ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

ĮSAKYMAS
DĖL ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIRBTINIO INTELEKTO TAIKYMO TAISYKLIŲ PATVIRTINIMO

2025 m. lapkričio d. Nr.
Šakiai

Vadovaudamasis Lietuvos Respublikos vietos savivaldos įstatymo 34 straipsnio 6 dalies 2 ir 3 punktais**,** 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 2024/1689, Lietuvos Respublikos viešojo administravimo įstatymo 3 straipsnio 3 ir 7 punktais, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 1 straipsnio 3 dalimi, 2 straipsniu ir Valstybės skaitmeninių sprendimų agentūros pavyzdiniais Dirbtinio intelekto taikymo politikos dokumentais:

1. T v i r t i n u Šakių rajono savivaldybės administracijos dirbtinio intelekto taikymo taisykles (pridedama).

2. P a v e d u :

2.1. Šakių rajono savivaldybės administracijos Bendrųjų reikalų skyriaus vyresniajai sekretorei Irenai Bacevičienei Dokumentų valdymo sistemos priemonėmis su įsakymu supažindinti rajono savivaldybės administracijos skyrių vedėjus, seniūnus, valstybės tarnautojus, neįeinančius į struktūrinių padalinių sudėtį.

2.2. Šakių rajono savivaldybės administracijos skyrių vedėjams su įsakymu supažindinti skyrių darbuotojus.

2.3. Šakių rajono savivaldybės administracijos seniūnijų seniūnams su įsakymu supažindinti seniūnijų darbuotojus.

Administracijos direktorius Vytautas Ižganaitis

Parengė
Bendrųjų reikalų skyriaus
vedėja

Rita Vaičiūnienė
2025-11-05

PATVIRTINTA
Šakių rajono savivaldybės administracijos
direktoriaus 2025 m. lapkričio d.
įsakymu Nr. AT-

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIRBTINIO INTELEKTO TAIKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Dirbtinio intelekto taikymo taisyklių (toliau – Taisyklės) nustato sąlygas ir reikalavimus dirbtinio intelekto (toliau – DI) naudojimui Šakių rajono savivaldybės administracijos (toliau – administracija) veikloje, vadovaujantis pagrindiniais DI taikymo principais, nustatytais administracijos direktoriaus tvirtinamoje Dirbtinio intelekto taikymo politikoje, ir siekiant užtikrinti patikimą, saugią, etišką, skaidrią, atsekamą ir teisėtą administracijos veiklą.

2. Taisyklės taikomos administracijos struktūriniams padaliniams ir administracijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau kartu – darbuotojai), naudojant DI sistemą, t. y. mašina grindžiamą sistemą, suprojektuotą veikti įvairiais autonomijos lygiais, kuri po diegimo gali veikti prisitaikydama ir kuri, siekiant aiškių ar numanomų tikslų, iš gautos įvesties duomenų daro išvadą, kaip generuoti išvedinius, pavyzdžiui, predikcijas, turinį, rekomendacijas ar sprendimus, kurie gali turėti įtakos fizinei ar virtualiai aplinkai.

3. Taisyklės taikomos administracijos veiklos srityse, kuriose numatyta taikyti DI sistemas.

4. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas).

II SKYRIUS
DIRBTINIO INTELEKTO TAIKYMO PRINCIPAI

5. Administracijoje naudojamos tik patvirtintos vidinės, mišrios ir (ar) išorinės DI sistemos (Taisyklių priedas).

6. Prieš pradedant taikyti DI sistemą administracijos veikloje, privaloma atlikti poveikio asmens duomenų apsaugai ir galimų rizikų lygio vertinimus. Nustatytam rizikų lygiui privaloma taikyti technines ir organizacines priemones. Didelės rizikos DI sistemas diegti ir (ar) taikyti leidžiama sumažinus rizikas iki leistino lygio. Rizikų valdymas – tai nuolatinis procesas per visą DI sistemos gyvavimo ciklą, kai identifikuojamos ir vertinamos galimos neigiamos pasekmės (pvz.: šališkumas, saugumo spragos, privatumo pažeidimai) ir imamasi priemonių joms sumažinti. Galutinė atsakomybė už DI sistemas atitenka DI sistemų savininkams ir administratoriams, todėl nėra leidžiama tokia DI autonomija, kad neliktų aišku, kas priėmė galutinį sprendimą ar kas gali jį peržiūrėti. Atsakingi už DI kūrimą ir (ar) diegimą bei taikymą administracijos veikloje darbuotojai privalo suprasti DI sistemos veikimą, sekti jos rezultatus ir prireikus

imtis veiksmų, taisant klaidas ar nutraukiant DI sistemos naudojimą, jei kyla grėsmė saugumui ir (ar) teisėtumui.

7. Taikant DI, būtina užtikrinti informacijos saugumą. Draudžiama naudoti asmenines, viešas ar nepatvirtintas DI paskyras, platformas ir įrankius (tokių kaip asmeninis ChatGPT, Google Gemini, Copilot ar viešos generatyvinio DI sistemos) administracijos veikloje, kai tvarkomi administracijos duomenys, vykdomi darbo procesai ar teikiamos paslaugos.

8. DI taikymas neturi pažeisti žmonių privatumo. Informacinių technologijų (toliau – IT), informacinių sistemų (toliau – IS), aplikacijų (programinės įrangos) techninėje specifikacijoje ir privatumo politikoje privalo būti nurodyta informacija apie DI taikymą.

