



## Priloga 5. Arhitektura, integracije in infrastruktura

---

# Kazalo

<b>1</b>	<b>Arhitektura</b>	<b>4</b>
1.1	Splošne smernice in arhitekturni principi IS ADRZ	4
1.2	Arhitekturni pristop	5
1.3	Funkcionalna, komponentna, podatkovna arhitektura	6
1.3.1	Visokonivojska aplikacijska in funkcionalna arhitektura - statični pogled	6
1.3.2	Diagram glavnih podatkovnih tokov - dinamični pogled	8
1.3.3	Porazdeljena obdelava podatkov (ang. grid computing)	9
<b>2</b>	<b>Seznam integracij, povezava s primeri uporabe in funkcionalnimi zahtevami in tehnična analiza integracij</b>	<b>11</b>
2.1	Pridobitev in posodabljanje podatkov o organizacijski strukturi iz IS Kadrovska evidenca	11
2.1.1	Opis integracije	11
2.1.2	Povezani primeri uporabe in funkcionalne zahteve	11
2.1.3	Tehnična analiza integracije	12
2.2	Pridobitev in posodabljanje podatkov o zdravstvenem delavcu iz IS Kadrovska evidenca	12
2.2.1	Opis integracije	12
2.2.2	Povezani primeri uporabe in funkcionalne zahteve	13
2.2.3	Tehnična analiza integracije	13
2.3	Pridobitev in posodabljanje podatkov o opravljenih urah zdravstvenega delavca iz IS Registracija delovnega časa	13
2.3.1	Opis integracije	13
2.3.2	Povezani primeri uporabe in funkcionalne zahteve	14
2.3.3	Tehnična analiza integracije	14
2.4	Pridobitev podatkov o zahtevkih za odsotnost iz IS Kadrovska evidenca	14
2.4.1	Opis integracije	14
2.4.2	Povezani primeri uporabe in funkcionalne zahteve	15
2.4.3	Tehnična analiza integracije	15
2.5	Izvoz podatkov o delovnih razporedih v IS Registracija delovnega časa (IS RDČ)	16
2.5.1	Opis integracije	16
2.5.2	Povezani primeri uporabe in funkcionalne zahteve	16
2.5.3	Tehnična analiza integracije	17
<b>3</b>	<b>Nefunkcionalne zahteve</b>	<b>18</b>
3.1	Avtentikacija in avtorizacija	18
3.1.1	Uporabniške vloge	18
3.1.2	Uporaba varnostne sheme EUEZ	18
3.2	Varnostne zahteve	19
3.2.1	Varnostne zahteve	19
3.2.2	Izvedba varnostnega pregleda	20

3.3	Ostale splošne zahteve glede arhitekture .....	21
3.3.1	Razpoložljivost .....	21
3.3.2	Zanesljivost.....	22
3.3.3	Razširljivost.....	24
3.3.4	Zmogljivost.....	25
3.3.5	Interoperabilnost.....	26
3.3.6	Vzdržljivost .....	27
3.3.7	Prilagodljivost.....	28
4	Infrastruktura .....	30
4.1	Tehnološka infrastruktura .....	30
4.1.1	Okolja in platforma.....	30
4.1.2	Sistem za upravljanje s podatkovno bazo.....	30
4.1.3	Podatkovni center .....	31
4.1.4	Vključitev ADRZ v NIJZ storitveni center .....	31
4.1.5	Interna ADRZ baza podatkov .....	31
4.2	Vhodni podatki za oceno potrebne infrastrukture .....	33

# 1 Arhitektura

## 1.1 Splošne smernice in arhitekturni principi IS ADRZ

Večnivojska arhitektura - IS ADRZ je tro ali večnivojska arhitektura z lahkim odjemalcem (spletnim brskalnikom). Arhitektura IS ADRZ je spletna, več-nivojska (npr. podatkovna zbirka, aplikacijski strežniki, spletni strežniki, spletni brskalnik). IS ADRZ mora delovati brez uporabe posebnih odjemalcev ali vtičnikov.

Modularnost - Informacijska rešitev mora biti zgrajena modularno. Predstavitveni nivo mora biti logično ločen od poslovne logike. Arhitektura mora upoštevati varnostna pravila in dobre prakse s področja informacijske varnosti.

Različni odjemalci - IS ADRZ mora omogočati uporabnikom nemoteno delo z uporabo najpogostejše uporabljenih spletnih odjemalcev: Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari in operacijskih sistemov: Microsoft Windows 11, Linux, Mac OS, brez namestitvenih ali konfiguracijskih posegov na strani odjemalca, vključujoč brskalnik, operacijski sistem ali katerokoli komponento uporabniške delovne postaje. Podprte morajo biti naslednje različice brskalnikov:

- Google Chrome različica 138 in novejše,
- Mozilla Firefox različica 140 in novejše,
- Microsoft Edge različica 138 in novejše,
- Apple Safari različica 18.5 in novejše.

Odprti standardi - V največji možni meri, ki jo še dopušča ciljno izvajalno okolje, naj bodo uporabljeni sodobni, odprti in neodvisni tehnološki standardi in specifikacije pri razvoju spletnih rešitev:

- Odprti standard je dobro dokumentiran in je celotna specifikacija javno dostopna.
- Odprti standard lahko prosto implementiramo brez ekonomskih, političnih ali pravnih omejitev glede implementacije in uporabe.
- Odprti standard je standardiziran in ga vzdržuje odprta neprofitna organizacija v odprtem procesu.

zNET okolje - IS ADRZ bodo primarno uporabljali uporabniki znotraj omrežja zNET, vendar bodo določene funkcionalnosti na voljo uporabnikom na mobilnih napravah izven zNET.

Razširljivost - IS ADRZ ne sme biti zaklenjen na število procesorjev, količino spomina, velikost diska ali na kakršnekoli druge programske in strojne parametre.

Enotna poslovna logika - Poslovna logika in procesiranje istovrstnih opravil in nalog je podprto znotraj ADRZ enkrat in z enotno kodo rešitve ter odprto preko vmesnikov za uporabo drugim modulom znotraj ADRZ, uporabniškim vmesnikom ADRZ, kot tudi navzven proti zunanjim deležnikom skladno z upravljanim in varnim dostopom

Integracija z zavodi - Dostop do ADRZ s strani zunanjim deležnikov mora biti omogočen vsaj na dva načina, ki upošteva, da so zavodi na različni stopnji razvoja svojih informacijskih sistemov (npr. en način preko REST API, drug način preko SFTP izmenjave datotek).

Skalabilnost in samodejno razporejanje - Za poslovno kritične module ali storitve ADRZ, kjer je zahtevana velika razpoložljivost in odzivnost ter občasno bistvena povečana obremenjenost (npr. Modul za samodejno razporejanje) je zahtevana samodejna horizontalna skalabilnost aplikacije in razporejanje opravil, ki omogoča na eni strani tako varčevanje z infrastrukturnimi viri v času manjše obremenjenosti, kot dodajanje virov ob hitrem povečanju obremenjenosti (npr. dnevi v mesecu ko zavodi pripravljajo delovne razporede).

Dostopi do podatkov preko vmesnikov - Dostopi do podatkov drugega modula morajo potekati preko vmesnikov in ne neposredno z dostopom do baze. Vsak modul obvladuje svoje podatke pri čemer lahko vsi moduli uporabljajo določene skupne šifranke (ločen modul), ki so praviloma ravno tako dostopni preko vmesnikov.

Enoten dostop zunanjih sistemov - Zunanji sistemi so z IS ADRZ povezani na način, da IS ADRZ izpostavlja skupne vmesnike in storitve, katerim se prilagajajo in jih uporabljajo zunanji sistemi zavodov (za pošiljanje podatkov, zahtevanje obdelave).

Večnajemniški model - IS ADRZ mora biti zasnovan večnajemniško (ang. multitenant) pri čemer so podatkovni nivoji posameznega zavoda ločeni in medsebojno izolirani. Rešitev lahko uporablja določene skupne šifranke (npr. Šifrant vseh zavodov, Skupna zakonska pravila), evidence ali integracije, ki jih ravno tako nudijo namenski servisi znotraj rešitve in jih vsi moduli uporabljajo enotno. IS ADRZ mora izpolnjevati zahteve večnajemniške arhitekture, kjer so podatki vsakega zdravstvenega zavoda popolnoma ločeni. Za večnajemniški model se lahko uporablja skupna podatkovna baza, vendar uporabniki ne smejo dostopati do podatkov drugih najemnikov. Ob prijavi mora biti jasno določeno, kateremu najemniku pripada uporabnik. Pravice morajo biti določene tako na ravni uporabnika kot na ravni najemnika.

## 1.2 Arhitekturni pristop

Pri IS ADRZ gre za novo rešitev, ki jo bo vzpostavil izbrani zunanji izvajalec, za katerega predvidevamo, da ima vzpostavljene moderne pristope k razvoju programske opreme, kot je DevOps, CI/CD. Predvideva se postopna uvedba IS ADRZ s postopnim večanjem števila uporabnikov, potreb po virih in veliko razliko med posameznimi moduli glede potreb po virih. Hkrati je za določene storitve zahtevana velika fleksibilnost in avtomatska skalabilnost glede na potrebe uporabnikov. Zahtevana je tudi visoka odpornost za napake, ki morajo biti čimbolj lokalizirane in obvladovanje z možnostjo hitrih popravkov neodvisno od drugih delov sistema, saj bodo storitve ADRZ med drugim služile tudi organizacijam, ki so del kritične infrastrukture.

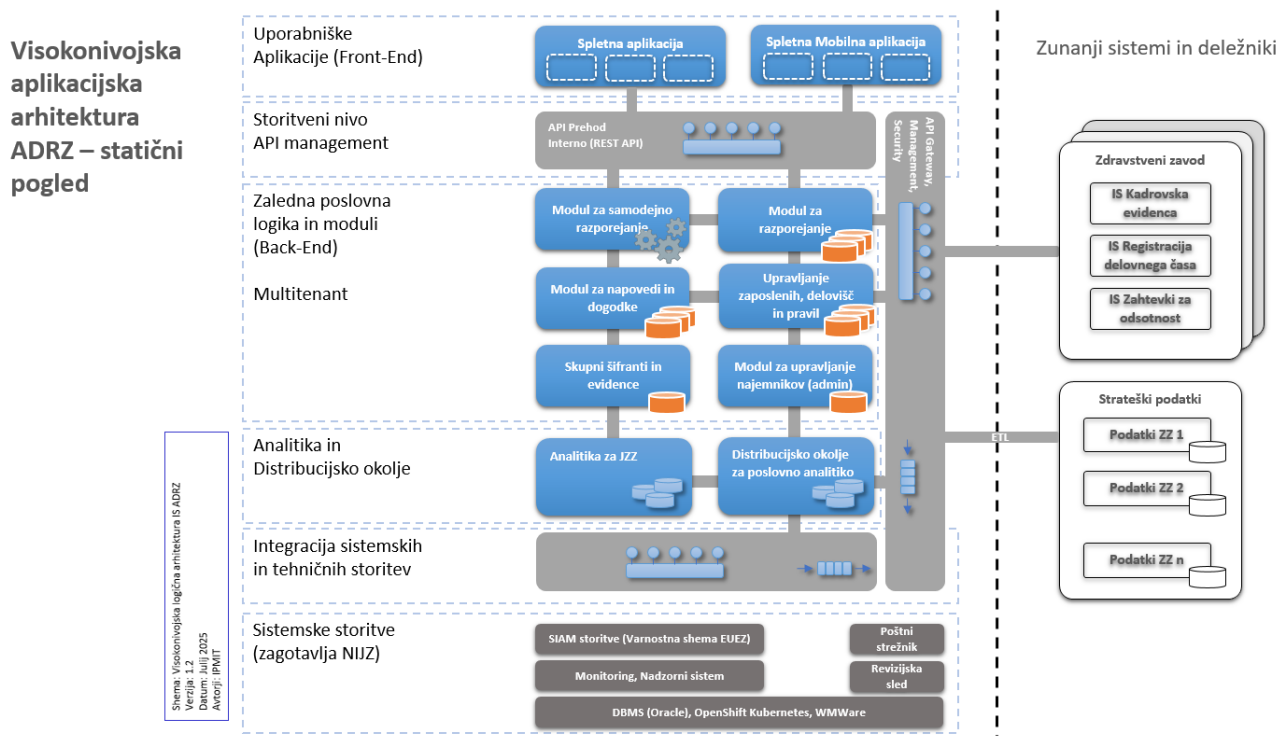
Sistem IS ADRZ bo deloval na infrastrukturi (virtualni strežniki na okolju s hipervizorjem ESX/ESXi, diskovna polja, mrežna oprema, varnostne kopije), s katero upravlja NIJZ.

