Obsah

[Provozní a technické požadavky na HR systém 1](#_Toc80134706)

[1. Popis IT prostředí Zadavatele 1](#_Toc80134707)

[2. HR IS požadavky na IT prostředí 3](#_Toc80134708)

[2.1. Provoz HR systému 3](#_Toc80134709)

[2.2. Provoz klientské části 4](#_Toc80134710)

[2.3. Odezva systému 5](#_Toc80134711)

[3. Bezpečnost 5](#_Toc80134712)

[3.1. Požadavky na bezpečnost HR systému 5](#_Toc80134713)

[3.2. Autentizace a autorizace 6](#_Toc80134714)

[3.3. Důvěrnost a integrita 6](#_Toc80134715)

[3.4. Auditovatelnost a nepopiratelnost 6](#_Toc80134716)

[3.5. Zálohování 7](#_Toc80134717)

[4. Integrace do prostředí Zadavatele 7](#_Toc80134718)

[5. Migrace dat 9](#_Toc80134719)

[6. Školení 9](#_Toc80134720)

# Provozní a technické požadavky na HR systém

V této příloze je popsáno IT prostředí pro provoz HR systému (dále také jako HR IS) a požadavky související s provozem HR systému v prostředí Zadavatele. Účastník/Dodavatel podáním nabídky garantuje, že jím dodávaný HR systém splňuje požadované a je provozuschopný v tomto prostředí.

# Popis IT prostředí Zadavatele

Systém HRIS musí využívat standardní systémové komponenty a nastavení ZP MV ČR a musí být do tohoto prostředí implementovatelný.

1. Servery
   * + Při použití těchto komponent ZP MV ČR zajišťuje jejich licence
   1. Hardware
      * Všechny servery v ZP MV ČR jsou provozovány na platformě VMware vSphere 6.7, která je pravidelně upgradovaná
      * Diskové systémy jsou v kombinaci SAN pro virtuální disky a NAS pro virtuální disky a sdílená úložiště
   2. Operační systémy
      * MS Windows Server 2016 Datacenter a vyšší
      * SUSE Linux Enterprise Server 12 SP4 a vyšší
   3. Databáze
      * MS SQL Server 2019 (sdílený s dalšími systémy)
   4. Aplikační servery
      * Apache HTTP Server 2.4
      * Apache Tomcat 8 a vyšší
      * MS IIS 10 a vyšší
      * Jiné
      * ZP MV ČR preferuje kontejnerové řešení aplikačního serveru
   5. Dohled
      * Zabbix 5
2. Infrastruktura
   * + Servery jsou propojeny 10Gb LAN
     + HRIS bude mít k dispozici samostatný segment LAN
     + Přístup k ostatním systémům a internetu bude řízen politikami na firewallu, komunikace mezi komponentami HRIS, bude-li jich více, bude bez omezení
     + Přístup klientů i ostatních systémů ZP MV ČR k HRIS bude řízen politikami na firewallu
   1. Zálohování
      * Simpana Commvault 11
      * Možnost zálohování celých virtuálních strojů
      * Možnost zálohování filesystem
      * Možnost zálohování DB
   2. Bezpečnost
      * Centrální firewall v ZP MV ČR je CheckPoint 5900 R80.40
      * Doplňkový firewall je Fortinet FortiGate-100 sloužící pro segmentaci serverových sítí
      * Základem ověřování v ZP MV ČR Je MS Active Directory
      * Antivirový systém je Symantec Endpoint Protection verze 9 (a bude pravidelně upgradovaná)
      * DLP systém pro klientská zařízení je Safetica 9
      * DLP systém na bázi sítí je součástí fw Checkpoint
      * Správa a analýza logů – probíhá výběrové řízení, podporovány budou minimálně protokoly syslog a RELP, HRIS musí umožnit sběr logů, nebo zajistit jejich odesílání
3. Klientská zařízení
   * + Windows 10 Enterprise/Professional
     + MS Office 365
     + MS Internet Explorer v aktuální verzi
     + MS Edge v aktuální verzi
     + Google Chrome v aktuální verzi
     + Výchozím prohlížečem v ZP MV ČR je Google Chrome
   1. Bezpečnost
      * Symantec Endpoint Protection 14
      * Safetica 9
      * Ověřování je možné v Active Directory nebo v Azure Active Directory
4. VPN
   * + ZP MV ČR při splnění bezpečnostních zásad stanovených vnitřními předpisy ZP MV ČR umožňuje vzdálený přístup pomocí vpn klienta CheckPoint a hw klíče s certifikátem
5. Systémové služby
   1. Elektronická pošta
      * ZPMV používá cloudové MS Exchange v rámci M365
   2. Tisková zařízení
      * ZP MV ČR využívá systém chráněného tisku YSoft SafeQ 5
      * Základem jsou tiskárny Konica Minolta Bizhub C308, C368, C454e
      * Dále je využíván mix malých tiskáren a multifunkcí značky HP
   3. Řízení systémového času
      * ZP MV ČR má vlastní NTP server
      * V případě nutnosti je možné využít i externí ntp servery, se kterými se ZP MV ČR synchronizuje, tik.cesnet.cz, tak.cesnet.cz, ntp.cesnet.cz
   4. Internet (DMZ)
      * V případě nutnosti vystavení nějaké části systému do internetu je možné část systému umístit do DMZ