9. Užtikrinant skaidrų DI taikymą, naudotojai turi būti informuoti, kai sąveikauja su DI sistema (pvz., virtualiu asistentu ar pokalbių robotu), o DI generuotas turinys privalo būti aiškiai pažymėtas, kad būtų išvengta naudotojų klaidinimo. DI sugeneruotas turinys (dokumentas, prezentacija, piešiniai, vaizdai, vaizdo ir garso medžiaga ir pan.) pradžioje ir pabaigoje turi būti aiškus – paženklinti žyme „DI“ ir skaičiumi nuo 1 iki 5, kuris parodo DI taikymo lygį (1 – žemiausias, 2 – žemas, 3 – vidutinis, 4 – aukštas, 5 – aukščiausias), pvz. „DI-5“ arba, kai medžiaga parengta anglų kalba – „AI-5“. Turi būti suteikta aiški ir paprasta informacija apie DI sistemos veikimą, duomenų šaltinius, pagrindinius sprendimų kriterijus ar logiką. Tai leidžia suinteresuotiems asmenims suprasti, kaip buvo gautas konkrečios DI sistemos rezultatas, ir suteikia galimybę jį užginčyti ar peržiūrėti. Siekiant skaidrumo, IT, IS, aplikacijų (programinės įrangos) dokumentacijoje turi būti visa informacija apie kiekvieną DI sistemą: jos paskirtis, naudojami duomenys, taikomi modeliai, versijų istorija, atlikti testavimai ir poveikio vertinimai. Asmens duomenų tvarkymo įrašai – duomenų žemėlapis (toliau Duomenų žemėlapis), tai yra vidinis registras, kuris užtikrina, kad informacija apie taikomą DI būtų prieinama atsakingiems asmenims, auditoriui ir prireikus – priežiūros institucijoms. Skaidrumui užtikrinti, DI sistemų bei IT, IS, aplikacijų (programinės įrangos) kur yra taikomas DI, privatumo politikose viešai skelbiama bendro pobūdžio informacija apie institucijos naudojamus DI (neatskleidžiant saugomų ar konfidencialių detalių), kad visuomenė žinotų apie DI taikymą viešajame sektoriuje.

10. DI taikymas turi būti etiškas kitų žmonių atžvilgiu ir nepažeisti jų teisių bei teisėtų interesų. DI taikymas negali diskriminuoti žmonių, turi išlikti kontroliuojamas bei suprantamas, vadovaujantis etiškumo principais:

10.1. nediskriminavimas ir sąžiningumas: DI sistemos neturi šališkai diskriminuoti asmenų ar grupių pagal rasę, lytį, amžių, negalią, etninę kilmę, religiją ar kitus požymius, saugomus įstatymų. Kuriant ir diegiant DI sistemas, būtina atsižvelgti, ar mokymo duomenų rinkiniai nėra šališki ir ar juose neatsispindi istorinė diskriminacija. Ankstyvoje DI kūrimo fazėje įvertinamos galimos šališkumo apraiškos – tai gali labai prisidėti prie teisėto ir sąžiningo DI naudojimo. Rekomenduojama atlikti diskriminacijos rizikos vertinimą: turi būti patikrinta, ar renkami ir naudojami duomenys yra tikslūs, reprezentatyvūs, patikimi ir aktualūs visoms tikslinėms grupėms, kurioms bus taikoma DI sistema. Taip pat gali būti modeliuojamos DI sistemų pasekmės skirtingoms visuomenės grupėms – sudaromas „žemėlapis“, kaip kiekvienas DI priimamas sprendimas gali paveikti atskiras grupes, ir nustatoma, ar tokie padariniai yra priimtini ir teisingi. Jei nustatoma, kad DI sistema sistemingai blogiau vertina ar traktuoja tam tikrą grupę (pvz.: moteris, vyresnio amžiaus asmenis, mažumų atstovus) lyginant su kitais, toks DI turi būti tobulinamas arba atsisakoma jo naudojimo, nebent yra objektyviai pateisinamos priežastys ir pritaikytos šališkumą mažinančios priemonės. Administracija turi atlikti reguliarias patikras dėl šališkumo: periodiškai tikrinti naudojamų DI sistemų duomenis ir išvestis, ieškant galimų diskriminacijos požymių. Rezultatai turi būti dokumentuojami ir viešinami, taip didinant pasitikėjimą. Šie veiksmai atitinka tarptautinius reikalavimus užtikrinti, kad DI gerbtų asmenų lygybę ir įvairovę;

10.2. žmogaus kontrolė ir sprendimų priežiūra: nepaisant DI automatizavimo, galutinis sprendimų valdymas turi likti žmogaus rankose. DI technologijos administracijoje diegiamos tam, kad padėtų žmogui

priimti sprendimus, o ne visiškai jį pakeistų (ypač kritinėse srityse). Jokie sprendimai, turintys teisinį ar reikšmingą poveikį asmeniui, nėra paliekami vien tik DI valiai be galimybės žmogui peržiūrėti ar pakeisti tą sprendimą. Prieš pradedant naudoti DI konkrečiam sprendimų priėmimui, administracija nustato, ar DI veikia tik kaip pagalbinis įrankis, ar priims sprendimus savarankiškai – atitinkamai parenkamas kontrolės mechanizmas. Kiekvienu atveju, kai DI sistema priima sprendimą automatiškai, duomenų subjektas (pilietis ar darbuotojas, kuriam taikomas sprendimas) turi teisę reikalauti, kad sprendimą peržiūrėtų žmogus. Gavus duomenų subjekto prašymą dėl sprendimo peržiūrėjimo administracijoje turi būti paskiriami atsakingi darbuotojai arba sudaryta komisija, kuri išnagrinėtų tokį prašymą ir peržiūrėtų DI priimtą sprendimą. Išnagrinėjus prašymą duomenų subjektas informuojamas apie administracijos sprendimą dėl peržiūrėto DI sistemos sprendimo (palikti galioti DI sistemos sprendimą, jį pakeisti ar panaikinti). Administracijos atsakingų darbuotojų ar komisijos atliekama peržiūra turi būti tikslinga ir prasminga, t. y. peržiūra turi būti ne formali – peržiūrai atlikti turi būti skiriami kvalifikuoti specialistai, kurie geba suprasti DI sistemos veikimą ir kritiškai vertinti jos pateiktus rezultatus bei turi turėti pakankamus įgaliojimus (pvz., gali sustabdyti ar pakoreguoti DI sistemos sprendimą, jei nustato klaidingą jo veikimą ar nesąžiningumą). Administracija privalo užtikrinti, kad darbuotojams, prižiūrintiems DI, būtų sudaryta galimybė mokytis, tobulinti ir kelti savo kompetenciją bei kvalifikaciją. Šis žmogaus įsikišimo principas atitinka ir Reglamento (ES) Nr. 2024/1689 reikalavimus dėl žmogaus priežiūros didelės rizikos DI sistemose, taip pat Ekonominio bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) rekomendacijas, kad būtų užtikrinta galimybė žmogui atlikti DI stebėseną ir kontrolę;

