TEHNISKĀ SPECIFIKĀCIJA
Aklātajam konkursam

"Mākoņrisinājumā balstīta programmatūras izstrāde, kas ietver datu bāzi, analīzes un citu funkcionalitāti"

(identifikācijas numurs LMT/BRAVO/2026-5**)**

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/2026-5) 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**	**Klientu prasības ****
1	Nodrošināt mākoņrisinājumos balstītu platformu (izstrādāt jaunu platformu vai pielāgot esošu platformu) kā pakalpojumu medicīnisko pētījumu veikšanai saistībā ar izelpas analīzi	1	Platforma	Platformai jāatrodas ES un tai jāatbilst citām GDPR (un HIPAA) prasībām. Platformai jāspēj saņemt datus, veikt reāllaika vai gandrīz reāllaika datu analīzi, kvalitātes kontroli ar anomāliju noteikšanu un nodrošināt lietotāja saskarni pētniekiem/ārstiem, lai tie varētu strādāt ar datiem un rezultātiem. Platformai jāievieš atbilstoša darbību žurnalēšana un uzraudzība. Platformai jānodrošina novirzes kompensācija, signāla datu normalizācija atbilstoši vides izmaiņām, kā arī vairāku instrumentu harmonizēšana. Platformai jābūt ieviestai kā mākoņtehnoloģijās balstītai, vairāku nomnieku tīmekļa lietojumprogrammai platformā AWS vai līdzvērtīgā platformā, izmantojot Amazon ECS ar AWS Fargate vai Amazon EKS (vai līdzvērtīgus risinājumus no cita pakalpojumu sniedzēja) konteineru orķestrēšanai, un visiem pakalpojumiem jābūt konteinerizētiem un glabātiem Amazon ECR vai ekvivalentā pakalpojumā. Galvenie transakciju un konfigurācijas dati jāglabā Amazon Aurora PostgreSQL (šifrēti ar AWS KMS), savukārt liela apjoma sensoru un žurnālu dati jāglabā Amazon S3 un, ja nepieciešams izmantot laikrindu vaicājumus, Amazon Timestream vai ekvivalentos risinājumos no citiem piegādātājiem. Visa datplūsma jāšifrē, izmantojot TLS pārtraukšanu lietojumprogrammu slodzes līdzsvarotājā (ALB) vai Amazon (vai līdzvērtīgā) API vārtejā, un ilgstoši neizmantotiem datiem jāizmanto KMS pārvaldīta šifrēšana S3, Aurora (vai ekvivalentos risinājumos) un visās pievienotajās glabātuvēs. Autentifikācijai un autorizācijai jāizmanto Amazon Cognito vai AWS IAM Identity Center vai līdzvērtīgos risinājumos, izmantojot uz lomām balstītu piekļuves kontroli API, kas ir uz āru pieejami, izmantojot API vārteju. Žurnalēšanai un uzraudzībai jāizmanto Amazon

