

## **Solution architektura – preambule**

### ***Context view***

Celkový kontextový pohled je popsán coby součást poskytnuté enterprise architektury a všechny v něm uvedené skutečnosti jsou v tomto dokumentu zohledněny.

Nejvýznamněji návrh a provoz řešení ovlivňují požadavky zákona o informačních systémech veřejné správy č. 365/2000 Sb. a zákona o kybernetické bezpečnosti č. 181/2014, ze kterých plyne náročnost atestací a budoucího provozu, zejména co se zajištění souvisejících *compliance* procesů týče.

V průběhu implementace bude vyžadována součinnost Zadavatele, spočívající zejména v doplnění a odsouhlasení solution architektury, vyřízení procesních požadavků registrace agendy a uživatelském testování. Předpokládaná časová náročnost je malých desítkách člověkodní.

V průběhu integrace a provádění atestací bude vyžadována součinnost Integrátora řešení a jednoho externího subjektu, vystupujícího v roli „Osoba oprávněná nahlížet“. Předpokládaná časová náročnost je malých desítkách člověkodní.

### ***Functional view***

Nabízené řešení pokrývá všechny služby a procesy, definované v enterprise architektuře.

Podrobněji jsou rozepsány v textu níže.

### ***Non-functional view***

Architektura řešení na aplikační vrstvě odpovídá tomu, že řešení bude postaveno v podobě Business Logiky nad GPC Frameworkem a provozováno nad GPC Platformou.

Řešení bude postaveno GPC Frameworkem, který vyvíjí Uchazeč a disponuje k němu veškerými právy užití. Součástí poskytnutého plnění budou licence na všechny potřebné funkcionality GPC Frameworku a zdrojové kódy aplikace, s licencí umožňující provoz v požadovaném rozsahu i budoucí úpravy, tak, jak je uvedeno v Tab. 44 přílohy 4a zadávací dokumentace, jejíž požadavky jsou tímto naplněny.

### ***Data view***

Zpracování dat probíhá s využitím funkcionalit GPC Frameworku pomocí temporální databáze.

Příslušné datové objekty jsou popsány níže.

Řešení bude vůči oprávněným třetím stranám figurovat v roli čtenářského AIS i zdrojového AIS. Toto bude zajištěno pomocí vrstvy interoperability GPC Frameworku, příslušné endpointy budou připojeny / zpřístupněny pomocí webových služeb, s autentizací a autorizací řešenou pomocí standardu SAML. Tímto budou řešeny požadavky dle Tab. 24 přílohy 4a zadávací dokumentace.

Podrobnosti jsou uvedeny v textu níže.

## ***Process view***

Procesní zpracování probíhá s využitím funkcionalit GPC Frameworku pomocí definovaných Workflow. Jednotlivé procesy jsou podrobněji popsány níže.

## ***Physical view***

Není z pohledu plánovaného způsobu nasazení a provozu relevantní.

## ***Deployment view***

Počítáme minimálně s níže uvedenými aplikačními komponentami:

- GPC UI WAAP / WAF zabezpečení, které bude tvořit logickou aplikační komponentu Frontend – Portál terapeutických programů dle požadované Enterprise architektury,
- GPC UI, které bude tvořit logickou aplikační komponentu Backend – aplikační logika terapeutických programů dle požadované Enterprise architektury,
- GPC Master společně s temporální databází, tvořící logickou aplikační komponentu. Backend – aplikační logika terapeutických programů v rozsahu ukládání strukturálních pasivních objektů a jim příslušných temporálních dat dle požadované Enterprise architektury a poskytování služeb interoperability pro napojení požadovaných systémů třetích stran.

Aplikační komponenty budou v případě potřeby rozšířeny o nativní aplikační komponenty GPC Platformy nebo aplikační komponenty třetích stran, a to podle požadavků a možností integrátora aplikace a vybraného poskytovatele eGovernment cloud infrastruktury. Tímto budou naplněny požadavky na úroveň služeb dle Tab. 14 zadávací dokumentace a na výkon při předpokládané zátěži podle Tab. 15 přílohy 4a zadávací dokumentace.

## ***Operational view***

Řešení pro svůj běh využívá GPC platformu, která je součástí poskytnutého plnění, která v sobě obsahuje nativní prostředky pro správu a kterou lze nasadit nad libovolným Docker řešením, případně nad jakoukoliv standardní IaaS službou. Plní tak požadavky zadání dle Tab. 41 přílohy 4a zadávací dokumentace.

## ***Security view***

Řešení bude jako přímý runtime využívat GPC platformu, která na úrovni middleware zajišťuje šifrování a transakční konzistenci. Dále v sobě zahrnuje bezpečnostní vrstvy:

- WAAP / WAF variantně na technologiích mod\_security+nginx, mod\_security+apache, případně jiný, dostupný v podobě služby u vybraného cloud poskytovatele,
- aplikační frontend v podobě GPC UI nad Java aplikačním serverem,
- databázový backend, využívající GPC temporální databázi.

WAAP plní i funkci reverzní proxy, potenciálně s funkcionalitou SSL offloading, ale standardně je směrem na aplikační frontend použito šifrované připojení pomocí protokolu HTTPS.

Z pohledu nastavení šifrování budou aplikována platná doporučení pro použité šifrovací a podepisovací algoritmy dle <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>. Certifikáty

obvykle dodává zákazník, případně provozovatel. Bude však možné použít i dynamicky generované certifikáty via ACME protokol.

Mezi aplikačním frontendem a databází je komunikace výhradně prostřednictvím databázového protokolu, který bude ve standardním nastavení šifrovaný.

GPC platforma interně využívá technologii Docker. Jsou podporovány a bude možné využít orchestrace typu Docker Swarm či Kubernetes, nicméně níže popsany návrh zabezpečení vychází z poskytnutého schématu Diagram technologické architektury dle přílohy P1a a Docker host je zde uveden v roli hypervizoru.

Plánovaný způsob nasazení, zajišťující ochranu před vnějšími kybernetickými útoky:

- Docker host s kontejnerizací nebude mít funkční rozhraní s přiřazenou IP adresou, která by byla přístupná z Internetu; naopak, bude dostupný pouze z prostřední „Administrativních nástrojů“ dle Diagramu technologické architektury.
- Kontejner s WAAP / WAF bude mít vypublikováno jedno síťové rozhraní do DMZ (pomocí Docker macvlan driveru) a druhé rozhraní do oddělené sítě, kde poběží (pouze) aplikační frontend.
- Pokud bude aplikační frontend provozován v kontejneru na stejném Docker hostu jako WAAP / WAF (což závisí na budoucím provozovateli systému), bude mezi nimi virtuální síťový adaptér (separátní Docker bridge).
- Obdobně bude postupováno při komunikaci mezi aplikačním frontendem a databázovým backendem.
- Alternativně bude možné jednu či všechny instance provozovat v oddělených sítích, potenciálně s vloženým firewallem, paketovým filtrem, access group připojenou na virtuální instanci apod. V těchto případech bude použita dedikovaná virtuální síť pro komunikaci mezi instancemi různého určení.
- V žádném podporovaném scénáři nebude existovat externě routovatelná síť se společným adresním prostorem mezi Docker hostem a WAAP / WAF, ani mezi WAAP / WAF a databázovým serverem. V rámci jednotlivých kontejnerů vždy poběží jen nezbytně nutné procesy použité aplikace (nad to explicitně poznamenejme, že se v případě kontejneru v žádném případě nejedná o plnohodnotný OS).

Konfigurace (image) daného kontejneru bude z pohledu diskových dat verzovaná, aktualizace budou probíhat atomicky a vždy se bude možné vrátit do výchozího stavu, případně konkrétního stavu v minulosti. Perzistentní data bude obsahovat jen kontejner s temporální databází. Tato data budou zabezpečena a bude k nim držena auditní stopa a transakční historie.

Logy z jednotlivých Docker kontejnerů i Docker hostů bude možné zasílat na jiné systémy (log managery) a tam je (dle vlastností použitého řešení třetí strany) v reálném čase ukládat a zpracovávat.

Díky výše uvedenému jsou plněny požadavky na zabezpečené zpracování dle Tab. 26 přílohy 4a zadávací dokumentace a aplikace bezpečnostních prvků dle Tab. 33 přílohy 4a zadávací dokumentace.

Veškeré změny, prováděné nad temporální databází jsou ze své podstaty logovány, při transakčním zpracování pomocí workflow existuje kompletní záznam o celém životním cyklu tiketu. Tyto informace jsou zaprvé ukládány interně, zadruhé mohou být v reálném čase zasílány na externí systém třetí strany. Tím budou zajištěny požadavky na nezávislé logování přístupů k osobním a citlivým údajům dle Tab. 26 přílohy 4a zadávací dokumentace.

Jak již bylo uvedeno, Zadavatel bude vystupovat v roli povinné osoby dle zákona č. 181/2014 o kybernetické bezpečnosti a souvisejících právních předpisů. Nabízené řešení aktuálně neobsahuje (nepoptávanou) podporu pro řízení procesní bezpečnosti, nicméně v případě zájmu Zadavatele bude budoucí rozšíření možné.

## Obsah

|                                                        |    |
|--------------------------------------------------------|----|
| Úvod.....                                              | 9  |
| Definice pojmů a zkratk.....                           | 9  |
| Definice požadavků.....                                | 11 |
| Vlastnosti požadovaného řešení.....                    | 11 |
| Návrh řešení.....                                      | 12 |
| Identifikace procesů a úkonů zahrnutých v systému..... | 12 |
| Datový model.....                                      | 13 |
| Datový záznam Osoba/Skupina.....                       | 13 |
| Datový záznam Účastník.....                            | 13 |
| Datový záznam Záznam o účasti na TP.....               | 14 |
| Datový záznam Platba.....                              | 14 |
| Datový záznam Lektor.....                              | 14 |
| Datový záznam Metodika.....                            | 15 |
| Popisy procesů.....                                    | 16 |
| Registr účastníků.....                                 | 16 |
| Registr lektorů.....                                   | 19 |
| Databáze terapeutických programů.....                  | 21 |
| Metodické vedení terapeutických programů.....          | 23 |
| Kontrola uskutečňování terapeutických programů.....    | 23 |
| Realizace nápravných opatření.....                     | 25 |
| Zajištění vzdělávání lektora.....                      | 26 |
| Párování plateb.....                                   | 27 |
| Informační procesy.....                                | 28 |
| Zvláštní úkony.....                                    | 31 |
| Automatické kontroly.....                              | 31 |
| Informační portál.....                                 | 32 |
| Poskytování informací.....                             | 32 |
| Propagace dat skrze veřejnou část webu CDV.....        | 33 |
| Napojení na registr evidence obyvatel.....             | 33 |
| Napojení na definované komunikační kanály.....         | 33 |
| Datové schránky (ISDS).....                            | 33 |
| ISSS/CMS.....                                          | 33 |
| Import příchozích plateb.....                          | 33 |
| Bezpečnost a připravenost k nasazení.....              | 34 |
| Bezpečnost.....                                        | 34 |
| Možné způsoby nasazení a provozování.....              | 34 |
| Provoz.....                                            | 35 |
| Standardní provoz a údržba IIP.....                    | 35 |
| Požadavky na infrastrukturu.....                       | 35 |
| Technické komponenty IIP.....                          | 35 |
| Logická architektura systému a způsob nasazení.....    | 36 |
| Požadavky na zdroje.....                               | 36 |
| Zálohování a obnova po havárii.....                    | 36 |
| Monitorování.....                                      | 37 |
| Logování.....                                          | 37 |
| Testování.....                                         | 37 |
| Exit strategie.....                                    | 37 |

