TEHNISKĀ SPECIFIKĀCIJA
Aklātajam konkursam
"Mākoņrisinājumā balstīta programmatūras izstrāde, kas ietver datu bāzi, analīzes un citu funkcionalitāti"
(identifikācijas numurs LMT/BRAVO/2026-13**)**

1. Šī specifikācija apraksta izstrādājamās programmatūras produktu, kura mērķis ir ievākt medicīniskās informācijas un sensoru ierīču datus, veikt to validāciju, saglabāšanu, organizēšanu, kā arī apstrādi kontekstā ar citiem datiem (lineāri un ar MI algoritmiem) un piekļuves organizēšanu ārējām sistēmām, nodrošinot mākoņrisinājumos balstītu platformu (izstrādāt jaunu platformu vai pielāgot esošu platformu) kā pakalpojumu medicīnisko pētījumu veikšanai saistībā ar izelpas analīzi.
2. Pretendents iesniedz Tehnisko piedāvājumu atbilstoši AS "LabMedTech" atklātā konkursā izsludinātā iepirkuma "Mākoņrisinājumā balstīta programmatūras izstrāde, kas ietver datu bāzi, analīzes un citu funkcionalitāti" (identifikācijas numurs LMT/BRAVO/2026-13) Nolikuma un Tehniskās specifikācijas prasībām, Tehniskajā piedāvājumā detalizēti aprakstot visu prasību izpildi, nodrošināšanu un realizāciju, ietverot visas ar izstrādi, piegādi, un garantijas tehnisko atbalstu saistītās darbības, kuru rezultātā tiks nodrošināta Iepirkuma priekšmeta realizācija. Aprakstam jābūt tik detalizētam, lai Pasūtītājs gūtu pārliecību par Pretendenta spējām izpildīt visas iepirkuma Nolikumā un Tehniskajā specifikācijā izvirzītās prasības.

TEHNISKĀS PRASĪBAS / SPECIFIKĀCIJA:

Izstrāde/ Piegāde/Garantijas tehniskais atbalsts*	**Skaits**	**Vienība**	**Prasības**
1. Bāzes platforma mākoņrisinājumā medicīnisko pētījumu veikšanai	1	Platforma	● **Atrašanās vieta un atbilstība:** Platformai jāatrodas Eiropas Savienībā (ES) un tai stingri jāatbilst VDAR (GDPR) un HIPAA datu aizsardzības prasībām. ● **Datu apstrāde un veiktspēja:** Platformai jāspēj saņemt datus, veikt reāllaika vai gandrīz reāllaika datu analīzi, kvalitātes kontroli ar anomāliju noteikšanu. Tai jānodrošina novirzes kompensācija, signāla datu normalizācija atbilstoši vides izmaiņām, kā arī vairāku instrumentu harmonizēšana. ● **Arhitektūra:** Risinājumam jābūt ieviestam kā vairāku nomnieku (multi-tenant) tīmekļa lietojumprogrammai, kas balstīta mikropakalpojumu arhitektūrā un konteineru orķestrēšanā. Visiem pakalpojumiem jābūt konteinerizētiem un glabātiem centralizētā konteineru reģistrā. ● **Datu glabāšana:** Galvenie transakciju un konfigurācijas dati jāglabā pārvaldītā relāciju datubāzē. Liela apjoma sensoru un žurnālu dati jāglabā mērogojamā objektu krātuvē, bet laikrindu vaicājumiem jāizmanto specializēta laikrindu datubāze. ● **Drošība un šifrēšana:** Visa datplūsma jāšifrē. Ārējai datplūsmai jāizmanto TLS pārtraukšana slodzes līdzsvarotājā vai API vārtejā. Ilgstoši neizmantotiem datiem (miera stāvoklī) datubāzēs, objektu krātuvēs un pievienotajās glabātuvēs jāizmanto pārvaldīta šifrēšana ar atslēgu pārvaldības sistēmu. ● **Piekļuves kontrole un uzraudzība:** Autentifikācijai un autorizācijai jāizmanto centralizēta identitātes pārvaldības sistēma ar uz lomām balstītu piekļuves kontroli. Platformā jāievieš atbilstoša darbību žurnalēšana, metrikas un sistēmas uzraudzība, izmantojot centralizētus auditēšanas un drošības stāvokļa

