PRAKTISKĀS VADLĪNIJAS MI IEVIEŠANAI IESTĀŽU DARBĀ UN PAKALPOJUMOS

Vadlīnijas ir veidotas sadarbībā ar Valsts administrācijas skolas projektu “Publiskās pārvaldes digitālā akadēmija” (projekta Nr. 2.3.2.2.i.0/1/23/I/VARAM/001).

Finansē Eiropas Savienība – NextGenerationEU. Tomēr paustie uzskati un viedokļi ir tikai autora(-u) uzskati un viedokļi un ne vienmēr atspoguļo Eiropas Savienības vai Eiropas Komisijas uzskatus un viedokļus. Par tiem nav atbildīga ne Eiropas Savienība, ne Eiropas Komisija.

2025. gada oktobris

Finansē Eiropas Savienība NextGenerationEU

2027 Nacionālais attīstības plāns

Digitālā akadēmija

Viedās administrācijas un reģionālās attīstības ministrija

MĀKSLĪGĀ INTELEKTA LAT>IJAS ASOCIĀCIJA

Valsts administrācijas skola

Priekšvārdi

Viedās administrācijas un reģionālās attīstības (VARAM) ministra priekšvārds

Attīstoties Mākslīgā intelekta (MI) tehnoloģijām, arī Latvijas publiskā pārvalde sastopas ar nozīmīgām pārmaiņām. Iedzīvotāji sagaida efektīvākus, drošākus un pieejamākus pakalpojumus, savukārt iestādēm ir iespēja strādāt arvien gudrāk un mērķtiecīgāk. Šīs vadlīnijas sniedz praktisku ceļa karti kā izmantot mākslīgo intelektu atbildīgi un ar skaidru pievienoto vērtību sabiedrībai – no idejas līdz risinājuma ieviešanai, uzturēšanai un drošai lietošanai.

Aicinu visas valsts pārvaldes iestādes izmantot šīs vadlīnijas kā ikdienas atbalsta rīku un iedvesmas avotu. Mūsu kopīgais uzdevums ir veidot modernu, inovatīvu un uzticamu valsts pārvaldi, kur tehnoloģijas kalpo cilvēkam un sabiedrības labumam.

Kiberincidentu novēršanas institūcijas (CERT.LV) priekšvārds

Mākslīgā intelekta izmantošana publiskajā pārvaldē ir saistīta ar jauniem drošības izaicinājumiem. Ir būtiski nodrošināt, lai MI sistēmas tiktu izmantotas atbildīgi, rūpīgi izvērtējot iespējamos riskus, kas var apdraudēt iestāžu, valsts vai sabiedrības intereses. CERT.LV aicina kritiski izvērtēt MI izmantošanas mērķus, personāla un iekārtu atbilstību un iegūtos rezultātus, kā arī izmantot šīs vadlīnijas kā atskaites punktu ikvienā MI iniciatīvā.

Datu valsts inspekcijas (DVI) priekšvārds

MI ir rīks, ko var izmantot, lai uzlabotu valsts iestāžu darbu un efektīvāk izmantot resursus. Tomēr jaunā rīka izmantošana nevar būt pretrunā ar cilvēktiesībām. Tāpēc, izmantojot MI rīkus, tas jādara, ievērojot personas datu aizsardzības noteikumus: likumīgi, godprātīgi un caurspīdīgi. Šīs vadlīnijas palīdzēs iestādēm, ieviešot MI rīkus savā ikdienā, nodrošināt, ka personas dati ir izmantoti cilvēka labā, ar tiesisko konkrētu nolūku un ir aizsargāti iestādes ietvaros.

Valsts administrācijas skolas (VAS) priekšvārds

Mākslīgā intelekta izmantošana ir viena no aktuālākajām un nozīmīgākajām digitālajām kompetencēm publiskajā pārvaldē. Lai mākslīgā intelekta sniegtās iespējas izmantotu jēgpilni un atbildīgi, ir svarīgi veidot zināšanas, prasmes un izpratni par tā darbības principiem, riskiem un pielietojumu.

Mācīšanās šajā jomā ir nepārtraukts process – no pamatzināšanām līdz praktiskiem risinājumiem, kas palīdz efektīvāk strādāt un radīt sabiedrībai lielāku vērtību. OECD pētījumi apliecina, ka tieši mācīšanās un attīstība visvairāk veicina darbinieku iesaisti un motivāciju. Valsts administrācijas skola aicina neapstāties mācīšanās ceļā un kopīgi attīstīt prasmes mākslīgā intelekta jomā.

Mākslīgā intelekta Latvijas asociācijas (MILA) priekšvārds

Šīs vadlīnijas izstrādāja MILA un tās biedra AI Master Lab eksperti ciešā sadarbībā ar valsts iestādēm, kuru pieredze un atziņas palīdzēja padarīt dokumentu praktisku un piemērotu publiskās pārvaldes vajadzībām. Vadlīnijas paredzētas kā atbalsts iestādēm mākslīgā intelekta drošā un atbildīgā izmantošanā, vienlaikus veicinot inovatīvu un sabiedrības interesēm atbilstošu pakalpojumu attīstību.

PATEICĪBA IESTĀDĒM

Šo vadlīniju izstrāde balstīta uz ciešu sadarbību ar Latvijas publiskā sektora iestādēm. Īpaša pateicība iestādēm, kas piedalījās padziļinātajās intervijās un darbnīcās:

- Aizsardzības ministrija;
- Datu valsts inspekcija;
- Ekonomikas ministrija;
- Kultūras informācijas sistēmu centrs;
- Latvijas Nacionālais akreditācijas birojs;
- Liepājas Centrālā administrācija;
- Rīgas Dome / Rīgas digitālā aģentūra;
- Tiesībsargs;
- Tieslietu ministrija;
- Uzņēmumu reģistrs;
- Valsts administrācijas skola;
- Valsts digitālās attīstības aģentūra;
- Valsts ieņēmumu dienests;
- Valsts kontrole;
- Valsts sociālās apdrošināšanas aģentūra;
- Valsts zemes dienests;
- Viedās administrācijas un reģionālās attīstības ministrija.

Pateicamies par sniegtajām atziņām, pieredzi un diskusijām, kas ļāva šo dokumentu veidot praktisku un piemērotu publiskās pārvaldes vajadzībām.

Satura rādītājs

Ievads

Šo vadlīniju mērķis ir nodrošināt publiskās pārvaldes iestādēm vienotu, atbildīgu un drošu pieeju MI risinājumu izmantošanai praksē. Ir svarīgi atcerēties, ka MI risinājums nav universāls instruments – dažkārt efektīvāks būs cits tehnoloģisks vai organizatorisks risinājums. Pareizi piemeklēts MI risinājums var dot lielu ieguvumu ar mazākiem resursiem, savukārt nepiemērots – radīt kļūdas, izmaksas un lieku laika patēriņu.

MI sistēmas un citi digitālie risinājumi ir pakļauti visiem tiem pašiem normatīvajiem aktiem, kas attiecas uz citiem IT risinājumiem, papildus ievērojot Eiropas Savienības Mākslīgā intelekta aktu (MI Aktu) ar tā prasībām par riska līmeņu noteikšanu un risku pārvaldīšanu. Īpaša uzmanība jāpievērš arī personas datu aizsardzībai, kā to nosaka Vispārīgā datu aizsardzības regula (VDAR).

Vadlīnijas ir ieteikuma rakstura dokuments, kas kalpo kā vienots labās prakses standarts visām publiskās pārvaldes iestādēm. Tajās ietvertas praktiskas metodes, piemēram, shēmas, tabulas, lēmumu koki, kontrolsaraksti un piemēri, kas palīdz iestādēm droši un efektīvi izmantot MI risinājumus ikdienas darbā. Praktiskā ieviešana balstās uz iestādes apstiprinātu balto sarakstu ar iestādē atļautajiem MI rīkiem.

Dokuments paredzēts vadītājiem stratēģiskās plānošanas un uzraudzības atbalstam, IT un kiberdrošības speciālistiem tehnisko prasību nodrošināšanai, kā arī darbiniekiem drošai ģeneratīvā MI un citu MI rīku lietošanai ikdienas darbā.

Šajās vadlīnijās lietotie jēdzieni tiek izmantoti atbilstoši to nozīmei un kontekstam:

- **MI sistēma** – juridiski definēts jēdziens saskaņā ar MI aktu. Tā ir mašinizēta sistēma, kas spēj patstāvīgi analizēt informāciju un radīt iznākumus (prognozes, ieteikumus, saturu vai lēmumus), kas var ietekmēt cilvēku vai digitālo vidi.
- **MI risinājums** – praktisks MI sistēmas pielietojums iestādes darbā vai pakalpojumos. Šis termins vadlīnijās tiek lietots vispārīgā nozīmē, apzīmējot MI izmantošanu praksē.
- **MI rīks** – konkrēts instruments vai programmatūra, kas izmanto MI sistēmu, piemēram, tulkošanas platformas, teksta ģeneratori vai čatboti.
- **MI tehnoloģija** – tehniska pieeja vai metode, uz kuras balstās MI sistēma, piemēram, mašīnmācīšanās, dabīgās valodas apstrāde vai ģeneratīvais MI.
- **MI modelis** – matemātisks modelis, kas apstrādā datus un nodrošina MI sistēmas darbību.

Vienotas izpratnes nodrošināšanai vadlīnijās galvenokārt lietots termins **“MI risinājums”** kā kopīgs apzīmējums MI sistēmu izmantošanai publiskajā pārvaldē.

Vadības kopsavilkums

Mākslīgais intelekts (MI) var sniegt būtisku atbalstu publiskajai pārvaldei, paaugstinot efektivitāti, uzlabojot pakalpojumu kvalitāti un samazinot administratīvo slogu. Vienlaikus tā ieviešana rada riskus personas datu un citas ar normatīvajiem aktiem aizsargātas informācijas aizsardzības, kiberdrošības, uzticamības un reputācijas jomās. MI ir pakļauts tiem pašiem normatīvajiem aktiem, kas attiecas uz citiem informācijas tehnoloģiju risinājumiem, papildus ievērojot Eiropas Savienības Mākslīgā intelekta akta prasības.

Darbiniekiem ikdienā visbiežāk redzamā MI forma ir MI rīki – praktiski instrumenti, piemēram, tulkošanas platformas, čatboti vai teksta kopsavilkumu ģeneratori, kas balstās uz MI risinājumiem un tiek izmantoti konkrētu uzdevumu veikšanai.

Vispārējie principi informācijas ievadīšanai un apstrādei MI rīkos

Iestādēm šie principi jāievēro un jāizmanto kā pamats iekšējo noteikumu un praktisko atgādņu izstrādei darbiniekiem drošai MI lietošanai:

- **Publiski pieejamas informācijas izmantošana** – pēc noklusējuma publisku informāciju drīkst apstrādāt ar MI rīkiem, ja iestāde nav noteikusi citus ierobežojumus.
- **Informācija, kurai ir noteikti ierobežojumi un papildu aizsardzības prasības** – personas datu, ierobežotas pieejamības informācijas un citas normatīvajos aktos aizsargātas informācijas izmantošanu ar MI risinājumiem drīkst veikt tikai tādā apjomā un kārtībā, kādu nosaka iestādes iekšējie noteikumi.
- **Baltā saraksta prioritāte** – iestādes baltais saraksts ir galvenais praktiskais instruments MI rīku lietošanas noteikšanai, taču tā saturam vienmēr jāatbilst normatīvo aktu prasībām.

Pieci iestādes un vadības pamatsoļi MI drošai un lietderīgai ieviešanai

1. Stratēģija un mandāts

- Definēt, kā MI risinājumi palīdz sasniegt iestādes stratēģiskos mērķus.
- Izvēlēties jomas, kur MI risinājumi sniedz vislielāko pievienoto vērtību (piem., dokumentu apstrāde, klientu atbalsts, datu analītika).
- Nodrošināt, ka atbildību par gala lēmumu vienmēr nes darbinieks un iestāde, nevis MI sistēma.

2. Atbildība un komanda

- Nozīmēt galveno atbildīgo par MI iniciatīvām iestādē.
- Nodrošināt MI risinājumu ieviešanas, juridisko, datu aizsardzības un kiberdrošības kompetenci (iekšēji vai ārpakalpojumos).
- Nodrošināt MI rīku baltā saraksta un lietošanas noteikumu izstrādi.

3. Resursi un kapacitāte

- Atvēlēt budžetu pilotprojektiem, uzturēšanai un atjauninājumiem.
- Nodrošināt darbinieku apmācības un praktiskās atgādnes MI rīku drošai lietošanai (skat. 9.–11. pielikums).
- Pieņemt lēmumus par ārējo piegādātāju iesaisti, izvērtējot riskus un līgumu nosacījumus.

4. Uzraudzības mehānismi

- Pieprasīt riska un atbilstības novērtējumu pirms jebkura MI risinājuma ieviešanas.
- Noteikt regulāru MI projektu pārskatu iesniegšanu vadībai.
- Nodrošināt incidentu reģistrācijas un ziņošanas sistēmu.

5. Kultūra un sadarbība

- Skaidri paust vadības atbalstu drošai MI izmantošanai.
- Veicināt sadarbību ar citām iestādēm un atbalstīt savus "MI čempionus".
- Regulāri pārskatīt iestādes noteikumus un balto sarakstu atbilstoši jaunākajai praksei un normatīvajām prasībām.

Praktiskie instrumenti vadībai pieejami vadlīniju pielikumos – tie ietver lēmumu kokus, kontrolsarakstus un darbinieku atgādnes, kurus izmanto speciālisti pēc vadības deleģējuma.

1. Mākslīgā intelekta pamati, principi un normatīvais ietvars

Šī sadaļa skaidro, kas ir mākslīgais intelekts (MI), kā arī principus un ieteikumus tā drošai un atbildīgai praktiskai pielietošanai publiskajā pārvaldē.

MI tiesiskā regulējuma īpatnība ir tāda, ka uz to attiecas gan specifisks tieši ar MI saistītu jautājumu regulēšanai pieņemts tiesiskais regulējums, gan arī, noteiktos gadījumos un atkarībā no konteksta, jau pastāvošais normatīvais regulējums, jo īpaši personas datu aizsardzības un kiberdrošības jomā:

- Latvijai kā Eiropas Savienības dalībvalstij ir saistošs MI Akts, kas ir pirmais visaptverošais MI regulējums pasaulē. Turklāt jau šobrīd Latvijā atsevišķos normatīvajos aktos ir iekļauti uz MI specifiski attiecināmi noteikumi (piemēram, Mākslīgā intelekta centra likumā, Priekšvēlēšanu aģitācijas likumā).
- MI tehnoloģijai ir plašas pielietojuma iespējas (dažādas nozares un uzdevumi), līdz ar to atkarībā no tās konkrēta pielietojuma veida un konteksta uz to attieksies nozares normatīvais regulējums un noteiktu procesu normatīvais regulējums.
- Tā kā MI balstās uz datiem (tie ir nepieciešami gan MI trenēšanai, gan izmantošanai), atkarībā no izmantoto datu veida (publiski pieejami dati (piemēram, statistikas dati), personas dati, ierobežotas pieejamības informācija, valsts noslēpums, komercnoslēpums, ar autortiesībām aizsargājami darbi u. tml.) būs piemērojams normatīvais regulējums, kas nosaka šādu datu izmantošanu (piemēram, ja tiek apstrādāti personas dati, jāievēro VDAR prasības, ja tiek apstrādāti ar autortiesībām aizsargājami darbi, jāievēro Autortiesību likuma prasības).
- MI pieder pie informācijas un komunikācijas tehnoloģijām, līdz ar to uz to attiecas šādām tehnoloģijām piemērojamais normatīvais regulējums (piemēram, kiberdrošības jomā – Nacionālās kiberdrošības likums).

MI pamati, principi un normatīvais ietvars vadlīnijās skaidrots, ievērojot minētās īpatnības.

1.1. Mākslīgā intelekta izpratne un piemēri publiskajā sektorā

Mākslīgais intelekts kā zinātnes nozare pastāv jau vairāk nekā 70 gadus, taču vienota definīcija Latvijas normatīvajos aktos līdz šim nav nostiprināta. Tas ir saistīts ar to, ka MI ir plašs pielietojums un tehnoloģiju daudzveidība. Vienlaikus Latvijā ir juridiski saistošs un tieši piemērojams Eiropas Savienības **Mākslīgā intelekta akts**, kurā ir definēts MI sistēmas jēdziens. Tāpēc vadlīnijās ir izmantota šī definīcija, tādējādi nodrošinot konsekventu un vienotu izpratni publiskās pārvaldes iestādēs.

> ““MI sistēma” ir mašinizēta sistēma, kura projektēta darboties ar dažādiem autonomijas līmeņiem, kura var pēc ieviešanas būt adaptīva, un kura eksplicītiem vai implicītiem mērķiem secina no informācijas, ko tā saņem, kā ģenerēt iznākumus, piemēram, prognozes, saturu, ieteikumus vai lēmumus, kas var ietekmēt fizisko vai virtuālo vidi.”[1]

Šī definīcija aptver plašu tehnoloģiju spektru – no mašīnmācīšanās un neironu tīkliem līdz ģeneratīvajam MI. Tā ir elastīga, lai pielāgotos tehnoloģiju attīstībai, un saskaņota ar starptautisku organizāciju, jo īpaši ar Ekonomiskās sadarbības un attīstības organizācijas (OECD), pieejām.[2]

Vienkāršoti **mākslīgo intelektu** var skaidrot **kā tehnoloģiju kopumu**, kas ne tikai izpilda iepriekš noteiktus soļus, bet arī **spēj mācīties no datiem, pielāgoties, prognozēt un radīt jaunu saturu**, piemēram, tekstu, attēlus vai video.

Atšķirībā no automatizācijas, kas atkārto noteiktas darbības, vai datu analītikas, kas palīdz izprast esošās tendences, **MI tehnoloģijas ļauj atklāt jaunas sakarības un piedāvāt inovatīvus risinājumus**.

Darbiniekiem ikdienā visbiežāk redzamā forma ir **MI rīki – praktiski instrumenti**, piemēram, tulkošanas platformas, čatboti vai teksta kopsavilkumu ģeneratori, kas balstās uz **MI risinājumiem** un tiek izmantoti **konkrētu uzdevumu veikšanai**.

Valsts pārvaldē MI risinājumi jau plaši tiek izmantots vairākos stabilos un pārbaudītos uzdevumos:

- **politikas veidošanā** – datu apkopošana un analīze, scenāriju prognozēšana un veidošana;
- **pakalpojumu sniegšanā iedzīvotājiem** – mašīntulkošana, e-pasta un čatu šķirošana ar atbilžu sagatavošanu, zvanu centru kvalitātes kontrole, protokolēšana un transkripcijas;
- **iekšējo uzdevumu atbalstam** – dokumentu sākotnējā pārbaude un klasifikācija, protokolēšana un transkripcijas.

Šie ir droši un praksē pārbaudīti piemēri, kas sniedz skaidru pievienoto vērtību iestādēm. Tomēr MI iespējas ir plašākas, un jau šobrīd iezīmējas tendences tā izmantošanai **prognozēšanā un modelēšanā** (piemēram, līdzīgi kā Covid-19 laikā, lai izvērtētu iespējamos scenārijus un lēmumus), kā arī **riska analīzē, resursu plānošanā un sabiedrības noskaņojuma analīzē**.

MI tehnoloģiju klāsts ir plašs, taču trīs galvenās pieejas veido pamatu lielākajai daļai risinājumu:

1. **Noteikumos balstītā pieeja jeb ekspertu sistēmas.** Šīs sistēmas izmanto iepriekš definētus noteikumus vai zināšanu bāzes, lai piemērotu loģiskus secinājumus un nonāktu pie lēmuma. Šādi risinājumi tiek uzskatīti par MI, ja tie ietver spriešanas vai secināšanas spējas, ne tikai mehānisku darbību izpildi. Piemēram, Tiesu administrācijas anonimizācijas rīks, kas dokumentos aizvieto sensitīvus datus.

[1] Sīkāk definīcijas skaidrojumu sk. Komisijas paziņojums “Komisijas pamatnostādnes par mākslīgā intelekta sistēmas definīciju, kas noteikta Regulā (ES) 2024/1689 (MI aktā)”, C(205) 5053 final, 29.07.2025.
[2] Sk. *Explanatory Memorandum on the Updated OECD Definition of an AI System*. OECD Artificial Intelligence Papers. March 2024, No. 8, p. 4.

2. **Datu balstītā pieeja jeb mašīnmācīšanās.** Šī pieeja ļauj MI sistēmām mācīties no datiem, atklāt sakarības un prognozēt rezultātus, neveidojot iepriekš noteiktus noteikumus. To izmanto datu klasifikācijai, analīzei, riska novērtēšanai vai lēmumu atbalstam. Piemēram, Valsts zemes dienesta LIDAR datu analīze, kas palīdz atklāt ēkas zem kokiem un noteikt kadastra neatbilstības.
3. **Ģeneratīvā pieeja.** Tā ietver sistēmas, kas spēj radīt jaunu saturu – tekstu, attēlus, audio vai programmēšanas kodu. Šādi rīki spēj apvienot apgūto informāciju un piedāvāt jaunas versijas vai idejas. Piemēram, *Hugo.lv* tulkošanas rīki, Rīgas 1. slimnīcas virtuālais asistents "Maija". Ģeneratīvais MI jāuztver kā palīgrīks, kas palīdz sagatavot pirmo versiju vai attīstīt ideju, taču gala lēmums jāpieņem un atbildība vienmēr paliek cilvēkam.