# HR IS požadavky na IT prostředí

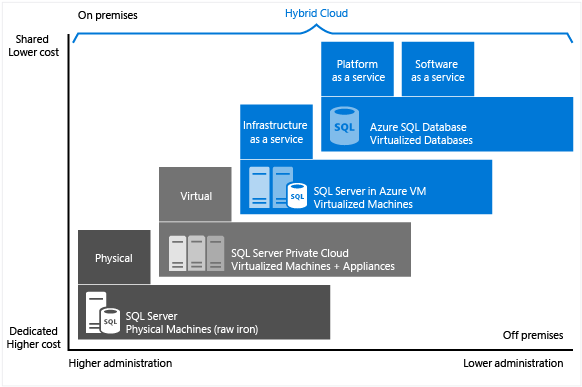
Dodavatel jako součást nabídky předloží požadovanou technickou specifikaci provozního a testovacího prostředí, tedy požadavky na počet virtuálních strojů a jejich konfiguraci (CPU, RAM, diskový prostor) a kompletní popis požadovaného nastavení prostředí, které je nezbytné pro provoz instance HR IS.

Bude-li HR systém provozován na výše uvedených prostředcích, potřebné provozní licence zajistí ZP MV ČR. Bude-li dodán HR systém vyžadující pro svůj provoz odlišné prostředky, je Dodavatel povinen s HR systémem dodat i licence k těmto prostředkům.

# Provoz HR systému

HR IS bude provozován v provozním a testovacím prostředí zadavatele a to On-Premises.

Zároveň systém musí být uzpůsoben pro budoucí přesun do cloudového prostředí Zadavatele, preferovaná je možnost **kontejnerizace.**



Umožňovat systém HR provozovat pomoci platformy PaaS služby webové aplikace nebo řešení využívající aplikační server a omezující utilizaci mezi koncovou stanicí a serverem.

Pokud HR IS využívá produktů třetích stran, pro jejichž používání je třeba pořízení licence, musí být tyto licence součástí nabídky v počtu a rozsahu nezbytném pro provozování systému na obou prostředích (testovacím a provozním). Cena za tyto licence je však zahrnuta v ceně uvedené v čl. 8 Smlouvy.

Dodavatel musí disponovat vlastním vývojovým prostředím, tedy případný dovývoj probíhá u dodavatele, poté je rolován do testovacího prostředí zadavatele a po uvolnění do produkce.

Dodavatele zajišťuje instalaci a následnou pravidelnou aktualizaci serverové vrstvy systému HR IS, instalace a aktualizace OS na serverové části a klientskou část bude instalovat a aktualizovat Zadavatel, avšak v součinnosti a na základě doporučení Dodavatele (vč. pravidelných patchů).

Instalace a aktualizaci prováděné Dodavatelem budou prováděny na základě vyžádaného přístupu pod dohledem, případně pracovníkem Dodavatele v prostorách Zadavatele.

Dodavatel bude používat pro implementaci a podporu provozu databází a aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Zadavatele nebo bezpečným mechanismem schváleným Zadavatelem. Administrátorské účty spravuje Zadavatel.

Dodavatel nastaví replikace dat z ostrého systému do testovací verze dle požadavků Zadavatele (např. na denní bázi) pro případné ověření postupů a simulace výpočtu v testovací verzi.

