

Na podlagi, 51. in 89. člena Statuta Mestne občine Ljubljana (Uradni list RS, št. 31/21 – uradno prečiščeno besedilo) in 4. člena Odredbe o informacijski varnostni politiki št. 386-1/2024-1 z dne 11.10.2024 izdaja župan Mestne občine Ljubljana

## **P R A V I L N I K O UPORABI STORITEV RAČUNALNIŠTVA V OBLAKU**

### **I. SPLOŠNE DOLOČBE**

#### **1. člen**

Ta pravilnik za uporabo storitev računalništva v oblaku Mestne občine Ljubljane (v nadaljnjem besedilu: MOL) določa informacijsko-varnostne kontrole za zaščito podatkov MOL ter predpisuje postopke odobritve, operativne postopke upravljanja in pravila uporabe storitev računalništva v oblaku MOL z namenom zagotavljanja zakonske skladnosti ter razpoložljivosti, zaupnosti in celovitosti storitev, in sicer za naslednja področja:

1. odobritev poslovne uporabe storitve,
2. nadzor ustreznosti pogodbenih določil za najem storitev,
3. upravljanje storitvenih licenc ponudnikov;
4. sistemsko-administrativno upravljanje storitev, ki vključuje upravljanje sistemskih funkcij in uporabniških funkcionalnosti ter upravljanje z uporabniškimi identitetami;
5. uporaba storitev s strani uporabnikov, ki pri delu z informacijskimi sredstvi v upravljanju MOL MU ali z osebnimi uporabniškimi informacijskimi sredstvi prek svetovnega spleta uporabljajo storitve.

Ta pravilnik je namenjen uporabnikom in uporabnicam storitev računalništva v oblaku MOL (v nadaljnjem besedilu: uporabnik), ki so zaposleni na MOL ali so zunanji pogodbeni izvajalci, ki za poslovne potrebe Mestne uprave MOL (v nadaljnjem besedilu: MU MOL) uporabljajo storitve računalništva v oblaku MOL, ter izvajalcem Službe za digitalizacijo MU MOL (v nadaljevanju: SDIGI), ki administrativno-tehnično upravlja s storitvami računalništva v oblaku MOL.

Storitev računalništva v oblaku MOL je storitev, ki jo ponudnik javno dostopnih storitev računalništva v oblaku (v nadaljevanju: ponudnik) ponuja skladno z določili zakonodaje EU in RS in jo vodstvo MOL odobri ter MU MOL uporablja za poslovne namene v okolju ponudnika skladno s pogodbo o najemu konkretne storitve (v nadaljnjem besedilu: storitev).

#### **2. člen**

V MOL je dovoljena uporaba storitev naslednjih storitvenih modelov računalništva v oblaku:

1. Infrastruktura kot storitev (angl. »Infrastructure as a Service - IaaS«), to je računalniška infrastruktura, pogosto ponujeno z uporabo virtualizacije. V to kategorijo sodijo strežniki, hramba, omrežje ali infrastruktura kot storitev (IaaS).
2. Platforma kot storitev (angl. »Platform as a Service - PaaS«), to so storitve, ki že vključujejo osnovne dodatne funkcionalnosti, praviloma v obliki programskega vmesnika, ki ga uporabnik kot platformo uporablja pri razvoju lastnih informacijskih rešitev oziroma uporabi s strani ponudnika predvidenih licenčnih funkcionalnosti.
3. Programska oprema kot storitev (angl. »Software as a Service - SaaS«), to so storitve zagotavljanja celotne infrastrukture skupaj s programsko opremo, nastavitvami za njeno delovanje ter hrambo podatkov. V to kategorijo sodijo funkcionalnosti poslovnih aplikacij ali programska oprema kot storitev (SaaS), za uporabo katerih praviloma zadošča brskalnik in dostop do interneta, vse ostalo zagotavlja ponudnik storitve.

### **II. ODOBRITEV POSLOVNE RABE STORITVE**

#### **3. člen**

SDIGI predlaga vodstvu MOL uvedbo storitve. Storitve se praviloma lahko uporabljajo le za obravnavo informacijskih premoženj, za katere SDIGI in pooblaščen oseba za varstvo osebnih podatkov MU MOL

ocenita, da niso varnostno kritična, ter za informacijska premoženja, pri katerih so opredeljene naslednje mejne varnostne zahteve:

1. Zaupnost:
  - Dostop omejen na uslužbenca organa.
  - Nepooblaščen razkritje informacij ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike.
2. Celovitost:
  - Celovitost je lahko okrnjena, vendar je okrnjenost mogoče prepoznati
  - Nepooblaščen sprememba ali uničenje informacij in informacijskih sistemov ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike.
3. Razpoložljivost:
  - Nerazpoložljivost več kot 24 ur.
  - Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko omejene negativne učinke na poslovanje organa, premoženje organa ali posameznike.

V primeru izrednih poslovnih okoliščin SDIGI lahko vodstvu MOL predlaga tudi storitev z višjo stopnjo varnostnega tveganja. V takem primeru je potrebno v predlogu jasno opredeliti vse višje varnostne zahteve naročnika in potrditi sposobnosti izpolnjevanja takih zahtev s strani izvajalca storitve v oblaku.