10.3. paaiškinamumas ir teisė paaiškinimui: kiekvienas DI sistemos sprendimas, darantis įtaką asmeniui (pvz., piliečiui atsisakoma suteikti tam tikrą paslaugą remiantis DI įvertinimu), turi būti paaiškinamas suprantama forma to pageidaujančiam asmeniui. Administracija turi teikti paaiškinimus, kaip DI sistema suformavo konkretų rezultatą: nurodyti, kokie duomenys buvo naudojami, pagal kokius kriterijus ar taisykles modelis vertino situaciją, kokie veiksniai labiausiai nulėmė sprendimą. Svarbu vengti „juodosios dėžės“ efekto – DI taikymas turi būti visiškai suprantamas. Jei naudojami sudėtingi mašininio mokymosi modeliai (pvz., gilieji neuroniniai tinklai), administracija taiko papildomas priemones paaiškinamumui didinti: naudoja interpretuojamus modelius arba specialius DI paaiškinimo įrankius (angl. *Explainable AI*), kurie gali atskleisti, kodėl modelis priėmė tam tikrą sprendimą. Paaiškinamumas svarbus užtikrinant žmonių pasitikėjimą DI bei galimybę jiems apginti savo teises. EBPO principai akcentuoja, kad DI vykdytojai turi teikti prasmingą informaciją apie DI sistemų sprendimus, įskaitant duomenų šaltinius, veiksnius ir logiką, lėmusią rezultatą, kad paveikti asmenys galėtų suprasti ir prireikus apskųsti sprendimą. Administracija šiuo tikslu turi parengti ir viešai paskelbti DI etikos kodeksą arba gaires arba apibrėžia tai privatumo politikoje, kurioje, greta kitų dalykų, nurodomi įsipareigojimai paaiškinti DI sistemos sprendimus naudotojams ir suinteresuotoms šalims;

10.4. socialinė nauda ir žalos nedarymas: DI diegiamas tik ten, kur jis atneša didesnę naudą nei galimą žalą. Administracija vykdo DI projektų poveikį visuomenei: siekiama, kad DI sistemos prisidėtų prie viešųjų paslaugų gerėjimo, didesnio darbo efektyvumo, personalizuotų paslaugų, tuo pačiu nekenkdami visuomenei ar atskiroms grupėms. Pavyzdžiui, diegiant DI, kuris optimizuos procesus, bus vertinama, ar tai nediskriminuos skaitmeninės atskirties požiūriu (nepaliks nuošalyje technologijomis nesinaudojančių asmenų), ar neigiamai nepaveiks darbuotojų – administracija laikosi žalos nedarymo principo ir naudos visuomenei prioriteto – DI turi tarnauti visuomenės gerovei, tvariai aplinkai ir taikai. Jei nustatoma neigiama DI poveikio rizika (pvz., kai automatizavus tam tikrą sprendimą, tam tikra socialinė grupė nebegalės veiksmingai pasinaudoti paslauga), imamasi priemonių tai rizikai mažinti (pvz., išlaikoma alternatyvi neautomatinė paslaugos teikimo galimybė);

10.5. atitiktis etikos standartams ir teisės viršenybei: DI sistemos privalo gerbti teisės viršenybę ir demokratines vertybes. Tai reiškia, kad ne tik laikomasi visų privalomų teisės aktų, bet ir vadovaujamasi bendrosiomis etikos normomis – sąžiningumu, skaidrumu, pagarba asmens orumui. DI neturi pažeisti

Konstitucijos ir tarptautinių žmogaus teisių (pvz., nekuriamos DI priemonės, galinčios riboti saviraiškos laisvę ar atlikti masinę neteisėtą stebėseną). Administracija vengia DI naudojimo srityse, kuriose nėra aiškaus teisinio reglamentavimo arba kyla svarūs etikos klausimai, iki kol nebus gauti aiškūs teisiniai ir etikos išaiškinimai. Dalyvaudama pilotiniuose DI projektuose, administracija konsultuojasi su etikos ekspertais, visuomene bei atsižvelgia į Europos ir tarptautinių organizacijų rekomendacijas.

11. Taikant DI, atskaitomybė (atsekamumas) užtikrinama kaupiant įrašus DI sistemų veiklos žurnaluose (angl. *Log Files*), kad būtų galima atsekti, kokie duomenys ir kokiais veiksmais lėmė tam tikrą rezultatą. Visi reikšmingi DI veiksmai turi būti užregistruojami, kad vėliau iškilus klausimams ar tyrimams būtų galima peržiūrėti sprendimo kelią ir duomenis.

12. DI sistemų taikymas galimas tik esant teisiniam pagrindui ir nepažeidžiant DI reglamentuojančių teisės aktų.

13. Administracijos darbuotojai, kurie projektuoja, diegia, prižiūri (administruoja) ir (ar) naudoja DI sistemas arba sprendimus, privalo:

13.1. DI naudoti kaip įrankį, kuris padeda vykdyti veiklas, atlikti užduotis, siūlo alternatyvas ar didina darbo efektyvumą, tačiau DI turi būti naudojamas tik kaip pagalbinis įrankis darbuotojui, nepakeičiant atsakomybės, kompetencijos ar gebėjimo priimti sprendimus. DI turi papildyti veiklą, o ne ją perimti, ypač srityse, kur būtinas žmogiškasis, etinis vertinimas ar sprendimas;