Ponudnik mora upoštevati infrastrukturno postavitev in omejitve naročnikovega okolja (predstavljeno v tem dokumentu), ki ga naročnik zagotavlja in zanj izvaja procese za zagotavljanje ustreznega nivoja storitev.

## 1.3 Funkcionalna, komponentna, podatkovna arhitektura

### 1.3.1 Visokonivojska aplikacijska in funkcionalna arhitektura - statični pogled

Naslednja shema predstavlja visokonivojsko aplikacijsko arhitekturo ADZ, na kateri so razvidni glavni logični funkcionalni moduli, ki nudijo storitve tako predstavitevsem nivoju, kot tudi zunanjimi sistemom preko enotnih vmesnikov. Ponudnik mora zagotoviti najmanj predstavljeno delitev na pod-module, podrobnejša granularija na pod-module ali storitve je v domeni izbranega ponudnika glede na predlagano arhitekturo rešitve in izbrano tehnologijo.



Slika: Visokonivojska aplikacijska arhitektura - statični pogled

#### 1.3.1.1 Opisi modulov

##### Modul za razporejanje

Modul za razporejanje je osrednji modul za obvladovanje delovnih razporedov. Nudi storitve ročne priprave delovnih razporedov, izvajanje kontrol in skladnosti razporedov s postavljenimi pravili za določen zavod in skladnost z zakonskimi opravili, izvaja obveščanje deležnikov o delovnih razporedih in morebitnih spremembah, komunicira z modulom za samodejno razporejanje, od katerega zahteva pripravo delovnega razporeda ob danih vhodnih parametrih.

Modul obvladuje svoje podatke o delovnih razporedih in so za vsak zavod ločeni.

##### Modul za samodejno razporejanje

Modul za samodejno razporejanje je procesorsko in spominsko najzahtevnejši gradnik. Ob danih vhodnih parametrih, ki jih zahtevajo drugi moduli ali zunanji deležniki mora uporabniku v zahtevanem času predlagati optimalen delovni razpored za določeno delovišče, ob upoštevanju omejitev in pravil,

ki veljajo za ta zavod. Rezultat obdelave in optimizacije je delovni raspored ter seznam kršitev postavljenih pravil in omejitev, v kolikor priprava delovnega rasporeda brez teh ni bila možna. Predlagan delovni raspored lahko uporabnik nadalje spreminja in ročno prilagaja v Modulu za razporejanje.

Modul praviloma ne bo imel trajnejše hrambe podatkov, ker bo vse vhodne podatke o zavodu, razporedu, omejitvah in pravilih pridobil preko vhodnega klica storitve.

Za izračun delovnega rasporeda IS ADRZ oziroma modul za samodejno razporejanje ne sme uporabljati zunanjih storitev (plačljivih ali brezplačnih), ki niso del IS ADRZ in modula za samodejno razporejanje. Vsi izračuni delovnega rasporeda morajo biti izvedeni v okviru modula za samodejno razporejanje, ki je del IS ADRZ in nameščen na infrastrukturi kot navedeno v poglavju 4.1 Tehnološka infrastruktura.

Upravljanje zdravstvenih delavcev, delovišč in pravil

Modul je namenjen za urejanje pretežno statičnih podatkov o zavodih, zdravstvenih delavcih, deloviščih in pravilih zavoda. Predvidoma ne bo vključeval procesne logike oz. podpore delovnim procesom, ampak v večjem delu samo urejanje navedenih podatkov.

Vsak zavod bo imel svoj ločen del podatkov, ki je značilen samo zanj in neodvisen od drugih zavodov.

Modul za napovedi in dogodke

Modul je namenjen podpori določenim delovnim procesom, kot tudi evidentiranju že odločenih dogodkov v zvezi z zdravstvenimi delavci, delovišči ipd., ki jih zavodi že uskladijo in potrdijo v okviru svojega informacijskega sistema. Omogočeno bo sprejemanje napovedi za različne odsotnosti in spremembe, obravnava teh napovedi skladno s procesnim tokom (npr. potrditev odsotnosti) ter obveščanje deležnikov o odločitvah.

Osnovna procesna logika bo enaka za vse zavode pri čemer morajo biti določeni parametri delovanja in izvajanja procesov biti nastavljivi za vsak zavod ločeno (npr. rok za oddajo napovedi, čas za potrditev napovedi, obvestilo za zdravstvenega delavca, obvestilo za nadrejenega).

Skupni šifranti in evidence

Gre za modul, ki na enem mestu zagotavlja skupne šifrante, evidence in druge enostavne zbirke podatkov, ki jih enotno uporabljajo drugi moduli ali zunanji deležniki preko vmesnikov.

Distribucijsko okolje za poslovno analitiko

Distribucijsko okolje je namenjeno zbiranju surovih podatkov o delovnih razporedih za potrebe nadaljnje poslovne analitike in zunanje platforme "Strateški podatki".

Modul ne bo smel obremenjevati ostalih modulov v času njihove največje obremenitve. Modul bo hranil podatke za določeno (nastavljivo) obdobje. Podatki bodo za zunanje deležnike in zajem v poročilne sisteme dostopni preko vmesnikov.

Analitika za JZZ

IS ADRZ mora omogočati obdelavo, prikaz in pripravo poročil nad podatki, ki se zbirajo v IS, kot je to določeno v funkcionalnih zahtevah (npr. konfiguracija poročil, izvoz poročila). Na področju poročanja o delovnih razporedih morajo biti uporabnikom glede na njihove pravice na voljo poročila, ki zajemajo različne podatke in dimenzije (npr. število izdelanih delovnih razporedov, število spremenjenih delovnih razporedov, strošek oziroma vrednost delovnega rasporeda).

### Notranji API prehod

Notranji API prehod ali širše integracijska komponenta skrbi za varno, standardizirano in nadzorovano komunikacijo med posameznimi moduli znotraj IS ADRZ. Omogoča usmerjanje zahtev, validacijo vhodnih podatkov, nadzor nad klici ter centralizirano spremljanje napak in zmogljivosti. Omogoča notranjo avtentikacijo in avtorizacijo (npr. s pomočjo tokenov). Podpira različne komunikacijske protokole (REST, gRPC, event bus) ter omogoča transakcijsko doslednost, če je potrebna. Ključna funkcionalnost je tudi odkrivanje storitev (ang. service discovery) in avtomatska registracija storitev. Vpelje lahko tudi enostavno orkestracijo med moduli, če je smiselna. Lahko deluje kot del internega "service mesh" sistema. Deluje v istem omrežnem okolju kot storitve in ni izpostavljena navzven. Cilj je povečati robustnost, standardizacijo in zmanjšati povezanost (ang. de-coupling) med notranjimi komponentami (moduli).

### API prehod za integracijo znotraj zNET in zunaj

Integracijska komponenta in upravljanje integracij predstavlja varno in kontrolirano vstopno točko za zunanje sisteme, ki dostopajo do storitev ADRZ prek API-jev ali spletnih storitev. Omogočati mora dostop za sisteme znotraj zNET (zavodi), kot tudi zunaj zNET (za potrebe uporabniških aplikacij, ki jih bodo uporabniki uporabljali izven zNET). Lahko gre za dve ločeni komponenti in postavitvi. Poskrbljeno mora biti za avtentikacijo in avtorizacijo (prek varnostne sheme EUEZ), validacijo vhodnih zahtevkov, kontrolo dostopa in zaščito notranjih storitev pred zlorabo ali preobremenitvijo. Lahko izvaja transformacijo podatkovnih formatov (npr. XML ↔ JSON) in poenotenje različnih zunanjih zahtev. Omogoča nadzor nad dostopom posameznih partnerjev, beleženje klicev (audit log) in spremljanje SLA parametrov. Vključen mora biti mehanizem za verzioniranje API-jev in varno objavo sprememb. Njena glavna naloga je zaščita notranjega sistema in omogočanje standardiziranega dostopa za zunanje partnerje.

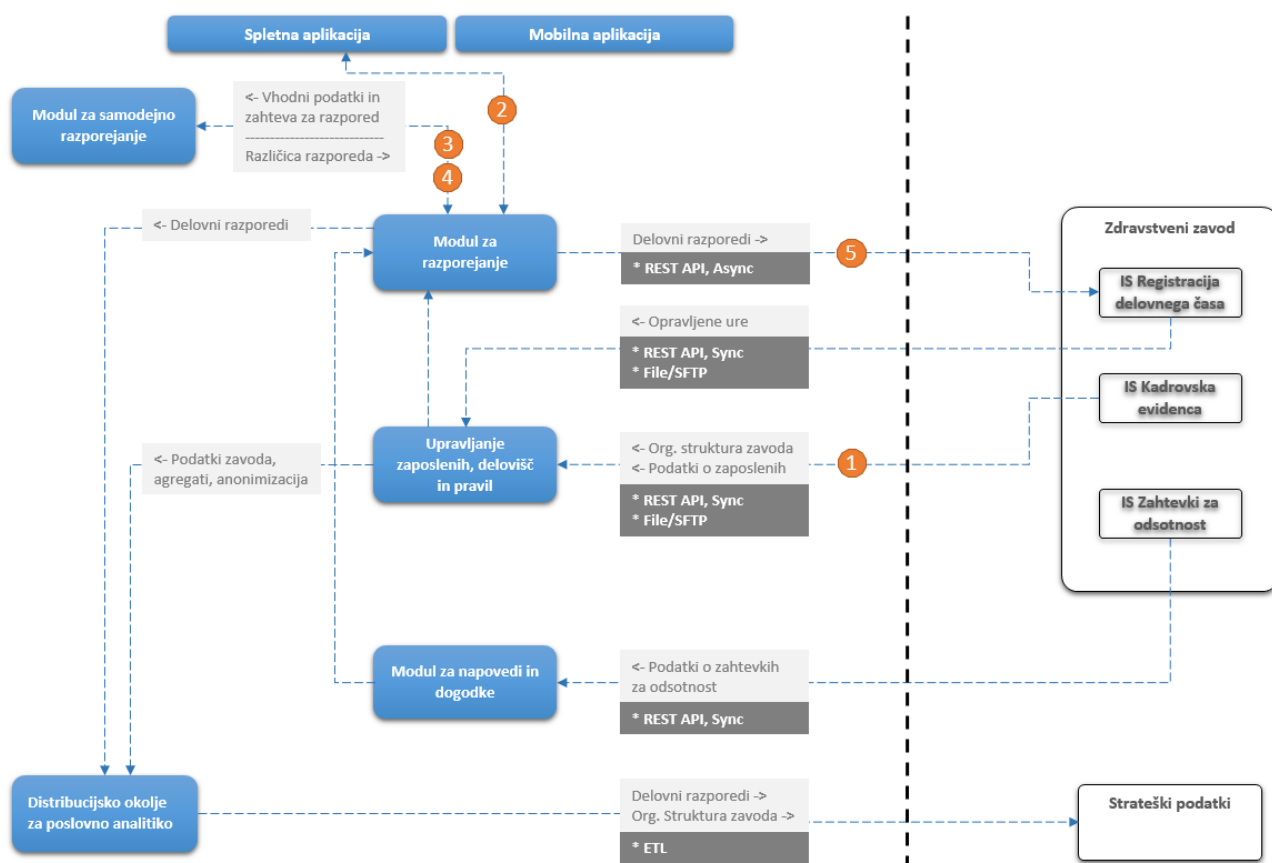
### Sistemske storitve NIJZ

Sistemske storitve NIJZ so storitve, ki jih zagotavlja NIJZ in jih lahko uporabi izbrani izvajalec v sklopu svoje rešitve. NIJZ ima za ponujene storitve na voljo ustrezne licence in kupljeno vzdrževanje za nudenje ustrezne ravni storitve. Dejanska uporaba storitev NIJZ mora biti predstavljena v podrobnih načrtih rešitve ter usklajena z NIJZ tako v testni kot produkcijski fazi.