Praksē šīs pieejas bieži tiek izmantotas kopā ar citām tehnoloģijām, piemēram, datu analīze var nodrošināt ievaddatus MI modelim, savukārt automatizācija palīdz īstenot tā ieteikumus. Atbildības un normatīvo prasību ziņā šīs pieejas atšķiras, tāpēc iestādēm ir būtiski **precīzi noteikt, vai risinājums ir MI, datu analītika vai automatizācija**.

Šajās vadlīnijās praktiskai lietošanai tiek raksturotas trīs tehnoloģiskās pieejas:

- **Automatizācijas risinājumi (piemēram, RPA)** – paredzēti atkārtotu un noteiktu darbību veikšanai pēc iepriekš definētiem noteikumiem un nav uzskatāmi par mākslīgā intelekta risinājumiem.
- **MI risinājumi datu analīzei un prognozēšanai** – izmanto mašīnmācīšanos un citus datu modeļus analītiskiem uzdevumiem, piemēram, riska novērtēšanai, tendenču analīzei un lēmumu pieņemšanas atbalstam.
- **Ģeneratīvie MI risinājumi** – paredzēti jauna satura vai ideju radīšanai (teksts, attēli, audio, video, programmēšanas kods).

Būtiski: ģeneratīvais MI (piemēram, *ChatGPT*) ir tikai viena MI daļa. Ne viss, kas ir automatizēts, ir MI. MI palīdz strādāt ātrāk, bet gala atbildība vienmēr ir cilvēkam.

Šajās vadlīnijās turpmāk lietots vispārīgais termins "MI risinājums", apzīmējot MI sistēmas praktisku izmantošanu publiskajā pārvaldē.

1.2. Normatīvais ietvars

MI risinājumi publiskās pārvaldes iestādēs jāievieš, ievērojot normatīvo regulējumu. Ieviešot MI risinājumus, publiskās pārvaldes iestādēm ir jāidentificē, kuri normatīvie akti attiecināmi uz konkrēto MI sistēmu un tās pielietojumu. Iestādēm ir jāpārbauda:

1. Vai uz attiecīgo pielietojumu attiecas nozares speciālais regulējums (piemēram, aviācijas jomā vai tiesībaizsardzības jomā).
2. Vai attiecīgais uzdevums ir saistīts ar kādu normatīvajos aktos regulētu procesu (piemēram, atbildes sniegšana uz iesniegumu).

3. Kādi dati izmantoti MI sistēmas trenēšanā un kādus datus ir paredzēts ievadīt MI sistēmā, un vai šādu datu izmantošana ir regulēta vai ierobežota normatīvajos aktos.
4. Vai un kādas kiberdrošības prasības ir izvirzāmas attiecīgajai MI sistēmai.
5. Kādas pakāpes risku MI sistēma rada un vai ir jāizpilda kādas MI Aktā noteiktās prasības.

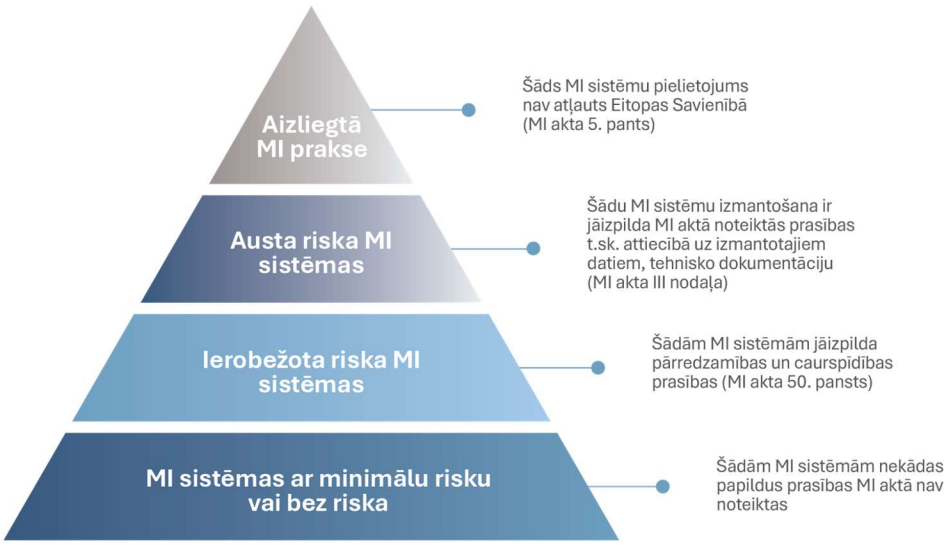
Dažas MI sistēmas, to pielietojuma veida un izmantoto datu dēļ, iestādēs var izmantot bez ierobežojumiem, un tām nav jāizpilda īpašas normatīvo aktu prasības, piemēram, izmantojot publiski pieejamas MI sistēmas prezentāciju vai skaidrojošu materiālu sagatavošanai un vizuālai noformēšanai.

Savukārt citas MI sistēmas, to pielietojuma veida, izmantoto datu vai kiberdrošības prasību dēļ, publiskās pārvaldes iestādes drīkst izmantot tikai tad, ja tiek izpildītas piemērojamo normatīvo aktu prasības.

Pirms jebkura MI risinājuma ieviešanas iestādei jāpārliecinās, kādi normatīvie akti ir piemērojami un kādas prasības tai jāizpilda. Izpildāmās prasības atšķirsies atkarībā no katras iestādes darbības specifikas, MI sistēmu pielietojuma un izmantotajiem datiem.

MI Akts stājās spēkā 2024. gada 1. augustā, bet tā ieviešana noritēs pakāpeniski līdz 2027. gada 2. augustam. No 2025. gada 2. februāra ir spēkā MI pratības prasības un aizliegtās MI prakses, no 2025. gada 2. augusta ir spēkā prasības vispārīga lietojuma MI modeļiem, bet prasības augsta riska MI sistēmām būs jāpiemēro no 2026. gada 2. augusta.

Lai arī MI Akts šobrīd ir piemērojams tikai daļēji, jau šobrīd iestādēm ir svarīgi apzināties, kurā riska kategorijā to izmantotās vai nākotnē plānotās MI sistēmas ietilpst, un savlaicīgi sagatavoties piemērojamo MI Akta prasību izpildei.



1. attēls. ES Mākslīgā intelekta akta riska līmeņu hierarhija

MI akts paredz uz risku balstītu pieeju, klasificējot MI sistēmas četrās riska kategorijās atkarībā no riska nopietnības pakāpes, ko rada attiecīgās sistēmas izmantošana (skat. 1. attēlu):

1. Aizliegta MI prakse – rada nepieņemamu riska līmeni un ir aizliegta pilnībā.

- **Piemēri**: kaitīga MI balstīta manipulācija un maldināšana, kaitīga neaizsargātības izmantošana, sociālā vērtēšana, atsevišķu noziedzīgu nodarījumu riska novērtējums vai prognozēšana, sejas atpazīšanas datu bāzes, kas iegūtas no interneta vai drošības kamerām bez īpašas atlases, emociju atpazīšana un vērtēšana sensitīvās vietās, piemēram, darba vietās vai izglītības iestādēs, biometriskā kategorizācija, lai izdarītu secinājumus par tādiem sensitīviem raksturlielumiem kā rase, reliģija vai politiskie uzskati, reāllaika biometriskā identifikācija tiesībaizsardzības nolūkos sabiedriskās vietās.[3]
- **Prasības:** aizliegta pilnībā, nav izmantojama.

2. Augsta riska MI sistēmas – atļautas, taču izmantojamas tikai ar stingrām drošības un pārredzamības prasībām.

- **Piemēri**: jomas, kur ir iespējama ietekme uz pamattiesībām, drošību un veselību: drošības sastāvdaļas tādos izstrādājumos, kā medicīnas iekārtas, uz kuriem attiecas ES saskaņošanas tiesību akti un kuriem saskaņā ar tiem pašiem ES saskaņošanas tiesību aktiem ir jāveic trešās puses atbilstības novērtējums, kritiskā infrastruktūra, biometrija, izglītība un arodmācības, nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai, piekļuve privātiem pamatpakalpojumiem un sabiedriskajiem pamatpakalpojumiem un pabalstiem un to izmantošanai, tiesībaizsardzība, migrācijas, patvēruma un robežkontroles pārvaldība, tiesvedība un demokrātijas procesi.[4]
- **Prasības**: izmantošanai MI Akts izvirza papildu prasības, kā riska pārvaldības sistēmas izveidi, noteiktas prasības datiem un datu pārvaldībai, tehniskajai dokumentācijai, notikumu uzskaitei, pārredzamībai, cilvēka virsvadībai, precizitātei, robustumam un kiberdrošībai.[5] Atkarībā no lomas MI sistēmas dzīvesciklā, katrai iesaistītajai personai – MI sistēmu nodrošinātājiem, viņu pilnvarotajiem pārstāvjiem, importētājiem, izplatītājiem un MI sistēmu uzturētājiem – MI Aktā ir noteikti konkrēti pienākumi.[6] Ieviešot MI sistēmas jomās, kur pastāv augsts risks, publiskās pārvaldes iestādēm ir jāizpilda MI sistēmu uzturētājiem noteiktās prasības, t. sk. jāveic augsta riska MI sistēmu ietekmes uz pamattiesībām novērtējums,[7] kā arī publiskā iepirkuma ietvaros no piegādātājiem jāpieprasa viņiem MI Aktā noteikto pienākumu izpildi, piemēram, MI sistēmas sertificēšanu.

[3] Detalizētāk sk. MI Akta 5. panta 1. punktu, kur arī noteikti izņēmuma gadījumi, kad norādītās prakses ir atļautas, un Komisijas paziņojumu "Komisijas Pamatnostādnes par aizliegtu mākslīgā intelekta praksi, kas noteikta Regulā (ES) 2024/1690 (MI aktā)", C(2025) 5052 final. Brisele, 29.07.2025.
[4] MI Akta 6. panta 1.–3. punkts, I un III pielikums.
[5] MI Akta 9. –15. pants.
[6] Sk. MI Akta III nodaļas 2. un 3. iedaļu.
[7] MI Akta 27. pants.

3. Ierobežota riska MI sistēmas – atļautas, taču obligāti jānodrošina lietotāju informēšana un pārredzamība.

- **Piemēri**: čatboti, MI sistēmas, kas ģenerē sintētisku audio, attēla, video vai teksta saturu.
- **Prasības**: izmantošanai MI Akts izvirza papildu prasības, kā pārredzamības un caurskatāmības prasības, piemēram, fizisko personu informēšanu par to, ka tās mijiedarbojas ar MI sistēmu.[8]

4. MI sistēmas ar minimālu risku vai bez riska – brīvi izmantojamas, visas pārējās sistēmas, kas neklasificējas kā aizliegta MI prakse, augsta riska MI sistēmas vai ierobežota riska MI sistēmas.

- **Piemēri**: mēstuļu filtri, automātiska formatēšana.
- **Prasības**: MI sistēmām MI Aktā nekādas prasības nav izvirzītas.

Atbalsta saņemšanai MI risinājumu ieviešanā, lai nodrošinātu normatīvo aktu prasību izpildi, var vērsties kompetentās institūcijās:

- **CERT.LV** – kiberdrošība un incidentu novēršana;
- **Datu valsts inspekcija** – personas datu aizsardzība;
- **Iepirkumu uzraudzības birojs** – publisko iepirkumu organizēšanas jautājumi;
- **Tiesībsargs** – pamattiesību ievērošana;
- **Valsts administrācijas skola** un **Digitālā akadēmija** – darbinieku kompetenču attīstība;
- **VARAM** – MI politikas koordinācija publiskajā sektorā.

1.3. Mākslīgā intelekta principi

Eiropas Savienības un starptautiskā līmenī MI ētiskai, drošai un atbildīgai izmantošanai ir definēti vairāki principi (piemēram, OECD,[9] UNESCO,[10] ES augsta līmeņa ekspertu grupas 7 principi[11]). No tiem publiskajā pārvaldē praktiskai ieviešanai akcentēti tie, kas visciešāk sasaistās ar MI akta prasībām un iestāžu ikdienas darbību. Izvēlētie principi neizslēdz pārējo nozīmi — tie joprojām ir aktuāli politikas un stratēģijas līmenī. Praktiskajās vadlīnijās īpaši akcentēti tie principi, kas tieši ietekmē **lēmumu pieņemšanu, drošību un sabiedrības uzticēšanos**, bet katras iestādes ziņā ir noteikt arī papildu principus, ko tā uzskata par būtiskiem.

---

[8] Sīkāk sk. MI Akta 50. pantu.

[9] *Recommendation of the Council on Artificial Intelligence*. OECD Legal Instrument 0449. Paris: OECD, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, pp. 8-9.

[10] *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137, pp. 7-10.

[11] Neatkarīga AI augsta līmeņa ekspertu grupa, ko 2018. gada jūnijā izveidojusi Eiropas Komisija. *Ētikas vadlīnijas uzticamam AI*. Pieejams: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_LV.pdf.

Tie ir četri MI drošas un atbildīgas izmantošanas principi:

- **Cilvēka kontrole** – galavārds vienmēr pieder cilvēkam, īpaši, ja lēmumi ietekmē pamattiesības.
- **Drošība un uzticamība** – MI risinājumiem jābūt drošiem un jādarbojas paredzētajā veidā, neradot nepieļaujamus riskus.
- **Caurskatāmība un izskaidrojamība** – lietotājiem (gan iestādēm, gan iestāžu klientiem) jāzina, ka tiek izmantots MI, un jāsaprot tā loma lēmuma pieņemšanas procesā.
- **Sabiedrības labums un uzticēšanās** – MI risinājumiem jāsniedz skaidrs ieguvums sabiedrībai un jāstiprina iedzīvotāju uzticēšanās publiskajam sektoram.

Šie MI drošas un atbildīgas pielietošanas un publiskās pārvaldes vispārīgie darbības principi tiek pārvērsti darbiniekiem saprotamās ikdienas darbībās MI pielietošanai:

- **Zini**, kad izmantot MI un kādi ir tā ierobežojumi.
- **Nekad neievadi** publiskos MI rīkos personas datus vai konfidenciālu informāciju.
- **Vienmēr pārbaudi** MI sniegtos rezultātus.
- **Atceries**, ka atbildība vienmēr ir cilvēkam, nevis MI.
- **Ievēro** iestādes kiberdrošības un datu aizsardzības prasības.

Izvērstāks saraksts ar skaidrojumiem ikdienas darbībām MI pielietošanai pievienots **1. pielikumā**.

1.4. Mākslīgā intelekta risinājumu pārvaldība

MI risinājumu pārvaldība nozīmē kontroles un pārraudzības pasākumu kopumu, ar kuriem iestāde pārliecinās, ka MI risinājums darbojas droši, atbilstoši normatīvo aktu prasībām un iestādes noteiktajiem mērķiem šim risinājumam. Tas ietver gan atbildības noteikšanu un procesu uzraudzību, gan regulāras pārbaudes, lietotāju iesaisti un dokumentāciju, šos pasākumus pielāgojot konkrētu MI risinājumu pielietošanas veidam un ar to saistīto risku pakāpei.

Katras iestādes pienākums ir izveidot un regulāri atjaunot **balto sarakstu** – sarakstu ar iestādē apstiprinātajiem MI rīkiem, kurus drīkst izmantot darba vajadzībām. Par **apstiprinātiem MI rīkiem** uzskatāmi tikai tie, kurus iestāde ir izvērtējusi un atļāvusi lietot, iepazīstoties ar licences noteikumiem, pārliecinoties par to atbilstību normatīvajiem aktiem, t. sk. kiberdrošības prasībām. Visi pārējie pieejamie rīki (gan bezmaksas, gan maksas) tiek uzskatīti par **neapstiprinātiem rīkiem.**

Iestādei, kas ievieš MI risinājumu, ir jāizvērtē šādu pasākumu nodrošināšanas nepieciešamība, jo īpaši ievērojot ar konkrēto MI risinājumu saistītus riskus, lietošanas kontekstu un izmantotās informācijas un datu veidu:

- atbildīgie darbinieki par datu kvalitāti, drošību un procesa uzraudzību;
- regulāras pārbaudes un monitorings (drošība, precizitāte, atbilstība mērķiem);

- iespēja lietotājiem sniegt atgriezenisko saiti un ziņot par problēmām;
- dokumentācija par risinājuma darbību, testiem, izmaiņām un lēmumiem.

Šo pasākumu īstenošanas nepieciešamība ir jānovērtē visos MI risinājuma dzīves cikla posmos – no sagatavošanās līdz izņemšanai no lietošanas. Detalizēti pārvaldības un uzraudzības piemēri ir apkopoti **2. pielikumā**, kas kalpo kā praktisks atbalsta materiāls vadībai un speciālistiem.

Vadībai MI risinājumu kontrole un pārraudzība nozīmē:

- zināt, kādas MI sistēmas un kādiem uzdevumiem tiek izmantotas iestādē, tai skaitā apzināt arī neatļautas lietošanas gadījumus, lai novērstu riskus un lemtu par turpmāko rīcību;
- paredzēt procedūras, atbildības sadali un resursus, lai nodrošinātu izmantoto MI risinājumu atbilstību piemērojamiem normatīvajiem aktiem un MI principiem;
- izveidot MI risku novērtēšanas un pārraudzības sistēmu;
- sekot līdzi Latvijas un starptautiskajām labajām praksēm un aktualitātēm.

Darbiniekiem MI risinājumu kontrole un pārraudzība nozīmē:

- lietot tikai tos MI risinājumus, kas ir iekļauti iestādes baltajā sarakstā, izņemot gadījumus, kad tiek apstrādāta tikai publiski pieejama informācija, ja iestādes iekšējie noteikumi neparedz stingrākus ierobežojumus;
- lietot tos droši un atbildīgi, ievērojot noteiktos ierobežojumus un prasības;
- zināt, pie kā vērsties jautājumu vai problēmu gadījumā;
- ziņot par problēmām un paļauties, ka apstiprinātie risinājumi tiek uzraudzīti atbilstoši drošības un darbības kvalitātes standartiem.

Iestāžu vadītājiem un speciālistiem ieteicams nodrošināt regulāru pieredzes apmaiņu ar citām institūcijām, piemēram, piedaloties kopīgās darba grupās, semināros vai citās sadarbības platformās. Šāda sadarbība ļauj veidot kopīgu labo prakšu apmaiņu, tostarp par baltā saraksta uzturēšanu un apstiprināto rīku izvērtēšanu, un attīstīt risinājumus, kurus iespējams izmantot plašāk visā valsts pārvaldē, kā arī veicina MI pratības celšanu.

2. Uzdevuma izvēle un izvērtēšana

Pirmais solis ceļā uz mākslīgā intelekta (MI) risinājumu izmantošanu ir piemērotu uzdevumu identificēšana un izvērtēšana. Šajā posmā ir būtiski noteikt, vai konkrētā problēma patiešām prasa MI pielietojumu, vai arī to efektīvāk iespējams risināt ar automatizācijas vai datu analītikas palīdzību. Šāda pakāpeniska, "soli pa solim" pieeja palīdz izvēlēties tādus MI risinājumus, kas sniedz reālu pievienoto vērtību, ir tehniski īstenojami un atbilst normatīvo aktu prasībām.

2.1. Ideju apkopošana un sākotnējais izvērtējums

Iestādē ieteicams izveidot plašu potenciālo uzdevumu sarakstu, iesaistot gan vadību, gan darbiniekus, piemēram, ar idejošanas sesiju un iekšējo ierosinājumu apkopšanas palīdzību. Šādu aktivitāšu mērķis ir iegūt pietiekami plašu ideju kopumu (5–10–20 idejas), no kura iespējams atlasīt perspektīvākos un MI risināšanai piemērotākos uzdevumus.

Ideju apkopošanā, var vadīties pēc šādiem kritērijiem:

- uzdevums tiek veikts regulāri un prasa ievērojamu laiku vai cilvēkresursus;
- uzdevumam ir skaidrs mērķis un sagaidāms izmērāms uzlabojums;
- uzdevuma veikšanai tiek izmantoti vai ir pieejami dati pietiekamā apjomā un kvalitātē;
- kļūdas gadījumā sekas ir kontrolējamas un labojamas;
- gala rezultātu var pārbaudīt un apstiprināt darbinieks;
- uzdevums nav tieši saistīts ar juridiski saistošu lēmumu pieņemšanu;
- sagaidāms būtisks efektivitātes, kvalitātes vai lietotāju pieredzes uzlabojums.

Tipiski piemēri iekšējiem procesiem, kas bieži vien ir drošākie kandidāti MI risinājumu izmantošanai, ir dokumentu klasifikācija, e-pastu un iesniegumu maršrutēšana, sanāksmju audioierakstu transkripcija un kopsavilkumu sagatavošana, normatīvo aktu salīdzināšana un kopsavilkumi, datu vizualizācija un atskaišu sagatavošana, revīziju un iekšējās kontroles atbalsts. Ideju atrašanai var izmantot arī tipveida MI uzdevumu katalogu **3. pielikumā**.

Pēc ideju apkopošanas, tās ieteicams izvērtēt pēc diviem galvenajiem kritērijiem:

- **lietderīgums / ieguvums** – sagaidāmā pievienotā vērtība iestādei un sabiedrībai;
- **sasniedzamība / sarežģītība** – datu pieejamība, tehniskās iespējas un resursu apjoms.

Šāds sākotnējais izvērtējums palīdz no plašā ideju saraksta atlasīt perspektīvākās, kuras virzīt tālākai detalizētai analīzei.

Ir ieteicams dokumentēt gan sākotnējo ideju sarakstu, gan izvērtējuma rezultātus. Tas nodrošina caurskatāmību, ļauj noraidītās idejas atkārtoti izvērtēt vēlāk.