				CloudWatch žurnāli, CloudWatch metrikas/signāli un AWS X-Ray vai ekvivalenti risinājumi, savukārt atbilstība, drošības stāvoklis un auditējamība jānodrošina, izmantojot AWS CloudTrail, AWS Config, AWS Security Hub, Amazon GuardDuty un AWS Audit Manager nepārtrauktai kontrolei un pierādījumu vākšanai (vai līdzvērtīgus risinājumus). Platforma jāpadara pieejama klientam pēc projekta pabeigšanas, un tā jāizvieto arī Pasūtītāja serverī (kā dokerizēts konteiners vai līdzvērtīgs risinājums). Gala platformai jābūt realizētai tā, lai ļautu Pasūtītājam izmantot datus modeļu apmācībai un pievienot savus datu apstrādes un analīzes soļus/algoritmus/metodes, kas izstrādātas Python vidē un tās standarta bibliotēkās Nolikumā noteiktajā termiņā.
1.1	Droša, automatizēta datu apmaiņa	1	Modulis	Nodrošināt datu pārraides funkcionalitāti ar nepieciešamo datu šifrēšanu pārraides laikā (vismaz AES-256 šifrēšana un TLS 1.3), zaudējumiem izturīgu datu pārraidi un uzglabāšanu nepieciešamajos drošības līmeņos mērījumu datiem (ieskaitot pacientu un potenciāli sensitīvus veselības aprūpes datus), instrumentu datiem un kalibrēšanas datiem. Ņemot vērā sistēmā uzglabāto datu raksturu, piegādātājam jānodrošina incidentu reaģēšanas plāni saskaņā ar VDAR/HIPAA. Drošajam datu apmaiņas modulim ir jāatver RESTful galapunkti un uz notikumiem balstītas integrācijas, izmantojot Amazon API Gateway un Amazon EventBridge (vai līdzvērtīgus risinājumus no citiem piegādātājiem), ar asinhronu piegādi un buferizāciju, ko apstrādā Amazon SQS vai Amazon SNS (vai citi risinājumi ar līdzīgu funkcionalitāti), ja nepieciešams atdalīšanai un uzticamībai. Drošai failu pārsūtīšanai (piemēram, no medicīnas ierīcēm vai partneru sistēmām) platformai ir jāizmanto AWS Transfer Family vai līdzvērtīgi risinājumi (SFTP/FTPS/FTP), rakstot tieši S3 segmentos, kas šifrēti ar SSE-KMS atslēgām vai ekvivalentā veidā. Visiem galapunktiem ir jānodrošina TLS tranzītā un uz KMS (vai līdzvērtīgu) balstīta šifrēšana miera stāvoklī, ar akreditācijas datiem, API atslēgām un sertifikātiem, kas tiek glabāti AWS Secrets Manager vai AWS Systems Manager Parameter Store (SecureString) vai ekvivalentā risinājumā. Piekļuves kontrole apmaiņas API jāpārvalda, izmantojot Amazon Cognito vai IAM vai līdzvērtīgus autorizētājus, kas integrēti ar API Gateway, un visa piekļuve, datu pārvietošana un konfigurācijas izmaiņas jāreģistrē, izmantojot AWS CloudTrail, un jāuzrāda AWS Security Hub ar Amazon GuardDuty draudu noteikšanu un papildu izmeklēšanas atbalstu, izmantojot Amazon Detective vai risinājumus ar līdzvērtīgu funkcionalitāti, lai nodrošinātu automatizētas, prasībām atbilstošas incidentu noteikšanas un reaģēšanas darbplūsmas, kas atbilst veselības aprūpes un VDAR prasībām.
1.2	Datu priekšapstrāde, mērogošana, transformācija, datu bāze	1	Modulis	Modulis, kas īsteno laikrindu un citu datu tipu priekšapstrādi elektroniskā deguna sensoru datu analīzei, tostarp: - mērījuma posma un izelpas fāzes noteikšana un sensora bāzes līniju un reakciju vizualizācija,

