



# **Dokumentace**

**k projektu Czech POINT**

**Agendy a činnostní role v Jednotném  
identitním prostoru (JIP)**

Vytvořeno dne: 23. 9. 2013

Aktualizováno: 16. 10. 2018

Verze: 1.5

© 2013-2018 MVČR

## Obsah

|           |   |          |
|-----------|---|----------|
| <b>1.</b> | <b>Úvod .....</b>                             | <b>3</b> |
| 1.1.      | Účel dokumentu .....                          | 3        |
| 1.2.      | Manažerské shrnutí .....                      | 3        |
| 1.3.      | Definice pojmů .....                          | 3        |
| <b>2.</b> | <b>Registr práv a povinností.....</b>         | <b>5</b> |
| 2.1.      | Ohlášení a registrace agend .....             | 5        |
| 2.2.      | Oznámení výkonu působnosti v agendě .....     | 5        |
| <b>3.</b> | <b>Jednotný identitní prostor .....</b>       | <b>6</b> |
| 3.1.      | Agendy a činnostní role v JIP .....           | 6        |
| 3.2.      | Činnostní role a uživatelé v JIP .....        | 6        |
| 3.3.      | Přístupové role do AIS a uživatelé v JIP..... | 6        |
| <b>4.</b> | <b>Dostupné zdroje informací.....</b>         | <b>8</b> |

# 1. Úvod

## 1.1. Účel dokumentu

Tento dokument popisuje problematiku agend a činnostních rolí, tedy pojmů týkajících se základních registrů, a jejich vztah k Jednotnému identitnímu prostoru (JIP), který je provozován v rámci systému Czech POINT.

## 1.2. Manažerské shrnutí

Ohlašovatel agendy (ústřední správní úřad, který má gesci nad příslušným zákonem) provede ohlášení agendy v registru práv a povinností. V rámci tohoto ohlášení specifikuje, jaké orgány veřejné moci (OVM) tuto agendu vykonávají a v jakých činnostních rolích.

Uživatel, který bude pracovat v AIS RPP Působnostní, musí lokální administrátor přidělit přístupovou roli a činnostní roli. Podrobnosti jsou uvedeny v příručce pro lokálního administrátora.

V ohlášení agendy definuje ohlašovatel daný(é) OVM k výkonu agendy v příslušných činnostních rolích. Tyto role (spolu s danou agendou) jsou z RPP načteny do JIP a uloženy k danému OVM. V aplikaci Správa dat může pak lokální administrátor přidělit tyto činnostní role konkrétním uživatelům ve svém OVM.

Kdy má smysl činnostní roli uživateli přidělovat? Záleží to na informačních systémech, s nimiž uživatel pracuje. Pokud se jedná o systémy, které nezískávají data ze základních registrů, uživatel činnostní role nepotřebuje. Pokud se jedná o systémy, které přistupují do základních registrů, ale nejsou integrovány s JIP, pak uživatelé sice činnostní role potřebují, ale je zbytečné role přidělovat v aplikaci Správa dat. Informační systém se totiž k takto nastaveným rolím „nedostane“ právě kvůli chybějící integraci na JIP – v tomto případě se musí činnostní role nastavit v rámci daného systému.

Správci AIS, které jsou integrovány s JIP, mohou dále definovat tzv. přístupové role, pomocí kterých se řídí přístup uživatelů k funkcím AIS. Správce AIS nejprve stanoví množinu OVM, které mohou přistupovat do AIS, a těmto OVM nastaví přístupové role. Poté lokální administrátoři přidělí přístupové role konkrétním uživatelům v OVM.

## 1.3. Definice pojmů

**Základní registry** jsou centrální registry veřejné správy, jejichž pomocí je možné sdílet data v rámci veřejné správy. Základním legislativním předpisem je zákon č. 111/2009 Sb., o základních registrech, který definuje tyto základní registry:

- základní registr obyvatel – zkráceně registr obyvatel (ROB)
- základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci – zkráceně registr osob (ROS)
- základní registr územní identifikace, adres a nemovitostí (RUIAN)
- základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností – zkráceně registr práv a povinností (RPP)

Velice zjednodušeně lze chápat základní registry jako centrální databáze s údaji o občanech ČR, právnických osobách, podnikatelích a nemovitostech.

