# 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.

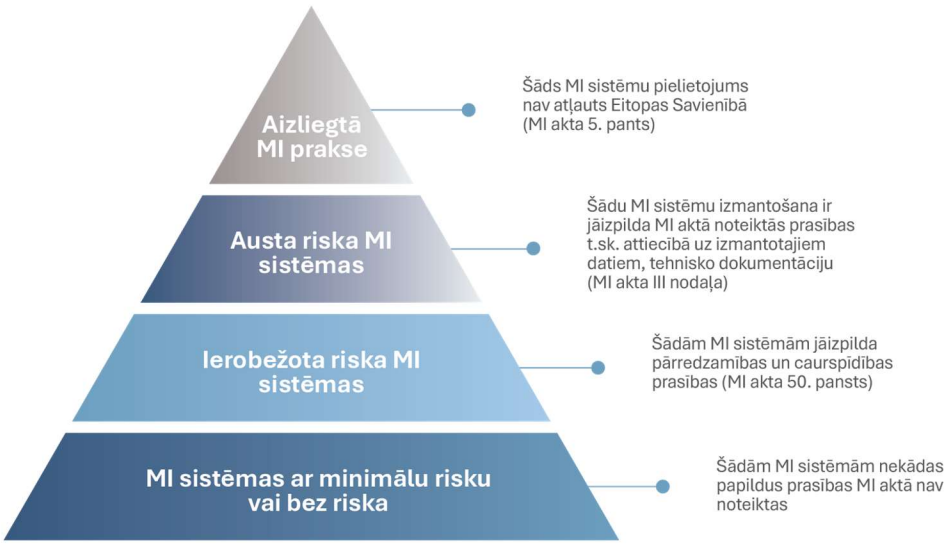
Dažas MI sistēmas, to pielietojuma veida un izmantoto datu dēļ, iestādēs var izmantot bez ierobežojumiem, un tām nav jāizpilda īpašas normatīvo aktu prasības, piemēram, izmantojot publiski pieejamas MI sistēmas prezentāciju vai skaidrojošu materiālu sagatavošanai un vizuālai noformēšanai.

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.