Ocena učinkov v zvezi z varstvom osebnih podatkov pri projektu »Skrinja 2.0 - vzpostavitev sistema poslovne analitike v državni upravi«

Ljubljana, 30. 4. 2018

SPREJEM DPIA

Razlog za sprejem DPIA

DPIA je v interesu MJU. MJU bo namreč izvajalo storitev Skrinja 2.0, ki naj bi v delu vsebovala tudi obdelavo podatkov, ki bi lahko imeli značaj osebnih podatkov. Ker so viri podatkov na začetku projekta vsaj deloma nepredvidljivi, MJU ocenjuje, da obstaja zaradi odsotnosti te informacije možnost velikega tveganja za pravice in svoboščine posameznikov.

Potrjevalci in podpisnik Ocene učinkov v zvezi z varstvom osebnih podatkov

Ocena učinkov v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: DPIA) v letu 2018, pričujoča je prvotna DPIA, pred začetkom vključevanja podatkovnih virov v storitev.

	Ime in priimek	Podpis
Osnutek pripravil	Tamara Gliha	Evidentirano kot dokument št. 382-114/2018/1 z dne 30. 4. 2018
Pregledali in dopolnili	Člani projektne skupine za vzpostavitev sistema poslovne analitike v državni upravi – Skrinja 2.0	Potrjeno v okviru projektne skupine
Podpisnik	mag. Jurij BERTOK	Elektronski podpis je izveden na dokumentu št. 382-114/2018/1 z dne 30. 4. 2018

DPIA ne bo posredovana v mnenje uporabnikom, ker gre za splošno DPIA za storitev. Pred vključitvijo posameznega vira podatkov v storitev bo izvedena posamezna DPIA.

DPIA je posredovana v mnenje Informacijskemu pooblaščencu.

VSEBINA

1 SPLOŠNO O PROJEKTU

1.1.1 Predpostavke

Temeljni cilji Strategije razvoja javne uprave 2015-2020 (SJU 2020) so usmerjeni v kakovost in učinkovitost, transparentnost in odgovornost javne uprave. V tem okviru Ministrstvo za javno upravo (v nadaljnjem besedilu: MJU) prepoznava kot eno temeljnih nalog vzpostavitev čim bolj uspešne javne uprave tako z vidika organizacije kot zaposlenih. Temeljni pogoj za njeno doseganje je zagotovitev merljivih podatkov, na podlagi katerih je mogoče stanje nadzirati in ga v primeru ustrezne analize tudi izboljševati. Ministrstvo izvaja vrsto aktivnosti, ki skupaj tvorijo celovito zgodbo za dosego strateškega cilja učinkovite in produktivne javne uprave, pričujoči projekt je le eden izmed njih. V tem okviru MJU izvaja projekt vzpostavitve poslovne analitike v državni upravi (Skrinja 2.0), katerega cilj je podpora odločanju na podlagi podatkov. Vzpostavlja se sistem, sestavljen iz skupnega podatkovnega skladišča, ki bo fizično in vsebinsko razdeljen na področna podatkovna skladišča ter pripadajoči sistem poslovne analitike (prav tako razdeljen na področne poslovne analitike) skladno s pristojnostmi posameznega organa – lastnika področnega podatkovnega skladišča. V ciljnem stanju, do leta 2022, bo MJU omenjeni sistem ponujalo kot horizontalno storitev Skrinja 2.0 tudi drugim organom državne uprave vključno z razvojem, vzdrževanjem, zagotavljanjem varnosti ter uporabo. Med predhodniki pričujočega projekta je pilotni projekt, v okviru katerega je bila izvedena »Presoja vplivov na zasebnost pri analizi velikih podatkov na infrastrukturi državnega računalniškega oblaka (DRO) – statistično znanstveno raziskovalni pilotni projekt«, in je kot takšna skupaj s pridobljenimi rezultati pomagala pri pridobivanju izkušenj ter ugotovitev, ki so bile ključne za postavitev pričujočega projekta. Tudi na podlagi ugotovitev izvedenega pilotnega projekta se je potrdilo, da je uporaba velikih podatkov lahko učinkovito orodje za upravljanje sistema državne uprave. Predstavlja namreč podlago za učinkovito in realno načrtovanje politik.

Za ustrezno izvedbo projekta sta varstvo in zaščita (osebnih) podatkov izjemno pomemben vidik, ki ga MJU upošteva pri oblikovanju sistema skladno z zahtevami veljavne zakonodaje s posebnim poudarkom na ureditvi varstva posameznikov pri obdelavi osebnih podatkov, ki ga zahteva Zakon o varstvu osebnih podatkov (ZVOP-1) in Splošna uredba o varstvu podatkov (GDPR). V ta namen bo MJU vzpostavil ustrezna pravila in dogovore o razmejitvi odgovornosti skladno z veljavno zakonodajo. Minimalni zahtevi za obdelovanje osebnih podatkov v okviru storitve Skrinja 2.0 bosta zagotovitev ocene učinkov v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: DPIA) za posamezno področno podatkovno skladišče in maskiranje – psevdonimizacija osebnih podatkov pred njihovim prenosom v sistem podatkovnega skladiščenja. Sistem bo vseboval tudi takšne komponente in gradnike (registri, evidence, šifranti), ki so uporabljeni pri drugih podatkovnih virih v že obstoječih informacijskih sistemih državne uprave in jih bodo različni lastniki področnih podatkovnih skladišč uporabljali kot enotne skupne dimenzije. Za skupne dimenzije bo skrbel MJU kot ponudnik horizontalne storitve Skrinja 2.0. Predviden način delovanja ter varnostnega arhiviranja sistema podatkovnega skladišča in poslovne analitike na infrastrukturi naročnika bo temeljil na obstoječem sistemu varnostnega arhiviranja pri naročniku s smiselno uporabo trenutno veljavnih Generičnih tehnoloških zahtev (v nadaljevanju GTZ) za razvoj informacijskih sistemov na MJU.

1.1.2 Izhodišče projekta

Infrastruktura državnega računalniškega oblaka (DRO), ki je v upravljanju MJU, predstavlja eno od predhodnih pogojenosti za vzpostavitev platforme podatkovnega skladišča, poslovne analitike in analitike masovnih podatkov, obenem pa na področju podatkovne analitike v slovenski javni upravi še niso dovolj izkoriščeni potenciali, ki jih ponuja digitalni način poslovanja za povečevanje uspešnosti poslovanja in podporo uporabnikom. Zato se je vodstvo MJU odločilo za projekt Skrinja 2.0, s katerim želi pospešiti razvoj podatkovne analitike kot novega načina delovanja in odločanja na podlagi podatkov za vse ravni odločevalcev v državni upravi.

