

**DARS d.d.**

Ulica XIV. divizije 4, 3000 Celje,

ki ga zastopa Uprava

Matična številka: **5814251000**

Davčna številka: **SI 92473717**

(v nadaljevanju: DARS)

in

Matična številka: **5xxxxxxx**

Davčna številka: **SI xxxxxx**

(v nadaljevanju: Dobavitelj IKT rešitev)

skleneta naslednjo

**POGODBO O IZPOLNJEVANJU ZAHTEV INFORMACIJSKE VARNOSTI**

**1. člen**

**(uvodne določbe in predmet pogodbe)**

- 1.1. S to pogodbo se stranki dogovorita za izpolnjevanje zahtev informacijske varnosti, ki jih mora izpolniti Dobavitelj IKT rešitev. Ta pogodba predstavlja **krovni okvir** za zagotavljanje informacijske varnosti v okviru **vseh obstoječih, veljavnih in prihodnjih pogodb ali pogodbenih razmerij**, ki jih Dobavitelj IKT rešitev sklene z DARS-om, in sicer **ne glede na njihov predmet, vrednost ali trajanje**.
- 1.2. Sistem upravljanja varovanja informacij (v nadaljevanju: SUVI) pomeni nabor vseh postopkov in aktivnosti, ki jih mora izvajati Ponudnik IKT rešitve, z namenom, da se vzpostavi nadzorovano okolje glede varovanja zaupnosti, verodostojnosti in dostopnosti informacij.

**2. člen**

**(ISO/IEC 27001)**

- 2.1. Če je Dobavitelj IKT rešitev imetnik certifikata za standard ISO/IEC 27001 (v nadaljevanju tudi: Imetnik ISO certifikata), se šteje, da je izpolnil pogoje iz 3., 4., 5., 6., 7., 8., 9., 10., 11., 12., 13., 14., 15., 16., 17. in 22. člena te pogodbe. Vendar pa mora Imetnik ISO certifikata neposredno na

podlagi te pogodbe, izpolniti obveznosti iz (i) točke b) 7.1. te pogodbe, (ii) 9.2. člena te pogodbe ter (iii) in 18. člena te pogodbe.

- 2.2. Imetnik ISO certifikata mora DARS-u predložiti veljaven certifikat ISO/IEC 27001 ob podpisu te pogodbe, nato pa redno najkasneje 30 dni po vsakokratni obnovi certifikata ISO/IEC 27001, sicer se šteje, da ga nima več (od dne poteka zadnjega predloženega certifikata ISO/IEC 27001). DARS pa lahko Ponudnika IKT rešitve občasno tudi pozove, da certifikat ISO/IEC 27001 predloži in mu za predložitev določi rok, ki ne sme biti krajši od 15 dni.
- 2.3. Stranki ugotavljata, da lahko DARS, kadar koli preveri veljavnost certifikata ISO/IEC 27001 pri izdajatelju certifikata ISO/IEC 27001.
- 2.4. Če Dobavitelj IKT rešitev v času veljavnosti te pogodbe izgubi (ne glede na razlog) certifikat ISO/IEC 27001, predpostavke iz prvega odstavka tega 2. člena te pogodbe o izpolnjevanju nekaterih pogojev iz te pogodbe ne veljajo več (od dne poteka zadnjega predloženega certifikata ISO/IEC 27001), Dobavitelj IKT rešitev pa je še vedno dolžan izpolnjevati vse obveznosti iz te pogodbe, sicer se upošteva določbe 26.4 člena te pogodbe.

### **3. člen** **(pravila in postopki varovanja informacij)**

- 3.1. Dobavitelj IKT rešitev mora imeti sprejete pravilnike, standarde ali druga pravila (v nadaljevanju: Pravilniki) o SUVI. Pravilniki se morajo vsaj enkrat na leto pregledati in po potrebi posodobiti. Pravilnike in posodobitev Pravilnikov mora sprejeti vodstvo (zakoniti zastopniki) Dobavitelja IKT rešitve.
- 3.2. Dobavitelj IKT rešitev mora Pravilnike predati v pregled DARS-u pred podpisom pogodbe ali najkasneje 90 dni po podpisu pogodbe. DARS lahko občasno od Dobavitelja IKT rešitev zahteva, da ponovno predloži Pravilnike in posodobitve Pravilnikov. Če Dobavitelj IKT rešitev Pravilnikov ne predloži v določenem roku ali se kasneje izkaže, da Pravilniki ne izpolnjujejo več kriterijev iz te pogodbe, se to šteje za primer iz 26.4 člena te pogodbe.

### **4. člen** **(nadzor in usposabljanje)**

Zaposleni in druge osebe, ki pri Dobavitelju IKT rešitve opravljajo delo na drugi pravni podlagi (v nadaljevanju: Kadri) morajo v zvezi z varovanjem informacij uspešno zaključiti ustrezno usposabljanje glede zahtev za varovanje in varno ravnanje z informacijami. Na zahtevo DARSa mu mora Dobavitelj IKT rešitev predložiti poročilo o zaključenem usposabljanju Kadrov.