## Tabulka obrázků

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Obrázek 1: Proces registrace účastníka dobrovolná.....                   | 16 |
| Obrázek 2: Proces podání žádosti o prominutí úhrady služeb.....          | 17 |
| Obrázek 3: Proces rozhodnutí o prominutí úhrady služeb.....              | 17 |
| Obrázek 4: Proces přihlášení lektora do kurzu průběžného vzdělávání..... | 18 |
| Obrázek 5: Proces pozastavení akreditace.....                            | 19 |
| Obrázek 6: Proces udělení certifikátu o absolvování.....                 | 21 |
| Obrázek 7: Vytvoření a zveřejnění metodiky.....                          | 22 |
| Obrázek 8: Proces kontroly uskutečňování terapeutických programů.....    | 23 |
| Obrázek 9: Proces <i>přezkoumání</i> stížností.....                      | 24 |
| Obrázek 10: Proces <i>opatření ke zjednání nápravy</i> .....             | 24 |
| Obrázek 11: Proces párování plateb.....                                  | 26 |
| Obrázek 12: Proces informování o kurzu.....                              | 27 |
| Obrázek 13: Poskytnutí údajů úřadům.....                                 | 27 |
| Obrázek 14: Proces poskytnutí údajů účastníkovi.....                     | 28 |
| Obrázek 15: Proces poskytnutí údajů <i>lektorovi</i> .....               | 28 |

## Seznam tabulek

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Tabulka 1: Pojmy a zkratky.....                                                      | 8  |
| Tabulka 2: Parametry datového záznamu Osoba/Skupina.....                             | 12 |
| Tabulka 3: Parametry datového záznamu Účastník.....                                  | 12 |
| Tabulka 4: Parametry datového záznamu Záznam o účasti na TP.....                     | 13 |
| Tabulka 5: Parametry datového záznamu <i>Platba</i> .....                            | 13 |
| Tabulka 6: Parametry datového záznamu <i>Lektor</i> .....                            | 13 |
| Tabulka 7: Parametry datového záznamu <i>Metodika</i> .....                          | 14 |
| Tabulka 8: Parametry procesu registrace účastníka dobrovolné.....                    | 16 |
| Tabulka 9: Parametry procesu přihlášení se k terapeutickému programu.....            | 16 |
| Tabulka 10: Parametry procesu podání žádosti o prominutí úhrady služeb.....          | 17 |
| Tabulka 11: Parametry procesu rozhodnutí o prominutí úhrady služeb.....              | 17 |
| Tabulka 12: Parametry procesu úhrady správního poplatku za terapeutický program..... | 18 |
| Tabulka 13: Parametry registrace.....                                                | 19 |
| Tabulka 14: Parametry žádosti o akreditaci lektora.....                              | 19 |
| Tabulka 15: Parametry procesu úhrady poplatku za akreditaci.....                     | 19 |
| Tabulka 16: Parametry procesu rozhodnutí o akreditaci.....                           | 19 |
| Tabulka 17: Parametry přihlášení lektora do kvalifikačního kurzu.....                | 20 |
| Tabulka 18: Parametry přihlášení lektora do kurzu průběžného vzdělávání.....         | 20 |
| Tabulka 19: Parametry pozastavení akreditace lektora.....                            | 20 |
| Tabulka 20: Parametry procesu realizace terapeutického programu.....                 | 21 |
| Tabulka 21: Parametry bloku/sezení terapeutického programu.....                      | 21 |
| Tabulka 22: Parametry procesu udělení certifikátu o absolvování.....                 | 22 |
| Tabulka 23: Parametry procesu kontroly na základě podnětu.....                       | 23 |
| Tabulka 24: Parametry procesu přezkoumání stížností.....                             | 24 |
| Tabulka 25: Parametry procesu uložení opatření ke zjednání nápravy.....              | 25 |
| Tabulka 26: Parametry odebrání akreditace lektora.....                               | 25 |
| Tabulka 27: Parametry procesu kurzu průběžného vzdělávání lektorů.....               | 25 |
| Tabulka 28: Parametry bloku kurzu průběžného vzdělávání lektorů.....                 | 26 |
| Tabulka 29: Parametry procesu párování plateb.....                                   | 26 |
| Tabulka 30: Parametry procesu informování o kurzu.....                               | 27 |
| Tabulka 31: Parametry procesu poskytnutí údajů úřadům.....                           | 28 |
| Tabulka 32: Parametry procesu poskytnutí údajů účastníkovi.....                      | 28 |
| Tabulka 33: Parametry procesu poskytnutí údajů lektorovi.....                        | 29 |

# Úvod

Zadávací dokumentace pro vývoj Informačního internetového portálu pro zajištění organizace terapeutických programů dle §102a až §102e zákona č.361/2000Sb. ve znění účinném od 1. července 2023.

## Definice pojmů a zkratk

Tabulka 1: Pojmy a zkratky

| Pojem/Zkratka | Znění                                                     |
|---------------|-----------------------------------------------------------|
| AIFO          | Agendový Identifikátor Fyzické Osoby                      |
| AIS           | Agendové Informační Systémy                               |
| AISP          | Agendový Informační Systém Působnostní                    |
| AIS RPP       | Agendový Informační Systém Registru Práv a Povinností     |
| AMVS          | Agendový Model Veřejné Správy                             |
| CA            | Certifikační Autorita                                     |
| CMS           | Centrální Místo Služeb                                    |
| Czech POINT   | Český Podací Ověřovací Informační Národní Terminál        |
| eGC           | eGovernment Cloud                                         |
| eGSB          | eGovernment On-Line Service Bus/eGon Service Bus          |
| FAIS          | Formulářový Agendový Informační Systém                    |
| IaaS          | Infrastructure as a Service                               |
| ICT           | Information and Communication Technologies                |
| ICT VS ČR     | ICT Veřejné Správy ČR                                     |
| ID-DS         | IDentifikátor Datové Schránky                             |
| IKČR          | Informační Koncepce ČR                                    |
| ISDS          | Informační Systém Datových Schránek                       |
| ISEO          | Informační Systém Evidence Obyvatel                       |
| ISSS          | Informační Systém Sdílené Služby                          |
| ISVS          | Informační Systém Veřejné Správy                          |
| ISZR          | Informační Systém Základních Registrů                     |
| JIP           | Jednotný Identitní Prostor                                |
| KAAS          | Katalog Autorizačních a Autentizačních Služeb             |
| KIVS          | Komunikační Infrastruktura Veřejné Správy                 |
| MOOL          | portál územní samosprávy Města a Obce OnLine              |
| MŘICT         | Metody Řízení ICT VS ČR                                   |
| NAKIT         | Národní Agentura pro Komunikační a Informační Technologie |
| NAP           | Národní Architektonický Plán                              |
| NAR           | Národní Architektonický Rámec                             |
| NDC           | Národní Datové Centrum                                    |
| NIA           | Národní Identitní Agentura                                |
| OHA           | Odbor Hlavního Architekta eGovernmentu                    |
| ORP           | Obec s Rozšířenou Působností                              |
| OVM           | Orgán Veřejné Moci                                        |
| PaaS          | Platform as a Service                                     |
| PPDF          | ProPojený Datový Fond                                     |
| PVS           | Portál Veřejné Správy                                     |
| RAZR          | Registrační Autorita Základních Registrů                  |
| RISVS         | Rejstřík ISVS                                             |
| ROB           | Registr Obyvatel                                          |
| ROS           | Registr OSob                                              |

|         |                                                                |
|---------|----------------------------------------------------------------|
| ROVM    | Rejstřík OVM                                                   |
| RPP     | Registr Práv a Povinností                                      |
| RÚIAN   | Registr Územní Identifikace, Adres a Nemovitostí               |
| SDM SZR | Service Desk Manager Správy Základních Registrů (aplikace)     |
| SPAIS   | SpoluPublikující Agendový Informační Systém                    |
| SPUÚ    | SoukromoPrávní Uživatel Údajů                                  |
| SSVÚ    | Soukromoprávní Systém pro Využívání Údajů                      |
| SZR     | Správa Základních Registrů                                     |
| TSÚA    | Technická Struktura Údajů Agendy                               |
| ÚEP     | Úplné Elektronické Podání                                      |
| ÚSÚ     | Ústřední Správní Úřady                                         |
| VDF     | Veřejný Datový Fond                                            |
| ZFO     | přípona souboru zfo                                            |
| ZIFO    | Zdrojový Identifikátor Fyzické Osoby                           |
| ZoISVS  | zákon č. 365/2000 Sb., o informačních systémech veřejné správy |
| ZOZ     | Zvláštní Odborná Způsobilost                                   |
| ZR      | Základní Registry                                              |

# Definice požadavků

## Vlastnosti požadovaného řešení

Požadované řešení má naplnit požadavky na internetový informační portál podle § 102d zákona 361/2000 Sb. tak, aby vhodným způsobem sloužil k podpoře organizace terapeutických programů (dle požadavků v §102a až §102e zákona 361/2000 Sb.) a minimalizoval administrativní zátěž na pracovníky Metodického centra.

Plní požadavky Národního architektonického plánu – Architektury eGovernmentu ČR (NAP) a minimální bezpečnostní standard dle NÚKIB (MBS).

Využívá design dle <https://designsystem.gov.cz/> a to včetně responzivního designu a možnosti přístupu z běžných mobilních a počítačových platforem.

Důležitým prvkem je pohled občana, který tento systém bude využívat v roli Uživatel, tedy frekventanta terapeutického kurzu.

V rámci digitalizace státní správy je také potřeba v maximální míře podporovat možnost provádění úkonů elektronicky s využitím standardních prostředků identifikace a autentizace NIA. Proto budou všechny úkony podporovány pouze elektronicky s výjimkou samotných sezení terapeutických programů.

Řešení musí být navrženo dostatečně flexibilně tak, aby bylo možno provádět úpravy funkčnosti dle případných budoucích změn legislativy a případných prováděcích předpisů.

# Návrh řešení

## Identifikace procesů a úkonů zahrnutých v systému

Pro implementaci v systému byly identifikovány tyto procesy a úkony:

- registr účastníků
  - přihlášení účastníka
  - vygenerování platby (platební údaje, QR kód)
  - žádost o odpuštění poplatku
    - žádost
    - schválení/zamítnutí
  - zápis do konkrétního programu
  - vygenerování certifikátu po ukončení kurzu
- seznam lektorů
  - akreditace lektora
    - žádost
    - vygenerování platby (platební údaje, QR kód)
    - schválení/zamítnutí
    - po připsání platby poskytnutí přístupu do systému
  - reakreditace lektora
  - pozastavení akreditace
    - žádost
    - schválení/zamítnutí
- databáze terapeutických programů
  - vytvoření nového kurzu lektorem
    - možnost uložení rozpracovaného konceptu
    - zveřejnění
  - provádění kurzu
    - zápis docházky
    - úpravy termínů
- informační portál
  - zahrnující jak přihlašování do programů, tak povinné poskytování údajů dle §102d, odst.6 zákona 361/2000 Sb.
- záznamy o kontrolách programů
- záznamy o uložených nápravných opatřeních
- evidence vydaných metodik
- kvalifikační kurzy lektorů
- kurzy průběžného vzdělávání lektorů
- stížnosti
  - na kurz/lektora/platbu/jiné
- informační procesy
  - informování o kurzu
  - poskytnutí údajů účastníkovi v rozsahu údajů o něm vedených
  - poskytnutí údajů lektorovi v rozsahu údajů o něm vedených
  - poskytnutí údajů silničním správním úřadům, orgánům územních samosprávních celků, orgánům činným v trestním řízení a Probační a mediační službě
- zvláštní úkony
  - vytváření účtů a přidělování práv pro privilegované účty (Administrátor IIP, „Metodické centrum – úřední osoba“ a „Osoba oprávněná nahlížet“)
- zveřejňování souhrnných statistických dat o terapeutických programech
  - dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím a dle pokynů a dobré praxe popsané na portále otevřených dat <https://data.gov.cz>

Dále bude potřeba pokrýt:

- napojení na registr evidence obyvatel
- napojení na definované komunikační kanály (datové schránky, ISSS)

- import souborů pro párování plateb/bankovní API

V systému budou následující role:

- Účastník
- Lektor
- Metodické centrum – úřední osoba
- Metodické centrum
- Osoba oprávněná nahližet – nebude se přihlašovat do systému, bude využívat sdílené služby ISSS
- Administrátor IIP

## Datový model

Každý datový záznam v GPC frameworku má parametry jméno a id, tyto parametry jsou systémové a nelze je odebrat. Proto se také v grafu datového modelu neuvádí.

