí „MOJE daně“ pracuje na vybudování nového daňového informačního systému. Vedle nutnosti soutěžit nový systém z důvodu *vendor lock-in* stávajícího systému (snížení exkluzivity stávajícího dodavatele a závislosti na něm) je tuto změnu nezbytné provést, aby byly vytvořeny podmínky k rozvoji služeb poskytovaných Finanční správou a byla zvyšována efektivita procesů v rámci správy daní a dalších působností zabezpečovaných těmito orgány.

Rozvoj elektronizace správy daní v rámci Finanční správy umožní následující:

1. Vybudování portálu umožňujícího oboustrannou efektivní komunikaci mezi Finanční správou a daňovými subjekty. Tento portál umožní naplnit související cíle tohoto akčního plánu ke snižování administrativní zátěže daňové veřejnosti při respektování zásad daňové mlčenlivosti. Mezi uvažovanými aplikacemi je například podávání předvyplněných daňových přiznání, sledování stavu osobního daňového účtu, nahlížení do daňového spisu, generování tzv. potvrzení o bezdlužnosti, výměna údajů vztahujících se k individuálním daňovým subjektům jako například potvrzení o příjmu zaměstnavatele či vytvoření rozhraní pro systémy třetích stran pro zvýšení využitelnosti na straně daňových subjektů.
2. V návaznosti na budování portálu bude řešena maximalizace automatizace procesů s cílem zefektivnit činnost Finanční správy. Dále bude zabezpečena centralizace dat Finanční správy při respektování zásad kybernetické bezpečnosti, která umožní efektivnější využívání kapacit Finanční správy.
3. Realizace projektů popsaných v bodech 1. a 2. vytvoří základ pro sjednocení výběru daní s výběrem sociálního a zdravotního pojištění v budoucnu s minimálními dodatečnými náklady.
	1. ePortál České správy sociálního zabezpečení

Přihlašovací údaje vydávané ČSSZ v budoucnu otevřou služby ePortálu všem, a to i bez datových schránek. Obliba služeb ePortálu České správy sociálního zabezpečení pomalu stoupá, i když mnohé občany od jeho využívání dosud odrazuje nutnost vlastnit datovou schránku. ČSSZ má proto připravený záměr na zjednodušení přístupu k ePortálu dalším klientům. Hodlá zahájit realizaci projektu, který umožní poskytovat veřejnosti vlastní autentizační (přihlašovací) údaje.

Přihlašování do ePortálu ČSSZ bude rovněž možné prostřednictvím elektronického občanského průkazu (eOP) poté, co Ministerstvo vnitra začne plošně a bez poplatků vydávat elektronický občanský průkaz s čipem.

V polovině roku 2015 ČSSZ úspěšně dokončila projekt zavedení interaktivních formulářů. Na ePortálu ČSSZ je dnes vystaveno více než 100 tiskopisů pro online vyplnění včetně zákonem předepsaných tiskopisů. Tiskopisy obsahují funkce kontroly dat, elektronického odesílání a uložení odeslaných dat, dále funkce ukládání rozpracovaných formulářů, tisku. Přihlášenému (autentizovanému) uživateli je formulář předvyplněný daty z databáze ČSSZ.

* 1. Infrastruktura pro dopravně správní agendy

Ministerstvo dopravy plánuje zajištění služeb provozu infrastruktury pro dopravně správní agendy (DSA) Ministerstva dopravy a jeho ekonomického a personálního systému. Pod dopravně správní agendu spadá například Centrální registr vozidel, jenž obsahuje technické údaje o vozidlech (rok výroby, palivo, rozvory kol apod.). Dále je součástí DSA také Centrální registr řidičů, který obsahuje informace o osobách, jež vlastní řidičský průkaz. Pod DSA rovněž spadá Rejstřík podnikatelů v silniční dopravě, což je jednotná databáze informací o podnikatelích v silniční dopravě a řidičích taxislužby.

Realizovat se bude služba zajištění provozu IT infrastruktury DSA, ekonomického a personálního systému MD, dále služba zajišťující soulad provozu IT infrastruktury se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a služba Call Centra.

Potřeba realizace vyplývá z nutnosti zajištění infrastruktury pro dopravně správní agendy a ekonomický a personální systém MD, kdy uvedené služby jsou v současnosti zajištěny stávajícím poskytovatelem (O2 IT Services s.r.o.) na základě smlouvy „Zajištění provozu infrastruktury pro dopravně správní agendy a systémy ERP a HR – přechodné období“, jejíž účinnost končí nejpozději 25. září 2017. Zároveň je zadavatel nucen realizovat povinnosti vyplývající mu jako správci informačních systémů kritické informační infrastruktury a významných informačních systémů a z provedených bezpečnostních a organizačních opatření dle zákona o kybernetické bezpečnosti. MD hodlá migrovat kompletní IT infrastrukturu od stávajícího provozovatele do národního datového centra.

1. Koordinační středisko pro resortní zdravotnické informační systémy. [↑](#footnote-ref-1)
2. Zdroj: Výsledky dotazníkového šetření a prezentace s názvem „Problematika čerpání ve Specifickém cíli 3.2 Integrovaného regionálního operačního programu (SC 3.2 IROP)“, která byla představena dne 9. 9. 2016 na zasedání Rady vlády pro informační společnost náměstkem pro řízení Sekce evropských programů Ministerstva pro místní rozvoj ČR Zdeňkem Semorádem. [↑](#footnote-ref-2)
3. Způsobilými výdaji se rozumí výdaje vynaložené na stanovený účel a v rámci období stanoveného v právním aktu o poskytnutí / převodu podpory, které jsou v souladu s příslušnými předpisy EU a ČR, příslušným metodickým pokynem NOK a dalšími pravidly stanovenými řídicím orgánem pro daný program. [↑](#footnote-ref-3)