2.2. Padziļināta idejas analīze un MI riska noteikšana

Nākamais solis pēc ideju atlases ir padziļināti izvērtēt, kādu pieeju uzdevuma risināšanai lietot un kādam riska līmenim izvēlētais MI risinājums atbilst. Šim nolūkam izmanto lēmumu kokus.

Piemērotākās pieejas izvēle – ar **4. pielikumā** ietverto lēmumu koku iestāde noskaidro, kā konkrētais uzdevums labāk risināms:

- **automatizācija**, ja tas ir vienkāršs un atkārtots process (piemēram, procesu robotizācija vai biznesa noteikumu dzinēji);
- **datu analītika**, ja galvenais mērķis ir apkopot, izprast vai vizualizēt esošos datus;
- **MI risinājums**, ja nepieciešama prognozēšana, pielāgošanās vai jauna satura radīšana.

Detalizētāks alternatīvo pieeju skaidrojums atrodams **6. pielikumā.**

MI risinājuma riska un prasību noteikšana – ja izvēlēts uzdevumam izmantot MI risinājumu, ar **5. pielikumā** ietverto lēmumu koku tiek noteikts riska līmenis atbilstoši MI Aktam. Līdz ar riska kategorijas noteikšanu jānoskaidro arī, kādas prasības risinājuma izstrādei un lietošanai ir obligātas katrā gadījumā.

Papildu noteikumi sabiedrībai sniegtajos pakalpojumos – ja MI risinājums tiek izmantots publiskajos pakalpojumos, īpaši svarīga ir precizitāte, uzticamība un pamattiesību ievērošana. Tāpēc papildus riska noteikšanai jāievēro šādi praktiskie principi:

- **MI nedrīkst aizstāt cilvēka vadītu lēmuma pieņemšanas procesu, ja lēmums var ietekmēt personas pamattiesības vai radīt juridiskas sekas**. Izņēmumi ir gadījumi, kad automatizētu lēmumu pieņemšanu atļauj normatīvie akti (piem., fotoradaru fiksēti administratīvie pārkāpumi). Taču arī šādos gadījumos jānodrošina cilvēka kontrole, vismaz paredzot pārsūdzības iespējas.
- **Klientu atbalsta čatboti.** Ja tiek izmantoti MI čatboti, lietotājiem jābūt skaidri informētiem, ka atbildes sagatavojis MI un ka tās ir informatīvas, nevis juridiski saistošas. Jānodrošina iespēja sarežģītākos gadījumos sazināties ar cilvēku.
- **MI izmantojams kā atbalsta rīks.** MI drīkst izmantot analīzes, kopsavilkumu vai priekšlikumu sagatavošanai, bet gala lēmumu vienmēr pārbauda un pieņem cilvēks, ja vien normatīvajos aktos nav paredzēts citādāk. Tas ir īpaši svarīgi, ja lēmums var ietekmēt personas pamattiesības vai radīt juridiskas sekas.
- **Caurskatāmība.** Iedzīvotājam vienmēr ir tiesības zināt, vai ar viņu sazinās cilvēks vai MI, kā arī saņemt skaidrojumus par to, kāda ir MI loma gala rezultātā.

Rezultātā no plašā ideju saraksta tiek izvēlētas dažas perspektīvākās (parasti 2–3), kuras iestāde virzīs kā uzdevumus MI risinājumu izstrādei vai ieviešanai. Šīs idejas ir jānoformulē skaidros uzdevumu aprakstos, norādot:

- risināmo problēmu vai iespēju;
- īsu lietotāja stāstu par to, kā risinājums darbosies praksē;
- plānoto pieeju (automatizācija, datu analītika vai MI);
- sagaidāmo izmērāmo ieguvumu.

2.3. Sadarbība un tālākā rīcība

Kad piemērotā pieeja ir izvēlēta un MI risinājuma riska līmenis noteikts, iestāde var pāriet uz nākamo posmu – risinājuma pārbaudi un ieviešanu, kā aprakstīts **3. nodaļā**.

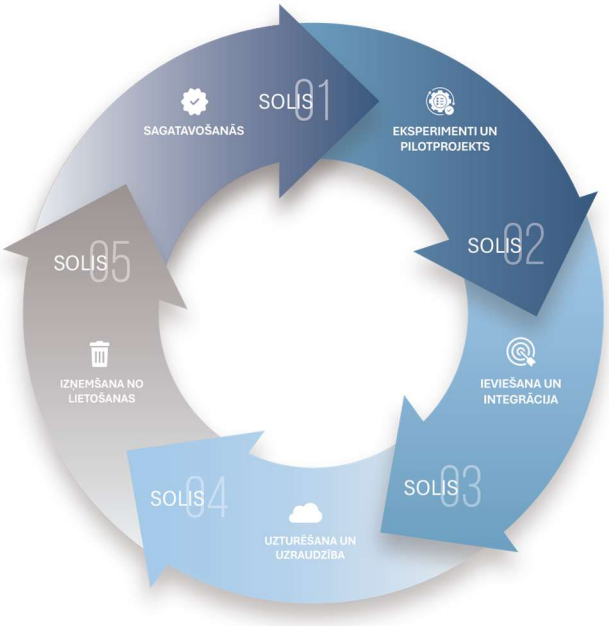
Lai arī konkrētu MI risinājumu izvēle un ieviešana ir katras atsevišķas iestādes pārziņā, citas iestādes var sniegt nozīmīgu atbalstu uzdevumu atlasē un risinājumu izvēlē. Daudzi uzdevumi ir līdzīgi dažādās iestādēs, tādēļ pieredzes apmaiņa un sadarbība var veicināt, atvieglot un paātrināt MI risinājumu ieviešanu.

- **Prakses kopienas.** Vairākās iestādēs jau veidojas MI prakses kopienas resoru ietvaros. Tās ļauj darbiniekiem dalīties ar praktisku pieredzi, testēt jaunos MI rīkus un apzināt tipiskākās problēmas.
- **Pieredzes apmaiņa starp iestādēm.** Regulāras diskusijas par veiksmīgiem un neveiksmīgiem pilotprojektiem palīdz citām institūcijām no tiem mācīties un izvairīties no kļūdām.
- **Koplietojami risinājumi.** Iestādes var attīstīt MI risinājumus sadarbībā vai pārņemt jau pārbaudītus risinājumus no citām institūcijām. Tas paātrina ieviešanu, samazina izmaksas un nodrošina vienotus kvalitātes un kiberdrošības standartus.

Šāda sadarbības kultūra ļauj efektīvāk izmantot resursus, mazināt riskus un paātrināt uzticamu MI risinājumu ieviešanu publiskajā pārvaldē.

3. MI risinājuma dzīves cikla metodika

Mākslīgā intelekta (MI) risinājuma ieviešana iestādē ir pakāpenisks process, kas sākas ar gatavības izvērtējumu un turpinās ar eksperimentiem, pilotprojektiem un plašāku ieviešanu (skat. 2. attēls). Šī metodika palīdz samazināt riskus, nodrošināt atbilstību normatīvajām prasībām un sasaistīt iniciatīvas ar iestādes stratēģiskajiem mērķiem. Katrs posms sniedz praktisku pieredzi, kas ir vērtīga neatkarīgi no tā, vai risinājums tiek ieviests tālāk.



2. attēls. MI risinājuma dzīves cikla posmi

3.1. Sagatavošanās

MI risinājumi nav vienreizēji projekti, bet ilgtermiņā lietojamas sistēmas, kurām nepieciešama regulāra uzraudzība, uzturēšana un atjaunināšana. Tāpēc jau sagatavošanās posmā ir būtiski skatīt MI risinājuma ieviešanu kā dzīves ciklu – no sagatavošanās līdz uzturēšanai un izņemšanai no lietošanas.

MI risinājuma ieviešana nav tikai tehnoloģisks projekts, bet pārmaiņu process visā iestādē. Pirms uzsākt jebkuru iniciatīvu, iestādei jāizvērtē sava gatavība un jānodrošina, ka pastāv skaidri priekšnoteikumi datu, kompetenču, resursu un vadības atbalsta ziņā.

Svarīgākie sagatavošanās elementi:

- **Vadības iesaiste un stratēģiskais ietvars.** Iestādes vadībai jādefinē, kā MI projekti atbilst iestādes stratēģiskajām prioritātēm, kādi ir sagaidāmie ieguvumi un kas ir atbildīgie par MI projektu īstenošanu. Bez vadības mandāta MI iniciatīvas mēdz būt fragmentāras un īslaicīgas.

- **Datu gatavība un drošība.** MI risinājumus darbina ar datiem, tāpēc to kvalitātei un pieejamībai ir būtiska nozīme, īpaši tāpēc, lai novērstu aizspriedumus un tiešas vai netiešas diskriminācijas riskus. Ja dati ir nepilnīgi, MI var palīdzēt tos uzlabot, taču jo kvalitatīvāki dati sākumā, jo labāks un uzticamāks rezultāts. Papildus tam, jebkurā gadījumā vienmēr ir jāidentificē, kāda veida dati tiek izmantoti, un jāievēro šādu datu izmantošanai un glabāšanai normatīvajos aktos noteiktās prasības.
- **Darbinieku kompetences un apmācības.** Sagatavošanās posmā darbiniekiem jānodrošina pamata izpratne par MI iespējām, riskiem un lietošanas noteikumiem. Konkrētu rīku apmācības veic pēc risinājuma izvēles un resursu apzināšanas. Sarežģītiem projektiem nepieciešamas specializētas lomas (datu, kiberdrošības un MI risinājumu ieviešanas speciālisti, juristi un projektu vadītāji), kuru kompetences var nodrošināt ar apmācībām vai ārpakalpojuma ceļā.
- **Iekšējās kapacitātes un resursi.** Iestādei jāizvērtē, kādi cilvēkresursi, finansējums un infrastruktūra ir pieejami. Produktivitātes rīku ieviešanai parasti pietiks ar esošajiem resursiem, bet lielāki projekti prasa ilgtermiņa investīcijas un skaidru resursu plānošanu.
- **Cilvēka kontrole.** Ja MI risinājums ietekmē pamattiesības vai rada juridiski saistošus lēmumus, pašā lēmuma pieņemšanas procesā vai arī pēc lēmuma pieņemšanas obligāti jānodrošina cilvēka kontrole (*human-in-the-loop*). Viens no veidiem, kā to nodrošināt, ir ieviest piemērotus un efektīvus pārsūdzības vai ziņošanas mehānismus.
- **Atbalsta mehānismi.** Jāizmanto pieejamās ekspertu kopienas un pieredzes apmaiņas tīkli ministriju vai valsts līmenī, kā arī jāseko labo prakšu katalogiem[12] un centralizēti pieejamiem rīkiem.[13]

Lomas un komanda

MI projektu ieviešana prasa skaidru atbildību un sadarbību starp dažādām lomām. Komanda var būt neliela, bet tai jāaptver noteiktas kompetences un atbildībām jābūt skaidri sadalītām, kā arī ir jānozīmē par MI projekta vadīšanu atbildīgā persona.

- **Vadība** – nosaka stratēģiju, nodrošina atbildību un resursus.
- **Datu speciālisti/analītiķi** – veic sagatavošanu, analīzi un nodrošina tehnisko pamatu.
- **Juristi** – identificē piemērojamos normatīvos aktus un nodrošina to prasību izpildi, t. sk. augsta riska MI sistēmām veic MI Aktā noteikto ietekmes uz pamattiesībām novērtējumu.
- **Datu aizsardzības speciālisti** – novērtē izmantojamo datu klasifikāciju un veic pasākumus, lai izpildītu attiecīgo datu izmantošanai noteiktās normatīvo aktu prasības, t. sk. nepieciešamības gadījumā veic VDAR noteikto novērtējumu par ietekmi uz datu aizsardzību.
- **Kiberdrošības speciālisti** – pārrauga kiberdrošību un piekļuves kontroli.

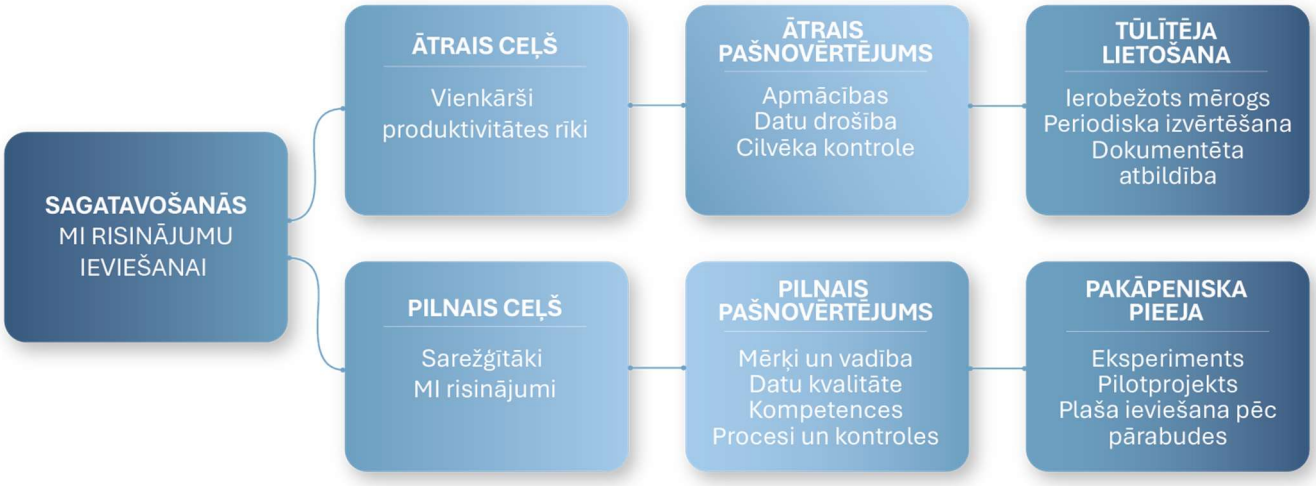
[12] Viedās administrācijas un reģionālās attīstības ministrija, *Mākslīgais intelekts valsts pārvaldē,* https://www.varam.gov.lv/lv/maksligais-intelekts-valsts-parvalde.
[13] Hugo.lv, https://hugo.lv/lv.

- **Procesa īpašnieki/turētāji** – iesaistās uzdevumu atlasē un izvērtēšanā un skaidro procesus, lai MI risinājumi jēgpilni iekļautos procesos.
- **Praktiskie lietotāji (gan iekšējie, gan ārējie)** – testē risinājumu, sniedz atgriezenisko saiti un palīdz pieņemt to lietošanā.

Šādas komandas kompetences nodrošina, ka MI projekti tiek virzīti ne tikai kā tehnoloģiski, bet gan kā organizācijas un lietotāja vajadzībām atbilstoši projekti, kā arī ieviesto MI risinājumu atbilstību normatīvo aktu prasībām.

Iestādes gatavības pašnovērtējums

Pirms pāriet uz nākamo posmu – eksperimentiem un pilotprojektiem – iestādei jāveic pašnovērtējums, lai noteiktu, cik tā ir gatava MI risinājuma ieviešanai. Pastāv divi ceļi (skat. 3. attēlu).



3. attēls. Sagatavošanās ceļi MI risinājuma ieviešanai: ātrais un pilnais

- **Ātrais ceļš** attiecas uz vienkāršiem produktivitātes rīkiem (piemēram, dokumentu kopsavilkumi, e-pasta uzmetumi, tulkošana). Šādā gadījumā pietiek ar **ātro pašnovērtējumu**, kas pārbauda:
  - vai darbinieki ir apmācīti;
  - vai tiek ievērotas datu drošības prasības;
  - vai gala rezultātu pārbauda cilvēks.
- **Pilnais ceļš** attiecas uz sarežģītākiem MI risinājumiem. Šeit nepieciešams padziļināts **pilnais pašnovērtējums**, kas ietver:
  - risinājuma atbilstību stratēģiskajiem mērķiem;
  - datu kvalitāti un pieejamību;
  - kompetenču un resursu nodrošinājumu;

- procesus un iekšējās kontroles.

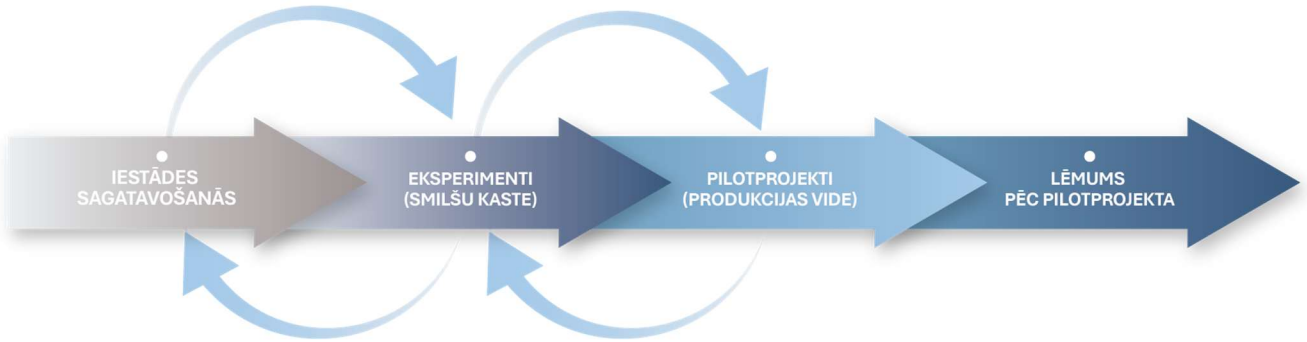
Pašnovērtējums jāskata kā pirmais solis visā MI risinājuma dzīves ciklā. Tas ne tikai palīdz pieņemt lēmumu par eksperimentiem, bet arī nodrošina, ka jau sākumā iestāde domā par uzturēšanu, uzraudzību un ilgtspējīgu risinājuma izmantošanu.

Ātrais un pilnais iestādes pašnovērtējums MI risinājuma ieviešanai aprakstīts **7. pielikumā**.

3.2. Eksperimenti un pilotprojekti

Eksperimenti un pilotprojekti ir centrālais instruments MI risinājuma drošai ieviešanai. Process ir iteratīvs – ja tiek atklāti trūkumi, iespējams atgriezties pie iepriekšējiem posmiem (skat. 4. attēlu). Atšķirība starp eksperimentiem un pilotprojektiem:

- **Eksperimenti** notiek drošā testēšanas vidē ("smilšu kastēs"), izmantojot simulētus vai anonimizētus datus. Mērķis ir ātri pārbaudīt ideju un nepieciešamības gadījumā uzlabot risinājuma pieeju vai prototipu.
- **Pilotprojektus** īsteno produkcijas vidē ar reāliem datiem, bet ierobežotā mērogā. To mērķis ir praksē novērtēt risinājuma darbību, identificēt riskus un gūt pieredzi tālākiem uzlabojumiem.



4. attēls. MI risinājumu sagatavošanas, eksperimentu un pilotprojekta posmi

Gan eksperimenti, gan pilotprojekti ir ne tikai īstermiņa pārbaudes posmi, bet arī svarīga dzīves cikla daļa, kas palīdz savlaicīgi atklāt riskus un nodrošina drošu pāreju uz ieviešanu un uzturēšanu. Lai eksperimenti un pilotprojekti būtu noderīgi, jāievēro vairāki principi:

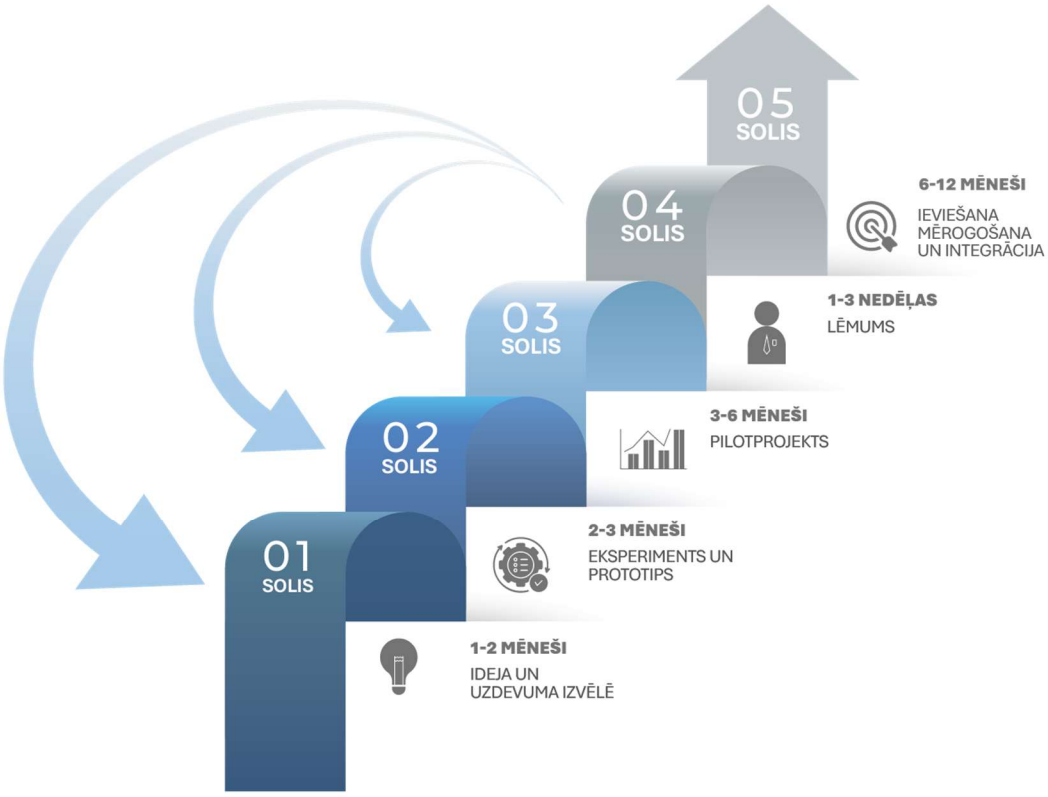
- Katrs risinājums jāsaista ar iestādes stratēģiskajām prioritātēm un sabiedrības vajadzībām, kuras tā apkalpo.
- Jānosaka izmērāmi panākumu kritēriji (piemēram, laika vai citu resursu ietaupījums, kļūdu samazinājums, klientu apmierinātība) un skaidri definēti tehniskie pieņemšanas kritēriji konkrētajam MI risinājumam (piemēram, dokumenta apstrāde 30 sekunžu laikā, teksta atpazīšana ar vismaz 80 % precizitāti).