# Provoz klientské části

Pokud HR IS využívá produktů třetích stran (např. JAVA), pro jejichž používání je třeba pořízení licence, musí být tyto licence součástí nabídky v počtu a rozsahu nezbytném pro provozování systému na obou prostředích (testovacím a produktivním). Cena za tyto licence je však zahrnuta v ceně uvedené v čl. 8 Smlouvy.

Instalace klientské části HR IS na uživatelské stanice není preferována. Instalace software na klientskou stanici je prováděna především prostřednictvím vzdálené automatické instalace. Instalace musí být kompatibilní se službou MS Installer (standardní služba operačního systému). Instalace programového vybavení na klientskou stanici je prováděna centrálně pomocí SCCM, tedy bez nutnosti zvýšených oprávnění jako „Power User“ nebo „Administrator“.

Není přípustné ukládat na klientskou stanici/Desktop data trvalé hodnoty, taková data je nutno ukládat na centrální diskové kapacity. Na klientské stanici nesmí být prováděno dávkové zpracování dat IS.

Dávkové zpracování centrálně uložených dat je přípustné spouštět a provádět pouze na databázovém serveru nebo případně na aplikačním serveru.

Pro práci oddělení lidských zdrojů a pro oblast správy systému je přípustná instalace lokálního systému na pracovní stanici (dále jen „tlustý klient“).

Pro práci tenkého klienta je používán prohlížeč Google Chrome a MS Edge v posledních verzích.

# Odezva systému

Odezva systému na běžné úlohy uživatelů (jednoduchá vyhledávání, založení záznamu, editace záznamu apod.) by měla být obvyklá, aby neomezovala uživatele v běžné práci.

HR Systém musí umožnit paralelní práci v jednotlivých úlohách, tj. umožnit vyvolání předem neomezeného počtu úloh (i stejných úloh s jinými parametry) tak, aby byla možná práce pomocí přepínaných formulářů a nebylo nutné přerušit práci v jedné úloze kvůli nutnosti otevřít (spustit) úlohu jinou. K tomu účelu musí být řešeno efektivní a neblokující zamykání.

Doba měsíčního zpracování mezd by měla být při maximálním množství zpracovávaných kmenových záznamů (1000) do 45 minut.

# Bezpečnost

HR systém je součástí významného informačního systému dle § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), jehož je Zadavatel provozovatelem a správcem dle § 3 písm. e) výše zmíněného zákona o kybernetické bezpečnosti. Systém proto musí naplnit všechny požadavky vyplývající ze zákonů a dalších právních předpisů v souvislosti s kvalifikací systému a obsažených údajů.

# Požadavky na bezpečnost HR systému

Systém musí být odolný proti známým bezpečnostním hrozbám a útokům. Systém nesmí obsahovat žádné známé kritické zranitelnosti, vysoké zranitelnosti a střední zranitelnosti dle CVSS score.   
Splnění požadavku se ověří Reportem ze skenu zranitelností.

Test zranitelnosti ve fázi testování systému provede Zadavatel ve spolupráci Dodavatelem.

Kategorie zranitelností se klasifikují dle CVSS score, který je aplikován do bezpečnostního skeneru. Zranitelnosti kategorie 4 a vyšší nejsou akceptovatelné.

Systém musí být ošetřen dle OWASP. V závěrečném protokolu musí být minimálně uvedeny četnosti těchto zranitelností:

a) - Injection Flaws

b) - Cross Site Scripting (XSS)

c) - Broken Authentication and Session Management

d) - Insecure Direct Object Reference

e) - Cross Site Request Forgery (CSRF)

f) - Security Misconfiguration

g) - Failure to Restrict URL Access

h) - Unvalidated Redirects and Forwards

i) - Insecure Cryptographic Storage

j) - Insufficient Transport Layer Protection

Systém a jeho dokumentace musí vyhovovat požadavkům legislativy, a to Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (tzv. GDPR).

Součástí údajů vedených v HR IS budou údaje klasifikované dle právních předpisů upravujících ochranu osobních údajů jako:

* osobní údaje
* citlivé údaje

# Autentizace a autorizace

Každý uživatel HR IS musí být pro přístup do HR IS řádně autentizován.

