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