### Datový záznam Osoba/Skupina

Jedná se o nativní datový záznam GPC frameworku umožňující pro danou osobu nebo skupinu definovat základní údaje typu jména, role a přihlašovací údaje do aplikace. Obsahuje i další údaje (adresa trvalého pobytu, adresa doručovací, email), které jsou společné pro lektora i účastníka.

Tabulka 2: Parametry datového záznamu Osoba/Skupina

| Parametr          | Popis                                   |
|-------------------|-----------------------------------------|
| Jméno             | text                                    |
| Příjmení          | text                                    |
| Login             | přihlašovací jméno (text)               |
| Role              | role přiřazená dané osobě/skupině (LOV) |
| Adresa pobytu     | text                                    |
| Doručovací adresa | (nepovinný údaj)                        |
| E-mailová adresa  | (nepovinný údaj)                        |
| AIFO              | string                                  |

### Datový záznam Účastník

Tento datový záznam je určen pro uložení informací o účastníkovi. Nebude obsahovat údaje o účtu (ty budou v záznamu typu Osoba) ani o účasti v terapeutickém programu (tyto informace budou v záznamu typu Záznam o účasti na TP, aby byla možná opakovaná účast i v době do 5 let, kdy se záznam zachovává).

Tabulka 3: Parametry datového záznamu Účastník

| Parametr                              | Popis                               |
|---------------------------------------|-------------------------------------|
| Adresa pobytu                         | text                                |
| Datum narození                        | datum                               |
| Číslo OP/pasu                         |                                     |
| Stav registrace                       | LOV (registrován/neregistrován)     |
| Souhlas s obchodními podmínkami       | LOV (souhlas potvrzen, neznám)      |
| Souhlas se zpracováním osobních údajů | LOV (souhlas potvrzen, neznám)      |
| Datum expirace záznamu                | po datu expirace bude záznam smazán |

## Datový záznam Záznam o účasti na TP

Tento datový záznam obsahuje informace o účasti na terapeutickém programu a byl oddělen ze záznamu Účastník, aby byla možná opakovaná účast na terapeutickém programu v průběhu doby, kdy má Metodické centrum povinnost držet záznam o předchozí účasti.

Tabulka 4: Parametry datového záznamu Záznam o účasti na TP

| Parametr       | Popis                                                       |
|----------------|-------------------------------------------------------------|
| Datum žádosti  | datum                                                       |
| Důvod účasti   | text                                                        |
| Stav účasti    | LOV (nezapsán, probíhá, ukončen neúspěšně, ukončen úspěšně) |
| Stav platby    | LOV (vytvořena, zaplacená, žádost o prominutí, prominuta)   |
| Datum ukončení | datum, kdy byl kurz ukončen                                 |

## Datový záznam Platba

Tento datový záznam obsahuje informace o platbě, která byl předepsána Metodickým centrem.

Tabulka 5: Parametry datového záznamu Platba

| Parametr          | Popis                                                                     |
|-------------------|---------------------------------------------------------------------------|
| Vytvořeno         | datum a čas vytvoření                                                     |
| Účet              | účet na který má být zaplacen                                             |
| Variabilní symbol | VS platby (potřebný ke spárování)                                         |
| Částka            | částka předepsaná k zaplacení                                             |
| Splatnost         | datum splatnosti                                                          |
| Zaplaceno         | datum, kdy byla platba připsána na účet Metodického centra nebo prominuta |
| Stav platby       | LOV (vytvořena, zaplacená, úhrada prominuta)                              |

## Datový záznam Lektor

Tento datový záznam je určen pro uchování informací, které je potřeba v souvislosti s osobou lektora.

Tabulka 6: Parametry datového záznamu Lektor

| Parametr                                | Popis                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Datum narození                          | datum                                                                                                           |
| E-mailová adresa                        | (nepovinný údaj)                                                                                                |
| Stav akreditace                         |                                                                                                                 |
| Platnost akreditace                     | datum, kdy platnost současné akreditace končí. Prodlužuje se po absolvování kurzu průběžného vzdělávání lektorů |
| Datum absolvování průběžného vzdělávání | datum posledního úspěšného ukončení kurzu průběžného vzdělávání lektorů                                         |
| Přílohy                                 | pro přílohy dle potřeby (např. dokumenty dokladující vzdělání a praxi)                                          |
| Datum expirace záznamu                  | po datu expirace bude záznam smazán, datum se nastavuje při ukončení spolupráce s lektorem                      |

## Datový záznam Metodika

Tento datový záznam obsahuje informace o metodice, její platnosti, návaznosti na nahrazované a nahrazující metodiky a samozřejmě metodiku samotnou.

Tabulka 7: Parametry datového záznamu Metodika

| Parametr                | Popis                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------|
| Datum zveřejnění        | datum a čas vytvoření                                                                    |
| Datum začátku platnosti |                                                                                          |
| Datum konce platnosti   |                                                                                          |
| Stav                    | LOV (v přípravě, schválena, zveřejněna, platná, neplatná)                                |
| Nahrazovaná metodika    | link na datový záznam typu Metodika, pokud tato metodika nahrazuje nějakou předchozí     |
| Metodika nahrazující    | link na datový záznam typu Metodika, pokud je tato metodika nahrazena nějakou navazující |
| Přílohy                 | zde je možno přiložit dokument s danou metodikou, případně další doprovodné dokumenty    |

## Popisy procesů

### Registr účastníků

Z důvodu možné opakované účasti v terapeutickém programu byla data uložená o účastníkovi rozdělena na dva záznamy. Záznam „Účastník“ s informacemi týkajícími se osoby a záznam „Záznam o účasti na TP“ s údaji týkajícími se konkrétní účasti na terapeutickém programu. Zvláště pak jsou informace použité v žádosti o prominutí úhrady – žádost je čistě procesní, data specifická pro danou žádost jsou tedy součástí workflow/tiketu žádosti o prominutí.

Registr účastníků umožňuje registraci účastníka do systému, přihlášení se k terapeutickému programu, podání žádosti o prominutí úhrady služeb a obsahuje také procesy rozhodnutí o prominutí úhrady, uhrazení správního poplatku.

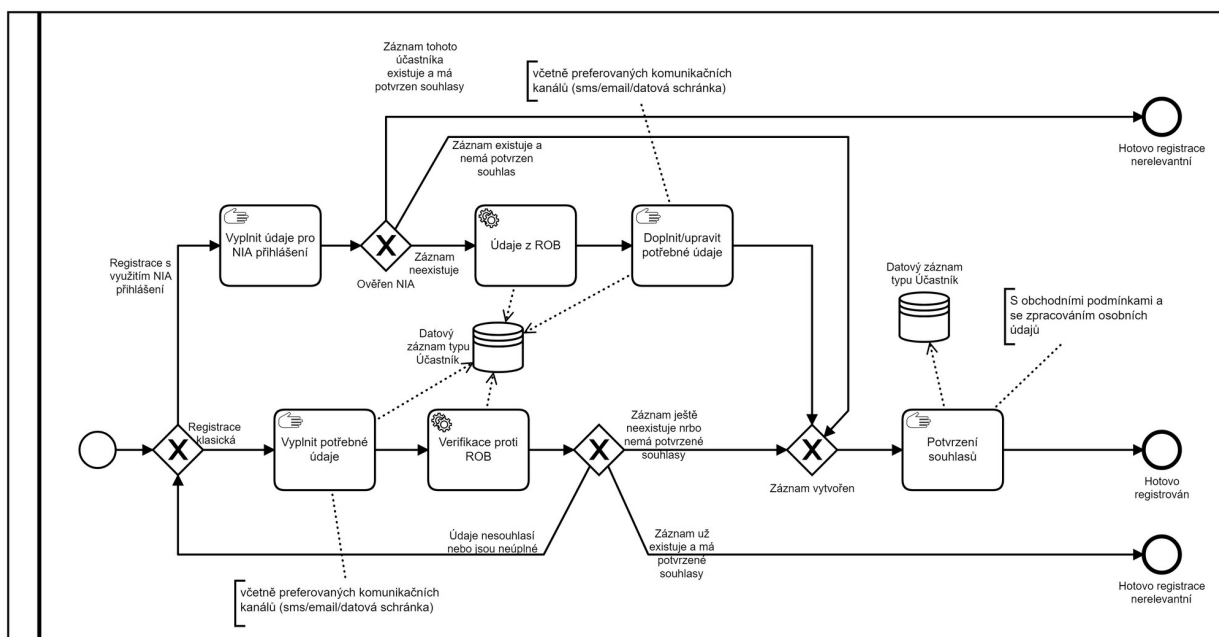
Při registraci účastníka je vytvořen účet účastníka, jeho datový záznam a informace o účastníkovi jsou ověřeny pomocí informací z registru obyvatel (ROB). Zároveň účastník dává souhlas se zpracováním osobních údajů a s obchodními podmínkami.

Při přihlášení se účastníka k terapeutickému programu si účastník vybere terapeutický program a jsou mu vygenerovány údaje pro úhradu poplatku za terapeutický program. Platba je navázána na účast na programu a ne na účastníka z důvodu možné opakované účasti, jak je popsáno výše. Po zaplacení je příjem v bance spárován s platbou a platba je označena za zaplacenou. Alternativně může účastník požádat o odpuštění úhrady a v případě kladného rozhodnutí je platba označena za uhrazenou na základě tohoto rozhodnutí. Přihlášenému účastníkovi uhrazenou platbou je potvrzena účast.

Účastník může požádat o prominutí úhrady prostřednictvím portálu, kde přiloží dokumenty prokazující splnění zákonných požadavků pro odpuštění úhrady. O odpuštění úhrady rozhoduje uživatel systému v roli „Metodické centrum – úřední osoba“. V případě nedostatečné dokumentace může vrátit účastníkovi k doplnění.

Funkcionalita registru účastníků odpovídá službě EA „Přihlášení se k terapeutickému programu“ a bude realizována procesy:

- registrace účastníka dobrovolná
- přihlášení se k terapeutickému
- podání žádosti o prominutí úhrady služeb
- rozhodnutí o prominutí úhrady služeb
- úhrada správního poplatku za terapeutický program



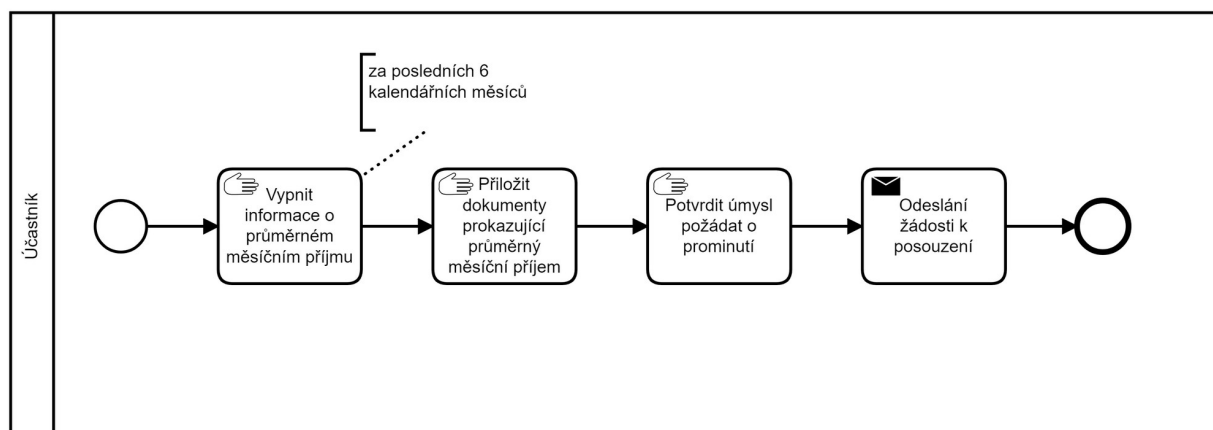
Obrázek 1: Proces registrace účastníka dobrovolná