## 1.3.2 Diagram glavnih podatkovnih tokov - dinamični pogled

Naslednji diagram prikazuje glavne podatkovne tokove med posameznimi deli sistema (moduli) IS ADRZ in zunanjimi deležniki - gre za dinamični pogled na arhitekturo. Povezave med posameznimi moduli ali storitvami prikazujejo smer pretoka podatkov, glavne sklope poslovnih podatkov, ki se med njimi prenašajo ter predlagan način integracije (npr. REST API).





Slika: Visokonivojska aplikacijska arhitektura - dinamični pogled

Primer delovnega toka – opis korakov glede na oznake od 1 – 5 na zgornji sliki:

1. Zavod preko vmesnikov določi nove nastavitve za delovišča, delovna mesta in zdravstvene delavce v ADRZ. Pravila in zakonske omejitve so že določene.
2. Načrtovalec delovnih razporedov se preko namenske ADRZ spletne aplikacije dostopa do Modula za razporejanje, kjer vidi zadnje razporede. Z izbrano akcijo zahteva izdelavo novega razporeda, ki bo upošteval nova dejstva (npr. nastavitve delovišč, nove dopuste in druge odsotnosti).
3. Zahteva za izdelavo novega razporeda se pošlje v Modul za samodejno razporejanje, ki izračuna in predlaga optimalni razpored pri čemer upošteva vse potrebne podatke delovišča, delovnih mest, zdravstvenih delavcev, že opravljenih ur v tem obdobju, odsotnosti, pravil in omejitev.
4. Modul za samodejno razporejanje vrne predlagan razpored, ki ga načrtovalec pregleda in po potrebi dopolni v Modulu za razporejanje. Po potrditvi postane razpored veljaven. Isto akcijo lahko načrtovalec izvede tudi preko vmesnikov.
5. Informacijski sistem zavoda lahko preko vmesnikov prenese potrjen razpored v svoj informacijski sistem kot veljaven.

### 1.3.3 Porazdeljena obdelava podatkov (ang. grid computing)

V okviru predmetnega javnega naročila naročnik dopušča možnost, da ponujena rešitev vključuje funkcionalnost za porazdeljeno obdelavo podatkov (ang. grid computing), s čimer se omogoči

razbremenitev centralnega strežniškega sistema in prenos določenih obdelovalnih nalog na računalnike končnih uporabnikov (odjemalcev). Minimalne tehnične zahteve v tem primeru arhitekture so naslednje:

- Rešitev omogoča dinamično razporejanje obdelovalnih nalog na razpoložljive odjemalske naprave, ob upoštevanju njihove trenutne obremenitve in zmogljivosti.
- Obdelava na strani odjemalca je varna, zanesljiva in nadzorovana, z možnostjo prekinitve ali ponovnega zagona nalog.
- Sistem omogoča centralizirano upravljanje in spremljanje izvajanja porazdeljenih nalog (npr. prek nadzorne plošče ali API-ja).
- Rešitev vključuje mehanizme za zaščito podatkov med prenosom in obdelavo (npr. šifriranje).
- Odjemalska komponenta je kompatibilna vsaj z operacijskim sistemom Windows 11 in z vsemi novejšimi različicami Microsoft operacijskega sistema Windows ali pa je rešitev zasnovana kot platformno neodvisna (npr. prek spletnega brskalnika ali kontejnerske tehnologije).

Opcijska zahteva po porazdeljeni obdelavi na strani odjemalcev izhaja iz potrebe po učinkovitejši rabi razpoložljivih virov, zmanjšanju obremenitve centralne infrastrukture ter povečanju zmogljivosti in odzivnosti sistema.

## 2 Seznam integracij, povezava s primeri uporabe in funkcionalnimi zahtevami in tehnična analiza integracij

### 2.1 Pridobitev in posodabljanje podatkov o organizacijski strukturi iz IS Kadrovska evidenca

#### 2.1.1 Opis integracije

IS Kadrovska evidenca samodejno posreduje podatke o organizacijski strukturi zdravstvenega zavoda v IS ADRZ.

IS Kadrovska evidenca s klicem vmesnika IS ADRZ redno dnevno prenese spremembe organizacijske strukture. Ključ za prenos podatkov je oznaka (šifra) organizacijske enote v IS Kadrovska evidenca, ki je enolična na ravni zdravstvenega zavoda. Iz IS Kadrovska evidenca v IS ADRZ se prenesejo naslednji podatki:

- Oznaka (šifra) organizacijske enote v IS Kadrovska evidenca: Če OE z oznako že obstaja v IS ADRZ, se obstoječi zapis v IS ADRZ ažurira s podatki iz IS Kadrovska evidenca. Če OE z oznako v IS ADRZ še ne obstaja, se kreira nov OE v IS ADRZ in prenesejo vsi podatki iz IS Kadrovska evidenca.
- Naziv organizacijske enote,
- Oznaka nadrejene organizacijske enote,
- Oznaka vodje organizacijske enote (enaka oznaka kot se uporablja pri zdravstvenem delavcu),
- Datum in ura zadnje spremembe.

#### 2.1.2 Povezani primeri uporabe in funkcionalne zahteve

##### 2.1.2.1 *Povezani primeri uporabe*

Integracija je povezana z naslednjim primerom uporabe:

- Priprava podatkov o organizacijski strukturi zavoda (glej dokument Priloga 2. Primeri uporabe, poglavje 5.1).

##### 2.1.2.2 *Povezane funkcionalne zahteve*

Integracija je povezana z naslednjimi funkcionalnimi zahtevami:

- Urejanje organizacijske strukture zdravstvenega zavoda (glej dokument Priloga 3. Funkcionalne zahteve, poglavje 3.8).

### 2.1.3 Tehnična analiza integracije

- Podatkovni vir: Vir podatkov je IS Kadrovska evidenca zdravstvenega zavoda
- Podatkovno strukturo klica: Glej seznam podatkov pri opisu integracije
- Opredelitev zahtev glede uporabe standardnih protokolov za komunikacijo in izmenjavo podatkov. Tehnična izvedba integracije: IS Kadrovska evidenca izvede klic metode z imenom npr. PosodobiOrganizacijskoStrukturo na REST API vmesniku IS ADRZ. Vmesnik na strani IS ADRZ na podlagi ključa ter datuma in ure spremembe ustrezno posodobi podatke.
- Frekvenca osveževanja podatkov: Podatki se osvežijo dnevno glede na nastavljeno periodo. Obstaja možnost ročnega zagona osvežitve na strani IS Kadrovska evidenca za posamezen zdravstveni zavod. Obstaja možnost vpogleda v zgodovino prenosov na strani IS ADRZ in po možnosti tudi na strani kadrovskega sistema.
- Prožilec osvežitve (dogodek, časovna perioda): Glej predhodno alinejo.

## 2.2 Pridobitev in posodabljanje podatkov o zdravstvenem delavcu iz IS Kadrovska evidenca

### 2.2.1 Opis integracije

IS Kadrovska evidenca samodejno posreduje podatke o zdravstvenih delavcih v IS ADRZ.

IS Kadrovska evidenca redno dnevno prenese nove zdravstvene delavce v IS ADRZ in vse spremenjene podatke o zdravstvenih delavcih. Ključ za prenos podatkov je enolična oznaka zdravstvenega delavca na ravni zdravstvenega zavoda iz IS Kadrovske evidence, ki jo uskladi naročnik in izvajalec. Iz IS Kadrovska evidenca v IS ADRZ se prenesejo naslednji podatki:

- Številka RIZDDZ: RIZDDZ št. delavca je dodeljena zdravstvenim delavcem in sodelavcem, ki redno ali pogodbeno (kot zunanji sodelavci) opravljajo svoj poklic pri izvajalcih zdravstvene dejavnosti.
- Oznaka (šifra) zdravstvenega delavca v IS Kadrovska evidenca,
- Ime in priimek,
- Spol,
- Datum zaposlitve oziroma začetka pogodbenega sodelovanja,
- Datum prenehanja zaposlitve oziroma pogodbenega sodelovanja,
- Vrsta pogodbe (redna zaposlitev, podjemna pogodba, dopolnilno delo, pogodba, študentsko delo)
- Obseg zaposlitve: 40 ur oziroma 36 ur za polni delovni čas, delovni čas v zmanjšanem obsegu, Delovni čas za tiste, ki niso razpoložljivi vse dni v tednu
- Oznaka organizacijske enote zdravstvenega delavca,
- Število ur odmerjenega dopusta za tekoče koledarsko leto,
- Število ur neizkoriščenega dopusta za preteklo koledarsko leto,
- Vrednost osnovne urne postavke zdravstvenega delavca,
- Podatki o omejitvah,
- Podatki o soglasjih,
- Datum in ura zadnje spremembe podatkov o zdravstvenem delavcu.

## 2.2.2 Povezani primeri uporabe in funkcionalne zahteve

### 2.2.2.1 Povezani primeri uporabe

Integracija je povezana z naslednjim primerom uporabe:

- Priprava podatkov o zdravstvenih delavcih (glej dokument Priloga 2. Primeri uporabe, poglavje 1.2).

### 2.2.2.2 Povezane funkcionalne zahtev

Integracija je povezana z naslednjimi funkcionalnimi zahtevami:

- Urejanje podatkov o zdravstvenem delavcu (glej dokument Priloga 3. Funkcionalne zahteve, poglavje 3.2)

## 2.2.3 Tehnična analiza integracije

- Podatkovni vir: Vir podatkov je IS kadrovska evidenca posameznega zdravstvenega zavoda
- Podatkovno strukturo klica: Glej seznam podatkov pri opisu integracije
- Opredelitev zahtev glede uporabe standardnih protokolov za komunikacijo in izmenjavo podatkov. Tehnična izvedba integracije: IS Kadrovska evidenca izvede klic metode z imenom npr. PosodobiZaposlene na REST API vmesniku IS ADRZ. Vmesnik na strani IS ADRZ na podlagi ključa ter datuma in ure spremembe ustrezno posodobi podatke.
- Frekvenco osveževanja podatkov: Podatki se osvežijo dnevno glede na nastavljeno periodo. Obstaja možnost ročnega zagona osvežitve na strani IS Kadrovska za posamezen zdravstveni zavod. Obstaja možnost vpogleda v zgodovino prenosov na strani IS ADRZ in po možnosti tudi na strani kadrovskega sistema.
- Prožilec osvežitve (dogodek, časovna perioda): Glej predhodno alinejo.