Výše uvedený zákon dále vyjmenovává tzv. **referenční údaje**, které jsou uloženy v jednotlivých základních registrech. Referenční údaje jsou oprávněni měnit pouze stanovení editoři, zatímco ostatní OVM mohou tyto údaje pouze číst, případně reklamovat jejich nesprávnost u editora. Díky tomuto principu je zaručeno, že dva různé OVM nebudou mít různé informace např. o občanech ČR. A jelikož referenční údaje může měnit pouze omezený počet editorů, je tak zaručena jejich správnost.

Referenční údaje mohou ze základních registrů získávat pouze OVM a soukromoprávní uživatelé údajů<sup>1</sup>. Je však možné, aby např. konkrétní fyzická osoba požádala o poskytnutí jejích referenčních údajů z ROB jiné fyzické nebo právnické osobě, která nemá do základních registrů ze zákona umožněn přístup. Informace jsou zasílány do datové schránky dané osoby.

OVM má několik možností, jak může získávat referenční údaje ze základních registrů:

- prostřednictvím informačních systémů, které jsou označovány jako **agendové informační systémy (AIS)**<sup>2</sup>;
- prostřednictvím formulářů Czech POINT nebo CzechPOINT@office;
- podáním žádosti do datové schránky Správy základních registrů (webové formuláře pro podání žádosti jsou umístěny na [Portálu veřejné správy](#)).

Přístup ke konkrétním referenčním údajům v základních registrech musí být samozřejmě omezen pouze na ty subjekty, které mají mít k těmto datům přístup podle příslušných zákonných ustanovení. Informace pro řízení přístupu k referenčním údajům jsou uloženy v registru práv a povinností (RPP).

V RPP jsou proto definovány **agendy**, které jsou podle zákona o základních registrech definovány jako „souhrn činností spočívajících ve výkonu vymezeného okruhu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci“. Zjednodušeně řečeno lze agendu přirovnat k procesnímu přepisu zákona. Detailněji se agendami zabývá kapitola 2.1.

V rámci agendy je definován seznam **činnostních rolí**, které udávají, kdo a co se v agendě vykonává a k jakým referenčním údajům v základních registrech může daný subjekt přistupovat. Činnostní role lze přirovnat k jednotlivým paragrafům v zákonu.

Návazně pak jednotlivé OVM oznamují vykonávání **působnosti v agendě**, kde např. upřesňují počty osob podílejících se na výkonu agendy.

**Jednotný identitní prostor (JIP)** je zabezpečený adresář OVM a úředníků státní správy, který je provozován v rámci systému Czech POINT. Uživatelské účty v JIP slouží úředníkům pro přihlašování do centrálních AIS, jako je Czech POINT, AIS RPP Působnostní, ISUI, apod.

**Katalog autentizačních a autorizačních služeb (KAAS)** je sada webových služeb, která poskytuje dvě základní funkcionality:

- autentizace uživatelů přistupujících do externích AIS za použití přihlašovacích údajů k uživatelskému účtu v JIP;
- editace údajů OVM a správa uživatelských účtů v JIP.

Aby externí AIS mohl využívat webové služby KAAS, musí se nejprve zaregistrovat do JIP. Správce zaregistrovaného AIS následně nadefinuje sadu tzv. **přístupových rolí**, které opravňují uživatele vykonávat určité činnosti v daném AIS. Přístupové role jsou přidělovány jednotlivým OVM a následně konkrétním uživatelům v těchto OVM.

Zatímco činnostní role (definovaná v RPP) povoluje přístup k určitým referenčním údajům v základních registrech, přístupová role (definovaná v JIP) dovoluje uživateli vykonávat v konkrétním AIS určité činnosti.

Činnostní role tedy povoluje přístup k datům v základních registrech, přístupová role povoluje přístup k funkcím AIS.

<sup>1</sup> Podnikající fyzické osoby nebo právnické osoby, které mají umožněn přístup k referenčním údajům v základních registrech nebo údajům v jiných agendových informačních systémech.

<sup>2</sup> Může se jednat o lokální AIS daného OVM, nebo AIS provozované centrálně, do kterých úředníci OVM přistupují dálkově.

## 2. Registr práv a povinností

Ohlášení agendy se provádí v informačním systému AIS RPP Působnostní. Jelikož je tento systém integrován s JIP/KAAS, musí se uživatelům tohoto systému nastavit odpovídající přístupové a činnostní role v JIP (prostřednictvím administrační aplikace Správa dat). Návod, jaké role je potřeba nastavit, je uveden v příručce pro lokálního administrátora [4].