Tabulka 8: Parametry procesu registrace účastníka dobrovolné

| Parametr          | Popis                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------|
| Jméno             | uloženo v datovém záznamu „Osoba“                                                         |
| Další jména       | uloženo v datovém záznamu „Osoba“                                                         |
| Příjmení          | uloženo v datovém záznamu „Osoba“                                                         |
| Adresa pobytu     | uloženo v datovém záznamu „Osoba“                                                         |
| Datum narození    | uloženo v datovém záznamu „Účastník“                                                      |
| Důvod účasti      | Důvod účasti na terapeutickém programu, uloženo v datovém záznamu „Záznam o účasti na TP“ |
| Doručovací adresa | (nepovinný údaj) uloženo v datovém záznamu „Osoba“                                        |
| Mailová adresa    | (nepovinný údaj) uloženo v datovém záznamu „Osoba“                                        |
| Číslo OP/pasu     | uloženo v datovém záznamu „Účastník“                                                      |

Tabulka 9: Parametry procesu přihlášení se k terapeutickému programu

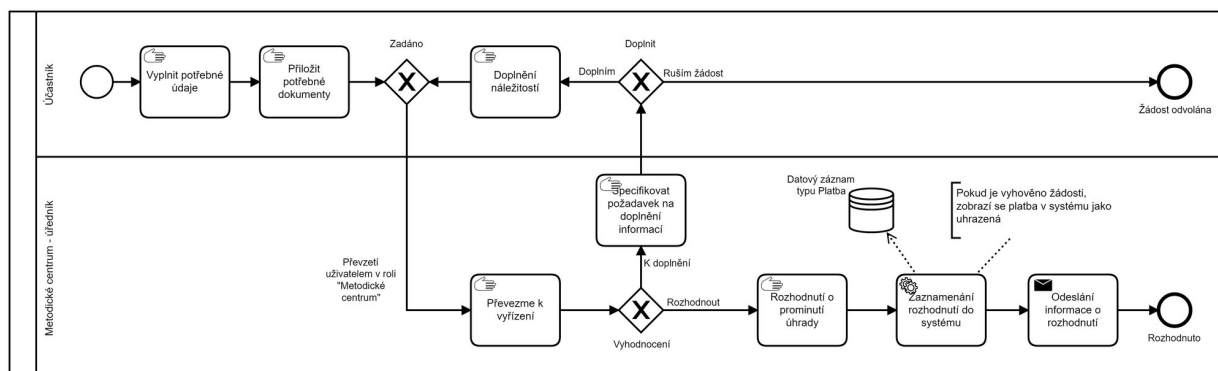
| Parametr                    | Popis                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------|
| Vybraný program             | link na workflow/tiket „Terapeutický program“                                       |
| Záznam o účasti na programu | link na datový záznam „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“) |
| Žádost o prominutí          | link na workflow/tiket „Rozhodnutí o prominutí úhrady“ (pokud je požádáno)          |
| Platba                      | link na datový záznam „Payment“                                                     |



Obrázek 2: Proces podání žádosti o prominutí úhrady služeb

Tabulka 10: Parametry procesu podání žádosti o prominutí úhrady služeb

| Parametr        | Popis |
|-----------------|-------|
| Průměrný příjem | číslo |
| Přílohy         |       |



Obrázek 3: Proces rozhodnutí o prominutí úhrady služeb

Tabulka 11: Parametry procesu rozhodnutí o prominutí úhrady služeb

| Parametr                    | Popis                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Záznam o účasti na programu | link na datový záznam „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“)                                      |
| Přílohy                     | přiložené soubory prokazující skutečnosti požadované §102b, odst. 3 zákona č. 361/2000Sb. ve znění platném od 1. 7. 2023 |
| Poznámky k žádosti          | případné poznámky žadatele (nepovinný údaj)                                                                              |
| Poznámky k rozhodnutí       | (nepovinný údaj)                                                                                                         |
| Výsledek rozhodnutí         | LOV (schváleno/zamítnuto)                                                                                                |

Tabulka 12: Parametry procesu úhrady správního poplatku za terapeutický program

| Parametr                    | Popis                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------|
| Záznam o účasti na programu | link na datový záznam „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“) |
| Seznam nespárovaných plateb | buď jako csv nebo importovaný via bankovní API                                      |

## Registr lektorů

Registr lektorů zahrnuje registraci lektora do systému, akreditační proces, proces úhrady poplatku za akreditaci, proces úhrady za akreditaci, proces rozhodnutí o akreditaci, přihlášení do kvalifikačního kurzu, přihlášení do kurzu průběžného vzdělávání a pozastavení akreditace.

Při registraci lektora jsou jeho údaje verifikovány vůči registru obyvatel, je vytvořen jeho účet v systému a potvrdí souhlas se zpracováním osobních údajů a s obchodními podmínkami (jestli bude požadováno). Dostane přihlašovací údaje do systému a je mu umožněno požádat o akreditaci.

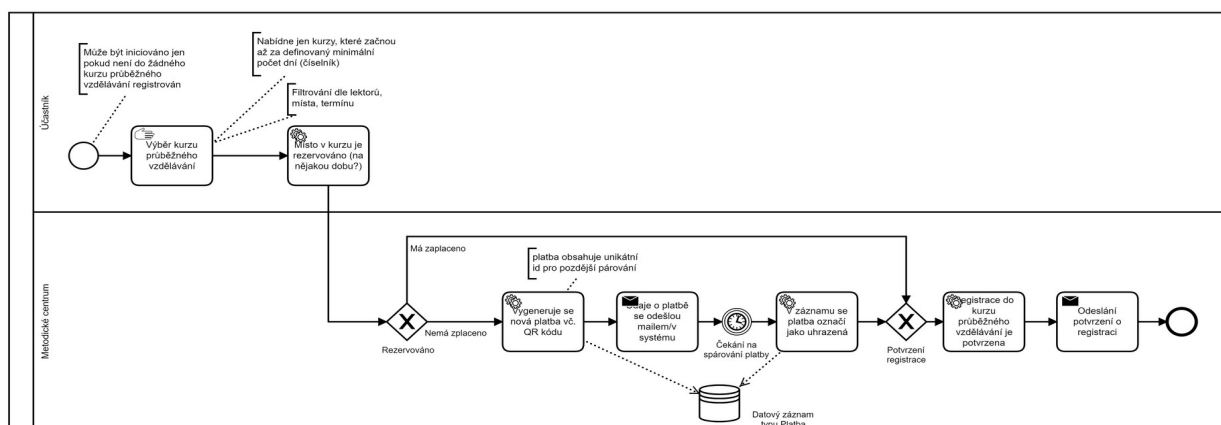
Následně lektor požádá o akreditaci, doloží všechny požadované skutečnosti. V případě splnění všech požadavků mu jsou vygenerovány platební údaje k úhradě poplatku za akreditaci. Po spárování platby lektor potvrdí seznámení se s platnými metodikami. Následně je vyrozuměn o úspěšné akreditaci a je mu v systému umožněno vypisovat terapeutické programy.

Za účelem splnění kvalifikačních požadavků se lektor může přihlásit do kvalifikačního kurzu pořádaného Metodickým centrem a zakončeného zkouškou. Podrobnosti budou specifikovány prováděcím předpisem, který není v době přípravy tohoto dokumentu znám, takže popis tohoto procesu bude vytvořen později v průběhu přípravy projektu.

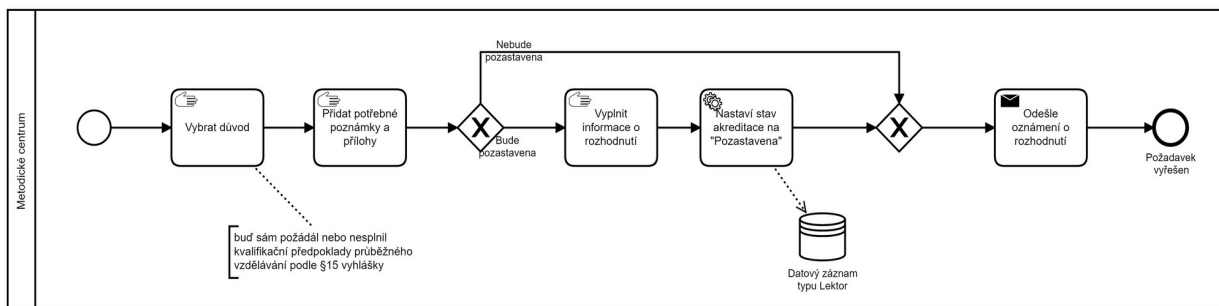
Proces pozastavení akreditace je zmíněn v Enterprise architektuře, není ale definován zákonem. Pokud bude definován prováděcím předpisem, bude se zřejmě níže popsany proces modifikovat, jinak bude potřeba se domluvit se zadavatelem jak přesně má vypadat.

Funkcionalita registru lektorů odpovídá službě EA „Řízení lektorů“ a bude realizována procesy:

- žádost o akreditaci
- úhrada poplatku za akreditaci
- rozhodnutí o akreditaci
- zajištění vzdělávání lektora
  - kvalifikační kurzy lektorů
    - přihlášení lektora do kvalifikačního kurzu
  - průběžné vzdělávání lektorů
    - přihlášení lektora do kurzu průběžného vzdělávání
- pozastavení akreditace



Obrázek 4: Proces přihlášení lektora do kurzu průběžného vzdělávání



Obrázek 5: Proces pozastavení akreditace

Tabulka 13: Parametry registrace

| Parametr          | Popis                                |
|-------------------|--------------------------------------|
| Jméno             | uloženo v datovém záznamu „Lecturer“ |
| Další jména       | uloženo v datovém záznamu „Lecturer“ |
| Příjmení          | uloženo v datovém záznamu „Lecturer“ |
| Adresa pobytu     | uloženo v datovém záznamu „Lecturer“ |
| Datum narození    | uloženo v datovém záznamu „Lecturer“ |
| Doručovací adresa | (nepovinný údaj)                     |
| Mailová adresa    |                                      |
| Telefonní číslo   |                                      |
| Stav akreditace   | LOV (akreditován/neakreditován)      |

Tabulka 14: Parametry žádosti o akreditaci lektora

| Parametr          | Popis                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------|
| Lektor            | link na datový záznam „Lecturer“                                                            |
| Přílohy           | pro doklady potvrzující kvalifikaci lektora                                                 |
| Kvalifikační kurz | link na workflow/tiket kvalifikačního kurzu lektorů, který lektor absolvuje nebo absolvoval |
| Platba            | link na datový záznam „Payment“                                                             |
| Rozhodnutí        | položka, kam se zaznamená rozhodnutí o akreditaci                                           |

Tabulka 15: Parametry procesu úhrady poplatku za akreditaci

| Parametr | Popis                            |
|----------|----------------------------------|
| Lektor   | link na datový záznam „Lecturer“ |
| Platba   | link na datový záznam „Payment“  |

Tabulka 16: Parametry procesu rozhodnutí o akreditaci

| Parametr            | Popis                                             |
|---------------------|---------------------------------------------------|
| Lektor              | link na datový záznam „Lecturer“                  |
| Žádost o akreditaci | link na nadřazený proces/workflow                 |
| Rozhodnutí          | položka, kam se zaznamená rozhodnutí o akreditaci |

Tabulka 17: Parametry přihlášení lektora do kvalifikačního kurzu

| Parametr          | Popis                                                                       |
|-------------------|-----------------------------------------------------------------------------|
| Lektor            | link na datový záznam „Lecturer“                                            |
| Kvalifikační kurz | link na workflow/tiket kvalifikačního kurzu lektorů, který si lektor zvolil |
| Platba            | link na datový záznam „Payment“                                             |