				- atbilstoša normalizācija un standartizācija/kalibrēšana, lai kompensētu temperatūras, mitruma un spiediena izmaiņu izraisītu nobīdi, sensora novecošanos, tostarp kalibrēšanas statistisko validāciju, - saskaņošana starp dažādiem instrumentiem, - kļūdaina signāla noteikšana (piemēram, pārmērīgi lieli maksimumi, trūkstošs signāls un troksnis), - signāla priekšapstrāde, tostarp pazīmju iegūšana (delta normalizācija attiecībā pret absolūtajām vērtībām, maksimumi un plato, izelpas raksturīgās pazīmes un citas elpošanas signāla īpašības). Priekšapstrādes un transformācijas slānis jāievieš, izmantojot AWS Glue vai ekvivalentu (Python/Spark) un/vai AWS Lambda (vai ekvivalentu) funkcijas, ko pārvalda AWS Step Functions vai Amazon Managed Workflows for Apache Airflow (MWAA), darbojoties datu ezerā, kas izveidots uz Amazon S3, ar metadatiem, ko pārvalda AWS Glue Data Catalog vai ekvivalentiem risinājumiem no citiem piegādātājiem. Sensoru laikrindas un apstrādātās atribūtu kopas jāglabā vai nu Amazon Aurora PostgreSQL (strukturētiem un relāciju vaicājumiem), vai Amazon Timestream (optimizētām laikrindu apstrādēm) vai līdzvērtīgos risinājumos, savukārt sagatavotie un vēsturiskie dati paliek S3 kā šifrēti Parquet vai CSV. Datu piekļuve, shēmas evolūcija un harmonizācijas loģika jāierobežo un jāauditē, izmantojot AWS Lake Formation vai ekvivalentu, nodrošinot, ka dažādi projekti, vietnes un lomas redz tikai atļautos datus. Pakešu un gandrīz reāllaika transformācijas jāuzrauga Amazon CloudWatch vai ekvivalentā, konfigurācijas nobīdes un resursu atbilstība jāizseko AWS Config vai ekvivalentu, un sensitīvu datu atklāšanu neapstrādātos un iepriekš apstrādātos slāņos var atbalstīt Amazon Macie vai ekvivalentu risinājumu, lai atklātu un aizsargātu personas datus.
1.3.	Datu analīze un modeļu izveide	1	Modulis	Modulis, kas īsteno matemātisku, statistisku un uz mašīnmācīšanos balstītu izelpas datu analīzi (neironu tīkli utt.), ģenerējot prognozes rezultātu un nosakot grupas piederību (slimības un citas īpašības), ņemot vērā novirzes kompensāciju un citas izelpas datu īpatnības. Modulim jānodrošina arī pazīmju un to ietekmes uz mērījumiem un kohortām analīze. Analīzes un modeļu izstrādes moduļa izveidei jābalstās uz Amazon SageMaker vai ekvivalentu platformu, izmantojot to kā centrālo vidi datu izpētei, modeļu izstrādei un sadarbībai. Apmācībai jādarbojas kā pārvaldītiem apmācības darbiem, izmantojot iebūvētus algoritmus vai pielāgotus konteinerus, ar ievades datiem, kas iegūti no Amazon S3, Amazon Aurora vai Amazon Redshift vai ekvivalentus risinājumus pēc nepieciešamības. Eksperimentu izsekošana, modeļu versiju pārvaldība un izsekošana jābalsta uz SageMaker Experiments un SageMaker Model Registry, savukārt datu apstrāde un pazīmju inženierijai jāizmanto SageMaker Processing. Modeļa izskaidrojamību un neobjektivitātes analīzi medicīniskiem lietošanas gadījumiem jābalsta uz SageMaker Clarify, un atkārtojamu mašīnmācīšanās darbplūsmu konveijeri jāpārvalda, izmantojot SageMaker Pipelines vai jāizmanto risinājumi ar līdzvērtīgu funkcionalitāti. Visu pamatā esošo infrastruktūru (S3, ECR, KMS, IAM un līdzīgi) joprojām pilnībā jāpārvalda AWS vai līdzvērtīgā mākoņpakalpojumu platformā, un žurnāli un metrikaas jānovirza uz Amazon CloudWatch, bet atbilstības/kontroles pierādījumi