## **5. člen**

### **(varovanje v okviru kadrovanja)**

- 5.1. Preden novi Kadri začnejo z delom, mora Dobavitelj IKT rešitev izvesti ustrezna preverjanja novih Kadrov, vključno s preverjanjem njihove (ne)kaznovanosti, pregledom življenjepisov, priporočil in izkušenj ter z intervjuji.
- 5.2. Kadri morajo ob nastopu dela podpisati sporazum o nerazkrivanju in varovanju informacij (»NDA«) ali temu vsebinsko podoben sporazum (v nadaljevanju: Sporazum o varovanju informacij). Sporazum o varovanju informacij mora vključevati najmanj:
  - a. obveznost varovanja DARS-ovih informacij (kot so te definirane v 6. členu te pogodbe);
  - b. obveznost varovanja zaupnosti SUVI pri Dobavitelju IKT rešitev;
  - c. določbe, da Sporazum o varovanju informacij Kadre zavezuje tudi po prenehanju dela.
- 5.3. Dobavitelj IKT rešitev mora v Pravilnikih vključiti določbe, ki urejajo, na kakšen način je dovoljeno uporabljati elektronska sredstva, zlasti uporabo elektronskih sredstev na strokoven, zakonit in etičen način.
- 5.4. Dobavitelj IKT rešitev mora v Pravilnikih vključiti tudi pravila, ki omogočajo identifikacijo in prevzem sredstev (fizičnih in elektronskih) od Kadrov, ki ne delajo več za Dobavitelja IKT rešitev in/ali ko sredstev več ne uporabljajo.

## **6. člen**

### **(dostop do informacij)**

- 6.1. V primeru, ko ima Dobavitelj IKT rešitev informacije, ki pripadajo ali so zaupane DARS-u in se te nahajajo zunaj DARS-ovega okolja in/ali v primerih, ko ima Dobavitelj IKT rešitev oddaljen dostop do DARS-ovega okolja (v nadaljevanju: DARS-ove informacije), Dobavitelj IKT rešitev zagotavlja, da ima sprejete najmanj naslednje elemente kontrole glede aktivacije računov, ki omogočajo dostop do DARS-ovih informacij:
  - a. v Pravilnikih določen formalni postopek za pridobitev soglasja za dostop do informacij, pri čemer je soglasje odobreno le, če dostop temelji na poslovni potrebi izvajanja delovnih nalog (kar pomeni le najmanjši možen nivo dostopa, ki je potreben, in ne več);
  - b. o prošnji in odobritvi dovoljenja za dostop do informacij morajo odločati različne osebe;
  - c. uporabniški račun za dostop do informacij mora biti dodeljen vsakemu posamezniku posebej in si ga ne sme deliti več oseb;
  - d. privilegirani in administratorski uporabniški računi, to so računi s širokim nivojem dostopa, ki v okviru računalniškega sistema omogočajo obseg pravic, ki občutno presegajo obseg pravic običajnega uporabnika (v nadaljevanju: Privilegirani računi) se morajo razlikovati od standardnih uporabniških računov in morajo imeti unikatno uporabniško ime za dostop. Privilegirani računi morajo biti omejeni in dodeljeni le uporabnikom, ki imajo za to posebno dovoljenje (avtorizacijo).
- 6.2. Dobavitelj IKT rešitev mora imeti vzpostavljen nadzor nad gesli, kar vključuje najmanj naslednje:
  - a. pregled nad zgodovino uporabe in periodičen pretek (prenehanje veljavnosti) gesel;

- b. začasna gesla se mora sporočiti na varen način, po prvi uporabi pa jih je treba nemudoma spremeniti;
  - c. geslo je treba spremeniti takoj, ko nastopi razlog za sum, da je prišlo do nedovoljenega dostopa v račun;
  - d. gesla za dostop do računalniških sistemov in uporabniških računov s skupnim dostopom (generični računi) je treba spremeniti vedno, ko oseba, ki geslo pozna, ne dela več za Dobavitelja IKT rešitev ali iz drugega razloga nima več poslovne potrebe po dostopu;
  - e. pred ponastavitvijo gesla je treba preveriti identiteto osebe, ki zahteva ponastavitev;
  - f. vsa privzeta gesla je treba ob prvem dostopu spremeniti;
  - g. zahteve glede zadostne zaščitne moči gesel morajo biti skladne s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST) glede njihove dolžine in kompleksnosti.
- 6.3. Dobavitelj IKT rešitev mora imeti vzpostavljene nadzorne mehanizme glede onemogočenja računov, ki vključujejo vsaj naslednje:
- a. v Pravilniku določen postopek, glede ažurnega (npr. v roku 24 ur) onemogočenja računov tistih oseb, ki prenehajo z delom za Dobavitelja IKT rešitev ali nimajo poslovne potrebe za dostop;
  - b. v Pravilnikih določen postopek, ki zagotavlja, da je DARS v 24 urah obveščen o spremembah Kadrov Dobavitelja IKT rešitev, ki imajo dovoljenje za dostop do DARS-ovih informacij.
- 6.4. Dobavitelj IKT rešitev mora imeti vzpostavljene nadzorne mehanizme glede dostopa do računalniških sistemov in storitev, ki vključujejo najmanj:
- a. pregled dostopov vseh oseb, pri čemer se mora pregled sistemskih računov, testnih računov in generičnih računov izvesti in dokumentirati vsaj enkrat letno;
  - b. uporabniški račun se mora zakleniti po določenem številu neuspešnih poskusov dostopa;
  - c. račune, na katerih ni aktivnosti 90 dni je treba onemogočiti. Če se za določen račun predvideva, da se bo uporabljal redkeje kot je rok iz prejšnjega stavka (npr. četrtnetne, polletne ali letne obdelave), se šteje, da račun ni več aktiven, če na takšnem računu ni aktivnosti v obdobju, ki je dvakratnik predvidenega dostopanja;
  - d. nadzor nad sejami (uporabo računa), vključno z odjavami z računa in potekom seje;
  - e. vse aplikacije, do katerih se dostopa preko interneta, morajo imeti vzpostavljeno dvo-faktorsko avtentikacijo;
  - f. pri metodah oddaljenega dostopa (npr. zasebna virtualna omrežja, protokoli oddaljenega namizja) mora biti vzpostavljena dvo-faktorska avtentikacija.