### 2.1. Ohlášení a registrace agend

**Ohlášení agendy provádí pouze několik OVM označovaných jako ohlašovatelé agendy, jejichž seznam je dostupný na webových stránkách Správy základních registrů (jedná se např. o ministerstva).**

Ohlášení agendy se provádí např. v případě, že vstoupí v platnost nový zákon a ohlášení agendy provádí ten ohlašovatel, který má tento zákon ve své gesci.

Ohlašovatel agendy se přihlásí do AIS RPP Působnostní a otevře si formulář pro vytvoření nového ohlášení agendy. Formulář je rozdělen pomocí záložek na několik částí, do kterých se zadává název agendy, výčet právních předpisů, na jejichž základě je agenda vykonávána, výčet OVM vykonávajících agendu, seznam činností vykonávaných v agendě a rozsah oprávnění k referenčním údajům v základních registrech, která jsou přiřazena k jednotlivým činnostem. Jsou nadefinovány činnostní role jako vazba mezi souhrnnými či konkrétními označeními OVM a činnostmi v agendě.

Ohlášení nové agendy je odesláno správci RPP (tj. Ministerstvu vnitra). Nyní začíná běžet proces registrace agendy, kdy správce RPP posuzuje podané ohlášení agendy, žádá o stanovisko zainteresované strany (např. správce dalších ZR či AIS) a přiděluje kód agendy. Pokud je ohlášení v pořádku, zaregistruje správce RPP agendu a oznámí její registraci ohlašovateli a dotčeným OVM, které budou agendu vykonávat.

Pro tento proces je na webových stránkách Správy základních registrů zveřejněna metodika [1].

### 2.2. Oznámení výkonu působnosti v agendě

OVM obdrží datovou zprávou informaci o zaregistrování nové agendy a provede oznámení působnosti v této agendě. Podle zákona § 55 zákona č. 111/2009 Sb., o základních registrech má tak učinit do 30 dní ode dne registrace agendy.

Určená osoba OVM se přihlásí do AIS RPP Působnostní. Vybere akci „Oznámení o vykonávání působnosti v agendě“. Zobrazí se seznam nových nebo rozpracovaných oznámení.

Kliknutím na kód oznámení se zobrazí formulář s konkrétním oznámením. Úkolem určené osoby OVM je na seznamu činnostních rolí doplnit počet osob, které se podílejí na výkonu dané činnostní role, a celkový počet osob podílejících se na výkonu agendy. Také může upřesnit adresu pracoviště OVM, které vykonává tzv. úkon na žádost nebo údaj o převedení výkonu úkonu na žádost na jiný OVM.

Stisknutím příslušného tlačítka se dané oznámení odešle k registraci správci RPP (tj. Ministerstvu vnitra).

Pro tento proces je na webových stránkách Správy základních registrů zveřejněna metodika [2]. Na webových stránkách Ministerstva vnitra je k dispozici příručka pro kraje a obce [3] se stručným popisem tohoto procesu.

## 3. Jednotný identitní prostor

### 3.1. Agendy a činnostní role v JIP

JIP si pravidelně jednou denně stahuje z RPP seznam OVM s agendami a činnostními rolemi, k nimž má daný OVM „zaregistrovanu“ působnost v agendě.

Seznam agend a činnostních rolí si může zobrazit lokální administrátor daného OVM v aplikaci Správa dat na stránce s detailem subjektu (záložka „Správa rolí“). Postup pro zobrazení detailu subjektu je popsán v příručce pro lokálního administrátora [4].

Seznam agend a činnostních rolí je určen pouze pro prohlížení. Nejedná se rozhodně o náhradu AIS RPP Působnostní.

### 3.2. Činnostní role a uživatelé v JIP

Činnostní role, které byly danému OVM „definovány“ v rámci agendy, může lokální administrátor přidělit konkrétním osobám (přesněji jejich uživatelským účtům v JIP).

Přidělení činnostní role uživateli provádí lokální administrátor OVM v aplikaci Správa dat. Zobrazí si detail uživatelského účtu a přidělení činnostních rolí provede na záložce „Správa rolí“. Detailní postup je popsán v příručce pro lokálního administrátora [4] v samostatné kapitole.

#### **Kdy má smysl přiřazovat činnostní roli uživateli v JIP?**

Jedině v případě, že ji uživatel vysloveně potřebuje k práci v konkrétním AIS. Takový AIS musí především čerpat data ze základních registrů. AIS musí být dále integrován s JIP/KAAS, jinak se k této informaci v JIP nedostane. Příkladem AIS integrovaného s JIP/KAAS je např. právě AIS RPP Působnostní, proto je na začátku kapitoly 2 zmiňována nutnost nastavit činnostní roli.