13.2. darbuotojai privalo atlikti peržiūrą prieš priimdami galutinius sprendimus, ypač jei sprendimai gali turėti reikšmingos įtakos fizinių ar juridinių asmenų teisėms, teisėtiems interesams ar reputacijai. Reikšmingų sprendimų priėmimas negali būti visiškai perduotas algoritmams. Naudodamiesi DI sistemomis, darbuotojai turi suprasti jų veikimo principus, vertinti funkcionalumą, žinoti jų privalumus ir trūkumus;

13.3. draudžiama naudoti ar skleisti DI sugeneruotą turinį, kuris gali būti diskriminuojantis, žeidžiantis, stereotipinis ar kitaip neatitinkantis žmogaus teisių ir (ar) gali pažeisti lygių galimybių principus;

13.4. draudžiama skleisti DI sistemų sugeneruotą slaptą, konfidencialią (neskelbtiną), asmeninę informaciją arba specialių kategorijų asmens duomenis (informacija apie sveikatą, biometriniai duomenys, prisijungimo slaptažodžiai, religiniai ir politiniai įsitikinimai, lytinė orientacija ir pan.);

13.5. naudodami DI sugeneruotą informaciją ar sprendimus, darbuotojai privalo įsitikinti jų tikslumu ir tinkamumu naudoti konkrečiu atveju. Už pateiktą turinį atsakingas darbuotojas, o ne DI sistema;

13.6. esant poreikiui, pasikonsultuoti dėl DI taikymo (projektavimo, diegimo, naudojimo ir pan.) arba iškilus klausimams dėl DI sistemų, būtina kreiptis į Dirbtinio intelekto pareigūną (toliau – DIP).

III SKYRIUS
REIKALAVIMAI DI SISTEMŲ ĮSIGIJIMUI

14. Perkant ir taikant DI sistemas (produktai: programinė įranga ir debesijos paslaugos su DI funkcijomis), būtina užtikrinti, kad tiekėjų siūlomos DI sistemos atitiktų administracijos keliamus reikalavimus. DI sprendimų viešųjų pirkimų vykdymo ir tiekėjų valdymo taisyklės apima:

14.1. reikalavimai viešųjų pirkimų dokumentacijai: rengiant viešųjų pirkimų dokumentus DI sistemų pirkimui, turi būti įtraukiami aiškūs reikalavimai dėl atskaitomybės, skaidrumo, nediskriminavimo, saugumo ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) laikymosi. Pavyzdžiui, tiekėjas turi įrodyti, kad jo siūloma DI sistema buvo testuota dėl šališkumo ir nediskriminuoja (pateikti bandymų ataskaitas), kad užtikrina žmogaus įsikišimo galimybę (pvz., produkto funkcinės

galimybės leidžia naudotojui apskųsti ar koreguoti DI sistemos sprendimą), kad yra paaiškinamas naudotojui (pvz., generuoja paaiškinimus ar turi dokumentuotą algoritmų logiką). Taip pat reikalaujama, jog tiekėjas atskleistų DI modelio kilmę: ar modelis kurtas savarankiškai, ar pasitelkta trečiųjų šalių komponentų ir kokių (pvz.: atvirojo kodo bibliotekos, iš anksto apmokyti modeliai), ar tie komponentai neturi licencinių ar etinių apribojimų. Tiekėjų pasiūlymų vertinimo kriterijai taip pat apima etikos aspektus – pvz., papildomi balai gali būti skiriami už geresnius skaidrumo sprendimus, už nepriklausomo audito patvirtinimus, kad produktas atitinka tam tikrus DI etikos standartus.

14.2. Sutartiniai įsipareigojimai: Sutartyse su DI sistemų tiekėjais, turi būti numatytos sutartinės sąlygos, užtikrinančios administracijos DI taikymo politikos reikalavimų laikymąsi. **Duomenų apsauga:** sutartyse aiškiai apibrėžiama, kokius duomenis tiekėjas gali gauti tvarkymui, ir nurodoma, kad tiekėjas neturi teisės naudoti įstaigos duomenų jokiems kitiems tikslams, išskyrus sutartyje numatytus (pvz., draudžiama naudoti surinktus duomenis savo DI modelių tobulinimui, nebent gautas atskiras rašytinis leidimas). Taip pat sutartyse nustatoma, kad tiekėjas privalo imtis visų Reglamento (ES) 2016/679 reikalaujamų priemonių, o įstaiga išlieka duomenų valdytoja. **Atsakomybė ir garantijos:** tiekėjas sutartimi patvirtina, kad jo DI sistema atitinka taikomus įstatymus (pvz., jei sprendimas priskiriamas *didelės rizikos* kategorijai pagal EK DI aktą, tiekėjas turi užtikrinti, kad iki produkto pateikimo rinkai atliktos visos privalomos atitikties įvertinimo procedūros, gautas CE atitikties ženklinimas ir pan.). Tiekėjas taip pat garantuoja, kad produkto veikimas yra dokumentuotas ir leidžia įstaigai vykdyti priežiūrą bei patikrinimus. Įtraukiama sąlyga, leidžianti įstaigai arba jos paskirtiems ekspertams atlikti DI sistemos patikrą (peržiūrėti algoritmo šaltinį ir (ar) testuoti jį naudojant demonstracinius duomenis) tiek pirkimo metu, tiek nustatytais intervalais vykdant priežiūrą. Incidentų atveju tiekėjas įsipareigoja bendradarbiauti: pvz., jei dėl DI sistemos veikimo kiltų incidentas (duomenų saugumo ar klaidingų sprendimų), tiekėjas turi padėti išspręsti problemą, pateikti reikiamą informaciją tyrimui. Sutartys apibrėžia ir atsakomybę už žalą – atsižvelgiant į Reglamento (ES) Nr. 2024/1689 nuostatas, tiekėjas gali prisiimti dalinę ar visą atsakomybę dėl DI klaidų padarytų žalos.