## 7. člen

### (varnost omrežja in računalniških sistemov)

- 7.1. V primerih, ko ima Dobavitelj IKT rešitev DARS-ove informacije, je Dobavitelj IKT rešitev dolžan vzpostaviti najmanj naslednje nadzorne mehanizme za zagotavljanje varnosti omrežja in računalniških sistemov:
- a. uporabljati se morajo standardi utrjevanja operacijskih sistemov, aplikacij in omrežnih naprav;
  - b. na vse računalniške sisteme, ki obdelujejo DARS-ove informacije za katere je odgovoren in jih vzdržuje dobavitelj, je treba nameščati popravke za operacijski sistem, aplikacije in omrežne naprave in posodobitve glavnih komponent ob izdaji popravka (»patch«), glede na stopnjo tveganja v skladu s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST):

- visoko tvegane ranljivosti storitev, ki so dostopne preko interneta, se morajo odpraviti v roku do 30 dni;
  - c. računalniške sisteme, ki obdelujejo DARS-ove informacije in za katere je odgovoren in jih vzdržuje dobavitelj, je treba vzdrževati na način, ki omogoča nameščanje najnovejših varnostnih popravkov / servisnih paketov.
- 7.2. Dobavitelj IKT rešitev mora izvajati nadzor nad varnostjo omrežja, najmanj pa naslednje:
- a. DARSove informacije se ne sme shranjevati v de-militariziranem območju (DMZ);
  - b. na požarni pregradi (»firewall«), morajo biti vzpostavljena pravila, ki na vseh omrežnih vmesnikih omejujejo notranji (»inbound«) in zunanji (»outbound«) promet, pri čemer morajo ta pravila temeljiti na minimalnih varnostnih potrebah (torej mora biti promet čim bolj omejen, v okviru potreb);
  - c. sistemi za odkrivanje in preprečevanje vdorov morajo biti implementirani tako, da zaznajo in reagirajo na nedovoljen ali zlonameren omrežni promet;
  - d. zagotovljeno mora biti posodabljanje varnostnih nastavitev omrežnih naprav Dobavitelja IKT rešitev tako, da se kontinuirano zagotavlja informacija varnost skladno s tem 7. členom te pogodbe.
- 7.3. Če Dobavitelj IKT rešitev zagotavlja DARS-u tudi vzdrževanje (SLA) računalniškega sistema ali aplikaciji in pri tem zagotavlja tudi infrastrukturo, mora Dobavitelj IKT rešitev zagotoviti tudi zaščito proti porazdeljenim napadom z onemogočenjem storitve (DDoS). Dobavitelj IKT rešitev mora zagotavljati varnost računalniških sistemov, najmanj pa naslednje:
- a. končne naprave morajo biti šifrirane in zavarovane z geslom;
  - b. mobilne končne naprave (pametni telefoni, tablice) morajo biti varovane s sistemom upravljanja mobilne naprave (MDM);
  - c. strežniki in končne naprave morajo biti varovani s protivirusno zaščito, ki se redno posodablja.

## **8. člen**

### **(beleženje dogodkov in nadzor)**

Beleženje aktivnosti na računalniških sistemih mora biti izvedeno v skladu s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST). Prednostno se morajo beležiti anomalije v delovanju.

## **9. člen**

### **(upravljanje z ranljivostmi in grožnjami)**

- 9.1. Dobavitelj IKT rešitev mora imeti vzpostavljen postopek, ki je opredeljen v Pravilnikih, za stalno ocenjevanje in pravočasno odpravo ranljivosti v aplikacijah, operacijskih sistemih in drugih računalniških sistemih. Poleg tega mora biti delo in postopki pri Dobavitelju IKT rešitev oblikovano tako, da se identificira, oceni, odpravi in zaščiti pred novimi in obstoječimi varnostnimi ranljivostmi in grožnjami, vključno z virusi, »boti« in drugo zlonamerno kodo.
- 9.2. Dobavitelj IKT rešitev mora DARS-u dovoliti izvedbo varnostnega pregleda računalniškega sistema in aplikacij, ki obdelujejo DARS-ove informacije in ki jih ima ali z njimi upravlja Dobavitelj IKT rešitev in pri tem sodelovati, zlasti tako, da dopusti dostop do svojega računalniškega sistema, ni

pa dolžan kriti stroškov takšnega varnostnega pregleda. Na podlagi soglasja k tej pogodbi se šteje, da Dobavitelj IKT rešitev podaja soglasje k takšnim varnostnim pregledom. Po končanem varnostnem pregledu mora Dobavitelj IKT rešitev odpraviti vse odkrite ranljivosti.