Predlog SDIGI za odobritev storitve oziroma konkretne storitvene licence vsebuje najmanj:

1. Ocenilo varnostnega tveganja informacijskega premoženja zagotovi ključni uporabnik storitve. Pri tem uporablja metodologijo vrednotenja varnostnega tveganja informacijskega premoženja MOL, ki jo opredelita SDIGI in pooblaščen oseba za varstvo osebnih podatkov MU MOL;
2. Opis funkcionalnosti storitve, kot jih omogoča storitvena licenca ponudnika;
3. Opis predvidenega obsega poslovne rabe funkcionalnosti in ukrepi omejevanja, če zaradi varnostnih ali drugih poslovnih razlogov ni predvidena raba vseh funkcionalnosti;
4. Presojlo vpliva na poslovanje, upošteva pogodbeno tveganja, najmanj za kontrole:
  - a) Zaupanje v ponudnika
    - neenakomerne pogajalske moči (ponudnik-uporabnik),
    - netransparentnost ponudnikov (zasebnost, zaupnost, celovitost, razpoložljivost),
    - problem »multi-tenancy« (sobivanje naročnikov na isti opremi),
    - zamegljena lokacija podatkov,
    - neustrezna raven medsebojne izolacije souporabnikov virov,
    - nerazumevanje obsega prenešenih odgovornosti na ponudnika,
    - odpoved storitve ali prenehanje ponudnika,
    - prevzem ponudnika skupaj s podatki,
    - zloraba posebnih (najvišjih) pooblastil,
    - razkritje podatkov organom pregona, industrijsko vohunjenje,
  - b) Zanesljivost vira financiranja
    - začasna prekinitve pravic rabe zaradi nezmožnosti plačila licenčnine zaradi višje sile,
    - nezmožnost elastičnosti – najem storitve po dejanski porabi za določeno obdobje aktivnosti,
    - finančna odgovornost za neizpolnjevanje pogodbenih zahtev.
  - c) Varnost (zaupnost, celovitost, razpoložljivost)
    - zmanjšana prenosljivost podatkov – prenosljivost storitve med ponudniki,
    - nezmožnost merljivosti storitve za kontrolo odzivnosti – netransparentnost zagotovljene procesne moči za procesiranje zahtev, kar onemogoča razmejitev odgovornosti med procesnimi zakasnitvami/zakasnitvami na prenosni poti,
    - nezadostno, nepopolno ali neučinkovito brisanje podatkov,
    - zmanjšanje vpliva na upravljanje - nezmožnost preverjanja izvajanja politik varovanja podatkov (ustreznost antivirusne zaščite, uveljavljanje politik izvajanje varnostnega kopiranja za naročnike zahteve za primere incidentov: (a) časovno obdobje še znosne izgube sprememb podatkov, ki jih poslovni proces prenese ob izpadu in bi jih morali uporabniki ponovno vnesti sami, (b) še sprejemljiv čas za okrevanje po obvestilu o motnjah, okrevalni postopki v primeru razpada celovitosti podatkov zaradi napake naročnika ali zunanjega napada),
    - zagotavljanje podpore v primeru incidenta oziroma nedelovanja pogodbenih funkcionalnosti,
    - odtekanje podatkov pri nalaganju/snemanju ali znotraj oblaka,
    - razkritje ali izguba šifrirnih ključev,

- neskladnost pri zaščiti podatkov pri ponudniku in odjemalcu (običajno nezadostna zaščita pri odjemalcu),
- zloraba vmesnika za upravljanje storitve.

Tveganja morajo biti naslovljena s pripadajočimi določili v pogodbi o najemu za vsako konkretno storitev. V primeru tipskih pogodb ponudnika mora ponudnik zagotoviti pojasnila za navedena tveganja.

5. Presoja vpliva na poslovanje, upošteva tveganja informacijsko-komunikacijskih kanalov, najmanj za kontrole:
  - neustrezna prepustnost prenosnih poti,
  - razkritje podatkov med njihovim prenosom prek prenosnih poti.
6. Presoja vpliva na zasebnost v primeru hrambe ali obdelave osebnih podatkov;
7. Opis preverjanja ravni zavarovanja osebnih podatkov na podlagi kontrolnega seznama (Priloga 1);
8. Opis operativnih postopkov za zavarovanje dokumentarnega gradiva zbranega v okviru storitve;
9. Opis operativnih tehničnih postopkov nadzora in upravljanja za zagotavljanje celovitosti, zaupnosti, razpoložljivosti storitve.

V primeru, da ponudnik storitve razširi obseg funkcionalnosti v okviru iste storitvene licence, SDIGI dopolni predlog za odobritev storitve in za tako funkcionalnost ponovno pridobi odobritev vodstva MOL. Do potrditve s strani vodstva MOL mora biti raba funkcionalnosti, če to omogočajo licenčni administrativni postopki, s strani tehničnega skrbnika storitve onemogočena.

SDIGI odobrene storitve prevzame v upravljanje in preda v uporabo ter zagotavlja sistemsko in uporabniško podporo.

Uporabnik ob upoštevanju znanih tveganj in omejitev odgovorno uporablja storitev skladno z Odredbo o informacijski varnostni politiki (št. 386-1/2024-1 z dne 11. 10. 2024; v nadaljnjem besedilu: Odredba) in tem pravilnikom.

### III. UPRAVLJANJE LICENC

#### 4. člen

MOL kot naročnik storitve je odgovoren za pravočasnost zagotavljanja pogodbeno predvidenih kritičnih pogojev, ki vključujejo zagotavljanje rednih in neprekinjenih finančnih virov, ki so pogoj za poslovno razpoložljivost storitve računalništva v oblaku MOL.