1.1.3 Namen in cilji projekta

V državni upravi bo, skladno s sodobnimi smernicami poslovanja, uvedena poslovna analitika kot nov način delovanja in odločanja na podlagi podatkov za vse ravni odločevalcev. Na podlagi rezultatov pilotnega projekta za vzpostavitev skladišča podatkov in sistema poslovne analitike »Skrinja 2.0« bo do leta 2022 vzpostavljeno nudenje storitev na področju podatkovnega skladiščenja in poslovne analitike, ki bodo v ciljnem stanju horizontalno ponujene tudi drugim organom državne uprave predvsem za skupne aplikacije. Aplikacija bo v celoti delovala na naročnikovem privatnem oblaku (DRO) – on premise. Z vzpostavitvijo skladišča podatkov in sistema poslovne analitike v državni upravi se na vseh ravneh prvenstveno želi izboljšati in optimalneje organizirati sistem upravljanja s podatki, sistem poročanja in proces odločanja.

1. Ključne neposredne možne izboljšave z vidika zagotavljanja kakovostnih informacij bodo:
   - analitični sistem bo omogočal prilagodljiv dostop do relevantnih podatkov;
   - povečala se bo učinkovitost priprave podatkov, poročil in analiziranja podatkov, posledično pa se bo zmanjšala infrastrukturna (podatkovna in analitična) zakasnitev oz. bodo podatki dostopni za analiziranje v krajšem času;
   - analitični sistem bo ob enakih pogojih omogočal ponovljivost pripravljenih izračunov;
   - povečala se bo kakovost prikaza (vizualizacije) in s tem razumljivost informacij za sprejemanje boljših odločitev.
2. Cilj je postaviti model analitičnega sistema, katerega storitve bodo v ciljnem stanju horizontalno ponujene tudi drugim organom državne uprave predvsem za skupne aplikacije.

1.1.4 Vsebina projekta

MJU v okviru projekta Skrinja 2.0 zagotavlja storitev Skrinja 2.0 kot storitev ponudbe sistema poslovne inteligence, in sicer horizontalne storitve, ki zajema različne ravni storitev na različnih elementih sistema, njegovega razvoja, vzdrževanja in uporabe, in to tako sistem podatkovnega skladišča kot tudi podatkovne analitike.

Storitev Skrinja 2.0, ki jo zagotavlja MJU v okviru projekta Skrinja 2.0, je podrobno opisana v Elaboratu: Koncept sistema poslovne inteligence ter poslovnih in uporabniških zahtev na MJU za podatkovna vira ISPAP in MFERAC IT, z dne 27. november 2017, in sicer v poglavju 6.2 BI kot storitev, ki je kot priloga 5 sestavni del te DPIA.

V navedenem elaboratu so podrobneje opisane tudi različne vloge, v katerih nastopa MJU pri zagotavljanju projekta Skrinja 2.0, pričujoča DPIA pa obravnava MJU izključno v vlogi ponudnika storitve Skrinja 2.0. Ko bo MJU nastopalo kot lastnik podatkovnega skladišča, bo izpolnilo vse zahteve, ki jih ta DPIA določa za zagotavljanje storitve Skrinja 2.0.

2 OSEBNA IZKAZNICA

2.1 NABOR OSEBNIH PODATKOV

Nabor osebnih podatkov (v nadaljnjem besedilu: OP) je odvisen od vsakokratnega podatkovnega vira, za katerega se bodo lastniki področnega podatkovnega skladišča odločili, da ga bodo vključili v sistem poslovne inteligence, ki jo MJU ponuja kot svojo storitev Skrinja 2.0.

MJU ugotavlja, da se bodo z vidika obdelave osebnih podatkov posamezni podatkovni viri delili na tiste, ki:

A) ne vsebujejo OP in

B) vsebujejo OP.

MJU ne razpolaga z ustreznimi znanji področne zakonodaje, zato samo ne bo ugotavljalo, kateri od virov vsebuje OP, posledično bo to ugotovitev prepustilo lastniku področnega podatkovnega skladišča, ki bo odločal o vključitvi posameznega podatkovnega vira v storitev. Če se izkaže, da podatkovni vir vsebuje osebne podatke, je lastnik podatkovnega skladišča njihov upravljavec, ponudnik storitve Skrinja 2.0 pa obdelovalec.

A)

Če posamezni podatkovni vir ne vsebuje OP, MJU kot ponudnik storitve Skrinja 2.0 zaradi narave storitve zahteva od lastnika področnega podatkovnega skladišča izpolnitev izjave, ki je Priloga 1 te ocene učinkov.

B)

Če podatkovni vir vsebuje OP, morajo lastniki področnih podatkovnih skladišč pred vključitvijo v storitev Skrinja 2.0 vsaj:

a) zagotoviti oceno učinkov v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: DPIA) za vključitev svojega podatkovnega vira v storitev Skrinja 2.0,

b) zagotoviti morebitno potrditev DPIA s strani odgovorne osebe za varstvo osebnih podatkov ali Informacijskega pooblaščenca, če to zahteva relevantna zakonodaja,

c) zagotoviti vse ukrepe, ki so v posameznem DPIA prepoznani kot smiselni za zagotovitev varstva OP, pri čemer mora biti minimalni ukrep za zagotavljanje ustreznega varstva OP v okviru področnega podatkovnega skladišča psevdonimizacija OP na način, da iz posameznega podatka identifikacija posameznika, na katerega se nanaša podatek, ni mogoča, in sicer tako, da se pred prenosom podatkov v okolje podatkovnega skladišča prenesejo že psevdonimizirani podatki. Za psevdonimizacijo poskrbi lastnik področnega podatkovnega skladišča.

Formati vseh podatkov bodo vsebovani v DPIA posameznega področnega podatkovnega skladišča.

Pred začetkom zagotavljanja storitve Skrinja 2.0, ponudnik zahteva izpolnitev osnovnih zahtev postopka, navedenega v Prilogi 2, ki je sestavni del te DPIA.

2.2 RAVNANJA Z OP

Lastnik področnega podatkovnega skladišča:

V okviru storitve Skrinja 2.0 se bodo obdelovali podatki na podlagi zahteve posameznega lastnika področnega podatkovnega skladišča, ki bo zagotovil, da bo vsak podatkovni vir pred prenosom v okolje podatkovnega skladišča pripravljen na način, da iz posameznega podatka ni mogoča identifikacija posameznika, na katerega se nanaša podatek.

Če posamezen podatkovni vir vsebuje psevdonimizirane podatke, mora lastnik področnega podatkovnega skladišča z MJU skleniti pogodbo o obdelavi psevdonimiziranih OP v delu zagotavljanja storitve Skrinja 2.0.

Hramba:

Podatki se bodo v skladu z varnostnimi standardi MJU hranili v področnih podatkovnih skladiščih, ki se bodo med seboj tehnično in logično ločena na način, da bo zagotovljena varnost in zaupnost podatkov.

Posredovanje:

Podatki se bodo posredovali ali bili dostopni izključno lastniku področnega podatkovnega skladišča - ali z njihove strani določenim subjektom ali informacijskim sistemom. Lastniki podatkov bodo opredeljeni v dogovoru o obdelavi psevdonimiziranih podatkov.

Varnost:

MJU bo v okviru zagotavljanja storitve Skrinja 2.0 namenil posebno pozornost pred naključnimi in namernimi zlorabami, izgubo in uničenjem podatkov posameznega podatkovnega vira, in sicer na ravni celotne storitve.