				jāpārsūta uz AWS Security Hub un AWS Audit Manager vai ekvivalentos risinājumos, ja nepieciešams.
1.4	Modeļa izvietošana izmantošanai pētniekiem un veselības aprūpes personālam	1	Modulis	Modulis, kas platformā pielieto izstrādāto(-s) modeli(modeļus), nodrošinot atbilstību VDAR un HIPAA, mērogojamību un izvietošanas elastīgumu. Analīzes modeļu implementācijai jābūt viegli lietojamai un jānodrošina pētniekiem un veselības aprūpes speciālistiem vadības panelis, lai analizētu un vizualizētu dažādas kohortas. Modeļu pielietošanas modulim jāizmanto Amazon SageMaker galapunkti (tostarp Serverless Inference vai Multi-Model Endpoints vai līdzvērtīgi citu piegādātāju risinājumi, ja nepieciešams), lai mitinātu un mērogotu apstiprinātus modeļus klīniskai un pētnieciskai lietošanai, kurus nodrošina Amazon API Gateway konsekventai API pārvaldībai un ierobežošanai. Tīkla piekļuve galapunktiem jāierobežo, izmantojot VPC galapunktus, drošības grupas un pēc nepieciešamības PrivateLink vai līdzvērtīgu risinājumu, lai nodrošinātu, ka klīnisko pētījumu sistēmas un slimnīcu tīkli tiek savienoti, izmantojot kontrolētus, privātus ceļus. Autentifikācija un detalizēta autorizācija modeļa pielietošanas API jāievieš, izmantojot Amazon Cognito, IAM vai līdzīgus autorizētājus, un visi izsaukumi jāreģistrē ar pilnīgu izsekojamību, izmantojot Amazon CloudWatch žurnālus un AWS CloudTrail vai ekvivalentos risinājumos, un atbilstības stāvoklis jāuzrauga AWS Security Hub vai līdzīgā risinājumā. Darbības rādītāji (latentums, kļūdu līmenis, caurlaidspēja) jāizseko, izmantojot Model Monitor un CloudWatch vai līdzīgā risinājumā, savukārt modeļu uzraudzība jākonfigurē tā, lai noteiktu datu un modeļa novirzes, nodrošinot kontrolētus atjauninājumus un drošas modeļa attīstības darbplūsmas, kas atbilst normatīvajām prasībām.
1.5	Saskarne datu pārlūkošanai, pētniecībai	1	Modulis	Modulis ārstiem un pētniekiem, lai strādātu ar datiem (tostarp apkopotiem datiem, metadatiem) un rezultātiem. Lomu balstīta piekļuve apkopotiem datiem, atbilstoši VDAR/HIPAA, tostarp darbību revīzijas žurnāli, kas saistīti ar piekļuvi datiem. Ziņojumu par pacientu datiem un statistiku izveide. Rezultātu vizualizācija un datu apkopošana, pamatojoties uz grupas piederību (piemēram, dzimums, slimība utt.) un mērījumiem. Datu pārlūkošanas un pētniecības saskarne jāveido kā droša tīmekļa lietojumprogramma, kas tiek mitināta, izmantojot AWS Amplify Hosting, vai kā statiska SPA platformā Amazon S3, ko pārvalda Amazon CloudFront, vai ekvivalentu risinājumu globālai piekļuvei ar zemu latentumu, izmantojot AWS WAF vai līdzīgus pakalpojumus aizsardzībai pret izplatītākajiem tīmekļa uzbrukumiem. Ārējai saskarnei jāizmanto aizmugursistēmas pakalpojumus, kas pieejami, izmantojot API Gateway (REST vai GraphQL, izmantojot AWS AppSync vai līdzvērtīgu risinājumu), kas izveido savienojumu ar tādiem datu avotiem kā Amazon Aurora PostgreSQL, Amazon Timestream, Amazon Athena, Amazon S3 un līdzīgiem. Kohortas līmeņa informācijas paneļus, izpētes analīzi un apkopotas vizualizācijas var ieviest tieši tīmekļa lietotāja saskarnē vai papildināt ar Amazon QuickSight vai līdzīgiem informācijas paneļiem, kas iegulti lietojumprogrammā interaktīvai analītikai un pārskatu