			uzraudzības rīkus incidentu un draudu noteikšanai. ● **Pārnesamība:** Platforma jāpadara pieejama klientam pēc projekta pabeigšanas, un tā jāveido tā, lai to varētu izvietot arī Pasūtītāja serverī (kā konteinerizētu risinājumu). Pasūtītājam jāspēj patstāvīgi izmantot datus modeļu apmācībai un pievienot savus *Python* vidē izstrādātus datu apstrādes algoritmus.
1.1. Droša, automatizēta datu apmaiņa	1	Modulis	● **Šifrēšana un drošība:** Jānodrošina datu pārraides funkcionalitāte ar obligātu šifrēšanu tranzītā (vismaz AES-256 un TLS 1.3 standarti) un šifrēšanu miera stāvoklī. ● **Datu apmaiņas mehānismi:** Modulim jāatver RESTful vai līdzvērtīgi saskarnes (API) galapunkti. Jānodrošina uz notikumiem balstītas integrācijas ar asinhronu piegādi un ziņojumu buferizāciju uzticamai atsaistei. RESTful API ir jāļauj elpošanas analīzes instrumentiem augšupielādēt jaunus mērījumu datus. ● **Failu pārsūtīšana:** Drošai failu pārsūtīšanai no medicīnas ierīcēm vai partneriem jāatbalsta standarta protokoli (piemēram, SFTP). ● **Pārvaldība:** API atslēgas, sertifikāti un akreditācijas dati jāglabā drošā noslēpumu pārvaldības (secrets management) sistēmā. Piekļuves kontrole jāintegrē ar API vārteju. Visa piekļuve un konfigurācijas izmaiņas jāreģistrē audita žurnālos un jāsasaista ar automatizētu draudu noteikšanas sistēmu atbilstoši veselības aprūpes un VDAR prasībām. Piegādātājam jānodrošina incidentu reaģēšanas plāni saskaņā ar VDAR un HIPAA.
1.2. Datu priekšapstrāde, mērogošana, transformācija, datu bāze	1	Modulis	● **Signālu apstrādes loģika:** Modulim jāīsteno laikrindu un citu datu tipu priekšapstrāde elpas analīzes instrumentu datu analīzei. Elpas analīzes instrumenta dati satur mērījumu parametrus, palīgdatus (piemēram, vides un instrumenta apstākļus), kā arī sensoru reakcijas datus no vairākiem sensoriem. Signālu apstrādes konveijeram jābūt konfigurējamam un paplašināmam, lai vēlāk varētu pievienot jaunus instrumentus ar mainīgu datu struktūru. Signālu apstrādes konveijeram jāietver mērījumu perioda un izelpas fāzes noteikšana, sensora bāzes līnijas vizualizācija, normalizācija un kalibrēšana (lai kompensētu temperatūras, mitruma un spiediena svārstības, kā arī sensora novecošanos). ● **Kļūdu noteikšana:** Jānodrošina kļūdaina signāla noteikšana (piemēram, troksnis, pārmērīgi lieli maksimumi) un pazīmju iegūšana (delta normalizācija, izelpas raksturīgās pazīmes). ● **Datu konveijeri (Pipelines):** Priekšapstrāde jāīsteno, izmantojot mērogojamus datu transformācijas rīkus, kas darbojas datu ezerā ar centralizētu datu katalogu. ● **Instrumentu kalibrēšanas dati**: jāuzglabā sistēmā un atbilstoši jāintegrē datu plūsmā. Kalibrēšanas dati var ietvert atsauces mērījumus. Jāievieš īpaša kalibrēšanas plūsma, kas no kalibrēšanas mērījumiem iegūst kalibrēšanas parametrus, tādējādi samazinot nobīdes un sensoru novecošanās, savstarpējo traucējumu un ierīču atšķirību ietekmi. ● **Datu glabāšanas formāti:** Sagatavotie un vēsturiskie dati jāglabā objektu krātuvē optimizētos, šifrētos formātos (piemēram, CSV vai JSON). Strukturētiem vaicājumiem jāizmanto relāciju datubāze, bet