Rok hrambe:

MJU bo v okviru storitve Skrinja 2.0 nudil na razpolago storitev za podatkovne vire, za katere bo posamezni lastnik področnega podatkovnega skladišča določil, da se vključijo v storitev, MJU teh podatkov ne bo kopiral ali kako drugače hranil izven zagotavljanja primarne storitve obdelave podatkov za namene poslovne analitike posameznega lastnika področnega podatkovnega skladišča. Tako bo lastnik področnega podatkovnega skladišča tisti, ki bo samostojno določal čas, ko bodo posamezni podatki, vključeni v zagotavljanje storitve in posledično obdelavo podatkov.

Uničenje podatkov:

V okviru uporabe storitve Skrinja 2.0 je posamezen lastnik področnega podatkovnega skladišča tisti, ki določi, koliko časa se posamezen podatek nahaja na infrastrukturi MJU, po preteku tega časa pa se podatki sistemsko izbrišejo.

MJU v okviru storitve Skrinja 2.0 tudi zagotavlja, da se bodo nosilci podatkov po prenehanju njihove uporabe uničili v skladu s predpisi MJU o uničevanju nosilcev zapisov.

Pomembno:

Vsa določila tega dokumenta, ki se nanašajo na vzpostavljanje storitve Skrinja 2.0, se uporabljajo smiselno enako tudi ob vsaki spremembi nabora podatkov ali njihovih atributov. Lastnik področnega podatkovnega skladišča je dolžan sproti preverjati skladnost s pravili uporabe storitve Skrinja 2.0.

2.3 PODROČNA ZAKONODAJA

MJU bo kot ponudnik storitve Skrinja 2.0 zahteval popolno izpolnjevanje zahtev zakonodaje, ki ureja obdelavo OP in v ta namen zagotavlja pričujočo oceno učinkov, ki predvideva aktivnosti, ki jih mora zagotoviti posamezen lastnik področnega podatkovnega skladišča pred prenosom njegovih podatkovnih virov v sistemska okolja Skrinja 2.0.

V tem okviru je posamezen lastnik področnega podatkovnega skladišča odgovoren za zakonito obdelavo podatkov v okviru namena njihovega zbiranja, če so ti podatki OP, pripravo nabora podatkov, ki se bodo obdelovali, in določitev ostalih pogojev obdelave podatkov v okviru storitve MJU.

3 KONKRETNI UKREPI OCENE UČINKOV

3.1 SORAZMERNOST

Sorazmernost obdelave OP se bo v okviru projekta Skrinja 2.0 zagotavljala na način, da bo MJU kot ponudnik storitve Skrinja 2.0 vztrajal na:

- vključevanju podatkovnih virov, ki bodo vsebovali le psevdonimizirane podatke, pri čemer MJU kot ponudnik storitve Skrinja 2.0 ne bo imel dostopa do izvornih podatkov, ki so bili psevdonimizirani;
- tehnični ločitvi posameznih podatkovnih virov, razen če kasneje lastnik področnega podatkovnega skladišča ne bo izkazal ustrezne zakonske podlage za njihovo povezovanje, pri čemer iz pridobljenih povezav ne bo mogoča identifikacija posameznika, na katerega se kateri od podatkov nanaša.

3.2 PRAVNA PODLAGA

Pravno podlago za obdelavo OP v okviru posameznega področnega podatkovnega skladišča bo moral zagotavljati vsak posamezni lastnik področnega podatkovnega skladišča in jo izkazati v DPIA za posamezen podatkovni vir.

3.3 POGODBENA OBDELAVA

MJU bo za izvedbo storitve Skrinja 2.0 sodelovalo z več pogodbenimi izvajalci, ki se bodo v času zagotavljanja storitve lahko spreminjali.

Vsi pogodbeni izvajalci bodo skladno s pogodbenimi določili podatke obdelovali le v imenu in za račun MJU kot ponudnika storitve Skrinja 2.0 ter zgolj v mejah pooblastil MJU, predvsem pa osebnih podatkov ne bodo smeli obdelovati za noben drug namen, predvsem jih ne bodo smeli združevati ali niti poskusiti depsevdonimizirati.

MJU pred podelitvijo pravic za dostop do sistema, ki ga upravlja zunanji izvajalec in vsebuje OP, zagotovi izpolnjevanje pogojev iz Priloge 3 »Vključitev zunanjih izvajalcev, obdelovalcev OP, v zagotavljanje storitve Skrinja 2.0«.

Zunanjim izvajalcem se bo omogočil dostop z lokacije izvajalca le do razvojnega okolja Skrinja 2.0 na DRO. Dostop do testnega in produkcijskega okolja bodo imeli izvajalci le na lokaciji naročnika pod njegovim nadzorom.

3.4 TOČNOST IN AŽURNOST

Točnost in ažurnost podatkov v okviru storitve Skrinja 2.0 bo lahko le tolikšna, kakršna bo točnost in ažurnost izvornih podatkov.

Če se bodo v okviru obdelave podatkov pokazala odstopanja med izvornimi podatki in podatki v okolju Skrinja 2.0, se šteje, da so točni podatki tisti, ki so izvorni podatki.

MJU bo v okviru zagotavljanja storitve Skrinja 2.0 zagotovilo protokole za pregledovanje ustreznosti podatkov, če se bo izkazalo, da preneseni podatki niso točni. Pri tem se pričakuje aktivno sodelovanje lastnikov področnih podatkovnih skladišč in lastnikov podatkovnih virov.

3.5 PREGLEDNOST IN INFORMIRANJE POSAMEZNIKA

Ponudnik storitve Skrinja 2.0 ne bo razpolagal s podatki o tem, kateri podatki se nanašajo na katerega posameznika, zato bo moral informiranje posameznikov, na katere se bodo osebni podatki nanašali, zagotavljati posamezen lastnik področnega podatkovnega skladišča, na katerega ga bo MJU naslovil.

Ponudnik storitve Skrinja 2.0 bo ob prejemu morebitne zahteve posameznika ugotovil njegovo upravičenje do dostopa do splošnih podatkov o zagotavljanju storitve.

3.6 OSTALE PRAVICE POSAMEZNIKA

Ponudnik storitve Skrinja 2.0 ne bo razpolagal s podatki o tem, kateri podatki se nanašajo na katerega posameznika, zato bo moral pravice posameznika do seznanitve in prenosljivost podatkov, do popravka in izbrisa podatkov ter do ugovora in omejitve obdelave, zagotavljati posamezen lastnik področnega podatkovnega skladišča.

3.7 UPORABA ISTEGA POVEZOVALNEGA ZNAKA

V okviru zagotavljanja storitve Skrinja 2.0 bo mogoča uporaba istega povezovalnega znaka izključno za podatke, ki niso osebni podatki, kar bo zagotavljalo MJU s šifranti skupnih dimenzij (država, organ, lokacijski podatki,…).