Tabulka 18: Parametry přihlášení lektora do kurzu průběžného vzdělávání

| Parametr                   | Popis                                                                              |
|----------------------------|------------------------------------------------------------------------------------|
| Lektor                     | link na datový záznam „Lecturer“                                                   |
| Kurz průběžného vzdělávání | link na workflow/tiket kurzu průběžného vzdělávání lektorů, který si lektor zvolil |
| Platba                     | link na datový záznam „Payment“                                                    |

Tabulka 19: Parametry pozastavení akreditace lektora

| Parametr   | Popis                                                |
|------------|------------------------------------------------------|
| Lektor     | link na datový záznam „Lecturer“                     |
| Úkon       | LOV (pozastavení, odebrání)                          |
| Důvod      | text                                                 |
| Přílohy    | (nepovinná položka) dokumenty přiložené k rozhodnutí |
| Rozhodnutí | LOV (zamítnuto, akreditace pozastavena)              |

## Databáze terapeutických programů

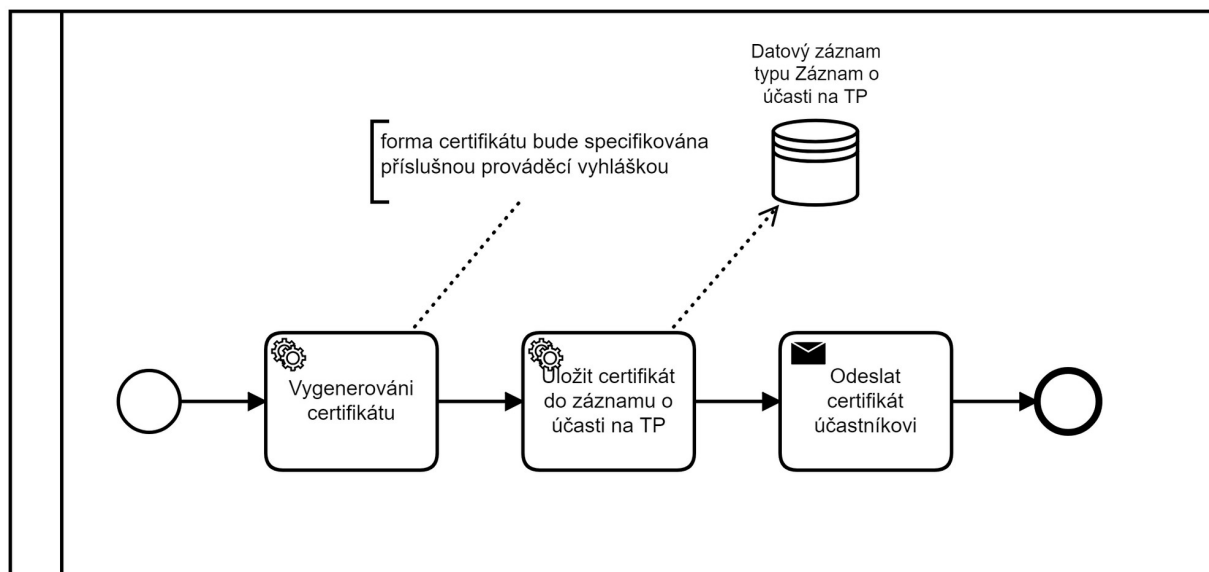
Databáze terapeutických programů umožňuje vytvoření a realizaci terapeutických programů, obsahuje proces popisující jednotlivé bloky terapeutického programu, proces udělení certifikátu o absolvování terapeutického programu a proces, který umožňuje sloučit terapeutické programy třeba pro případ, že počet studentů ve dvou programech jednoho lektora nepřiměřeně poklesne.

Terapeutický program je vypsán akreditovaným lektorem, který vyplní termín konání programu, termíny a místa konání jednotlivých sezení. Po provedení jednotlivých sezení vyplňuje účasti jednotlivých účastníků.

Po úspěšném absolvování terapeutického programu je účastníkům vygenerován certifikát, podrobnosti teprve upřesní prováděcí předpis.

Funkcionalita databáze terapeutických programů odpovídá službě EA „Realizace terapeutického programu“ a bude realizována procesy:

- realizace terapeutického programu
- udělení certifikátu o absolvování
- informování o kurzu (ten je popsán v kapitole Informační procesy)



Obrázek 6: Proces udělení certifikátu o absolvování

Tabulka 20: Parametry procesu realizace terapeutického programu

| Parametr                       | Popis                                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Lektor                         | vedoucí lektor programu, link na datový záznam „Lecturer“                                                               |
| Bloky terapeutického programu  | linky na workflow/tikety jednotlivých bloků terapeutických programů (zde budou uloženy data a časy konání těchto bloků) |
| Náhradní bloky                 | linky na náhradní bloky pro účastníky s jednou absencí (pokud se nebude brát začátek prvního bloku a konec posledního)  |
| Datum začátku a konce programu |                                                                                                                         |
| Místo konání programu          |                                                                                                                         |
| Účastníci programu             | linky na datové záznamy typu „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“)                              |
| Přílohy                        | pro vložení rozvrhu témat jednotlivých bloků, popřípadě nějakých školících materiálů                                    |

Tabulka 21: Parametry bloku/sezení terapeutického programu

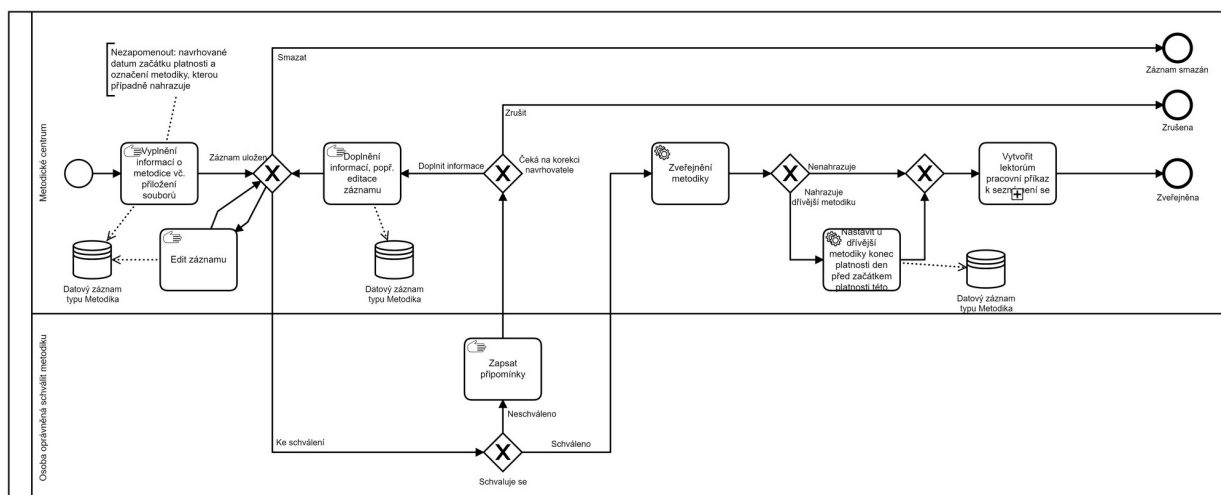
| Parametr             | Popis                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------|
| Terapeutický program | link na workflow/tiket terapeutického programu                                                                      |
| Datum konání         |                                                                                                                     |
| Čas začátku          |                                                                                                                     |
| Čas konce            |                                                                                                                     |
| Místo konání         | (nepovinný údaj – použije se pokud je odlišné od místa konání uvedeného pro celý terapeutický program)              |
| Účastníci programu   | linky na datové záznamy typu „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“)                          |
| Záznamy o účasti     | pro každého účastníka, obsahuje jestli se zúčastnil, omluvenky (včetně příloh), potvrzení aktivní účasti a poznámku |
| Přílohy              | pro vložení školících materiálů                                                                                     |

Tabulka 22: Parametry procesu udělení certifikátu o absolvování

| Parametr                    | Popis                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------|
| Záznam o účasti na programu | link na datový záznam „Záznam o účasti na TP“ (ten je navázán na záznam „Účastník“) |

## Metodické vedení terapeutických programů

Metodické vedení terapeutických programů umožňuje vytvoření metodiky včetně nastavení její platnosti a návaznosti na předchozí a následně i na navazující metodiku. Obsahuje i schválení metodiky pověřeným pracovníkem.

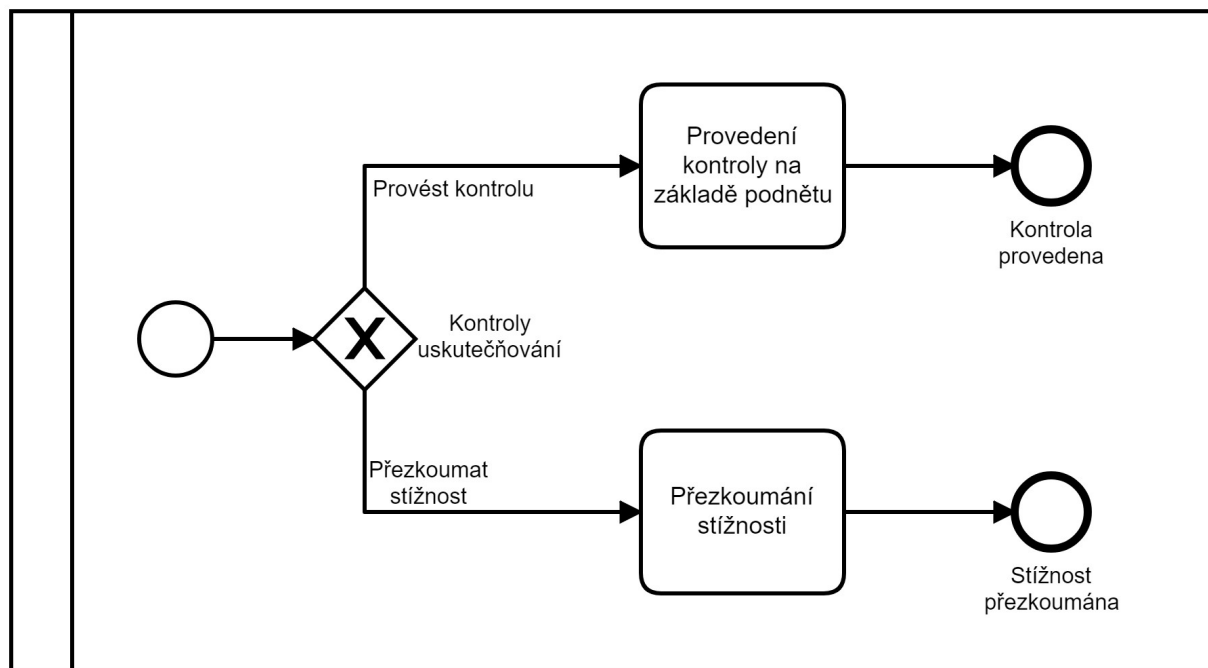


Obrázek 7: Vytvoření a zveřejnění metodiky

Workflow/tiketu vytvoření a zveřejnění pracuje s parametry datového záznamu „metodika“.