## 2.3 Pridobitev in posodabljanje podatkov o opravljenih urah zdravstvenega delavca iz IS Registracija delovnega časa

### 2.3.1 Opis integracije

IS Registracija delovnega časa samodejno posreduje podatke o dejansko opravljenih urah zdravstvenega delavca v IS ADRZ.

IS Registracija delovnega časa redno dnevno prenese stanje opravljenih ur zdravstvenega delavca v IS ADRZ. Ključ za prenos podatkov je enolična oznaka zdravstvenega delavca na ravni zdravstvenega zavoda iz IS Kadrovske evidence, ki jo uskladiata naročnik in izvajalec. Iz IS Registracija delovnega časa v IS ADRZ se prenesejo naslednji podatki za vsakega zdravstvenega delavca:

- Datum in ura prenosa podatka,
- Število ur v mesecu (v trenutku prenosa),

- Število nadur (v trenutku prenosa),
- Drugi podatki.

### 2.3.2 Povezani primeri uporabe in funkcionalne zahteve

#### 2.3.2.1 *Povezani primeri uporabe*

Integracija je povezana z naslednjim primerom uporabe:

- Priprava podatkov o zdravstvenih delavcih (glej dokument Priloga 2. Primeri uporabe, poglavje 1.2).

#### 2.3.2.2 *Povezane funkcionalne zahteve*

Integracija je povezana z naslednjimi funkcionalnimi zahtevami:

- Urejanje podatkov o zdravstvenem delavcu (glej dokument Priloga 3. Funkcionalne zahteve, poglavje 3.2)

### 2.3.3 Tehnična analiza integracije

- Podatkovni vir: Vir podatkov je IS Registracija delovnega časa posameznega zdravstvenega zavoda
- Podatkovno strukturo klica: Glej seznam podatkov pri opisu integracije
- Opredelitev zahtev glede uporabe standardnih protokolov za komunikacijo in izmenjavo podatkov. Tehnična izvedba integracije: IS Registracija delovnega časa izvede klic metode PosodobiZaposlene na REST API vmesniku IS ADRZ. Vmesnik na strani IS ADRZ na podlagi ključa ter datuma in ure spremembe ustrezno posodobi podatke.
- Frekvenco osveževanja podatkov: Podatki se osvežijo dnevno glede na nastavljeno periodo. Obstaja možnost vpogleda v zgodovino prenosov na strani IS ADRZ in po možnosti tudi na strani sistema.
- Prožilec osvežitve (dogodek, časovna perioda): Glej predhodno alinejo.

## 2.4 Pridobitev podatkov o zahtevkih za odsotnost iz IS Kadrovska evidenca

### 2.4.1 Opis integracije

IS Kadrovska evidenca samodejno posreduje podatke o zahtevkih za odsotnost v IS ADRZ. Pogoji za pridobivanje podatkov o zahtevkih za odsotnost je, da so tudi podatki o zdravstvenih delavcih preneseni iz IS Kadrovska evidenca.

IS Kadrovska evidenca periodično (v skladu z nastavitvami) prenese nove zahtevke za odsotnost v IS ADRZ in vse spremenjene zahtevke za odsotnost. Ključ za prenos podatkov je oznaka (šifra) zahtevka

za odsotnost v IS Kadrovska evidenca, ki je enolična na ravni zdravstvenega zavoda. Iz IS Kadrovska evidenca v IS ADRZ se prenesejo naslednji podatki:

- Oznaka (šifra) zahtevka za odsotnost v IS Kadrovska evidenca: Če zahtevke za odsotnost z oznako že obstaja v IS ADRZ, se obstoječi zapis v IS ADRZ ažurira s podatki iz IS Kadrovska evidenca. Če zahtevke za odsotnost z oznako v IS ADRZ še ne obstaja, se kreira nov zahtevke za odsotnost v IS ADRZ in prenesejo vsi podatki iz IS Kadrovska evidenca.
- Številka RIZDDZ,
- Oznaka (šifra) zdravstvenega delavca v IS Kadrovska evidenc,
- Ime in priimek,
- Datum oddaje oziroma zadnje spremembe,
- Datum od,
- Datum do,
- Vrsta odsotnosti,
- Status.

Uvozijo se zahtevki, ki imajo status, da jih je potrdil vodja oddelka.

## 2.4.2 Povezani primeri uporabe in funkcionalne zahteve

### 2.4.2.1 Povezani primeri uporabe

Integracija je povezana z naslednjim primerom uporabe:

- Posredovanje zahtevka za odsotnost (glej dokument Priloga 2. Primeri uporabe, poglavje 2.4).

### 2.4.2.2 Povezane funkcionalne zahteve

Integracija je povezana z naslednjimi funkcionalnimi zahtevami:

- Zahtevki za odsotnost (glej dokument Priloga 3. Funkcionalne zahteve, poglavje 2.2).

## 2.4.3 Tehnična analiza integracije

- Podatkovni vir: Vir podatkov je IS Zahtevki za odsotnost posameznega zdravstvenega zavoda
- Podatkovno strukturo klica: Glej seznam podatkov pri opisu integracije
- Opredelitev zahtev glede uporabe standardnih protokolov za komunikacijo in izmenjavo podatkov. Tehnična izvedba integracije: IS Kadrovska evidenca izvede klic metode z imenom npr. PosodobiZahtevkiZaOdsotnost na REST API vmesniku IS ADRZ. Vmesnik na strani IS ADRZ na podlagi ključa ter datuma in ure spremembe ustrezno posodobi podatke.
- Frekvenco osveževanja podatkov: Podatki se osvežijo glede na nastavljeno periodo enkrat na uro. Obstaja možnost ročnega zagona osvežitve na strani IS Kadrovska evidenca za posamezen zdravstveni zavod. Obstaja možnost vpogleda v zgodovino prenosov na strani IS ADRZ in po možnosti tudi na strani kadrovskega sistema.
- Prožilec osvežitve (dogodek, časovna perioda): Glej predhodno alinejo.

## 2.5 Izvoz podatkov o delovnih razporedih v IS Registracija delovnega časa (IS RDČ)

### 2.5.1 Opis integracije

V IS RDČ je treba prenesti podatke o delovnem razporedu oziroma delovnih razporedih na ravni zdravstvenega zavoda. Podatke o delovnih razporedih je treba prenesti ob vsaki potrditvi (objavi) delovnega razporeda in ob potrditvi (objavi) vsake spremembe delovnega razporeda. Iz IS ADRZ v IS RDČ se prenesejo podatki za vsako izmeno v okviru delovnega razporeda:

- Številka RIZDDZ: RIZDDZ št. delavca je dodeljena zdravstvenim delavcem in sodelavcem, ki redno ali pogodbeno (kot zunanji sodelavci) opravljajo svoj poklic pri izvajalcih zdravstvene dejavnosti.
- Oznaka (šifra) zdravstvenega delavca v IS Kadrovska evidenca,
- Oznaka delovnega razporeda v IS RDČ (v IS ADRZ se izvede transformacija),
- Začetek izmene datum in ura,
- Konec izmene datum in ura,
- Dodatek za mentorstvo,
- Dodatek za nevarno delovišče.

Podatki se prenesejo iz IS ADRZ v IS RDČ ob vsaki spremembi delovnega razporeda.

Navedeni podatki delovnega razporeda se prenesejo iz IS ADRZ v IS RDČ z namenom usklajevanja podatkov delovnega razporeda in podatkov evidentiranja delovnega časa. Predpostavka je, da se usklajevanje kršitev / odstopanj izvaja v IS RDČ in ta funkcionalnost ni zahtevana v IS ADRZ.

### 2.5.2 Povezani primeri uporabe in funkcionalne zahteve

#### 2.5.2.1 *Povezani primeri uporabe*

S funkcionalnostjo so povezani naslednji primeri uporabe:

- Samodejno ustvarjanje delovnega razporeda (glej dokument Priloga 2. Primeri uporabe, poglavje 1.6).
- Samodejno spreminjanje delov razporeda (glej dokument Priloga 2. Primeri uporabe, poglavje 1.7).
- Ročno spreminjanje delov razporeda (glej dokument Priloga 2. Primeri uporabe, poglavje 1.8).
- Ročno ustvarjanje delovnega razpored (glej dokument Priloga 2. Primeri uporabe, poglavje 1.9).
- Pregled in potrjevanje delovnih razporedov (glej dokument Priloga 2. Primeri uporabe, poglavje 3.2).

#### 2.5.2.2 *Povezane funkcionalne zahteve*

Integracija je povezana z naslednjimi funkcionalnimi zahtevami:



- Potrjevanje in objava delovnega razporeda (glej dokument Priloga 3. Funkcionalne zahteve, poglavje 1.5).

### 2.5.3 Tehnična analiza integracije

- Podatkovni vir: Vir podatkov je IS ADRZ.
- Podatkovno strukturo klica: Glej seznam podatkov pri opisu integracije.
- Opredelitev zahtev glede uporabe standardnih protokolov za komunikacijo in izmenjavo podatkov. Tehnična izvedba integracije: IS ADRZ izvede klic API vmesnika IS Registracija delovnega časa na zdravstvenem zavodu. IS RDČ na podlagi ključa ustrezno posodobi podatke o delovnih razporedih.
- Frekvenco osveževanja podatkov: Podatki se osvežijo ob vsaki spremembi delovnega razporeda oziroma novem delovnem razporedu. Obstaja možnost vpogleda v zgodovino prenosov na strani IS ADRZ in po možnosti tudi na strani kadrovskega sistema.
- Prožilec osvežitve (dogodek, časovna perioda): Glej predhodno alinejo.

## 3 Nefunkcionalne zahteve

### 3.1 Avtentikacija in avtorizacija

#### 3.1.1 Uporabniške vloge

IS ADRZ podpira vsaj naslednje uporabniške vloge:

- načrtovalec delovnih razporedov,
- vodja oddelka,
- zdravstveni delavec,
- administrator na ravni celotnega IS ADRZ,
- administrator na ravni zdravstvenega zavoda.

Podrobnosti glede uporabniških zgodb, procesov in funkcionalnosti, ki jih uporablja posamezna vloga so razvidne v naslednjih dokumentih:

- Tehnična specifikacija IS ADRZ definira nabor uporabniških vlog.
- Priloga 1. Uporabniške zgodbe definirajo uporabniške zgodbe po uporabniških vlogah.
- Priloga 2. Primeri uporabe definirajo primere uporabe za posamezne uporabniške vloge.
- Priloga 3. Funkcionalne zahteve definirajo funkcionalnosti za posamezne uporabniške vloge.

#### 3.1.2 Uporaba varnostne sheme EUEZ

IS ADRZ omogoča prijavo uporabnikov prek obstoječe varnostne sheme (EueZ) v sklopu eZdravja, ki za avtentikacijo uporablja mehanizem SAML 2.0 oz. OpenID Connect ter povezavo prek omrežja zNET.

Uporabniške vloge, omenjene v poglavju 3.1.1 Uporabniške vloge, se v celoti naslanjajo na varnostno shemo EUEZ. IS ADRZ ne vodi lastnega seznama uporabniških vlog, temveč slednje uporabi iz EUEZ skladno s pooblastili.

Ponudnik IS ADRZ specifikira točen šifrant uporabniških vlog in ga komunicira z NIJZ zato, da ta v varnostno shemo EUEZ doda »IS ADRZ uporabniške vloge«. Članstvo ureja nadzornik organizacije v posameznem zdravstvenem zavodu. Ponudnik IS ADRZ predvidi, da lahko naročnik v prihodnosti zahteva dodatne uporabniške vloge, ki bodo usklajene z EUEZ (tj. ponudnik uskladi z NIJZ vse uporabniške vloge, tudi nove). Zato EUEZ z ustreznim grafičnim vmesnikom omogoča naknadno dodajanje poljubnih uporabniških vlog v IS ADRZ (ki so usklajene z naročnikom) ter poskrbi, da je možno z matriko dodeljevati dostope do posameznih funkcionalnosti znotraj IS ADRZ (omenjenim novim in že obstoječim) uporabniškim vlogam.