Isti povezovalni znak za osebne podatke, ki bodo psevdonimizirani, se bo lahko uporabljal izključno v okviru posameznega področnega podatkovnega skladišča, če bo lastnik področnega podatkovnega skladišča predhodno zagotovil, da bo povezovalni znak kot takšen psevdonimiziran, torej bo šlo za negovoreči znak, ki ni vsebovan v nobenem od uradnih registrov. S šifrantom morebiti uporabljenih povezovalnih znakov bo razpolagal izključno lastnik področnega podatkovnega skladišča, oziroma v dogovoru z njim lastnik posameznega podatkovnega vira, pri čemer se posebej poudari, da MJU kot ponudnik storitve Skrinja 2.0 s takšnim ključem ne bo razpolagal.

Pogoji za povezovanje zbirk so natančneje opredeljeni v poglavju 4 Povezovanje zbirk osebnih podatkov.

3.8 ROK HRAMBE

Rok hrambe posameznega podatkovnega vira določi lastnik področnega podatkovnega skladišča, oziroma v dogovoru z njim lastnik posameznega podatkovnega vira, MJU pa kot ponudnik storitve Skrinja 2.0 teh podatkov ne bo kopiral ali kako drugače hranil izven zagotavljanja primarne storitve obdelave podatkov za namene poslovne analitike posameznega lastnika področnega podatkovnega skladišča (kar vključuje na primer varnostne kopije, revizijske sledi,…). Tako bo lastnik področnega podatkovnega skladišča, oziroma v dogovoru z njim lastnik posameznega podatkovnega vira, tisti, ki bo samostojno določal čas, ko bodo posamezni podatkovni viri ali v njihovem okviru posamezni podatki, vključeni v zagotavljanje storitve in posledično obdelavo podatkov.

Za brisanje podatkov po preteku roka hrambe je odgovoren lastnik področnega podatkovnega skladišča.

3.9 POSREDOVANJE

Lastnik področnega podatkovnega skladišča določi uporabnike podatkov, ki se jim omogoči neposreden dostop do podatkov, ki se nahajajo v sistemu, in morebitno posredovanje podatkov.

3.10 ZAVAROVANJE

Zavarovanje celotnega sistema bo izvedeno v skladu s pravili poslovanja MJU ter dokumentacijo, ki bo pripravljena za izvedbo projekta in vključuje vse aktivnosti, ki so naštete tako v tem, kot spremljajočih dokumentih.

3.11 INTERNI AKTI

Pri zagotavljanju storitve Skrinja 2.0 se uporabljajo dokumenti:

- Elaborat: Koncept sistema poslovne inteligence ter poslovnih in uporabniških zahtev na mju za podatkovna vira ISPAP in MFERAC IT, Center poslovne odličnosti Ekonomske fakultete Univerze v Ljubljani, Avtorji: dr. Jurij Jaklič, dr. Jure Erjavec, dr. Luka Tomat, Ljubljana, 27. 11. 2017,
- Predlog tehnične rešitve za izvedbo računalniških storitev izdelave predloga rešitve za tehnično postavitev podatkovnega skladišča, interno gradivo, december 2017, Avtorji: Žiga Vaupot, Mojca Gros, Matjaž Zupan 22. 12. 2017,
- Generične tehnološke zahteve GTZ_2.2.7, dokument je objavljen na portalu NIO, dostopen na spletnem naslovu: https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743, marec 2018, Ministrstvo za javno upravo, Direktorat za informatiko.
- Generične tehnološke zahteve GTZ-LOP_1.1.1, dokument je objavljen na portalu NIO, dostopen na istem spletnem naslovu: https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743, maj 2017, Ministrstvo za javno upravo, Direktorat za informatiko

Pri izvajanju storitve Skrinja 2.0 se bo upošteval splošni dokument MJU:

- Akt o postopkih in ukrepih za zavarovanje osebnih podatkov v Ministrstvu za javno upravo št. 020-83/2016/1 z dne 22. 7. 2016.

Pri izvajanju storitve Skrinja 2.0 se bodo upoštevali tudi interni dokumenti, ki opredeljujejo delo MJU kot ponudnika informacijske infrastrukture in se nahajajo na intranetnih straneh MJU kot interni dokumenti.

3.12 DOLOČITEV ODGOVORNIH OSEB

Odgovorna oseba za zagotavljanje izvajanja storitve Skrinja 2.0 je generalni direktor Direktorata za informatiko, Ministrstva za javno upravo.

Odgovorne osebe v zvezi z vsebino vsakokratnega področnega podatkovnega skladišča so lastniki področnih podatkovnih skladišč, ki bodo določeni v sporazumu o zagotavljanju in uporabi storitve Skrinja 2.0.

3.13 NOTRANJA SLEDLJIVOST OBDELAVE

Notranjo sledljivost obdelave se zagotavlja z upoštevanjem varnostne sheme, z dnevniškimi zapisi in revizijskimi sledmi.

3.14 SLEDLJIVOST POSREDOVANJA (ZUNANJA SLEDLJIVOST)

V okviru storitve Skrinja 2.0 MJU ne bo posredoval osebnih podatkov izven sistema.

V okviru storitve Skrinja 2.0 bo MJU posredoval izključno agregirane podatke in takšne, ki jih bo lastnik področnega podatkovnega skladišča opredelil kot javno dostopne.

3.15 SISTEMI ZA UPRAVLJANJE VAROVANJA INFORMACIJ (SUVI)

Storitev Skrinja 2.0 se bo zagotavljala na DRO infrastrukturi, ki ima vzpostavljen sistem upravljanja varovanja informacij skladno z internimi akti. Obenem je MJU aktivno pristopil k pridobivanju pridobivanja certifikata ISO27001 za DRO.

Za izvajanje same storitve Skrinja 2.0 se pravila postavljajo z navedenimi v tem dokumentu, s pravili, po katerih posluje Direktorat za informatiko, Ministrstva za javno upravo, ter s pravili, ki bodo nastajala pri vzpostavljanju in kasneje, zagotavljanju storitve Skrinja 2.0.

3.16 POSTAVITEV ODGOVORNIH OSEB ZA VARSTVO OSEBNIH PODATKOV

Katarina Janjič, odgovorna oseba za varstvo osebnih podatkov na Ministrstvu za javno upravo.

3.17 EVIDENCA DEJAVNOSTI OBDELAVE OSEBNIH PODATKOV

Ponudnik storitve Skrinja 2.0 bo obdelovalec OP, ne glede na to, da bodo podatki, ki se bodo nahajali v področnem podatkovnem skladišču, psevdonimizirani, zaradi česar bo moral skrbeti za evidenco dejavnosti obdelave OP. Vnos novega vira OP v evidenco ponudnik storitve Skrinja 2.0 zagotovi po sklenitvi sporazuma o zagotavljanju in uporabi storitve.

Vsak lastnik področnega podatkovnega skladišča bo kot upravljavec skrbel za svojo evidenco dejavnosti obdelave osebnih podatkov in bo v okviru sporazuma o zagotavljanju in uporabi storitve Skrinja 2.0 seznanil MJU kot ponudnika storitve s podatki, ki jih bo psevdonimizirane obdeloval z zagotavljanjem storitve Skrinja 2.0 – seznam se bo moral ujemati z dogovorom o pogodbeni obdelavi osebnih podatkov.