HR systém musí podporovat funkce Single Sign-On s využitím služby Microsoft Active Directory u Zadavatele a možnost napojení na Identity Access Management

# Důvěrnost a integrita

HR IS musí umožňovat zajištění důvěrnosti a integrity dat na úrovni DB stroje, a to i před správci provozního prostředí (vyjma administrátorů DB Zadavatele přistupujících k datům pomocí administračních nástrojů DB). Pokud data nebudou uložena v MS SQL Zadavatele musí Dodavatel zajistit šifrování dat uložených v databázi dle platného doporučení NÚKIB ohledně aktuálně odolných kryptografických prostředků.

HR Systém musí zajistit důvěrnost a integritu dat na celé cestě mezi databázovým serverem a klientem, tedy je požadováno zabezpečené propojení mezi všemi architektonickými vrstvami systému vyjma zásahů a úprav realizovaných administrátory DB Zadavatele.

Důvěrnost a integrita dat musí být zachována i při zálohování a archivaci, a to jak při vlastním procesu, tak i následně vzhledem k médiím, na nichž jsou zálohy a archivní data uloženy vyjma zásahů a úprav realizovaných administrátory DB Zadavatele.

# Auditovatelnost a nepopiratelnost

Logování akcí musí být škálovatelné. Musí umožnit, aby bylo zaznamenáno nejen kdo, kdy a k jaké datové entitě přistupoval, ale také ke kterým konkrétním datovým objektům (řádky a sloupce entity) uživatel přistupoval (mohou být poznamenána též konkrétní data (datový obsah), která si uživatel zobrazil, avšak není to nutné vzhledem k možnosti rekonstrukce obsahu datových objektů k danému času). Pravidla pro ukládání záznamů o přístupech a činnosti specifikované pro uživatele je nutné přiměřeně uplatnit i pro činnost okolních systémů přistupujících k HR IS prostřednictvím nějakých rozhraní. Systém musí umožnit parametrické konfigurování pro jednotlivé auditované prvky. Požaduje se, aby záznamy o činnosti byly logovány a zaznamenány a systém musí umožnit tyto záznamy uložit do externího nástroje typu SIEM.

Veškeré změny dat v HR IS musí být logovány včetně zásahů a úprav realizovaných správci systému tak, aby bylo možné zjistit kdo, kdy, jak a která data v HR IS modifikoval:

* u nově založených záznamů (operace INSERT) musí být možno dohledat informace kdo, kdy a v jakém stavu (obsahu dat) záznam založil;
* u změněného záznamu (při každé operaci UPDATE) musí být umožněno zjištění kdo, kdy a jakým způsobem data změnil; a to v plné šíři datové věty a plné historii změn;
* u smazaného záznamu nesmí dojít k trvalému odstranění dat („nepodporovat operaci DELETE“), ale pouze k logickému zneplatnění záznamu (provést operaci UPDATE s nastavením ukončení platnosti) a musí být zaznamenáno kdo, kdy a v jakém stavu dat záznam logicky zneplatnil.
* Záznamy o neúspěšných i úspěšných přístupech musí být monitorovány a v případě zvýšeného počtu neúspěšných pokusů se požaduje vyvolání odpovídající akce.

Všechny záznamy o činnosti v HR IS musí být zabezpečeny proti:

* neoprávněnému přístupu k datům (zachování důvěrnosti);
* neoprávněné manipulaci (zachování integrity a prokazatelnosti, resp. principu nepopiratelnosti);
* ztrátě uložených informací v požadované době dostupnosti záznamů (zálohování a archivace).

Přístup k záznamům o činnosti musí být umožněn pouze oprávněným osobám (nemusí být administrátoři daného provozního prostředí).

# Zálohování

Zálohování a plná obnova systému HR IS a jejích dat bude zajištěna centrálním zálohovacím řešení Zadavatele. Implementace provádění záloh a obnovy vč. otestování bude řešena Zadavatelem v součinnosti s Dodavatelem na základě jím dodaných specifikací pro provádění záloh a obnovy.

Systém musí umožňovat průběžné i dávkové zálohování všech dat, která jsou dotčena užíváním HRIS tedy nejen těch, která jsou uložena v databázi ale současně i dalších nastavení a konfigurací, která vznikají a jsou modifikována v průběhu užívání. Přesný seznam objektů (souborů), které jsou dotčeny chodem systému, musí být uveden v technické specifikaci v dokumentaci.

Pokud nebude databáze HR IS typu MS SQL, musí být součástí nabídky i řešení zálohy této databáze a Disaster recovery.