#### **10. člen** **(upravljanje sprememb)**

Dobavitelj IKT rešitev mora imeti v Pravilnikih vzpostavljena pravila glede upravljanja sprememb, ki vključujejo najmanj:

- a. zahteve glede odobritve, klasifikacije, testiranja in načrta vrnitve pred spremembo;
- b. razmejevanje dolžnosti med zahtevo, odobritvijo in implementacijo;
- c. upravljanje in pregled nujnih sprememb znotraj določenega časa (npr. 24 ur).

#### **11. člen** **(upravljanje s sredstvi)**

- 11.1. Dobavitelj IKT rešitev mora hraniti aktualen seznam sredstev, vključno z računalniškimi sistemi, strojno opremo in programsko opremo (v nadaljevanju: Sredstva), če ima Dobavitelj IKT rešitev DARS-ove informacije.
- 11.2. Dobavitelj IKT rešitev mora po prenehanju njihove uporabe uničiti nosilce, na katerih so nameščene DARS-ove informacije, da se zagotovi varno ravnanje z informacijami (v fizični ali elektronski obliki) skladno s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST), pri čemer mora imeti vzpostavljen nadzor nad uničenjem Sredstev z namenom, da zagotovi ravnanje z informacijami (v fizični ali elektronski obliki) skladno s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST), ko se jih več ne potrebuje in hraniti dokumentiran dokaz o ustreznem uničenju.

#### **12. člen** **(ravnanje z informacijami)**

- 12.1. Dobavitelj IKT rešitev mora zagotoviti ločitev informacij drugih strank in DARS-ovih Informacij. Poleg tega mora Dobavitelj IKT rešitev ob podpisu te pogodbe predložiti opis toka informacij preko vseh njegovih okolij.
- 12.2. Komunikacija med DARS-om in Dobaviteljem IKT rešitev (vključno z elektronsko pošto, prenosom datotek, oddaljeno povezavo ipd.) mora biti zaščitena z ukrepi, ki nepooblaščenim preprečujejo prilaščanje ali uničenje informacij ter neupravičeno seznanjanje z njihovo vsebino.
- 12.3. Dobavitelj IKT rešitev mora imeti v Pravilnikih vzpostavljena ustrezna pravila in orodja za preprečevanje, odkrivanje in odziv v primeru izgube informacij.

- 12.4. DARS-ovih informacij se ne sme shranjevati ali prenašati z uporabo prenosnih naprav za shranjevanje, brez pisnega soglasja DARSa (pridobljenega preko postopkovne odobritve).

### **13. člen (šifriranje)**

- 13.1. V primerih, ko ima Dobavitelj IKT rešitev DARS-ove informacije, je treba za prenos informacij zagotoviti šifriranje.
- 13.2. Šifrirni ključi, ki jih ima v lasti ali jih upravlja Dobavitelj IKT rešitev, morajo biti shranjeni na varnem mestu z varovanim dostopom, poleg tega mora obstajati možnost obnovitve ključev.
- 13.3. Postopki in prakse šifriranja morajo biti skladni s splošno sprejetimi varnostnimi standardi (npr. ISO, NIST).

### **14. člen (fizična varnost)**

- 14.1. Dobavitelj IKT rešitev zagotavlja, da ima v Pravilnikih vzpostavljene postopke in fizičen nadzor, ki zagotavljajo varovanje fizičnih kopij in računalniškega sistema (npr. strojna in programska oprema, dokumentacija ter informacije), v primerih, ko ima Dobavitelj IKT rešitev DARS-ove informacije.
- 14.2. Podatkovni centri Dobavitelja IKT rešitev morajo biti fizično varovani, pri čemer mora biti v Pravilnikih dostop do podatkovnih centrov postopkovno urejen. V podatkovnih centrih mora biti zagotovljen ustrezen nadzor okolja (temperature, vlažnosti, zasilno napajanje) namenjen preprečitvi uničenja ali izgube informacij.
- 14.3. Dobavitelj IKT rešitev mora zagotoviti vsakoletno neodvisno oceno fizične varnosti prostorov. DARS lahko zahteva poročilo o opravljenih pregledih.

### **15. člen (neprekinjeno poslovanje in varnostne kopije)**

- 15.1. Dobavitelj IKT rešitev mora imeti vzpostavljen sistem neprekinjenega poslovanja in ponovne vzpostavitve delovanja v primeru katastrofe ali motnje v delovanju, skladno s (a) kritičnostjo informacij in/ali (b) pogodbenimi poslovnimi zahtevami, če ta pogodba take zahteve vključuje, ter zagotoviti naslednje nadzorne mehanizme:
- a. v okviru primarne lokacije mora biti zagotovljeno redundantno električno napajanje in zmožnost obdelave informacij;
  - b. zagotoviti je treba dodatno lokacijo za obdelavo informacij zaradi ponovne vzpostavitve funkcionalnosti DARSa znotraj dogovorjenega časovnega okvira po tej pogodbi;
  - c. letno je treba izvesti test odpornosti, da se izkaže sposobnost učinkovite ponovne vzpostavitve funkcionalnosti;
  - d. Operacijski sistemi in informacije v uporabi se morajo periodično varnostno kopirati, pri čemer je periodika odvisna od kritičnost informacij. Uporabnost varnostnih kopij je treba redno testirati;
  - e. varnostni mediji in/ali prenosi le-teh morajo biti ustrezno varovani.