- Jāveic mērījumi gan pirms, gan pēc pilotprojekta, lai izvērtētu rezultātu sasniegšanu.
- Projekta beigās jānovērtē projekta rezultāti un šis novērtējums ir jādokumentē.
- Nepieciešama atbilstoša komunikācija ar vadību, sabiedrību un kontrolējošām institūcijām.

Pat neveiksmīgs eksperiments vai pilotprojekts ir vērtīgs, ja iespējams skaidri parādīt, ka bija definēti izmērāmi mērķi un darbs tika veikts mērķtiecīgi. Tas stiprina uzticību un apliecina, ka iestāde mācās no pieredzes.

3.3. Ieviešana un integrācija

MI risinājuma ceļš no idejas līdz ieviešanai iestādes procesos notiek pakāpeniski (skat. 5. attēlu). Katrs posms balstās uz iepriekšējo, un tikai tad, ja attiecīgais posms novērtēts kā veiksmīgs, iespējams pāriet tālāk pie nākamā posma. Svarīgi atcerēties, ka process ir iteratīvs – ja kādā posmā tiek atklāti trūkumi, iespējams atgriezties pie iepriekšējā soļa. Tas ļauj mācīties no pieredzes un pakāpeniski uzlabot risinājumu.



5. attēls. Process no MI risinājuma idejas līdz ieviešanai

Pēc veiksmīgiem eksperimentiem vai pilotprojektiem iestāde var pieņemt lēmumu MI risinājumu ieviest plašākā mērogā. Šis posms nozīmē risinājuma integrāciju ikdienas procesos un pakalpojumos.

Ieviešanas laikā būtiski ir:

- nodrošināt, ka risinājuma lietošana atbilst iestādes stratēģiskajiem mērķiem un sabiedrības interesēm;
- nodrošināt skaidru komunikāciju ar darbiniekiem un lietotājiem par risinājuma mērķiem, iespējām un ierobežojumiem;
- dokumentēt ieviestā risinājuma darbību un rezultātus.

Ieviešana nav tikai tehnoloģiska ieviešana, bet arī pārmaiņu vadība organizācijā. Ir svarīgi nodrošināt darbinieku apmācības, procesu pielāgošanu un atbalsta mehānismus, lai risinājums tiktu lietots atbildīgi un lietderīgi.

Integrācija nozīmē arī to, ka MI risinājums kļūst par daļu no iestādes informācijas sistēmām un pakalpojumiem, kas prasa:

- integrāciju ar esošajiem datu un procesu pārvaldības mehānismiem;
- drošības un datu aizsardzības prasību ievērošanu;
- uzraudzības un atbildības punktu noteikšanu.

Šajā posmā jāparedz arī mehānismi atgriezeniskās saites saņemšanai no lietotājiem un sabiedrības, kā arī jāveic nepieciešamie uzlabojumi, lai risinājums būtu gan tehniski, gan funkcionāli ilgtspējīgs.

3.4. Uzturēšana un uzraudzība

Kad MI risinājums ir ieviests un integrēts, sākas ilgtermiņa posms – tā uzturēšana un uzraudzība. Šis posms ir būtisks, jo nodrošina risinājuma drošu un efektīvu darbību visā tā dzīves ciklā.

Uzturēšana nozīmē:

- regulārus programmatūras un modeļu atjauninājumus, lai tie saglabātu precizitāti un atbilstību normatīvajām prasībām;
- tehnisko atbalstu lietotājiem;
- procesu pielāgošanu, ja mainās normatīvie akti vai organizācijas vajadzības;
- drošības pārvaldību, t. sk. piekļuves kontroli un aizsardzību pret ļaunprātīgiem uzbrukumiem.

Uzraudzība un audits ietver:

- risinājuma darbības regulāru pārbaudi pret sākotnēji definētajiem mērķiem un panākumu kritērijiem;
- atbilstības pārbaudi normatīvajiem aktiem un iekšējām prasībām;
- dokumentācijas uzturēšanu, kas ļauj skaidri izsekot risinājuma darbībai un pieņemtajiem lēmumiem;

- lietotāju un sabiedrības atgriezeniskās saites ievākšanu un izmantošanu uzlabojumu veikšanai;
- neatkarīgu auditu pēc nepieciešamības – piemēram, ja risinājums ietekmē būtiskas sabiedrības intereses vai pamattiesības.

Šajā posmā svarīgi saglabāt caurskatāmību un nodrošināt, ka risinājums darbojas saskaņā ar iestādes mērķiem un sabiedrības interesēm. Uzturēšana un uzraudzība nav vienreizēji pasākumi, bet gan nepārtraukts process, kas nosaka risinājuma uzticamību ilgtermiņā.

3.5. Izņemšana no lietošanas

MI risinājumi nav paredzēti neierobežoti ilgai lietošanai. Kad risinājums vairs neatbilst iestādes vajadzībām, normatīvajām prasībām vai tehnoloģiskajām iespējām, jāpieņem lēmums par tā izņemšanu no lietošanas. Šajā posmā būtiski ir:

- **droši pārtraukt risinājuma darbību,** nodrošinot, ka dati un piekļuves tiek slēgti;
- **pārvaldīt uzkrātos datus,** tos arhivējot vai dzēšot atbilstoši normatīvajām prasībām;
- **informēt lietotājus un iesaistītās puses,** skaidrojot lēmuma iemeslus un piedāvājot alternatīvas, ja nepieciešams;
- **izvērtēt aizstājējus vai alternatīvus risinājumus,** ja funkcionalitāte joprojām ir vajadzīga;
- **dokumentēt lēmumu un procesu,** lai saglabātu pārskatāmību un pieredzi turpmākajiem projektiem.

Izņemšana no lietošanas ir tikpat nozīmīgs dzīves cikla posms kā ieviešana vai uzturēšana, jo tas nodrošina, ka risinājumi tiek pārvaldīti atbildīgi visā to izmantošanas laikā.

Visos MI risinājuma dzīves cikla posmos ir svarīga **dokumentēšana un caurskatāmība**. Iestādēs ir jāglabā dokumenti par mērķiem, testiem, izvērtējumiem, pārbaudēm un veiktajām izmaiņām. Gan iestādēm, gan sabiedrībai jābūt skaidram, kā un kāpēc risinājums tiek izmantots, un to iestādei ir jāspēj skaidrot un pamatot ar dokumentiem.

Detalizēts kontrolsaraksts ar obligātajiem soļiem un atbildīgajām lomām katrā dzīves cikla posmā pieejams šī dokumenta **8. pielikumā**.

Kopsavilkums. Dzīves cikla pieeja nodrošina, ka MI risinājums tiek pārvaldīts kā ilgtermiņa sistēma ar skaidru pārvaldību, caurskatāmību un pastāvīgu uzraudzību. Šāda pieeja veicina sabiedrības uzticēšanos, garantē drošību un nodrošina, ka MI risinājums atbalsta iestādes stratēģiskos mērķus visā tā lietošanas laikā.

4. Konkrētā MI risinājuma un piegādātāja izvēle

Mākslīgā intelekta (MI) risinājuma izvēle ir viens no izšķirošākajiem brīžiem projekta gaitā, jo tā tieši nosaka ieguvumus, drošību un iestādes reputāciju. Publiskajā pārvaldē risinājums jāizvēlas tā, lai tas vienlaikus būtu drošs, normatīvajiem aktiem atbilstošs, praktiski noderīgs iestādes stratēģisko mērķu sasniegšanai, kā arī ilgtspējīgs un izmaksu ziņā saprātīgs.

Bieži drošāk un saimnieciski izdevīgāk ir izmantot tirgū pārbaudītus un jau aprobētus MI rīkus un risinājumus, savukārt jaunu MI risinājumu izstrādi parasti būs pamatoti īstenot tikai tad, ja tirgū nav piemērotu alternatīvu vai ir nepieciešami būtiski tirgū pieejamo risinājumu pielāgojumi.

4.1. Izvēles kritēriji

Izvēloties MI risinājumu, iestādei ieteicams vērtēt šādus kritērijus:

- **Stratēģiskā atbilstība** – risinājums palīdz sasniegt iestādes stratēģiskos mērķus un risina reālu vajadzību, nevis tiek ieviests "tehnoloģijas dēļ".
- **Drošība un datu aizsardzība** – risinājums atbilst kiberdrošības, datu aizsardzības un iekšējās drošības prasībām.
- **Normatīvā atbilstība** – risinājums atbilst piemērojamo normatīvo aktu prasībām.
- **Lietojamība un uzticamība** – risinājums ir pārbaudīts praksē, ar pietiekamu dokumentāciju un lietotāju pieredzes apliecinājumiem.
- **Izmaksu un ieguvumu samērīgums** – jāizvērtē kopējās izmaksas, uzturēšanas prasības un ilgtermiņa ieguvumi.
- **Ilgtspēja un attīstība** – vai risinājumu iespējams paplašināt vai integrēt ar citām sistēmām, vai piegādātājs spēj nodrošināt atbalstu ilgtermiņā.

4.2. MI risinājumu izvietošanas pieeja

Pēc MI risinājuma izvēles saskaņā ar 4.1. nodaļas kritērijiem iestādei jāizvēlas piemērotākā izvietošanas pieeja, ņemot vērā tehnisko arhitektūru, datu aizsardzības un drošības prasības, licences nosacījumus un pieejamos resursus.

Šeit aprakstītas tipiskākās izvietošanas pieejas un būtiskie faktori, kas papildina risinājuma izvēles kritērijus, pievēršoties praktiskajai ieviešanai un uzturēšanai.

Izvietošanas pieeja	Piemēri
Publiskie bezmaksas rīki (tiešsaistes platformas) – Ātri izmantojami, bez licences maksas – Ievadītie dati tiek izmantoti modeļu apmācībai	*ChatGPT (free)*, *Bard*, *DALL·E* bezmaksas versija
Publiskie maksas rīki (SaaS, abonementi) – Pieejami ar licenci vai abonementu, kas nosaka lietošanas tiesības un ierobežojumus. – Bieži ļauj atteikties no datu izmantošanas modeļu apmācībai – Drošības līmenis atkarīgs no līguma nosacījumiem (DPA, SLA)	*ChatGPT Enterprise/Teams*, *Perplexity Pro*, *MidJourney* (maksas)
Integrētie pakalpojumu sniedzēju risinājumi – Mākoņpakalpojumi integrēti iestādes darba vidē – Nepieciešama līgumu izvērtēšana par drošību un auditu	*Microsoft Copilot (Office 365)*, *Google Workspace Duet AI*
Mākoņpakalpojumi ar atsevišķu klienta vidi (*tenant*) ES – Katram klientam izolēta vide kopējā infrastruktūrā – Dati glabājas un tiek apstrādāti tikai ES teritorijā	*Azure OpenAI Service* (EU datu centri), *Amazon Bedrock* (ES serveri)
Lokāli izvietoti risinājumi (*on-premise*) – Maksimāla kontrole pār datiem un sistēmām – Apstrāde notiek iestādes serveros vai valsts mākonī	Atvērtā koda MI modeļi (*TildeOpen*, *LLaMA*, *Falcon*, *Mistral*)
Hibrīdie risinājumi – Apvieno lokālo un mākoņvides elementus	Lokāla apstrāde kombinācijā ar mākoņa API, piem., *Hugging Face* integrācija
Centralizētie valsts risinājumi – Koplietošanas platformas, ko uztur valsts līmenī	*Hugo.lv*
Eksperimentu un testēšanas vides (“smilšu kastes”) – Drošas vides ar anonimizētiem vai sintētiskiem datiem	Iestāžu, universitāšu iekšējās testēšanas platformas

Būtiskie izvēles faktori

Papildus 4.1. nodaļā minētajiem izvēles kritērijiem, izvēloties MI risinājuma izvietošanas pieeju, iestādei jāņem vērā šādi praktiskie faktori:

- **Informācijas pieejamības statuss** – publiski pieejama vai ierobežotas pieejamības informācija (personas dati, komercnoslēpums, iekšējie dokumenti, informācija ar klasifikāciju "dienesta vajadzībām").
- **Normatīvā atbilstība** – VDAR, Informācijas atklātības likums, kiberdrošības regulējums, MI akts.
- **Licences nosacījumi** – jāvērtē gan ievadīto datu apstrāde un glabāšana (vai tie tiek izmantoti modeļu apmācībai, vai glabāti ārpus ES), gan arī radītās informācijas tālākas izmantošanas tiesības (vai ģenerēto saturu drīkst izmantot oficiālai komunikācijai, vai tas nav ierobežots ar autortiesībām).
- **Datu drošība un glabāšanas vieta** – vai dati apstrādāti tikai ES/NATO serveros, vai nodrošināta šifrēšana un piekļuves kontrole.
- **Līguma un atbildības nosacījumi** – DPA, SLA, incidentu pārvaldība, atbildības sadalījums.
- **Izmaksas un resursi** – licences, uzturēšanas izmaksas, iestādes kapacitāte.
- **Tehniskās iespējas un mērogojamība** – integrācija ar esošajām sistēmām, paplašināmība nākotnē.
- **Caurspīdīgums un uzraudzība** – auditējamība, uzskaites iespējas, sabiedrības uzticēšanās.

4.3. Iepirkuma process

Izvēloties iepirkuma procedūru MI risinājumu iegādei, ir jāvadās pēc Publisko iepirkumu likuma prasībām, paturot prātā turpmāk norādītās MI risinājumu ieviešanas un izmantošanas īpatnības.

MI risinājumi no klasiskiem IT risinājumiem atšķiras ar to, ka šeit īpaši svarīga ir praktiska pārbaude un risinājuma piemērotības izvērtēšana pirms ieviešanas plašākā mērogā. Tas palīdz samazināt riskus, novērst neefektīvas investīcijas un nodrošināt, ka iegādātais risinājums patiešām atbilst iestādes vajadzībām un normatīvo aktu prasībām.

MI risinājumu iegādē, ciktāl to atļauj normatīvo aktu prasības, ieteicams izmantot šādas praksē pārbaudītas pieejas:

- **Lietotāju stāsti un vajadzību apraksti** – prasības formulē, balstoties uz reālām biznesa vajadzībām un lietotāju scenārijiem, nevis tikai tehniskajām specifikācijām.
- **Pilotprojekts kā daļa no iepirkuma** – ļauj pārbaudīt risinājumu ierobežotā apjomā, testēt to praksē ar reāliem datiem un pārliecināties par tā drošību, lietojamību un atbilstību normatīvajām prasībām.

- **Vērtēšanas kritēriju daudzpusība** – papildus izmaksām un tehniskajām prasībām jāvērtē arī datu drošība, caurskatāmība, ilgtermiņa uzturēšana, integrējamība ar citām sistēmām un piegādātāja spēja nodrošināt atbalstu.
- **Inovācijas publiskais iepirkums**[14] – orientēts uz iestāžu darbības efektivitātes paaugstināšanu, procesu optimizāciju un pieprasījuma veidošanu pēc inovatīviem risinājumiem, kur pieprasītājs rīkojas kā sākuma klients attiecībā uz inovatīvām precēm, procesu vai pakalpojumiem, kas vēl nav pieejami plašā komerciālā mērogā.

4.4. Līguma nosacījumi un sadarbība ar piegādātājiem

Līgums par MI risinājuma iegādi un/vai uzturēšanu sagatavojams un noslēdzams, ievērojot Publisko iepirkumu likuma prasības. Sagatavojot līguma projektu, jāraugās, lai tas nodrošinātu ilgtermiņa drošību, uzticamību un iestādes intereses. Līguma noteikumi katrā konkrētā situācijā atšķirsies, ievērojot izvēlētā MI risinājuma un tā ieviešanas īpatnības. Taču jebkurā gadījumā ir jāraugās, lai līgums paredz pietiekamu elastību reaģēt uz iepriekš neparedzētiem apstākļiem, kas atklājušies tikai līguma izpildes laikā, lai pēc iespējas atrastu risinājumu šādām situācijām un sekmīgi ieviestu MI risinājumu, bet gadījumā, ja tas esošā līguma ietvaros nav iespējams, rīkotos saimnieciski, t. sk. izbeigtu līgumu.

Līgumā par MI risinājuma iegādi un/vai uzturēšanu ieteicams pievērst uzmanību šādiem jautājumiem un tos noregulēt līgumā, ciktāl to pieļauj Publisko iepirkumu likums:

- **Uzturēšana.** Piegādātājam būtu jānodrošina regulāri atjauninājumi, kļūdu novēršana un drošības uzlabojumi.
- **Datu aizsardzība.** Līgumā būtu jāiekļauj noteikumi par datu apstrādi, glabāšanu un drošību, pielāgojot tos izmantoto datu veidam un normatīvo aktu prasībām.
- **Dokumentācija un apmācības.** Piegādātājam būtu jānodrošina sistēmas lietošanas dokumentācija, darbinieku apmācības, kā arī atbilstības sertifikāti un citi nepieciešamie apliecinājumi (t. sk. apliecinājumi par informācijas apstrādi).
- **Atbildība par rezultātiem.** Līgumā būtu jāietver noteikumi par atbildību par MI risinājuma kvalitāti un pareizu darbību, nodefinējot, kādos apstākļos atbildība jānes iestādei un kādos – piegādātājam. Līgumā būtu jāparedz, kā šī atbildība īstenojama, t. sk. kā novēršami defekti.
- **Līguma priekšmets.** Vēlams līgumā paredzēt noteikumus, kas līguma izpildes laikā nepieciešamības gadījumā ļauj veikt precizējumus darba uzdevumā/specifikācijā, lai sasniegtu iecerēto rezultātu.

[14] Vairāk informāciju meklēt: Iepirkumu uzraudzības birojs, *Inovācijas publiskais iepirkums*, https://www.iub.gov.lv/lv/inovativais-iepirkums; Ekonomikas ministrija, *Vadlīnijas inovāciju iepirkuma īstenošanai*, https://www.em.gov.lv/lv/media/11394/download; Ekonomikas ministrija, *Inovācijas iepirkums. Būtiskākais*, https://www.em.gov.lv/sites/em/files/inovacijas20iepirkums_butiskakais1_0.pdf.

- **Līguma izbeigšana.** Līgumā būtu jāparedz kārtība defektu novēršanai un nosacījumi līguma izbeigšanai gadījumos, kad piegādātājs būtiski nepilda saistības vai risinājums atkārtoti neatbilst līguma specifikācijai un drošības prasībām.
- **Modeļu izmantošana.** Ieteicams paredzēt iespēju izmantot vairākus MI modeļus (multimodeļu pieeja) vai aizstāt izmantoto modeli ar citu, saskaņojot to ar pasūtītāju. Izvēloties vai mainot modeli, būtu jāveic tā piemērotības, priekšrocību, trūkumu un ierobežojumu izvērtējums, nodrošinot risinājuma atbilstību iestādes vajadzībām un drošības prasībām.
- **Elastība un nākotnes attīstība.** Līgums būtu jāveido tā, lai tas pēc iespējas ļautu paplašināt risinājuma izmantošanu vai integrēt to ar citiem rīkiem un sistēmām. Tas palīdzētu izvairīties no pārmērīgas atkarības no viena piegādātāja un nodrošinātu risinājuma ilgtspēju.
- **Audita tiesības.** Līgums var paredzēt iestādes tiesības veikt auditu vai pieprasīt neatkarīgu pārbaudi, lai pārliecinātos par piegādātāja atbilstību datu aizsardzības, drošības un kvalitātes prasībām. Šāds nosacījums ir īpaši noderīgs lielākiem vai kritiskiem projektiem, bet var nebūt nepieciešams mazākiem produktivitātes rīkiem.

5. Droša MI lietošana iestādēs

Šajā nodaļā izklāstīti galvenie principi drošai un atbildīgai mākslīgā intelekta (MI) rīku izmantošanai publiskajā pārvaldē. Norādītie principi ir vienoti un piemērojami visām iestādēm, taču detalizētus lietošanas nosacījumus, tostarp to, kāda informācija drīkst tikt izmantota konkrētos MI rīkos un kādi ierobežojumi ir spēkā, nosaka katra iestāde pati, balstoties uz risku izvērtējumu un balto sarakstu.

5.1. MI rīku izvēle un informācijas apstrāde

MI rīku izvēle un lietošana ir iestādes atbildība. Pirms konkrēta MI risinājuma ieviešanas vai lietošanas iestādei ir jāiepazīstas ar tā licences noteikumiem un jānovērtē tā atbilstība drošības un normatīvo aktu prasībām, kā arī jāizvērtē piegādātāja uzticamība. Tikai pēc šādas izvērtēšanas rīku drīkst iekļaut iestādes **baltajā sarakstā** un noteikt tā lietošanas nosacījumus.

