REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

REVIZIJSKO POROČILO

Učinkovitost Ministrstva za notranje zadeve pri upravljanju Centralnega registra prebivalstva

2026

POSLANSTVO

Računsko sodišče pravočasno in objektivno obvešča javnosti o pomembnih razkritjih poslovanja državnih organov in drugih uporabnikov javnih sredstev ter svetuje, kako naj državni organi in drugi uporabniki javnih sredstev izboljšajo svoje poslovanje.

REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

REVIZIJSKO POROČILO

Učinkovitost Ministrstva za notranje zadeve pri upravljanju Centralnega registra prebivalstva

Številka: 320-1/2025-30
Ljubljana, 28. avgusta 2026

Povzetek

Računsko sodišče je revidiralo učinkovitost poslovanja **Ministrstva za notranje zadeve** (v nadaljevanju: MNZ) pri upravljanju Centralnega registra prebivalstva (v nadaljevanju: CRP) v obdobju od 1. 1. 2023 do 30. 6. 2025. Po mnenju računskega sodišča je bilo MNZ pri upravljanju CRP **učinkovito.**

CRP je osrednja zbirka podatkov o prebivalstvu v Republiki Sloveniji. V njej se zbirajo, obdelujejo, hranijo in uporabljajo ključni osebni podatki o državljanih in določenih kategorijah tujcev, kot so enotna matična številka občana, kraj rojstva, ime in priimek, državljanstvo, podatki o prebivališču ter zakonskem stanu. CRP torej predstavlja temeljni vir informacij za delovanje državnih organov in drugih upravičenih uporabnikov. Podatke iz CRP prek 6 informacijskih rešitev na primer pridobivajo Zavod za pokojninsko in invalidsko zavarovanje Slovenije, Zavod za zdravstveno zavarovanje Slovenije, Finančna uprava Republike Slovenije ter občine in porodnišnice, ki novorojencem takoj po rojstvu določijo enotno matično številko občana. Samo v letu 2024 je MNZ posredovalo več kot 70 milijonov podatkov.

Računsko sodišče je v reviziji preverilo, ali je MNZ učinkovito načrtovalo in organiziralo CRP, ali je učinkovito upravljalo z razvojem, spremembami, posodobitvami in vzdrževanjem CRP ter njihovo vpeljavo, ali je učinkovito izvajalo in podpiralo CRP ter ali je učinkovito spremljalo in nadziralo CRP.

V zvezi z načrtovanjem je računsko sodišče ugotovilo, da MNZ ni imelo lastne poslovne strategije CRP niti lastne IT strategije CRP, temveč je sledilo veljavni zakonodaji na področju CRP in ciljem Strategije digitalnih javnih storitev 2030. Letno načrtovanje CRP je bilo zato pretežno odvisno od sprotnih potreb institucionalnih uporabnikov in sprememb zakonodaje in je potekalo v okviru letnih načrtov dela in letnih planov nadgradenj. MNZ je pripravilo informacijsko arhitekturo CRP na način, da je bila ta jasno opredeljena in dokumentirana. Poslovni procesi, vezani na CRP, so bili popisani, prav tako so bili določeni lastniki procesov in podatkov. Tveganja v informacijski podpori CRP so bila sistemsko obvladovana in dokumentirana.

Pri upravljanju razvoja, sprememb, posodobitev in vzdrževanja CRP je MNZ poslovne zahteve pred izvedbo pisno odobrilo, razvoj in vpeljavo sprememb pa je izvajalo po postopkih iz pogodb z zunanjim izvajalcem. Pogodbi z zunanjim izvajalcem sta jasno določali roke, obveznosti, plačila, nadzor, varovanje podatkov in tehnične zahteve, njuno izvajanje pa se je preverjalo na rednih mesečnih sestankih in z mesečnimi poročili izvajalca. MNZ je imelo uporabniška in tehnična navodila za informacijske rešitve CRP ter je glede na potrebe institucionalnih uporabnikov izvedlo izobraževanja

in usposobilo nove uporabnike. Pogodbe o razmejitvi odgovornosti, sklenjene leta 2011 z Ministrstvom za digitalno preobrazbo, pa MNZ ni uskladilo z zahtevami predpisov s področja varstva osebnih podatkov. Računsko sodišče je ugotovilo tudi, da sta pogodbi z zunanjim izvajalcem med dopolnilno vzdrževanje uvrščali razvoj novih funkcionalnosti, kar po vsebini pomeni investicijsko vlaganje, takšno evidentiranje pa zmanjšuje preglednost porabe javnih sredstev.

V zvezi z izvajanjem in podpiranjem CRP je računsko sodišče ugotovilo, da je MNZ način posredovanja podatkov in s tem povezano informacijsko rešitev določilo skupaj z institucionalnim uporabnikom glede na njegove potrebe in tehnične zmogljivosti. MNZ je vodilo tudi razvid uporabnikov podatkov CRP v varnostnih shemah. Na področju upravljanja varnostnih shem oziroma upravljanja s pravili administracije institucionalnih uporabnikov in uporabnikov, ki so fizične osebe, je MNZ zagotavljalo sistem dodeljenih dostopnih pooblastil do informacijskih rešitev CRP, ki so omejena glede na vloge. MNZ je imelo za informacijske rešitve CRP vzpostavljen sistem za pomoč uporabnikom ter tudi sistem odpravljanja napak, varovalo je dostope do podatkov, zagotavljalo varnostne kopije in revizijske sledi ter izvajalo redna testiranja. MNZ pa ni imelo oblikovanega standardiziranega osnutka dogovora, ki bi ga uporabljalo pri vseh odobrenih posredovanjih osebnih podatkov iz CRP institucionalnim uporabnikom ter ki bi ga za posameznega institucionalnega uporabnika prilagodilo glede na njegove posebnosti. Poleg tega je računsko sodišče ugotovilo, da je MNZ podatke iz CRP v posameznih primerih zagotavljalo brez popolne dokumentacije ali zakonske podlage.

V zvezi s spremljanjem in nadziranjem CRP je računsko sodišče ugotovilo, da je MNZ področje informacijske podpore CRP redno obravnavalo na sestankih in upoštevalo sklepe iz zapisnikov teh sestankov. Zagotavljalo je tudi redno poročanje odgovornih oseb vodstvu. Informacijske rešitve CRP pa do konca obdobja, na katero se nanaša revizija, niso bile predmet notranje ali zunanje revizije, kar pomeni, da MNZ ni zagotovilo neodvisnih preveritev njihovega delovanja.

Računsko sodišče je Ministrstvu za notranje zadeve in javno upravo podalo več priporočil v povezavi s strateškim načrtovanjem CRP, s poenotenjem in preverjanjem dogovorov z institucionalnimi uporabniki podatkov iz CRP, z evidentiranjem izdatkov za razvoj informacijskih rešitev ter z vključitvijo informacijskih rešitev CRP v notranje revidiranje.

Kazalo

1. Uvod

Revidirali smo učinkovitost Ministrstva za notranje zadeve pri upravljanju CRP. Revizijo smo izvedli na podlagi Zakona o računskem sodišču[1] in Poslovnika Računskega sodišča Republike Slovenije[2] ter v skladu z mednarodnimi revizijskimi standardi, ki jih določa Napotilo za izvajanje revizij[3]. Sklep o izvedbi revizije[4] je bil izdan 13. 5. 2025.

Naša pristojnost je na podlagi izvedene revizije podati opisno mnenje o učinkovitosti MNZ pri upravljanju CRP v obdobju od 1. 1. 2023 do 30. 6. 2025. Revizijo smo načrtovali in izvedli tako, da smo pridobili zadostna in ustrezna zagotovila za izrek mnenja.

1.1 Opredelitev revizije

Revizija je bila opredeljena kot revizija smotrnosti poslovanja. Cilj revizije je bil izrek mnenja o učinkovitosti MNZ pri upravljanju CRP. Revizija je obsegala obdobje od 1. 1. 2023 do 30. 6. 2025.

Predmet revizije je bila učinkovitost MNZ pri upravljanju CRP. Revizija je bila usmerjena v presojo, kako je MNZ zagotavljalo delovanje informacijskih rešitev, ki omogočajo vodenje CRP in dostop do podatkov CRP, ter kako je zagotavljalo njihovo vzdrževanje, nadgrajevanje, nadzor nad njihovim delovanjem ter zagotavljanjem podatkov iz CRP uporabnikom. Revizija je zajemala predvsem postopke in aktivnosti MNZ, povezane z načrtovanjem, razvojem, uvajanjem, uporabo, podporo in izvajanjem ter nadzorom informacijskih rešitev CRP.

Viri podatkov za CRP (izvorni registri in evidence), proces posredovanja podatkov v CRP, kontrola vhodnih podatkov ter informacijske rešitve institucionalnih uporabnikov, ki se povezujejo z informacijskimi rešitvami MNZ, ki iz podatkovnih zbirk CRP posredujejo podatke, niso bili predmet te revizije.

Da bi lahko izrekli mnenje, smo si zastavili glavno revizijsko vprašanje, **ali je MNZ učinkovito upravljalo CRP.**

Odgovor na glavno revizijsko vprašanje smo pridobili z odgovori na naslednja revizijska podvprašanja:

- Ali je MNZ učinkovito načrtovalo in organiziralo informacijsko podporo CRP?
  - Preverili smo, ali je imelo MNZ poslovno in IT strategijo CRP ter je letno načrtovalo aktivnosti, povezane s CRP, ali je MNZ informacijsko arhitekturo CRP dokumentiralo in je ta bila usklajena s strategijami in operativnimi cilji, ali so bili poslovni procesi, lastništvo poslovnih procesov in podatkov ter odgovornosti in naloge jasno določeni ter ali je bilo

1 Uradni list RS, št. 11/01, 109/12 in 57/25 – ZF.

2 Uradni list RS, št. 91/01.

3 Uradni list RS, št. 122/22.

4 Št. 320-1/2025/7 z dne 13. 5. 2025.

ustrezno urejeno varovanje informacij in obvladovanje tveganj, povezanih z informacijsko podporo CRP.

- Ali je MNZ za potrebe informacijske podpore CRP učinkovito upravljalo z razvojem, spremembami, posodobitvami in vzdrževanjem CRP ter njihovo vpeljavo?
  - Preverili smo, ali je MNZ poslovne zahteve v povezavi z informacijsko podporo CRP pred razvojem, spremembami in posodobitvami pisno odobrilo in pri razvoju, vzdrževanju in vpeljavi CRP sledilo veljavnim internim procesom in dobri praksi[5], ali je upravljalo pravna razmerja z zunanjim izvajalcem storitev informacijskih rešitev CRP, ali je imelo MNZ ustrezna uporabniška in tehnična navodila za uporabo CRP ter ali je zagotavljalo usposabljanje novih uporabnikov.
- Ali je MNZ učinkovito izvajalo in podpiralo CRP?
  - Preverili smo, ali je MNZ upravljalo storitve za institucionalne uporabnike pri posredovanju podatkov, ali je zagotavljalo sistem dostopnih pooblastil do CRP in pomoč uporabnikom, ali je izvajalo varnostno kopiranje podatkov in redna testiranja oziroma restavriranja podatkov iz varnostnih kopij ter ali je upravljalo revizijske sledi.
- Ali je MNZ učinkovito spremljalo in nadziralo aktivnosti v zvezi z informacijsko podporo CRP?
  - Preverili smo, ali je MNZ področje informacijske podpore CRP redno obravnavalo na sestankih in upoštevalo na sestankih sprejete sklepe ter ali je zagotovilo redno poročanje odgovornih oseb vodstvu o aktivnostih v zvezi z razvojem in izvajanjem informacijske podpore CRP. Zanimalo nas je tudi, ali je MNZ redno izvajalo nadzor nad izpolnjevanjem načrtovanih aktivnosti, izpolnjevanjem ciljev ter sprejemom morebitnih korektivnih ukrepov ter ali je na področju CRP izvajalo notranje kontrole in revizije.

Poslovanje MNZ smo ocenili kot učinkovito, če je bilo v pretežnem delu v skladu s sodili za presojo učinkovitosti, oziroma kot neučinkovito, če je bilo v pretežnem delu v neskladju s sodili za presojo učinkovitosti. V ostalih primerih smo poslovanje MNZ ocenili kot delno učinkovito.

1.2 Predstavitev revidiranca

V obdobju, na katero se nanaša revizija, je MNZ na podlagi 34. člena Zakona o državni upravi[6] opravljalo naloge na področjih javne varnosti in policije, upravnih notranjih zadev in migracij. Po obdobju, na katero se nanaša revizija, je MNZ skladno z Zakonom o spremembah Zakona o Vladi Republike Slovenije[7] nadaljevalo delo kot Ministrstvo za notranje zadeve in javno upravo (v nadaljevanju: MNZJU) z delovnim področjem Ministrstva za notranje zadeve, kot ga določa 34. člen Zakona o državni upravi, delovnim področjem Ministrstva za digitalno preobrazbo, kot ga določa 28.a člen Zakona o državni upravi, in delovnim področjem Ministrstva za javno upravo, kot ga določa 34.a člen Zakona o državni upravi, razen delovnega področja lokalne samouprave.[8]

---

5 Dobra praksa pomeni priporočeni način izvajanja postopkov v skladu s strokovnimi smernicami in običajnimi standardi.

6 Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23.

7 Uradni list RS, št. 555/26.

8 Sprememba velja od 4. 6. 2026.

MNZ je na podlagi 4. člena Zakona o centralnem registru prebivalstva[9] (v nadaljevanju: ZCRP) upravljavec CRP ter skladno s 23.a členom istega zakona izvaja nadzor nad izvrševanjem določb ZCRP. Njegove naloge v zvezi z upravljanjem CRP izhajajo med drugim tudi iz Uredbe o vodenju in vzdrževanju centralnega registra prebivalstva ter postopku za pridobivanje in posredovanje podatkov[10] (v nadaljevanju: uredba o vodenju in vzdrževanju CRP), Uredbe o načinu določanja osebne identifikacijske številke[11] in Navodila za elektronsko poslovanje centralnega registra prebivalstva[12].

MNZ lahko v skladu z določili 8. člena Zakona o državni upravi, ki določa, da državna uprava za Vlado Republike Slovenije pripravlja predloge zakonov, podzakonskih predpisov in drugih aktov, predlaga Vladi Republike Slovenije v obravnavo predlog sprememb in dopolnitev ZCRP.

Delo na MNZ je glede na vrsto in obseg dejavnosti ter strokovnost nalog organizirano v 4 direktoratih in sekretariatu, kjer je bilo na dan 30. 5. 2025 631 zaposlenih. Znotraj MNZ je za naloge, povezane z registracijo prebivalstva, in s tem tudi za upravljanje CRP pristojen Direktorat za upravne notranje zadeve (v nadaljevanju: DUNZ), znotraj njega pa Sektor za registracijo prebivalstva in javne listine in Sektor za informacijske storitve upravnih notranjih zadev.

V Sektorju za registracijo prebivalstva in javne listine je bilo zaposlenih 19 javnih uslužbencev in v Sektorju za informacijske storitve upravnih notranjih zadev 7 javnih uslužbencev.