## Kontrola uskutečňování terapeutických programů

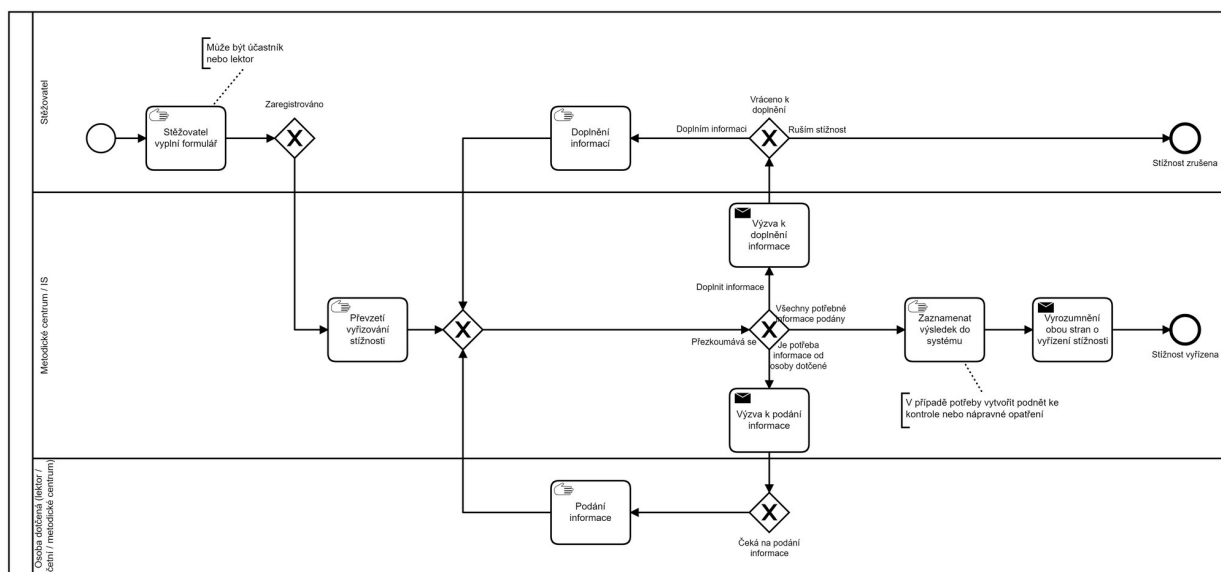
Kontroly uskutečňování terapeutických programů obsahují jak samotný proces provedení kontroly na základě podnětu, tak i proces přezkoumání stížností. Proces kontroly se řídí zákonem 255/2012 Sb. o kontrole (kontrolní řád).



Obrázek 8: Proces kontroly uskutečňování terapeutických programů

Tabulka 23: Parametry procesu kontroly na základě podnětu

| Parametr                              | Popis                                         |
|---------------------------------------|-----------------------------------------------|
| Důvod kontroly                        | text                                          |
| Datum kontroly                        |                                               |
| Místo kontroly                        | text                                          |
| Kontrolovaná osoba(y)                 | link(y) na datové záznamy typu „person/group“ |
| Protokol o kontrole                   | příložený dokument(y)                         |
| Vyjádření vedoucího kontrolní skupiny | (text, nepovinný údaj, v případě námítky)     |
| Vyjádření ředitele Metodického centra | (text, nepovinný údaj, v případě námítky)     |
| Přílohy                               |                                               |



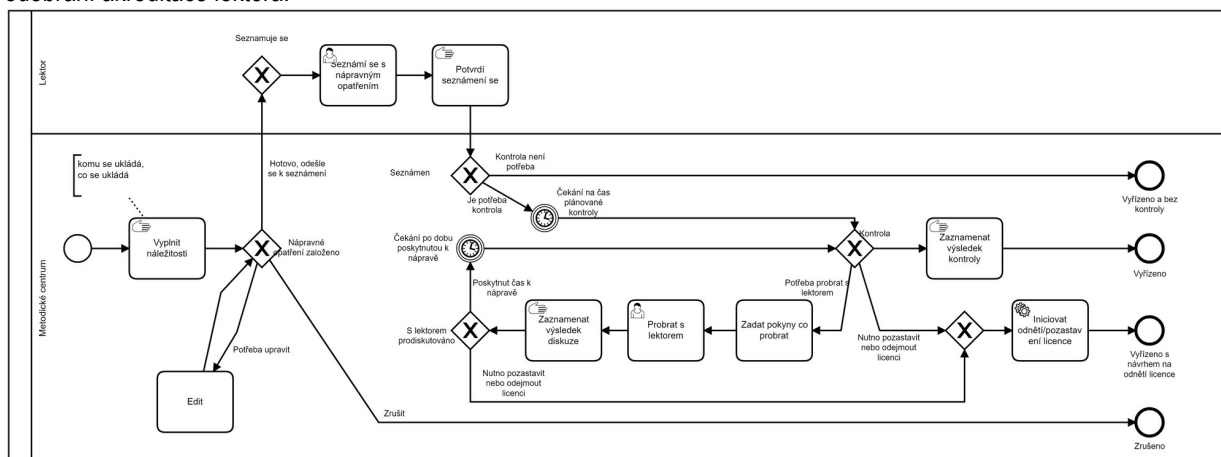
Obrázek 9: Proces přezkoumání stížnosti

Tabulka 24: Parametry procesu přezkoumání stížnosti

| Parametr              | Popis                                                           |
|-----------------------|-----------------------------------------------------------------|
| Stěžovatel            | Osoba, která stížnost podala                                    |
| Tvůrce                | Ten, kdo stížnost vytvořil (stěžovatel, asistovaná přepážka,..) |
| Datum vytvoření       |                                                                 |
| Popis stížnosti       | Popis problémového stavu jak jej vidí stěžovatel                |
| Řešitel               | Osoba v roli „Metodické centrum“, která stížnost řeší           |
| Poznámky ke stížnosti | Mohou vkládat všichni zainteresovaní                            |
| Předmět stížnosti     | Lektor/kurz/platba/jiné                                         |
| Řešení                | Popis jak byla stížnost vyřešena/vyřízena                       |
| Přílohy               |                                                                 |

## Realizace nápravných opatření

Realizace nápravných opatření obsahují jak proces uložení opatření ke zjednání nápravy, tak proces případného odebrání akreditace lektora.



Obrázek 10: Proces opatření ke zjednání nápravy

Tabulka 25: Parametry procesu uložení opatření ke zjednání nápravy

| Parametr                     | Popis                                                                              |
|------------------------------|------------------------------------------------------------------------------------|
| Lektor                       | lektor, kterému ukládáme nápravné opatření - link na datový záznam typu „Lecturer“ |
| Text opatření                |                                                                                    |
| Přílohy                      | (nepovinný údaj)                                                                   |
| Kdo ukládá                   | uživatel v roli Metodické centrum - link na datový záznam typu „user/group“        |
| Kontroly dodržování          | linky na workflow/tikety typu „Provedení kontroly“                                 |
| Výsledek nápravného opatření | text                                                                               |

Tabulka 26: Parametry odebrání akreditace lektora

| Parametr                   | Popis                                                |
|----------------------------|------------------------------------------------------|
| Lektor                     | link na datový záznam „Lecturer“                     |
| Úkon                       | LOV (pozastavení, odebrání)                          |
| Důvod                      | text                                                 |
| Přílohy                    | (nepovinná položka) dokumenty přiložené k rozhodnutí |
| Linky na nápravná opatření | (nepovinná položka)                                  |
| Linky na stížnosti         | (nepovinná položka)                                  |
| Rozhodnutí                 | LOV (zamítnuto, akreditace odebrána)                 |

## Zajištění vzdělávání lektora

### Kvalifikační kurzy lektorů

Kvalifikační kurzy lektorů vypisuje Metodické centrum.

Zájemci z řad uchazečů o pozici lektora se hlásí na tyto kurzy prostřednictvím internetového informačního portálu. Kurz je zpoplatněn částkou dle aktuálního ceníku.

V průběhu kurzu je vyplňována docházka v jednotlivých termínech, u závěrečné zkoušky pak vyplní hodnocení zkoušky. Úspěšné složení závěrečné zkoušky je zaznamenáno mezi informace vedené o uchazeči.

### Průběžné vzdělávání lektorů

Termíny kurzů průběžného vzdělávání lektorů vypisuje Metodické centrum. Lektori se hlásí na jednotlivé kurzy prostřednictvím internetového informačního portálu.

V průběhu kurzu je zaznamenávána docházka a na konci je úspěšné absolvování kurzu uvedeno v záznamu lektora.

Tabulka 27: Parametry procesu kurzu průběžného vzdělávání lektorů

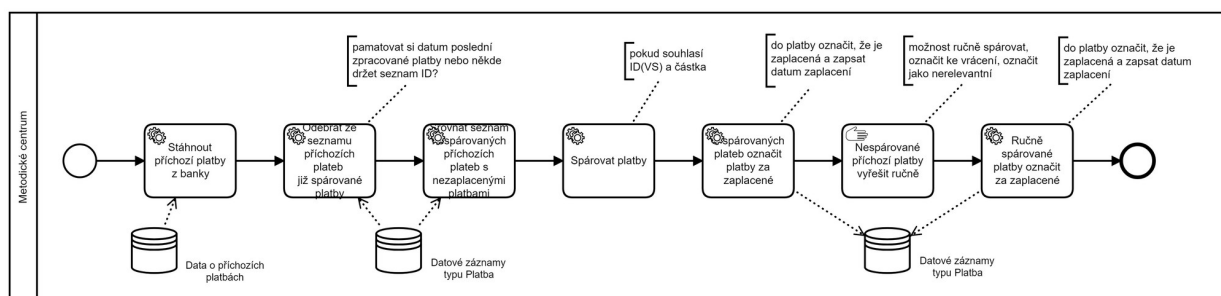
| Parametr                          | Popis                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Vedoucí kurzu                     | vedoucí kurzu průběžného vzdělávání                                                                                         |
| Bloky kurzu průběžného vzdělávání | linky na workflow/tikety jednotlivých bloků kurzu průběžného vzdělávání (zde budou uloženy data a časy konání těchto bloků) |
| Datum začátku a konce kurzu       | (pokud se nebude brát začátek prvního bloku a konec posledního)                                                             |
| Místo konání kurzu                |                                                                                                                             |
| Účastníci kurzu                   | linky na datové záznamy typu „Lecturer“                                                                                     |
| Přílohy                           | pro vložení rozvrhu témat jednotlivých bloků, popřípadě nějakých školících materiálů                                        |

Tabulka 28: Parametry bloku kurzu průběžného vzdělávání lektorů

| Parametr                   | Popis                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------|
| Kurz průběžného vzdělávání | link na workflow/tiket kurzu průběžného vzdělávání                                        |
| Datum konání               |                                                                                           |
| Čas začátku                |                                                                                           |
| Čas konce                  |                                                                                           |
| Místo konání               | (nepovinný údaj – použije se pokud je odlišné od místa konání uvedeného pro celý kurz)    |
| Účastníci kurzu            | linky na datové záznamy typu „Lecturer“                                                   |
| Záznamy o účasti           | pro každého účastníka, obsahuje jestli se zúčastnil, omluvenky (včetně příloh) a poznámku |
| Přílohy                    | pro vložení školících materiálů                                                           |

## Párování plateb

Příchozí platby jsou párovány automaticky, k uživateli v roli Metodické centrum se pak dostanou pouze příchozí platby, které se nepodařilo automaticky spárovat. Uživatel pak buď spáruje platbu ručně nebo ji označí k vrácení nebo jako nerelevantní.



