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.