Pokud tedy některý uživatel pracuje s lokálním informačním systémem v OVM (tj. bez jakékoliv vazby na JIP; např. spisová služba GINIS) a pro svoji práci potřebuje např. činnostní roli CR1509, nastavení této role ve Správě dat (tj. v JIP) nemá smysl. Roli je potřeba nastavit v daném lokálním informačním systému.

Nutnost nastavení činnostní role uživateli určitého AIS a specifikaci, o jakou (jaké) roli se jedná, by měl sdělit správce daného AIS např. v uživatelské dokumentaci. Zejména pokud se jedná o některý z centrálních AIS, ke kterým přistupuje více OVM.

**Poznámka:** Lokálním administrátorům subjektů typu OVM je automaticky přiřazována činnostní role, která je nezbytná pro oznámení působnosti v agendě. Pokud je role lokálnímu administrátorovi odebrána, je mu později automatickým procesem opět přidělena.

### 3.3. Přístupové role do AIS a uživatelé v JIP

Správce AIS, integrovaného s JIP/KAAS, může definovat tzv. přístupové role, pomocí nichž se definuje, které funkce AIS mohou uživatelé využívat.

Správce AIS přidělí přístupové role jednotlivým OVM – tím definuje množinu OVM, které mohou do AIS přistupovat. Seznam přístupových rolí přidělený danému OVM si může zobrazit lokální administrátor ve Správě dat na stránce s detailem subjektu (záložka „Správa rolí“). Postup přidělení přístupových rolí správcem AIS i postup zobrazení detailu subjektu lokálním administrátorem je popsán v příručce pro lokálního administrátora [4].

V rámci každého OVM pak lokální administrátor ve Správě dat přidělí přístupové role konkrétním uživatelům. Proveďte se to v detailu uživatelského účtu na záložce „Správa rolí“. Detailní postup je popsán v příručce pro lokálního administrátora [4] v samostatné kapitole.

#### **Kdy má smysl přiřazovat přístupovou roli uživateli v JIP?**

Jen v případě, že uživatel potřebuje pracovat v daném AIS a pro svoji práci potřebuje danou roli. Ba naopak, nastavení přístupové role uživateli, který nemá pracovat s daným AIS, by představovalo bezpečnostní riziko, protože by daný uživatel mohl neoprávněně vykonávat činnosti, k nimž nemá oprávnění.

Informace pro správné nastavení přístupových rolí uživatelům by měl dodat správce daného AIS např. v uživatelské dokumentaci.

**Poznámka:** Lokálním administrátorům subjektů typu OVM je automaticky přiřazována přístupová role pro přístup do AIS RPP Působnostní. Pokud je role lokálnímu administrátorovi odebrána, je mu později automatickým procesem opět přidělena.

## 4. Dostupné zdroje informací

- [1] Ministerstvo vnitra. *Metodika ohlášení agend a oznámení o vykonávání působností v agendě ve smyslu zákona č. 111/2009 Sb., o základních registrech*. 2017. 209 s. Dostupný z: <<http://www.szrcr.cz/file/51>>
- [2] Ministerstvo vnitra. *Metodika oznámení o vykonávání působností v agendě ve smyslu zákona č. 111/2009 Sb., o základních registrech*. 2012. 58 s. Dostupný z: <[http://www.szrcr.cz/uploads/download/RPP\\_spravce/Methodika\\_ozname\\_ni\\_pusobnosti.pdf](http://www.szrcr.cz/uploads/download/RPP_spravce/Methodika_ozname_ni_pusobnosti.pdf)>
- [3] Ministerstvo vnitra. *Příručka pro kraje a obce : Jak na základní registry?*. 2012. 66 s. Dostupný z: <<http://www.mvcr.cz/soubor/prirucka-pro-kraje-a-obce-jak-na-zakladni-registry-pdf.aspx>>
- [4] Ministerstvo vnitra. *Seznam orgánů veřejné moci : Příručka pro lokálního administrátora*. 2013. 58 s. Dostupný z: <[http://www.czechpoint.cz/data/prirucky/files/SOVM\\_lokalni\\_administrator.pdf](http://www.czechpoint.cz/data/prirucky/files/SOVM_lokalni_administrator.pdf)>