#### 1. Nadzor funkcionalne ustreznosti in pogodbene skladnosti – Tehnični skrbnik storitve

#### 5. člen

Pogodba o najemu storitev lahko vsebuje več konkretnih licenčnih storitev. Izbrane konkretne licenčne storitve so lahko s strani ponudnika vključene v konkretni namensko zaokrožen licenčni sveženj (»bundle«) (v nadaljnjem besedilu: licenčni sveženj).

Tehnični skrbnik storitve je odgovoren za tehnični nadzor izvajanja pogodbenih obveznosti ponudnika za pogodbene licenčne storitve ali licenčne svežnje ter za izvajanje formalne operativne komunikacije s ponudnikom.

Tehnični skrbnik storitve mora poznati funkcionalni namen licence oziroma sestavo licenčnega svežnja in redno zagotavlja tehnična pojasnila, ki omogočajo učinkovito tehnično vzdrževanje, uporabo ali izvajanje poslovnih prilagoditev zaradi morebitnih sprememb licenčnih funkcionalnosti s strani ponudnika.

Tehnični skrbnik o vsaki spremembi funkcionalnosti takoj seznani vodjo SDIGI in skrbnika licenc v SDIGI. Spremembe storitve morajo biti obravnavane in ustrezno dokumentirane na način, kot to predpisuje ta pravilnik.

## 2. Enotno upravljanje storitev - skrbnik licenc

### 6. člen

S strani vodje SDIGI pooblaščen oseba (v nadaljevanju: skrbnik licenc) vodi skupno evidenco MU MOL pogodb o najemu storitev in vodi SDIGI poročila o stanju.

Skrbnik licenc v okviru evidence pogodb vodi evidenco licenc storitev, ki so vključene v pogodbo in ki vključujejo najmanj: rok veljavnosti, opis licence, opis storitvenega modela, seznam podsklopov licenčnih funkcionalnosti v primeru licenčnega svežnja, seznam uporabnikov licenc odobrenih storitev, skupaj z identificiranimi uporabniškimi potrebami za vsak posamezni najem. Za systemske storitve je evidentiran kot uporabnik tehnični skrbnik storitve, za poslovne storitve konkreten uporabnik MU MOL.

Skrbnik licenc izvaja redni nadzor veljavnosti licenc, koordinira izvajanje pravočasnih operativnih ukrepov za zagotavljanje trajne aktivnosti licenc, izvaja redni nadzor izvajanja določil pogodb o najemu, ustreznosti kontaktov ter kontrole načina upravljanja storitve pri ponudniku in koordinira izvajanje požarnih vaj.

Skrbnik licenc v primeru zaznanega informacijsko-varnostnega tveganja o tem takoj obvesti vodjo SDIGI.

## 3. Vodstveni nadzor

### 7. člen

Vodja SDIGI določi obdobja za periodično izvajanje nadzora. O rezultatih notranjega nadzora poročata vodstvu MOL.

## IV. SISTEMSKO-ADMINISTRATIVNO UPRAVLJANJE STORITEV

### 8. člen

SDIGI opredeli in izvaja systemske operativne postopke za namene zaščite celovitosti, zaupnosti in razpoložljivosti licenčnih storitev.

SDIGI za vsako storitev pripravi in redno dopolnjuje tehnična navodila za upravljanje ter uporabniška navodila storitve, pogoje rabe in opis potencialnih tveganj.

SDIGI vodi in redno posodablja evidenco storitev skladno z Odredbo v okviru enotnega seznama sredstev in pravic, ki za namene upravljanja storitev vsebuje najmanj naslednje informacije, ki jih zagotovi tehnični skrbnik storitve:

1. Licenčne politike s kontrolami za periodično preventivno preverjanje veljavnosti licenc;
2. Opis enotnih internih pravil tehničnega administriranja storitve za usklajeno upravljanje tako v primeru, da upravljanje konkretne storitve izvaja en sam ali več internih izvajalcev podpore;
3. Opis načina pridobivanja zadostnega obsega poslovnih informacij za aktiviranje funkcionalnih sklopov storitve:
  - a) SDIGI pripravi obrazec za zajem informacij uporabniških potreb v obsegu, ki zagotavlja varno in pregledno upravljanje vsebinskih poslovnih področij. Pri tem upošteva vse licenčne funkcionalne lastnosti, ki jih omogoča storitev. V obrazcu so predstavljene splošne informacije o pogojih in omejitvah rabe, o obratovalnem času, v katerem je zagotovljena uporabniška podpora SDIGI, in razmejitve odgovornosti. Obrazec mora vsebovati rubrike za vnos informacij, in sicer najmanj za:
    - sistematično poimenovanje in avtorizacijo rabe delovnega področja;
    - identifikacijo osebnih podatkov za zagotovitev varne hrambe;
    - opredelitev lastnosti dokumentarnega gradiva (klasifikacijski znak, rok hrambe) za zagotovitev varnega ravnanja;

- postopek sistematičnega prevzema gradiva iz okolja storitve v dolgoročno hrambo v lokalno računalniško omrežje MOL MU brez vpliva na celovitost gradiva;
  - postopek za končno izločitev (dekomisioniranje) področja po poteku obdobja rabe.
- b) Informacije iz prejšnje točke mora zagotoviti ključni uporabnik v MU MOL (v nadaljevanju: ključni uporabnik) pred vzpostavitvijo delovnega področja za konkreten poslovni namen. Ključni uporabnik mora v primeru sprememb o le-teh takoj obvestiti skrbnika storitve, zlasti, če gre za spremembe uporabniških pravic ali vlog.
4. Seznam uporabnikov z uporabniškim opisom namena in predvidenega obdobja uporabe.
  5. Opis s strani MOL predvidenega obsega odobrenih uporabniških funkcionalnosti z opisom tveganj v primeru rabe za namene hrambe osebnih podatkov in hrambe dokumentarnega gradiva, ločeno in pregledno za vsako konkretno licenčno funkcionalnost. Priloga 1 opisuje vsebuje izjavo o seznanjenosti s pravili in načinom rabe storitve.
  6. Opis s strani MOL omejenih funkcionalnosti z opisom razlogov in tveganj v primeru rabe za namene hrambe osebnih podatkov in hrambe dokumentarnega gradiva.
  7. Opis postopkov za izločitev (dekomisioniranje) uporabniških področij po zaključku rabe in postopkov za sproščanje licenc.