14.3. Tiekėjų patikrinimas: Prieš įsigyjant ar integruojant DI sistemą iš išorės tiekėjo, atliekamas detalus tiekėjo patikimumo ir kompetencijos vertinimas. Įvertinama tiekėjo reputacija, ankstesnė patirtis viešajame sektoriuje, saugumo ir privatumo standartų laikymasis, sertifikatai. Tiekėjų prašoma pateikti informacijos apie jų naudojamus DI modelius, duomenų valdymo praktiką, ar jie taiko „*Privacy by Design*“ ir „*AI Ethics by Design*“ principus savo produktuose. Prašoma, kad tiekėjai laikytųsi *gerąja praktika* pagrįstų standartų (pvz., turėtų savo dirbtinio intelekto etikos politiką arba būtų pasitvirtinę duomenų etikos kodeksą). Perkant DI sistemas, turi būti reikalaujama atskaitomybės – tiekėjai turi demonstruoti etišką požiūrį į duomenų naudojimą.

14.4. Tiekėjų vertinimas ir (ar) auditavimas: administracija periodiškai peržiūri esamų DI sistemų tiekėjų darbą: ar jie vykdo sutartinius įsipareigojimus, ar teikia naujinimus, ar reagavo į nustatytas problemas. Nesilaikant etikos ar saugumo reikalavimų, numatomos sankcijos (sutartyse – nuo reikalavimo ištaisyti trūkumus iki sutarties nutraukimo už esminius pažeidimus). Ateityje, atsižvelgiant į reguliacinius pokyčius, administracija pirmenybę teiks tiekėjams, kurie bus oficialiai sertifikuoti pagal patikimo DI valdymo reguliavimo normas. Taip pat planuojama viešinti informaciją apie administracijos naudojamas DI sistemas ir tiekėjus (laikantis skaidrumo iniciatyvų), todėl tiekėjai skatinami veikti taip, kad galėtų didžiuotis savo sprendimų patikimumu.

14.5. Tiekėjų bendradarbiavimas ir rizikos valdymas: administracija laiko tiekėjus partneriais, atsakingais už saugų DI integravimą, todėl su pasirinktu tiekėju dar prieš diegiant sistemą aptariami ir suderinami rizikų valdymo planai: kartu atliekamas (ar bent peržiūrimas) poveikio duomenų apsaugai vertinimas (jei tiekėjo DI sistemas tvarkys asmens duomenis), aptartos naudojimo ribos (kuriais atvejais sistema tinkama, o kuriais ne), susitariama dėl stebėsenos rodiklių (pvz., sutarta, kokį tikslumo lygį palaikys modelis, kaip greitai tiekėjas reaguos, jei našumas kristų). Numatomos ir atsarginės priemonės:

pvz., jeigu DI paslauga sutriktų, kokia bus atsarginė (angl. *fallback*) procedūra, ar tiekėjas suteiks galimybę laikinai naudoti ankstesnę versiją. DI rizikų valdyme dalyvauja visi suinteresuoti subjektai – įskaitant tiekėjus – bendradarbiaudami tarpusavyje. Administracijos sutartys ir bendradarbiavimo praktika atspindi šį principą: tiekėjas nelaikomas vien tik paslaugos pardavėju, jis tampa atsakingu ekosistemos dalyviu, padedančiu palaikyti DI sistemos patikimumą per visą jo naudojimo laikotarpį.

IV SKYRIUS
STEBĖSENA IR AUDITAVIMAS

15. Siekiant užtikrinti DI sistemų atsekamumą, skaidrumą, informacijos saugumą ir nuolatinį tobulinimą bei vykdant administracijos DI sistemų diegimą, tobulinimą, stebėseną bei patikrinimus ir (ar) auditavimą, atliekami:

15.1. DI sistemų inventorizacija:

15.1.1. Administracija naudoja tik patvirtintas DI sistemas (Taisyklių priedas). Duomenų žemėlapyje pateikiama informacija apie kiekvieną sistemą, kurioje naudojamos DI sistemos: pavadinimas, paskirtis, atsakingas padalinys, savininkas, administratoriai, įdiegimo data, sąsajos su kitomis informacinėmis sistemomis, nuorodos į susijusią dokumentaciją (pvz., poveikio asmens duomenų apsaugai vertinimas (toliau – PDAV, techninės specifikacijos ir pan.).

15.1.2. Duomenų žemėlapis nuolat atnaujinamas. Atsakingi asmenys privalo informuoti DIP ir registruoti naujas DI sistemas iki jų įdiegimo (planavimo stadijoje), taip pat pagal poreikį atnaujinti duomenis apie esamas sistemas. Duomenų žemėlapyje registruojamos vidinės, mišrios ir išorinės DI sistemos jei jos yra patvirtintos ir naudojamos administracijos veikloje. Duomenų žemėlapis užtikrina atskaitomybę priežiūros institucijoms ir visuomenei.

15.1.3. Inventorizacija vykdoma reguliariai ir yra svarbi ne tik DI sistemų valdymui, bet ir informacijos saugumo užtikrinimui – žinant visas veikiančias DI sistemas, galima reguliariai vykdyti rizikų vertinimus, užtikrinti ir kontroliuoti informacijos saugumą, atsižvelgiant į Reglamento (ES) Nr. 2024/1689 reikalavimus.

15.2. Peržiūros ir (ar) auditai:

15.2.1. kiekvienai DI sistemai nustatomas peržiūros ir (ar) audito periodiškumas, priklausomai nuo rizikos lygio ir svarbos:

15.2.1.1. didelės rizikos DI sistemos audituojamos ne rečiau kaip vieną kartą per metus ir prieš pradedant taikyti;

15.2.1.2. vidutinės, mažos ir labai mažos rizikos DI sistemoms taikomos supaprastintos peržiūros ir ne rečiau kaip vieną kartą per metus savianalizės būdu patikrinama, ar DI sistemos dirba numatytu režimu ir neatsirado naujų rizikų.