V primeru, da določene granulacije vlog EUEZ še ne podpira, ponudnik IS ADRZ v dogovoru z NIJZ izvede razširitev vlog varnostne sheme za potrebe IS ADRZ tako, da bo moč podpreti vse potrebne Uporabniške vloge.

Upravljanje z uporabniki IS ADRZ izvaja po posameznem zdravstvenem zavodu nadzornik organizacije (vloga VS\_NADZORNIK\_ORGANIZACIJE). Upravljanje z vlogami se v celoti izvaja prek varnostne sheme EUEZ, ki je integrirana z IS ADRZ in na voljo uporabnikom.

Prijava uporabnika v IS ADRZ prek EUEZ je omogočena z uporabo enega ali več prijavnih mehanizmov:

- digitalno potrdilo, pri čemer lahko uporabnik uporabi vsa v Sloveniji priznana kvalificirana digitalna potrdila (SIGEN-CA, AC-NLB, HALCOM-CA, POŠTAR-CA, SIGOV-CA, REKONO-CA),
- s profesionalno kartico (PK): dovoljena je uporaba digitalnih potrdil, ki se nahajajo na ZZZS profesionalnih karticah (PK) in sicer tako PK-KDP (kvalificirano digitalno potrdilo) kot tudi PK-NDP (nekvalificirano digitalno potrdilo izdajatelja ZZZS-CA), v skladu s pravili ZZZS,
- z elektronsko osebno izkaznico in čitalnikom tovrstnih kartic (lahko je vgrajen v napravo),
- z elektronsko osebno izkaznico in mobilno aplikacijo eOsebna.

Pri uporabi digitalnega potrdila, bodisi enega izmed vseh v Sloveniji priznanih kvalificiranih digitalnih potrdil, bodisi tistega na PK, je potrebno zagotoviti, da so potrdila dostopna in funkcionalna na vseh napravah, ki podpirajo delovanje IS ADRZ, vključno s tabličnimi računalniki in mobilnimi telefoni.

V primeru, da ima uporabnik uporabniške vloge / pravice pri različnih zdravstvenih zavodih, IS ADRZ upošteva, v kateri zdravstveni ustanovi se trenutno uporablja. IS ADRZ upošteva uporabnikov dostop do podatkov skladno s pravicami, ki jih prejme v sklopu prijavnih mehanizmov iz EUEZ. V avtorizacijskem žetonu, ki ga izda varnostna shema EUEZ IS ADRZ se pridobi / je zapisan podatek o pravicah za vse zdravstvene zavode, s tem da je za vsako pravico navedeno, za kateri zdravstveni zavod pravica velja. IS ADRZ, ki prejme avtorizacijski žeton, mora vedeti, za kateri zdravstveni zavod je bil zahtevan žeton in iz spiska pravic izluščiti tiste, ki so relevantni za posamezni zdravstveni zavod. Opcijsko lahko IS ADRZ zahteva avtorizacijski žeton samo za določeni zdravstveni zavod in v tem primeru bo varnostna shema EUEZ v žetonu navedla pravice za zahtevani zdravstveni zavod in IS ADRZ.

## 3.2 Varnostne zahteve

### 3.2.1 Varnostne zahteve

Informacijska rešitev mora biti izdelana z upoštevanjem predpisov, ki urejajo področje informacijske varnosti ter vseh dobrih praks in ustreznih rešitev, ki zagotavljajo visoko stopnjo informacijske varnosti. Rešitev ne sme imeti ranljivosti po OWASP TOP 10 seznamu. Informacijska rešitev mora prestati vsa varnostna testiranja, ki so predpisana v postopku gostovanja, vse morebitne odkrite pomanjkljivosti mora ponudnik IS ADRZ odpraviti pred začetkom produkcijske uporabe.

Upravljelec infrastrukture lahko zahteva ponovno preverjanje od ponudnika IS ADRZ kadarkoli kasneje v življenjskem ciklu IS ADRZ. Ponudnik IS ADRZ mora pomanjkljivosti odpraviti v čim krajšem možnem času. V primeru, da ponudnik IS ADRZ pomanjkljivosti ne odpravi, se lahko upravljelec infrastrukture posluži ustreznih, nujnih in sorazmernih ukrepov za zaščito centralnega informacijsko-komunikacijskega sistema. Ukrepi lahko vključujejo tudi začasni odklop varnostno neustrezne informacijske rešitve iz centralnega informacijsko-komunikacijskega sistema, dokler ugotovljene pomanjkljivosti niso odpravljene.

IS ADRZ, uporabljene knjižnice in tehnološko izvajalno okolje morajo temeljiti na podprti programski opremi. Uporaba »End-of-life« programske opreme, ki se ji je iztekla podpora (podpora proizvajalca, podpora skupnosti) v produkciji ni sprejemljiva, ker predstavlja varnostna tveganja. Planiranje rokov podpore posameznih sestavnih delov informacijske rešitve in izvajalnega okolja je potrebno načrtovati in spremljati v celotnem obdobju življenjske dobe informacijske rešitve.

### 3.2.2 Izvedba varnostnega pregleda

Ponudnik IS ADRZ svoje aktivnosti izvaja skladno s standardom ISO 27001.

Ponudnik IS ADRZ zagotavlja in v celoti financira v sklopu svoje ponudbe pregled informacijske varnosti, ki bo zajemal vse programske komponente IS ADRZ (npr. strežniški del, spletno aplikacijo) po naslednjih metodologijah:

- CWE Top 25 (po najnovejšem letniku) in
- OWASP Top 10 (po najnovejšem letniku).

Varnostni pregled lahko, poleg navedenih, vključuje tudi druge metodologije, kot npr. OSSTMM (Open Source Security Testing Methodology) in druge standarde, dobre prakse in metodologije s tega področja, kot npr. ISO/IEC 27002:2005 ali PTEST ali primerljiv.

Ponudnik IS ADRZ izvedbo varnostnega pregleda naroči zunanjemu izvajalcu pregleda, ki razpolaga s certifikatom ISO 9001 ter strokovnost s področja dodatno izkazuje s certifikati, kot npr. CEH, OSCP, eWPT ali primerljivim certifikatom.

Naročnik izbiro zunanjega izvajalca pregleda na podlagi informacij o referencah potrdi ali zavrne in ima možnost zahtevati drugega zunanjega izvajalca pregleda. Zunanji izvajalec pregleda ne sme biti lastniško ali na drugačen način povezan s ponudnikom IS ADRZ, temveč mora biti v celoti neodvisen od ponudnika IS ADRZ.

Ponudnik IS ADRZ zunanjemu izvajalcu pregleda pripravi vsebinski opis predvidenih načinov uporabe sistema (npr. po user story pristopu) in zagotovi, da zunanji izvajalec pregleda razpolaga z vsemi vsebinskimi informacijami, ki so potrebne za celovito in kakovostno izvedbo varnostnega pregleda.

Poseben poudarek varnostnega pregleda predstavlja preizkus izolacije najemnikov (angl. multitenancy data isolation test), kar pomeni, da mora biti varnostni pregled izveden tudi na nivoju implementacije pri vsaj treh posamičnih zdravstvenih zavodih.

Varnostni pregled se izvaja v okolju UAT. Izvaja se lahko sprotno, dokončno bo potrjen v okolju UAT po tem, ko bo potrjena uporabniška sprejetost in bo sistem pripravljen na prenos v produkcijsko okolje.

Zunanji izvajalec pregleda, ki izvede varnostni pregled IS ADRZ, pripravi podrobno tehnično poročilo, ki zajema ugotovitve, klasificirane po stopnji kritičnosti, in priporočila za sanacijo pomanjkljivosti. Ponudnik IS ADRZ ni dolžan deliti podrobnega tehničnega poročila z naročnikom, razen na pisno zahtevo naročnika.

Zunanji izvajalec pregleda pripravi tudi vodstveni povzetek poročila (angl. executive summary), ki bo med drugim zajemalo pregleden povzetek varnostnega pregleda za netehnične osebe s popisom števila zaznanih pomanjkljivosti, klasificiranih po stopnji kritičnosti. Ponudnik IS ADRZ vodstveni povzetek poročila deli z naročnikom.

Ponudnik IS ADRZ je dolžan po prejemu podrobnega tehničnega poročila izvesti sanacijo zaznanih pomanjkljivosti skladno s priporočili. V primeru, da se ponudnik IS ADRZ odloči načrtno ne sanirati ene ali več zaznanih pomanjkljivosti, mora za vsako izmed takšnih nesaniranih pomanjkljivosti podati pisno argumentacijo naročniku, zakaj pomanjkljivosti ne bo saniral, in pisno sprejeti tveganje zanjo. Odločitev je dolžan sporočiti tudi zunanjemu izvajalcu pregleda, da je ta seznanjen o neodpravljeni pomanjkljivosti.

Po zaključku sanacije zaznanih pomanjkljivosti zunanji izvajalec pregleda izvede verifikacijo sanacije. V primeru, da vse v varnostnem pregledu zaznane pomanjkljivosti niso bile bodisi odpravljene bodisi načrtno nesanirane (s pisno argumentacijo o sprejemu tveganja), mora ponudnik ponavljati sanacijo pomanjkljivosti, dokler verifikacija ni uspešno zaključena.

Ob vsaki verifikaciji je zunanji izvajalec pregleda dolžan pripraviti podrobno verifikacijsko poročilo za ponudnika in vodstveni povzetek verifikacijskega poročila, ki ga ponudnik vsakič deli z naročnikom.

Uspešno zaključena verifikacija je potreben predpogoj za prenos v produkcijsko okolje.

### 3.3 Ostale splošne zahteve glede arhitekture

#### 3.3.1 Razpoložljivost

Sistem ADRZ mora biti na voljo uporabnikom v določenih časovnih okvirih, ki jih določi zavod oz. naročnik sistema. Ker je sistem ključen za nemoten potek razporejanja in izvajanja zdravstvene dejavnosti, morajo biti definirani standardi glede obsega razpoložljivosti in dopustnih izpadov.

##### 3.3.1.1 Cilji razpoložljivosti

- Funkcionalnosti sistema morajo biti na voljo v najmanj 99,9 % časa glede na letno raven.
- V okviru enega meseca sta dopustni največ 2 uri izpada, na letnem nivoju največ 8 ur in 45 min izpada.
- V posameznem incidentu je dopustna prekinitev najdlje 4 ure.
- Sistem mora biti razpoložljiv v režimu 24/7/365.

##### 3.3.1.2 Upravljanje z izpadi in vzdrževanjem

- Vzdrževalne aktivnosti (nadgradnje, posodobitve) se izvajajo izven delovnega časa načrtovalca delovnih razporedov oziroma v času manjše obremenitve sistema. Okno za vzdrževalne aktivnosti dogovorita naročnik in izvajalec predvidoma od 23.00 do 03.00.
- Vzdrževalne aktivnosti se ne smejo izvajati med 10. in 21. v mesecu, ko bo IS ADRZ najbolj obremenjen.
- V primeru predvidenega izpada mora biti obveščanje o nedelovanju poslano vsaj 72 ur pred dogodkom z navedbo termina, trajanja in obsega nedelovanja.
- Kritične napake, ki zahtevajo interventni poseg, se odpravljajo po vnaprej določenem odzivnem času (SLA).