				veidošanai. Pētnieku, klīnicistu un administratoru autentifikācija jāveic, izmantojot Amazon Cognito, IAM Identity Center, vai līdzvērtīgus risinājumus, ar uz lomām un atribūtiem balstītām atļaujām, ko nodrošina API un datu slāņu politikas (Aurora, Lake Formation vai līdzīgi). Visas lietotāja saskarnes vadītās darbības, kas piekļūst datiem vai eksportē tos, jāreģistrē CloudWatch žurnālos, izmantojot API vārteju un CloudTrail, un jānodod AWS Security Hub un AWS Audit Manager vai līdzvērtīgos risinājumos, lai pierādītu lomai atbilstošu piekļuvi un atbilstību.
1.6	Platformas modulis pacientu metadatu vākšanai un piekrišanas pārvaldībai	1	Modulis	Nodrošina funkcionalitāti dalībnieku/pacientu metadatu ievadīšanai, uzglabāšanai, rediģēšanai un pārlūkošanai (ieskaitot piekrišanas pārvaldību), nodrošinot drošības un privātuma līmeni, kas atbilst VDAR un HIPAA prasībām. Pacientu metadati,reģistrācijas un piekrišanas ieraksti jāglabā PostgreSQL (vai pēc vajadzības Amazon DynamoDB vai līdzīgā datu bāzē liela mēroga atslēgas un vērtības piekļuvei), ar šifrēšanu miera stāvoklī, izmantojot AWS KMS vai līdzvērtīgu risinājumu, un stingru tīkla kontroli, izmantojot VPC apakštīklus un drošības grupas. Lietojumprogrammu slānis, kas pārvalda pacientu un piekrišanas loģiku, jāievieš kā mikropakalpojumi Amazon ECS Fargate vai AWS Lambda funkcijās aiz Amazon API Gateway vārtejas vai līdzvērtīgos risinājumos, ar autentifikāciju, izmantojot Amazon Cognito, un detalizētu autorizāciju, izmantojot IAM vai līdzīgus risinājumus, un, kur nepieciešams, datu piekļuves kontroli, izmantojot Lake Formation vai līdzīgu. Audita pieraksti visām izveides/atjaunināšanas/dzēšanas darbībām, kā arī piekrišanas izmaiņām un datu subjekta tiesību darbībām (piekļuve, labošana, ierobežošana, dzēšana) jāfiksē, izmantojot AWS CloudTrail un lietojumprogrammu žurnālus CloudWatch žurnālos, kas pēc tam jāapkopo un jānovērtē AWS Security Hub un AWS Audit Manager (izmantojot HIPAA/VDAR saskaņotus ietvarus kontroles pierādījumiem) vai līdzvērtīgā risinājumā. Sensitīvu personas datu atklāšanu un uzraudzību datu dublējumos, S3 eksportā un atvasinātajās datu kopās jāatbalsta ar Amazon Macie vai līdzīgu risinājumu, nodrošinot, ka pacientu identificējoša informācija tiek pienācīgi aizsargāta, klasificēta un pieejama tikai pilnvarotai lietošanai.
1.7	Platformas pielāgošana darbam ar jaunajiem datu veidiem (analīze utt.)	1	Atjaunināta platforma	Sākotnējā platforma ir jāatjaunina, lai tajā varētu iekļaut papildu datu modalitātes (MOX sensora rādījumus, kas papildināti ar gāzes hromatogrāfiju), kuras tiks ieviestas pēc izelpas analīzes (elektroniskā deguna) ierīces uzlabošanas, tostarp datu priekšapstrādi, analīzi, apkopošanu un citas platformas funkcijas. Paplašinātās funkcijas jānodrošina vismaz GC datu ielasīšana, maksimuma noteikšana, gaistošo savienojumu saskaņošana, un šie dati jāanalizē atsevišķi un kopā ar sensoru datiem, tai skaitā jāizvada atskaites un vizualizācijas par pacientu vai pacientu grupu līmenī. Atjauninātajā platformā jāparedz iespēja saskaņot un apkopot attiecīgos datus no abiem instrumentiem (ar GC un bez GC). Lai paplašinātu platformu apvienotajiem elektroniskā deguna sensoru un gāzu hromatogrāfijas (GC) datiem, ielasīšanas un apstrādes konveijeri jāievieš kā AWS Glue ETL darbi, AWS Lambda funkcijas

				vai SageMaker Processing darbi (vai līdzvērtīgi risinājumi citās platformās), kas darbojas ar GC izvadi, kas glabājas Amazon S3, ir katalogizēta ar AWS Glue Data Catalog un pārvaldīta, izmantojot AWS Lake Formation, vai līdzīgos risinājumos. Laikam piederīgas pazīmes un hromatogrāfiskie pīķi jāsaglabā PostgreSQL un/vai Amazon Timestream vai ekvivalentā, savukārt liela mēroga multimodālu pazīmju kopas jāglabā S3 kā Parquet (vai līdzvērtīgi) un pret tām jāvar veidot vaicājumus, izmantojot risinājumus kā Amazon Athena vai Amazon Redshift vai līdzīgus, ja nepieciešama augstas veiktspējas analītika. Multimodālajai modelēšanai (apvienojot no GC iegūtās agistošo organisko savienojumu (GOS) pazīmes ar MOX sensoru nolasījumiem) nepieciešams atkārtoti izmantot mākonī balstītas ML platformas (piemēram,Amazon SageMaker) steku (apmācība, apstrāde, eksperimenti, konveijeri un modeļu reģistrs), lai vienmodālie un multimodālie modeļi atbilstu tam pašam MLOps dzīves ciklam. Integrētu vizuālo analīzi hromatogrammām, GOS profiliem un sensoru pirkstu nospiedumiem nepieciešams padarīt pieejamu, izmantojot API (Athena/Redshift vaicājumi, Aurora SQL vai līdzīgi), un atveidot tīmekļa lietotāja saskarnē vai iegultos informācijas paneļos (piem., Amazon QuickSight), piekļuvi kontrolējot Cognito/Identity Center vai līdzvērtīgā risinājumā un visu lietošanu uzraugot un pierādot, izmantojot CloudTrail, Security Hub un Audit Manager vai rīkus ar līdzvērtīgu funkcionalitāti, lai uzturētu konsekventu atbilstību drošības prasībām visās datu modalitātēs.

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.