15.2.2. peržiūros gali būti atliekamos tiek administracijos specialistų, tiek pasitelktų išorinių ekspertų, o auditai atliekami išorinių nepriklausomų auditorių, turinčių kompetenciją vertinti DI sistemas. Peržiūros ir (ar) audito metu tikrinama ir peržiūrima:

15.2.2.1. ar DI sistema nepažeidžia nustatytų reikalavimų (šių Taisyklių, administracijos direktoriaus tvirtinamos Dirbtinio intelekto taikymo politikos ir kitų DI reglamentuojančių teisės aktų);

15.2.2.2. ar rezultatai atitinka lūkesčius (tikslumas, efektyvumas);

15.2.2.3. ar neatsirado šališkumo arba poslinkio (angl. *model drift*);

15.2.2,4. ar veikia įdiegtos kontrolės mechanizmai (pvz.: ar kaupiami žurnaliniai įrašai, ar veikia žmogaus priežiūros mechanizmai);

15.2.2.5, ar nepasikeitė DI sistemos rizikos lygis (pvz., išplitus naujam naudojimo būdui ar dėl sistemos sujungimo su naujais duomenų šaltiniais).

15.2.3. peržiūros ir (ar) audito rezultatai dokumentuojami ir pateikiami administracijos direktoriui. Jei aptinkama neatitikčių, problemų arba rizikų, inicijuojamos techninės ir (ar) organizacinės priemonės, kurios įtraukiamos į administracijos rizikų valdymo priemonių planą. Esant būtinumui, gali būti inicijuoti ir atlikti neeiliniai peržiūra ir (ar) auditas.

15.3. Žurnaliniai įrašai ir atsekamumas:

15.3.1. visos DI sistemos privalo generuoti ir saugoti veiklos žurnalinius įrašus (angl. *Log Files*), kurie fiksuoja pagrindinius DI sistemos veiksmus ir rezultatus;

15.3.2. didelės rizikos DI sistemų žurnaliniuose įrašuose turi atsispindėti: kokie duomenys ar užklausos gautos, koks modelio sprendimas priimtas, kokia tikimybė ar balas priskirtas (jei taikoma), sprendimo data ir laikas bei unikalus sprendimo arba įrašo identifikatorius. Ši informacija būtina, kad kilus ginčui ar tyrimo poreikiui būtų galima atskleisti DI sistemos sprendimo aplinkybes ir pagrindimą;

15.3.3. žurnaliniai įrašai taip pat naudojami stebėsenai – atsakingi darbuotojai ar automatinės priemonės analizuoja žurnalų duomenis, siekdami pastebėti anomalijas (pvz., netipinį DI sistemų šabloną, galintį rodyti modelio degradaciją ar galimą išorinę intervenciją). Veiklos registravimas leidžia vėliau patikrinti DI sistemos veikimą ir atsakomybės priskyrimą;

15.3.4. turi būti nustatyti ir Duomenų žemėlapyje pažymėti žurnalinių įrašų saugojimo terminai ir prieigos teisės: žurnaliniai įrašai turi būti saugomi ne trumpiau nei galioja su DI sistemų sprendimais susiję apskundimo terminai arba žurnalinių įrašų terminai gali būti nustatomi vadovaujantis kitais teisės aktais (informacinių sistemų nuostatais, administracijos dokumentacijos planu ir kt.). Prieigą prie visų žurnalinių įrašų gali turėti tik įgalioti asmenys.

15.4. Etikos vertinimai:

15.4.1. etikos patikra yra neatsiejama DI projekto inicijavimo dalis. Svarbiems (kritiniams) DI projektams turi būti atliktas platesnis DI algoritminio poveikio vertinimas (angl. *Algorithmic Impact Assessment*, *AIV*). Toks vertinimas apima galimą socialinį, etinį poveikį, poveikį pagrindinėms teisėms, galimas diskriminacijos ar žalos rizikas, visuomenės pasitikėjimo klausimus;

15.4.2. vadovaujantis gerąja praktika, kiekvienam didelės rizikos DI projektui sudaro tarpdisciplininę vertinimo grupę (įtraukiant teisininkus, etikos specialistus, IT ekspertus, duomenų apsaugos pareigūną (toliau – DAP), paslaugų administratorių ir prireikus – atstovą iš visuomenės ar grupės, kurią gali paveikti sprendimas). Ši grupė identifikuoja galimas problemas ir pateikia rekomendacijas, kaip projektą koreguoti prieš diegiant (pvz.: papildomas duomenų filtras, stipresnis žmogaus priežiūros lygis, komunikacijos planas visuomenei).

16. Vykdant stebėseną, vertinimus, peržiūras ir (ar) auditus, remiamasi tarptautiniais įrankiais ir standartais ar specializuotomis gairėmis (pvz., Europos Sąjungos parengtomis patikros priemonėmis DI patikimumui).

17. Tobulinimas ir problemų arba incidentų valdymas:

17.1. Stebėsenos, vertinimo, peržiūros ir (ar) audito metu nustatytos klaidos (spragos) ar sutrikimai DI sistemose nedelsiant registruojami ir sprendžiami incidentai.

17.2. Problemų ir (ar) incidentų valdymas apima:

17.2.1. DI sistemos naudojimo stabdymas, jei paaiškėja, kad dėl jos įvyko rimtas neigiamas poveikis (pvz., neteisingai atmestos šimtų žmonių paraiškos dėl sisteminės klaidos);

17.2.2. administracijos direktoriaus ir atsakingų darbuotojų informavimas ir, jei incidentas susijęs su asmens duomenimis ar teikiamos paslaugos sutrikdymu;

17.2.3. paveiktų asmenų informavimas, jeigu yra pavojus jų teisėms ir (ar) privatumui arba tai būtina jų teisėms apginti;

17.2.4. išsami problemos arba incidento priežasčių analizė, problemos ataskaitos ir prevencijos priemonių planas;

17.2.5. apie aukščiausio ir aukšto prioriteto problemas ir (ar) incidentus privaloma pranešti kompetentingoms institucijoms.

17.3. Jeigu aptinkamas reikšmingas nuokrypis (pvz., DI modelis pradeda dažniau klysti dėl pasikeitusių duomenų tendencijų), iš karto registruojama problema ir inicijuojamas modelio perkūrimas arba mokymas iš naujo su aktualesniais duomenimis. Visos korekcijos, modelio versijų pakeitimai dokumentuojami.