Apstiprināti MI rīki ir tikai tie risinājumi, kas iekļauti baltajā sarakstā, un tos drīkst izmantot darba vajadzībām saskaņā ar iestādes noteiktajiem ierobežojumiem un mērķiem. **Neapstiprināti MI rīki** (gan bezmaksas, gan maksas), kas nav iekļauti baltajā sarakstā, darba vajadzībām nav izmantojami, izņemot gadījumus, kad iestāde iekšējos noteikumos ir skaidri paredzējusi to lietošanu (piemēram, publiskas informācijas apstrādei vai testēšanai).

Šie ir vispārējie principi informācijas ievadīšanai un apstrādei MI rīkos. Iestādēm tie jāievēro un jāizmanto tos kā pamatu iekšējo noteikumu izstrādei:

- **Publiski pieejamas informācijas izmantošana** – pēc noklusējuma publisku informāciju drīkst apstrādāt ar MI rīkiem, ja iestāde nav noteikusi citus ierobežojumus.
- **Informācija, kurai ir noteikti ierobežojumi un papildu aizsardzības prasības** – personas datu, ierobežotas pieejamības informācijas un citas normatīvajos aktos aizsargātas informācijas izmantošanu ar MI rīkiem drīkst veikt tikai tādā apjomā un kārtībā, kādu nosaka iestādes iekšējie noteikumi.
- **Baltā saraksta prioritāte** – iestādes baltais saraksts ir galvenais praktiskais instruments MI rīku lietošanas noteikšanai, taču tā saturam vienmēr jāatbilst normatīvo aktu prasībām.

Darbiniekiem jāvar paļauties uz iestādes balto sarakstu un iekšējiem normatīvajiem aktiem. Viņiem pašiem nav jāvērtē rīku atbilstība – atbildība par baltā saraksta uzturēšanu un aktualizēšanu gulstas uz iestādi.

Šāda pieeja nodrošina, ka darbiniekiem ir pieejami skaidri saprotami un vienkārši MI izmantošanas principi, bet iestādes var elastīgi precizēt lietošanas noteikumus atbilstoši savām vajadzībām, riskiem un resursiem.

Lai darbiniekiem būtu vieglāk pieņemt ikdienas lēmumus, iestādei ieteicams izveidot **datu izmantošanas orientierus** – īsas un viegli saprotamas tabulas, kas kalpo kā praktisks atgādinājums par to, kādu informāciju drīkst vai nedrīkst ievadīt konkrētos MI rīkos. Orientieri ir jāizstrādā katram apstiprinātajam rīkam, lai darbiniekiem būtu praktisks atgādinājums par atļauto un aizliegto informāciju.

Piemērs – datu izmantošanas orientieris tiešsaistes bezmaksas prezentāciju ģenerēšanas rīkam.

Drīkst ievadīt	Nedrīkst ievadīt	Īpašie noteikumi
Publiskus dokumentus un datus (piem., iestādes mājaslapā publicētus paziņojumus, preses relīzes, publiskus statistikas datus)	Personas datus (piem., vārdi, personas kodi, kontaktinformācija)	Pirms izmantošanas prezentācijā pārbaudīt faktu pareizību

5.2. Droša ģeneratīvā MI rīku lietošana

Ģeneratīvā MI rīki (piemēram, teksta, attēlu vai koda ģenerēšanai) arvien biežāk tiek izmantoti ikdienas darbā. Tie var sniegt ātrus rezultātus, taču ir būtiski apzināties to ierobežojumus. Papildus vispārējiem principiem, ģeneratīvā MI rīkiem ir specifiski riski, kam jāpievērš īpaša uzmanība.

Darbiniekam jāapzinās trīs galvenie riski, lietojot ģeneratīvā MI rīkus:

- **Darbības nav anonīmas.** Katrs ievades vai ģenerēšanas solis var tikt reģistrēts un redzams rīka piegādātājam vai sistēmas pārvaldniekiem. Tas nozīmē, ka darbinieka darbības var tikt izsekotas, tāpēc MI rīkos nedrīkst ievadīt informāciju, kuras noplūde varētu radīt drošības vai reputācijas riskus iestādei.
- **Informācija var tikt saglabāta un izmantota ārpus iestādes kontroles.** Rīka piegādātājs var glabāt ievadītos datus un izmantot tos, piemēram, modeļu apmācībai vai pakalpojuma uzlabošanai. Tas var radīt risku, ka informācija kļūst pieejama ārpus iestādes vai tiek atklāta trešajām personām neatbilstošā kontekstā.
- **Ģenerētais saturs nav uzskatāms faktos balstītu.** Tas tiek radīts, balstoties uz līdzībām ar apmācības datiem, nevis veicot reālu informācijas pārbaudi. Tādēļ saturs var būt nepilnīgs, neprecīzs vai maldinošs (“halucinācijas”), un pirms izmantošanas tas vienmēr ir rūpīgi jāpārbauda.

Ģeneratīvā MI rīkus drīkst izmantot tikai saskaņā ar iestādes baltajā sarakstā vai iekšējos noteikumos paredzētajiem nosacījumiem. Darbiniekiem jāievēro šāda trīs soļu pieeja:

1. Droša datu ievade

- Lieto tikai tos rīkus, kas atļauti iestādes baltajā sarakstā vai noteikumos.
- Ievadi tikai tādu informāciju, ko iestāde ir atļāvusi šajā rīkā; ja datiem normatīvajos aktos ir paredzēti īpaši izmantošanas un aizsardzības noteikumi, tos ievadi tikai tad, ja rīks tam ir apstiprināts un drošs.
- Anonimizē vai aizstāj datus, ja iespējams.
- Ievadi tikai tik maz informācijas, cik nepieciešams uzdevuma veikšanai.

Piemērs praksē: pirms dokumenta augšupielādes darbinieks pārbauda, vai rīks ir baltajā sarakstā un vai dokumenta saturu drīkst izmantot šajā rīkā.

2. Rezultātu pārbaude

- Uztver ģeneratīvā MI rīka radīto saturu kā uzmetumu vai melnrakstu, nevis gatavu rezultātu.
- Pārbaudi faktus, skaitļus un atsauces uzticamos avotos.
- Novērtē, vai saturs ir pilnīgs un atbilst uzdevuma mērķim.
- Pārliecinies, ka saturs atbilst iestādes noteikumiem un normatīvajiem aktiem.
- Ja rodas šaubas, konsultējies ar kolēģi vai lietpratēju.

Piemērs praksē: MI sagatavotā atbildē uz iesniegumu darbinieks pārbauda visus faktus oficiālajos reģistros un atsauces uz normatīvajiem aktiem salīdzina ar normatīvo aktu teksta oriģinālu, pirms paraksta vēstuli.

3. Rezultāta akcepts un izmantošana

- Pārskati un rediģē saturu, nodrošinot, ka tas ir precīzs, korekts un atbilstošs normatīvajiem aktiem.
- Ievēro autortiesības un licencēšanas noteikumus (īpaši attēliem un vizuāliem materiāliem).
- Atzīmē gadījumus, kad saturs sagatavots ar MI rīka palīdzību, ja to prasa ārējie normatīvie akti vai iestādes noteikumi.
- Publiskai saziņai izmanto tikai saturu, kas ir pārbaudīts un saskaņots iestādes iekšējos normatīvajos aktos noteiktajā kārtībā.
- Ja MI rīks tiek izmantots klientu apkalpošanā, lietotājam jābūt informētam par MI iesaisti un jānodrošina iespēja saņemt atbildi no cilvēka.

Piemēri praksē: prezentācijā izmanto tikai licencētus attēlus (tai skaitā MI ģenerētus); pie melnraksta pievieno piezīmi "daļa teksta sagatavota ar [rīka nosaukums]"; pirms publicēt rakstu iestādes mājaslapā, darbinieks pats izlabo un apstiprina tekstu.

Piezīme darbiniekiem: ārējo normatīvo aktu (piemēram, MI akta, VDAR) prasības iestāde atspoguļo savos noteikumos un baltajā sarakstā. Darbiniekam pietiek sekot iestādes noteikumiem; neskaidrību gadījumā jāvēršas pie atbildīgās personas (piemēram, datu aizsardzības speciālista).

5.3. Atbalsts, apmācības un drošības kultūra

Droša MI lietošana nav tikai tehnoloģiju jautājums – tā ir iestādes organizācijas kultūras sastāvdaļa. Darbiniekiem jābūt pārliecinātiem, ka viņiem ir pieejamas zināšanas, praktisks atbalsts un skaidra atbildības sadale.

Apmācības un atbalsts. Darbinieku apmācībai par MI drošu lietošanu jāizmanto visi pieejamie veidi – gan valsts līmeņa, gan iestādes organizētie. Darbiniekiem jābūt pieejamām arī rokasgrāmatām un atgādnēm (piemēram, iekštīklā vai drukātā veidā). Jānodrošina skaidri atbalsta kanāli jautājumiem un problēmām (IT, datu aizsardzība, kiberdrošība), kā arī vienkāršs mehānisms incidentu ziņošanai. Vērtīgi ir atbalstīt arī "MI čempionus" – darbiniekus, kas palīdz kolēģiem apgūt drošu un atbildīgu lietošanu, kā arī veicināt pieredzes apmaiņu starp iestādēm.

Vadības stratēģiskā loma. Vadībai jāuzņemas līderība drošas lietošanas kultūras ieviešanā – tas nozīmē ne tikai pieņemt noteikumus, bet arī tos ikdienā ievērot un demonstrēt. Regulāri jāpārvērtē, vai baltā saraksta saturs un iekšējie noteikumi joprojām ir aktuāli, un jānodrošina resursi apmācībām, atbalstam un drošības uzlabošanai ilgtermiņā.

Praktiskai ikdienas lietošanai šo nodaļu papildina pielikumi:

- **9. pielikums. Ātrā atgādne "Dari / Nedari"** – koncentrēts pārskats ar galvenajiem principiem drošai MI lietošanai.
- **10. pielikums. Seši noteikumi darbiniekiem MI rīku lietošanā** – skaidrs atgādinājums par pamatnoteikumiem, kas jāievēro, strādājot ar MI.
- **11. pielikums. Ģeneratīvā MI rīku izmantošanas atgādne darbiniekam** – praktisks ceļvedis darbiniekiem drošai un atbildīgai ģeneratīvā MI lietošanai ikdienas darbā.
- **12. pielikums. Valsts administrācijas skolas mācību un pasākumu piedāvājums MI jomā** – detalizēts piedāvājuma apraksts ar saitēm uz papildu resursiem.

6. Praktiskie scenāriji un piemēri

Šī nodaļa sniedz ilustratīvus piemērus, kā mākslīgā intelekta (MI) risinājumus var izmantot valsts pārvaldē. Tie palīdz saprast, kuros procesos MI risinājumi sniedz ātru ieguvumu, kādi riski jāņem vērā un kādas kļūdas nedrīkst pieļaut. Papildus scenārijiem iekļauta arī detalizēta gadījuma analīze – MI risinājuma ieviešana LATAK akreditācijas procesā (**13. pielikums**).

6.1. Scenāriji publiskajā pārvaldē

MI risinājumus iestādes visbiežāk izmanto **iekšējiem procesiem**, kur riski ir zemāki un ieguvumi – tūlītēji. Savukārt **sabiedrībai sniegtajos pakalpojumos** riska līmenis pieaug, jo tiek skartas personas tiesības un sabiedrības uzticība publiskajai pārvaldei.

Tabulā apkopoti biežāk sastopamie scenāriji, norādot praktiskos ieguvumus un ilustratīvus piemērus no Latvijas publiskās pārvaldes. Šis apkopojums kalpo kā orientieris, lai iestādes vadība un speciālisti ātri identificētu, **kur MI var nest lielāko pievienoto vērtību**. Piemēru saraksts nav izsmeļošs – katra iestāde to var papildināt ar saviem piemēriem un specifiskiem lietojumiem.

Konteksts	Joma	Ieguvumi un kontroles mehānismi	Piemērs iestādē
Dokumentu melnraksti un kopsavilkumi	Iekšējie procesi	Taupa laiku, bet gala teksts obligāti jāpārskata darbiniekam (ģeneratīvais MI)	Valsts kontrole – MI palīdz sagatavot audita dokumentu uzmetumus
Dokumentu šķirošana/kārtošana (klasifikācija, strukturēšana)	Iekšējie procesi	Atvieglo apstrādi, bet nepieciešama kvalitātes kontrole (analītiskais MI)	—
Tulkojumi un valodas atbalsts	Iekšējie procesi	Ērti ikdienā, bet gala dokumentus apstiprina darbinieks vai valodas speciālists (ģeneratīvais MI)	*Hugo.lv* platforma – plaši izmantota publiskajā pārvaldē tulkošanai un runas atpazīšanai
Datu analīze un strukturēšana	Iekšējie procesi	Atklāj tendences, bet nepieciešama ekspertu pārbaude (analītiskais MI)	LATAK – MI risinājums KPI analīzei un efektivitātes uzlabošanai
Attēlu un datu vizuālā apstrāde (piem.,	Iekšējie procesi	Automatizē apstrādi, bet obligāta ekspertu validācija (analītiskais MI)	Valsts zemes dienests – MI izmanto kadastra datu

Konteksts	Joma	Ieguvumi un kontroles mehānismi	Piemērs iestādē
kadastra kartes, medicīnas attēli)			apstrādei un attēlu atpazīšanai
Iekšējās kontroles un audita atbalsts	Iekšējie procesi	Palīdz atklāt neatbilstības, bet gala izvērtējumu veic auditors (analītiskais MI)	Valsts kontrole – MI izmantošana dokumentu analīzē audita procesos
Klientu atbalsta čatboti	Ārējie pakalpojumi	Atbild uz biežākajiem jautājumiem, bet jāparedz iespēja sarunai ar darbinieku (ģeneratīvais MI)	Uzņēmumu reģistrs – virtuālais asistents UNA atbild uz bieži uzdotajiem jautājumiem
Iesniegumu klasifikācija	Ārējie pakalpojumi	Paātrina apstrādi, bet gala lēmumu pieņem darbinieks (analītiskais MI vai automatizācija/RPA)	Pašvaldību pilotprojekti – MI testēts iesniegumu grupēšanai un plūsmas optimizācijai

6.2. Negatīvie piemēri

Līdztekus veiksmīgiem projektiem Latvijā un citviet pasaulē ir sastopami arī gadījumi, kas atklāj kļūdas MI risinājumu izmantošanā bez pietiekamas sagatavošanās vai kontroles. Šie piemēri kalpo kā brīdinājums un palīdz citām iestādēm izvairīties no līdzīgām situācijām.

Kļūdu piemēri MI izmantošanā:

- **Nepārbaudīts dokumenta projekts.** Darbinieks sagatavo dokumentu ar MI rīku par tēmu, kuru pats nepārzina. Kolēģis tekstu virspusēji pārskata, nezinot, ka tas radīts ar MI. Rezultātā netiek pamanīti izdomājumi ("halucinācijas"), un iestāde pieņem kļūdainu lēmumu vai sniedz nepareizu atbildi uz iesniegumu, radot personas tiesību aizskārumu.
- **Aizspriedumi rekomendācijās.** MI risinājums sniedz ieteikumus par pabalstu piešķiršanu, bet nav paredzēta šo ieteikumu pārskatīšanas (apelācijas) kārtība. Rezultātā iestāde bez cilvēka iesaistes var pieņemt nepamatotus lēmumus.
- **Aizsargājami dati publiskā rīkā.** Darbinieks ievada personas datus publiski pieejamā MI risinājumā, lai sagatavotu atbildi uz iesniegumu. Rezultātā šie dati var tikt izmantoti risinājuma apmācībā un kļūt pieejami trešajām personām, apdraudot fiziskās personas pamattiesības.

Mācības no kļūdām:

- Ģeneratīvā MI rīka radītais saturs vienmēr jāpārbauda tēmas lietpratējam.
- Par visiem lēmumiem un MI rīku izmantošanas sekām atbild iestāde un tās darbinieki, nevis MI risinājums.
- Personas dati un ierobežotas pieejamības informācija nedrīkst tikt ievadīta publiski pieejamos rīkos.
- Vadībai jānodrošina darbinieku MI pratība, lai tie saprastu gan lietošanas iespējas, gan iespējamos riskus.

Kopsavilkums. Negatīvie piemēri rāda, ka lielākās problēmas rodas nevis tehnoloģijas dēļ, bet gan cilvēku rīcības un organizācijas kultūras dēļ – ja nav skaidru noteikumu, atbildības sadales un kontroles mehānismu.

Pielikumi

1. pielikums. Ikdienas darbības MI pielietošanai

Šie praktiskās pielietošanas principi ir paredzēti ikvienam publiskās pārvaldes darbiniekam, kas izmanto mākslīgā intelekta (MI) rīkus savā darbā, kā arī vadībai, kas atbild par šo MI risinājumu ieviešanu un uzraudzību. Tie palīdz nodrošināt, ka MI tiek lietots droši, tiesiski un atbildīgi.

Ikdienas darbības MI pielietošanai visiem darbiniekiem

Princips	Ko tas nozīmē	Kā rīkoties praksē
Tu zini, kas ir MI un kādi ir tā ierobežojumi	MI var palīdzēt ātrāk analizēt informāciju un sagatavot risinājumus, bet tas nekad nav pilnīgi precīzs vai neitrāls. MI rezultāti var būt kļūdaini, aizspriedumaini vai neatbilstoši konkrētajam kontekstam. Izpratne par šiem ierobežojumiem palīdz izvairīties no maldīgiem secinājumiem.	Iepazīsties ar nodrošinātajiem mācību materiāliem par MI un tā ierobežojumiem. Vienmēr pārbaudi MI rīku sniegtos rezultātus un pārliecinies, vai tie ir izmantojami konkrētajā situācijā. Nelieto iestādē neapstiprinātus MI rīkus darba vajadzībām.
Tu zini, kā izmantot MI tiesiski, ētiski un atbildīgi	MI izmantošanai jāatbilst spēkā esošajiem normatīvajiem aktiem, t. sk. personas datu aizsardzības prasībām, un publiskās pārvaldes ētikas standartiem. Tas nozīmē ne tikai ievērot likumu, bet arī nodrošināt, ka MI lietošana sniedz sabiedrībai ieguvumu, neveicina diskrimināciju un nekaitē sabiedrības uzticībai.	Vienmēr ievēro iestādes noteikumus par datu izmantošanu MI rīkos. Pirms ievadi informāciju MI rīkā, pārliecinies, vai tas ir atļauts. Publiski pieejamos MI rīkos neievadi datus, kurus iestāde noteikusi kā aizliegtus, piemēram, paroles, finanšu datus vai ierobežotas pieejamības informāciju. Ja rodas jautājumi par datu aizsardzību vai likumību, savlaicīgi konsultējies ar juristu vai datu aizsardzības speciālistu. Novērtē, vai MI izmantošana ir samērīga un kalpo sabiedrības interesēm.

Princips	Ko tas nozīmē	Kā rīkoties praksē
Tu zini, kā MI izmantot droši	Drošība nozīmē ne tikai kiberdrošību, bet arī organizācijas datu un sistēmu aizsardzību. MI risinājumi var radīt jaunus riskus, kurus trešās personas var izmantot ļaunprātīgiem mērķiem. Darbiniekam ir svarīgi saprast, kādi drošības noteikumi jāievēro un kā pasargāt iestādes informāciju.	Izmanto tikai iestādes atļautos MI rīkus. Nelieto MI rīkus no personīgām ierīcēm, ja tas ir pretrunā ar iestādes politiku. Vienmēr ievēro kiberdrošības noteikumus.
Tu nodrošini jēgpilnu cilvēka kontroli pareizajos posmos	MI var palīdzēt sagatavot ieteikumus un priekšlikumus, bet lēmuma pieņemšanas atbildība paliek cilvēkam. "Jēgpilna kontrole" nozīmē, ka cilvēks spēj izvērtēt MI sniegto informāciju un novērst iespējamo kaitīgo ietekmi.	Pirms izmantot MI rīku sagatavoto saturu, pārliecinies, ka tas ir faktoloģiski pareizs. Ja pamanīsi kļūdas, ziņo par tām. Atceries, ka MI rīku sniegtais ieteikums nekad nav galīgs — tu kā darbinieks esi atbildīgs par gala lēmumu.
Tu izmanto uzdevumam piemērotāko rīku	Ne visos gadījumos MI ir nepieciešamais vai labākais risinājums. Dažkārt problēmu var atrisināt ātrāk un drošāk ar vienkāršiem IT rīkiem vai datu analīzi. MI jālieto tikai tad, ja tas patiešām pievieno vērtību.	Pirms izvēlies MI rīku, pajautā sev: vai šo uzdevumu var atrisināt vienkāršāk? Piemēram, datu kārtošanai pietiek ar tabulām, bet MI vajadzīgs tikai sarežģītākos gadījumos. Ja neesi pārliecināts, konsultējies ar kolēģiem vai IT speciālistiem.
Tu esi atvērts un vērsts uz sadarbību	MI ieviešana un izmantošana publiskajā pārvaldē ir kopīgs process. Sadarbība ar kolēģiem un citu iestāžu darbiniekiem palīdz ātrāk apzināt riskus, atrast labākos risinājumus un veidot vienotu pieeju sabiedrības interesēs.	Dalies ar kolēģiem pieredzē par MI rīku izmantošanu — gan veiksmīgiem piemēriem, gan kļūdām. Informē par riskiem un sniedz ieteikumus, kā tos mazināt. Esi atklāts par to, kur un kā lieto MI savā darbā.