V primeru storitve, ki ni predvidena za uporabo s strani poslovnega uporabnika, se gradivo zagotovi v konkretno licenčno funkcionalnost smiselnem obsegu.

#### 1. Administrator storitve

#### 9. člen

S strani SDIGI pooblaščen administrator storitve lahko administriranje storitve izvaja le z uporabo predvidenih odjemalcev v lokalnem omrežju in ob obvezni uporabi okna brskalnika brez beleženja dejavnosti (Primer: MS Edge InPrivate).

Uporaba osebnega računalnika ali druge mobilne naprave izven omrežja MU MOL za potrebe administriranja je dovoljena izjemoma na podlagi predhodne pisne odobritve vodje SDIGI. Izvaja se lahko le prek informacijskih sredstev ali opreme, ki so v upravljanju SDIGI.

Administriranje storitve lahko administrator izvaja le z uporabo namenskega administrativnega računa za vsako konkretno storitev. Hranjenje gesla administrativnega računa na osebem računalniku ali drugi napravi administratorja, s katero se dostopa do administrativnega vmesnika storitve, ki omogoča samodejno prijavo brez ponovnega vnosa gesla, ni dovoljeno. Administrator mora takoj po izvedenem posegu administrativno sejo z delovnim brskalnikom ali drug vmesnikom zapreti.

V primeru dodeljevanja licenčnih funkcionalnosti, ki so vezane na konkreten licenčni sveženj, in ki jih je mogoče v celoti aktivirati z aktivacijo licenčnega svežnja, administrator uporabniku lahko dodeli samo odobrene funkcionalne licence, v okviru le-teh pa samo tiste, ki jih za konkretno delo potrebuje ter razume način njihove uporabe in tveganja v primeru napačne rabe.

Administrator storitve mora o odkritih novih tveganjih, povezanih z rabo konkretne storitve, takoj poročati vodji SDIGI. Pogostost poročanja o splošnem stanju rabe storitve določi vodja SDIGI. Pri tem upošteva stopnjo tveganja rabe storitve.

### **V. POGOJI RABE STORITEV RAČUNALNIŠTVA V OBLAKU MOL, KI VELJAJO ZA NEPOSREDNE UPORABNIKE**

#### 10. člen

Poslovna uporaba storitve z uporabniškim računom, ki ima administratorske pravice, ni dovoljena.

Uporabniško podporo zagotavlja tehnični skrbnik storitve oziroma za to pooblaščen zunanji izvajalec na način, kot ga opredeli SDIGI.

#### 1. Ključni uporabniki

## 11. člen

V primeru, ko licenčna storitev ključnemu uporabniku omogoča samostojno aktivacijo delovnih področij, mora ta namero najaviti tehničnemu skrbniku storitve, ki mora zagotoviti aktivacijo skladno s predpisanimi pravili poenotenega upravljanja.

Ključni uporabnik je odgovorni koordinator uporabniških aktivnosti, skrbnik vsebine in podatkov področja ter odgovoren za opredelitev dostopnih pravic in vlog uporabnikov.

Ključni uporabnik je odgovoren za seznanitev uporabnikov o načinu poslovne rabe konkretne storitve, s tveganji v primeru obdelave osebnih podatkov in za primere ravnanja s pomembnim zakonsko zaščitanim arhivskim dokumentarnim gradivom.

Ključni uporabnik mora v primeru obdelave osebnih podatkov o tem sezniniti skrbnika obdelav osebnih podatkov oddelka, ki novo obdelavo vključi v evidenco obdelav osebnih podatkov in o tem obvesti pooblaščen oseba za varstvo osebnih podatkov MU MOL .

V primeru ravnanja z dokumentarnim gradivom se mora ključni uporabnik o tem posvetovati s skrbnikom dokumentarnega gradiva oddelka, ki gradivo vključi v katalog dokumentarnega gradiva MU MOL, in z vodjo glavne pisarne MU MOL.

## 2. Poslovni uporabniki

## 12. člen

Poslovni uporabniki (zaposleni v MOL in morebitni zunanji gostujoči uporabniki) morajo biti seznanjeni s pravili rabe konkretnih storitev. Seznanjenost potrdijo s podpisom izjave o seznanjenosti z informacijskimi varnostnimi politikami, ki je kot Priloga 1 sestavni del Odredbe in s podpisom izjave o seznanjenosti z načinom rabe konkretne storitve, ki ga poslovnemu uporabniku posreduje tehnični skrbnik storitve iz SDIGI.

Uporabniku je dovoljena uporaba storitve prek zasebnega informacijskega sredstva, če je to informacijsko-varnostno urejeno in uporabljano skladno z zahtevami Odredbe in na njeni podlagi sprejetimi internimi pravilniki. SDIGI lahko od uporabnika zahteva posredovanje stanja konfiguracije. V primeru ugotovljenih neskladnosti uporabnika opozori in pozove k posodobitvi. SDIGI v primeru kršitev določil uporabniku onemogoči rabo storitve.