V SKYRIUS
INFORMACIJOS SAUGUMAS

18. Administracijos darbuotojai veikloje taikydami DI užtikrina informacijos saugumą, taiko būtinas technines bei organizacines priemones, siekiant nepažeisti kibernetinio saugumo ir asmens duomenų apsaugos reikalavimų.

19. Informacijos saugumas

19.1. informacijos saugumas užtikrinamas kibernetinio saugumo ir asmens duomenų apsaugos techninių ir organizacinių priemonių pagalba;

19.2. diegiant naujas DI sistemas privalomai atliekamas rizikos vertinimas ir techninių bei organizacinių priemonių peržiūra. Siekiant sumažinti nustatytas rizikas, tobulinamos esamos arba inicijuojamos ir diegiamos naujos techninės ir (ar) organizacinės priemonės;

19.3. konfidencialumas (privatumas), vientisumas ir prieinamumas DI sistemose turi būti įdiegtas nuo pat pradžių (angl. *by design and/or by default*). DI sistemų ar sprendimų kūrimo procese taikomas „įdiegtas ir numatytasis“ konfidencialumo, vientisumo ir pasiekiamumo principas. Tai reiškia, kad jau kuriant algoritmus ir renkant duomenis numatomos techninės ir organizacinės priemonės informacijos saugos užtikrinimui. Pavyzdžiui, duomenys anonimizuojami ar pseudonimizuojami, kiek tai įmanoma pasiekiant funkcinius tikslus, prieigą prie duomenų turi tik įgalioti asmenys, taikoma duomenų šifravimo, segmentavimo, griežto saugojimo terminų praktika ir prieigų valdymo politika;

19.4. kiekvienai DI sistemai, veikiančiai kaip atskira informacinė sistema, turi būti aiškiai nustatytas duomenų valdytojas ir tvarkytojas (-ai);

19.5. taikomos ir (ar) diegiamos naujos DI sistemos neturi pažeisti administracijos kibernetinio saugumo;

19.6. DI taikomas vadovaujantis asmens duomenų apsaugos pagrindiniais principais:

19.6.1. skaidrumas – administracija aiškiai komunikuoja naudotojams IS arba aplikacijų (programinės įrangos) taisyklėse, pranešimuose ir (ar) privatumo politikoje, kad asmens duomenys tvarkomi naudojant DI sistemas, pateikia teisinį pagrindą ir nurodo tikslus. Automatizuotų sprendimų atveju, kurie daro teisinį ar panašų reikšmingą poveikį asmeniui, turi būti užtikrinamas Reglamento (ES) 2016/679 nuostatų laikymasis: be žmogaus įsikišimo tokie sprendimai asmenims nėra daromi, išskyrus įstatymų numatytas išimtis, o jei daromi – asmuo informuojamas apie galimybę reikalauti, kad sprendimą peržiūrėtų žmogus;

19.6.2. teisėtumas (pagrįstumas) – visų DI sistemų taikymas turi būti pagrįstas, t. y. asmens duomenų tvarkymas, naudojant DI, turi turėti teisėtą pagrindą – vykdoma sutartis, teisinė prievolė arba duomenų subjekto gyvybiškai svarbių teisių apsauga, yra nustatytas aiškus duomenų valdytojo arba trečiosios šalies tesėtas interesas, kuris yra viršesnis už duomenų subjekto interesus, arba yra gautas duomenų subjekto sutikimas tvarkyti asmens duomenis;

19.6.3. tikslingumas – prieš pradedant naudoti naujus duomenų šaltinius DI sistemos modeliui, būtina įvertinti, ar nėra alternatyvų (pvz., sintetinių duomenų) ir kaip asmens duomenų tvarkymas dera su pirminiais tikslais, dėl kurių duomenys buvo surinkti;

19.6.4. būtinumas (minimizavimas) – renkami ir apdorojami tik tie asmens duomenys, kurie būtini konkrečiai DI sistemai įgyvendinti. Planuojant ir (ar) projektuojant DI projekto architektūrą, būtina

įvertinti, kuriuos asmens duomenis būtina naudoti, kad pasiekti nustatytą tikslą (tikslus) ir apsiriboti mažiausiu reikalingu jų kiekiu;

19.6.5. proporcingumas – dideli duomenų rinkiniai gali būti naudojami DI mokymui, tačiau privalu užtikrinti, kad tai būtų daroma teisėtai ir proporcingai. Pagal Reglamento (ES) 2016/679 principus tvarkomi duomenys turi būti tikslūs, tinkami, aktualūs ir ne pertekliniai konkrečiam DI taikymui.

19.6.6. tikslumas – taikant DI, asmens duomenys negali būti tyčia arba netyčia iškraipyti ar kitaip iškreipti ir tokiu būdu klaidinti naudotojus;

19.6.7. baigtumas – DI taikymas neturi pažeisti nustatytų asmens duomenų tvarkymo terminų, susietų su tikslingumu tvarkyti asmens duomenis. Jeigu DI taikymas pakeičia prieš tai nustatytus terminus ir tai yra pagrįsta, asmens duomenų tvarkymo terminai turi būti pakeisti, kartu pakečiant ir teisės aktus ar sutartis, kuriuose tokie terminai yra nustatyti, ir pažymėti Duomenų žemėlapyje;

19.6.8. saugumas – DI sistemos neturi pažeisti arba žymiai pabloginti asmens duomenų apsaugą nuo praradimo, netyčinių veiksmų ir (ar) išorinių atakų;

19.6.9. atskaitomybė – DI sistemos turi nepažeisti atskaitomybės principo – valdytojo gebėjimo įrodyti, kad yra laikomasi asmens duomenų tvarkymo principų.