Naloge s področja upravljanja CRP v Sektorju za registracijo prebivalstva in javne listine izvaja 5 javnih uslužbencev, ostali pa v manjšem obsegu in po potrebi. Koordinacijo osnovnega in dopolnilnega vzdrževanja ter investicij v informacijske rešitve CRP izvajajo javni uslužbenci Sektorja za informacijske storitve upravnih notranjih zadev.

Tabela 1 prikazuje osebe, ki so bile v obdobju, na katero se nanaša revizija, oziroma med izvajanjem revizije odgovorne za poslovanje MNZ.

Tabela 1 Odgovorne osebe MNZ v obdobju, na katero se nanaša revizija, in med izvajanjem revizije

Odgovorna oseba	Obdobje odgovornosti
Sanja Ajanović Hovnik, ministrica za javno upravo v funkciji ministrice za notranje zadeve	do 21. 2. 2023
Boštjan Poklukar, minister za notranje zadeve	od 21. 2. 2023 do 21.11. 2025
Branko Zlobko, minister za notranje zadeve	od 21. 11. 2025 do 4. 6. 2026
Franci Matoz, minister za notranje zadeve in javno upravo	od 4. 6. 2026

9 Uradni list RS, št. 72/06 – uradno prečiščeno besedilo, 3/22 – ZDeb in 32/24.

10 Uradni list RS, št. 70/00 in 28/02.

11 Uradni list RS, št. 8/99 in 43/24.

12 Uradni list RS, št. 107/02.

1.3 Revizijski pristop

Pri izvedbi revizije smo uporabili naslednje metode dela in načine pridobivanja podatkov:

- proučevanje pravnih in drugih podlag ter javno dostopnih podatkov s področja revizije;
- zbiranje, pregled in presojo dokumentacije MNZ;
- analizo pridobljenih podatkov in informacij o upravljanju CRP na MNZ;
- intervjuje in pisna vprašanja MNZ ter
- pregled uporabe in delovanja informacijskih rešitev CRP ter intervjuje z zaposlenimi na MNZ, ki informacijske rešitve CRP upravljajo.

1.4 Predstavitev področja revizije

CRP je osrednja zbirka podatkov:

- o državljanih, ki imajo stalno ali začasno prebivališče v Republiki Sloveniji, in tujcih, ki imajo dovoljenje za stalno ali začasno prebivanje v Republiki Sloveniji;
- o državljanih, ki so stalno ali začasno, za več kot 3 mesece, odsotni iz Republike Slovenije;
- o tujcih, ki v Republiki Sloveniji nimajo dovoljenja za stalno ali začasno prebivanje, imajo pa določene pravice ali obveznosti na področju pokojninskega in invalidskega zavarovanja, davkov, iz humanitarnih razlogov ali na drugem področju, če je tako določeno z zakonom.[13]

Podatki v CRP so enotna matična številka občana (v nadaljevanju: EMŠO), kraj rojstva, ime in priimek, državljanstvo, prebivališče in vrsta prebivališča ter naslovi za vročanje, zakonski stan, šolska izobrazba, volilna pravica, EMŠO matere, EMŠO očeta, EMŠO zakonca, EMŠO otrok, identifikatorji za povezovanje z administrativnimi zbirkami podatkov ter datumi in podatki o dogodkih, spremembah in popravkih.[14]

V CRP se zgoraj navedeni podatki centralno zbirajo, obdelujejo, hranijo in uporabljajo z namenom spremljati stanje in gibanje prebivalstva za potrebe državnih organov in drugih subjektov (v nadaljevanju: institucionalni uporabniki), ki jih ti potrebujejo za opravljanje predpisanih nalog oziroma za vodenje zbirk podatkov o posameznikih ter za namene izvajanja statističnih, socialno-ekonomskih in drugih raziskovanj, za katere imajo zakonsko podlago.

Poleg institucionalnih uporabnikov lahko do podatkov CRP dostopajo tudi uporabniki, ki so fizične osebe (v nadaljevanju: uporabniki fizične osebe), kadar dostopajo do svojih podatkov, če so pooblaščeni za dostop in kadar izvajajo svoje naloge pri institucionalnem uporabniku.

13 3. člen ZCRP.

14 11. člen ZCRP.

Uredba o vodenju in vzdrževanju CRP določa[15], da se CRP vodi kot računalniška podatkovna baza s podatki o trenutnem stanju prebivalstva in z zgodovino podatkov pred nastopom sprememb. MNZ pridobiva podatke od upravljavcev zbirk podatkov, ki jih ob nastanku dogodka po svoji pristojnosti prvi zabeležijo (v nadaljevanju: podatkovni vir). Podatkovna baza vsebuje posamezne evidence, ki so fizično in logično povezane. MNZ je odgovorno za vzdrževanje podatkovne baze ter za vzdrževanje in izboljšanje kakovostne ravni podatkov.[16] Zato mora občasno kontrolirati popolnost zajetja podatkov in primerjati njihovo usklajenost s podatkovnimi viri ali z dejanskim stanjem.[17]

Podatke za vodenje in vzdrževanje CRP pridobiva MNZ na obrazcih ter na uradnih in drugih dokumentih, ki jih upravljavec zbirke podatkov posreduje na papirju, na magnetnih medijih ali z neposredno računalniško povezavo.[18] Z namenom racionaliziranja opravil skupnega pomena lahko MNZ pooblasti upravljavca zbirke podatkov, ki posreduje določene podatke za CRP, za neposredno vzdrževanje teh podatkov v CRP.[19]

Skladno z določbami uredbe o vodenju in vzdrževanju CRP[20] mora MNZ upravljati CRP v skladu z zakonom, ki ureja varstvo osebnih podatkov, in internim aktom o varstvu in zavarovanju osebnih podatkov ter ob upoštevanju tehničnih zmožnosti upravljavskega sistema podatkovne baze.

1.5 Informacijske rešitve CRP

Informacijske rešitve CRP sestavljajo: transakcijska podatkovna zbirka CRP, distribucijska podatkovna zbirka eCRP, spletni servisi, spletne informacijske rešitve, IO Modul in eRISK. Navedene informacijske rešitve so vzpostavljene v okviru informacijskega sistema upravnih notranjih zadev (v nadaljevanju: ISUNZ) in so predstavljene v nadaljevanju tega poročila. ISUNZ gostuje na infrastrukturi državnega računalniškega oblaka, ki ga zagotavlja Ministrstvo za digitalno preobrazbo (v nadaljevanju: MDP), in se povezuje v državno komunikacijsko omrežje HKOM, ki je zasnovano tako, da zagotavlja neprekinjen in zanesljiv prenos podatkov med upravljavcem in odjemalcem. Informacijske rešitve CRP so podvržene tehnološkim zahtevam in tehničnemu varovanju infrastrukturnega okolja MDP.

V letu 2011 je MNZ z Ministrstvom za javno upravo (v nadaljevanju: MJU) sklenilo Dogovor MJU in MNZ o razmejitvi odgovornosti in načinih usklajevanja pri upravljanju ISUNZ[21] (v nadaljevanju: pogodba SLA[22]).

---

15 Prvi odstavek 2. člena uredbe o vodenju in vzdrževanju CRP.

16 Prvi in tretji odstavek 4. člena uredbe o vodenju in vzdrževanju CRP.

17 Tretji odstavek 4. člena uredbe o vodenju in vzdrževanju CRP.

18 18. člen ZCRP.

19 Drugi odstavek 19. člena ZCRP.

20 Prvi odstavek 31. člena uredbe o vodenju in vzdrževanju CRP.

21 Dogovor MJU in MNZ o razmejitvi odgovornosti in načinih usklajevanja pri upravljanju ISUNZ, št. 430-906/2010/45 z dne 22. 2. 2011, Aneks št. 1 k Dogovoru MJU in MNZ o razmejitvi odgovornosti in načinih usklajevanja pri upravljanju ISUNZ, št. 430-906/2010/87 z dne 30. 1. 2012 in Aneks št. 2 k Dogovoru MJU in MNZ o razmejitvi odgovornosti in načinih usklajevanja pri upravljanju ISUNZ, št. 430-906/2010/152 z dne 24. 10. 2012.

22 Angl.: *SLA – Service Level Agreement – pogodba o ravni storitev*. Gre za merljive parametre kakovosti storitev, ki jih mora izvajalec zagotavljati naročniku, kot na primer čas odziva na incidente, čas reševanja napak, dostopnost storitve, pogostost poročanja.

MDP je bilo ustanovljeno 28. 12. 2022[23], ko je od MJU prevzelo naloge na področjih informacijske družbe, elektronskih komunikacij, informatizacije javne uprave, upravljanja informacijsko-komunikacijskih sistemov, zagotavljanja elektronskih storitev javne uprave, delovanja državnega portala eUprava, varnih predalov ter centralne storitve za spletno prijavo in elektronski podpis. S prehodom nalog in pristojnosti z MJU na MDP je MDP vstopilo v pravni položaj MJU kot pogodbena stranka pogodbe SLA. Pogodba SLA natančno določa odgovornosti MNZ in MDP pri razvoju in vzdrževanju informacijskih rešitev in elektronskih storitev. MDP mora zagotavljati ustrezno tehnično informacijsko-komunikacijsko infrastrukturo, ustrezne komunikacijske povezave do produkcijskega in testnega okolja ter tehnično dokumentacijo, zagotavljati mora tudi stabilnost, zanesljivost in učinkovitost elektronskih storitev. MNZ je odgovorno za razvoj in vzdrževanje informacijskih rešitev, ki gostujejo na infrastrukturi državnega računalniškega oblaka, vodi postopke javnih naročil in izbira izvajalce, zagotavlja potrebna sredstva za vzdrževanje in razvoj informacijskih rešitev, od izvajalcev zahteva tehnično brezhibne izdelke, skladne s tehničnimi zahtevami MDP, in obveznost sodelovanja zunanjega izvajalca in MDP. MNZ in MDP skladno s pogodbo SLA sodelujeta pri testiranjih in razvoju elektronskih storitev.

Za vzdrževanje informacijskih rešitev je MNZ z zunanjim izvajalcem sklenilo Pogodbo o vzdrževanju distribucijskega sistema CRP - eCRP in razvoju novih storitev[24] (v nadaljevanju: pogodba o vzdrževanju eCRP in razvoju storitev), ki zajema vzdrževanje in razvoj distribucijske podatkovne zbirke eCRP, spletnih servisov CRP in spletnih informacijskih rešitev CRP, ter Pogodbo o vzdrževanju informacijskega sistema upravnih notranjih zadev (ISUNZ)[25] (v nadaljevanju: pogodba o vzdrževanju ISUNZ), ki zajema vzdrževanje in razvoj transakcijske zbirke podatkov CRP ter še 16 drugih evidenc in registrov, ki pa niso informacijske rešitve CRP.

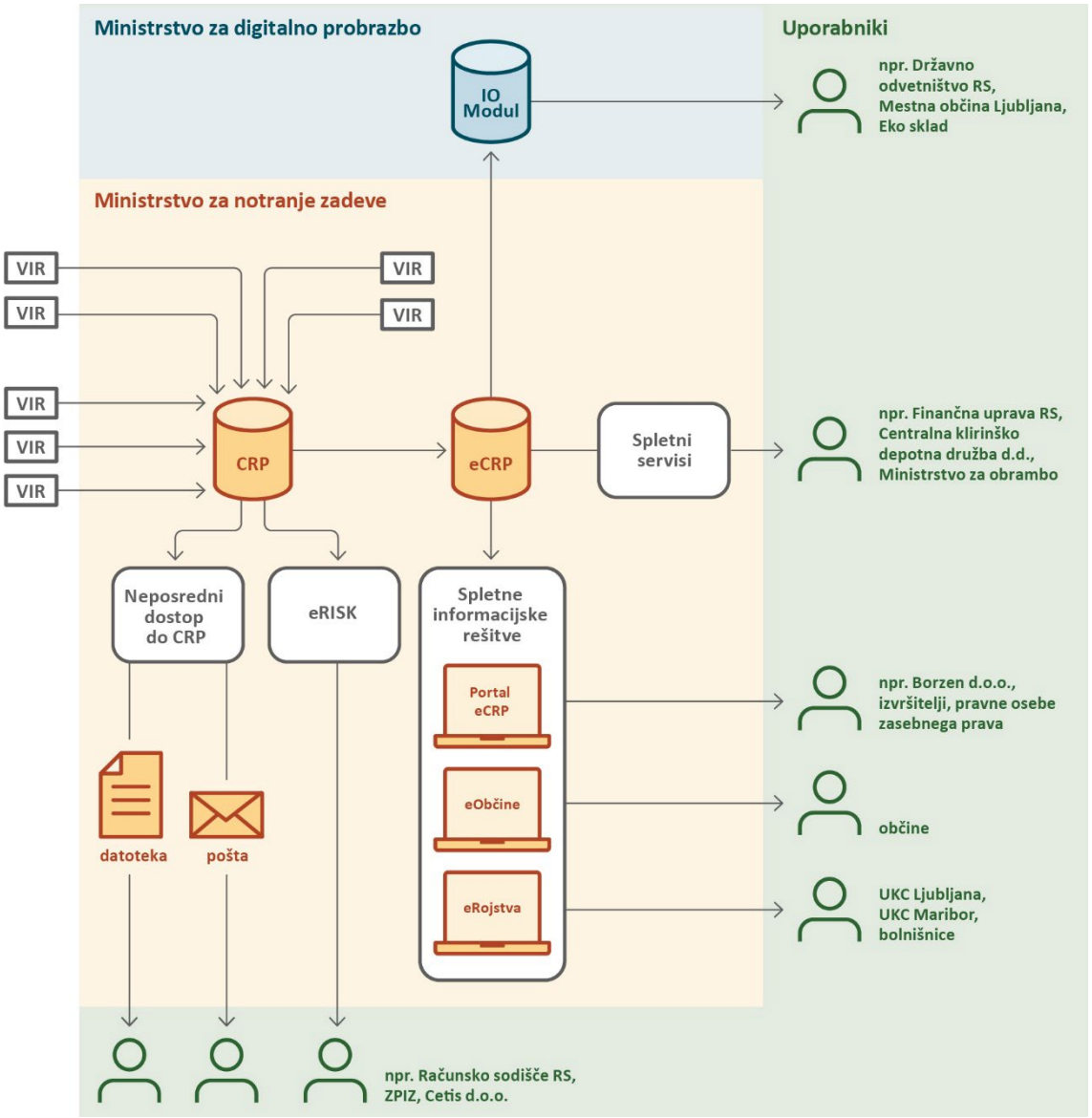
Slika 1 predstavlja distribucijsko shemo CRP s podatkovnimi viri.

23 Zakon o spremembah Zakona o Vladi Republike Slovenije (Uradni list RS, št. 163/22).

24 Št. C1711-22-460230 z dne 20. 9. 2022. K pogodbi je sklenjen Aneks št. 1 k Pogodbi o vzdrževanju distribucijskega sistema CRP - eCRP in razvoju novih storitev, št. C1711-22-460230 z dne 22. 7. 2024.

25 Št. C1711-21-460277 z dne 20. 9. 2021. K pogodbi sta sklenjena 2 aneksa, in sicer Aneks št. 1 k Pogodbi o vzdrževanju informacijskega sistema upravnih notranjih zadev (ISUNZ), št. C1711-21-460277 z dne 18. 7. 2023 in Aneks št. 2 k Pogodbi o vzdrževanju informacijskega sistema upravnih notranjih zadev (ISUNZ), št. C1711-21-460277 z dne 24. 12. 2024.