V primeru zaznanih zlonamernih varnostnih dogodkov mora uporabnik o tem takoj obvestiti SDIGI.

SDIGI poslovnim uporabnikom, ki jih predhodno pooblasti ključni uporabnik, posreduje navodila za uporabo, skupaj z opisom morebitnih varnostnih omejitev rabe funkcionalnosti storitve. Na podlagi prejetih podpisanih obrazcev iz prvega odstavka tega člena, se uporabnikom dodeli uporabniški račun.

Storitev se v poslovne namene uporablja lahko le skladno z zahtevami MOL in ponudnika storitve. Uporabnik storitve je v obdobju uporabe storitve odgovoren za varovanje celovitosti in zaupnosti okolja konkretne storitve, ki mu je s strani MOL predana v uporabo. Storitev lahko uporablja le sam osebno in le za konkretne poslovne namene. Prepovedana je vsaka nenamenska ali zlonamerna raba storitve ali predaja poverilnic tretjim osebam za namene opravljanja aktivnosti v njihovem imenu.

V primeru uporabe storitev za podporo sodelovanju, kjer je mogoča široka avtonomnost rabe, se lahko podatki ali informacije, ki za MOL predstavljajo trajno dokumentarno vrednost, hranijo po predhodni uskladitvi z SDIGI le na mestih, ki po zaključku poslovne rabe omogočajo ohranitev celovitosti gradiva – to je sledljivost verzij ter nemoten in vsebinsko neokrnjen ter zaupen prenos v lokalno računalniško omrežje MU MOL.

V primeru uporabe storitev za namene hitrega komuniciranja ali klepeta v okviru teh storitev ni dovoljena objava osebnih podatkov ali zaupnih podatkov, kot tudi ni dovoljena objava dokumentarnega gradiva za namene hrambe, če to za tako gradivo predstavlja edino mesto hrambe.

V primeru uporabe videokonferenčne storitve snemanje ni dovoljeno, če storitev ne zagotavlja zakonsko zahtevanih funkcionalnosti revizijskega sledenja vpogledovanja v video gradivo. SDIGI v okviru MOL informacijskih storitev ne zagotavlja revizijskega sledenja rabe video gradiva.

Izjemoma je snemanje dovoljeno:

- če je to prej odobreno s strani Informacijskega pooblaščenca RS;
- če je predhodno preverjena zakonska skladnost in dovoljeno s strani vodstva MOL.
- če organizator videokonference o namenu snemanja in javni ali interni objavi posnetka seznani udeležence in od vseh pridobi osebno privolitev;
- če posnetek ne vsebuje osebnih podatkov;
- če se videokonferenčni posnetek uporablja za izobraževalne namene ali za namene prikaza uporabe in funkcionalnosti različnih informacijskih storitev MOL.

Uporabniki brez predhodnega pisnega dovoljenja poslovnega skrbnika ne smejo izvažati podatkov ali dokumentarnega gradiva izven področja storitve, kjer se tako gradivo izvorno hrani. V primeru prenosa delovnih gradiv je uporabnik sam odgovoren za skrb za ažurnost in verodostojnost podatkov v takih od vira hrambe odklopljenih – lokalnih verzij dokumentov. Lokalnih verzij dokumenta po prenosu ni dovoljeno lokalno urejati in nameščati na izvorno lokacijo, ker bi lahko prišlo do spremembe verzije na izvoru.

Podatke ali dokumente lahko namešča le tisti uporabnik, ki ima za to dodeljene pravice.

Nameščanje dopolnilnih programov, ter nameščanje programske kode, ki se v okviru storitve lahko namesti brez posredovanja uporabnika, mora predhodno varnostno preveriti in odobriti SDIGI.

Pridobivanje, hranjenje in širjenje podatkov ali informacij, ki negativno vplivajo na poslovanje MOL je prepovedano.

Način rabe storitve je s strani ponudnika storitve praviloma nadzorovan. SDIGI lahko revizijsko beleži dostope do storitve.

### 13. člen

Ta pravilnik začne veljati naslednji dan po objavi na intranetni strani MOL.

Priloga 1: Seznam kontrol za preverjanje skladnosti z zahtevami ZVOP

Številka: 386-1/2024-4

Datum: 11-10-2024

Župan  
Mestne občine Ljubljana  
*Zoran Janković*



## Priloga 1: Seznam kontrol za preverjanje skladnosti z zahtevami ZVOP

Referenca: Kontrolni seznam Informacijskega pooblaščenca RS za zagotavljanje skladnosti z ZVOP: IP. Varstvo OP – Računalništvo v oblaku - tč 4 – str 15.

Kontrolni seznam predstavlja niz **obveznih kontrol, ki predstavljajo minimalne potrditvene zahteve, brez izpolnitve katerih odločitev za uporabo storitev računalništva v oblaku ni mogoča**. Pri vsaki kontroli je dodan podrobnejši opis kontrole. V primeru potrebe se izvede podrobnejša presoja ustreznosti ponujenih storitev, izvedbo ocene tveganja.

Kontrolni seznam je namenjen enotnemu razumevanju in ugotavljanju skladnosti z obstoječimi zahtevami zakona o varstvu osebnih podatkov s strani naročnika in ponudnika.

Koordinira izpolnjevanje naročnik. Najprej kontrole, ki pripadajo naročniku samostojno izpolniti naročnik, nato posreduje obrazec v dopolnitev ponudniku, pri skupnih kontrolah je potrebno končno usklajevanje.