19.7. Taikant DI, privaloma vadovautis Reglamento (ES) 2016/679 reikalavimais ir užtikrinti asmens duomenų subjektų teises:

19.7.1. būti informuotam apie asmens duomenų tvarkymą;

19.7.2. susipažinti su savo asmens duomenimis;

19.7.3. ištaisyti arba papildyti savo asmens duomenis;

19.7.4. apriboti arba sustabdyti asmens duomenų tvarkymą;

19.7.5. perkelti asmens duomenis kitam duomenų valdytojui arba tvarkytojui;

19.7.6. ištrinti savo asmens duomenis (kai taikoma);

19.7.7. pateikti skundą apie asmens duomenų apsaugos pažeidimą.

19.8. Planuojant ir (ar) projektuojant DI sistemų taikymą iki DI sistema bus pradėta naudoti, būtina atlikti PDAV, kuris padeda ankstyvoje stadijoje nustatyti ir sumažinti asmens duomenų apsaugos pažeidimo rizikas. PDAV atliekamas prieš diegiant DI sistemą, tokiu būdu užtikrinant, kad būtų numatytos tinkamos techninės ir (ar) organizacinės priemonės rizikoms mažinti. Vertinimą inicijuoja ir organizuoja DI sistemos savininkas, vykdo administratorius (administratoriai), dalyvauja DAP, kibernetinio saugumo vadovas (toliau – KSV), DIP ir kiti suinteresuoti arba atsakingi asmenys, kurie padeda nustatyti galimas grėsmes ir užtikrinti atitiktį teisės aktų reikalavimams. Jei PDAV metu nustatoma, kad lieka didelė nepašalinta rizika asmens duomenų apsaugai ir (ar) duomenų subjektų teisėms (pvz., DI galimai pažeistų duomenų subjektų konfidencialumą), prieš pradedant tokį tvarkymą privaloma informuoti priežiūros instituciją (Valstybinė duomenų apsaugos inspekcija).

19.9. Pasitelkiant išorinius DI sistemų ir (ar) paslaugų teikėjus, privaloma sudaryti duomenų tvarkymo sutartis, kuriose būtų apibrėžtas Reglamento (ES) 2016/679 reikalavimų užtikrinimas, vykdant DI sistemos pirkimo ir (ar) paslaugų teikimo sutartį.

19.10. Administracijoje užtikrinamas informacijos saugumo pažeidimų (incidentų), susietų su DI taikymu, valdymas:

19.10.1. pastebėjus arba įvykus informacijos saugumo (kibernetinio saugumo incidentui, elektroninės informacijos saugos arba asmens duomenų apsaugos pažeidimui) incidentui, susietam su DI taikymu, administracijos darbuotojas privalo nedelsdamas, bet ne vėliau kaip per 1 val. registruoti incidentą atsakingam darbuotojui ir informuoti savo tiesioginį vadovą, DIP bei priklausomai nuo incidento tipo – KVS, DAP ir saugos įgaliotinį (toliau – SĮ);

19.10.2. gavę informacijos apie informacijos saugumo incidentą, atsakingi asmenys, savo atsakomybių ribose imasi veiksmų:

19.10.2.1. tiesioginis vadovas užtikrina techninių ir organizacinių priemonių taikymą, siekiant sustabdyti arba sumažinti (minimizuoti) informacijos saugumo pažeidimo poveikį iki priimtino lygio, mobilizuoti ir koordinuoti pavaldžių darbuotojų veiklą ir užtikrinti būtiną kitų atsakingų asmenų (DIP, KSV, DAP ir SĮ) informavimą apie atliktus veiksmus;

20. DIP, KVS, DAP ir SĮ savo atsakomybių ribose įvertina pažeidimo galimą poveikį ir inicijuoja bei koordinuoja techninių ir organizacinių priemonių įgyvendinimą, siekiant nustatyti ir pašalinti informacijos saugumo pažeidimo priežastį (priežastis) bei pasekmes.

21. Kai informacijos pažeidimas susietas su DI sistemų taikymu, DIP komunikuoja administracijos direktoriui apie pažeidimą ir jo valdymą.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

22. Taisyklės peržiūrimos ne rečiau kaip vieną kartą per metus.

23. Už Taisyklių peržiūrą ir atnaujinimą atsakingas Taisyklių savininkas – DIP.

_____

Šakių rajono savivaldybės administracijos
dirbtinio intelekto taikymo taisyklių
priedas

LEIDŽIAMŲ NAUDOTI DIRBTINIO INTELEKTO SISTEMŲ SĄRAŠAS

Eil. Nr.	Dirbtinio intelekto sistemos naudojimo pradžia (data)	Dirbtinio intelekto sistemos pavadinimas	Taikymo sritis ir (ar) ribojimai	Tipas*
1.	2025-11-01	Microsoft Copilot	Vidiniai administracijos duomenys (be asmeninių duomenų). Naudotojai – administracijos deleguoti darbuotojai (testuotojai).	Vidinė
2.	2025-11-01	OpenAI (ChatGPT)	Vidiniai administracijos duomenys (be asmeninių duomenų) Naudotojai – administracijos deleguoti darbuotojai (testuotojai).	Vidinė

Pastabos:
* Tipas – vidinė, mišri, išorinė

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Šakių rajono savivaldybės administracija
Dokumento pavadinimas (antraštė)	Įsakymas dėl Šakių rajono savivaldybės administracijos dirbtinio intelekto taikymo taisyklių patvirtinimo
Dokumento registracijos data ir numeris	2025-11-07 Nr. AT-706
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Vytautas Ižganaitis Administracijos direktorius
Parašo sukūrimo data ir laikas	2025-11-07 12:19
Parašo formatas	Ilgalaikio galiojimo (XAdES-XL)
Laiko žymoje nurodytas laikas	2025-11-08 00:02
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA ECC
Sertifikato galiojimo laikas	2024-07-30 08:15 - 2028-07-29 08:15
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	DI_taisykles.docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20251030.1
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2025-11-10)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2025-11-10 nuorašą suformavo Irena Bacevičienė
Paieškos nuoroda	-
Papildomi metaduomenys	Nuorašą suformavo 2025-11-10 Dokumentų valdymo sistema „Kontora“