			laikrindām – laikrindu datubāze. ● **Datu pārvaldība (Governance):** Datu piekļuve un shēmas evolūcija stingri jāierobežo ar datu pārvaldības slāni, nodrošinot, ka lietotāji redz tikai atļautos datus. Jāievieš automatizēta sensitīvu personas datu atklāšana neapstrādātos un iepriekš apstrādātos slāņos.
1.3. Datu analīze un modeļu izveide	1	Modulis	● **Analītiskā funkcionalitāte:** Modulim jāīsteno matemātiska, statistiska un uz mašīnmācīšanos (ML) balstīta datu analīze (t.sk. neironu tīkli), lai ģenerētu prognozes un noteiktu grupas piederību slimībām. Jānodrošina pazīmju un to ietekmes analīze. ● **Mašīnmācīšanās (ML) platforma:** Modeļu izstrādei jāizmanto vienota, pārvaldīta ML platforma datu izpētei, izstrādei un sadarbībai. Jānodrošina pārvaldīti apmācības procesi, izmantojot iebūvētus algoritmus vai pielāgotus konteinerus. ● **MLOps un pārvaldība:** Jāievieš eksperimentu izsekošana, modeļu versiju pārvaldība (reģistrs), modeļa izskaidrojamības un neobjektivitātes (bias) analīze medicīniskiem mērķiem. Atkārtojamām darbplūsmām jāizmanto automatizēti ML konveijeri. ● **Infrastruktūras uzraudzība:** Visas darbības, atbilstības/kontroles pierādījumi un metrikas automātiski jānovirza uz centralizētu žurnalēšanas un audita sistēmu.
1.4. Modeļa izvietošana izmantošanai pētniekiem un veselības aprūpes personālam	1	Modulis	● **Izvietošanas arhitektūra:** Izstrādātie modeļi jāmitina un jāizmanto mērogojamā vidē, ko pārvalda caur API vārteju. Piekļuvei jābūt saderīgai ar VDAR un HIPAA prasībām. ● **Tīkla drošība un integrācija:** Tīkla piekļuve modeļu galapunktiem jāierobežo ar virtuāliem privātiem tīkliem, drošības grupām un privātām saitēm, nodrošinot drošu savienojumu ar slimnīcu un pētniecības tīkliem. ● **Uzraudzība:** Sistēmai reāllaikā jāseko līdzi darbības rādītājiem (latentums, kļūdu līmenis, caurlaidspēja), kā arī jānosaka datu un modeļa novirzes (drift). Visi API izsaukumi jāreģistrē ar pilnīgu izsekojamību audita žurnālos.
1.5. Saskarne datu pārlūkošanai, pētniecībai	1	Modulis	● **Lietotāja saskarne (UI):** Pētniekiem un ārstiem jānodrošina droša tīmekļa lietojumprogramma, kas pieejama globāli ar zemu latentumu un ir aizsargāta ar tīmekļa lietojumprogrammu ugunsmūri (WAF). ● **Funkcionalitāte:** Saskarnei jānodrošina datu pārlūkošana, pārskatu ģenerēšana, rezultātu vizualizācija un datu apkopošana, balstoties uz grupas piederību un mērījumiem. Jāintegrē biznesa intelekta (BI) vai interaktīvas analītikas paneļi informācijas atveidošanai. ● **Dažādiem lietotāju tipiem ir nepieciešamas dažādas lietotāja saskarnes**: Lietotāju tipi ietver administratorus (kuri var veikt dublēšanu, atjaunināšanu, lietotāju pārvaldību), klīnicistus (ārstus, medmāsas) ar piekļuvi datiem par saviem pacientiem un iespēju augšupielādēt jaunus mērījumus, pētniekus