Obrázek 11: Proces párování plateb

Tabulka 29: Parametry procesu párování plateb

| Parametr           | Popis                            |
|--------------------|----------------------------------|
| Příchozí platby    | data s příchozími platbami       |
| Nespárované platby | linky na datové položky „Platba“ |

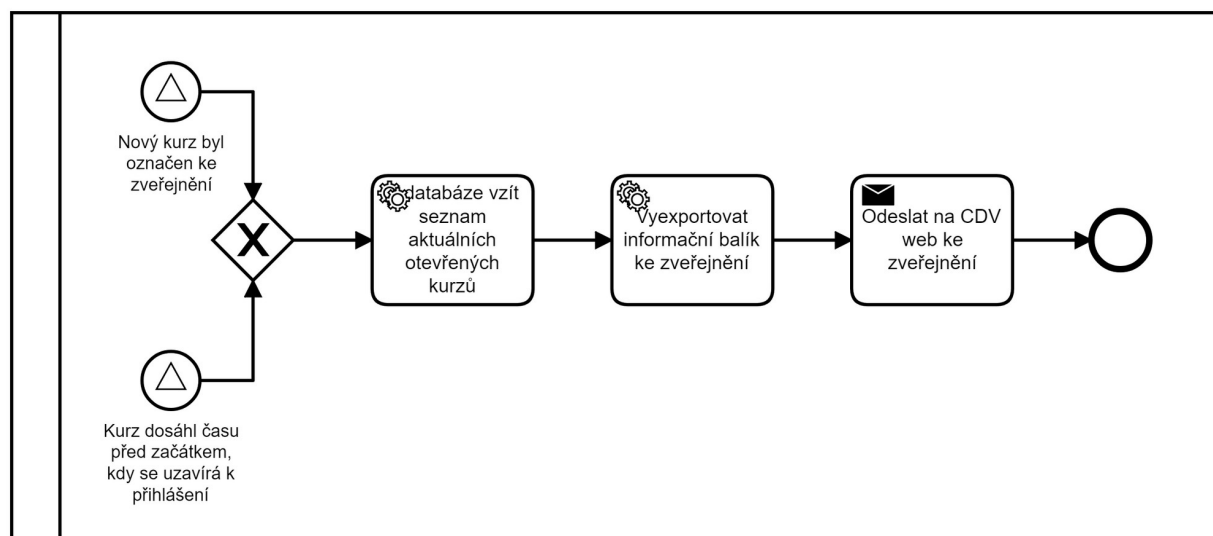
## Informační procesy

Informační procesy zahrnují informování veřejnosti o vypsání kurzech, informování účastníka o údajích o něm vedených, lektora o údajích o něm vedených a o údajích vedených o účastnících kurzu jím vedených a informování úřadů dle § 102d odst. 6a) zák. 361/2000 ve znění platném od 1. 7. 2023.

Mezi informační procesy patří:

- proces Informování o kurzu z databáze terapeutických programů (odpovídá službě EA „Realizace terapeutického programu“)
- v rámci služby EA „Poskytování údajů z evidence účastníků terapeutických programů“:
  - Poskytnutí údajů silničním správním úřadům, orgánům územních samosprávních celků, orgánům činným v trestním řízení a Probační a mediační službě
  - Poskytnutí údajů účastníkovi v rozsahu údajů o něm vedených
- v rámci služby EA „Poskytování údajů z evidence akreditovaných lektorů“:
  - poskytnutí údajů lektorovi

## Informování o kurzu



Obrázek 12: Proces informování o kurzu

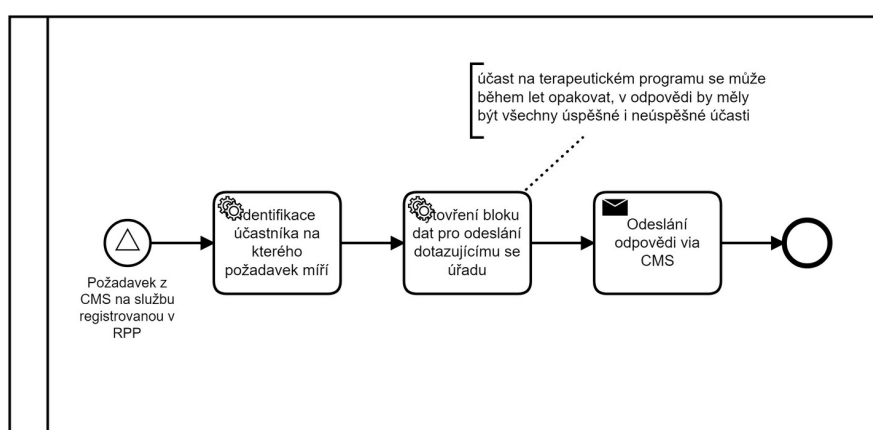
Tabulka 30: Parametry procesu informování o kurzu

| Parametr                           | Popis                                                         |
|------------------------------------|---------------------------------------------------------------|
| Seznam aktuálních otevřených kurzů | pole linků na workflow typu Realizace terapeutického programu |

**Poskytnutí údajů silničním správním úřadům, orgánům územních samosprávních celků, orgánům činným v trestním řízení a Probační a mediační službě o účastníkovi.**

A do budoucna jakýmkoliv úřadům, které získají zákonné oprávnění získat tyto údaje a zaregistrují si tuto pravomoc v RPP.

V rámci poskytování údajů je možno udělat varianty dotazu typu: dotaz na poslední účast, výpis všech účastí apod.

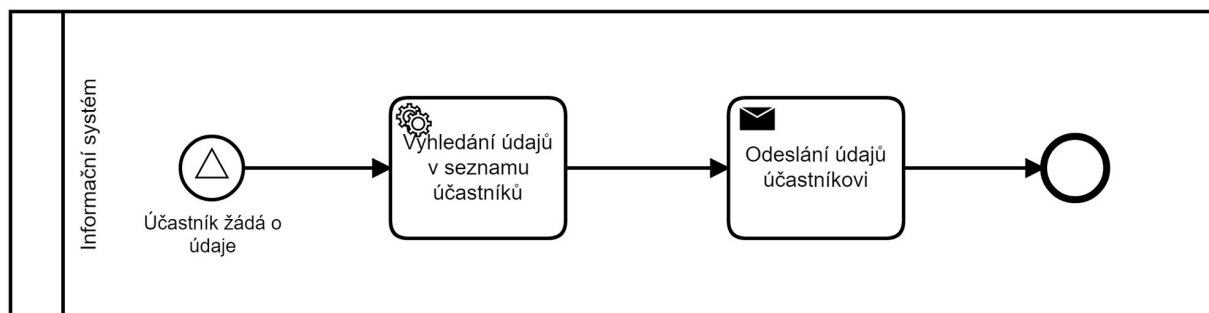


Obrázek 13: Poskytnutí údajů úřadům

Tabulka 31: Parametry procesu poskytnutí údajů úřadům

| Parametr                                 | Popis                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------|
| Seznam účastníků terapeutických programů | seznam datových záznamů typu Účastník, ze kterého budou vyhledány a zpracovány údaje pro odeslání |
| ID úřadu                                 | identifikace úřadu, který požádal o poskytnutí údajů                                              |

#### Poskytnutí údajů účastníkovi v rozsahu údajů o něm vedených



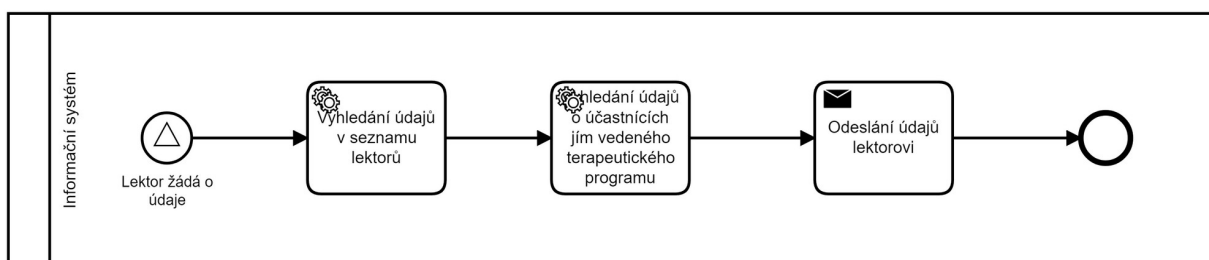
Obrázek 14: Proces poskytnutí údajů účastníkovi

Tabulka 32: Parametry procesu poskytnutí údajů účastníkovi

| Parametr                                 | Popis                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------|
| Seznam účastníků terapeutických programů | seznam datových záznamů typu Účastník, ze kterého budou vyhledány a zpracovány údaje pro odeslání |

#### Poskytnutí údajů z evidence akreditovaných lektorů

V tomto případě bude pravděpodobně potřeba poskytnout lektorovi údaje o něm vedené i v případě (ještě) neakreditovaného lektora, popřípadě lektora s pozastavenou nebo odebranou akreditací. Umožňuje také poskytnout lektorovi údaje o účastnících jím vedeného terapeutického programu.



Obrázek 15: Proces poskytnutí údajů lektorovi

Tabulka 33: Parametry procesu poskytnutí údajů lektorovi

| Parametr         | Popis                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Seznam lektorů   | seznam datových záznamů typu Lektor, ze kterého budou vyhledány a zpracovány údaje o něm vedené, pro odeslání                                      |
| Seznam účastníků | seznam datových záznamů typu Účastník, ze kterého budou vyhledány a zpracovány údaje o účastnících tímto lektorem vedených terapeutických programů |

## Zvláštní úkony

Zakládání účtů a přidělování privilegovaných rolí „Administrátor IIS“ (a popřípadě i „Metodické centrum – úřední osoba“ a „Osoba oprávněná nahlížet“) bude realizováno procesem řízení změn, kdy na základě požadavku schváleného Metodickým centrem bude tyto úkony realizovat provozovatel v rámci standardního provozu řešení.

## Automatické kontroly

### Kontroly

|                              |                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Smazání expirovaných záznamů | Denní kontrola všech záznamů a smazání těch, které expirovaly                                                            |
| Vyplnění docházky            | Denní kontrola vyplnění docházky – pokud od sezení uplynul stanovený čas a docházka není vyplněna, je lektor notifikován |

Další nutno dodefinovat se zadavatelem v průběhu přípravy realizace projektu.

# Informační portál

## Přihlášení a práva

### Uživatelé a lektori

- standardní přihlášení bude probíhat s využitím identifikace a autentizace NIA.
- budou mít přístup pouze ke svým osobním údajům a k agendám nutným k požadovaným úkonům
- lektori získají po registraci pouze práva pro úkony spojené s akreditací, po úspěšné akreditaci jim bude automaticky přidělen přístup k vytváření a práci s terapeutickými kurzy

### Metodické centrum – úřední osoba

- osoby v roli Metodické centrum – úřední osoba se budou přihlašovat s využitím NIA
- bude mít přístup k informacím o lektorech i uživatelích
- kromě svých agend bude mít přístup i k agendám pro roli Metodické centrum a k agendám pro roli Lektor (pro případ potřeby zástupu)

### Metodické centrum

- běžný pracovník Metodického centra se bude přihlašovat pomocí NIA

### Osoby oprávněné nahlížet

- nebudou se u nás přihlašovat, využijí služby propagované skrze ISSS/CMS
- budou mít přístup k informacím o úspěšném absolvování terapeutického programu dle § 102d odst. 6a) zákona 361/2000 Sb.

### Administrátor IIP

- administrátor se bude přihlašovat pomocí lokálního systému ověřování a nebude mít přístup k osobním informacím o uživateli a nebude moci provádět úkony v systému
- bude mít přístup k nastavení systému v rozsahu potřebném k provozu a úpravám fungování systému

## Poskytování informací

### Veřejnost

Veřejnosti budou poskytovány obecná data o prováděných a dokončených terapeutických programech dle 102d, odst. 6d) zákona č. 361/2000 Sb.

Dále budou poskytována veřejná data dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Budou to souhrnné anonymizované údaje o počtu úspěšných a neúspěšných klientů, členěno po letech - tyto informace budou zveřejňovány dle pokynů a dobré praxe popsané na portále otevřených dat <https://data.gov.cz>.

Veškerá data bude možné zpřístupnit (eventuálně na vyžádání, ale bez dodatečných nákladů) se stupněm otevřenosti 3.

### Lektor

Lektorům budou poskytovány informace potřebné k požadovaným úkonům (tj. metodické pokyny, zápisy z kontrol jeho kurzů, uživatelích zapsaných do jeho kurzů, jeho kurzů). Mimo to bude mít přístup k informacím o něm vedených.

### Účastník

Účastník bude mít přístup k informacím o něm vedeným. Kromě toho bude mít přístup k informacím potřebným k registraci na kurz, k podkladům připraveným pro daný kurz a k obecným informacím o průběhu kurzů.