Princips	Ko tas nozīmē	Kā rīkoties praksē
Tu izmanto šos principus līdzās savas organizācijas iekšējiem noteikumiem, un ir nodrošināti atbilstoši saskaņojumi	Katrai iestādei ir savi drošības, datu apstrādes un IT lietošanas noteikumi. MI rīku izmantošanai ir jāatbilst šīm prasībām. Darbiniekam ir jāzina, kāda ir viņa atbildība un kādos gadījumos jāsaņem papildu saskaņojumi.	Pirms sākt izmantot MI rīku, pārliecinies, vai tavā iestādē tas ir atļauts un atbilstoši regulēts. Ja nepieciešams, saņem apstiprinājumu no vadības vai speciālistiem. Ja notiek incidents, ievēro iestādes noteikto ziņošanas kārtību.

Ikdienas darbības MI pielietošanai iestādes vadībai un speciālistiem

Princips	Ko tas nozīmē	Kā rīkoties praksē
Tu saproti, kā vadīt MI risinājuma dzīves ciklu	MI risinājumiem tāpat kā citām tehnoloģijām ir dzīves cikls – no plānošanas un izstrādes līdz uzturēšanai un izņemšanai no lietošanas. Vadībai un speciālistiem ir jānodrošina, ka katrā posmā tiek ievērotas drošības, ētikas un tiesiskuma prasības, kā arī tiek novērtēti riski.	Izstrādā procedūras MI risinājumu testēšanai un uzraudzībai. Regulāri vērtē to ietekmi uz pamattiesībām un datu aizsardzību. Nodrošini, ka risinājumi tiek atjaunināti un droši izņemti no lietošanas, kad tie vairs nav aktuāli vai droši.
Tu sadarbojies ar komerciāliem partneriem no paša sākuma	Liela daļa MI risinājumu tiek iegādāti vai ieviesti sadarbībā ar ārējiem piegādātājiem. Lai nodrošinātu, ka tie atbilst prasībām, partneri jāiesaista savlaicīgi, un līgumos jāiekļauj skaidras prasības par atbildīgu un drošu MI izmantošanu.	Iepirkumos iekļauj prasības par MI Aktā noteikto prasību izpildi, datu aizsardzības un ētikas standartiem. Pieprasi piegādātājiem sniegt sertifikāciju, testēšanas dokumentāciju un skaidrojumu par risinājuma darbību. Regulāri izvērtē, vai piegādātā risinājuma izmantošana saglabā atbilstību.

Princips	Ko tas nozīmē	Kā rīkoties praksē
Tev ir prasmes un ekspertīze, kas nepieciešama MI ieviešanai un izmantošanai	Efektīvai un drošai MI ieviešanai vajadzīgas dažādas kompetences – IT, kiberdrošības, juridiskās, datu aizsardzības, kā arī izpratne par ētikas principiem un ietekmi uz sabiedrību. Vadībai ir jānodrošina, lai organizācijā šīs kompetences būtu pieejamas un attīstītas.	Organizē apmācības darbiniekiem par rīku un risinājumu drošu lietošanu un ar tiem saistītajiem riskiem. Veido starpdisciplināras komandas, kurās ietilpst gan tehniskie speciālisti, gan juristi, gan politikas veidotāji. Atbalsti zināšanu apmaiņu starp iestādēm, lai stiprinātu kopējo kapacitāti.

2. pielikums. MI risinājumu pārvaldības un uzraudzības piemēri

Šie piemēri ir paredzēti publiskās pārvaldes vadītājiem un speciālistiem, kas ievieš vai uzrauga mākslīgā intelekta (MI) risinājumus. Tie palīdz saprast, kādus pārvaldības un uzraudzības pasākumus iespējams īstenot dažādos dzīves cikla posmos – no sagatavošanās līdz izņemšanai no lietošanas –, lai nodrošinātu drošu, tiesisku un atbildīgu MI risinājumu izmantošanu.

Iestāde pati izvērtē, kuri pasākumi ir nepieciešami un piemērojami, ņemot vērā konkrētā risinājuma riskus, lietošanas kontekstu un izmantoto datu veidu.

1. Uzdevuma izvēle un sagatavošanās

Pasākums	Kad piemērot	Kā īstenot
Nosaka, vai MI ir piemērotākais risinājums	Vienmēr, kad apsver jaunu MI risinājumu.	Izmanto 4. pielikumā doto lēmumu koku, lai izvērtētu MI piemērotību.
Nosaka MI sistēmas riska kategoriju un attiecīgās prasības	Vienmēr, kad tiek plānots MI risinājums.	Izmanto 5. pielikumā doto lēmumu koku, lai noteiktu, vai risinājums ir aizliegts, augsta, ierobežota vai minimāla riska; noskaidro, kādas prasības attiecas uz konkrēto riska kategoriju (piem., sertifikācija, pārredzamības prasības).
Nodrošina tiesiskās atbilstības pārbaudi	Sagatavošanās posmā, īpaši, ja tiek apstrādāti personas dati.	Iesaista juristus un datu aizsardzības speciālistu; dokumentē atbilstību; ja pastāv augsts risks, veic novērtējumu par ietekmi uz datu aizsardzību.
Izvērtē ietekmi uz pamattiesībām	Ja risinājums var ietekmēt cilvēktiesības, pakalpojumu pieejamību vai sabiedrības uzticību.	Izvērtē diskriminācijas un cilvēktiesību riskus un paredz pasākumus iespējamā kaitējuma novēršanai vai mazināšanai (piem., papildu pārbaude, pārsūdzība, kompensācija).
Pārbauda datu kvalitāti	Pirms datu nodošanas testēšanai vai risinājuma izstrādei.	Pārskata datu avotus; nodrošina izlases pārbaudes un datu aktualizācijas procedūras.

Pasākums	Kad piemērot	Kā īstenot
Izstrādā riska analīzi	Pirms eksperimentiem un ieviešanas.	Izveido risku reģistru; novērtē ietekmi un iespējamību; sagatavo risku mazināšanas plānu.
Organizē sabiedrības un pušu iesaisti *(ieteicams)*	Ja risinājums ietekmē iedzīvotājus vai klientus.	Rīko konsultācijas ar ieinteresētajām pusēm; informē par risinājumu; ievāc atsauksmes.

2. Eksperimenti, pilotprojekti

Pasākums	Kad piemērot	Kā īstenot
Izstrādā un testē prototipu drošā vidē ("smilšu kastē")	Ja risinājums ir jauns vai nav pietiekami pārbaudīts.	Veido eksperimentālas versijas, pārbauda funkcionalitāti kontrolētā vidē, neapdraudot reālos datus vai procesus.
Veic pilotprojektu ierobežotā mērogā	Pirms plašas ieviešanas.	Testē risinājumu reālos apstākļos ar ierobežotu datu vai lietotāju skaitu; dokumentē rezultātus un secinājumus.
Nodrošina neatkarīgu auditu	Pirms risinājuma ieviešanas plašā lietošanā.	Iesaista iekšējo vai ārējo auditoru, lai pārbaudītu atbilstību noteiktajiem kritērijiem (tiesiskums, drošība, ētika).
Izstrādā testēšanas protokolu	Eksperimentu un pilotprojekta laikā.	Definē procedūras tehnisko kļūdu, drošības trūkumu un aizspriedumu identificēšanai; fiksē rezultātus.
Apmāca un informē lietotājus	Pirms un pilotprojekta laikā.	Nodrošina darbiniekiem zināšanas par MI risinājumu un to, kā rīkoties problēmu gadījumā.
Izveido cilvēka kontroles mehānismus (*human-in-the-loop*)	Ja MI lēmumi var ietekmēt pamattiesības vai būtiskus procesus.	Nodrošina iespēju cilvēkam pārtraukt vai koriģēt MI darbību; pārbauda, ka kontrole darbojas praksē.
Izstrādā incidentu vadības procedūru *(ieteicams)*	Ja risinājuma testēšanā vai pilotprojektā rodas būtiskas kļūdas.	Definē atbildīgos, darbības soļus un ziņošanas kārtību problēmu gadījumā.

3. Ieviešana un integrācija

Pasākums	Kad piemērot	Kā īstenot
Nodrošina procesa dokumentāciju	Pirms risinājuma nodošanas ekspluatācijā.	Dokumentē testu rezultātus, pieņemtos lēmumus un arhitektūras izvēles; saglabā pārskatāmā veidā.
Saskaņo ar atbildīgajām struktūrvienībām	Pirms risinājuma ieviešanas.	Iesaista juristus, drošības un datu aizsardzības speciālistus; nodrošina nepieciešamos saskaņojumus un atļaujas.
Informē lietotājus un sabiedrību	Kad risinājums tiek ieviests iestādē vai pakalpojumu sniegšanā.	Sagatavo skaidrojumu darbiniekiem un iedzīvotājiem par MI izmantošanu un tā lomu procesā.
Izvērtē integrācijas riskus *(ieteicams)*	Pirms risinājuma integrēšanas ar citām IT sistēmām.	Noskaidro datu migrācijas riskus, savietojamību un iespējamo ietekmi uz esošajiem procesiem.
Nosaka atbildības sadalījumu *(ieteicams)*	Pirms risinājuma nodošanas ekspluatācijā.	Skaidri definē, kura struktūrvienība vai amatpersona ir atbildīga par risinājuma darbību un uzraudzību pēc ieviešanas.

4. Uzturēšana un uzraudzība

Pasākums	Kad piemērot	Kā īstenot
Veic regulāru monitoringu	Pastāvīgi pēc risinājuma ieviešanas.	Uzrauga risinājuma darbību automātiski un manuāli; konstatē kļūdas vai novirzes (ieteicams nepārtraukti vai vismaz reizi mēnesī).
Nosaka atbildīgo par risinājuma darbību	Pirms vai tūlīt pēc risinājuma nodošanas ekspluatācijā.	Piešķir konkrētai personai vai struktūrvienībai atbildību par uzraudzību un incidentu risināšanu.
Vāc lietotāju un sabiedrības atsauksmes	Regulāri ekspluatācijas laikā.	Izveido mehānismus, kā darbinieki un iedzīvotāji var sniegt atgriezenisko saiti (piem., reizi ceturksnī).

Pasākums	Kad piemērot	Kā īstenot
Veic periodisku atbilstības pārbaudi	Vismaz reizi gadā vai biežāk, ja mainās normatīvais regulējums vai risinājums.	Organizē auditus, kas vērtē atbilstību normatīvajiem aktiem un ētikas prasībām.
Nodrošina datu pārvaldību	Pastāvīgi ekspluatācijas laikā.	Veic datu uzglabāšanu, dzēšanu un arhivēšanu atbilstoši normatīvajām prasībām un iestādes politikai.
Uztur notikumu reģistrāciju *(ieteicams)*	Pastāvīgi.	Nodrošina žurnālus par risinājuma darbību, lai varētu izmeklēt kļūdas un incidentus.
Veic drošības pārbaudes *(ieteicams)*	Regulāri ekspluatācijas laikā.	Organizē kiberdrošības testus, lai pārliecinātos par risinājuma noturību pret uzbrukumiem.

5. Izņemšana no lietošanas

Pasākums	Kad piemērot	Kā īstenot
Izstrādā risinājuma slēgšanas procedūru	Pirms plānotas risinājuma darbības pārtraukšanas.	Sagatavo plānu, kā droši pārtraukt risinājuma lietošanu, neradot riskus procesiem vai datiem.
Veic datu dzēšanu vai arhivēšanu	Risinājuma slēgšanas brīdī.	Nodrošina, ka dati tiek dzēsti vai arhivēti atbilstoši normatīvajām prasībām un iestādes politikai.
Izvērtē risinājuma pieredzi	Pēc risinājuma slēgšanas.	Analizē, kas darbojās labi un kādus uzlabojumus nepieciešams ieviest nākotnes projektos.
Saglabā dokumentāciju	Pēc risinājuma slēgšanas.	Nodrošina, ka tiek saglabāti pārskati par risinājuma darbību, testiem, izmaiņām un lēmumiem, lai ļautu auditēt arī pēc slēgšanas.
Izvērtē risinājuma ietekmi *(ieteicams)*	Pēc risinājuma slēgšanas.	Novērtē, kā risinājums ietekmēja iedzīvotājus, pakalpojumu kvalitāti un iestādes darbu; izmanto secinājumus nākotnes projektos.

3. pielikums. Tipveida MI uzdevumu katalogs

Katalogā apkopoti biežāk sastopamie uzdevumu veidi publiskajā pārvaldē, kuros iespējams izmantot **mākslīgā intelekta (MI)** vai **automatizācijas** pieejas. Katalogs kalpo kā **praktisks orientieris** iestādēm ideju apkopošanai un sākotnējai izvērtēšanai.

Paskaidrojums. Automatizācija šajās vadlīnijās ietver arī robotizēto procesu automatizāciju (RPA). **Automatizācija nav MI**, jo izpilda iepriekš noteiktus soļus bez mācīšanās vai prognozēšanas. Katalogā automatizācija iekļauta kā **alternatīva pieeja** līdzīgu uzdevumu veikšanai gadījumos, kad MI nav nepieciešams.

Kā lietot katalogu:

1. salīdzini savus uzdevumus ar piemēriem un pieraksti atbilstošās idejas;
2. tālāk vērtē idejas ar lēmumu kokiem un kritērijiem (2. nodaļa).

Joma	Uzdevuma veidi, piemēri un ieteicamā tehnoloģiskā pieeja
Dokumentu pārvaldība	**Automatizācija** – dokumentu virzīšana pa plūsmām, parakstīšanas un reģistrācijas darbību automatizācija (bez MI). **Analītiskais MI** – dokumentu klasifikācija, satura marķēšana, metadatu izvilkšana. *Ieteicamā pieeja:* mašīnmācīšanās, teksta klasifikatori. **Ģeneratīvais MI** – kopsavilkumi, tulkojumi, pārvēršana vieglajā valodā, vēstuļu vienkāršošana, runas atpazīšana (piem., *Hugo.lv*). *Ieteicamā pieeja:* dabīgās valodas apstrāde (NLP), runas atpazīšana/sintēze (ASR/TTS).
Administratīvie procesi	**Automatizācija** – e-pastu šķirošana pēc noteikumiem, grafiku plānošana, rēķinu datu iegrāmatošana, statusu atjaunināšana sistēmās. *Ieteicamā pieeja:* noteikumu balstīta automatizācija, skripti (bez MI). **Analītiskais MI** – iepirkumu dokumentu satura atbilstības pārbaude, protokolu sagatavošanas atbalsts (klasifikācija/izvilkšana). *Ieteicamā pieeja:* NLP, ML, procesu analīze.
Iekšējā komunikācija un apmācības	**Analītiskais MI** – zināšanu bāzu uzturēšana (meklēšanas uzlabošana ar klasifikāciju), biežāko jautājumu analīze. *Ieteicamā pieeja:* teksta klasifikācija, vektoru meklēšana, noteikumu dzinēji. **Ģeneratīvais MI** – mācību materiālu melnraksti, iekšējie asistenti, video ierakstu automātiski kopsavilkumi. *Ieteicamā pieeja:* NLP, runas uz tekstu, teksta uzrunu.
Tehniskais atbalsts	**Automatizācija** – datu validācijas skripti, datu anonimizācijas darbību automatizācija, IT atbalsta pieprasījumu klasifikācija un sadale pēc noteikumiem (bez MI).

Joma	Uzdevuma veidi, piemēri un ieteicamā tehnoloģiskā pieeja
	Analītiskais MI – automatizētas vizualizācijas, statistikas atskaišu ģenerēšana no datu modeļiem. *Ieteicamā pieeja:* datu analītika, statistiskie modeļi.
Analītika un revīzija	**Analītiskais MI** – risku un krāpšanas pazīmju prognoze, finanšu datu analīze, budžeta izlietojuma novērtēšana, anomāliju noteikšana, iekšējās kontroles atbalsts. *Ieteicamā pieeja:* mašīnmācīšanās, anomāliju detektēšana, statistika.
Sabiedrībai sniegti pakalpojumi	Atkarībā no sarežģītības – **analītiskais MI / automatizācija** – iesniegumu klasifikācija, zvanu centra pieprasījumu maršrutēšana. *Ieteicamā pieeja:* teksta klasifikācija (MI) vai noteikumu balstīta maršrutēšana (RPA). **Ģeneratīvais MI** – čatboti, BUJ atbilžu sagatavošana, vizuālu un informatīvu materiālu izveide. *Ieteicamā pieeja:* NLP, attēlu/teksta ģenerēšana.
Stratēģiskais atbalsts	**Analītiskais MI** – politikas ietekmes scenāriji, pieprasījuma prognozes, klimata datu modelēšana, veselības resursu prognozēšana. *Ieteicamā pieeja:* prognozējošie modeļi, simulācijas, datu analītika.

Paskaidrojumi par kategorijām

- **Automatizācija** – izpilda iepriekš noteiktus soļus **bez MI elementiem**; izmantojama, ja pietiek ar noteikumos balstītu pieeju.
- **Analītiskais MI** – analizē datus, klasificē, prognozē un atklāj sakarības, pamatojoties uz modeļiem, kas mācās no datiem.
- **Ģeneratīvais MI** – rada jaunu saturu vai priekšlikumus (teksts, attēli, audio).

Izmantošana praksē

- Iestādes salīdzina savus uzdevumus ar katalogā minētajiem un iekļauj atbilstošās idejas **ideju sarakstā**.
- Tālāk idejas **sākotnēji izvērtē** un **padziļināti pārbauda** ar lēmumu kokiem un kritērijiem (2. nodaļa).

4. pielikums. Lēmumu koks piemērotākās pieejas izvēlei

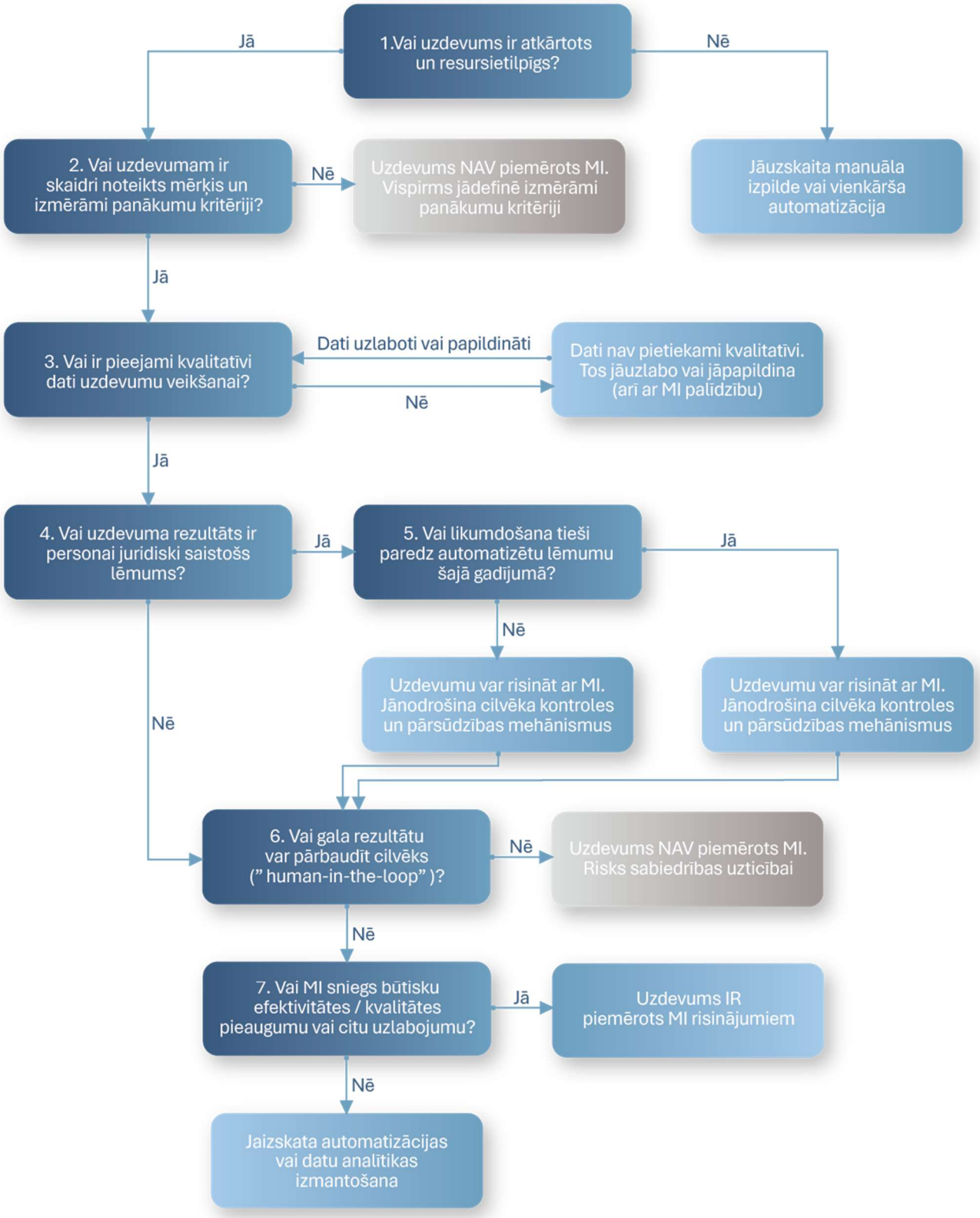
Pirms izvēlēties vai ieviest mākslīgā intelekta (MI) risinājumu, iestādei jāpārliecinās, ka konkrētais uzdevums tam ir piemērots. Šim nolūkam paredzēts lēmumu koks, kas soli pa solim palīdz noteikt, vai uzdevumu risināt ar MI risinājumu, vai arī piemērotāka būs cita pieeja – manuāla izpilde, klasiskā automatizācija vai datu analītika (skat. 6. attēls).