4 POVEZOVANJE ZBIRK OSEBNIH PODATKOV

Temeljni namen storitve Skrinja 2.0 je vzpostavitev enotnega sistema področnih podatkovnih skladišč in poslovne analitike za podporo odločanju na podlagi podatkov in ne povezovanje zbirk osebnih podatkov.

Povezovanje zbirk osebnih podatkov je eno najbolj občutljivih vprašanj varstva osebnih podatkov, zato mu bo ob morebitni izkazani potrebi MJU namenjalo posebno pozornost.

Povezovanje zbirk bo MJU izvedlo izključno v primeru:

- pisne zahteve lastnikov podatkovnih vir vseh povezanih zbirk, če so lastniki različni, z izrecno navedbo zakonske podlage, ki povezavo predvideva;
- po predhodni predložitvi ocene učinkov, za katero bo MJU, ob morebitni odsotnosti drugačnih zakonskih zahtev, lahko zahteval mnenje Informacijskega pooblaščenca.

5 INTERNI NADZOR

Interni nadzor se zagotavlja tako, da odgovorna oseba po predhodni odobritvi odgovorne osebe za varstvo osebnih podatkov enkrat letno pregleda poročilo o:

- ažurnosti seznama lastnikov področnih podatkovnih skladišč, kot uporabnikov storitve Skrinja 2.0
- ažurnosti seznama odgovornih oseb,

- seznamu morebitnih incidentov
- seznamu tveganj in ukrepov ter preveri njihovo izvajanje in ustreznost.

Poročilo pripravi vodja projekta Skrinja 2.0.

6 IZOBRAŽEVANJE

Vsi zaposleni na projektu vzpostavitve storitve Skrinja 2.0 so pri pripravi dokumentacije seznanjeni z zakonskimi zahtevami za varovanje OP ter z internim aktom o postopkih in ukrepih za zavarovanje osebnih podatkov v MJU.

Dolgoročno bo MJU vzpostavilo kompetenčni center, v okviru katerega bo MJU kot ponudnik storitve Skrinja 2.0 zagotavljalo ustrezno izobraževanje upravljavcev osebnih podatkov za namene uporabe storitve Skrinja 2.0.

7 IZNOS OSEBNIH PODATKOV V TRETJE DRŽAVE

Iznosa podatkov v tretje države ne bo, ker bo storitev Skrinja 2.0 nameščena na državnem privatnem oblaku DRO.

8 TVEGANJA IN UKREPI ZA OBVLADOVANJE TVEGANJ V POVEZAVI Z VARNOSTJO PODATKOV

MJU v okviru te ocene tveganja ne bo ocenjeval splošnih tveganj, ki se nanašajo na uspešnost zagotavljanja vseh storitev MJU (na primer: poplava, ki lahko uniči sistemsko sobo,…), temveč se bo omejil na tveganja v zvezi z varstvom osebnih podatkov in zasebnosti. Splošna tveganja obravnava MJU v okviru zagotavljanja infrastrukture DRO.

Ravni tveganja se ocenjujejo na lestvici: majhna, srednja, visoka.

MJU v zvezi s tveganji in ukrepi, ki se nanašajo na varstvo osebnih podatkov in zasebnosti ugotavlja:

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
1.	Zakonitost	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar lastnik področnega podatkovnega skladišča kot uporabnik storitve ne razpolaga z ustrezno pravno podlago za obdelavo osebnih podatkov	Majhna, saj bodo v storitev Skrinja 2.0 kot lastniki področnih podatkovnih skladišč vključeni izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP	Velika, pomanjkanje pravne podlage za obdelavo OP je največja kršitev varstva OP	Visoka, zaradi velike resnosti	MJU pred vzpostavitvijo novega področnega podatkovnega skladišča od lastnika področnega podatkovnega skladišča zahteva: - izjavo iz Priloge 1, iz katere izhaja, da podatkovni vir ne vsebuje OP, ali - lastnik področnega podatkovnega skladišča v okviru DPIA, kot dokumenta, ki se zahteva v skladu s Prilogo 2, navede pravno podlago za obdelavo OP.
2.	Zakonitost	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar lastnik področnega podatkovnega skladišča oceni, da bo v storitev vključil vir, ki sam po sebi ne vsebuje OP, zaradi česar ne bo obdeloval OP, ti podatki pa so takšni, da je mogoče določiti identiteto	Srednja, čeprav bodo v storitev Skrinja 2.0 kot lastniki področnih podatkovnih skladišč vključeni izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z	Velika, če organ ne bo ocenil, da obdeluje OP, in posledično ne bo izvajal ukrepov za zavarovanje podatkov, lahko pride do hude kršitve veljavnih	Visoka, zaradi velike resnosti ! Gre za eno največjih tveganj projekta, saj se ob napačni oceni vrste	MJU pred vključitvijo vsakega novega lastnika področnega podatkovnega skladišča v storitev Skrinja 2.0 zahteva izjavo iz Priloge 1, iz katere izhaja: - da podatkovni vir ne vsebuje OP, in - da bo ponudnik storitve prekinil z izvajanjem storitve do izpolnitve vseh pogojev za obdelavo OP v okviru storitve Skrinja 2.0 s strani lastnika

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
		posameznika, če se v obdelavo vključi druge, drugače dostopne vire podatkov	varstvom OP, je mogoče, da ne bi imeli dovolj znanja o drugače dostopnih podatkih, ki bi lahko pomenili obdelavo OP v kombinaciji s posameznim podatkovnim virom	predpisov	podatkov lahko celotnega vira podatkov ne bi obravnavalo z vidika zakonodaje, ki ureja obdelavo OP	področnega podatkovnega skladišča. MJU vzpostavi sistem pravil in aktivnosti za gostovanje in poslovanje v podatkovnem skladišču, ki bodo namenjeni izvedbi postopka prekinitve izvajanja storitve v primeru ugotovitve situacije iz opisanega tveganja. MJU vsebini nameni posebno pozornost pri zagotavljanju izobraževanj v okviru kompetenčnega centra, ko ga vzpostavi. Glede na to, da gre za eno največjih tveganj pri projektu, se ukrepom za obvladovanje tveganja ob vsakoletnem pregledu nameni posebna pozornost in poizkusi najti dodatne ukrepe za obvladovanje tveganja.
3.	Zakonitost	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar se v storitev vključita lastnika področnega podatkovnega skladišča, ki uporabita za svoje potrebe isti povezovalni znak	Majhna, saj bodo lastniki področnega podatkovnega skladišča izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP	Velika, saj bi isti povezovalni znak lahko pomenil identifikacijo posameznika	Visoka, zaradi velike resnosti	Uporaba istega povezovalnega znaka pri OP različnih lastnikov področnega podatkovnega skladišča storitve se ne dovoli, vprašanje se obravnava v okviru podpoglavja »Uporaba istega povezovalnega znaka«.
4.	Zakonitost / izobraževanje	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar lastnik področnega podatkovnega skladišča ne razpolaga z ustreznim znanjem	Majhna, saj bodo lastniki področnega podatkovnega skladišča izključno organi državne uprave, torej kot takšni	Majhna, saj lastniki področnega podatkovnega skladišča, ki ne	Majhna	MJU se bo proti neznanju borilo s pravili, ki jih bo moral lastnik področnega podatkovnega skladišča upoštevati.