Slika 1 Distribucijska shema CRP s podatkovnimi viri



Vir: povzeto po podatkih MNZ.

1.5.1 Podatkovni zbirki CRP

CRP sestavljata 2 samostojni podatkovni zbirki:

- transakcijska zbirka podatkov CRP, ki je namenjena zbiranju, obdelavi in hranjenju podatkov v CRP, ki se sproti prepisujejo oziroma neposredno preslikavajo v distribucijsko zbirko podatkov eCRP;
- distribucijska zbirka podatkov eCRP, ki je namenjena posredovanju podatkov iz CRP institucionalnim uporabnikom in uporabnikom fizičnim osebam, ki morajo imeti za to zakonsko podlago; prednost takšne ureditve je, da so podatki pri vseh sodelujočih sočasni in enaki.

1.5.2 Informacijske rešitve za posredovanje podatkov iz CRP

MNZ zaradi različnih zakonskih podlag in specifičnih potreb uporabnikov omogoča več različnih možnosti posredovanja podatkov in je zato razvilo več informacijskih rešitev, ki so predstavljene v nadaljevanju. Informacijski rešitvi, ki omogočata dostop do transakcijske zbirke podatkov CRP, sta:

- neposredni dostop do transakcijske zbirke podatkov CRP, ki omogoča dostop na podlagi ročne poizvedbe uslužbencem MNZ, in
- eRISK, ki omogoča pridobivanje različnih podatkov iz CRP uporabnikom fizičnim osebam za izvajanje nalog pri institucionalnem uporabniku.

Za institucionalne uporabnike ter uporabnike fizične osebe, ki vpogledujejo v lastne osebne podatke, pa MNZ zagotavlja spletne informacijske rešitve za dostop do distribucijske zbirke podatkov eCRP.

1.5.2.1 Neposredni dostop do transakcijske zbirke podatkov CRP

Transakcijska zbirka podatkov CRP omogoča neposredni dostop do podatkov CRP na podlagi ročne poizvedbe. Ročne poizvedbe dnevno izvajajo uslužbenci Sektorja za registracijo prebivalstva in javne listine na podlagi prejetih zaprosil manjših upravičencev do podatkov, kot so na primer odvetniki, izvršitelji. CRP omogoča kreiranje odgovorov oziroma dopisov, v primeru zaprosil za večje število posameznikov pa kreira zbirno datoteko z vsemi podatki.

Upravljanje dostopnih pravic, avtorizacijo in avtentikacijo[26] izvaja MNZ.

1.5.2.2 eRISK

Informacijska rešitev eRISK uporabnikom fizičnim osebam za izvajanje svojih nalog pri institucionalnem uporabniku omogoča pridobivanje različnih podatkov CRP iz transakcijske zbirke podatkov CRP (prek eRISK je mogoč dostop tudi do drugih zbirk podatkov, ki jih upravlja DUNZ, kot so podatki o vozilih in listinah). Informacijsko rešitev eRISK sestavljata 2 modula, in sicer eRISK Dispatcher, ki je skupek servisov, ki omogočajo priklic podatkov, in eRISK DUNZ, ki je uporabniški vmesnik, ki omogoča vpis iskalnih parametrov za priklic podatkov.

Avtentikacijo in avtorizacijo uporabnikov fizičnih oseb, ki izvajajo svoje naloge pri institucionalnem uporabniku, izvaja MNZ.

[26] Avtentikacija je postopek preverjanja identitete uporabnika. Avtorizacija je postopek določanja in preverjanja pravic dostopa avtenticiranega uporabnika do virov informacijskega sistema.

1.5.2.3 Spletne informacijske rešitve

Spletne informacijske rešitve, ki iz distribucijske zbirke podatkov eCRP črpajo podatke, so:

- Portal eCRP, ki je namenjen uporabnikom fizičnim osebam za samostojno iskanje podatkov pri izvajanju nalog pri manjših institucionalnih uporabnikih in uporabnikom fizičnim osebam, ki vpogledujejo v lastne osebne podatke;
- eObčine, ki je namenjena specifičnim potrebam občin, in
- eRojstva, ki jo uporabljajo porodnišnice in je namenjena avtomatizirani določitvi EMŠO otroku takoj po rojstvu.

Avtentikacijo in avtorizacijo uporabnikov fizičnih oseb, ki izvajajo svoje naloge pri institucionalnem uporabniku, in uporabnikov fizičnih oseb, ki vpogledujejo v lastne osebne podatke, zagotavlja MNZ, pri čemer uporabniki fizične osebe dostopajo do podatkov s kvalificiranim digitalnim potrdilom, izdanim s strani enega izmed akreditiranih slovenskih izdajateljev.

1.5.2.4 Spletni servisi eCRP

Spletni servisi eCRP omogočajo institucionalnim uporabnikom prevzem podatkov v svoje sisteme, pri čemer različni servisi omogočajo različne funkcionalnosti. Institucionalni uporabniki v svoje informacijske rešitve dnevno dobivajo spremembe podatkov o osebah, ki jih vodijo v svojih zbirkah podatkov (na primer Zavod za pokojninsko in invalidsko zavarovanje Slovenije, Zavod za zdravstveno zavarovanje Slovenije). Spletne servise za institucionalne uporabnike vzpostavlja in nadzoruje MNZ, avtentikacijo in avtorizacijo uporabnikov fizičnih oseb, ki izvajajo svoje naloge pri institucionalnih uporabnikih, pa izvaja institucionalni uporabnik v informacijskih rešitvah, v katere je prenesel podatke.

1.5.2.5 IO Modul

IO[27] Modul je vhodno/izhodni modul, namenjen institucionalnim uporabnikom za neposredne poizvedbe v CRP po podatkih o posameznih fizičnih osebah. IO Modul je ločena podatkovna zbirka podatkov, kamor se sprotno preslikujejo podatki iz distribucijske podatkovne zbirke eCRP in ki predstavljajo enega izmed virov za Pladenj[28], ki ga upravlja MDP. MNZ posreduje podatke iz eCRP v IO Modul, MDP pa tehnično omogoča poizvedovanje po podatkih iz različnih zbirk podatkov.

Avtentikacijo in avtorizacijo uporabnikov fizičnih oseb, ki izvajajo svoje naloge pri institucionalnem uporabniku, izvaja institucionalni uporabnik sam.

27 Angl.: *IO – Input/Output.*

28 Pladenj je centralna državna informacijska platforma za elektronsko izmenjavo podatkov in dokumentov med informacijskimi sistemi javne uprave v Sloveniji. Uporablja se za povezovanje različnih državnih evidenc, portalov in storitev ter omogoča varno, standardizirano in avtomatizirano komunikacijo med organi državne uprave.

1.6 Stroški vzdrževanja informacijskih rešitev CRP

Materialne stroške osnovnega in dopolnilnega vzdrževanja distribucijske podatkovne zbirke eCRP, spletnih servisov CRP in spletnih informacijskih rešitev CRP po pogodbi o vzdrževanju eCRP in razvoju storitev v obdobju, na katero se nanaša revizija, prikazuje Tabela 2.

Tabela 2 Materialni stroški osnovnega in dopolnilnega vzdrževanja po pogodbi o vzdrževanju eCRP in razvoju storitev v obdobju, na katero se nanaša revizija

v EUR

Stroški	2023	2024	2025 (do 30. 6. 2025)
Osnovno vzdrževanje	28.767,60	28.767,60	14.383,80
Dopolnilno vzdrževanje	171.056,20	217.385,70	73.572,10
SKUPAJ	**199.823,80**	**246.153,30**	**87.955,90**

Vir: podatki MNZ.

Tabela 3 prikazuje materialne stroške osnovnega in dopolnilnega vzdrževanja po pogodbi o vzdrževanju ISUNZ v obdobju, na katero se nanaša revizija.

Tabela 3 Materialni stroški vzdrževanja po pogodbi o vzdrževanju ISUNZ v obdobju, na katero se nanaša revizija

v EUR

Stroški	2023	2024	2025 (do 30. 6. 2025)
Osnovno vzdrževanje	198.302,71	202.500,47	118.319,99
Dopolnilno vzdrževanje	1.047.957,00	1.181.826,74	646.768,40
SKUPAJ	**1.246.259,71**	**1.384.327,21**	**765.088,39**

Vir: podatki MNZ.

1.7 Postopek posredovanja podatkov uporabnikom

Podatki CRP se posredujejo uporabnikom, ki imajo za pridobitev podatkov pravno podlago v zakonu, v pisni zahtevi ali pisni privolitvi posameznika, na katerega se podatki nanašajo. Uporabnikom, ki so za pridobivanje osebnih podatkov pooblaščeni z zakonom, se posredujejo podatki, navedeni v zakonu, in samo za namene, navedene v zakonu.[29]

Zahtevek za pridobitev podatkov iz CRP mora vsebovati obvezno navedbo pravne podlage in namena, za katerega se zahtevajo podatki, opis podatkov in časovni okvir, v katerem se podatki potrebujejo.[30]

29 Prvi in drugi odstavek 26. člena uredbe o vodenju in vzdrževanju CRP.

30 Četrti odstavek 26. člena uredbe o vodenju in vzdrževanju CRP.

Uporabniki lahko podajo posamezne zahtevke za pridobitev podatkov, lahko pa podatke prejemajo v rednih obdobjih.

Za namene elektronskega poslovanja mora MNZ voditi evidenco storitev vnaprej določljivih vrst uporabe podatkov, evidenco institucionalnih uporabnikov, ki izpolnjujejo pogoje za vključitev v elektronsko poslovanje, in pregled pooblastil uporabnikov fizičnih oseb.[31]

Način posredovanja podatkov in konkretno informacijsko rešitev za njihovo posredovanje določi MNZ skupaj z institucionalnim uporabnikom glede na tehnične in vsebinske zmogljivosti ter potrebe institucionalnega uporabnika. Institucionalni uporabniki, ki potrebujejo redno osveževanje podatkov o prebivalstvu za uporabo v svojih informacijskih rešitvah, te praviloma prejemajo prek spletnih servisov. Institucionalni uporabniki, ki potrebujejo podatke več organov, lahko prek Pladnja prejemajo podatke iz IO Modula, drugi institucionalni uporabniki, ki potrebujejo le podatke iz CRP, pa uporabljajo spletne informacijske rešitve ali spletne servise eCRP. MNZ podpiše z institucionalnim uporabnikom dogovor o posredovanju podatkov, ki vsebuje pravno podlago, namen, za katerega uporabnik potrebuje podatke, informacijski sistem za povezovanje, obseg in navedbo podatkov iz CRP, časovni okvir, v katerem jih potrebuje, ter kontaktne osebe in druge vsebine, pomembne za ureditev razmerja med MNZ in institucionalnim uporabnikom.

Po podatkih MNZ je bilo na dan 8. 1. 2025 524 institucionalnih uporabnikov podatkov CRP, in sicer:

- 21 institucionalnih uporabnikov IO Modula (na primer Državno odvetništvo Republike Slovenije, Mestna občina Ljubljana, Eko sklad, Ministrstvo za kulturo);
- 30 institucionalnih uporabnikov, ki so do podatkov dostopali prek spletnih servisov eCRP (na primer Finančna uprava Republike Slovenije, Klirinško depotna družba d.d., Ministrstvo za obrambo, Uprava Republike Slovenije za zaščito in reševanje);
- 96 institucionalnih uporabnikov Portala eCRP (na primer Borzen d.o.o., izvršitelji, pravne osebe zasebnega prava, ki imajo za to pravno podlago);
- 211 institucionalnih uporabnikov eObčine (razen Občine Žužemberk);
- 16 institucionalnih uporabnikov eRojstva (univerzitetna klinična centra Ljubljana in Maribor ter bolnišnice) in
- 150 institucionalnih uporabnikov eRISK (na primer računsko sodišče, Zavod za pokojninsko in invalidsko zavarovanje Slovenije, Cetis d.o.o.).

V letu 2024 je bilo na MNZ rešenih 7.217 ročnih poizvedb, na podlagi teh vlog so bili posredovani osebni podatki o 18.537 osebah. Prek eRISK, spletnih informacijskih rešitev in spletnih servisov eCRP pa je MNZ posredovalo 50,5 milijona osebnih podatkov o osebah na podlagi 399 vlog. Prek IO Modula je bilo institucionalnim uporabnikom posredovano 20,8 milijona podatkov, občine pa so prejele 13,2 milijona zapisov o prebivalcih njihovih občin.[32]

31 Tretji odstavek 27. člena uredbe o vodenju in vzdrževanju CRP.

32 Poročilo o delu MNZ v letu 2024, št. 0101-60/2025/6, april 2025.

2. Ugotovitve

2.1 Načrtovanje in organiziranje informacijske podpore CRP

Da bi ugotovili, ali je MNZ učinkovito načrtovalo in organiziralo informacijsko podporo CRP, smo preverili, ali je imelo MNZ dokumente dolgoročnega načrtovanja, ki se nanašajo na CRP, in ali so ti bili usklajeni z zakonodajo, nacionalnimi usmeritvami na področju eUprave ter s Strategijo digitalnih javnih storitev 2030[33]. Preverili smo tudi, ali je letno načrtovanje aktivnosti, povezanih s CRP, potekalo skladno s strateškimi cilji. Nadalje smo preverili, ali je bila informacijska arhitektura CRP jasno opredeljena, dokumentirana in usklajena s strategijami in cilji, ali so bili poslovni procesi, lastništvo procesov in podatkov ter odgovornosti jasno določeni ter ali je bilo urejeno varovanje informacij in upravljanje tveganj, vključno z vzpostavljenim in redno vzdrževanim registrom tveganj.

2.1.1 Poslovna in IT strategija CRP ter letno načrtovanje CRP

2.1.1.1 Strateško načrtovanje

2.1.1.1.a Upravljavec ključne državne evidence, kot je CRP, bi moral imeti strategijo z opredeljenim namenom, prednostnimi usmeritvami, dolgoročnimi cilji, odgovornostmi, načinom doseganja ciljev in razporeditvijo ključnih virov. Takšna strategija omogoča preglednost upravljanja, načrtovano razvijanje sistema, zagotavljanje potrebnih kadrovskih ter finančnih virov ter merljivost doseganja ciljev. Ugotovili smo, da MNZ v obdobju, na katero se nanaša revizija, ni imelo lastne poslovne strategije CRP niti lastne IT strategije CRP, temveč je sledilo veljavni zakonodaji na področju CRP, kot so elektronsko poslovanje CRP, vodenje in vzdrževanje CRP ter postopek za pridobivanje in posredovanje podatkov. MNZ je sledilo tudi ciljem Strategije digitalnih javnih storitev 2030. Čeprav ta strategija vsebuje splošne cilje digitalizacije javnih storitev, ki jih je mogoče deloma povezati tudi s CRP (na primer interoperabilnost, kakovost podatkov, kibernetska varnost, standardizacija), in je CRP v praksi deloval in se razvijal, pa MNZ brez lastne poslovne strategije CRP in IT strategije CRP povečuje tveganje za neusklajen razvoj, otežuje načrtovanje finančnih in kadrovskih virov ter zmanjšuje preglednost upravljanja ključne državne evidence.

