

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 pārlicinies, 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, pārlicinies, 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, pārlicinies, 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, pārlicinies, 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.