Šis ir **pirmais solis izvērtēšanas procesā**. Ja uzdevums atbilst MI risinājuma pielietošanas kritērijiem, nākamais solis ir izmantot 5. pielikumu, lai noteiktu MI sistēmas riska kategoriju saskaņā ar MI aktu.

Lēmuma koka diagramma ļauj vizuāli pārskatīt visu izvērtēšanas loģiku vienā attēlā un ātri noteikt piemērotāko pieeju.

Kā lietot lēmumu koku

- Lēmumu koks jāizmanto katra jaunā uzdevuma vai pakalpojuma izvērtēšanai.
- Jautājumi jāizvērtē secīgi un uz katru no tiem jāatbild ar "Jā" vai "Nē".
- Izvērtējumu ieteicams veikt komandā, iesaistot procesa īpašniekus, juristus, datu aizsardzības speciālistus, IT un kiberdrošības speciālistus, kā arī politikas veidotājus. Tas samazina kļūdu risku un nodrošina kompetentas atbildes.
- Ja nav skaidri definēti mērķi vai kvalitātes kritēriji, tie vispirms ir jānosaka. Tikai pēc tam drīkst turpināt izvērtēšanu.
- Ja dati ir nepilnīgi vai nekvalitatīvi, tie jāsakārto vai jāpapildina. Tas nav šķērslis uzdevuma tālākai analīzei, tomēr jo labāk strukturēti būs dati, jo kvalitatīvāks būs gala rezultāts.
- Ja uzdevuma rezultāts ir juridiski saistošs lēmums personai, MI drīkst izmantot tikai tad, ja to tieši paredz likums un ir nodrošināta cilvēka kontrole un pārsūdzības mehānisms.
- Ja gala rezultātu nav iespējams pārbaudīt cilvēkam, uzdevums nav piemērots MI risinājumam vai automatizētai pieejai bez cilvēka kontroles.



6. attēls. Lēmuma koka diagramma MI un alternatīvu automatizācijas metožu izvēlei

5. pielikums. Lēmuma koks MI risinājuma riska un prasību noteikšanai

Šis lēmumu koks palīdz iestādei noteikt, vai plānotais mākslīgā intelekta (MI) risinājums ir atļauts un kādas prasības tam piemērojamas saskaņā ar **Eiropas Savienības Mākslīgā intelekta aktu** (Regula (ES) 2024/1689). Tas ir praktisks instruments, lai saprastu, kāda riska kategorija attiecas uz konkrēto MI risinājumu un kādi turpmākie soļi nepieciešami (skat. 7. attēls).

Kā lietot lēmumu koku

- Izvērtēšana notiek secīgi, atbildot uz jautājumiem ar "Jā" vai "Nē".
- Rezultātā iegūstams viens no četriem risinājumiem, kas atbilst MI akta riska kategorijām.
- Ja rodas šaubas, ieteicams piesaistīt **juristus, datu aizsardzības speciālistus un IT kiberdrošības speciālistus**, kā arī konsultēties ar VARAM, CERT.LV un DVI.

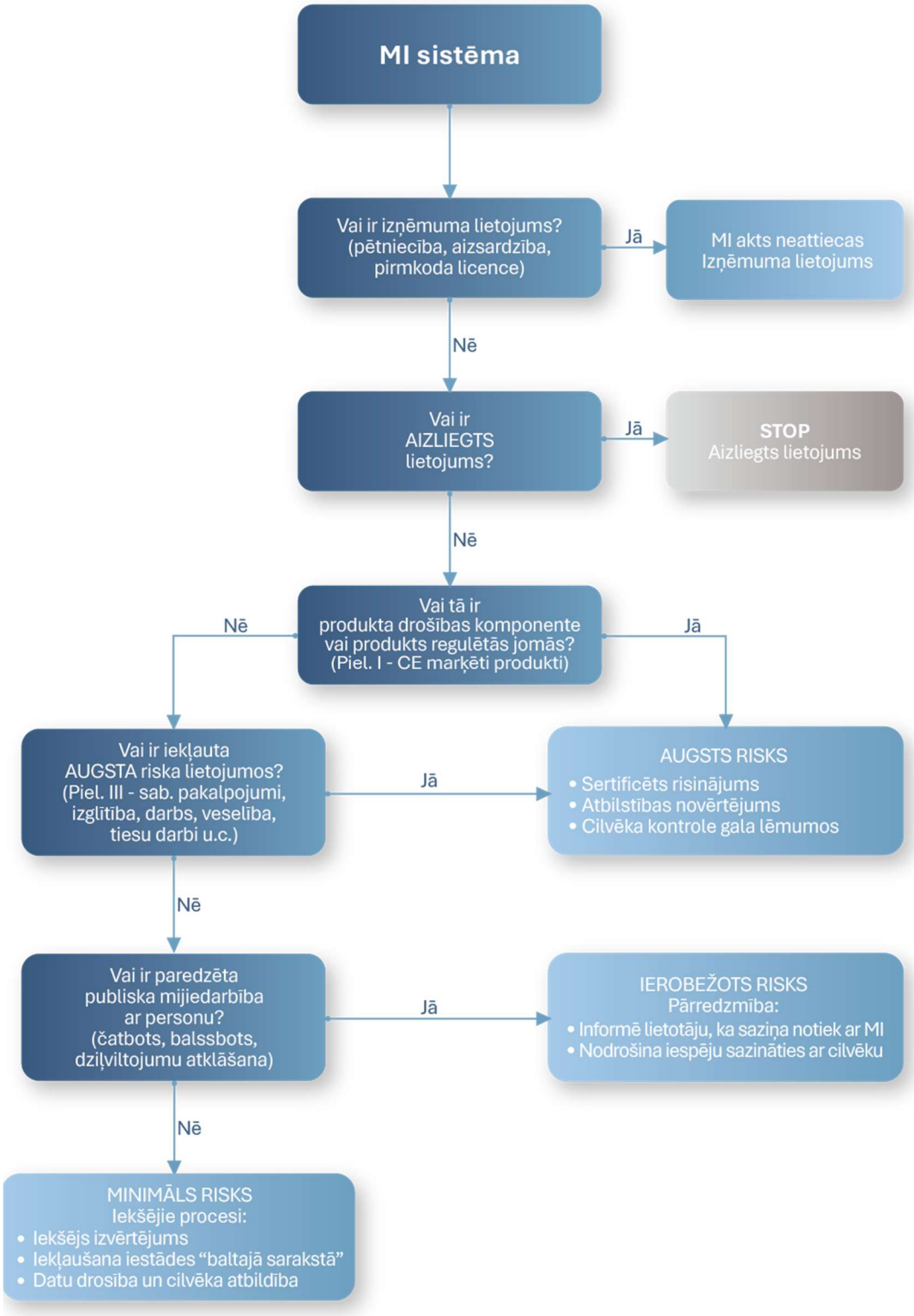
Riska kategorijas un prasības

Riska kategorija	Piemēri	Prasības iestādei
Aizliegtā prakse	– Kaitīga MI balstīta manipulācija un maldināšana – Kaitīga neaizsargātības izmantošana – Sociālā vērtēšana – Atsevišķu noziedzīgu nodarījumu riska novērtējums vai prognozēšana – Sejas atpazīšanas datu bāzes, kas iegūtas no interneta vai drošības kamerām bez īpašas atlases – Emociju atpazīšana un vērtēšana sensitīvās vietās, piemēram, darba vietās vai izglītības iestādēs – Biometriskā kategorizācija, lai izdarītu secinājumus par tādiem sensitīviem raksturlielumiem kā rase, reliģija vai politiskie uzskati – Reāllaika biometriskā identifikācija tiesībaizsardzības nolūkos sabiedriskās vietās	**Nedrīkst ieviest.** Projekts nekavējoties jāpārtrauc

Riska kategorija	Piemēri	Prasības iestādei
Augsta riska MI risinājumi	– Drošības sastāvdaļas medicīnas iekārtās Noteikta veida MI sistēmu pielietošana šādās nozarēs: – Kritiskā infrastruktūra – Biometrija – Izglītība un arodmācības – Nodarbinātība – Darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai – Piekļuve privātiem pamatpakalpojumiem un sabiedriskajiem pamatpakalpojumiem un pabalstiem un to izmantošanai – Tiesībaizsardzība – Migrācijas – Patvēruma un robežkontroles pārvaldība – Tiesvedība un demokrātijas procesi	Ieviešot MI risinājumus, kas ietver augsta riska MI sistēmas, publiskās pārvaldes iestādēm ir jāizpilda MI sistēmu uzturētājiem noteiktās prasības, t. sk. jāveic augsta riska MI sistēmu ietekmes uz pamattiesībām novērtējums, kā arī publiskā iepirkuma ietvaros no piegādātājiem jāpieprasa viņiem MI Aktā noteikto pienākumu izpildi, piemēram, MI sistēmas sertificēšanu
Ierobežota riska MI risinājumi	– Publiskie čatboti un virtuālie asistenti – Ģeneratīvā MI risinājumi vai rīki (teksts, attēli, audio) – Dziļviltojumu ģenerēšanas vai atpazīšanas rīki	– Lietotājs skaidri jāinformē, ka saziņa notiek ar MI – Jādod iespēja sazināties ar cilvēku – Nodrošināt pārredzamību un atbildību
Minimāla riska MI risinājumi	– Dokumentu melnraksti un kopsavilkumi – Tulkojumi iekšējām vajadzībām – Datu strukturēšana un analītikas atbalsts – Mēstuļu filtri, automātiska teksta formatēšana	– MI akts nekādas papildu prasības nenosaka – Pietiek ar iestādes iekšēju izvērtējumu – Risinājums jāiekļauj iestādes baltajā sarakstā – Jāievēro pamatprincipi par datu drošību un cilvēka atbildību

Praktiskais pielietojums

- Lēmumu koks jāizmanto pirms jebkura jauna MI risinājuma ieviešanas.
- Tas palīdz savlaicīgi noteikt riska kategoriju un vajadzīgos pasākumus, samazinot juridiskos, drošības un reputācijas riskus.
- Ja risinājums tiek lietots ilgstoši, iestādei periodiski jāpārskata tā riska kategorija, ņemot vērā izmaiņas normatīvajos aktos un tehnoloģijās.



7. attēls. MI risinājuma riska un prasību noteikšana

6. pielikums. Alternatīvās automatizācijas un analītikas metodes

Ne visi uzdevumi ir piemēroti mākslīgā intelekta (MI) risinājumu izmantošanai. Daudzos gadījumos efektīvāk, drošāk un vienkāršāk ir izmantot **automatizācijas** vai **datu analītikas** pieejas, kas neietver MI elementus. Šis pielikums sniedz pārskatu par alternatīvām metodēm, kuras var dot būtisku ieguvumu publiskajā pārvaldē un bieži kalpot kā priekšnoteikums MI ieviešanai.

Automatizācija – ietver robotizēto procesu automatizāciju (RPA) un biznesa noteikumu dzinējus

Automatizācija izpilda iepriekš noteiktus soļus un darbības, neizmantojot MI. Tā ir īpaši piemērota vienveidīgiem, atkārtojamiem uzdevumiem ar strukturētiem datiem.

RPA (robotizētā procesu automatizācija) – rīki, kas atdarina cilvēka darbības IT sistēmās, piemēram:

- datu ievade un pārkopēšana starp sistēmām;
- dokumentu vai e-pastu apstrāde;
- informācijas virzīšana pa noteiktām plūsmām.

Biznesa noteikumu dzinēji (*Business Rules Engines*) – rīki, kas sistemātiski piemēro iepriekš definētus *"ja–tad"* noteikumus, piemēram:

- normatīvo aktu prasību piemērošana;
- iekšējo procedūru ievērošana;
- vienkārša lēmumu pieņemšana ar skaidri noteiktiem nosacījumiem.

Galvenā priekšrocība – noteikumus un automatizācijas loģiku iespējams ātri pielāgot, ja mainās normatīvie vai iekšējie kritēriji.

Datu analītika un vizualizācija

Datu analītikas un vizualizācijas risinājumi ļauj apkopot, apstrādāt un interpretēt datus, lai sagatavotu pamatojumu lēmumu pieņemšanai. Tie ir noderīgi:

- budžeta un resursu plānošanā;
- sabiedrisko aptauju vai pakalpojumu lietojuma tendenču analīzē;
- risku un noviržu agrīnā identificēšanā.

Analītika palīdz sagatavot informāciju lēmumiem, taču **gala lēmumu vienmēr pieņem darbinieks**, saglabājot atbildību un tiesisko noteiktību.

Salīdzinošā tabula: piemērotākā pieeja uzdevumiem

(skat. arī 2.2 sadaļu par piemērotākās pieejas izvēli)

Pieeja	Kad vispiemērotāk izmantot	Piemēri publiskajā pārvaldē
Automatizācija (RPA un noteikumu dzinēji)	Vienkārši, atkārtojami un noteikumiem pakļauti uzdevumi ar strukturētiem datiem.	Datu kopēšana starp sistēmām, dokumentu reģistrēšana, e-pastu apstrāde, vienkārša lēmumu pieņemšana pēc noteiktiem kritērijiem.
Datu analītika un vizualizācija	Ja nepieciešams apkopot, analizēt un saprotami parādīt datus cilvēkiem lēmumu pieņemšanai.	Budžeta izpildes pārskati, pakalpojumu lietojuma analīze, iedzīvotāju aptauju rezultātu vizualizācija.
MI risinājumi (analītiskais vai ģeneratīvais MI)	Ja nepieciešama mācīšanās no datiem, prognozēšana, pielāgošanās jaunām situācijām vai satura ģenerēšana.	Mašīntulkošana, čatboti, risku prognozēšana, dokumentu sākotnējā pārbaude.

Kopsavilkums

Automatizācijas un datu analītikas pieejas bieži nodrošina ātrus un uzticamus rezultātus bez MI ieviešanas sarežģītības. Tās ieteicams apsvērt **pirms MI projekta uzsākšanas**, lai pārliecinātos, vai vienkāršāka pieeja nesniedz tādu pašu rezultātu ar mazākiem resursiem un riskiem. Savukārt, ja uzdevumam nepieciešama adaptācija, prognozēšana vai satura radīšana, piemērotākas būs **analītiskā vai ģeneratīvā MI risinājumu pieejas**.

7. pielikums. Ātrais un pilnais iestādes pašnovērtējums MI ieviešanai

Šie pašnovērtējuma rīki palīdz iestādei novērtēt savu gatavību droši un atbildīgi ieviest mākslīgā intelekta (MI) risinājumus. Izvēle starp ātro un pilno ceļu atkarīga no risinājuma sarežģītības un ietekmes:

- **Ātrais pašnovērtējums** – izmantojams vienkāršiem produktivitātes rīkiem (piemēram, dokumentu kopsavilkumi, e-pasta melnraksti, tulkojumi, sanāksmju protokolu strukturēšana).
- **Pilnais pašnovērtējums** – nepieciešams sarežģītākiem MI risinājumiem, kas ietekmē iestādes lēmumus vai sabiedrības tiesības (piemēram, pabalstu piešķiršanas sistēmas, iesniegumu klasifikācija, personāla atlases rīki, risinājumi veselības vai tieslietu jomā).

Šie rīki papildina lēmuma koku (5. pielikums), kas nosaka MI risinājumā izmantotās MI sistēmas riska kategoriju.

Ātrais pašnovērtējums

Šis rīks paredzēts vienkāršiem produktivitātes MI rīkiem vai lietotnēm, kurās tiek izmantoti ģeneratīvā MI risinājumi (piemēram, teksta vai tulkojumu ģenerēšanai). Ja uz visiem jautājumiem atbilde ir "Jā", rīku var sākt lietot.

Jautājums	Jā	Nē
Vai darbinieki ir iepazīstināti ar MI rīku lietošanas noteikumiem un ierobežojumiem?	☐	☐
Vai MI rīkā netiek ievadīta ierobežotas pieejamības informācija (IPI), tostarp personas dati vai klasificēta informācija?	☐	☐
Vai gala rezultātus vienmēr pārbauda cilvēks, pirms tos izmanto tālāk?	☐	☐

Piemēri, kam piemērots ātrais pašnovērtējums: dokumentu melnraksti, tulkojumi, publiski pieejamas informācijas apkopošana, prezentāciju uzmetumi.

Pilnais pašnovērtējums

Šis rīks paredzēts sarežģītākiem MI risinājumiem, kas ietver augstāka riska MI sistēmas un var ietekmēt sabiedrības tiesības vai iestādes saistošos lēmumus. Katru virzienu vērtē skalā:

- **Nepietiekami** – būtiski trūkumi, projektu nevar uzsākt.
- **Daļēji** – iespējams turpināt, bet nepieciešami uzlabojumi.
- **Atbilstoši** – atbilst prasībām, var virzīties uz plānošanu/pilotprojektu.

Novērtējuma virziens	Nepietiekami	Daļēji	Atbilstoši	Piezīmes
Stratēģiskie mērķi: Vai risinājums atbilst iestādes stratēģijai un vadības prioritātēm?	☐	☐	☐	
Dati: Vai dati ir pieejami, kvalitatīvi un droši pārvaldīti? Vai veikts datu aizsardzības ietekmes novērtējums?	☐	☐	☐	
Kompetences: Vai iestādē ir nepieciešamās zināšanas un lomas (piem., projekta vadītājs, datu aizsardzības speciālists, kiberdrošības speciālists)?	☐	☐	☐	
Procesi un kontroles: Vai noteikti atbildīgie, cilvēka kontroles punkti un riska pārvaldība?	☐	☐	☐	
Resursi: Vai pieejams finansējums, cilvēkresursi un infrastruktūra ilgtermiņā?	☐	☐	☐	

Rezultātu interpretācija:

- Ja lielākā daļa virzienu ir “Atbilstoši” → var virzīties uz pilotprojektu un nākamajiem soļiem.
- Ja dominē “Daļēji” → nepieciešami uzlabojumi pirms uzsākšanas.
- Ja ir “Nepietiekami” → projektu atlikt, līdz trūkumi novērsti.

Piemēri, kam piemērots pilnais pašnovērtējums: veselības datu apstrādes un diagnostikas MI sistēmas, pabalstu un atbalsta piešķiršanas MI risinājumi, izglītības vērtēšanas un uzņemšanas MI risinājumi, tiesībaizsardzības un uzraudzības MI rīki.

8. pielikums. MI risinājuma dzīves cikla kontrolsaraksts ar atbildībām

Šis kontrolsaraksts ir paredzēts kā praktisks atbalsta rīks iestādēm mākslīgā intelekta (MI) risinājumu pārvaldībā. Tas aptver galvenos dzīves cikla posmus – no sagatavošanās līdz izņemšanai no lietošanas – un palīdz nodrošināt, ka risinājums tiek izmantots droši, atbildīgi un atbilstoši iestādes mērķiem.

Kontrolsaraksts kalpo kā:

- **Plānošanas instruments** – lai pārliecinātos, ka iestāde apzinās visus būtiskos soļus pirms risinājuma ieviešanas.
- **Uzraudzības instruments** – lai pārbaudītu, vai dzīves cikla laikā tiek veikti nepieciešamie pasākumi.
- **Atbildības sadales instruments** – lai katram posmam būtu skaidri noteiktas lomas un atbildīgie.

Kontrolsaraksts nav izsmeļošs uzdevumu apkopojums, bet gan orientējošs rīks, kas palīdz strukturēti plānot, ieviest un pārvaldīt MI risinājumus. To ieteicams izmantot regulāri – ikgadējās pārskatīšanas laikā, kā arī pēc būtiskām izmaiņām (piemēram, modeļa atjauninājuma, jauna normatīvā akta stāšanās spēkā vai jaunu datu pievienošanas).

Atbildīgās lomas katrā posmā ir uzskaitītas no augstākā lēmumu līmeņa (iestādes vadība) līdz specializētām lomām (IT, kiberdrošība, juridiskā atbilstība u. c.), lai uzsvērtu hierarhiju un atbildības sadali.