### Skupina kontrol: Obdelava osebnih podatkov – splošno

V okviru storitve je predvidena hramba ali obdelava osebnih podatkov.

<b>Naročnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:

#### 1) Naročnik razpolaga s pravno podlago za obdelavo osebnih podatkov.

Smernice: Naročnik mora razpolagati s pravno podlago (npr. privolitev posameznika ali podlaga v zakonu) za obdelavo osebnih podatkov, da sploh lahko obdeluje in posreduje osebne podatke (še preden se torej odloči za uporabo storitev računalništva v oblaku).

<b>Naročnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:

#### 2) Naročnik ve, katere kategorije osebnih podatkov bo iznašal v oblak.

Smernice: Naročnik mora v vsakem trenutku vedeti, katere kategorije osebnih podatkov iznaša v oblak; to lahko predstavlja katalog zbirke osebnih podatkov, podatkovni model.

Naročnik mora od ponudnika pridobiti natančne informacije o tem, katere kategorije osebnih podatkov zbira oziroma dalje obdeluje njegov informacijski sistem (velja predvsem za model SaaS - Programska oprema kot storitev), kjer bi se naročnik lahko šele z uporabo rešitve seznanil s tem, da bo prišlo do obdelave določenih kategorij osebnih podatkov).

<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

#### 3) Ponudnik ustreza vsem pogojem uporabe storitve, ki jih je postavil naročnik.

Smernice: Smernico lahko izpolnijo tudi tipske pogodbe in splošni pogoji, če ustrezajo vsem zahtevam naročnika. Upoštevati je treba tudi možnost, da ponudnik sicer ne omogoča prilagajanja, da pa izpolnjuje vse pogoje (tako naročnika kot npr. zakonske). Naročnik mora biti pozoren na pogodbeni določila glede možnosti spreminjanja pogojev tekom obdelave podatkov s strani ponudnika in mora biti pripravljen na morebitno potrebo po zamenjavi ponudnika. Naročnik mora biti o spremembah vnaprej obveščen, da lahko, če se z njimi ne strinja, prekine sodelovanje s ponudnikom.

<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

### Skupina kontrol: Pogodbena obdelava osebnih podatkov

#### 4) S ponudnikom računalništva v oblaku smo sklenili pisno pogodbo.

Smernice: Pogodba je lahko sklenjena tudi v elektronski obliki, ki je zakonsko dopustna in enakovredna pisni (npr. ZEPEP). Pogodba naj vsebuje priporočene varovalke (glej mnenje Delovne skupine iz člena 29).

8



<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**5) Pisna pogodba s ponudnikom računalništva v oblaku vključuje konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov.**

Smernice: Dogovor o zavarovanju je lahko sestavni del pogodbe oz. splošnih pogojev, ali pa drug dokument, priložen pogodbi (npr. aneks) ali sklic na obstoječe pravilnike in druge dokumente, ki to opredeljujejo (varnostne politike ipd.)

Zgolj sklic na določen člen zakona ne izpolnjuje kontrolne točke.

Konkretiziran dogovor pomeni, da so postopki in ukrepi natančno opisani, npr.: varnostna služba, protivirusni sistem, protipožarni sistemi.

Opozorilo: ponudnik iz tretje države mora spoštovati določbe ZVOP-1 o postopkih in ukrepih za zavarovanje osebnih podatkov, posebej opozarjamo na zahtevo po sledljivosti obdelave osebnih podatkov. Sledljivost obdelave osebnih podatkov pomeni, da je mogoče pozneje ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil.

<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**6) V pogodbi s ponudnikom računalništva v oblaku je opredeljeno, katere obdelave osebnih podatkov izvaja ponudnik in kakšna so njegova pooblastila.**

Smernice: Pogodba (oz. ustrezni pripadajoči dokument kot sestavni del pogodbe) med naročnikom in ponudnikom mora jasno navajati, kakšno obdelavo osebnih podatkov sme oz. mora izvajati ponudnik – obseg pooblastil, ki jih naročnik predaja ponudniku storitev mora biti jasno opisan. Življenjski cikel zagotavlja varnost podatkov od zajema, uporabe do uničenja in ima definirane in dokumentirane postopke in procese.

Primer: Naročnik mora vedeti, ali ponudnik izdeluje (tudi) varnostne kopije.

V nekaterih primerih je pomembno opredeliti tudi, česa NE SME izvajati ponudnik (npr. izdelovati kopij podatkov za lastne namene).

<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**7) Naročnik mora biti v vsakem trenutku seznanjen z vsemi podizvajalci, ki v imenu in za račun ponudnika izvajajo obdelavo osebnih podatkov naročnika ter katere obdelave izvajajo (načelo transparentnosti).**

**Ponudnik mora naročniku dati razumen rok pred uporabo storitev novega podizvajalca, v katerem se lahko naročnik odloči, da bo odstopil od pogodbe, če se z uporabo storitev novega podizvajalca ne bo strinjal.**

**Prenos osebnih podatkov podizvajalcu, s katerim se naročnik ne strinja, ni dopusten.**

Smernice: Smernica je izpolnjena npr. na način, da ponudnik svojim naročnikom zagotavlja ažuren in dostopen seznam vseh svojih podizvajalcev z opisom storitev, ki jih ti opravljajo za ponudnika.

Podizvajalci morajo zagotavljati enako raven zavarovanja kot ponudniki – prenos pooblastil s ponudnika na podizvajalca ne sme pomeniti znižanja ravni zavarovanja osebnih podatkov.