Plán zálohování bude řešen po dohodě Zadavatele s Dodavatelem, na základě doporučení Dodavatele.

# Integrace do prostředí Zadavatele

HR IS musí poskytovat datové rozhraní umožňující zabezpečené předávání dat z pohledu důvěrnosti a integrity do dalších systémů (např. standardů RESTful API s podporou formátu JSON, XML apod.), včetně popisu rozhraní jednotlivých služeb v elektronické podobě. Rozhraní musí umožnit uživatelsky řídit tvorbu konkrétních výstupů na bázi otevřeného datového rozhraní (například možnost definovat konkrétní metodu webové služby, která poskytne vybraná data o vybraných entitách). **Dodavatel popíše navrhovaný způsob řešení způsobu zabezpečení přístupu a integrity dat pro implementovaná datová rozhraní.** Podrobná specifikace řešení vznikne v rámci Analýzy.

HR IS podporuje přenositelné a otevřené formáty (ODF, PDF a další) a formáty Microsoft Office (XLSX, DOCX a další). Je požadována možnost exportu dat z výstupních sestav nebo přímá tvorba datového výstupu namísto sestavy, a to do některého z otevřených standardních datových formátů (CSV, XML, TXT apod.). Veškeré výstupy dat z HR IS budou chráněny přístupovými právy.

HR IS musí umožnit integraci na všechny potřebné okolní systémy. V praxi se jedná jak o kompletní náhradu všech existujících vazeb stávajících HR IS na okolní systémy, tak i o požadavky na realizaci vazeb nových. Vazby na okolní systémy budou postaveny na otevřeném datovém rozhraní.

**Požadované vazby na externí systémy:**

* Napojení na bankovní systém (v současnosti Česká národní banka), případně ostatní bankovní systému, pokud dojde ke změně poskytovatele bankovních služeb
* ePodání ČSSZ – podání ELDP, Oznámení o nástupu do zaměstnání, Přehled o výši pojistného, Příloha k žádosti o dávku nemocenského pojištění, Potvrzení o studiu/o teoretické a praktické přípravě.
* Podpora elektronické komunikace se zdravotními pojišťovnami.
* Podpora elektronické komunikace s Finančním úřadem

**Integrace do prostředí Zadavatele:**

* **Konektor do Active Directory**

HR sytém bude napojen na služby Active Directory. Přenášet se bude kompletní hierarchie organizační struktury a údaje o zaměstnanci (jde zejména o tyto údaje osobní číslo, organizační struktura, zařazení zaměstnance v organizační struktuře, model pracovní doby, nadřízený, podřízený, pracovní středisko – název a kód, nákladové středisko, e-mail, telefon, mobil, pracovní místo – název a kód, místo výkonu práce – lokalita, kancelář).

* **Docházkový systém**

HR IS bude napojen na externí docházkový systém, z HR systému se do docházkového systému přenáší údaje o zaměstnanci a jeho zařazení do org. struktury, kompletní org. struktura, rozvržení pracovní doby. (jde zejména o tyto údaje osobní číslo, organizační struktura, zařazení zaměstnance v organizační struktuře, model pracovní doby, nadřízený, podřízený, pracovní středisko – název a kód, nákladové středisko, e-mail, pracovní místo – název a kód, možnost přenášení více pracovních poměru u jednoho zaměstnance).

Z docházkového sytému se přenáší do HR IS údaje zpracované údaje měsíční docházky zaměstnanců (negativní docházka) a nárok na stravenky

* **Elearningový systém**

HR IS bude napojen na elearningový systém (ITutor), požadované řešení napojení prostřednictví webových služeb. Popis stávající integrace bude předán Dodavateli v rámci analýzy. Dodavatel navrhne způsob integrace, který bude respektovat bezpečnostní požadavky Objednatele.

Přenášená data do elearningového systému se skládají ze dvou oblastí, první jsou údaje o zaměstnancích a organizační struktuře zaměstnanci (osobní číslo, organizační struktura, zařazení zaměstnance v organizační struktuře, nadřízený, podřízený, pracovní středisko – název a kód, nákladové středisko, e-mail, pracovní místo – název a kód, povinná školení související s prac. místem – BOZP, QMS, řidič referent,..) a druhá sada přenášených dat se týká požadavků na školení pracovníků dle připravených kurzů v elearningovém systému.