## 16. Člen

### (odziv na varnostne incidente, upravljanje in poročanje)

- 16.1. Dobavitelj IKT rešitev mora imeti v Pravilnikih vzpostavljene postopke upravljanja z varnostnimi incidenti (npr. odtekanje, razkritje ali kraja informacij ipd.) in postopke ukrepanja, ki v razumnih okvirih zagotavljajo zaznavo, preiskavo, odziv, odpravo in obveščanje o dogodkih, ki pomenijo grožnjo za zaupnost, verodostojnost in/ali dostopnost informacij, v primerih, ko ima Dobavitelj IKT rešitev DARS-ove informacije. Postopki upravljanja z varnostnimi incidenti in postopki ukrepanja morajo biti dokumentirani, preizkušeni in preverjani vsaj enkrat na leto. DARS lahko zahteva dodatne preglede teh postopkov. DARS lahko zahteva poročilo o opravljenih pregledih.
- 16.2. Dobavitelj IKT rešitev mora v 24 urah obvestiti DARS o sumu ali ugotovljenem varnostnem incidentu, ki ima lahko potencialni vpliv na informacije. Poleg tega mora imeti Dobavitelj IKT rešitev v Pravilnikih dokumentirane postopke z določenimi kontaktnimi osebami pri DARS-u in Dobavitelju IKT rešitev, za zagotavljanje skladnosti z zahtevami glede obveščanja.
- 16.3. Dobavitelj IKT rešitev mora polno sodelovati z DARS-om zaradi razumevanja okoliščin, ugotovitve vzroka in določitve potrebnih ukrepov glede dejanskega varnostnega incidenta ali suma varnostnega incidenta.

## 17. Člen

### (podizvajalci)

- 17.1. Dobavitelj IKT rešitev zagotavlja, da podizvajalci, s katerimi sodeluje in ki pridejo v stik z DARS-ovimi informacijami izpolnjujejo vse obveznosti, ki jih mora izpolnjevati sam Dobavitelj IKT rešitev po tej pogodbi.
- 17.2. Pogodbe med Dobaviteljem IKT rešitev in podizvajalci morajo biti sestavljene tako, da določajo nadzorne mehanizme, vključno z nadzornimi mehanizmi namenjeni varovanju zaupnosti, dostopnosti in verodostojnosti informacij.
- 17.3. Izvajati se morajo začetna in kasnejše redne ocene, da se zagotovi, da podizvajalci ravnaajo skladno s tem pravilnikom in da se v primeru varnostnih incidentov in težav ustrezno ravna.
- 17.4. Dobavitelj IKT rešitev mora pridobiti predhodno pisno soglasje DARSa, preden začne poslovati s podizvajalcem, ki bo imel dostop to DARS-ovih informacij.

## 18.

### (obdobje hrambe in uničenje)

- 18.1. Dobavitelj IKT rešitev mora DARS-ove informacije hraniti le tako dolgo, kot je to določeno v posamezni pogodbi, razen če je drugačno obdobje hrambe zahtevano v veljavnih predpisih. Če ta pogodba ne določa trajanja hranjenja informacij, se informacije hranijo v času trajanja te pogodbe.



- 18.2. Ob prenehanju hranjenja informacij, mora Dobavitelj IKT rešitev vrniti, izbrisati ali varno uničiti informacije skladno z navodili DARSa. Med trajanjem te pogodbe lahko DARS od Dobavitelja IKT rešitev kadar koli zahteva varno uničenje informacij, v skladu z navodili DARSa.
- 18.3. Na zahtevo DARSa mora Dobavitelj IKT rešitev potrditi in predložiti dokaz, da so bile informacije uničene skladno z navodili.

## **19. člen**

### **(pravica do preverjanja informacijske varnosti)**

- 19.1. Dobavitelj IKT rešitev mora DARS-u in njegovim predstavnikom (npr. revizorji (notranji in zunanji), državni organi, podizvajalec) dovoliti, da preverijo, revidirajo, pregledajo in ocenijo prostore, dokumentacijo, sisteme, zbirke, dostope, informacije, prakse in postopke Dobavitelja IKT rešitev (in katerega koli podizvajalca, s katerim Dobavitelj IKT rešitev sodeluje) z namenom preveriti verodostojnost informacij in namenom nadzorovati skladnost s to pogodbo, vključno z varnostnim testom iz 9.2 člena te pogodbe. Dobavitelj IKT rešitev pa mora z DARS-ovim predstavnikom sodelovati enako kot s DARS-om.
- 19.2. Dobavitelj IKT rešitev mora zagotoviti, da bo DARS lahko preglede iz tega člena opravil tudi pri podizvajalcih.