V primeru, da ponudnik in naročnik ne najdeta skupnega jezika glede določenega podizvajalca, mora ponudnik naročniku omogočiti ustrezen čas pred prekinitvijo pogodbenega razmerja, v katerem lahko k sebi prenese osebne podatke.

<b>Naročnik</b>	<b>Ponudnik</b>
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**8) Po preteku pogodbe ali na zahtevo naročnika bo ponudnik storitev računalništva v oblaku uničil vse osebne podatke, vključno z morebitnimi kopijami.**

Smernice: Naročnik mora biti natančno seznanjen, kdaj bodo osebni podatki, ki jih je zaupa ponudniku, dejansko izbrisani in na kakšen način.

Ponudniki, ki naročnikom ne znajo resnično in pošteno predstaviti, kdaj in kako bodo podatki dejansko uničeni ne izpolnijo tega pogoja.

h

Naročnik naj se zaveda, da si mora zagotoviti uporabnost podatkov tudi po preteku pogodbene obdelave, zato mora ponudnik naročniku omogočiti pridobitev kopije osebnih podatkov v strukturiranemu elektronskem formatu, ki naročniku omogoča nadaljnjo obdelavo podatkov.

Naročnik se mora zavedati, da k podatkom sodijo tudi dnevniki, ki izkazujejo sledljivost obdelave osebnih podatkov.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

## Skupina kontrol: Informacijska varnost (zavarovanje osebnih podatkov) - skladnost in revizija

### 9) Pred uporabo storitev računalništva v oblaku je naročnik sam ali s pomočjo zaupanja vredne tretje stranke izvedel analizo tveganja.

Smernice: Pri pripravi analize tveganja naj upravljavci upoštevajo sorazmernost z vidika obsega osebnih podatkov, kategorij osebnih podatkov ter občutljivosti osebnih podatkov, ki se bodo obdelovali v oblaku. (glej praktične primere v posebnih okvirčkih).

Priporočamo, da se analize tveganja izvedejo skladno z uveljavljenimi metodologijami, kot npr. ISO/IEC 27005:2008, ENISA Cloud Computing Security Risk Assessment ali drugimi uveljavljenimi standardi.

Naročnik
<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:

### 10) Fizična lokacija osebnih podatkov je znana v vseh fazah obdelave osebnih podatkov.

Smernice: Naročnik pozna lokacijo (točen naslov) vseh podatkovnih centrov, kjer bo potekala katerakoli faza obdelave osebnih podatkov, kar velja tudi za lokacije podizvajalcev.

Ponudnik mora naročniku podati resnično in pošteno predstavitev vseh informacij o tem, kje in kako bo obdeloval osebne podatke (naročniku npr. ne sme zamolčati, da v določeni fazi prihaja do iznosa osebnih podatkov v tretje države.) Naročnik lahko o tem zahteva izjavo od ponudnika.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

### 11) Naročnik ima pogodbeno pravico do revizije informacijskega sistema ponudnika oziroma ponudnik redno izvaja zunanje neodvisne revizije celotnega informacijskega sistema. Ponudnik strankam objavlja rezultate revizij informacijskega sistema in varnostnih pregledov v skladu z zakonodajo in varnostnimi standardi.

Smernice: Priporočamo, da ponudnik vsaj enkrat letno izvede zunanji revizijski pregled celotnega informacijskega sistema, ki zajema upravljanje IT, varnost in neprekinjeno poslovanje in pridobi neodvisno mnenje revizorja informacijskih sistemov za vse točke pregleda.

Notranja revizija ponudnika ne izpolnjuje te smernice.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

### 12) Ponudnik šifrira osebne podatke, ki se prenašajo v ali znotraj oblaka po nezaščitene komunikacijskih omrežjih.

Smernice. Zaščitena komunikacijska omrežja zagotavljajo zaupnost, avtentičnost in celovitost podatkov.

Ne velja za prenos podatkov izven nadzora upravitelja (npr. po internetu), če je med prenosom zagotovljena zaupnost in nespremenljivost podatkov.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**13) Naročnik je obveščen o dejanskih incidentih ter o načinih odkrivanja in rokovanja z incidenti, vključno s sredstvi pri ponudniku, ki so načrtovani in opisani v načrtu odziva na incidente**

Smernice: Incidenti naj se redno beležijo in obravnavajo. Postopki naj bodo vnaprej definirani in naj se redno posodablja. Ponudnikov SLA zagotavlja podporo pri rokovanju z incidenti, ki je potrebna za učinkovito izvedbo načrta odziva na incidente za vsako fazo v procesu:

- odkrivanje
- analiza
- obvladovanje
- izkoreninjenje
- obnovitev

Testiranje načrta odziva na incidente naj se izvaja vsaj enkrat letno.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**14) Naročnik mora biti seznanjen s pristopom, ki ga ponudnik uporablja za deljenje virov in s tehničnimi in drugimi ukrepi s katerimi ponudnik naslavlja varnostne vidike večstanovskosti (angl. multi-tenancy).**

Smernice: Naročnik mora vedeti, ali ima pri ponudniku zagotovljene svoje fizične vire ali svoje logične vire (s pomočjo virtualizacije), ter ali so njegovi podatki od podatkov drugih stanovalcev samo logično ločeni in shranjeni v skupni podatkovni bazi ali podatkovnih nosilcih ipd. Naročniki naj preverijo, ali sta logično ločevanje in uporaba večstanovskih sistemov (angl. multi-tenancy) sprejemljiva s strani zakonskih zahtev, ki urejajo njihovo poslovanje.