### 3.3.1.3 *Neodvisnost od zunanjih sistemov*

- Zahteve o razpoložljivosti se nanašajo na IS ADRZ in njegove storitve.
- Integracije z drugimi sistemi (npr. kadrovska evidenca, sistem registracije delovnega časa) ne vplivajo na štetje doseganja ciljev razpoložljivosti IS.

### 3.3.1.4 *Mehanizmi za zagotavljanje razpoložljivosti*

- V primeru izpada posamezne komponente mora biti sistem sposoben samodejne prerazporeditve delovanja na delujoče dele (failover, HA arhitektura).

### 3.3.1.5 *Pogodbeni okvir (SLA)*

- Vzpostavljena mora biti pogodba o ravni storitev (SLA), ki jasno določa:
  - Največji dopustni čas izpada.
  - Odzivni časi za reševanje incidentov.
  - Štetje nedelovanja, odpravo napak in kazni za nedoseganje.

## 3.3.2 Zanesljivost

Sistem ADRZ mora zagotavljati visoko stopnjo zanesljivosti tako na ravni programske opreme kot tudi podatkovne celovitosti. Ker gre za ključni IS pri razporejanju zdravstvenega osebja, so napake, nepravilni podatki ali izpadi sistema nesprejemljivi in lahko neposredno vplivajo na kakovost zdravstvene oskrbe. Poleg tega je treba upoštevati zahteve večnajemniškega modela kot opredeljeno v poglavju 1.1 Splošne smernice in arhitekturni principi IS ADRZ.

### 3.3.2.1 *Celovitost podatkov*

- Sistem preverja celovitost in točnost podatkov še pred njihovo uporabo pri razporejanju (npr. urejenost podatkov v šifrantu ali naboru vrednosti).
- Vnos podatkov naj bo izveden preko vnaprej določenih šifrantov, kjer je to mogoče (npr. delovišča, veščine, tipi odsotnosti).
- Vmesnik mora preprečevati vnos nepopolnih ali napačnih vrednosti z uporabo preverjanja dolžine, formata, dovoljenih vrednosti.
- Ob vnosu ali spremembi mora sistem samodejno preveriti konsistentnost vnesenih podatkov (npr. da se večina ujema z zahtevo iz delovišča).

### 3.3.2.2 *Razveljavitev sprememb*

- Sistem mora omogočiti pregled nad spremembami (audit log) in možnost sledenja kdo, kdaj in kaj je vnesel ali spremenil.
- V primeru napake mora imeti uporabnik možnost enostavne razveljavitve zadnje spremembe.
- Kadar pride do napak, mora biti omogočena ponastavitev posameznih segmentov (npr. razpored za en dan ali delovišče).

### 3.3.2.3 *Obnovitev po napakah*

- Sistem mora biti sposoben samodejne obnove po manjših napakah, brez posredovanja uporabnika.
- Implementiran mora biti mehanizem za samodejno zaznavanje napak na ravni aplikacije in sprožitev postopkov za obnovitev (npr. ponovni zagon storitve, ponovitev neuspele operacije).
- Uporaba nadzornih mehanizmov za preverjanje zdravja komponent (health checks), ki v primeru zaznane napake sprožijo sanacijo ali opozorilo.
- V primeru odpovedi delov sistema mora biti omogočena replikacija na rezervne komponente (failover mehanizmi), brez prekinitve delovanja.
- Podatkovna baza mora podpirati transakcijsko obnovitev (rollback), če pride do prekinitve ali nekonsistentnosti v podatkovni operaciji.
- V primeru prekinitve procesa zaradi napake se mora proces nadaljevati od zadnje stabilne točke (checkpoint restore) in ne od začetka.
- V primeru hujše napake (npr. sistemski izpad) mora biti možno ponovno vzpostaviti sistem v prvotno stanje iz zadnje stabilne točke.
- Arhitektura sistema mora podpirati transakcijsko obdelavo, kjer se ob neuspehu zapisovanja spremembe ne zapišejo.

### 3.3.2.4 *Nadzor in opozorila*

- Vključen mora biti sistem opozarjanja na izpade, kritične napake, zastoje v delovanju.
- Sistem mora podpirati samodejno beleženje neuspešnih operacij in omogočiti analizo vzrokov.
- Tehnični administrator mora imeti dostop do nadzorne plošče, kjer so prikazani vsi indikatorji stanja zanesljivosti.

### 3.3.2.5 *Redno preverjanje*

- Pred vsako ključno fazo (npr. objava razporeda) mora sistem preveriti skladnost podatkov in uporabnika opozoriti na morebitna odstopanja.
- Vključeni morajo biti redni testi za odkrivanje nepravilnosti, ki se lahko izvajajo samodejno v ozadju.

### 3.3.2.6 *Odpornost proti izpadom*

- IS ADRZ mora delovati v načinu visoke razpoložljivosti (High Availability – HA) z uporabo redundantnih komponent (npr. več strežnikov, replikacija podatkov).
- Podprta mora biti samodejna preklopitev (failover) na sekundarne strežnike ob nedelovanju primarnega. Alternativa je delovanje v načinu active-active.
- Vključeni morajo biti mehanizmi za zaščito pred izgubo podatkov ob izpadu (npr. transakcijski zapisi, periodične varnostne kopije).
- Vzpostavljen mora biti načrt za neprekinjeno poslovanje (Business Continuity Plan) in načrt za obnovo po katastrofi (Disaster Recovery Plan), s ciljnim časom ponovne vzpostavitve ( $RTO \leq 4$  ure) in dovoljenim obsegom izgube podatkov ( $RPO \leq 1$  minuta).
- IS ADRZ mora omogočati delno delovanje v načinu degradirane funkcionalnosti, če osnovne funkcije ostanejo nepoškodovane.

### 3.3.3 Razširljivost

IS ADRZ mora biti zasnovan tako, da omogoča prilagodljivo rast sistema v skladu z razvojnimi potrebami zdravstvenega sistema v Sloveniji, razvojem posamezne zdravstvene ustanove ter širitvijo obsega uporabe na dodatne organizacijske enote, delovišča, uporabniške vloge ali nove funkcionalnosti.

#### 3.3.3.1 *Podporna arhitektura*

- IS ADRZ mora biti modularno zasnovan, kar pomeni, da je možno posamezne module (npr. planiranje, nadomeščanje, poročila) neodvisno nadgrajevati ali dodajati nove.
- Strežniška infrastruktura mora podpirati horizontalno in vertikalno skaliranje glede na rast števila uporabnikov ali obsega podatkov.

#### 3.3.3.2 *Prilagodljivost funkcionalnosti*

- IS ADRZ mora omogočiti enostavno vključevanje novih tipov uporabnikov ali vlog (npr. pogodbeni kadri).
- Možnost dodajanja novih vrst razporedov, prilagojenih različnim tipom delovišč (npr. laboratorij, intervencije).
- Vmesnik in administracija morata podpirati dodajanje novih šifrantov brez posega v osnovno kodo (npr. nova delovišča, nove vrste izmen, nove veščine).

#### 3.3.3.3 *Integracija novih modulov*

- IS ADRZ mora omogočiti priklop novih analitičnih ali podpornih modulov (npr. napovedovalni modeli za kadrovske potrebe).
- Podprta mora biti uporaba standardnih vmesnikov (API) za povezovanje z drugimi informacijskimi sistemi.

#### 3.3.3.4 *Skaliranje števila uporabnikov*

- Ob povečanju števila uporabnikov (npr. vključitev dodatnega zdravstvenega zavoda) mora IS ADRZ ohraniti odzivnost in stabilnost.
- Vzpostavljen mora biti mehanizem za ločeno obravnavo več zavodov znotraj enotnega sistema (multitenancy).

#### 3.3.3.5 *Prilagoditev zakonodaji in interni politiki*

- IS ADRZ mora omogočiti enostavne nadgradnje zaradi sprememb zakonodaje.
- Prilagodljivost na različna interna pravila (npr. različen način načrtovanja delovni razporedov, različno število dni za oddajo želja, posebne vloge potrjevalcev).



### 3.3.4 Zmogljivost

IS ADRZ mora biti zmogljiv in odziven tudi pri intenzivni uporabi, saj se uporablja v okoljih z veliko uporabniki, obsežnimi podatkovnimi sklopi in visoko frekvenco sočasnih operacij (npr. med ustvarjanjem delovnih razporedov, itd.).

#### 3.3.4.1 *Splošne zmogljivostne zahteve*

- Posebne operacije kot je ustvarjanje delovnega razporeda lahko trajajo dalj časa.
- V primeru obremenjenosti mora IS ADRZ samodejno uravnavati vire in prioriteto obdelovati zahtevke z najvišjo poslovno pomembnostjo (npr. delovni razpored za naslednji mesec ima višjo prioriteto kot delovni razpored za 2 meseca naprej).

#### 3.3.4.2 *Raven storitve uporabniškega vmesnika IS ADRZ*

IS ADRZ mora zagotavljati ustrezno odzivnost pri delovanju v produkcijskem okolju kot sledi:

- Povprečni odzivni čas za vse uporabniške operacije zdravstvenega delavca ne sme presegati 1,5 sekunde, merjeno znotraj aplikacijskega okolja, na ravni aplikacijskega strežnika (brez vpliva zunanjega omrežja).
- Najdaljši odzivni čas za katerokoli uporabniško operacijo načrtovalca delovnih razporedov ne sme presegati 10 sekund, merjeno znotraj aplikacijskega okolja, na ravni aplikacijskega strežnika. Navedena zahteva ne velja za operacijo samodejne izdelave delovnega razporeda, ki se izvaja v ozadju.
- V meritev odzivnega časa niso vključeni vplivi komunikacijskih poti med uporabnikom in sistemom (npr. delovanje interneta, VPN povezav, lokalnih in širokopasovnih omrežij). Meritve se izvajajo neposredno na infrastrukturi, kjer je aplikacija nameščena (lokalno v podatkovnem centru NIJZ).
- Izvajalec mora ob zahtevi naročnika zagotoviti podatke o opravljenih meritvah odzivnosti (npr. dnevniki, izpisi, orodja za spremljanje delovanja), ki izkazujejo skladnost z zgoraj navedenim pogojem.
- V primeru odstopanj od zahtevane odzivnosti mora izvajalec predložiti obrazložitev in načrt ukrepov za odpravo neskladnosti.

#### 3.3.4.3 *Zahteve za odzivnost in raven storitev (SLA) za API IS ADRZ*

IS ADRZ mora zagotavljati stabilno, odzivno in visoko razpoložljivo delovanje API vmesnika, ki omogoča integracijo z drugimi informacijskimi sistemi.

##### 3.3.4.3.1 *Odzivnost API klicev*

- Povprečni odzivni čas za sinhrono API klice (npr. GET, POST) ne sme presegati 200 ms, merjeno na ravni aplikacijskega strežnika.
- Maksimalni odzivni čas posameznega API klica v normalnih pogojih ne sme presegati 500 ms.
- Meritve odzivnosti se izvajajo znotraj strežniške infrastrukture NIJZ, kjer je API gostovan.

- V oceno odzivnosti niso vključeni vplivi komunikacijskih poti med klicateljem in API (npr. omrežna latenca, VPN, internet).

#### 3.3.4.3.2 *Razpoložljivost API vmesnika*

- API mora biti na voljo najmanj 99,9 % časa na mesečni ravni.
- Nedosegljivost API vmesnika pomeni, da API ne sprejema ali ne vrača pravih odgovorov v okviru določenega odzivnega časa.