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
		za pripravo vseh potrebnih dokumentov za zakonito uporabo storitve Skrinja 2.0	zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP	bodo imeli ustreznega znanja, ne bodo mogli uporabljati storitve Skrinja 2.0 zaradi obveznosti, ki so potrebne za zagotovitev pogojev za njeno uporabo		Dolgoročno želi MJU zagotoviti storitev Skrinja 2.0 čim širšemu krogu organov državne uprave, zato bo dolgoročno gledano vzpostavil kompetenčni center. Vprašanje se obravnava v okviru podpoglavja »Izobraževanje«.
5.	Zakonitost / pogodbena obdelava	MJU z zunanjimi izvajalci ne bo sklenil potrebnih dogovorov	Majhna, saj bo MJU še posebej ob vključevanju novih deležnikov v proces zagotavljanja storitve Skrinja 2.0 skrbel za izpolnjevanje zakonskih zahtev varstva OP	Srednja, pomanjkanje pravne podlage za obdelavo OP je največja kršitev varstva OP, vendar v primeru obdelovanja podatkov sekundarna – pravna podlaga za obdelavo bo že obstajala, manjkal bo vezni člen z morebitnim zunanjim izvajalcem	Srednja	MJU pri izpolnjevanju obveznosti zunanjega izvajalca zagotovi vse ukrepe, opisane v podpoglavju »Pogodbena obdelava«.
6.	Zakonitost / Evidenca dejavnosti obdelave OP – ponudnik storitve Skrinja	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar se ponudnik storitve Skrinja 2.0 MJU zaveda, da kot ponudnik storitve z informacijsko sistemskega	Majhna, saj bo MJU še posebej ob vključevanju novih deležnikov v proces zagotavljanja storitve Skrinja 2.0 skrbel za izpolnjevanje	Majhna, ponudnik storitve Skrinja 2.0 bo moral za namene zagotavljanja storitve	Majhna	Ponudnik storitve Skrinja 2.0 pred začetkom izvajanja storitev preveri, če razpolaga z vso potrebno dokumentacijo v skladu s podpoglavjem »Evidenca dejavnosti obdelave osebnih podatkov«.

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
	2.0	vidika obdeluje OP, čeprav psevdonimizirane, zaradi česar bi moral razpolagati z evidenco dejavnosti obdelave OP, vendar je ta v določenem delu nepravilna ali pomanjkljiva	zakonskih zahtev varstva OP	zagotavljati dokumentacijo v skladu z veljavno zakonodajo, zato bo razpolagal s podatki, ki bi jih morala vsebovati evidenca obdelave tudi, če s samo evidenco ne bi razpolagal.		
7.	Zakonitost / Evidenca dejavnosti obdelave OP – lastnik področnega podatkovnega skladišča	Lastnik področnega podatkovnega skladišča bo v podatkovno skladišče prenesel psevdonimizirane podatke, vendar ne bo razpolagal z Evidenco dejavnosti obdelave OP.	Majhna, saj bodo lastniki področnega podatkovnega skladišča izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP.	Majhna, lastnik področnega podatkovnega skladišča bo moral za namene uporabe storitve zagotavljati dokumentacijo v skladu z veljavno zakonodajo, zato bo razpolagal s podatki, ki bi jih morala vsebovati evidenca obdelave tudi, če s samo evidenco ne bi razpolagal.	Majhna	Ponudnik storitve Skrinja 2.0 pred začetkom izvajanja storitev preveri, če razpolaga z vso potrebno dokumentacijo v skladu s podpoglavjem »Evidenca dejavnosti obdelave osebnih podatkov«.
8.	Poštenost in preglednost – ponudnik storitve Skrinja 2.0	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar bodo imeli posamezniki, na katere se bodo podatki nanašali, tudi vprašanja, ki se tičejo splošnega zagotavljanja	Majhna, saj storitev Skrinja 2.0 kot takšna ni namenjena obdelavi OP, zaradi česar se bo malo uporabnikov obračalo na ponudnika storitve	Majhna, ponudnik storitve Skrinja 2.0 ne bo vsebinsko obdeloval OP, temveč	Majhna	MJU bo morebitnim zainteresiranim posameznikom zagotovil informacije v skladu s podpoglavjem »Preglednost in informiranje posameznika«.

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
		storitve in ne le posameznega vira podatkov	Skrinja 2.0	zagotavljal storitev, za katero bo imel prej postavljena pravila		
9.	Poštenost in preglednost – lastnik področnega podatkovnega skladišča	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar lastnik področnega podatkovnega skladišča posameznikov, na katere se nanašajo podatki, ne obvesti ustrezno o obdelavi podatkov, če je to potrebno	Majhna, saj bodo lastniki področnih podatkovnih skladišč izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP	Srednja, obveščanje posameznika o obdelavi OP, ki se nanj nanašajo, bi morali lastniki področnega podatkovnega skladišča zagotavljati že v okviru pridobivanja OP	Srednja	MJU od vsakega lastnika področnega podatkovnega skladišča, ki bo obdeloval OP, zahteva izvedbo DPIA ter lastnik področnega podatkovnega skladišča opozori na obveznost izpolnjevanja Kriterijev za oceno ustreznosti ocene učinkov, ki so kot priloga 4 sestavni del te DPIA, konkretno ukrepov, ki zagotavljajo informiranje posameznika o obdelavi podatkov.
10.	Omejitev namena	Namen storitve Skrinja 2.0 je sicer nuditi storitev na področju podatkovnega skladiščenja in poslovne analitike, vendar lastniki področnih podatkovnih skladišč storitev uporabijo za neupravičeno povezovanje zbirk in s tem presežejo namen projekta	Majhna, saj bodo lastniki področnih podatkovnih skladišč izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP	Velika, neupravičeno povezovanje zbirk lahko pomeni veliko kršitev varstva OP	Visoka, zaradi velike resnosti	MJU omeji povezovanje zbirk na izpolnjevanje pogojev, zapisanih v podpoglavju »Povezovanje zbirk OP« te DPIA. MJU zagotovi tehnične načine za izvedbo ukrepa prekinitve izvajanja dogovora o uporabi storitve iz Priloge 1.
11.	Najmanjši obseg podatkov – ponudnik storitve Skrinja 2.0	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar ponudnik storitve v podatkovno skladišče odloži več OP, kot bi jih bilo potrebno za izvrševanje namena obdelave OP	Srednja, čeprav bodo lastniki področnih podatkovnih skladišč izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP, je	Velika, najmanjši obseg OP je eno od temeljnih načel varstva OP	Visoka, zaradi velike resnosti	Ponudnik storitve Skrinja 2.0 zahteva od lastnika področnega podatkovnega skladišča, da v podatkovno skladišče posreduje izključno psevdonimizirane podatke, zaradi česar ponudnik ne more nesorazmerno obdelovati OP. Za pridobitev izvornega OP mora lastnik področnega podatkovnega skladišča