Priporočilo MNZJU

MNZJU priporočamo, naj pripravi in sprejme poslovno strategijo in IT strategijo CRP.

[33] MJU, 2023.

2.1.1.2 Letno načrtovanje

Letno načrtovanje aktivnosti omogoča sistematično pripravo na predvidene spremembe in pravočasno zagotavljanje virov za njihovo izvedbo. MNZ je prihodnje aktivnosti v zvezi z delovanjem CRP načrtovalo v letnih načrtih dela skladno s potrebami. MNZ je tako v letu 2023[34] načrtovalo prilagoditev CRP novemu informacijskemu sistemu IS Kataster Geodetske uprave Republike Slovenije, s predvidenim zaključkom v letu 2024[35]. Poleg tega je MNZ za leto 2024 načrtovalo predlog sprememb in dopolnitev ZCRP[36] in predlog dopolnitev Uredbe o načinu določanja osebne identifikacijske številke[37], ki omogoča večji razpon pri določanju EMŠO, to je več kot 500 posameznikov istega spola, rojenih na isti dan. MNZ je za leto 2025 med drugim načrtovalo[38] tudi posodabljanje informacijskih rešitev z namenom zagotavljanja informacijske varnosti ter več drugih aktivnosti na tem področju.

Letno načrtovanje aktivnosti, ki se nanaša na CRP, je po navedbah MNZ odvisno predvsem od potreb institucionalnih uporabnikov. Kadar je v posameznem predlogu zakona, ki vpliva na poslovanje institucionalnega uporabnika, predvidena nova povezava s CRP (na primer nov vir podatkov za CRP ali sprememba strukture podatkov v CRP), MNZ predlog zakona prejme v medresorsko usklajevanje. Posledično je MNZ tako že seznanjeno s predvidenimi aktivnostmi, ki vplivajo na CRP. MNZ v povezavi s tem običajno predlaga določitev prehodnega obdobja, v katerem po sprejemu zakona ali njegovih sprememb izvede potrebne tehnične rešitve ali spremembe v informacijskih rešitvah in njihovo testiranje. Tehnološke prenove ter nekatere vsebinske prenove je MNZ vnaprej načrtovalo kot operativne cilje in so bile vključene v letni načrt dela in letni plan nadgradenj, ki ga je MNZ posredovalo zunanjemu izvajalcu. V letne načrte dela MNZ in letne finančne načrte so bile vključene tudi nabave za potrebe IT.

2.1.1.2.a Ugotovili smo, da je letno načrtovanje aktivnosti v zvezi s CRP na področju CRP zaradi odsotnosti dolgoročnih strateških dokumentov na področju CRP potekalo v okviru letnih načrtov dela MNZ. To načrtovanje je bilo pretežno odvisno od sprotnih potreb institucionalnih uporabnikov in sprememb zakonodaje. Posledično razvoj informacijskega sistema ni bil usmerjen v optimalno razporeditev virov in dolgoročno izboljšanje njegove učinkovitosti, pač pa v sprotno izpolnjevanje potreb in zakonodajnih zahtev.

2.1.2 Informacijska arhitektura CRP

Informacijska arhitektura CRP je znotraj ISUNZ v okolju Oracle Database. Integracija z ostalimi državnimi informacijskimi sistemi poteka prek varnih vmesnikov in v skladu z najvišjimi informacijsko-varnostnimi smernicami. Uporabljenih je več varnostnih mehanizmov, od PKI[39]

34 Načrt dela Ministrstva za notranje zadeve v letu 2023, št. 020-452/2022/22 z dne 23. 12. 2022.

35 Načrt dela Ministrstva za notranje zadeve v letu 2024, št. 020-45/2024/24 z dne 11. 4. 2024.

36 Zakon o spremembi Zakona o centralnem registru prebivalstva (Uradni list RS, št. 32/24).

37 Uredba o dopolnitvi Uredbe o načinu določanja osebne identifikacijske številke, Uradni list RS, št. 43/24.

38 Načrt dela Ministrstva za notranje zadeve v letu 2025, št. 020-70/2025/33 z dne 29. 4. 2025.

39 Angl.: *PKI – Public Key Infrastructure*. Infrastruktura javnih ključev je sistem, sestavljen iz strojne in programske opreme, politik, postopkov in organov, ki omogoča zanesljivo in varno komunikacijo z uporabo javnega in zasebnega ključa, ki ga je izdal certificiran izdajatelj.

certifikatov, LDAP[40] (varnostna shema RPAS) do digitalnih certifikatov, ki onemogočajo nepooblaščene dostope do podatkov.

MNZ je, upoštevaje pomembnost informacijske arhitekture CRP, razdelilo zadolžitve za postavitev informacijske arhitekture CRP. Uporabljeni postopki, orodja in tehnike so bili standardizirani in dokumentirani. Določena je bila večnivojska arhitektura, tehnologija informacijskih rešitev CRP je Oracle 19c. Servisi eCRP so bili izdelani v okolju podatkovne baze Oracle z uporabo programskega jezika PL/SQL. Uporabljena je bila sodobna tehnologija za razvoj informacijskih rešitev CRP (kot na primer JavaScript, CSS3, HTML5). MNZ ima model za informacijsko arhitekturo CRP, s katerim si je olajšalo optimalno ustvarjanje, uporabo in izmenjavo informacij na način, ki ohranja celovitost in je poleg tega prilagodljiv, funkcionalen, pravočasen, varen in zavarovan, če bi prišlo do odpovedi. MNZ je imelo skupne šifrante in registre, iz katerih aplikacije črpajo podatke.

MNZ je imelo za dokumentiranje informacijske arhitekture CRP izdelano informacijsko rešitev Big picture, ki omogoča celosten pogled na informacijsko arhitekturo CRP. Vzdrževal jo je zunanji izvajalec, ki je vsako novo različico odložil na odložišče datotek, MNZ pa jo je kot skrbnik preneslo v strežniško okolje MNZ-DUNZ, do katerega so imeli dostop le zaposleni znotraj DUNZ z dodeljenimi pravicami do strežniškega okolja MNZ-DUNZ, torej le avtorizirane zaposlene osebe znotraj DUNZ.

MNZ je pri informacijski arhitekturi CRP sledilo usmeritvam Strategije digitalnih javnih storitev 2030 in operativnim ciljem, ki zajemajo:

- zagotavljanje operativnega delovanja informacijskih rešitev CRP;
- izvajanje rednih penetracijskih testov v sodelovanju z MDP in zunanjim izvajalcem;
- poenostavitev in pospeševanje upravnih postopkov ter zmanjšanje z njimi povezanih stroškov;
- zagotovitev 99,9 % dostopnosti eCRP uporabnikom in drugo.

Večji del posodobitve informacijske arhitekture CRP se je usklajevalo zaradi implementacije zakonodaje s področja upravnih notranjih zadev, v kolikor so te uvajale širši nabor podatkov od podatkov, ki so se vodili v evidenci, oziroma je bila za implementacijo potrebna vzpostavitev integracije z drugim informacijskim sistemom. MNZ je poslovne usmeritve in operativne cilje prilagajalo tudi potrebam uporabnikov oziroma poenostavitvi in pohitritvi upravnih postopkov, na primer izmenjava podatkov med informacijskimi sistemi prek IO Modula, Pladnja in podobno. Posledično pa se je skladno s tem dopolnjevala tudi informacijska arhitektura CRP. Vse poslovne usmeritve so bile usklajene z zunanjim izvajalcem, ki je te informacijske rešitve tudi razvijal in prilagajal potrebam MNZ oziroma potrebam uporabnikov.

2.1.2.a MNZ je pripravilo informacijsko arhitekturo CRP z jasno opredelitvijo informacijskih sistemov in medsebojnih povezav ter jasno določenimi standardi za izmenjavo podatkov. Pri tem je MNZ sledilo operativnim ciljem, Strategiji digitalnih javnih storitev 2030, smernicam MDP in Generičnim tehnološkim zahtevam.

40 Angl.: *LDAP – Lightweight Directory Access Protocol*. Gre za omrežni protokol, ki se uporablja za avtentikacijo uporabnikov in upravljanje uporabniških računov.

2.1.3 Poslovni procesi CRP

Znotraj MNZ je bil za naloge, povezane z registracijo prebivalstva in s tem tudi za upravljanje CRP, pristojen DUNZ oziroma znotraj njega Sektor za registracijo prebivalstva in javne listine ter Sektor za informacijske storitve upravnih notranjih zadev.

2.1.3.a MNZ je opredelilo odgovornosti in naloge za informacijsko podporo CRP. MNZ je formalno opredelilo razmerja z zunanjimi izvajalci in večjim delom uporabnikov, s katerimi je sklenilo dogovore. Ugotovili smo, da je MNZ imelo opredeljene poslovne procese za CRP, določene lastnike procesov in podatkov.

2.1.4 Informacijska varnostna politika

Na MNZ so bile v avgustu 2024 sprejete politike in pripadajoči dokumenti – navodila s področja informacijske varnosti MNZ in Inšpektorata Republike Slovenije za notranje zadeve, in sicer:

- Krovna informacijska varnostna politika Ministrstva za notranje zadeve[41],
- Področna politika upravljanja informacijskih sistemov Ministrstva za notranje zadeve,
- Področna politika upravljanja omrežja Ministrstva za notranje zadeve,
- Področna politika uporabe informacijskih sistemov in omrežja Ministrstva za notranje zadeve,
- Navodilo Ministrstva za notranje zadeve o uporabi elektronske pošte in spletnih storitev,
- Navodilo za izvajanje analize vpliva na poslovanje ter analize in obravnave tveganj varovanja informacij in neprekinjenega poslovanja Ministrstvo za notranje zadeve[42],
- Načrt odzivanja Ministrstva za notranje zadeve na incidente informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave,
- Navodilo o izvajanju storitev Varnostnega operativnega centra Ministrstva za notranje zadeve,
- Področna politika storitev podatkovnega centra Ministrstva za notranje zadeve,
- Navodilo o upravljanju in uporabi informacijsko-komunikacijskih sredstev v Ministrstvu za notranje zadeve,
- Področna politika neprekinjenega poslovanja Ministrstva za notranje zadeve,
- Področna politika uporabe informacijskih sistemov in omrežja Ministrstva za notranje zadeve za pogodbene izvajalce in
- Navodilo za izvajanje varnostnega foruma, notranje presoje in vodstvenega pregleda informacijske varnosti na MNZ.

Od februarja 2024 deluje na MNZ tudi varnostno-obveščevalni center, ki skrbi za spremljanje in odzivanje na varnostne dogodke in incidente s področja informacijske varnosti v omrežju in informacijskih sistemih MNZ. Glede na specifične lastnosti ISUNZ, ki gostuje na državnem računalniškem oblaku, je ISUNZ podvržen tudi varnostnim politikam MDP.

41 Št. 007-103/2024/26 z dne 26. 7. 2024.

42 Št. 007-111/2024/13, z dne 26. 7. 2024.

Krovna informacijska varnostna politika MNZ je skupaj s področnimi politikami informacijske varnosti določala cilje in namene MNZ in Inšpektorata Republike Slovenije za notranje zadeve pri ohranjanju zaupnosti, celovitosti in razpoložljivosti podatkov, informacijskih sistemov in omrežja. Načrtovanje in uresničevanje krovne informacijske varnostne politike MNZ in področnih politik je bilo del procesov organiziranja in splošne strukture vodenja MNZ, varnost pa del zasnove vseh informacijskih storitev, poslovnih procesov in organiziranja dela pri varnosti podatkov, informacijskih sistemov in omrežja.

MNZ je želelo s politikami doseči naslednje cilje:

- zavarovati podatke, informacijske sisteme in omrežja pred nepooblaščenim dostopom;
- ohraniti celovitost podatkov, informacijskih sistemov in omrežja ter preprečiti nepooblaščene spremembe;
- zagotoviti razpoložljivost podatkov, informacijskih sistemov in omrežja, ki jih zaposleni, pogodbeni sodelavci in druge za to upravičene osebe potrebujejo za izvajanje svojih delovnih nalog;
- ozaveščati zaposlene, pogodbene sodelavce in druge za to upravičene osebe o pomenu informacijske varnosti in neprekinjenega poslovanja MNZ;
- vzpostaviti beleženje vseh zakonsko zahtevanih aktivnosti nad podatki, informacijskimi sistemi in omrežji;
- ustrezno obravnavati vse varnostne dogodke in incidente informacijske varnosti, ki vplivajo na podatke, informacijske sisteme in omrežja;
- raziskovati sume kršitev informacijskih varnostnih politik;
- zagotoviti skladnost MNZ z zakoni in predpisi na področju informacijske varnosti in neprekinjenega poslovanja;
- upoštevati priporočila in dobre prakse, ki temeljijo na standardih informacijske varnosti in neprekinjenega poslovanja.[43]

Na MNZ je pred sprejetjem teh dokumentov veljala Krovna politika varovanja informacij MNZ RS[44].

2.1.4.a Ugotovili smo, da je MNZ v povezavi z varovanjem informacij v letu 2024 sprejelo Krovno informacijsko varnostno politiko Ministrstva za notranje zadeve in pripadajoče dokumente, ki so nadomestili Krovno politiko varovanja informacij MNZ RS. Krovna informacijska varnostna politika MNZ naslavlja sodobna informacijska tveganja, vključno z naprednimi kibernetskimi grožnjami, upravljanji identitet ter zahtevami veljavne zakonodaje. S tem MNZ zmanjšuje tveganja varnostnih incidentov in neskladnosti z regulatornimi zahtevami.

43 Krovna informacijska varnostna politika Ministrstva za notranje zadeve.

44 Št. 024-10/2009/251 z dne 1. 2. 2011.

2.1.5 Upravljanje tveganj

MNZ je imelo vzpostavljen in vzdrževan register tveganj – analizo nevarnosti in oceno tveganj – za podatkovni zbirki CRP ter za informacijske rešitve za posredovanje podatkov, ki ga je redno letno posodabljalo. MNZ je upoštevalo usmeritve in sistematičen pristop k obvladovanju tveganj informacijske varnosti, kot je navedeno v dokumentu Metodologija obvladovanja tveganj informacijske varnosti v državni upravi[45].

Z vzpostavitvijo informacijskih varnostnih politik na MNZ v letu 2024 je MNZ sprejelo tudi Navodilo za izvajanje analize vpliva na poslovanje ter obravnave tveganj informacij in neprekinjenega poslovanja MNZ, ki določa, da se najmanj enkrat letno preveri ocena tveganja. V obseg ocenjevanja tveganj se vključijo vse grožnje, povezane z materialnimi, nematerialnimi, človeškimi in informacijskimi sredstvi v poslovnih procesih. MNZ je imelo pripravljen tudi katalog groženj tako za informacijske sisteme kot tudi za strojno, programsko in komunikacijsko opremo.

Postopek ocenjevanja tveganj je bil sledeč:

- analiza in prepoznavanje tveganj informacijsko-komunikacijskih sistemov;
- ugotavljanje groženj in ranljivosti;
- ocena verjetnosti nastanka incidenta;
- ocena posledic nastanka incidenta in
- ocena tveganja.