## **20. člen**

### **(izjava Dobavitelja IKT rešitev)**

Dobavitelj IKT rešitev podaja izjavo, da dobavljena programska oprema in rešitev po najboljšem vedenju Dobavitelja IKT rešitev nima skritih funkcionalnosti ali stranskih vrat (*hidden features or backdoors*).

## **21. člen**

### **(določbe po Zakonu o informacijski varnosti)**

- 21.1. Dobavitelj IKT rešitev je seznanjen s tem, da je DARS zavezanec po vsakokratno veljavnem Zakonu o informacijski varnosti (v nadaljevanju: ZInfV), zato je DARS dolžan izvajati nadzor pri Dobavitelju IKT rešitev glede izvajanja te pogodbe in glede izpolnjevanja drugih zahtev ZInfV (v nadaljevanju: Dolžno nadzorstvo).

- 21.2. Dobavitelj IKT rešitev je dolžan DARS-u dovoliti izvajanje Dolžnega nadzorstva. DARS lahko v okviru Dolžnega nadzorstva od Dobavitelja IKT rešitev zahteva izvajanje Dolžnega nadzorstva, tudi, če bi zahteve presegale obveznosti po tej pogodbi, če DARS utemeljeno obrazloži, zakaj je takšen nadzor nad delovanjem Dobavitelja IKT rešitev nujen za izpolnjevanje obveznosti DARSa kot zavezanca po ZInfV.
- 21.3. Dobavitelj IKT rešitev je dolžan pomanjkljivosti, ki so bile odkrite v okviru Dolžnega nadzorstva opraviti.
- 21.4. Stroške izvajanja Dolžnega nadzorstva krije DARS, odpravo ugotovljenih varnostnih pomanjkljivosti pa Dobavitelj IKT rešitev.
- 21.5. Če Dobavitelj IKT rešitev DARS-u onemogoči Dolžno nadzorstvo in tako DARS-u onemogoči izpolnjevanje svojih obveznosti kot zavezanca po ZInfV, je Dobavitelj IKT rešitev dolžan DARS-u povrniti vse stroške (vključno s plačilom morebitnih prekrškovnih glob).

## **22. člen**

### **(življenjski cikel razvoja sistemov)**

- 22.1. Določbe iz tega člena veljajo le, če Dobavitelj IKT rešitev za DARS razvija programsko opremo.
- 22.2. Metodologija razvoja programske opreme:
- a. v Pravilnikih mora biti določena standardna metodologija razvoja programske opreme, ki mora biti formalno vpeljana. Metodologija razvoja programske opreme mora biti sporočena relevantnim Kadrom, kar vključuje specifikacijo arhitekture in zasnove, pregled poslovnih konceptov, sprejem varnih algoritmov in knjižnic, odstranitev testne kode in odpravo pogostih varnostnih napak (npr. OWASP prvih deset ranljivosti);
  - b. izvajati se mora preverba kode, da se zagotovi skladnost s standardno metodologijo razvoja programske opreme;
  - c. uporaba produkcijskih informacij v ne-produkcijskih okoljih naj se izvede le, kadar je nujno potrebno, pri čemer je potrebno zagotoviti enake varnostne mehanizme, kot obstajajo v produkcijskem okolju, ali pa morajo biti produkcijske informacije zadostno zamegljene;
  - d. če se uporablja programska oprema, ki je javno dostopna (npr. odprto-kodna programska oprema, »shareware«, »freeware«), mora biti ustrezno pregledana z vidika potencialnih tveganj, vključno s potencialnimi pravnimi tveganji (npr. kršitev avtorskih pravic);
  - e. metodologija razvoja programske opreme mora vključevati nadzorne mehanizme, ki zagotavljajo, da ta programska oprema ne bo imela škodljivega vpliva na varnost (npr. virus, trojanski konj, stranska vrata);
  - f. izvorna koda se mora shranjevati v orodju za nadzor verzij, ki je sprejemljiv za industrijo, s strogim nadzorom glede objave izvirne kode;
  - g. zahteva se upravljanje varnosti življenjskega cikla vse interno razvite in nabavljene programske opreme.
- 22.3. Postopek izdaje kode:
- a. dobavitelj IKT rešitev si bo prizadeval za neprestano izboljševanje izbrane metodologije razvoja programske opreme;

- b. dobavitelj IKT rešitev mora imeti v Pravilnikih določene postopke upravljanja s spremembami/različicami za načrtovane nadgradnje programske opreme, iz katerih izhaja, da so izdaje načrtovane, vodene, testirane, odobrene in ustrezno sporočene in da bo DARS vnaprej obveščen o načrtovanih spremembah;
- c. cikli upravljanja sprememb/različic se začnejo z definiranjem zahtev. Povratne informacije in potrebe DARSa se morajo ustrezno upoštevati pri zahtevah načrtovanih izdaj;
- d. regresijsko testiranje mora biti izvedeno med vsakim ciklom izdaje. Testiranje mora biti izvedeno na različnih nivojih (npr. enota, integracija in sistem, uporabnik). Uporabniško testiranje mora temeljiti na formalnih načrtih testiranja, ki jih izvedejo osebe, ki so neodvisne od oseb, ki so oblikovale in razvijale sistem;
- e. formalna odobritev mora biti del vsake faze življenjskega cikla razvoja (zahteve, oblikovanje, testiranje, odobritev uporabnika, zagon produkcije ipd.). Pri pridobivanju odobritev mora biti jasno, kdo je dal odobritev, datum odobritve in predmet odobritve;
- f. različice in popravki morajo biti opremljeni z zadostnimi navodili za namestitev in uporabo. To velja za tiste rešitve, kjer je predvideno, da DARS različico ali popravek namesti sam, kot tudi, kadar je DARS obveščen o spremembi, ki jo je Dobavitelj IKT rešitev namestil v DARS-ovo okolje;
- g. zasnova rešitev mora biti formalno oblikovana tako, da se lažje prenesejo zahteve v programsko kodo.

#### 22.4. Vmesne spremembe in odprava napak:

- a. v Pravilnikih mora biti definiran postopek za implementacijo nujnih sprememb za odpravo napak, ki zagotavlja, da so te spremembe izvedene pravočasno in kontrolirano;
- b. v Pravilnikih mora biti definiran postopek za sporočanje ugotovljenih težav ali napak DARS-u;
- c. spremembe zaradi odprave napak morajo biti formalno testirane in dokumentirane ter odobrene. Soglasje mora podati druga oseba, kot oseba, ki je spremembo naredila.

### **23. člen** **(kontaktna oseba)**

#### 23.1. Kontaktni osebi po tej pogodbi sta:

- na strani DARSa: skrbnik sistema SUVI in SUNP (CISO);
- na strani Dobavitelja IKT rešitev odgovorna oseba: skrbnik sistema SUVI in SUNP (CISO);

Imena in kontakti se izmenjajo po podpisu pogodbe prek elektronskega naslova nasprotne stranke.

#### 23.2. Za morebitno spremembo kontaktne osebe zadostuje, da se spremembo sporoči na elektronski naslov nasprotne stranke, pri čemer za spremembo zadostuje samo obvestilo in se ne zahteva spremembe pogodbe. Kontaktni osebi lahko samostojno zastopata svojo stranko samo glede izvajanja pogodbe.

#### 23.3. Če ta pogodba zahteva pisno komunikacijo, je ta pogoj izpolnjen, če se uporabi elektronsko pošto kontaktnih oseb. Elektronska pošta se šteje za vročeno, ko jo prejemnik prejme, če prejemnikov sistem ne omogoča prejema elektronske pošte ali potrčila prejema elektronske pošte, pa se elektronska pošta šteje za vročeno, ko jo pošiljatelj pošlje.

## **24. člen**

### **(poslovna skrivnost)**

- 24.1. Pogodbeni stranki se zavezujeta, da bosta vse zaupne informacije po tej pogodbi varovali kot poslovno skrivnost in jih brez predhodne pisne privolitve druge stranke ne bosta posredovali, razkrili ali na drug način naredili dostopne tretjim osebam.
- 24.2. Za zaupne informacije po tej pogodbi se štejejo ta pogodba, vsebina te pogodbe ter vsa dokumentacija v zvezi z opravljanjem storitev po tej pogodbi. Pogodbeni stranki se zavezujeta varovati tudi vse poslovne skrivnosti, osebne podatke in druge zaupne informacije nasprotne stranke, s katerimi se seznani zaradi ali v zvezi z izvajanjem te pogodbe, in sicer ne glede na nosilec, na katerem so informacije vsebovane oziroma način, na katerega so bile zaupne informacije pridobljene.
- 24.3. Pogodbeni stranki soglašata, da bosta zagotavljali zaupnost zaupnih informacij in jih bosta uporabili le za namene te pogodbe. Nadalje pogodbeni stranki soglašata, da ne bosta razkrili zaupnih informacij nikomur, razen:
- matični družbi, odvisnim, pridruženim ali drugače skupaj obvladovanim družbam (v nadaljevanju: povezane družbe) ter
  - tistim svojim zaposlenim ali sodelavcem ter zaposlenim in sodelavcem v povezanih družbah, ki so zadalženi za pregled teh informacij in ki informacije potrebujejo za svoje delo.
- 24.4. Vsaka pogodbeni stranka se zavezuje zaupne informacije posredovati zgolj osebam, ki te informacije potrebujejo za izvajanje te pogodbe v imenu in za račun vsake pogodbene stranke, in sicer le v obsegu, ki je za to nujno potreben.
- 24.5. Vsaka pogodbeni stranka za kršitve varstva poslovnih skrivnosti in zaupnih informacij s strani oseb, ki delujejo v njenem imenu in za njen račun odgovarja kot za lastno kršitev.
- 24.6. Ne glede na navedeno pa lahko obe stranki razkrijeta samo dejstvo, da sta to pogodbo sklenili.
- 24.7. Poslovne skrivnosti oziroma zaupnih informacij ne predstavljajo naslednje informacije:
- informacije, ki jih pogodbeni stranka že poseduje, še preden jih je prejela od druge pogodbene stranke;
  - informacije, ki so bile ali postanejo javne iz drugega razloga, kot je kršenje tega dogovora;
  - informacije iz te pogodbe oziroma v zvezi s to pogodbo, ki v skladu z veljavno zakonodajo štejejo za informacije javnega značaja vsaj ene od pogodbenih strank in jih je ta pogodbeni stranka dolžna javno razkriti;
  - informacije, ki jih stranka razkrije na zahtevo pristojnega sodišča ali drugega državnega organa ali v povezavi s postopki pred temi organi;
  - informacije, ki jih stranka na podlagi pismenega pooblastila druge stranke lahko posreduje tretji osebi;
  - informacije, ki jih stranka prejme od tretje osebe brez podobnih omejitev in brez kršenja te pogodbe.
- 24.8. Pogodbeni stranka, ki krši določbe tega člena pogodbe, je dolžna drugi stranki plačati pogodbeno kazen v znesku 20.000 EUR. Če škoda zaradi razkritja zaupnih informacij presega pogodbeno kazen, je pogodbeni stranka, ki je zaupne informacije razkrila dolžna plačati razliko do popolne odškodnine.

24.9. Obveznosti iz tega člena ostanejo v veljavi tudi po prenehanju veljavnosti te pogodbe.

## **25. člen (osebni podatki)**

25.1. Pogodbeni stranki sta soglasni, da bosta v primeru obdelave osebnih podatkov sklenili ustrezno pogodbo, tako kot to predvidevajo predpisi, ki urejajo varstvo osebnih podatkov. Predlog osnutka navedene pogodbe bo pripravil DARS.

25.2. Obveznosti iz tega člena ostanejo v veljavi tudi po prenehanju veljavnosti te pogodbe.

## **26. člen (trajanje in odstop od pogodbe)**

26.1. Pogodba se sklepa za nedoločen čas, vendar najmanj tri leta.

26.2. Po preteku treh let lahko stranki pogodbo odpovesta z dvomesečnim odpovednim rokom.

26.3. Če Dobavitelj IKT rešitev ob podpisu pogodbe ne izpolnjuje obveznosti iz te pogodbe, jih mora izpolniti v roku 90 dni od podpisa pogodbe in o tem nemudoma obvestiti DARS.

26.4. Če Dobavitelj IKT rešitev po podpisu pogodbe ne izpolnjuje več zahtev iz te pogodbe, DARS pozove na odpravo teh kršitev, v roku, ki ne sme biti krajši od 30 dni. Če predmetne kršitve niso odpravljene v dogovorjenem roku, lahko DARS od Dobavitelja IKT rešitev zahteva plačilo pogodbene kazni v znesku do 20.000 EUR, ki jo je Dobavitelj IKT rešitev dolžan plačati.

26.5. Ne glede na navedeno (tudi pred potekom treh let) pa pogodbi zvesta stranka lahko odstopi od pogodbe brez odpovednega roka, če druga pogodbeni stranka bistveno krši določila te pogodbe. Kot bistvena kršitev pogodbe se šteje takšna kršitev, ki bistveno in dalj časa vpliva na možnost izvajanja obveznosti po tej pogodbi.

26.6. V primeru prenehanja te pogodbe iz kakršnegakoli razloga ostanejo v veljavi vse pravice in obveznosti pogodbenih strank, pridobljene ali nastale v času veljavnosti te pogodbe, v kolikor ta pogodba ne določa drugače. Določba tega člena te pogodbe ne posega v nobene druge pravice, ki bi jih pogodbeni stranka imela na podlagi veljavnih predpisov, v kolikor ta pogodba izrecno ne določa drugače.

## 27. člen (končne določbe)

- 27.1. Spremembe in dopolnitve te pogodbe so veljavne, če so sklenjene v obliki pisnega aneksa k tej pogodbi, ki ga podpišeta obe pogodbeni stranki.
- 27.2. Vsaka stranka ima pravico prenesti ali odstopiti to pogodbo in/ali katerokoli pravico in obveznost po tej pogodbi ali listin sklenjenih oz. izdanih v zvezi z njo na tretjega ob pogoju, da pridobi predhodno pisno soglasje druge stranke.
- 27.3. V primeru, da se katera koli določba te pogodbe ugotovi za nično, neveljavno ali neizvršljivo, to ne vpliva na ostale določbe te pogodbe. Pri tem sta pogodbeni stranki sporazumni, da se v tem primeru nična, neveljavna in neizvršljiva določba nadomesti z drugo določbo, veljavno po obliki in vsebini, in s katero se na pravno dopusten način doseže enak ali podoben namen.
- 27.4. Morebitne spore v zvezi z izvajanjem Pogodbe bosta pogodbeni stranki skušali rešiti sporazumno. Če spornega vprašanja ne bo možno rešiti sporazumno, lahko vsaka pogodbeni stranka sproži spor pri stvarno pristojnem sodišču v Ljubljani.
- 27.5. Pogodba je sklenjena z dnem podpisa pogodbenih strank.
- 27.6. Pogodba je sestavljena v dveh vsebinsko enakih izvornikih, od katerih vsaka pogodbeni stranka prejme en izvod.

Ljubljana, dne:	Ljubljana, dne:
Dobavitelj IKT rešitev:	DARS:
	DARS d.d., Ljubljana
Predsednik uprave	Predsednik uprave:  Mag. Andrej Ribič
Član uprave	Član uprave  mag. David Skornšek