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
			mogoče, da bi želeli zagotoviti čim večjo količino pridobljenih podatkov			dostopati do podatkov v zbirki podatkov, ki se nahaja v njegovem sistemu, do katerega ponudnik storitve nima dostopa. Vprašanje se obravnava v okviru podpoglavja »Sorazmernost«.
12.	Najmanjši obseg podatkov – lastnik področnega podatkovnega skladišča	Lastnik področnega podatkovnega skladišča v podatkovno skladišče odloži več OP, kot bi jih bilo potrebno za izvrševanje namena obdelave OP.	Srednja, čeprav bodo lastniki področnih podatkovnih skladišč izključno organi državne uprave, torej kot takšni zavedni izvrševalci veljavne zakonodaje v zvezi z varstvom OP, je mogoče, da bi želeli zagotoviti čim večjo količino pridobljenih podatkov	Velika, najmanjši obseg OP je eno od temeljnih načel varstva OP	Visoka, zaradi velike resnosti	Lastnik področnega podatkovnega skladišča v podatkovno skladišče posreduje izključno psevdonimizirane podatke, zaradi česar ne more priti do neposrednega posega v varstvo OP v velikem obsegu. Za pridobitev izvornega OP mora lastnik področnega podatkovnega skladišča dostopati do podatkov v zbirki podatkov, ki se nahaja v izvornem sistemu, kjer upošteva pravila tistega sistema. Vprašanje se obravnava v okviru podpoglavja »Sorazmernost«.
13.	Točnost in ažurnost – ponudnik storitve Skrinja 2.0	Sama storitev Skrinja 2.0 sicer ne vsebuje osebnih podatkov, vendar se bodo podatki, ki se bodo nahajali v podatkovnem skladišču, izkazali za netočne ali neažurne	Majhna, saj bi morale predhodne analize prenosa in obdelave podatkov odpraviti možnost netočnosti in neažurnosti	Majhna, prikazani podatki ne bi smeli biti OP, saj bi morali biti pred prikazom psevdonimizirani	Majhna	Točnost in ažurnost podatkov v podatkovnem skladišču bo le tolikšna, kolikšna bo točnost in ažurnost podatkov v izvorni bazi podatkov, pred njenim prenosom v podatkovno skladišče. Vprašanja točnosti in ažurnosti se obravnavajo v okviru podpoglavja »Točnost in ažurnost«.
14.	Omejitev shranjevanja	OP se v okviru storitve Skrinja 2.0 obdelujejo po času, ki je predviden za njihovo hrambo.	Majhna, saj bi morale predhodne analize prenosa in obdelave podatkov odpraviti možnost neustrezne hrambe	Srednja, hramba OP preko časa, ki je predviden za njihovo hrambo, sama po sebi povzroča veliko resnost, vendar se v podatkovnem	Srednja	Vprašanje roka hrambe se obravnava v okviru podpoglavja »Rok hrambe«.

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
				skladišču nahajajo le psevdonimizirani podatki, zaradi česar je resnost prekomerne hrambe le srednja.		
15.	Celovitost, zaupnost (informacijska varnost)	Pri izvajanju storitve Skrinja 2.0 se ne zagotavlja ustrezna informacijska varnost	Majhna, saj se celotna storitev Skrinja 2.0 zagotavlja v okviru zagotavljanja državnega računalniškega oblaka, ki deluje po uveljavljenih standardih za zagotavljanje informacijske varnosti	Velika, morebitna neustrezna varnost bi na primer lahko pomenila kopiranje podatkov, ki bi lahko bili neustrezno psevdonimizirani, …	Visoka, zaradi velike resnosti	Na vprašanja o informacijski varnosti storitve Skrinja 2.0 se odgovori v okviru podpoglavij: »Notranja sledljivost obdelave«, »Sledljivost posredovanja (zunanja sledljivost)«, »Zavarovanje« in »Sistemi za upravljanje varovanja informacij (SUVI)«. Glede na to, da gre za eno največjih tveganj pri projektu, se ukrepom za obvladovanje tveganja ob vsakoletnem pregledu nameni posebna pozornost.
16.	Celovitost, zaupnost (informacijska varnost) / razkritje	Pri izvajanju storitve Skrinja 2.0 pride do razkritja pri identificiranju posameznika, na katerega se podatki nanašajo	Majhna, saj se celotna storitev Skrinja 2.0 tehnično nahaja okviru zagotavljanja državnega računalniškega oblaka, ki zagotavlja najvišje standarde varovanja podatkov	Srednja, projekt predvideva centralizirano obdelavo le psevdonimiziranih podatkov, do razkritja bi lahko prišlo le v primeru, da bi bili podatki, ki jih lastnik področnega podatkovnega skladišča	Srednja, zaradi velike resnosti	MJU vzpostavi sistem pravil in aktivnosti za gostovanje in poslovanje v podatkovnem skladišču, ki bodo namenjeni izvedbi postopka prekinitve izvajanja storitve v primeru ugotovitve situacije iz opisanega tveganja. Dolgoročno želi MJU zagotoviti storitev Skrinja 2.0 čim širšemu krogu organov državne uprave, zato bo dolgoročno gledano vzpostavil kompetenčni center. Vprašanje se obravnava v okviru podpoglavja »Izobraževanje«.

	A	B	C	Č	D	E
	Načelo/vsebina	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
				posreduje v okolje podatkovnega skladišča, neustrezno psevdonimizirani		

9 SEZNAM UPORABLJENIH KRATIC

Kratica	Slovenski izraz/pojasnilo
DPIA	Ocena učinkov v zvezi z varstvom OP (angleško: Data protection impact assessment)
DRO	Državni računalniški oblak
DŠ	Davčna številka
GDPR	Splošna uredba o varstvu podatkov (General Data Protection Regulation)
ISPAP	Informacijski sistem za posredovanje in analizo podatkov o plačah, drugih izplačilih in številu zaposlenih v javnem sektorju
MFERAC	Enotni računovodski sistem Ministrstva za finance
MJU	Ministrstvo za javno upravo
OP	Osebni podatki

10 VIRI

1. Ocene učinkov na varstvo podatkov, Smernice Informacijskega pooblaščenca, Verzija: 1.0, datum izdaje: 23. 11. 2017;
2. Presoje vplivov na zasebnost pri projektih eUprave, Smernice Informacijskega pooblaščenca, Verzija: 1.0, datum izdaje: 22. 7. 2010;
3. Elaborat: Koncept sistema poslovne inteligence ter poslovnih in uporabniških zahtev na MJU za podatkovna vira ISPAP in MFERAC IT, Center poslovne odličnosti Ekonomske fakultete Univerze v Ljubljani, Avtorji: dr. Jurij Jaklič, dr. Jure Erjavec, dr. Luka Tomat, Ljubljana, 27. 1. 2017;
4. Predlog tehnične rešitve za izvedbo računalniških storitev izdelave predloga rešitve za tehnično postavitev podatkovnega skladišča, interno gradivo, december 2017, Avtorji: Žiga Vaupot, Mojca Gros, Matjaž Zupan 22. 12. 2017;
5. Dokument z generičnimi tehnološkimi zahtevami, MJU - objavljen na portalu NIO, zadnja verzija v2.2.3: dostopno na spletnem naslovu

   https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743
6. Dokument z generičnimi tehnološkimi zahtevami, MJU – objavljen na portalu NIO, zadnja GTU-LOP_1.1.1; dostopno na spletnem naslovu

   https://nio.gov.si/nio/asset/dokument+genericne+tehnoloske+zahteve+gtz-743
7. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo)
8. UREDBA (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 (Splošna uredba o varstvu podatkov)