2.1.5.a Ugotovili smo, da je MNZ upravljalo tveganja v informacijski podpori CRP in je imelo vzpostavljen register tveganj ter ga je letno vzdrževalo. Za informacijske rešitve CRP je imelo oblikovan okvir za obvladovanje tveganj IT, ki je bil skladen z okvirom MNZ za upravljanje tveganj, to je z Navodilom za izvajanje analize vpliva na poslovanje ter obravnave tveganj informacij in neprekinjenega poslovanja MNZ in z Metodologijo obvladovanja tveganj informacijske varnosti v državni upravi, ki sta opredeljevala, kdaj in kako pripraviti ocene tveganj v vzpostavljenem registru tveganj, ki ga je MNZ vzdrževalo in dokumentiralo. Izračunane in opredeljene so bile celotne in dogovorjene ravni IT tveganj.

2.2 Razvoj, spremembe, posodobitve in vzdrževanje CRP ter njihova vpeljava

V reviziji smo preverili, ali je MNZ poslovne zahteve glede informacijske podpore CRP formalno odobrilo ter ali je razvoj in uvajanje sprememb izvajalo skladno z internimi procesi in dobro prakso (vključno z vodenjem verzij, načrtovanjem in dokumentiranjem testiranj, odločitvami o ustreznosti za produkcijo, načrtovanimi prenosi in potrditvami odgovornih oseb pri prenosu v produkcijo). Poleg tega smo preverili, ali so bila pravna razmerja z zunanjim izvajalcem urejena s pogodbo, ki je upoštevala tehnološke zahteve, varstvo osebnih podatkov ter postopke naročanja, dokumentiranja,

45 MJU, z dne 20. 12. 2019.

komunikacije, poročanja in sodelovanja, ter ali je MNZ redno spremljalo izvajanje pogodbenih obveznosti zunanjega izvajalca. Nazadnje smo presojali, ali je MNZ imelo uporabniška in tehnična navodila za uporabo CRP ter ali je zagotavljalo usposabljanje novih uporabnikov.

2.2.1 Poslovne zahteve v povezavi z informacijsko podporo CRP

Tehnične specifikacije, ki so bile priloga pogodbe o vzdrževanju ISUNZ in pogodbe o vzdrževanju eCRP in razvoju storitev, so opredeljevale aktivnosti in postopke, ki so se nanašali na naročila dopolnilnega vzdrževanja informacijskih rešitev CRP (nadgradnje, nameščanje verzij, podpora naročniku MNZ).

2.2.1.a MNZ je sledilo postopkom, določenim v pogodbah, tako da je poslovno zahtevo oziroma zahtevo za nadgradnjo ali dopolnitev informacijskih rešitev CRP v primeru izkazane potrebe zaradi spremembe zakonodaje, poenostavitve postopkov, odprave pomanjkljivosti v informacijskih rešitvah CRP in v podobnih primerih naslovilo na zunanjega izvajalca. MNZ je vsebinsko opredelilo zahtevo, ki se je podrobneje razčlenila prek vprašanj izvajalca in odgovorov MNZ. Izvajalec je nato podal oceno stroškov in časa realizacije. MNZ je zahtevo potrdilo oziroma jo je nadalje razčiščevalo. Zunanji izvajalec je pristopil k realizaciji po pisni odobritvi MNZ. Ugotovili smo, da je MNZ poslovne zahteve pred razvojem in spremembami v povezavi z informacijsko podporo CRP pisno odobrilo.

2.2.2 Razvoj, vzdrževanje in vpeljava sprememb informacijskih rešitev CRP

Vzdrževanje in razvoj celotnega informacijskega sistema ISUNZ, vključno s podatkovnimi zbirkami CRP in nanje povezanimi informacijskimi rešitvami za posredovanje podatkov, je izvajalo MNZ oziroma zanj zunanji izvajalec, s katerim je imelo MNZ sklenjeno pogodbo o vzdrževanju ISUNZ in pogodbo o vzdrževanju eCRP in razvoju storitev.

MNZ je pri razvoju, vzdrževanju in vpeljavi sprememb informacijskih rešitev CRP sledilo postopkom, določenim v pogodbah in dobri praksi, in sicer na način, da po pisni odobritvi MNZ zunanji izvajalec pristopi k realizaciji oziroma k razvoju nove rešitve ali spremembe v razvojnem okolju. Nova verzija informacijske rešitve se je najprej postavila na testno okolje. MNZ je s testiranjem preverilo ustreznost rešitve. V primeru pomanjkljivosti ali neustrezne realizacije je o tem obvestilo zunanjega izvajalca, ki je izvedel popravek in na testno okolje namestil novo verzijo informacijske rešitve. Na takšen način je potekalo testiranje, vse dokler novost ni bila ustrezna za postavitev v produkcijsko okolje oziroma v realno uporabo. Poleg vsebinskega usklajevanja je bila vsaka zahteva obravnavana tudi na mesečnih sestankih MNZ z zunanjim izvajalcem, kjer se je zahteve umeščalo v terminski plan za realizacijo, po potrebi pa so se reševala tudi vprašanja, povezana s koordinacijo morebitnih vsebinskih neskladij ali potrebe po vključevanju drugih akterjev. Na mesečnih sestankih je bilo prisotno vodstvo DUNZ, o realizaciji posameznih aktivnosti pa se je redno poročalo tudi na kolegijih DUNZ.

MNZ je izvajalo testiranje informacijskih rešitev CRP. Testiranje je temeljilo na vsebinski zahtevi, torej se je testiralo to, kar se je spreminjalo ali dopolnjevalo. Ko je bila nadgradnja informacijske rešitve nameščena na testno okolje, so bili o tem obveščeni vodja sektorja, ki vsebinsko pokriva področje, ter druge osebe, ki so bile vsebinsko vključene v pripravo in usklajevanje zahteve.

Določili so se roki za testiranja, po potrebi je bil na internem sestanku dogovorjen tudi podrobnejši plan testiranja. V primeru, da je bilo treba v testiranje vključiti tudi institucionalnega uporabnika podatkov, se je izvedel dogovor o skupnem testiranju. Ob testiranjih so se izvajali tudi negativni testi, kar je omogočalo preverjanje, ali so se ustrezno preprečevale napake. O testiranju je potekala komunikacija med MNZ in zunanjim izvajalcem po elektronski pošti. Uspešnost testiranja je bila predpogoj za namestitev nadgradnje ali dopolnitve v produkcijsko okolje. Časovni okvir testiranja ter predvidene namestitve v produkcijsko okolje je bil dogovorjen na mesečnih koordinacijah, kjer je bilo prisotno tudi vodstvo DUNZ. O aktivnostih se je redno poročalo na kolegijih DUNZ.

Nove verzije informacijskih rešitev CRP se je na produkcijsko okolje nameščalo v skladu z urnikom namestitev in vzdrževanj, ki ga je pripravilo MDP za vsako koledarsko leto za vse uporabnike, ki so gostovali v okolju MDP. Nameščanje se je praviloma izvajalo enkrat mesečno (MNZ tretjo sredo v mesecu). Občasno se je nove verzije po predhodnem dogovoru z MDP nameščalo tudi izven rednih terminov, ki jih je MNZ prilagajalo zakonskim rokom.

MNZ je imelo vzpostavljena 2 SVN repozitorija[46] za vodenje verzij informacijskih rešitev. SVN repozitorij je bil vzpostavljen v strežniškem okolju MDP in je bil namenjen odlaganju kode za nameščanje novih verzij na testno in produkcijsko okolje. V okolju MNZ pa je bil vzpostavljen drug SVN repozitorij za namen odlaganja celotne izvorne kode. Za namestitev nove verzije na testno okolje je zunanji izvajalec oddal izvorno kodo v SVN repozitorij na okolju MDP. Ob namestitvi na produkcijsko okolje je zunanji izvajalec oddal izvorno kodo še v SVN repozitorij na okolju MNZ. Na SVN repozitoriju v okolju MDP so bile tako vse verzije, na SVN repozitoriju v okolju MNZ pa le produkcijske verzije.

2.2.2.a Ugotovili smo, da je MNZ, ki gostuje na državnem komunikacijskem omrežju HKOM oziroma državnem računalniškem oblaku, pri razvoju, vzdrževanju in vpeljavi sprememb informacijskih rešitev CRP sledilo smernicam MDP, podanim v Generičnih tehnoloških zahtevah, in postopkom, določenim v pogodbi o vzdrževanju ISUNZ in pogodbi o vzdrževanju eCRP in razvoju storitev. MNZ je imelo vzpostavljena 3 informacijska okolja, in sicer razvojno, testno in produkcijsko okolje, kar predstavlja dobro prakso upravljanja informacijskih sistemov, saj omogoča varno načrtovanje, razvoj, testiranje in uvajanje brez vpliva na produkcijsko delovanje. Takšna ureditev zmanjšuje tveganja za napake, motnje v delovanju in izgubo podatkov.

2.2.2.b MNZ je imelo vzpostavljeno vodenje verzij informacijskih rešitev, vodili so se načrti in zapisniki testiranj, dokumentirane so bile odločitve o ustreznosti za produkcijo. Prenosi v produkcijo so bili opravljeni skladno s pravili uvajanja sprememb, določenih v pogodbah z zunanjim izvajalcem, ki so vključevala potrditev odgovornih oseb za produkcijsko izvajanje. Prenosi novih verzij v produkcijo so bili načrtovani in izvedeni v naprej določenih terminih, ki so bili dogovorjeni z MDP, kar je omogočalo boljšo organizacijo aktivnosti ter zmanjšanje tveganja za nepredvidene posege v informacijski sistem CRP.

46 Angl.: *Subversion Repository*. To je okolje, v katerem sta shranjeni programska koda in zgodovina sprememb.

2.2.3 Upravljanje pravnih razmerij z zunanjimi izvajalci storitev informacijskih rešitev CRP

V obdobju, na katero se nanaša revizija, je imelo MNZ sklenjene 3 pogodbe z zunanjimi izvajalci, in sicer pogodbo SLA z MDP za gostovanje na infrastrukturi državnega računalniškega oblaka in 2 pogodbi za vzdrževanje ISUNZ ter vzdrževanje eCRP in razvoj novih storitev.

Namen pogodbe SLA je bil razmejiti odgovornost pri varovanju osebnih podatkov in določiti ravni informacijsko-komunikacijskih storitev, ki jih za podatke in informacijske sisteme, katerih upravljavec je MNZ in ki gostujejo na infrastrukturi državnega računalniškega oblaka, izvaja MDP. V pogodbi SLA sta bila podrobneje opredeljena namen in predmet dogovora ter določena razmejitev odgovornosti MDP in MNZ pri razvoju in vzdrževanju centralnih aplikacij in elektronskih storitev. Pogodba SLA je vsebovala tudi 7 prilog, ki so:

- Analiza učinka na poslovanje (BIA[47]);
- Matrika odgovornosti po segmentih in aplikacijskih sistemih oziroma modulih;
- Matrika postopkov tipa strank, statusa zakonske obveze in obratovalnega časa za potrebe načrtovanja režima zagotavljanja storitev;
- Tabela postopkov, vsebinskega skrbnika in obsega ter lokacije uporabnikov;
- Odzivni časi po posameznih komponentah;
- Navodila enotne vstopne točke (v nadaljevanju: EVT)[48] za izvajanje specifičnih situacij ter
- Protokol medsebojnega obveščanja in usklajevanja, ki natančneje opredeljuje:
  - tehnične skrbnike pogodbe SLA;
  - obveščanje EVT v primeru nepredvidenih in napovedanih dogodkov, ki povzročijo izpad storitve;
  - podatke za stalno povezavo med sistemskima ekipama Policije in MDP ter
  - postopek vključitve novih informacijskih rešitev v podporo.

2.2.3.a Ugotovili smo, da se pogodba SLA iz leta 2011 sklicuje na Zakon o varstvu osebnih podatkov (ZVOP-1)[49], ki je prenehal veljati v letu 2023. MNZ pogodbe SLA ni uskladilo z zahtevami Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES[50] (v nadaljevanju: splošna uredba o varstvu podatkov) in Zakonom o varstvu osebnih podatkov[51] (v nadaljevanju: ZVOP-2), ki je pričel veljati v letu 2023. Pogodba SLA sicer opredeljuje obdelavo osebnih podatkov oziroma obveznosti MJU in MNZ, ne opredeljuje pa obveznosti

47 Angl.: *Business Impact Analysis.*

48 EVT je enotna vstopna točka na MDP, ki predstavlja prvo raven podpore za vse storitve, ki so prevzete v podporo na MDP.

49 Uradni list RS, št. 94/07 – uradno prečiščeno besedilo,177/20 – ZVOPKD in 163/22 – ZVOP-2.

50 UL L 119, 4. 5. 2016, str. 1.

51 Uradni list RS, št. 163/22 in 40/25 – ZinfV-1.

sodelovanja pri uresničevanju pravic posameznikov in obveznosti poročanja pri kršitvah, niti pravice MNZ po nadzoru nad spoštovanjem določil pogodbe na področju obdelave osebnih podatkov.

Ukrep MNZ

MNZ je 9. 9. 2025 pozvalo MDP k sklenitvi nove pogodbe SLA in 18. 5. 2026 predlagalo MDP usklajevalni sestanek v zvezi z novo pogodbo SLA.

2.2.3.b Pogodbi z zunanjim izvajalcem sta določali izvedbene roke, prevzeme pogodbenega dela, plačilne pogoje ter obveznosti in odgovornosti MNZ in zunanjega izvajalca. Prav tako sta določali skrbnike pogodb, finančno zavarovanje za dobro izvedbo pogodbenih obveznosti in pogodbeno kazen v primeru zamude, kot tudi pogodbena določila o varovanju osebnih podatkov v skladu s splošno uredbo o varstvu podatkov. Obe pogodbi z zunanjim izvajalcem sta se sklicevali na tehnične specifikacije in Generične tehnološke zahteve za razvoj informacijskih rešitev, opredeljeni so bili postopki ob naročilu namestitve spremembe, dokumentiranja, zagotavljanja programske opreme, redna komunikacija, poročanje in sodelovanje z naročnikom. Realizacija se je redno mesečno preverjala na skupnih sestankih in z mesečnimi poročili zunanjega izvajalca.

Ugotovili smo, da je imelo MNZ z zunanjim izvajalcem sklenjeni pogodbi, ki sta bili opredeljeni kot pogodbi za vzdrževanje informacijskih rešitev, v okviru pogodbenih obveznosti pa so bile kot dopolnilno vzdrževanje vključene tudi aktivnosti, ki pomenijo razvoj in uvedbo novih funkcionalnosti oziroma nadgradnjo obstoječih informacijskih rešitev CRP. Takšne aktivnosti, ki se nanašajo na razvoj novih funkcionalnosti ali povečujejo uporabnost, kapaciteto ali življenjsko dobo, pa po vsebini predstavljajo investicijsko vlaganje v programsko opremo ter pomenijo investicijski strošek in ne materialni strošek. Zaradi evidentiranja razvoja IT rešitev med materialne stroške namesto med investicijske odhodke ni bila zagotovljena ustrezna ločitev med tekočo porabo in investicijskimi vlaganji. Takšna obravnava zmanjšuje preglednost strukture porabe javnih sredstev ter otežuje presojo učinkovitosti izvedenih investicij.