Naročniki naj ocenijo sprejemljivost tveganj, ki jih s sabo prinašajo večstanovskosti sistemi (logično ločevanje, superadministratorji, kršitve izolacije idr.).

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

**15) Ponudnik varuje svojo večstanovsko infrastrukturo in z načini varovanja seznaniti naročnika.**

Smernice: Naročnik naj od ponudnika zahteva opis (ali preverja delovanje) varnostnih kontrol, ki varujejo ponudnikovo večstanovsko platformo. Med njimi so najpomembnejše:

- Načini zagotavljanja ločitve med različnimi stanovalci njegovega informacijskega okolja (npr. ločevanje z omrežje VLAN, procesno /pomnilniško ločevanje virtualnih strojev, aplikativno ločevanje v aplikacijah SaaS, itd.).
- Načini zaščite ponudnikove programske opreme večstanovske platforme pred napadi.
- Načini utrjevanja in zagotavljanja odpornosti ponudnikove infrastrukture (npr. hipervizorja, omrežnih naprav, operacijskega sistema, lastne programske opreme) na programske varnostne napake. V to spadajo npr. postopki nameščanja popravkov programske opreme, testiranje in upravljanje sprememb lastne programske opreme ipd.

Na podlagi tega naj naročnik oceni dodatna tveganja, ki jim je zaradi večstanovskosti izpostavljen in potencialno uvede nove/dodatne kontrole.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

## Skupina kontrol: Pravice posameznika

**16) Naročnik je preveril, da postopki in infrastruktura ponudnika omogočata enostaven dostop do osebnih podatkov v primeru zahteve posameznika po seznanitvi z lastnimi osebnimi podatki v okviru predpisanih zakonskih rokov.**

Smernice: Naročnik naj se zaveda, da mora tudi pri uporabi storitev računalništva v oblaku zagotavljati izvrševanja pravice posameznika do seznanitve z lastnimi osebnimi podatki, pri čemer bo verjetno potrebno sodelovanje ponudnika.

Postopek in časovni okvir realizacije posameznikove zahteve po seznanitvi z lastnimi osebnimi podatki, ki se obdelujejo v oblaku, naj bo vnaprej predviden in opredeljen.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

## Skupina kontrol: Iznos osebnih podatkov v tretje države

### 17) Naročnik je seznanjen s podatkom, v katere (vse) tretje države se bodo iznašali osebni podatki.

Smernice: Osebni podatki bodo hranjeni in obdelovani izključno v državah EU/EGS

oz.

Osebni podatki se bodo iznašali v tretje države. (izven EU/EGS).

Naročnik
<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:

### 18) Pravne podlage za iznos OP v vsako izmed navedenih tretjih držav

Smernice: Naročnik mora imeti v primeru iznosa osebnih podatkov izven EU/EGS eno od možnih pravnih podlag (točke 18a-18g)

- a) Država, iz katere je ponudnik oblaka, oziroma v kateri bodo (tudi če le za kratek čas) hranjeni podatki, je na seznamu IP, v celoti ali delno zagotavlja VOP (Švica Hrvaška, ZDA-varni pristan, Makedonija) - odločba ni potrebna

Smernice:

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

- b) Ponudnik oblaka je zavezan Varnemu pristanu in izpolnjuje vse ostale kontrolne točke (odločba IP ni potrebna).

Smernice:

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

- c) Iznos bo opravljen na podlagi ene izmed navedenih izjem (odločba IP ni potrebna, tudi če država ne zagotavlja ustrezne ravni varstva OP): tako določa drug zakon ali obvezujoča mednarodna pogodba; podana je osebna privolitev posameznika, iznos je potreben za izpolnitev pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem osebnih podatkov ali za izvršitev predpogodbenih ukrepov, sprejetih kot odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki; iznos je potreben za sklenitev ali izvršitev pogodbe, ki je v korist posameznika, na katerega se nanašajo osebni podatki, sklenjeno med upravljavcem osebnih podatkov in tretjo stranko; iznos je potreben, da se pred hujšim ogrožanjem zavaruje življenje ali telo posameznika, na katerega se nanašajo osebni podatki; iznos se opravi iz registrov, javnih knjig ali uradnih evidenc, ki so po zakonu namenjene zagotavljanju informacij javnosti in so na voljo za vpogled javnosti na splošno ali katerikoli osebi, ki lahko izkaže pravni interes, da so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon

Smernice: Samo za iznose, ki niso masovni in pogosti!

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

- d) Država, v kateri bodo podatki, je na seznamu Evropske komisije (odločba IP je potrebna!)

Smernice:

Naročnik
<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:

- e) S ponudnikom oblaka, ki mu bomo zaupali OP smo sklenili standardne pogodbene klavzule (odločba IP je potrebna!)

Smernice: Navedite, kateri model: upravljavec-upravljavec/ upravljavec-pogodbeni obdelovalec.

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

- f) Ponudnik oblaka ima potrjena Zavezujoča poslovna pravila - odločba IP je potrebna!

Smernice:

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

- g) S ponudnikom oblaka smo sklenili drugo pogodbo, s katero zagotavljamo ustrezno raven varstva OP (zgled so standardne pogodbene klavzule) – odločba IP je potrebna!

Smernice:

Naročnik	Ponudnik
<input type="checkbox"/> DA <input type="checkbox"/> NE	<input type="checkbox"/> DA <input type="checkbox"/> NE
Opomba:	Opomba:

