

Naziv podjetja:
Naslov in kraj:
Davčna številka:
(v nadaljevanju upravljavec)

in

Naziv podjetja: A1 Informatika d.o.o.
Naslov in kraj: Polje, Cesta XLVI 1, 1260 Ljubljana-Polje
Davčna številka: 88334244
(v nadaljevanju obdelovalec)

sklepata

POGODBO o obdelavi in varovanju osebnih podatkov

1. člen (uvodne določbe in pojmi)

(1) Pogodbeni stranki uvodoma ugotavljata:

- da imata sklenjeno pogodbo, na podlagi katere obdelovalec za upravljavca izvaja dogovorjene storitve;
- da predmetno pogodbo sklepata zaradi ureditve pogodbene obdelave osebnih podatkov in določitve pravic in obveznosti pogodbenih strank v zvezi z obdelavo osebnih podatkov pri upravljavcu, kot jih določajo 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 (v nadaljevanju: Splošna uredba o varstvu podatkov ali Uredba), Zakon o varstvu osebnih podatkov (ZVOP-2) ter drugi vsakokrat veljavni predpisi s področja varstva osebnih podatkov;
- da obdelovalec podatkov zagotavlja zadostna jamstva o tem, da bo izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave z relevantnimi predpisi o varovanju osebnih podatkov.

V tej pogodbi uporabljeni pojmi imajo naslednji pomen:

Osebni podatek je katera koli informacija v zvezi z določenim ali določljivim posameznikom, ki se obdeluje v okviru storitev po tej pogodbi.

Posebni osebni podatki so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

Zbirka osebnih podatkov je vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi. Obdelava osebnih podatkov je vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.

Upravljavec osebnih podatkov je fizična ali pravna oseba, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov. V primeru te pogodbe je upravljavec osebnih podatkov upravljavec po tej pogodbi.

Obdelovalec osebnih podatkov je obdelovalec po tej pogodbi, ki obdeluje osebne podatke v imenu in za račun upravljavca osebnih podatkov.

Podobdelovalec je pravna ali fizična oseba, ki ji obdelovalec po tej pogodbi prenese v izvajanje določene naloge, ki vključujejo obdelovanje osebnih podatkov po tej pogodbi.

Tretja država je država, ki ni država članica Evropske unije.

2. člen

(predmet pogodbe)

(1) Predmet te pogodbe je ureditev medsebojnih razmerij za obdelavo osebnih podatkov pri upravljavcu zaradi varovanja pravic posameznikov, katerih osebni podatki se obdelujejo pri izvajanju dejavnosti upravljavca in jih zanj po njegovem naročilu obdeluje pogodbeni obdelovalec. Upravljavec osebnih podatkov bo obdelovalcu iz svojih evidenc posredoval oziroma omogočil dostop do osebnih podatkov, ki jih obdelovalec potrebuje za izvajanje storitev za upravljavca. Storitve obdelovalca obsegajo namestitve, vzdrževanje, posodabljanje in podporo programskega paketa Optima Prevent (moduli VZD, PV, HRM, CRM, ERP ter portala za stranke in za izvajalce medicine dela) ter obdelavo osebnih podatkov, ki se izvaja v okviru teh storitev.

(2) Obdelovalec osebnih podatkov bo te podatke sprejel in jih obdeloval zgolj za namen izvajanja pogodbenih storitev za upravljavca, skladno z dokumentiranimi navodili upravljavca ter v obsegu in na način, določen v tej pogodbi.

3. člen

(prenos podatkov)

(1) Upravljavec bo pogodbenemu obdelovalcu z namenom izvajanja pogodbene obdelave omogočil dostop oziroma posredoval osebne podatke iz evidenc osebnih podatkov, kot so razvidne iz preglednice, ki je priloga št. 1 te pogodbe.

4. člen

(namen obdelave)

(1) Upravljavec določa namen obdelave osebnih podatkov. Obdelovalec sme osebne podatke, ki jih prejme od upravljavca, obdelovati zgolj v obsegu, kot je določen v prilogi 1 te pogodbe, in zgolj za izvajanje s pogodbo določenih storitev za upravljavca in v okviru svoje dejavnosti. Obdelovalec sme osebne podatke obdelovati za drug namen le, če tako določa zakon ali predpis Evropske unije, ki je neposredno veljaven na območju Republike Slovenije (v nadaljevanju: predpis EU).

(2) Obdelovalec zagotavlja, da je registriran za opravljanje dejavnosti iz prvega odstavka tega člena.

5. člen

(obveznosti obdelovalca)

(1) Obdelovalec se za izvajanje obveznosti po tej pogodbi zavezuje:

1. da osebnih podatkov ne bo uporabil oz. obdeloval za noben drug namen, kot za izvajanje storitev na podlagi pogodbe med upravljavcem in obdelovalcem, razen za izvajanje obveznosti na podlagi zakona ali predpisa EU;
2. ves čas sodelovati z upravljavcem za izvajanje obveznosti skladno s Splošno uredbo o varstvu podatkov in mu posredovati vse podatke za zagotavljanje pravic posameznikov, katerih osebni podatki se obdelujejo;
3. zagotavljati upravljavcu vse informacije in podporo pri obravnavi zahtev posameznikov ali zaradi izvajanja nadzora nadzornih organov ves čas veljavnosti pogodbe in tudi po izteku pogodbe o izvajanju storitev za upravljavca;
4. obveščati upravljavca o statusnih ali drugih spremembah pri obdelovalcu, ki bi lahko vplivale na izvajanje pogodbenih obveznosti;
5. upravljavcu zagotoviti vse potrebne informacije, ki dokazujejo izpolnjevanje vseh njegovih obveznosti ter omogočiti preverjanja, vključno z izvajanjem revizij poslovanja, ki jih izvede upravljavec ali z njegove strani pooblaščen oseba, podjetje ali drug organ ter sodelovati pri njihovi izvedbi;
6. brez odlašanja upravljavca obveščati o vseh primerih, ko po njegovem mnenju navodilo upravljavca lahko pomeni kršitev določil uredbe ali zakona, ki ureja varovanje osebnih podatkov;
7. po izpolnitvi pogodbenih obveznosti med upravljavcem in obdelovalcem ali v primeru spora ali v primeru prenehanja sodelovanja med pogodbenima strankama iz kateregakoli razloga, brez odlašanja po predhodnem pisnem navodilu posredovati upravljavcu vse osebne podatke na ustreznem nosilcu podatkov in v obliki, da jih bo upravljavec lahko uporabil za nadaljnje obdelovanje ali posredovanje drugemu obdelovalcu, vse morebitne varnostne ali druge kopije osebnih podatkov pa bo izbrisal. Drugače bo ravnal le na podlagi pisnih navodil upravljavca ali zaradi izpolnjevanja obveznosti na podlagi veljavnih predpisov države ali Evropske unije, ki ga zavezujejo;
8. pravočasno obveščati upravljavca, v kolikor bo menil, da je določeno navodilo iz pogodbe ali dogovora ali na njuni podlagi v nasprotju z določbami zakona, ki ureja varstvo osebnih podatkov;

9. v primeru zavezanosti upravljavca k odobrenemu kodeksu ravnanja upoštevati določila tega kodeksa;

6. člen (obveznosti upravljavca)

(1) Upravljavec je odgovoren za ustrezno pravno podlago za pridobivanje in obdelavo osebnih podatkov, ki jih posreduje obdelovalcu.

(2) Upravljavec se prav tako zavezuje obveščati obdelovalca o posebnostih in obveznostih obdelovalca za zagotavljanje pogodbenih obveznosti ter o morebitnih znanih tveganjih glede zagotavljanja pravic posameznikom, katerih osebni podatki se obdelujejo.

7. člen (varovanje podatkov)

(1) Pogodbeni stranki se zavezujeta, da bosta sodelovali pri zagotavljanju ustreznih organizacijskih in tehničnih ukrepov za varovanje osebnih podatkov in odpravljanju ali zmanjševanju tveganj povezanih z varnostjo osebnih podatkov.

(2) Pogodbeni stranki se zavezujeta, da bosta pri izvajanju te pogodbe ves čas zagotavljali ustrezno varovanje osebnih podatkov, ne glede na to ali se bosta z osebnimi podatki seznanili pri neposrednem opravljanju storitev na lokaciji upravljavca ali pogodbenega obdelovalca, pri nadzoru izvajanja določil te pogodbe, preko pisne dokumentacije ali na kakršenkoli drug način. Obdelovalec se zavezuje, da bo pri tem upošteval določila predpisov s področja varstva osebnih podatkov.

(3) Obdelovalec se posebej zavezuje:

1. s prejetimi osebnimi podatki ravnati skrbno in skladno z določili Splošne uredbe o varstvu podatkov in zakona, ki določajo standarde varovanja osebnih podatkov tako, da bo zagotavljal ustrezne organizacijske in tehnične varnostne ukrepe za varno pridobivanje, obdelavo in pošiljanje osebnih podatkov;
2. zagotoviti, da bodo pri njem pooblaščen osebe za obdelavo osebnih podatkov, ki so predmet te pogodbe, ves čas obdelovanja podatkov in tudi po prenehanju obdelovanja, zavezane k varovanju zaupnosti podatkov;
3. zagotavljati spremljanje varnosti osebnih podatkov in v primeru ugotovljenih razlogov za povečano tveganje za varnost osebnih podatkov ali v primeru kršitve takoj o tem obveščati upravljavca in izvesti vse potrebne ukrepe za odpravo ali zmanjšanje škode in nastalih tveganj na najmanjšo možno mero;
4. v primeru nastanka kršitve varnosti osebnih podatkov (npr. uničenje podatkov, vdor v informacijski sistem ali v prostore obdelovalca, nepooblaščen dostop, itd.) o tem nemudoma oziroma še isti dan, obveščati upravljavca ter izvesti vse možne ukrepe za prenehanje kršitve in odpravo škodljivih posledic. Obdelovalec mora ves čas sodelovati z upravljavcem z namenom odprave ali zmanjšanja posledic kršitve, ugotavljanja morebitne škode, izvedbe zakonskih obveznosti glede obveščanja nadzornega organa in posameznikov ter izvajanja navodil nadzornega organa;
5. da bo osebne podatke varoval skladno z ustreznimi tehničnimi in organizacijskimi ukrepi, navedenimi v 8. členu te pogodbe.

8. člen (ukrepi za varovanje)

(1) Obdelovalec se zavezuje varnost obdelave zagotoviti tako, da se:

1. varujejo prostori v katerih se nahajajo nosilci osebnih podatkov, oprema in sistemska programska oprema, vključno z vhodno-izhodnimi enotami, tako da se onemogoči dostop nepooblaščenim osebam do osebnih podatkov;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki, predvsem z uporabo gesel za dostop s strani pooblaščenih oseb;
3. zagotavlja zanesljiv in učinkovit način hrambe podatkov ter uničenja in izbrisa osebnih podatkov po navodilu upravljavca;
4. pri prenosu osebnih podatkov zagotavlja varnost obdelave, še zlasti pri prenosu posebnih vrst osebnih podatkov pa se zagotavljajo dodatni zaščitni ukrepi z uporabo kriptografskih metod, elektronskega podpisa ali drugega ukrepa, s katerim se zagotavlja nečitljivost oziroma neprepoznavnost vsebine v primeru nepooblaščenega dostopa;
5. pri obdelavi osebnih podatkov s temi seznanijo le s strani obdelovalca pooblaščen osebe, ki dostop potrebujejo za izvajanje pogodbeno dogovorjenih nalog obdelovalca in za izvajanje nadzora ter jih obdelovalec določi z internimi akti;

6. zagotavlja postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti varnostnih ukrepov.

9. člen **(varnostne tehnologije)**

- (1) Dostop do programa prek interneta – HTTPS / SSL certifikat, navidezno zasebno omrežje (VPN) na zahtevo, namestitev za požarnim zidom (NAT);
- (2) Zaščita pred pregledovanjem ranljivosti, napadi z ugibanjem gesel (brute force) in ribarjenjem (phishing) – obratni HTTPS proxy z aktivnim blokiranjem;
- (3) Prijava uporabnika v program – obvezno geslo z najmanj 8 znaki in zahtevano kompleksnostjo, šifriran prenos podatkov (SSL/TLS);
- (4) Šifriranje podatkov – šifriranje podatkovne baze in šifriranje datotečnega sistema na ravni jedra operacijskega sistema;
- (5) Redno posodabljanje sistema (Apache2, PHP, operacijski sistem) – mesečno, operacijski sistem v različici LTS;
- (6) Varnostne kopije – na zahtevo upravljavca;
- (7) Fizično varovanje – zagotavlja upravljavec. Podatkov ni mogoče brati neposredno z diska (šifriranje datotečnega sistema).
- (8) Revizijska sled (audit log) – beleženje dostopov do programa (uporabniško ime, IP naslov) in zgodovine sprememb zapisov;
- (9) Digitalno podpisovanje dokumentov – avtomatsko digitalno podpisovanje izdanih PDF dokumentov (digitalno potrdilo P12);
- (10) Nadzor dostopov – dostop do podatkov imajo samo pooblaščen osebe obdelovalca, z ločevanjem uporabnikov po vlogah in ločitvijo podatkov posameznih strank.

10. člen **(vključitev podobdelovalcev)**

- (1) Obdelovalec se zavezuje, da brez predhodnega pisnega dovoljenja upravljavca v obdelavo ne bo vključil drugih pogodbenih podobdelovalcev (podizvajalcev, zunanjih izvajalcev), pri čemer ima upravljavec pravico zavrniti dovoljenje za vključitev drugega obdelovalca, če to po oceni upravljavca lahko vpliva na povečano tveganje za varnost osebnih podatkov. Pisno dovoljenje upravljavca je lahko tudi splošno za več primerov.
- (2) Podobdelovalca zavezujejo enake dolžnosti varstva osebnih podatkov, kot obdelovalca, o čemer ga je pogodbeni obdelovalec dolžan seznanimi. Če drugi obdelovalec ne izpolnjuje vseh svojih obveznosti glede varstva osebnih podatkov, za izpolnjevanje obveznosti drugega obdelovalca v odnosu do upravljavca v celoti odgovarja obdelovalec.

11. člen **(prenos podatkov v 3. države)**

- (1) Obdelovalec ne sme brez predhodnega pisnega dovoljenja posredovati ali hraniti ali drugače obdelovati osebnih podatkov upravljavca izven EU območja (v tretje države) ali posredovati podatke mednarodni organizaciji, razen če to od upravljavca zahteva pravo Evropske unije ali pravo države članice, ki velja za pogodbenega obdelovalca. V slednjem primeru mora pogodbeni obdelovalec pred začetkom izvajanja pogodbene obdelave osebnih podatkov obvestiti upravljavca osebnih podatkov, razen če zadevno pravo prepoveduje tako obvestilo na podlagi pomembnih razlogov v javnem interesu.
- (2) Upravljavec lahko zavrne izdajo pisnega dovoljenja obdelovalcu za prenos podatkov v tretje države ali mednarodno organizacijo, če mu obdelovalec ne uspe izkazati ustrezno raven varstva podatkov na enakovredni ravni, kot ga zagotavlja Splošna uredba o varstvu podatkov in drugi predpisi v Republiki Sloveniji.

12. člen **(odgovornost)**

- (1) Obdelovalec je v primeru kršitve te pogodbe ali kršitve pravic posameznikov zaradi obdelave njihovih osebnih podatkov, ki jih prejme od upravljavca, upravljavcu odškodninsko odgovoren za vso materialno in nematerialno škodo, ki bi morebiti nastala upravljavcu ali za katero bi bil lahko odgovoren upravljavec, če so razlogi za nastanek škode na strani obdelovalca ali pogodbenega podobdelovalca.
- (2) Če bi bila ugotovljena materialna odgovornost upravljavca zaradi kršitve varstva osebnih podatkov iz razloga na strani obdelovalca, je obdelovalec dolžan upravljavcu povrniti vso škodo, ki bi mu s tem nastala.

(3) Upravljavec sme brez odpovednega roka odstopiti od pogodbe z obdelovalcem za izvajanje storitev in od te pogodbe v primeru večjih kršitev varstva osebnih podatkov ali v primeru ponavljajočih se kršitev (več kot 1x), ki jih obdelovalec ne odpravi na način in v roku, kot to pisno zahteva upravljavec ali nadzorni organ. Upravljavec ima pravico odločiti, v katerih primerih gre za večjo ali manjšo kršitev. Za večjo kršitev gre v primeru s strani nadzornega organa ugotovljene kršitve varovanja osebnih podatkov ali kršitve pravic posameznikov na podlagi Splošne uredbe o varstvu podatkov.

13. člen (reševanje sporov)

(1) Stranki bosta spore reševali sporazumno. Če to ne bo mogoče, je za reševanje sporov pristojno sodišče, ki bi bilo pristojno za reševanje sporov iz pogodbe o izvajanju storitev med pogodbenima strankama. Če to ni določeno, je za reševanje sporov pristojno sodišče na območju katerega ima upravljavec svoj sedež.

14. člen (veljavnost)

(1) Pogodba začne veljati z dnem podpisa obeh pogodbenih strank in velja za čas trajanja pogodbe o izvajanju storitev med pogodbenima strankama.

15. člen (končne določbe)

(1) Ta pogodba je sestavljena v dveh enakih izvodih, od katerih vsaka pogodbeni stranka prejme po en izvod.

V Ljubljana dne: _____

Upravljavec:

Obdelovalec:
A1 Informatika d.o.o.
Direktor: Ivan Primorac

PRILOGA 1:**Preglednica obdelav osebnih podatkov**

ZAP. ŠT.	ZBIRKA OSEBNIH PODATKOV	KATEGORIJE in VRSTE OSEBNIH PODATKOV, DO KATERIH IMA POGODBENI OBDELOVALEC DOSTOP	DOVOLJENA OBDELAVA OSEBNIH PODATKOV
1.	Evidenca podatkov iz nameščenega programa Optima Prevent na strežniku pri upravljavcu podatkov:	Dostop obsega podatke, ki se nahajajo v programskem paketu Optima Prevent (v nadaljevanju: program), nameščenem na strežniku pri upravljavcu, vključno s podatki, ki jih v program vnesejo upravljavec, njegovi pooblašteni uporabniki ali njegove stranke. Do podatkov se dostopa izključno zaradi zagotavljanja podpore uporabnikom, odpravljanja tehničnih težav ter posodabljanja in vzdrževanja programa, ali na izrecno zahtevo upravljavca. Dostop do podatkov (vsebine) vključuje osebne podatke, ki jih upravljavec ali njegovi uporabniki prenesejo na lokalni strežnik oziroma v program. To vključuje tudi vse podatke, ki jih v program naložijo stranke upravljavca. Do podatkov se dostopa tudi v primeru težav z delovanjem programa ali na zahtevo upravljavca. Dostop do podatkov: • Datoteke • Podatkovne baze • Dnevniški zapisi Kategorije posameznikov: Zaposleni upravljavca in zaposleni njegovih strank; Uporabniki programa (pooblašcene osebe upravljavca); Pogodbeni partnerji upravljavca in njihovi zaposleni; Druge osebe, katerih podatke v program vnese upravljavec (npr. izvajalci medicine dela in zdravniki, kandidati za zaposlitev). Vrste osebnih podatkov: Identifikacijski in kontaktni podatki: ime in priimek, datum rojstva, EMŠO, spol, naslov, e-pošta, telefon; Podatki o zaposlitvi: delovno mesto, izobrazba, delovna doba, datum zaposlitve, podatki o delovnem mestu in tveganjih; Podatki o usposabljanjih, preverjanjih znanja in izdanih potrdilih; Podatki o delovni opremi, osebni varovalni opremi (OVO) in pregledih; Posebne vrste osebnih podatkov – podatki v zvezi z zdravjem (9. člen Uredbe): podatki o zdravniških pregledih, oceni zmožnosti za delo, omejitvah in napotitvah zdravnika, podatki o delovnih nezgodah in poškodbah, ocene telesnih obremenitev (RASSL) in ocene tveganj kemičnih snovi (RASSC); Podatki o pravnih osebah – pogodbenih partnerjih: naziv, naslov, kontaktni podatki, odgovorna oseba; Podatki o uporabnikih programa: uporabniško ime, e-pošta, dodeljene pravice dostopa ter zapisi o dostopih (uporabniško ime, IP naslov, čas). Rok hrambe: podatki se obdelujejo ves čas trajanja pogodbe o izvajanju storitev; po prenehanju pogodbe se podatki skladno s 7. točko 5. člena te pogodbe vrnejo upravljavcu oziroma izbrišejo, razen če zakon določa drugače. Podobdelovalci: obdelovalec pri izvajanju storitev ne vključuje podobdelovalcev. Vsako morebitno vključitev podobdelovalca bo izvedel le na podlagi predhodnega pisnega soglasja upravljavca (10. člen te pogodbe). Podatki se shranjujejo v varnostne kopije, ki so v domeni upravljavca; obdelovalec do njih dostopa le na zahtevo upravljavca v primeru odpravljanja tehničnih napak oziroma ponovne vzpostavitve strežnika. Na strežniku se beležijo dostopi do programa (uporabniško ime, IP naslov).	zbiranje, beleženje, urejanje, shranjevanje, vpogled, uporaba, razvrščanje, povezovanje, razkritje s posredovanjem, omejevanje, anonimiziranje, izbris, uničenje, prenos na zahtevo upravljavca.