			ar iespēju piekļūt datu kopām un konfigurēt/ieviest datu analīzes plūsmas. ● **Piekļuve un kontrole:** Autentifikācijai un autorizācijai jāizmanto centralizēts risinājums ar uz lomām un atribūtiem balstītām atļaujām (RBAC/ABAC). Visas lietotāja saskarnes darbības, īpaši datu eksports un piekļuve, jāreģistrē un jāsaglabā audita vajadzībām.
1.6. Platformas modulis pacientu metadatu vākšanai un piekrišanas pārvaldībai	1	Modulis	● **Datu bāze un drošība:** Pacientu metadati un piekrišanas ieraksti jāglabā izolētā datubāzē ar stingru tīkla kontroli un šifrēšanu. ● **Arhitektūra:** Datu ievades un rediģēšanas loģika jāīsteno kā mikropakalpojumi aiz API vārtejas. ● **Privātums un atbilstība:** Visām datu subjekta tiesību darbībām (piekļuve, labošana, dzēšana) un piekrišanas izmaiņām jāizveido nemaināmi auditācijas pieraksti. Sistēmai jānodrošina saskarne, kurā persona dod aktīvu piekrišanu darbībām ar datiem. Visi personas dati visās datu kopās jāuzglabā un jāapstrādā tā, lai nodrošinātu aizsardzību saskaņā ar VDAR un HIPAA ietvariem.
1.7. Platformas pielāgošana darbam ar jaunajiem datu veidiem (GC un MOX integrācija)	1	Atjaunināta platforma	● **Paplašināmība:** Platformai jābūt spējīgai asimilēt papildu datu modalitātes, piemēram, gāzes hromatogrāfijas (GC) un metāla oksīda (MOX) sensoru rādījumus. Jānodrošina GC datu ielasīšana, maksimuma noteikšana un savienojumu saskaņošana. ● **Datu konveijeri:** Jauno datu apstrādes un ielasīšanas loģika jāievieš kā automatizēti datu apstrādes darbi, kas strādā ar objektu krātuvē saglabātajiem datiem un ir pārvaldīti caur centrālo datu katalogu. ● **Lielapjoma analītika:** Laikam piederīgas pazīmes un pīķi jāsaglabā relāciju vai laikrindu datubāzēs. Liela mēroga multimodālas pazīmju kopas jāglabā optimizētā formātā, nodrošinot iespēju veikt ātrdarbīgus SQL vaicājumus, izmantojot analītiskās datu noliktavas vai vaicājumu rīkus. ● **Multimodālā modelēšana:** Lai apvienotu GC iegūtās un MOX sensoru pazīmes, vienmodālajiem un multimodālajiem modeļiem jāizmanto vienots MLOps dzīves cikls (apmācība, eksperimenti, konveijeri un reģistrs) centralizētajā ML platformā. ● **Vizuālā analīze:** Integrētai hromatogrammu, GOS profilu un sensoru nospiedumu vizuālajai analīzei jābūt pieejamai caur API un atveidotai drošos, iegultos informācijas paneļos. Visai piekļuvei abām datu modalitātēm jābūt centralizēti auditējamai un aizsargātai.

Pretendenta vai tā pilnvarotā pārstāvja vārds un uzvārds _____
Amats _____

Šī dokumenta parakstīšanas datums ir pievienotā droša elektroniskā paraksta un tā laika zīmoga datums.
Piedāvājumu (t.sk. šo dokumentu) paraksta pretendenta pārstāvis ar drošu elektronisko parakstu un laika zīmogu.