## **Úřady**

Úřady, stanovené § 102d odst. 6a) zákona 361/2000 Sb. (silniční správní úřady, orgány územních samosprávných celků, orgány činné v trestním řízení a Probační a mediační služba), budou mít přístup k informacím o absolvování kurzu jednotlivých účastníků podle výše zmíněného zákona.

## **Propagace dat skrze veřejnou část webu CDV**

- Data ze zákona poskytovaná veřejnosti (termíny terapeutických programů)
- Přístup účastníků pro provádění úkonů
- Přístup lektorů pro provádění úkonů

## **Napojení na registr evidence obyvatel**

Dle §102d, odst.8 zákona 361/2000 Sb. poskytne Ministerstvo vnitra referenční údaje ze základního registru obyvatel:

- poskytuje jméno, popřípadě jména, příjmení,
- datum narození,
- adresa místa pobytu, popř. adresa na kterou mají být doručovány písemnosti

Napojení proběhne pomocí služeb ISSS/CMS.

## **Napojení na definované komunikační kanály**

### **Datové schránky (ISDS)**

Systém bude k ISDS připojen standardně pomocí webových služeb.

## **ISSS/CMS**

Předpokládáme že napojení bude provedeno prostřednictvím KIVS poskytovatele eGovernment cloudu, kde bude systém provozován. Bude řešit budoucí provozovatel řešení.

## **Import příchozích plateb**

Příchozí platby budou importovány jako csv/xml soubor nebo skrze napojení na bankovní API, dle způsobu nasazení a provozování, které bude k dispozici dle konkrétního budoucího provozovatele systému.

# Bezpečnost a připravenost k nasazení

## Bezpečnost

V rámci řešení bezpečnosti systému a jím zpracovávaných dat vznikne tzv. **Security guide** s pokyny pro dodržení všech potřebných bezpečnostních aspektů při nasazení i provozu systému.

Následuje soupis nejdůležitějších aspektů bezpečnosti systému v bodech.

Systém:

- provoz v prostředí eGovernment cloudu
  - v prostorách CDV není fyzický přístup k výpočetním prostředkům používaným pro běh systému
  - bezpečnostní standardy provozu ISVS zajištěny certifikací poskytovatele eGovernment cloudu
- kompletní logování přístupů a držení auditní stopy
- WAAP
- TLS encapsulator
- Business continuity management – zóny dostupnosti, zálohování, archivace, definováno RPO, RTO a RTA pro všechny komponenty řešení
- identifikace a autentifikace bude probíhat s využitím NIA
  - s výjimkou role Administrátor IIP
- Business Recovery Plan – plán pro obnovení systému po fatálním selhání následkem selhání nebo útoku

Data:

- Pro identifikované subjekty v roli „Účastník“ a „Lektor“ bude jako interní identifikátor využíván AIFO. Pro ostatní role bude využit interní systémový identifikátor, přebíraný v návaznosti na SSO z CDV Directory services | ESB.
- šifrování dat na úrovni aplikace (příslušných datových položek, jejich atributů, procesů, transakcí apod.), a to standardními kryptografickými prostředky

## Možné způsoby nasazení a provozování

Aplikace bude jako přímý runtime využívat GPC platformu a její bezpečnostní prvky. Toto v sobě zahrnuje vrstvy:

- WAAP / WAF variantně na technologiích mod\_security+nginx, mod\_security+apache, případně jiný, dostupný v podobě služby u vybraného cloud poskytovatele,
- aplikační frontend v podobě GPC UI nad java aplikačním serverem,
- databázový backend, využívající GPC temporální databázi.

WAAP plní i funkci reverzní proxy, potenciálně s funkcionalitou SSL offloading, ale standardně je směrem na aplikační frontend použito šifrované připojení pomocí protokolu HTTPS.

Z pohledu nastavení šifrování budou aplikována platná doporučení pro použité šifrovací a podepisovací algoritmy dle <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>. Certifikáty obvykle dodává zákazník, případně provozovatel. Bude však možné použít i dynamicky generované certifikáty via ACME protokol.

Mezi aplikačním frontendem a databází je komunikace výhradně prostřednictvím databázového protokolu, který bude ve standardním nastavení šifrovaný.

GPC platforma interně využívá technologii Docker. Jsou podporovány a bude možné využít orchestrace typu Docker Swarm či Kubernetes, nicméně níže popsany návrh zabezpečení vychází z poskytnutého schématu Diagram technologické architektury dle přílohy P1a a Docker host je zde uveden v roli hypervizoru.

Plánovaný způsob nasazení, zajišťující ochranu před vnějšími kybernetickými útoky:

- Docker host s kontejnerizací nebude mít funkční rozhraní s přiřazenou IP adresou, která by byla přístupná z Internetu; naopak, bude dostupný pouze z prostředí „Administrativních nástrojů“ dle Diagramu technologické architektury.

- Kontejner s WAAP / WAF bude mít vypublikováno jedno síťové rozhraní do DMZ (pomocí Docker macvlan driveru) a druhé rozhraní do oddělené sítě, kde poběží (pouze) aplikační frontend.
- Pokud bude aplikační frontend provozován v kontejneru na stejném Docker hostu jako WAAP / WAF (což závisí na budoucím provozovateli systému), bude mezi nimi virtuální síťový adaptér (separátní Docker bridge).
- Obdobně bude postupováno při komunikaci mezi aplikačním frontendem a databázovým backendem.
- Alternativně bude možné jednu či všechny instance provozovat v oddělených sítích, potenciálně s vloženým firewallem, paketovým filtrem, access group připojenou na virtuální instanci apod. V těchto případech bude použita dedikovaná virtuální síť pro komunikaci mezi instancemi různého určení.
- V žádném podporovaném scénáři nebude existovat externě routovatelná síť se společným adresním prostorem mezi Docker hostem a WAAP / WAF, ani mezi WAAP / WAF a databázovým serverem.

V rámci jednotlivých kontejnerů vždy poběží jen nezbytně nutné procesy použité aplikace (nad to explicitně poznamenejme, že se v případě kontejneru v žádném případě nejedná o plnohodnotný OS).

Konfigurace (image) daného kontejneru bude z pohledu diskových dat verzována, aktualizace budou probíhat atomicky a vždy se bude možné vrátit do výchozího stavu, případně konkrétního stavu v minulosti. Perzistentní data bude obsahovat jen kontejner s temporální databází. Tato data budou zabezpečena a bude k nim držena auditní stopa a transakční historie.

Logy z jednotlivých Docker kontejnerů i Docker hostů bude možné zasílat na jiné systémy (log managery) a tam je (dle vlastností použitého řešení třetí strany) v reálném čase ukládat a zpracovávat.

Detailní informace o způsobu nasazení a požadavcích na správné provedení nasazení budou uvedeny ve specializovaném dokumentu, tzv. **Deployment guide**.

## Provoz

### Standardní provoz a údržba IIP

Všechny technické komponenty IIP budou vyvinuty a nasazeny formou CI / CD. Jednotlivé verze kontejnerů pro testovací a následně ostrý provoz poskytujeme provozovateli formou docker kontejnerů, dostupných z internetového repository dodavatele, popřípadě vlastního docker repository provozovatele, kam budou nahrávány aktualizace dodavatelem.

Zároveň bude odděleno testovací a produkční prostředí pro testování nových verzí u zákazníka.

Upgrady produkčního prostředí provádí provozovatel dle potřeby při zajištění dostupnosti řešení z pohledu zákazníka, upgrady dodávaných kontejnerů se provádějí po řádném otestování a dohodě se zákazníkem a dodavatelem v rámci domluvených maintenance window.

Co se týče upgrade kontejnerů v testovacím prostředí, provádí se průběžně vždy na základě domluvy mezi zákazníkem, provozovatelem a dodavatelem.

## Požadavky na infrastrukturu

### Technické komponenty IIP

Jsou dodávány následující instance:

- master komponenta
- databázová komponenta
- user interface (UI) komponenta
- webserver (reverzní proxy s WAF) komponenta

## Logická architektura systému a způsob nasazení

Řešení bude obsahovat jednu centrální instanci v IP rozsahu určené pro interní uživatele, a jednu dialogovou instanci, určenou pro přístup uživatelů z internetu, umístěnou v DMZ.

Pro testovací prostředí není dialogová instance potřeba.

### Centrální instance

Centrální instance IPP obsahuje všechny technické komponenty potřebné pro běh aplikace.

Její součástí jsou zejména komponenty master, databáze a user interface (UI).

### Dialogová instance

Pomocí dialogových instancí probíhá interaktivní práce uživatelů z internetu. Dialogové instance slouží k posílení propustnosti řešení v silně zatížených prostředích, případně k vzájemné separaci různých skupin uživatelů z důvodů bezpečnosti, úrovně SLA, požadavků na jiný design či nastavení pracovního prostředí aj.

Obsahuje komponenty: user interface (UI), webserver (reverzní proxy s WAF)

Přes identicky nakonfigurované dialogové instance lze provádět aplikační loadbalancing (se zachováním session persistency).

## Požadavky na zdroje

### Centrální instance

#### **Testovací prostředí:**

Minimálně 16 GB RAM, 8 vcpu, 100 GB diskového prostoru s možností rozšíření kapacity za provozu

#### **Produkční prostředí:**

Minimálně 64 Gb RAM, 16 vcpu, 500 GB diskového prostoru s možností rozšíření kapacity za provozu

### Dialogová instance

Minimálně 16 GB RAM, 8 vcpu, 50 GB diskového prostoru s možností rozšíření kapacity za provozu

## Zálohování a obnova po havárii

Zálohování bude probíhat podle zálohovací politiky dle volby provozovatele systému a na jeho zodpovědnost, respektive na zodpovědnost poskytovatelů zálohovacího řešení. V odůvodněných případech je dodavatel oprávněný požadovat ad hoc provedení zálohy a obnovy dat, například za účelem kopií a klonování systému, migrací systému, troubleshootingu apod.

Obnovu dat provádí poskytovatel zálohovacího řešení, s eventuální dopomocí provozovatele, dle standardních postupů. O takto provedené obnově bude vyrozuměn dodavatel, který provede následnou kontrolu aplikace.

## Monitorování

Dodané řešení může být monitorováno libovolnými nástroji, které provozovatel standardně využívá.

Externí testy: testy dostupnosti IP a odezvy (čas, obsah) aplikace z pohledu uživatele v internetu.

Interní testy: testy dostupnosti IP a odezvy aplikace z pohledu interního uživatele, dostupnosti a odezvy (čas, obsah) spolupracujících systémů provozovatele a sledování zdrojů:

- zátěže CPU
- spotřeby paměti
- latence I/O
- obsazení diskového prostoru

## Logování

Veškeré použité technické komponenty interně logují v rámci instance, na které jsou nainstalovány, a to zejména pro potřeby maintenance a troubleshootingu. Dále jsou logy posílány do externího log management systému dle specifikace provozovatele (např. pomocí protokolu syslog).

## Testování

Pro potřeby automatického ověřování správného fungování dílčích částí systému při nasazování nových verzí v průběhu vývoje a testování budou vytvořeny jednotkové testy.

Za účelem testování bude, minimálně do doby přechodu do běžného provozu, v provozu zvláštní instance systému dedikovaná pro účely testování. Tato instance bude fungovat v prostředí odpovídajícímu prostředí dle doporučení pro budoucího provozovatele systému.

## Exit strategie

Data bude možno exportovat v xml formátu s definovaným schématem, tedy se stupněm otevřenosti 3. Data bude možno exportovat uživatelsky v roli Metodické centrum.

Součástí dodávky budou jak všechny soubory definující business logic (tzn. datový model, jednotlivá workflow i definice formulářů), tak licence nutná provozování této business logic. Součástí bude i dokumentace nasazení a provozní dokumentace systému.

Systém bude využívat Docker kontajnery tak, aby jej bylo možno provozovat s využitím standardních IaaS nebo PaaS služeb. V průběhu akceptačního řízení bude demonstrováno převedení homogenní kopie aplikace mezi různými cloud providery.