Priporočilo MNZJU

MNZJU priporočamo, naj izdatke, ki se nanašajo na razvoj novih funkcionalnosti ali nadgradnjo sistema, obravnava kot investicijo v neopredmetena osnovna sredstva ter prilagodi pogodbe z zunanjimi izvajalci, tako da bodo jasno opredeljene razvojne aktivnosti, in sicer na način, da bodo ločene od storitev rednega vzdrževanja ter nadgradenj, ki ne povečujejo funkcionalnosti sistema.

2.2.4 Navodila in izobraževanje uporabnikov CRP

MNZ je imelo za vse uporabnike spletnih servisov CRP (eRojstva, Portal CRP, in eObčine) izdelana uporabniška navodila, ki jih je ob spremembah posodabljalo. Uporabniška navodila so se nahajala na vstopni maski za posamezne spletne informacijske rešitve. MNZ je po potrebi in na prošnjo institucionalnih uporabnikov organiziralo tudi spletno izobraževanje za nove uporabnike spletnih servisov in usposobilo nove uporabnike CRP. Tako je v letu 2024 za Zavod Republike Slovenije za zaposlovanje, v letu 2025 pa za Zavod za zdravstveno zavarovanje Slovenije izvedlo spletno

izobraževanje v zvezi s servisom za določanje EMŠO. MNZ je za navedeni usposabljanji za spletne servise prejelo pozitivne odzive uporabnikov. Izdelana so tudi uporabniška navodila za eRISK.

Pri spletnih servisih je imelo MNZ pripravljeno tehnično dokumentacijo, ki jo je institucionalni uporabnik potreboval za povezovanje svoje baze podatkov s podatki v CRP. MNZ dodatnih izobraževanj ni izvajalo, ker gre za bazne servise, ki so integrirani neposredno v informacijske sisteme pri posameznih institucionalnih uporabnikih in ki zato ne potrebujejo dodatnega izobraževanja za njihovo uporabo.

MNZ je imelo za vse informacijske rešitve CRP izdelano tudi tehnično dokumentacijo za produkcijsko okolje.

2.2.4.a Ugotovili smo, da je v obdobju, na katero se nanaša revizija, MNZ imelo uporabniška in tehnična navodila za informacijske rešitve CRP, ki so vključevala način delovanja in uporabe informacijskih rešitev CRP ter pogoje povezovanja. MNZ je glede na potrebe institucionalnih uporabnikov organiziralo in izvedlo izobraževanja ter usposobilo nove uporabnike CRP. Vzpostavljena navodila in izvajanje izobraževanj so po naši oceni predstavljali primerno podporo uporabnikom in obvladovanje tveganj, povezanih z uporabo informacijskih rešitev CRP.

2.3 Izvajanje in podpiranje CRP

V reviziji smo preverili, ali je imelo MNZ urejeno upravljanje storitev za institucionalne uporabnike (vključno z ažurnimi evidencami uporabnikov, pravnimi podlagami, nameni uporabe in sklenjenimi dogovori, ki so omejeni na upravičen obseg podatkov ter skladni s predpisi o varstvu osebnih podatkov), ali je zagotavljalo ustrezen sistem dodeljevanja in nadzora dostopnih pooblastil na podlagi dokumentiranih zahtev, ali je uporabnikom nudilo podporo ter ali je imelo urejene ključne varnostne kontrole, predvsem varnostno kopiranje in preizkušanje obnovitev podatkov ter vzpostavljen sistem revizijskih sledi za vpise, spremembe, izbrise in vpoglede v podatke.

2.3.1 Upravljanje storitev za institucionalne uporabnike

Postopek vključevanja institucionalnih uporabnikov v sistem prejemanja podatkov iz CRP se je začel s povpraševanjem institucionalnega uporabnika po zagotovitvi podatkov. MNZ se je, če je bilo to potrebno, z institucionalnim uporabnikom sestalo in se glede na zakonske okvire, potrebe institucionalnega uporabnika ter glede na obseg in vrsto podatkov ter tehnične zmogljivosti z njim dogovorilo o načinu dostopa in informacijsko rešitev za zagotavljanje podatkov iz CRP. MNZ je pripravilo predlog dogovora ter kratko obrazložitev potreb in pravnih podlag ter dokumente uskladilo in podpisalo z institucionalnim uporabnikom. MNZ je v dogovorih z institucionalnimi uporabniki za dostop do podatkov CRP poleg pravne podlage, namena, obdobja in obsega podatkov ter informacijskih rešitev opredelilo tudi način medsebojne komunikacije in reklamacije v zvezi z delovanjem informacijske rešitve ter varovanjem osebnih podatkov, kar ni bilo zajeto v drugih dokumentih, izdanih za namen pridobivanja osebnih podatkov, kot so zahtevki za pridobitev podatkov, soglasja komisije za sprejemanje tehničnih standardov za priključevanje uporabnikov CRP, soglasja upravljavca davčnega registra ali odločbe Informacijskega pooblaščenca.

Iz predložene dokumentacije in obrazložitev MNZ izhaja, da se je postopek priprave dogovora MNZ z institucionalnim uporabnikom začel s kreiranjem številke dogovora v MFERAC[52], kjer je mogoče spremljati status dogovora in morebitne anekse. Dogovore in drugo gradivo je pripravil DUNZ v sodelovanju z institucionalnim uporabnikom. Pregledali in potrdili so jih Sektor za registracijo prebivalstva in javne listine, DUNZ ter pooblaščene osebe za varstvo osebnih podatkov, pravne in finančne službe. Zgodovina potrjevanja se je beležila v interni evidenci za elektronsko potrjevanje gradiv. Pred podpisom pristojnega ministra so dogovor ponovno potrdili Sektor za registracijo prebivalstva in javne listine, DUNZ, državna sekretarka in kabinet ministra.

2.3.1.a Ugotovili smo, da MNZ ni imelo oblikovanega standardiziranega osnutka dogovora, ki bi ga dosledno uporabljalo pri vseh odobrenih posredovanjih osebnih podatkov iz CRP institucionalnim uporabnikom ter ki bi ga za posameznega institucionalnega uporabnika prilagodilo glede na njegove posebnosti. MNZ je dogovore pripravljalo posamično, brez skupnih izhodišč in smernic ter brez kontrolnih seznamov ali drugih oblik preverjanja skladnosti in popolnosti. Standardiziran osnutek dogovora namreč poveča učinkovitost pri sklepanju dogovorov, zmanjšuje možnost napak, podvajanja dela in pravnih neskladij ter omogoča učinkovitejšo rabo kadrovskih in organizacijskih virov. Četudi je MNZ imelo dokumentirano potrjevanje dokumentov v interni evidenci, pa to zaradi odsotnosti formalno opredeljenega procesa vključevanja novih institucionalnih uporabnikov podatkov CRP z opredeljenim postopkom priprave, usklajevanja ter potrjevanja dogovorov in prilog glede na konkretne okoliščine in konkretnega institucionalnega uporabnika ter zaradi odsotnosti standardiziranega osnutka dogovora s potrebnim naborom prilog ni zagotavljalo celovite kontrole in vključitve vseh ključnih elementov (na primer pravna podlaga, odgovorne osebe za izvajanje posameznih rednih postopkov in postopkov v primeru napak in težav, varnostni ukrepi za zagotavljanje zaupnosti in integritete osebnih podatkov, soglasja upravljavcev drugih registrov) v pripravo dogovorov in njihovo obravnavo pred podpisom (povezava s točkama 2.3.1.c in 2.3.1.d).

Priporočilo MNZJU

MNZJU priporočamo, naj:

- *oblikuje standardiziran vzorec dogovora z institucionalnimi uporabniki podatkov CRP z bistvenimi elementi dogovora in nabora prilog ter zagotovi njegovo redno posodabljanje;*
- *oblikuje kontrolne sezname ali drugo obliko preverjanja skladnosti in popolnosti dogovora in prilog.*

MNZ je vodilo razvid uporabnikov podatkov CRP za spletne servise eCRP, spletne informacijske rešitve in eRISK v varnostnih shemah.

2.3.1.b Ugotovili smo, da je MNZ v obdobju, na katero se nanaša revizija, zagotavljalo podatke iz CRP 1 institucionalnemu uporabniku brez zahtevka za pridobitev podatkov in ne da bi sklenilo dogovor o zagotavljanju podatkov. Iz predložene dokumentacije ni razvidno, s kakšnim postopkom in na podlagi katerega dokumenta je MNZ institucionalnega uporabnika 18. 2. 2009 ob namestitvi

52 MFERAC je informacijska rešitev, ki podpira poslovanje proračunskih uporabnikov na finančnem, računovodskem in plačno-kadrovskem področju ter omogoča vnos in evidenco pogodb.

informacijske rešitve eRISK v produkcijo vključilo v prejemanje podatkov iz CRP. MNZ tako ni opredelilo niti pravne podlage in namena niti kdo je odgovoren za izvajanje posameznih rednih postopkov in postopkov v primeru napak in težav, prav tako niso bili določeni varnostni ukrepi za zagotavljanje zaupnosti in integritete osebnih podatkov, zaradi česar bi lahko prišlo do podvajanja ali neizvršitve določenih nalog ter neučinkovite medsebojne koordinacije.

Ukrep MNZ

MNZ je z institucionalnim uporabnikom 27. 3. 2026 sklenilo pogodbo o obdelavi in dostopu do podatkov CRP.

2.3.1.c MNZ je v obdobju, na katero se nanaša revizija, zagotavljalo podatke iz CRP 2 institucionalnima uporabnikoma brez sklenjenega dogovora, temveč le na podlagi soglasja komisije za sprejemanje tehničnih standardov za priključevanje uporabnikov CRP, in 2 institucionalnima uporabnikoma brez sklenjenega dogovora, temveč le na podlagi odločbe Informacijskega pooblaščenca. Iz dokumentov je bila razvidna le potrditev ustreznosti pravne podlage in namena ter ustreznosti zagotavljanja varstva osebnih podatkov po tedaj veljavnem zakonu, ki opredeljuje varstvo osebnih podatkov, niso pa bile dogovorjene niti odgovorne osebe za izvajanje posameznih rednih postopkov in postopkov v primeru napak in težav niti niso bili medsebojno dogovorjeni varnostni ukrepi za zagotavljanje zaupnosti in integritete osebnih podatkov.

2.3.1.d Ugotovili smo, da je MNZ imelo sklenjene dogovore z 11 institucionalnimi uporabniki za večji obseg podatkov, kot je dovoljevala zakonska podlaga, pri čemer je MNZ v 5 primerih dovoljevalo dostop do večjega obsega podatkov zaradi potreb institucionalnega uporabnika. Ugotovili smo tudi, da je imelo MNZ v 1 primeru sklenjen dogovor, iz katerega obseg podatkov ni bil razviden.

Ukrep MNZ

MNZ je v dogovore, ki so bili sklenjeni v letu 2026, vneslo zahtevo, da mu institucionalni uporabniki takoj posredujejo informacijo o spremembi katerekoli okoliščine, ki bi vplivala na dogovor in dostop do osebnih podatkov. Dogovori vsebujejo določbo o obveznosti obeh pogodbenih strank, da se obveščata o vseh zadevah in okoliščinah, ki bi lahko vplivale na izvajanje dogovora. V primeru, da se za uporabnika spremeni pravna podlaga ali namen posredovanja podatkov, je uporabnik dolžan upravljavca pisno obvestiti takoj po uveljavitvi predpisa. Prav tako dogovori vsebujejo obveznost obeh pogodbenih strank, da se nemudoma obvestita o spremembah podatkov kontaktnih oseb.

2.3.1.e MNZ je po uveljavitvi ZVOP-2 v letu 2023 sicer pristopilo k uskladitvi dogovorov, ki jih je imelo sklenjene z občinami, s splošno uredbo o varstvu podatkov in ZVOP-2, vendar je do konca obdobja, na katero se nanaša revizija, uskladilo le 65 dogovorov z občinami[53]. MNZ tako pri dostopih do osebnih podatkov v CRP z dogovori, ki jih še ni prilagodilo in niso bili usklajeni, ni zagotavljalo

[53] Na dan 4. 4. 2025

natančnejše opredelitve obveznosti MNZ in institucionalnih uporabnikov pri izpolnjevanju pravic posameznikov v primeru zahteve za dostop do informacij kdo vse, kdaj in zakaj je dostopal do osebnih podatkov posameznikov, opredelitev tehničnih in organizacijskih ukrepov za zaščito podatkov, zagotavljanje obveznosti obveščanja in sodelovanja ter nadzora in revizije nad spoštovanjem obveznosti institucionalnega uporabnika.

Pojasnilo MNZJU

Aktivnost prenove pogodbenih razmerij z občinami ni bila zaključena, ker je MNZ med procesom prenove pogodbenih razmerij prejelo odločbo Informacijskega pooblaščenca, št. 0612-101/2024/9 z dne 25. 3. 2025 (v nadaljevanju: odločba IP), s katero je bilo MNZ naloženo, da občinam preneha omogočati, da paketno dostopajo in paketno izvažajo osebne podatke posameznikov iz CRP. MNZ je navedeno odločbo IP dne 2. 4. 2025 izvršilo in občinam prenehalo paketno izvažati osebne podatke iz CRP. MNZ je zoper izdano odločbo IP vložilo tožbo. V upravnem sporu do 3. 7. 2026 še ni bilo odločeno. MNZJU bo z aktivnostjo prenove pogodbenih razmerij z občinami nadaljevalo, ko bo sodišče odločilo v upravnem sporu in ko bo na podlagi vsebine sodne odločbe znano, na kakšen način bo v prihodnje potekalo posredovanje podatkov občinam.

Ukrep MNZJU

MNZJU je julija 2026 pripravilo načrt aktivnosti za pregled in uskladitev pogodbenih razmerij z institucionalnimi uporabniki podatkov iz CRP. S tem bo v dogovorih zagotovilo upoštevanje zakonskih določb, ki dovoljujejo dostop in opredeljujejo obseg podatkov iz CRP, zakonskih določb s področja varstva osebnih podatkov ter določitev odgovornih oseb za izvajanje rednih postopkov in postopkov v primeru napak in težav. V načrtu aktivnosti je opredelilo posamezne aktivnosti, njihove nosilce in roke izvedbe.

2.3.2 Zagotavljanje sistema dodeljenih dostopnih pooblastil

MNZ za dodeljevanje pravic uporabnikom Portala CRP uporablja 2 varnostni shemi, in sicer varnostno shemo RPAS in varnostno shemo na Portalu CRP. V varnostno shemo RPAS se dodeljujejo pravice uporabnikom portalov eObčine in eRojstva, v varnostni shemi Portala CRP pa uporabniške pravice vseh uporabnikov Portala CRP. Pri uporabi servisov eCRP in IO Modula se izvaja posredovanje podatkov do drugega upravljavca, ki mora avtentikacijo in avtorizacijo uporabnikov fizičnih oseb izvajati sam, MNZ pa zagotavlja dnevnike dela oziroma žurnale za posredovanje podatkov do drugega upravljavca. MNZ vodi uporabnike eRISK v varnostni shemi RPAS.

Avtentikacijo in avtorizacijo uporabnikov fizičnih oseb za dostop do informacijskih rešitev ISUNZ, katerega manjši del je tudi CRP, zagotavlja MNZ prek namenske aplikacije RPAS. Uporabnik fizična oseba, ki ima ustrezne pravice za dostop do informacijskih rešitev, lahko prek vstopnega portala oziroma s klicem baznega ali spletnega servisa pridobi podatke iz informacijskih rešitev ISUNZ.