Do HR IS systému se přenáší potvrzení o absolvování školení s platností od a do, vystavený certifikát (pdf).

Integrace musí řešit přidávání a ukončování osob v evidenci školení, notifikace plánovaných školení.

* **Spisová služba**

HR systém musí podporovat standardní napojení na rozhraní spisové služby.

* **Přenos údajů do účetního a controllingového systému Zadavatele**

HR systém umožní export mzdových dat pro zaúčtování do ekonomického systému.

HR systém podporuje export objednávek externích školení do ekonomického systému, návaznost na zpracování faktur přijatých.

* **Přenos aktuální org. struktury, nadřazenost/podřazenost pracovníků do dalších systémů Zadavatele**

# Migrace dat

Dodavatel navrhne rozhraní a postupy pro migrace dat ze stávajícího systému HR systému a popíše nezbytnou organizační a technickou součinnost, již bude potřebovat. Export dat ze stávajícího systému se předpokládá standardními nástroji HR systému se součinností stávajícího dodavatele. Zadavatel zajistí naplnění dohodnutých datových struktur (xls; csv).

Migrovaná data zahrnují jak číselníky nutné pro provoz nového systému, tak historická data, jejichž uchování je dáno platnou legislativou.

Rozsah migrace dat do nového systému je předpokládán v následujícím rozsahu:

* Aktuální organizační struktura a systematizace (pracovní místa, pracovní pozice), včetně roční historie
* Celou oblast personalistiky, data zaměstnanců včetně pracovně právní historie, smluv, mzdového zařazení, souvisejících dokumentů apod.

Migrací provádí Dodavatel v rámci dodávky HR systému v předpilotní fázi.

# Školení

* **Školení administrátorů**

Dodavatel zajistí proškolení administrátorů Zadavatele na správu jednotlivých agend HR systému. Administrátoři musí být schopni bez součinnosti Dodavatele řídit přístupy uživatelů k jednotlivým částem HR systému, provádět základní správu systému dle metodiky dodané Dodavatelem.

Předpoládáný rozsah 2 pracovní dny pro max. 3 administrátory

* **Školení garantů**

Dodavatel zajistí proškolení garantů jednotlivých oblastí HR IS, školení může probíhat v prostorách Zadavatele nebo po dohodě i v prostorách Dodavatele, pokud budou na území Prahy. Školení proběhne na základě předané uživatelské dokumentace.

Bude zaměřeno na:

* základní architekturu řešení HR IS;
* základní parametrizaci a konfiguraci modulů HR IS;
* realizaci HR procesů v jednotlivých modulech, půjde zejména o:
  + personalistika (zavedení zaměstnance, změna osobních údajů, vytvoření pracovně právního vztahu a dokumentace)
  + organizační management (zařazení do org. struktury, změny ve struktuře, práce s typovou pozicí a pracovním místem apod.);
  + hodnocení pracovního výkonu;
  + zadání a zpracování podkladů mezd, na základě předchozího hodnocení, zpracování docházky, výpočet mezd, uzávěrkové operace mezd, sestavy a přenos dat do účtárny, vytvoření příkazů do banky a povinné odvody;
  + vzdělávání
  + pracovně lékařské prohlídky
  + docházka
  + benefity
  + správa portálu
  + hlášení a předávání dat - zdravotní pojišťovny a CSSZ;
  + práce s evidenčními a mzdovými listy;
  + práce s kompetenčním modelem a navazujícím hodnocení, stanovování KPIs a cílů;
  + obecná znalost práce se sestavami;
  + opravy záznamů (chybná zadání).

Rozsah školení 3 pracovní dny pro max. 10 zaměstnanců.

* **Školení manažerů**

Dodavatel zajistí proškolení manažerů jednotlivých oblastí manažerského rozhraní, školení může probíhat v prostorách Zadavatele nebo po dohodě i online prostředky Zadavatele. Školení proběhne na základě předané uživatelské dokumentace.

Bude zaměřeno zejména na:

* Základní obsluhu manažerského rozhraní
* Správa osobních údajů, požadavky na personální změny
* Hodnocení pracovního výkonu
* Odměňování a schvalování návrhů odměn, požadavky na mzdové změny
* Rozvoj a vzdělávání pracovníků
* Schvalovací procesy

Rozsah skolení 2 pracovní dny pro max. 60 vedoucích pracovníků.