#### 3.3.4.3.3 *Omejitve in zmogljivost*

- API mora zagotavljati najmanj 50 hkratnih zahtevkov na sekundo brez degradacije delovanja.
- Rešitev mora omogočati skalabilnost API/Integracijskega dela, skladno z rastjo števila integracij s strani zdravstvenih zavodov ali povečanega števila klicev.
- V primeru nepravilnega ali omejenega delovanja API zmogljivosti mora le ta vračati ustrezne informacije (error kode), ki jih sprejemnik lahko interpretira.

#### 3.3.4.3.4 *Spremljanje in poročanje*

- Izvajalec mora omogočiti sistem za spremljanje delovanja API v realnem času (npr. dashboard ali API monitoring).
- Naročniku mora biti na voljo mesečno poročilo o:
  - številu klicev,
  - času odziva,
  - stopnji uspešnosti (uspešni/neuspešni odgovori),
  - morebitnih izpadih ali napakah.

#### 3.3.4.4 *Razširljivost zmogljivosti*

- IS ADRZ mora omogočiti nadgradnjo virov (procesna moč, pomnilnik, pasovna širina) brez ponovnega nameščanja sistema.
- Zmogljivostne lastnosti morajo biti spremljane z uporabo metrik in grafov, ki omogočajo napovedovanje ozkih grl.

#### 3.3.4.5 *Stresni in obremenitveni testi*

- Pred uvedbo v produkcijo mora IS ADRZ prestati stresne teste, ki simulirajo špice v uporabi (npr. zadnji dan za oddajo želja, ustvarjanje delovnih razporedov za cel zdravstveni zavod).
- Redno izvajanje obremenitvenih testov je potrebno tudi po glavnih nadgradnjah ali spremembah arhitekture.

### 3.3.5 Interoperabilnost

IS ADRZ mora omogočati varno, standardizirano in zanesljivo izmenjavo podatkov z drugimi informacijskimi sistemi, ki so relevantni za delovanje zdravstvenih zavodov. Integracije z zunanjimi

sistemi so ključne za avtomatizacijo procesov, zmanjšanje ročnega vnosa ter zagotavljanje skladnosti z zakonodajnimi in poslovnimi zahtevami.

#### 3.3.5.1 *Zahteve za integracijo*

- IS ADRZ mora omogočati dvosmerno integracijo z:
  - Kadrovskimi evidencami (podatki o zdravstvenih delavcih, omejitvah, soglasjih),
  - IS registracijo delovnega časa,
  - IS za oddajo in potrjevanje zahtevkov za odsotnost,
- IS ADRZ mora imeti dokumentirane in standardizirane vmesnike:
  - API (REST, izjemoma SOAP),
  - Možnost uvoza/izvoza preko SFTP.

#### 3.3.5.2 *Standardi in varnost pri povezovanju*

- Podprti standardi za izmenjavo:
  - OAuth2, SAML 2.0 (za varno avtentikacijo),
  - TLS 1.2+ (za šifrirano komunikacijo).
- Integracije morajo spoštovati:
  - Politike dostopa (glede na vloge in pravice),
  - Validacijo podatkov pri vnosu in izmenjavi,
  - Samodejno logiranje vseh povezanih dogodkov.

#### 3.3.5.3 *Upravljanje napak in nadzor*

- IS ADRZ mora ob prekinitvi povezave:
  - Zabeležiti neuspešno poizvedbo,
  - Poskusiti ponoven prenos,
  - Obvestiti skrbnika o napaki.
- Na voljo mora biti nadzorna plošča za spremljanje stanja integracij (uspešnost, zakasnitve, napake).

#### 3.3.5.4 *Testna okolja*

- Vsaka integracija mora biti mogoča v testnem okolju brez vpliva na produkcijske podatke.
- Dokumentacija o povezavah mora biti dostopna, pregledna in posodobljena.

#### 3.3.6 Vzdržljivost

IS ADRZ mora biti zasnovan tako, da zagotavlja stabilno delovanje tudi v pogojih dolgotrajne uporabe, izjemnih obremenitev ali delnih napak. IS ADRZ mora biti sposoben prenesti različne vrste napak brez izgube podatkov ali funkcionalnosti, kar je ključno za zanesljivo delovanje v zdravstvu.

##### 3.3.6.1 *Odpornost na motnje v delovanju*

- IS ADRZ mora ostati stabilen tudi ob nepopolnih ali napačnih uporabniških vnosih.

- V primeru napake mora biti omogočena obnova operacije ali nadaljevanje dela brez ponovnega zagona sistema.
- Komponente sistema morajo biti neodvisne, da napaka v enem modulu ne vpliva na druge (napaka v modulu za poročila ne sme vplivati na razporejanje delovnega časa).

#### 3.3.6.2 *Neodvisnost od uporabniških napak*

- IS ADRZ mora pred kritičnimi operacijami (brisanje, potrjevanje) zahtevati potrditev.
- Ob potencialno napačnem vnosu mora uporabniku ponuditi popravek ali alternativni predlog.
- V primeru nepravilnega zaporedja korakov (workflow) mora IS ADRZ voditi uporabnika nazaj na ustrezno potekanje procesa.

#### 3.3.7 *Prilagodljivost*

IS ADRZ mora biti prilagodljiv, da se lahko enostavno prilagaja spremembam organizacije, zakonodaje, uporabniških potreb in drugih kontekstualnih dejavnikov kot je opisano v funkcionalnih zahtevah. Prilagodljivost je ključna za dolgoročno vzdrževanje sistema brez potrebe po pogostih tehničnih posegih.

##### 3.3.7.1 *Nastavljivost sistema*

- IS ADRZ mora omogočati administrativno urejanje glavnih nastavitev brez posredovanja ponudnika sistema (npr. šifranti, organizacijska struktura organizacije, tipi izmen, pravila razporejanja delovnega časa).
- Spreminjanje parametrov sistema mora biti možno brez prekinitve delovanja.

##### 3.3.7.2 *Prilagodljivost pravil in algoritmov*

- Vhodne podatke za algoritme za samodejno razporejanje mora biti možno prilagoditi preko uporabniškega vmesnika (npr. uteži, prioritete, zakonske omejitve, itd.).
- IS ADRZ mora omogočati različna pravila za različne zdravstvene zavode, različna delovišča, različne vrste izmen, itd.

##### 3.3.7.3 *Večjezičnost in lokalna prilagoditev*

- IS ADRZ mora poleg slovenskega jezika podpirati uporabniški vmesnik v angleškem jeziku.
- Podprta mora biti lokalizacija datuma, časa, decimalnih mest, valut, standardov.
- Sistemski elementi (sporočila, oznake) morajo biti prevedljivi brez posega v kodo.
- Uporabniški vmesnik IS ADRZ za zdravstvene delavce mora biti skladen z zahtevami Zakona o dostopnosti spletišč in mobilnih aplikacij (ZDSMA).

##### 3.3.7.4 *Uporabniški vmesnik za mobilne naprave*

- UI mora biti odziven (responsive) in prilagojen različnim dimenzijam zaslonov (mobilni telefoni, tablice, prenosniki, namizni računalniki).
- Slike in multimedijske vsebine morajo biti responsive.

- Besedilo mora biti berljivo na vseh zaslonih (npr. velikost črk naj bo sorazmerna širini zaslona).
- Pomembne funkcionalnosti morajo biti dostopne ne glede na velikost zaslona.
- Prehodi in animacije morajo biti nemoteči in prilagojeni napravi.
- Na mobilnih napravah mora biti zagotovljena zadostna velikost klikabilnih elementov.

#### *3.3.7.5 Nadgradljivost uporabniškega vmesnika*

- Uporabniški vmesnik mora omogočati prilagoditev posameznim vlogam (prikaz samo relevantnih funkcij).
- Prikaz podatkov mora biti sortiran in prilagodljiv po vsebini in obsegu. Na voljo je iskalnik po vsebini in filter prikaza vsebine.

#### *3.3.7.6 Podpora različnim scenarijem uporabe*

- IS ADRZ mora omogočati konfiguracijo za zavode z različno kompleksnostjo (zelo veliki zdravstveni zavodi z distribuirano odgovornostjo za delovne razporede, majhni zdravstveni zavodi s centralizirano odgovornostjo za delovne razporede).
- Možnost hkratnega ročnega in samodejnega razporejanja v različnih organizacijskih enotah po izbiri.
- Možnost uporabe samo posameznih modulov IS (npr. samo evidenca izmen, brez samodejnega razporejanja).

## 4 Infrastruktura

### 4.1 Tehnološka infrastruktura

#### 4.1.1 Okolja in platforma

Sistem IS ADRZ bo deloval na infrastrukturi (virtualni strežniki na okolju s hipervizorjem ESX/ESXi, diskovna polja, mrežna oprema, varnostne kopije), s katero upravlja NIJZ.

Ponudnik IS ADRZ mora sam upravljati s strežniško infrastrukturo, ki bo potrebna za vzpostavitev in delovanje IS ADRZ (redno nameščanje kritičnih popravkov na operacijskem sistemu, sodelovanje pri nadgradnjah operacijskega sistema na strežnikih na nove verzije, podporo pri nameščanju kritičnih popravkov na operacijski sistem in reševanje morebitnih težav, ažurno verzijo Windows Server Update Services na Windows strežnikih, največ 3 mesece stara verzija VMWare Tools ali Open VM Tools nameščena na operacijskem sistemu). Ponudnik IS ADRZ mora sodelovati pri vseh posegih na sistemski in mrežni infrastrukturi, ki posegajo v delovanje strežniških aplikacij, in pri testu okrevanja, ki se izvaja dvakrat letno. Vsa programska oprema in operacijski sistemi morajo biti ob namestitvi na zadnji priporočljivi verziji, kar mora biti usklajeno tudi z upraviteljem infrastrukture NIJZ.

Virtualni strežniki lahko podpirajo tako Microsoft Windows Server kot Oracle Linux strežniške operacijske sisteme (64-bit). Ponudnik IS ADRZ v svojo ponudbo vključi licence in vzdrževanje za operacijske sisteme za IS ADRZ za čas trajanja garancije in vzdrževanja ADRZ, zagotovljenega v okviru tega javnega naročila za sklop 1.

Ponudnik IS ADRZ mora pravočasno obveščati o potrebi po novih sistemskih virih (vsaj 6 mesecev vnaprej), usklajevati morebitne nakupe dodatnih sistemskih virov z naročnikom in pomagati pri pripravi specifikacij za nabavo nove strojne in programske opreme.

Nakup strežniške opreme je zagotovljen v sklopu 2 tega javnega naročila. Predvideno je, da se bo infrastruktura širila glede na potrebe IS ADRZ rešitve, skladno s časovnico uvajanja v bolnišnice.

#### 4.1.2 Sistem za upravljanje s podatkovno bazo

Za shranjevanje IS ADRZ podatkov bo v okviru infrastrukture eZdravja uporabljena naslednja Oracle programska oprema, ki bo zagotavljala visoko razpoložljivost, v naslednjih količinah:

Licenčni produkt	Metrika	Količina
Database Enterprise Edition	Processor, Full Use	2
Real Application Clusters One Node	Processor, Full Use	1
Diagnostics Pack	Processor, Full Use	2
Tuning Pack	Processor, Full Use	2
Audit Vault & Database Firewall	Processor, Full Use	2

Oracle programska opreme zagotavlja funkcionalnost revizijske sledi (angl. *audit log*) na nivoju same podatkovne baze, in sicer za vse CRUD operacije.

Ponudniku IS ADRZ v svojo ponudbo ni potrebno vključiti licence za Oracle programsko opremo za produkcijsko, UAT in testno IS ADRZ okolje, vključi pa ADRZ okolje za usposabljanje uporabnikov (šolsko okolje, v primeru, da bo potrebno in dogovorjeno med ponudnikom in naročnikom) in lastno testno okolje, kjer tip podatkovne baze ni pomemben, za čas trajanja garancije in vzdrževanja ADRZ, zagotovljenega v okviru tega javnega naročila, sklop 1.

