

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 (<i>ieteicams</i>)	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 (<i>human-in-the-loop</i>)	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 (<i>ieteicams</i>)	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 (<i>ieteicams</i>)	Pirms risinājuma integrēšanas ar citām IT sistēmām.	Noskaidro datu migrācijas riskus, savietojamību un iespējamo ietekmi uz esošajiem procesiem.
Nosaka atbildības sadalījumu (<i>ieteicams</i>)	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 (<i>ieteicams</i> 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 <i>(ieteicams)</i>	Pastāvīgi.	Nodrošina žurnālus par risinājuma darbību, lai varētu izmeklēt kļūdas un incidentus.
Veic drošības pārbaudes <i>(ieteicams)</i>	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 <i>(ieteicams)</i>	Pēc risinājuma slēgšanas.	Novērtē, kā risinājums ietekmēja iedzīvotājus, pakalpojumu kvalitāti un iestādes darbu; izmanto secinājumus nākotnes projektos.