MI risinājuma dzīves cikla kontrolsaraksts ar atbildībām

Dzīves cikla posms	Obligātie soļi	Atbildīgās lomas
1. Sagatavošanās	– Definēts risinājuma mērķis un sagaidāmie ieguvumi – Veikts uzdevuma piemērotības izvērtējums (automatizācija vai MI) – Noteikta MI riska kategorija – Vadības lēmums par resursu piešķiršanu – Nodrošināta vadības iesaiste un stratēģiskais ietvars – Izvērtēta datu gatavība un drošība – Izvērtētas darbinieku kompetences un apmācību vajadzības – Izvērtēti pieejamie resursi (cilvēkresursi, finansējums, infrastruktūra) – Noteikta cilvēka kontroles pieeja (“human-in-the-loop”, ja piemērojams)	Iestādes vadība, procesa īpašnieks, IT/datu speciālists, kiberdrošības speciālists, jurists, datu aizsardzības speciālists

Dzīves cikla posms	Obligātie soļi	Atbildīgās lomas
	– Piesaistīti atbalsta mehānismi (ekspertu kopienas, labās prakses) – Veikts iestādes MI gatavības pašnovērtējums (ātrais vai pilnais ceļš)	
2. Eksperimenti un pilotprojekti	**Eksperimenti (smilšu kastē):** – Izveidots prototips ar anonimizētiem vai simulētiem datiem – Pirms testēšanas definēti mērķi un izmērāmi panākumu kritēriji – Rezultāti, problēmas un secinājumi dokumentēti – Novērtēti drošības un datu aizsardzības aspekti **Pilotprojekts (produkcijas vidē):** – Veikts riska un ietekmes izvērtējums, ja risinājums ir augsta riska – Nodrošināta cilvēka kontrole (“human-in-the-loop”), ja risinājums skar pamattiesības vai juridiski saistošus lēmumus – Lietotāji informēti par MI izmantošanu, ja to paredz normatīvie akti – Definēti un izmērīti KPI – Projekta rezultāti un lēmums par turpmāko ieviešanu dokumentēts **Visā posmā:** – Procesa gaita un rezultāti skaidri komunicēti vadībai un lietotājiem – Atzīts, ka arī neveiksmīgs eksperiments vai pilots ir vērtīgs, ja mērķi bijuši skaidri un darbs dokumentēts	Iestādes vadība, procesa īpašnieks, IT/datu speciālists, kiberdrošības speciālists, jurists, datu aizsardzības speciālists
3. Ieviešana un integrācija	– Risinājums integrēts iestādes procesos un informācijas sistēmās – Noslēgti līgumi ar piegādātāju, ietverot drošības, uzturēšanas un audita prasības – Nodrošināta lietotāju apmācība un atbalsta mehānismi – Nodrošināta organizācijas pārmaiņu vadība (procesu pielāgošana, darbinieku iesaiste) – Risinājums iekļauts iestādes oficiālajā baltajā sarakstā – Izveidoti atgriezeniskās saites kanāli ar lietotājiem un sabiedrību	Iestādes vadība, procesa īpašnieks, IT/datu speciālists, kiberdrošības speciālists, jurists, datu aizsardzības speciālists, mācību koordinators

Dzīves cikla posms	Obligātie soļi	Atbildīgās lomas
	– Veikti nepieciešamie uzlabojumi, balstoties uz saņemto atgriezenisko saiti	
4. Uzturēšana un uzraudzība	– Regulāri programmatūras un MI modeļa atjauninājumi, lai nodrošinātu precizitāti un atbilstību prasībām – Pārvaldīti piekļuves un drošības mehānismi, aizsardzība pret uzbrukumiem – Dokumentētas visas izmaiņas un uzlabojumi – Lietotājiem nodrošināts kanāls atgriezeniskajai saitei un tās izmantošana risinājuma pilnveidei – Regulārs tehniskais monitorings (pieejamība, kļūdas) – Regulārs funkcionālais monitorings (rezultātu kvalitāte, KPI) – Periodiska atbilstības pārbaude (iekšējās un ārējās prasības) – Augsta riska MI risinājumiem organizēts neatkarīgs audits – Nodrošināta pārredzamību un atbildības sadale visā uzturēšanas periodā	Iestādes vadība, procesa īpašnieks, IT/datu speciālists, kiberdrošības speciālists, jurists, datu aizsardzības speciālists, iekšējais auditors
5. Izņemšana no lietošanas	– Pieņemts dokumentēts lēmums par risinājuma slēgšanu – Veikta datu arhivēšana vai droša dzēšana atbilstoši normatīvajām prasībām – Lietotāji un iesaistītās puses informēti par risinājuma slēgšanu, ja tas ir būtiski – Saglabāta dokumentācija un pieredzes materiāli, lai izmantotu nākotnes projektiem – Izvērtēta nepieciešamība pēc aizstājēja risinājuma vai alternatīvas pieejas	Iestādes vadība, procesa īpašnieks, IT/datu speciālists, kiberdrošības speciālists, jurists, datu aizsardzības speciālists

9. pielikums. Ātrā atgādne MI lietotājiem: “Dari / Nedari”

Dari	Nedari
Lieto tikai **apstiprinātus rīkus**, kas iekļauti iestādes **baltajā sarakstā**.	Nelieto rīkus, kas **nav** iekļauti baltajā sarakstā, ja vien iestāde nav noteikusi īpašus nosacījumus.
Ievadi tikai to informāciju, kuru iestāde ir skaidri **atļāvusi**.	Neievadi informāciju, kuras izmantošanu iestāde nav atļāvusi.
Vienmēr **pārbaudi MI radīto rezultātu** pirms izmantošanas.	Neuztver MI radīto saturu kā gala lēmumu vai oficiālu dokumentu.
Pārliecinies, ka ievēro **autortiesības** un avotu norādes.	Neizmanto MI radītu saturu kā savu, ja tas neatbilst autortiesību prasībām.
Informē, ja saturs radīts ar MI, un nodrošini iespēju sazināties ar cilvēku.	Neradi maldinošu iespaidu, ka MI atbilde ir cilvēka sagatavota vai gala lēmums.

Kur vērsties šaubu gadījumā?	**Vispirms** jautā savam **tiešajam vadītājam**, ja neesi pārliecināts, vai konkrētā situācijā drīkst izmantot MI.
	Ja jautājums skar datu drošību vai privātumu, vadītājs vai Tu pats vari vērsties pie iestādes **IT, kiberdrošības vai datu aizsardzības speciālista**.
	Ja parādās tehniskas problēmas vai aizdomas par drošības incidentu, nekavējoties ziņo IT vai drošības atbalstam.

ATCERIES	Labāk uzdot jautājumu, nekā riskēt ar datu noplūdi vai citu problēmu.

10. pielikums. Seši noteikumi darbiniekiem MI rīku lietošanā

1. Lieto tikai apstiprinātus rīkus

Vadi savu darbu pēc iestādes baltā saraksta un iekšējiem noteikumiem.

2. Ievadi tikai atļauto informāciju

Respektē iestādes noteiktos ierobežojumus datu izmantošanai.

3. Vienmēr pārbaudi rezultātu

MI radītais rezultāts jāuztver kā uzmetums vai projekts; gala kvalitāte un precizitāte jānodrošina cilvēkam.

4. Par gala rezultātu atbild cilvēks

Juridiski saistošus lēmumus pieņem darbinieks, nevis MI sistēma.

5. Respektē autortiesības

Izmanto tikai tādus tekstus un attēlus (arī MI ģenerētus), kuru lietošanas tiesības un avoti ir skaidri zināmi.

6. Esi atklāts

Ja saturu ir sagatavojis MI, to skaidri norādi un nodrošini iespēju sazināties ar cilvēku.

Kur vērsties šaubu gadījumā?	**Vispirms** jautā savam **tiešajam vadītājam**, ja neesi pārliecināts, vai konkrētā situācijā drīkst izmantot MI.
	Ja jautājums skar datu drošību vai privātumu, vadītājs vai Tu pats vari vērsties pie iestādes **IT, kiberdrošības vai datu aizsardzības speciālista**.
	Ja parādās tehniskas problēmas vai aizdomas par drošības incidentu, nekavējoties ziņo IT vai drošības atbalstam.

ATCERIES	Labāk uzdot jautājumu, nekā riskēt ar datu noplūdi vai citu problēmu.

11. pielikums. Ģeneratīvā MI rīku izmantošanas atgādne darbiniekam

Pamatprincips – ģeneratīvais mākslīgais intelekts (MI) veido saturu, balstoties uz līdzībām ar apmācības datiem, tāpēc rezultāts var būt nepilnīgs, neprecīzs vai maldinošs. Gala atbildība par saturu vienmēr ir darbiniekam, nevis MI rīkam.

Piemēri tipisku MI rīku lietojumam iestādēs

Teksts: kopsavilkumi, melnraksti, paskaidrojumi (*Microsoft Copilot, ChatGPT*).

Prezentācijas: slaidi, uzmetumi, vizualizācijas (*Microsoft Copilot PowerPoint vidē, Canva*).

Attēli un ilustrācijas: vizualizācijas, skices, ilustratīvi materiāli (*Canva, Adobe Firefly*).

Kods un formulas: aprēķini, datu apstrādes skripti (*GitHub Copilot, Microsoft Copilot for Excel/*Power *BI*).

Pirms izmantot konkrētu MI rīku, vienmēr pārliecinies, vai tas ir iekļauts iestādes baltajā sarakstā. Ja rodas šaubas – vērsies pie atbildīgā darbinieka.

Atceries – informācijas ievade MI rīkos balstās uz trim pamatprincipiem:

- **Publiski pieejama informācija** – drīkst izmantot un apstrādāt ar MI rīkiem, ja iestāde nav noteikusi citus ierobežojumus.
- **Informācija, kurai ir noteikti ierobežojumi un papildu aizsardzības prasības (t. sk. personas dati, iekšēji dokumenti, autortiesību objekti)** – drīkst izmantot tikai tādā apjomā un kārtībā, kā to paredz iestādes noteikumi.
- **Baltais saraksts** – izmanto tikai tos MI rīkus, kas iekļauti iestādes baltajā sarakstā.

1. Droša datu ievade

Ko darīt

Lieto tikai rīkus no baltā saraksta; ievadi tikai tādu informāciju, kuras izmantošanu šajos rīkos ir atļāvusi iestāde; ievadi tikai tik daudz informācijas, cik nepieciešams.

Ko nedarīt

Neizmanto rīkus, kas nav iekļauti iestādes baltajā sarakstā; neievadi personas datus vai konfidenciālu informāciju neapstiprinātos rīkos; neievadi visu dokumentu, ja pietiek ar fragmentu.

Piemēri

Pirms teksta augšupielādes pārbaudi, vai rīks ir baltajā sarakstā; ja gatavo prezentāciju ar konfidenciālu informāciju, noformējumu veido ar iestādes apstiprinātu rīku.

2. Rezultātu pārbaude

Ko darīt

Uztver ģenerēto saturu kā uzmetumu; pārbaudi faktus, skaitļus un atsauces; konsultējies ar kolēģi vai lietpratēju, ja rodas šaubas.

Ko nedarīt

Nepaļaujies uz MI radīto saturu kā gala versiju bez cilvēka pārbaudes; neizplati tekstu vai datus, par kuru precizitāti šaubies.

Piemēri

Pārlasi vēstules melnrakstu pirms nosūtīšanas; pārbaudi statistiku oficiālajā datu bāzē; šaubu gadījumā lūdz kolēģa viedokli/saskaņojumu/palīdzību.

3. Rezultāta akcepts un izmantošana

Ko darīt

Rediģē saturu un pielāgo normatīvo aktu prasībām; pārbaudi autortiesības un licences; norādi, ka izmantoji MI, ja to paredz iestādes noteikumi.

Ko nedarīt

Nepublicē MI ģenerētu tekstu bez pārbaudes; nelieto MI ģenerētus attēlus, ja to izcelsme vai lietošanas tiesības nav skaidras; neslēp MI izmantošanu.

Piemēri

Pirms publicēšanas izlabo valodu un faktus; prezentācijā lieto tikai licencētus attēlus; melnrakstā norādi, ja tekstu sagatavojis MI.

Šī atgādne neaizstāj iestādes noteikumus vai balto sarakstu – vienmēr vadies pēc tiem un šaubu gadījumā vērsies pie atbildīgā darbinieka.

12. pielikums. VAS atbalsts MI kompetenču attīstībā publiskajā pārvaldē

Valsts administrācijas skola (VAS) īsteno projektu **"Publiskās pārvaldes digitālā akadēmija"**[15], kura mērķis ir stiprināt publiskās pārvaldes darbinieku prasmes digitālajā transformācijā un tehnoloģiju izmantošanā. Projekts palīdz gan speciālistiem, gan vadītājiem kļūt par digitālās transformācijas virzītājspēkiem savās iestādēs.

Digitālā akadēmija (DA) piedāvā šādas iespējas MI un digitālo prasmju pilnveidei:

- **Publiskās pārvaldes digitālo prasmju ietvars** – definē nepieciešamās prasmes un kompetences, kalpo kā pamats darbinieku attīstībai, mācībām un cilvēkresursu vadībai.
- **Pašnovērtējuma rīks** – ļauj novērtēt digitālo un MI prasmju līmeni.
- **Mācību ietekmes mērīšanas rokasgrāmata un novērtēšanas rīks** – palīdz analizēt mācību rezultātus, novērtēt sasniegtos mērķus un plānot uzlabojumus, balstoties uz datiem.
- **Profesionāļu un mentoru atbalsts** – sniedz palīdzību digitālo un MI risinājumu izstrādē un ieviešanā, nodrošinot, ka apgūtās prasmes tiek pielietotas praksē.

DA īsteno arī daudzveidīgas mācības MI un digitālo prasmju pilnveidei – praktiskus kursus, e-mācības, vebinārus, darbnīcas, mentoringu un prototipēšanu. Mācības pielāgotas dažādām amatu lomām[16], tostarp tiem, kas nosaka digitālās transformācijas attīstības virzienu (atslēgas lomas) vai piedalās tās plānošanā un īstenošanā (sadarbības lomas):

- **Mākslīgā intelekta pamati publiskajai pārvaldei** (6 akad. st.) – ievadkurss par MI tehnoloģijām, ētiku un praktisko pielietojumu e-mācību formātā.
- **Mākslīgais intelekts produktīvākam darbam publiskajā pārvaldē** (16 akad. st.) – mācības MI lietošanas prasmju attīstīšanai ikdienas darbā.
- **Mākslīgā intelekta risinājumu ieviešana un vadība** (100 akad. st.) – padziļināta programma MI ieviešanas, datu izmantošanas, juridisko, ētisko un drošības aspektu jomā.
- **Mākslīgā intelekta pielietojums un iespējas publiskajā pārvaldē** (16 akad. st.) – darbnīcas, kas pielāgotas konkrētu iestāžu vajadzībām.

Vebināri regulāri aptver aktuālas MI tēmas – MI rīku izmantošanu ikdienas darbā, uzvedņu (promtu) inženieriju, MI aktu, jaunākās tendences un labās prakses piemērus. Vebināru ieraksti ir pieejami VAS *YouTube* kontā.

Plašāka informācija par mācībām un pasākumiem pieejama tīmekļvietnē digitalaakademija.lv.

[15] Projekta "Publiskās pārvaldes digitālā akadēmija" (Nr.2.3.2.2.i.0/1/23/I/VARAM/001) aktivitāšu īstenošana ir līdz 2026. gada 31. maijam.

[16] Loma ir strukturēts amatu funkciju kopums, kas ietver konkrētus uzdevumus, atbildības un nepieciešamās kompetences, lai efektīvi sasniegtu iestādes mērķus. Loma nav tikai amats iestādes hierarhijā – tās apraksts sniedz izpratni par amata nozīmi un pievienoto vērtību iestādē.

13. pielikums. Gadījuma analīze: Mākslīgā intelekta risinājuma ieviešana LATAK akreditācijas procesā

Konteksts un problēma

Pakalpojuma izpildes komplicētība

Valsts aģentūra "Latvijas Nacionālais akreditācijas birojs" (LATAK) īsteno atbilstības novērtēšanas institūciju akreditāciju, kas ir komplicēts pakalpojums, kura ietvaros tiek ievēroti Latvijas Republikas un Eiropas Savienības normatīvie akti, nacionālie, Eiropas un starptautiskie standarti, kā arī savstarpējos atzīšanas līgumos ar starptautiskajām akreditācijas organizācijām (Eiropas Akreditācijas kooperācijas, Starptautiskā akreditācijas foruma, Starptautisko laboratoriju akreditācijas kooperācijas) un uz to pamata izdotos saistošos dokumentos noteiktās prasības.

Liels manuālā darba apjoms, ko īsteno augsti kvalificēts darba spēks

16 vadošie darbinieki ik gadu manuāli lasa, pārskata un analizē apmēram 2500 dokumentus, kā arī ik gadu manuāli sagatavo apmēram 4900 dokumentus; ik gadu tiek īstenotas apmēram 380 akreditācijas procedūras un manuāli izvērtētas un izskatītas apmēram 1200 korektīvās darbības. Būtiska darba daļa tiek patērēta rutīnai, nespējot rast laiku stratēģiskiem darbiem.

Pastāvīgi augsts risks nesasniegt stratēģiskos mērķus

Pārrunās ar darbiniekiem un iekšējos auditos tika identificētās atsevišķās novirzes no stratēģisko prioritāšu sasniegšanas – noteiktā termiņā, apjomā un kvalitātē sniegts starptautiski atzīts pakalpojums.

Risinājuma izstrāde un pieeja

Vadības iniciatīva un stratēģiska pieeja

Projekta uzsākšanu ierosināja LATAK augtākā vadība, apzinoties, ka tikai ar cilvēkresursiem akreditācijas procesa kvalitāti ilgtermiņā nodrošināt nebūs iespējams.

Piegādātāju un risinājumu izvērtēšana

LATAK augstākā vadība noteica principu akreditācijas procesa izpildē izmantot tikai LATAK oficiāli apstiprinātu MI rīku. Pēc tirgū pieejamo MI risinājumu un rūpīgas licenču nosacījumu, datu apstrādes drošības un risinājuma ilgtspējas, t.sk. ieguldījumu atdeves izvērtēšanas LATAK darbiniekiem tika nodrošināta pieeja *MS 365 Copilot* rīkiem, vienlaikus apzinoties pastāvošo risku pārvaldības integrācijas nepieciešamību.

Stratēģiska risku pārvaldības pieeja

Mazinot viena piegādātāja atkarības riskus un stiprinot drošības pārvaldību ilgtermiņā tiek apzināti projekti alternatīvu MI risinājumu integrācijai, t.sk. ar dalību ES fondu projektos. Plānots izstrādāt jaunu *low-code/no-code* MI atbalstītu digitālo koplietošanas platformu, kas nodrošina automatizētu un datos balstītu dažādu prasību izpildes izvērtēšanas procesu.

MI integrācijas process

Sprinti, testi, darbnīcas

Testēti risinājumi dokumentu sagatavošanai, komunikācijai ar klientiem, sanāksmju sagatavošanai un iekšējo procesu izstrādei un pārvaldībai.

Kritiskie lēmumi par datu apstrādi

LATAK apzināti atteicās no atvērtā koda MI modeļiem, izvēloties MS infrastruktūru, lai izvairītos no sensitīvu datu noplūdes riska. Visi MI rezultāti ir cilvēku uzraudzīti un pārskatīti.

Darbinieku iesaiste un apmācība

Organizētas praktiskas darbnīcas, sprinti un apmācības ar ārējiem mentoriem, kā arī nodrošināta dalība Valsts administrācijas skolas Digitālās akadēmijas rīkotajās mācībās digitālo prasmju attīstībai. Apmācību optimizācija balstīta uz individuālām vajadzībām un reāllaika atgriezenisko saiti.

Sasniegtie rezultāti

Kultūras un domāšanas maiņa

Darbinieki ir kļuvuši pārliecinātāki par savām digitālajām prasmēm, atvērtāki eksperimentiem un inovācijām, aizrautīgāki MI izmantošanai ikdienā.

Frāzes *"Tas nav iespējams"* nomainījušās *"Pamēģinām ar MI", "Pajautājam MI"*.

MI ir kļuvis par dabisku instrumentu, kas palīdz efektīvāk izpildīt darba uzdevumu un rosina radošumu.

Produktivitātes uzlabojumi

- **Tekstu kvalitāte:** MI būtiski uzlabo kvalitatīva teksta sagatavošanu, samazinot nepieciešamību pēc stilistiskiem labojumiem saskaņošanas procesā.
- **E-pasta vēstuļu sagatavošana:** Process kļuvis daudz ātrāks un vieglāks, it īpaši svešvalodās.
- **Veidlapu aizpildīšana: Atsevišķos** gadījumos 8 stundu darbu ir bijis iespējam izpildīt nedaudz vairāk par 1 stundu.

- **Iekšējie dokumenti:** Jaunu iekšējo **dokumentu** (procedūru, politiku u. c.) sagatavošanai iespējams ietaupīt līdz pat 70 % laika.
- **Sanāksmju sagatavošanās:** Sagatavošanās laiku **iespējams** samazināt no 2 stundām uz 20 minūtēm.

Rezultāti parāda ievērojamu efektivitātes pieaugumu un pozitīvu darbinieku attieksmes maiņu pret tehnoloģiju izmantošanu.

Panākumu faktori un mācības

- **Vadības līderība un iesaiste:** augstākā vadība iesaistījās testēšanā un mācībās.
- **Droša vide eksperimentiem:** iespēja izmēģināt jaunas pieejas un mācīties no kļūdām.
- **Pastāvīga mācīšanās:** nodrošinātas regulāras darbnīcas un pieredzes apmaiņas sesijas.
- **Sistēmiska pieeja:** MI risinājumi ieviesti kā stratēģisks, nevis īslaicīgs elements.
- **Sadarbība:** pieredze dalīta ar citām iestādēm, stiprinot kopīgu mācīšanās kultūru

Ieteikumi citām iestādēm

- **Stratēģiskā līmenī:** apziniet galvenās problēmas un definējiet ilgtermiņa mērķus, sasaistot tos ar organizācijas stratēģiju.
- **Organizatoriskā līmenī:** nodrošiniet vadības iesaisti, veidojiet starpdisciplināras komandas un īstenojiet riska balstītu pieeju.
- **Operacionālā līmenī:** sāciet ar nelieliem pilotprojektiem, lai ātri gūtu pieredzi un redzamus rezultātus.
- **Cilvēkresursu līmenī:** veidojiet mācīšanās kultūru un drošu vidi ideju izmēģinājumiem, atbalstiet iniciatīvu un kļūdu pieļaušanu kā mācību procesu.
- **Ekosistēmas līmenī:** meklējiet sadarbības partnerus publiskajā un privātajā sektorā, dalieties pieredzē un sekojiet MI regulējuma un standartu attīstībai.

Kopsavilkums

LATAK pieredze apliecina, ka MI ieviešana publiskajā pārvaldē nav tikai tehnoloģisks projekts, bet **sistēmiska pārmaiņa**, kas apvieno cilvēkus, procesus un kultūru. Pakāpeniska pieeja, droša vide eksperimentiem un vadības iesaiste ļāva sasniegt būtisku produktivitātes pieaugumu un kultūras maiņu. Šis piemērs parāda, kā MI var kļūt par praktisku atbalstu efektīvai, drošai un uz cilvēku orientētai publiskajai pārvaldei.