Uporabniki fizične osebe morajo za dostop do podatkov v ISUNZ uporabiti uporabniško ime in geslo oziroma je dostop v določenih primerih možen z uporabo digitalnega potrdila, ki je bilo izdano pri slovenskih akreditiranih izdajateljih. Veljavnost dostopov z gesli je 254 dni, veljavnost dostopov z digitalnimi potrdili pa je vezana na veljavnost digitalnega potrdila.

Postopek dodeljevanja pravic uporabnikom fizičnim osebam se prične tako, da odgovorna oseba institucionalnega uporabnika in uporabnik fizična oseba izpolnita obrazec MNZ za dodeljevanje dostopnih pooblastil. Obrazec se posreduje na MNZ bodisi pisno bodisi prek elektronske pošte, na podlagi česar pooblaščeni administrator varnostne sheme skladno z navedeno ustrezno zakonsko podlago in podatki na obrazcu dodeli pravice za dostop. Pravice v CRP so razdeljene na različne vloge (pregledovalec CRP, referent CRP, skrbnik CRP).

Odgovornost za sporočanje vseh sprememb v zvezi s pravicami dostopa, vključno z odvzemom pravic posameznega uporabnika fizične osebe, je na odgovorni osebi institucionalnega uporabnika, ki je zaprosila za dostop do ISUNZ oziroma CRP.

Postopek dodeljevanja pravic za občine se prične tako, da predstojnik občine za vsakega uporabnika fizično osebo izpolni obrazec – Vloga za dodelitev pravic uporabniku za dostop do portala eObčine, ki ga posreduje upravljavcu MNZ. MNZ po prejemu vloge za dodelitev pravic opravi avtentikacijo uporabnika fizične osebe in o tem obvesti občino. Podatke in številko digitalnega potrdila uporabnika fizične osebe vnese v varnostno shemo. Po opravljeni avtentikaciji lahko uporabniki fizične osebe dostopajo do podatkov CRP prek portala eObčine.

Občina se ob sklenitvi dogovora o obdelavi, posredovanju in dostopanju do osebnih podatkov iz CRP, s katerim upravlja MNZ, prek portala eObčine zaveže, da dostop do osebnih podatkov, ki jih obdeluje, omogoči samo tistim osebam občine, ki so se zavezale k zaupnosti ali so ustrezno statusnopravno zavezane glede zaupnosti, in samo glede na izkazano potrebo po dostopu do podatkov.

Občina je dolžna MNZ nemudoma pisno obvestiti o ukinitvi dostopnih pravic uporabnika fizične osebe občine. Odgovornost za sporočanje vseh sprememb v zvezi s pravicami dostopa, vključno z odvzemom pravic posameznemu uporabniku fizični osebi, je na odgovorni osebi občine, ki je zaprosila za dostop do portala eObčine.

Na smiselno enak način potekata tudi avtentikacija in avtorizacija za uporabo portalov eCRP in eRojstva, do katerih se dostopa z digitalnimi potrdili.

Za stalno kontrolo, upravljanje in podporo varnostne sheme ISUNZ so zadolženi pooblaščeni administratorji varnostne sheme na MNZ.

Pri uporabi servisov eCRP in IO Modula se izvaja posredovanje podatkov do drugega upravljavca, ki mora avtentikacijo in avtorizacijo uporabnikov fizičnih oseb izvajati sam, MNZ pa zagotavlja dnevnike dela oziroma žurnale za posredovanje podatkov do drugega upravljavca.

MNZ navaja, da dostopna pooblastila dodeljuje po tem, ko se sklene dogovor o posredovanju podatkov iz CRP in ko predstojnik institucije poda zahtevo, da se določenim fizičnim osebam, zaposlenim pri instituciji, dodelijo pravice za pridobivanje osebnih podatkov.

2.3.2.a Na podlagi dokumentacije, tehničnih in uporabniških navodil ter vpogleda v delovanje informacijskih rešitev CRP smo ugotovili, da je MNZ z upravljanjem varnostnih shem oziroma s pravili administracije institucionalnih uporabnikov in uporabnikov fizičnih oseb zagotavljalo sistem dodeljenih dostopnih pooblastil do informacijskih rešitev CRP, ki so bila omejena glede na vloge. Dostopna pooblastila je MNZ dodeljevalo v skladu s pravili administracije institucionalnih uporabnikov in uporabnikov fizičnih oseb. Omenjene dostope je dodelilo samo na podlagi

dokumentiranih in potrjenih uporabniških zahtev. Opredeljeni in nadzorovani so bili vsi dostopi z najvišjimi pooblastili.

2.3.2.b Ugotovili smo, da je MNZ v letu 2025 začelo z izvajanjem preverjanja dostopnih pravic uporabnikov fizičnih oseb, zaposlenih pri institucionalnih uporabnikih, in sicer z vidika, če so še bili upravičeni do dostopov ali če so bile ob prenehanju ali spremembi delovnega mesta njihove uporabniške pravice ukinjene, ni pa tega preverjalo periodično. Odgovornost za sporočanje vseh sprememb v zvezi s pravicami dostopa, vključno z odvzemom pravic posameznemu uporabniku fizični osebi, je na odgovorni osebi institucije, ki je zaprosila za dostop do CRP. Priporočljivo pa je, da MNZ za zmanjšanje tveganja neustreznih, zastarelih ali prekomernih dostopnih pravic periodično izvaja preglede dodeljenih uporabniških pravic ter preverja, ali so te še vedno ustrezne glede na dejanske potrebe uporabnikov.

2.3.2.c Na podlagi vpogleda v sezname institucionalnih uporabnikov spletnih servisov eCRP smo ugotovili, da je MNZ v informacijski rešitvi sicer imelo vpogled v seznam aktivnih institucionalnih uporabnikov, vendar teh podatkov ni moglo samostojno izvoziti. Celosten vpogled v seznam vseh institucionalnih uporabnikov, tako aktivnih kot neaktivnih, in možnost izvoza podatkov je imel le zunanji izvajalec, ki je vzdrževal informacijsko rešitev, ne pa tudi pooblaščeni administratorji na MNZ. Takšna odvisnost od zunanjega izvajalca lahko povzroča zamude pri pridobivanju podatkov in izvajanju kontrol ter povečuje administrativne obremenitve pri spremljanju institucionalnih uporabnikov.

Ukrep MNZJU

MNZJU je 22. 6. 2026 pogodbenemu izvajalcu naročilo nadgradnjo informacijske rešitve za dopolnitev z izpisi celotnega seznama vseh uporabnikov v informacijskih rešitvah CRP.

2.3.3 Zagotavljanje pomoči uporabnikom

Zagotavljanje podpore uporabnikom predstavlja pomembno aktivnost, ki prispeva k učinkoviti uporabi informacijskih rešitev CRP ter nemotenemu zagotavljanju podatkov iz CRP. Pravočasna in kakovostna pomoč uporabnikom omogoča hitrejše reševanje težav, zmanjšuje prekinitve pri delu in tveganja napak pri uporabi informacijskih rešitev CRP ter prispeva k pravilni in enotni uporabi informacijskih rešitev CRP.

2.3.3.a Ugotovili smo, da je imelo MNZ vzpostavljen tako sistem za pomoč uporabnikom kot tudi sistem odpravljanja napak. Skladno s pogodbo SLA je imelo MNZ zagotovljeno prvo raven podpore prek EVT, in sicer predvsem na področju težav z dostopi do informacijskih rešitev, pozabljenih ali pretečenih gesel ter na področju obveščanja institucionalnih uporabnikov in uporabnikov fizičnih oseb o predvidenih oziroma možnih motnjah pri delovanju informacijskih rešitev. EVT je vse primere evidentirala, vključno s primeri, ki jih je EVT predala MNZ v nadaljnje reševanje. MNZ je zagotavljalo pomoč uporabnikom na način, da je imelo z institucionalnimi uporabniki sklenjene dogovore, v katerih so bile navedene kontaktne osebe, e-naslovi in telefonske številke, na katere so lahko uporabniki fizične osebe, ki so zaposleni pri institucionalnih uporabnikih, prek spletnih servisov sporočali napake ali težave pri uporabi servisov. Napake ali težave s CRP pa so zaposleni na MNZ

sporočali prek posebnega sistema komentarjev in na ta način ažurno komunicirali z zunanjim izvajalcem.

2.3.4 Izvajanje varnostnega kopiranja podatkov in rednih testiranj

V skladu s pogodbo SLA je MDP v sklopu nudenja gostovanja izvajalo tudi varovanje dostopa do podatkov, izdelavo varnostnih kopij in njihovo shranjevanje ter morebitno obnavljanje podatkov ob upoštevanju dokumentiranih in usklajenih zahtev. Tako bi se lahko v primeru izpada storitev podatkovnega centra MDP vse funkcije, ki se izvajajo v prizadetem podatkovnem centru, prestavile v sekundarni podatkovni center.

V primeru poškodbe ali izgube podatkov v informacijskem sistemu in podatkovnih bazah se podatki zagotovijo iz varnostnih kopij. Ob poškodbah je treba najprej opraviti analizo in ugotoviti čas nastanka škode/izgube podatkov in njen obseg, nato pa iz varnostnih kopij zagotoviti zadnjo kopijo podatkov. Ob poškodovanju oziroma izgubi podatkov ima MNZ 2 možnosti:

- nadaljevanje z uporabo podatkov iz varnostne kopije ali
- vrnitev podatkov v stanje pred izgubo/poškodbo.[54]

Natančnejši opis varnostnega kopiranja in restavriranja podatkov v sklopu celotnega MNZ, ki vključuje tudi ISUNZ, je opredeljen v dokumentu Postopki neprekinjenega poslovanja in načrti okrevanja MNZ – ISUNZ.

2.3.4.a Ugotovili smo, da je imelo MNZ v skladu s pogodbo SLA v sklopu nudenja gostovanja zagotovljeno varovanje dostopa do podatkov, izdelavo varnostnih kopij in njihovo shranjevanje ter morebitno obnavljanje podatkov ob upoštevanju dokumentiranih in usklajenih zahtev. Tako bi se lahko v primeru izpada storitev podatkovnega centra MDP vse funkcije, ki so se izvajale v prizadetem podatkovnem centru, prestavile v sekundarni podatkovni center. Izvajali so se testni preklopi s primarne lokacije na rezervno lokacijo in obratno, s čimer se je preverjalo nemoteno delovanje produkcijskih (Oracle) baz ISUNZ, med katerimi je tudi CRP. Navedeno sta izvajala MDP in njegov zunanji izvajalec v sodelovanju MNZ. MNZ testnega preklopa na rezervno lokacijo za leto 2024 ni izvedlo. Kot razlog je MNZ navedlo nujne nadgradnje informacijskih rešitev. V letu 2023 je bil samoiniciativno izveden testni preklop, pripravljen je bil tudi zapisnik. Preklop predhodno ni bil obvezujoč, je pa obvezen od leta 2025, ko je MNZ oblikovalo postopke neprekinjenega poslovanja in načrte okrevanja. Varnostne kopije podatkov so shranjene za 14 dni nazaj za vse podatkovne baze ISUNZ, kar pomeni, da se lahko katerokoli bazo povrne v katerikoli trenutek v zadnjih 14 dneh. Varnostne kopije za ISUNZ nastajajo v sklopu MDP, ustvarja jih zunanji izvajalec. ISUNZ informacijske rešitve uporabljajo podatkovne baze Oracle, ki imajo funkcionalnost Data Guard, ki omogoča varnostno kopijo v realnem času. Ta funkcionalnost zagotavlja stalno razpoložljivost, obnovitev po katastrofi oziroma varnostnem incidentu in varnost podatkov kot takih. MNZ je letno testiralo in restavriralo podatke z varnostnih kopij, zapisalo ugotovitve testiranja in sprejelo potrebne ukrepe.

54 Pogodba SLA.

2.3.5 Upravljanje revizijske sledi

Revizijska sled v informacijskem sistemu predstavlja temeljni mehanizem zagotavljanja sledljivosti uporabniških aktivnosti, sprememb podatkov ter delovanja sistemskih procesov, saj omogoča celovito rekonstrukcijo dogodkov in ugotavljanje odgovornosti za izvedene aktivnosti. Revizijska sled zmanjšuje tveganje nepooblaščenih dostopov, nepooblaščenih sprememb podatkov in omogoča zaznavanje in preiskovanje varnostnih incidentov.

2.3.5.a MNZ je imelo v skladu z 22. členom ZVOP-2 vzpostavljen sistem revizijskih sledi, to je dnevnik obdelave za naslednje obdelave osebnih podatkov: zbiranje, spreminjanje, vpogled, razkritje (vključno s prenosi), izbris in druga dejanja obdelave, ki jih določa ZVOP-2. Za vse informacijske rešitve CRP, s katerimi je upravljalo, je imelo vzpostavljen sistem revizijskih sledi z natančnim časovnim zapisom v obliki dnevnikov dela, kar je omogočalo pregled vseh zapisov, povezanih z vsemi poslovnimi dogodki in vsemi shranjenimi informacijami, od nastanka podatka ali informacije dalje do trenutnega stanja. Ta sistem je v celoti upošteval smernice mednarodno uveljavljenih standardov varovanja informacij, kot so standardi iz družine ISO/IEC 27000[55], splošna uredba o varstvu podatkov ter ZVOP-2. Ob vsakem priklicu podatkov so se ne glede na način priklica (spletni servis ali neposredni vpogled) zabeležili podatki, ki so naknadno omogočili ugotavljanje, kdaj, komu in na kakšen način so bili osebni podatki posredovani ter za kakšen namen. Odgovorna oseba za dostop do dnevnikov dela je bila pooblaščena oseba na MNZ.

MNZ je vodilo podatke o paketnih obdelavah, ki so jih prožili posamezni institucionalni uporabniki iz eCRP, vzpostavljen je bil dnevnik obdelave. MNZ je vodilo tudi podatke o spremembah osebnih podatkov, ki so se beležili v dnevnik obdelave.

2.4 Spremljanje in nadziranje CRP

V reviziji nas je zanimalo, ali je MNZ učinkovito spremljalo in nadziralo aktivnosti v zvezi z informacijsko podporo CRP, zato smo preverili, če je MNZ področje informacijske podpore CRP redno obravnavalo na sestankih in upoštevalo na sestankih sprejete sklepe ter ali je zagotovilo redno poročanje odgovornih oseb vodstvu o aktivnostih v zvezi z razvojem in izvajanjem informacijske podpore CRP. Zanimalo nas je tudi, ali je MNZ redno izvajalo nadzor nad izpolnjevanjem načrtovanih aktivnosti, izpolnjevanjem ciljev ter sprejemom morebitnih korektivnih ukrepov ter ali je na področju CRP izvajalo notranje kontrole in revizije.