11 PRILOGE DPIA

Priloga 1: Izjava lastnik področnega podatkovnega skladišča, da podatki, ki jih bo prenesel v podatkovno skladišče MJU v okviru projekta Skrinja 2.0, ne vsebujejo osebnih podatkov;

Priloga 2: Postopek za ugotovitev izpolnjevanja osnovnih zahtev uporabe storitve Skrinja 2.0

Priloga 3: Vključitev zunanjih izvajalcev, obdelovalcev OP, v zagotavljanje storitve Skrinja 2.0

Priloga 4: Kriteriji za oceno ustreznosti ocene učinkov

Priloga 5: Elaborat: Koncept sistema poslovne inteligence ter poslovnih in uporabniških zahtev na MJU za podatkovna vira ISPAP in MFERAC IT, Center poslovne odličnosti Ekonomske fakultete Univerze v Ljubljani, Avtorji: dr. Jurij Jaklič, dr. Jure Erjavec, dr. Luka Tomat, Ljubljana, 27. 1. 2017

Priloga 6: Predlog tehnične rešitve za izvedbo računalniških storitev izdelave predloga rešitve za tehnično postavitev podatkovnega skladišča, interno gradivo, december 2017, Avtorji: Žiga Vaupot, Mojca Gros, Matjaž Zupan 22. 12. 2017

Priloga 1

IZJAVA

lastnika področnega podatkovnega skladišča, da podatki, ki jih bo prenesel v podatkovno skladišče MJU v okviru projekta Skrinja 2.0, ne vsebujejo osebnih podatkov

Lastnik področnega podatkovnega skladišča _____

izjavljam, da smo celotno vsebino zbirke podatkov_____,

ki bo prenesena v podatkovno skladišče MJU v okviru projekta Skrinja 2.0, pregledali in ugotovili, da ne vsebujejo osebnih podatkov.

Iz prenesenih podatkov ni mogoče niti neposredno niti posredno določiti identitete posameznika.

Če bi se naknadno izkazalo, da bi bilo mogoče iz prenesenih podatkovnih virov na kakršenkoli način in iz katerikoli razlogov določiti identiteto posameznika, se strinjamo, da ponudnik storitve Skrinja 2.0 MJU prekine izvajanje dogovora o uporabi storitve do izpolnitve vseh zahtev, ki jih je treba izpolnjevati v primeru obdelave OP v okviru storitve Skrinja 2.0.

Podpis_____

Datum_____

Postopek za ugotovitev izpolnjevanja osnovnih zahtev uporabe storitve Skrinja 2.0

1. Podatkovni vir vsebuje osebne podatke:

NE: Bodoči lastnik področnega podatkovnega skladišča mora predložiti izjavo iz Priloge 1.

DA: Bodoči lastnik področnega podatkovnega skladišča mora izpolniti zahteve:

a. Bodoči lastnik področnega podatkovnega skladišča:

- predloži ponudniku storitve Skrinja 2.0 navedbo pravne podlage za obdelavo OP;
- predloži ponudniku storitve Skrinja 2.0 DPIA, ki jo ponudnik pregleda z vidika izpolnjevanja Kriterijev za oceno ustreznosti ocene učinkov, ki je kot Priloga 4 del te DPIA;
- predloži ponudniku storitve Skrinja 2.0 obrazložitev, da DPIA ni potrebna.

b. Bodoči lastnik področnega podatkovnega skladišča podpiše pogodbo o obdelavi psevdonimiziranih podatkov v delu zagotavljanja storitve v okviru tega projekta.

Priloga 3

Vključitev zunanjih izvajalcev, obdelovalcev OP, v zagotavljanje storitve Skrinja 2.0

Pred podelitvijo pravic za dostop do sistema, ki ga upravlja zunanji izvajalec in vsebuje OP, za zagotovi, da:

1. Zunanji izvajalec razpolaga s pravno podlago za izvajanje konkretne storitve, ki vključuje pravno podlago za obdelavo OP (pogodba, dogovor,…).
2. Zaposleni pri zunanjem izvajalcu so podpisali ustrezne izjave v zvezi z obdelovanjem OP.

Kriteriji za oceno ustreznosti ocene učinkov

Kriteriji za oceno ustreznosti DPIA - katere elemente mora vsebovati DPIA - podajajo smernice A29 WP:

 Podan je sistematičen opis obdelave (člen 35(7a)):

 Upoštevani so narava, obseg, okoliščine in nameni obdelave (uvodna določba 90);

 Opredeljen je nabor podatkov, upravljavci in uporabniki ter roki hrambe;

 Podan je opis podatkovnih tokov in udeleženih subjektov;

 Podan je opis sredstev obdelave (strojne in programske opreme, omrežij, človeških virov in uporabljenih komunikacijskih sredstev);

 Upoštevana je skladnost z odobrenimi kodeksi ravnanja (člen 35(8)).

 Podana je ocena nujnosti in sorazmernosti (člen 35(7b)):

 Opredeljeni so ukrepi za zagotavljanje skladnosti, ki vključujejo:

 ukrepe, ki prispevajo k upoštevanju nujnosti in sorazmernosti, in spoštovanju temeljnih načel:

 določeni, izrecni in zakoniti namen(i) (člen 5(1b));

 zakonitost obdelave (člen 6);

 obdelava je ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki (člen 5(1c));

 upoštevani je omejitev shranjevanja – roki hrambe (člen 5(1e));

 ukrepe, ki prispevajo k varstvu pravic posameznika:

 informiranje posameznika o obdelavi podatkov (členi 12, 13 in 14);

 pravica do seznanitve in prenosljivosti podatkov (člena 15 in 20);

 pravica do popravka in izbrisa podatkov (člena 16, 17 in 19);

 pravica do ugovora in omejitve obdelave (členi 18, 19 in 21);

 odnosi s (pogodbenimi) obdelovalci (člen 28);

 varovalke glede prenosa podatkov v tretje države (Poglavje V.);

 predhodno posvetovanje (člen 36).

 Obvladovana so tveganja za pravice in svoboščine posameznika:

 Podana je ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84), pri čemer so tveganja ocenjena z vidika posameznika, tako da:

 so upoštevani viri tveganj (uvodna določba 90);

 so upoštevani možni učinki na pravice posameznika v primeru nezakonitega dostopa, spremembe ali izgube podatkov;

 sta ocenjeni verjetnost in resnost tveganj (uvodna določba 90).

 Opredeljeni so ukrepi za obvladovanje tveganj (člen35(7d) in uvodna določba 90).

 Vključene so zainteresirane strani:

 Pridobljeno je mnenje DPO (člen 35(2));

 Pridobljena so mnenja posameznikov oziroma predstavnikov posameznikov, kjer je to primerno (člen 35(9)).