Podatki so kriptirani pred shranjevanjem, z uporabo ustrezno močnih in preverjenih šifrnih algoritmov, skladno z najboljšimi praksami stroke (tj. najmanj AES z dolžino ključa vsaj 256 bitov za simetrično šifriranje ali ECC za asimetrično šifriranje). Ključi za šifriranje in dešifriranje so varno hranjeni na strežniški strani in nikoli neposredno dostopni s strani odjemalca. Preverjanje integritete podatkov je zagotovljeno z uporabo ustreznih kriptografskih funkcij (HMAC), s čimer se prepreči nepooblaščen spreminjanje podatkov. Salt in Initialization Vector (IV) sta uporabljena za dodatno varnost pri šifriranju, skladno z značilnostmi izbranega algoritma.

Nakup Oracle licenčne programske opreme je zagotovljen sklopu 3 tega javnega naročila. Predvideno je, da se bo le-ta širila glede na potrebe IS ADRZ rešitve, skladno s časovnico uvajanja v bolnišnice.

#### 4.1.3 Podatkovni center

IS ADRZ mora delovati v dvojčku podatkovnih centrov, predvidoma active-passive način delovanja Oracle programske opreme (tj. dva povezana redundančna podatkovna centra na različnih lokacijah) in omogoča ne le vertikalno, temveč tudi horizontalno skalabilnost (npr. več instanc strežniške aplikacije, ki so dostopne za izenačevalnikom obremenitve (*load balancer*)) in zagotavlja visoko razpoložljivost:

- z gručami na nivoju aplikacijskih strežnikov in konektorjev na baze,
- okrevanje aplikacij s "stand-by" ali repliciranimi aplikacijskimi strežniki in bazami na rezervni lokaciji.

#### 4.1.4 Vključitev ADRZ v NIJZ storitveni center

IS ADRZ mora omogočati vključitev v nadzorne sisteme NIJZ, zaradi česar mora ponudnik IS ADRZ zagotoviti uporabniške račune za namestitev nadzornih agentov in pomagati pri parametrizaciji alarmov; vsi sistemi so dostopni vzdrževalcem IKT (administrativni dostop do vseh sistemov in rešitev). Ponudnik IS ADRZ obravnava alarme za ADRZ sistem v svojem upravljanju.

Ponudnik IS ADRZ in vsi delavci, ki bodo upravljali posege na infrastrukturi, se morajo strinjati, da se njihove seje snemajo. Vsi delavci, ki bodo imeli dostop do IS ADRZ sistema, v katerem bodo kadrovski podatki zdravstvenih zavodov, morajo imeti podpisano izjavo o varstvu podatkov.

#### 4.1.5 Interna ADRZ baza podatkov

Za shranjevanje podatkov informacijskega sistema ADRZ bo v okviru infrastrukture eZdravja uporabljena Oracle programska oprema, kot je pojasnjeno v poglavju 4.1.2 »Sistem za upravljanje s podatkovno bazo«. Oracle baza deluje na ločeni infrastrukturi NIJZ, ki obsega zgolj strežnike za podatkovno bazo, do katerih dostopajo vse rešitve eZdravja. Zato ni potrebe po vzpostavitvi internih podatkovnih baz znotraj strežnikov, na katerih so nameščene posamezne rešitve.

V primeru, da ima ponudnik rešitev, pri kateri je aplikativni nivo (ADRZ aplikacija) tesno povezan s podatkovnim nivojem (ADRZ podatkovna baza), ki ni Oracle, in te baze ne želi ali ne more zamenjati z Oracle, naročnik dopušča uporabo katerekoli interne ADRZ baze podatkov za interno delovanje informacijskega sistema ADRZ, pod pogojem, da ta baza izpolnjuje naslednje zahteve:

- Temelji na komercialno podprti distribuciji, kot je npr. EDB (EnterpriseDB) z rešitvijo EDB Postgres Advanced Server ali na primerljivih podatkovnih bazah, ki ustrezajo zahtevam Zakona o kritični infrastrukturi (ZKI-1) (zahteve po: zagotavljanju visoke stopnje odpornosti informacijskih sistemov, zmanjševanju tveganja za motnje delovanja, neprekinjenem delovanju tudi v primeru incidentov in napak, vzdrževanju ter varnostnem posodabljanju), ter zahtevam Evropskega zdravstvenega podatkovnega prostora (EHDS), Priloga II (zahteve po: interoperabilnosti, varnosti in zagotavljanju kakovosti podatkov), in so skladne z ostalimi evropskimi in slovenskimi predpisi (npr. GDPR).
- Omogoča redne varnostne posodobitve.
- Zagotavlja visoko raven varnosti podatkov (šifriranje, avtentikacija, upravljanje dostopa).
- Zagotavlja celovitost pri obdelavi podatkov v celotnem ciklu.
- Ponuja 24/7 tehnično podporo z odzivnim časom, krajšim od 15 minut za kritične incidente.
- Varnostne posodobitve so certificirane po mednarodnih standardih (npr. FIPS, Common Criteria).
- Ima dokumentirane dogovore o ravni storitev (SLA), vključuje hotfix popravke ter preverjene nadgradnje s strani proizvajalca oziroma principala.
- Izvaja se izključno na lokaciji NIJZ, brez kakršnegakoli dostopa do oblčnih storitev.

V primeru, da ponudnik ponudi svojo interno ADRZ bazo podatkov, bo Oracle baza podatkov, ki se naroča v sklopu 3, še naprej služila kot osrednja shramba vseh podatkov informacijskega sistema ADRZ, medtem ko bo interna ADRZ baza podatkov namenjena delovanju ADRZ aplikacije.

Če ponudnikova rešitev uporablja interno ADRZ bazo podatkov, ki ni Oracle, mora ponudnik na lastne stroške zagotoviti ustrezne licence in vzdrževanje te baze podatkov. Prav tako mora zagotavljati enak nivo storitev (SLA) za delovanje aplikacije IS ADRZ, kot bi ga zagotavljal v primeru uporabe Oracle baze podatkov kot interne (v tem primeru, ponudnik ni odgovoren za nivo storitve Oracle baze podatkov, saj jo upravlja in vzdržuje NIJZ).

Ponudnik ne zagotavlja licenc, namestitve in vzdrževanja Oracle baze podatkov kot take, mora na lastne stroške:

- Implementirati in vzdrževati integracije ter sinhronizacijo podatkov med interno ADRZ bazo podatkov in Oracle bazo podatkov.
- Zagotavljati 100 % konsistentnost podatkov med obema bazama, kar vključuje implementacijo orodij za nadzor konsistentnosti podatkov ter reševanje konfliktov pri sinhronizaciji.
- Zagotavljati in vzdrževati podatkovni model IS ADRZ v Oracle bazi.
- Vzpostaviti in vzdrževati integracije za prenos podatkov (dvosmerno, kjer je to potrebno) med Oracle bazo podatkov ter kadrovskimi sistemi in sistemi za evidentiranje delovnega časa v 26 bolnišnicah (zvezdasta topologija integracij), kot je opisano v poglavju »2. Seznam integracij, povezava s primeri uporabe in funkcionalnimi zahtevami in tehnična analiza integracij«.



- Zagotoviti 100 % konsistentnost podatkov med Oracle bazo podatkov ter integriranimi sistemi (kadrovski, evidentiranje časa) v bolnišnicah, vključno z orodji za nadzor konsistentnosti in reševanje konfliktov pri sinhronizaciji.

## 4.2 Vhodni podatki za oceno potrebne infrastrukture

Za oceno potrebnih kapacitet infrastrukture so pomembni vhodni podatki o številu načrtovalcev in številu zdravstvenih delavcev, ki se razporejajo po javnih zdravstvenih zavodih. Podatki so na voljo v spodnji tabeli.

	Javni zdravstveni zavod	Število zdravstvenih delavcev, ki se razporejajo	Število načrtovalcev	Število organizacijskih enot	Povprečno število sprememb - dnevno	Povprečno število sprememb - tedensko
1	Bolnišnica za ginekologijo in porodništvo Kranj	106	12	10	0	1
2	Bolnišnica za ženske bolezni in porodništvo Postojna	91	2	5	0	3
3	Bolnišnica Sežana	97	3	6	2	5
4	Bolnišnica za otroke Šentvid pri Stični	110	15	10	1	7
5	Ortopedska bolnišnica Valdoltra	176	11	12	1	7
6	Psihiatrična bolnišnica Begunje	80	5	2	0	1
7	Psihiatrična bolnišnica Idrija	100	2	6	0 do 5	
8	Psihiatrična bolnišnica Vojnik	112	3	9	1 do 3	5 do 10
9	Splošna bolnišnica Celje	2050	34	70	1 do 5	5 do 20
10	Splošna bolnišnica Brežice	368	19	9	1	7

	Javni zdravstveni zavod	Število zdravstvenih delavcev, ki se razporejajo	Število načrtovalcev	Število organizacijskih enot	Povprečno število sprememb - dnevno	Povprečno število sprememb - tedensko
11	Splošna bolnišnica Izola Ospedale generale Isola	790	55	70	15	75
12	Splošna bolnišnica Jesenice	602	25	35	5	5
13	Splošna bolnišnica Murska Sobota	943	59	23	3	/
14	Splošna bolnišnica dr. Franca Derganca Nova Gorica	776	40	41	1	5
15	Splošna bolnišnica Novo mesto	944	60	35	1	/
16	Splošna bolnišnica dr. Jožeta Potrča Ptuj	640	31	20	1 do 2	1 do 2
17	Splošna bolnišnica Slovenj Gradec	729	42	26	5 do 10	30
18	Splošna bolnišnica Trbovlje	300	25	17	1	7
19	Univerzitetna klinika za pljučne bolezni in alergijo Golnik	415	44	24	1	7
20	Univerzitetni rehabilitacijski inštitut RS Soča	120	6	6	1	5
21	Univerzitetni klinični center Ljubljana	6.880	330	470	1 do 12	Do 50
22	Univerzitetni klinični center Maribor	2.563	150	46		Cca 15
23	Onkološki inštitut Ljubljana	1.175	37	70	1	3

	Javni zdravstveni zavod	Število zdravstvenih delavcev, ki se razporejajo	Število načrtovalcev	Število organizacijskih enot	Povprečno število sprememb - dnevno	Povprečno število sprememb - tedensko
24	Bolnišnica Topolšica	248	17	19	3	10
25	Psihiatrična bolnišnica Ormož	167	13	22	2	4
26	Univerzitetna psihiatrična klinika Ljubljana	350	8	8	5	20

Iz zgornje tabele in s predvidevanjem je razvidno, da se v vseh 26 bolnišnicah razporeja do 23.000 zdravstvenih delavcev, ki jih razporeja do 1.200 načrtovalcev delovnih razporedov. Število organizacijskih enot, na katerih se razporejajo zdravstveni delavci je do 1.200. Razmerje med številom načrtovalcev in številom organizacijskih enot se po JZZ zelo razlikuje. V večini zdravstvenih zavodov je število načrtovalcev večje od števila organizacijskih enot in razmerje dosega skoraj 2:1, pri nekaterih zdravstvenih zavodih pa je število načrtovalcev manjše od števila organizacijskih enot in razmerje dosega tudi 1:3. Običajno gre v slednjem primeru za manjše zdravstvene zavode, kjer je izjema Splošna bolnišnica Celje z razmerjem 1:2.

Povprečno število sprememb delovnih razporedov je vsaj enkrat na dan, kjer se določeni delovni razporedi spreminjajo tudi večkrat na dan.