2.4.1 Spremljanje CRP in zagotavljanje učinkovitega nadzora nad izvajanjem CRP

2.4.1.a MNZ je izvajalo redne mesečne sestanke, vezane na področje informacijske podpore CRP, na katerih so bili prisotni generalni direktor DUNZ ali njegov namestnik, vodja Sektorja za informacijske storitve upravnih notranjih zadev, vodja Sektorja za registracijo prebivalstva in javne

[55] ISO/IEC 27000 je družina mednarodnih standardov za upravljanje informacijske varnosti, ki jih je objavila Mednarodna organizacija za standardizacijo (ISO) v sodelovanju z Mednarodno elektrotehniško komisijo (IEC).

listine, tehnični skrbnik pogodbe in predstavniki zunanjega izvajalca, s čimer je MNZ zagotovilo odobritev, spremljanje in potrjevanje sprememb v informacijskem sistemu CRP. V okviru mesečnih sestankov so bili obravnavani terminski načrti nadaljnjih aktivnosti, odprta naročila, realizacija dogovorov oziroma sklepov, sprejetih na preteklih sestankih, in finančna realizacija sklenjenih pogodb, reševala pa so se tudi odprta vprašanja in neskladja ter obravnavale potrebe po vključevanju drugih udeležencev. Redni mesečni sestanki so zagotavljali stalno medsebojno interakcijo in stalen nadzor nad realizacijo dogovorjenih aktivnosti. Komunikacija je potekala tudi dnevno, in sicer komunikacija med tehničnim skrbnikom pogodbe in zunanjim izvajalcem v zvezi z naročanjem in realizacijo posameznih zahtev in reševanjem posameznih vprašanj.

Ugotovili smo, da je MNZ področje informacijske podpore CRP redno obravnavalo na sestankih in upoštevalo sklepe iz zapisnikov teh sestankov. Zagotavljalo je tudi redno poročanje odgovornih oseb vodstvu o aktivnostih v zvezi z razvojem in izvajanjem informacijske podpore CRP. Vodstvo odgovornih organizacijskih enot je bilo namreč prisotno na rednih sestankih z zunanjim izvajalcem, kjer je izvajalo nadzor nad izpolnjevanjem načrtovanih aktivnosti, izpolnjevanjem ciljev in sprejemom morebitnih korektivnih ukrepov ter izvajalo notranje kontrole.

2.4.1.b Informacijske rešitve CRP v obdobju, na katero se nanaša revizija, še niso bile predmet notranje oziroma zunanje revizije, ki omogoča sistematično in neodvisno oceno izvajanja postopkov, spremljanje skladnosti z veljavnimi zakoni, predpisi in internimi akti ter identifikacijo morebitnih pomanjkljivosti ali nepravilnosti.

Priporočilo MNZJU

MNZJU priporočamo, naj v okviru notranje revizije načrtuje in izvede tudi revizije informacijskih rešitev CRP.

2.4.2 Izvajanje aktivnosti na podlagi ugotovitev nadzora

2.4.2.a MNZ je spremljalo razvoj in delovanje informacijskih rešitev CRP, obravnavalo težave, napake in reklamacije ter izvajalo aktivnosti za njihovo reševanje na mesečnih sestankih. Na rednih mesečnih sestankih je MNZ izvajalo stalen nadzor nad realizacijo dogovorjenih aktivnosti, sprejemalo ukrepe za izvedbo rešitev v primeru morebitnih odklonov pri načrtovanih aktivnostih ter spremljalo tudi izvedbo sprejetih ukrepov.

Ugotovili smo, da je MNZ izvajalo ukrepe za odpravo posameznih zaznanih pomanjkljivosti delovanja informacijskih rešitev CRP, ki so bile obravnavane na rednih mesečnih sestankih, ter spremljalo in nadzorovalo ter izvajalo aktivnosti za vse spremembe in dopolnitve, vendar pa ni zagotovilo izvajanja neodvisnih preveritev, saj v okviru notranje ali zunanje revizije še ni izvedlo revizije informacijskih rešitev CRP (povezava s točko 2.4.1.b).

3. Mnenje

Revidirali smo učinkovitost Ministrstva za notranje zadeve pri upravljanju Centralnega registra prebivalstva (CRP) v obdobju od 1. 1. 2023 do 30. 6. 2025.

Mnenje smo oblikovali na podlagi presoje, ali je Ministrstvo za notranje zadeve učinkovito načrtovalo in organiziralo CRP, učinkovito upravljalo z razvojem, spremembami, posodobitvami in vzdrževanjem CRP ter njihovo vpeljavo, učinkovito izvajalo in podpiralo CRP ter učinkovito spremljalo in nadziralo CRP. Menimo, da je Ministrstvo za notranje zadeve v obdobju, na katero se nanaša revizija, **učinkovito** upravljalo CRP. Ministrstvo za notranje zadeve je zagotavljalo nemoteno delovanje informacijskih rešitev CRP in podporo uporabnikom. Razvoj, spremembe in vzdrževanje CRP je upravljalo po dokumentiranih postopkih z jasno določenimi odgovornostmi, obvladovalo je tveganja, izvajalo in podpiralo CRP ter redno spremljalo aktivnosti informacijske podpore CRP. Poslovanje Ministrstva za notranje zadeve je bilo tako v pretežnem delu skladno s sodili za presojo učinkovitosti. Ugotovili pa smo, da Ministrstvo za notranje zadeve ni imelo lastne poslovne in IT strategije CRP in ni celovito uredilo dogovorov z institucionalnimi uporabniki podatkov iz CRP, saj je nekaterim podatke zagotavljalo brez popolne dokumentacije oziroma zakonske podlage.

V zvezi z načrtovanjem in organiziranjem informacijske podpore CRP smo ugotovili, da Ministrstvo za notranje zadeve ni imelo lastne poslovne strategije CRP niti lastne IT strategije CRP, temveč je sledilo ciljem Strategije digitalnih javnih storitev 2030, ki vsebuje strateške cilje digitalizacije javnih storitev, ki jih je Ministrstvo za notranje zadeve pri informacijskih rešitvah CRP upoštevalo. Letno načrtovanje aktivnosti, povezanih s CRP, je potekalo v okviru letnih načrtov dela in letnih planov nadgradenj, ki so bili posredovani zunanjemu izvajalcu. To načrtovanje je bilo pretežno odvisno od sprotnih potreb institucionalnih uporabnikov in sprememb zakonodaje. Ministrstvo za notranje zadeve je pripravilo informacijsko arhitekturo CRP na način, da je bila ta jasno opredeljena in dokumentirana. Na Ministrstvu za notranje zadeve je izvajanje poslovnih procesov CRP v praksi potekalo in se nemoteno izvajalo, poslovni procesi CRP so bili popisani, določeni so bili lastniki procesov in podatkov, določene so bile tudi odgovornosti in naloge za informacijsko podporo CRP. Ministrstvo za notranje zadeve je v povezavi z varovanjem informacij sprejelo Krovno informacijsko varnostno politiko Ministrstva za notranje zadeve in pripadajoče dokumente. Prav tako je upravljalo tveganja v informacijski podpori CRP in imelo vzpostavljen ter vzdrževan register tveganj.

V zvezi z upravljanjem z razvojem, spremembami, posodobitvami in vzdrževanjem CRP ter njihovo vpeljavo smo ugotovili, da je imelo Ministrstvo za notranje zadeve z zunanjim izvajalcem sklenjeni pogodbi za razvoj, spremembe in vzdrževanje CRP. Poslovne zahteve v povezavi z informacijsko podporo CRP je pred razvojem in spremembami pisno odobrilo. Ministrstvo za notranje zadeve je pri razvoju, vzdrževanju in vpeljavi sprememb informacijskih rešitev CRP sledilo postopkom, določenim v pogodbah in z dobro prakso. Vzpostavljeno je imelo vodenje verzij informacijskih rešitev, vodili so se načrti in zapisniki testiranj, odločitve o ustreznosti za produkcijo so bile dokumentirane. Prenosi v produkcijo so bili načrtovani in opravljeni skladno s pravili uvajanja sprememb, določenih v pogodbah z zunanjim izvajalcem, ki vključujejo potrditev odgovornih oseb za produkcijsko izvajanje. Odnosi z zunanjim izvajalcem so bili formalno opredeljeni. Ministrstvo za notranje zadeve pogodbe SLA z Ministrstvom za digitalno preobrazbo ni uskladilo z zahtevami Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES in Zakonom o varstvu osebnih podatkov (ZVOP-2), ki je pričel veljati v letu 2023. Pogodbi z zunanjim izvajalcem sta jasno

določali roke, obveznosti, plačila, nadzor, varovanje podatkov in tehnične zahteve, pri čemer je uvedba novih funkcionalnosti oziroma nadgradnja obstoječih informacijskih rešitev CRP v pogodbah vključena kot dopolnilno vzdrževanje, čeprav gre po vsebini za investicijsko vlaganje. Realizacija pogodbenih obveznosti se je redno mesečno preverjala na skupnih sestankih in z mesečnimi poročili zunanjega izvajalca. Ministrstvo za notranje zadeve je imelo uporabniška in tehnična navodila za informacijske rešitve CRP, glede na potrebe institucionalnih uporabnikov pa je organiziralo in izvedlo izobraževanja ter usposobilo nove uporabnike CRP.

V zvezi z izvajanjem in podpiranjem CRP smo ugotovili, da je pri upravljanju storitev za institucionalne uporabnike način posredovanja podatkov in konkretno informacijsko rešitev za njihovo posredovanje določilo Ministrstvo za notranje zadeve skupaj z institucionalnim uporabnikom glede na tehnične in vsebinske zmogljivosti ter potrebe institucionalnega uporabnika. Ministrstvo za notranje zadeve pa ni imelo oblikovanega standardiziranega osnutka dogovora, ki bi ga uporabljalo pri vseh odobrenih posredovanjih osebnih podatkov iz CRP institucionalnim uporabnikom ter ki bi ga za posameznega institucionalnega uporabnika prilagodilo glede na njegove posebnosti. Vodilo je razvid uporabnikov podatkov CRP za spletne servise eCRP, spletne informacijske rešitve in eRISK v varnostnih shemah. Ugotovili smo, da je MNZ podatke iz CRP nekaterim institucionalnim uporabnikom zagotavljalo brez popolne dokumentacije ali zakonske podlage. Ministrstvo za notranje zadeve je po uveljavitvi Zakona o varstvu osebnih podatkov (ZVOP-2) v letu 2023 pristopilo k uskladitvi dogovorov, ki jih je imelo sklenjene z občinami. Ministrstvo za notranje zadeve je na področju upravljanja varnostnih shem oziroma upravljanja s pravili administracije institucionalnih uporabnikov in uporabnikov fizičnih oseb zagotavljalo sistem dodeljenih dostopnih pooblastil do informacijskih rešitev CRP, ki so omejena glede na vloge. Omenjene dostope je dodelilo samo na podlagi dokumentiranih in potrjenih uporabniških zahtev. Ministrstvo za notranje zadeve je v letu 2025 pristopilo k preverjanju dostopnih pravic uporabnikov fizičnih oseb, zaposlenih pri institucionalnih uporabnikih, ni pa tega izvajalo periodično. Informacijske rešitve CRP niso imele možnosti izvoza oziroma izpisa celotnih evidenc uporabnikov brez posredovanja zunanjih izvajalcev. Ministrstvo za notranje zadeve je imelo za informacijske rešitve CRP vzpostavljen sistem za pomoč uporabnikom ter tudi sistem odpravljanja napak. Ugotovili smo, da je Ministrstvo za notranje zadeve v skladu s pogodbo SLA v sklopu nudenja gostovanja izvajalo varovanje dostopa do podatkov, izdelavo varnostnih kopij in njihovo shranjevanje ter morebitno obnavljanje podatkov ob upoštevanju dokumentiranih in usklajenih zahtev. Letno je testiralo in restavriralo podatke z varnostnih kopij, zapisalo ugotovitve testiranja in sprejelo potrebne ukrepe. Ministrstvo za notranje zadeve je imelo v informacijskih rešitvah CRP vzpostavljen sistem revizijskih sledi oziroma vzpostavljen dnevnik obdelave.

V zvezi s spremljanjem in nadziranjem CRP smo ugotovili, da je Ministrstvo za notranje zadeve področje informacijske podpore CRP redno obravnavalo na sestankih in upoštevalo sklepe iz zapisnikov teh sestankov. Zagotavljalo je tudi redno poročanje odgovornih oseb vodstvu o aktivnostih v zvezi z razvojem in izvajanjem informacijske podpore CRP. Vodstvo odgovornih organizacijskih enot je bilo namreč prisotno na rednih sestankih z zunanjim izvajalcem, kjer je izvajalo nadzor nad izpolnjevanjem načrtovanih aktivnosti, izpolnjevanjem ciljev ter sprejemom morebitnih korektivnih ukrepov ter izvajalo notranje kontrole. Ugotovili smo, da informacijske rešitve CRP do zaključka obdobja, na katero se nanaša revizija, še niso bile predmet notranje oziroma zunanje revizije. Ministrstvo za notranje zadeve je sicer izvajalo ukrepe za odpravo posameznih zaznanih pomanjkljivosti delovanja informacijskih rešitev CRP, ki so bile obravnavane na rednih mesečnih sestankih, ter spremljalo in nadzorovalo ter izvajalo aktivnosti za vse spremembe in

dopolnitve, vendar pa ni zagotovilo izvajanja neodvisnih preveritev, saj v okviru notranje ali zunanje revizije še ni zvedlo revizije informacijskih rešitev CRP.

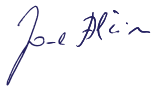
4. Priporočila

Ministrstvu za notranje zadeve in javno upravo priporočamo, naj:

- pripravi in sprejme poslovno strategijo in IT strategijo Centralnega registra prebivalstva;
- izdatke, ki se nanašajo na razvoj novih funkcionalnosti ali nadgradnjo sistema, obravnava kot investicijo v neopredmetena osnovna sredstva ter prilagodi pogodbe z zunanjimi izvajalci, tako da bodo jasno opredeljene razvojne aktivnosti, in sicer na način, da bodo ločene od storitev rednega vzdrževanja ter nadgradenj, ki ne povečujejo funkcionalnosti sistema;
- oblikuje standardiziran vzorec dogovora z institucionalnimi uporabniki podatkov Centralnega registra prebivalstva z bistvenimi elementi dogovora in nabora prilog ter zagotovi njegovo redno posodabljanje;
- oblikuje kontrolne sezname ali drugo obliko preverjanja skladnosti in popolnosti dogovora in prilog;
- v okviru notranje revizije načrtuje in izvede tudi revizije informacijskih rešitev Centralnega registra prebivalstva.

Pravni pouk

Tega poročila na podlagi tretjega odstavka 1. člena Zakona o računskem sodišču ni dopustno izpodbijati pred sodišči in drugimi državnimi organi.



Digitalno podpisal Jana Ahčin
Datum: 2026.08.28 09:16:25 +02'00'

Jana Ahčin,
generalna državna revizorka

Vročiti:

1. Ministrstvu za notranje zadeve in javno upravo,
2. Sanji Ajanović Hovnik,
3. Boštjanu Poklukarju,
4. Branku Zlobku,
5. Državnemu zboru Republike Slovenije.

Bdimo nad potmi javnega denarja

Računsko sodišče Republike Slovenije
The Court of Audit of the Republic of Slovenia
Slovenska cesta 50, 1000 Ljubljana, Slovenija
tel.: +386 (0) 1 478 58 00
sloaud@rs-rs.si
www.rs-rs.si