ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

ĮSAKYMAS
DĖL ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIRBTINIO INTELEKTO TAIKYMO POLITIKOS 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 politiką (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. d. įsakymu Nr.

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIRBTINIO INTELEKTO TAIKYMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Dirbtinio intelekto taikymo politika (toliau – Politika) nustato dirbtinio intelekto (toliau – DI) atsakingo naudojimo Šakių rajono savivaldybės administracijoje (toliau – administracija) veikloje principus, užtikrinant informacijos saugumą, privatumą, etiką, atskaitomybę, skaidrumą ir teisėtumą.

2. Politikos tikslas – nustatyti pagrindines administracijos DI taikymo sritis ir principus, užtikrinant administracijos veiklos optimizavimą, atsižvelgiant į administracijos veiklą, procesus, teisės aktais priskirtas funkcijas, strateginius tikslus, teikiamas paslaugas bei teisės aktus, reglamentuojančius DI taikymą.

3. DI taikymo tikslai:

3.1. optimizuoti administracijos veiklą, procesus bei vidaus administravimą;

3.2. užtikrinti efektyvų ir kokybišką administracijos informacinių technologijų (toliau – IT), IT infrastruktūros, informacinių sistemų (toliau – IS), priemonių, duomenų valdymą ir administracijos paslaugų teikimą;

3.3. padėti administracijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau kartu – darbuotojai), efektyviai ir kokybiškai vykdyti priskirtas funkcijas, pavedimus, užduotis.

4. DI taikymo sritys:

4.1. administracijos administravimas:

4.1.1. personalo valdymas;

4.1.2. biudžeto planavimas, finansų analizė, prognozavimas;

4.1.3. darbotvarkių, susitikimų planavimas ir protokolavimas.

4.2. administracijos dokumentacija (administracinė, teisinė, techninė ir kita):

4.2.1. dokumentų rengimas, vertimas, analizė, klasifikavimas, santraukų kūrimas, paieška ir tūrinio tikrinimas (pvz., šablonų ataskaitų, sutarčių generavimas);

4.2.2. teisinių rizikų analizė ar atitikties tikrinimas;

4.2.3. techninės dokumentacijos generavimas (pvz., IT sistemų aprašymų sudarymas, schemų rengimas ir kita);

4.3. administracijos IT infrastruktūra, IS, priemonės, duomenys ir teikiamos paslaugos:

4.3.1. duomenų analitikos sprendimai (statistinė analizė, prognozės, anomalijų aptikimas);

4.3.2. IT pagalba ir paslaugų naudotojų konsultavimas;

4.3.3. informacinių sistemų pranešimų, užklausų, el. laiškų klasifikavimas, prioritezavimas, kategorizavimas ir kita;

4.3.4. informacijos saugumo informacinių sistemų pranešimų ir užklausų analizė, pažeidžiamumų aptikimas ir prevencija;

4.3.5. duomenų kokybės, nuoseklumo, tikslumo tikrinimas;

4.4. administracijos veikla, procesai, teisės aktais priskirtų funkcijų vykdymas:

4.4.1. procesų, projektų, sutarčių valdymas;

4.4.2. paslaugų stebėsena, analizė ir prognozavimas;

4.4.3. skundų, prašymų, užklausų nagrinėjimas (pvz., skaitmeninis sprendimų priėmimas dėl paslaugų suteikimo, pakeitimo ar nutraukimo);

4.4.4. veiklos analizė ir ataskaitos;

4.5. kitos sritys, suderintos su Dirbtinio intelekto pareigūnu (toliau – DIP) ir patvirtintos administracijos direktoriaus:

4.5.1. tęstiniai, pilotiniai arba eksperimentiniai projektai ir DI sistemos;

4.5.2. nauji procesai ir (ar) funkcijos;

4.5.3. kitos suderintos ir patvirtintos sritys.

5. DI sistema – mašina grindžiama sistema, suprojektuota 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. Ji gali būti kuriama, diegiama ir (ar) taikoma vadovaujantis Politikoje nustatytais pagrindiniais DI taikymo principais..

6. Politika taikoma administracijos struktūriniams padaliniams, darbuotojams ir veikloms, susijusioms su DI taikymu (sprendimai, kūrimas, diegimas, viešieji pirkimai ir t. t.).

7. Politikoje 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
DI TAIKYMO PRINCIPAI

8. Pagrindiniai DI taikymo principai:

8.1. Rizikingumas (rizikų valdymas) – visos DI sistemos klasifikuojamos pagal rizikos lygį, remiantis Reglamente (ES) Nr. 2024/1689 nustatytomis rizikų kategorijomis:

8.1.1. labai didelė rizika (nepriimtina rizika, kai yra draudžiami tokie DI naudojimo atvejai kaip socialinis reitingavimas ar kenksminga manipuliacija);

8.1.2. didelė rizika (DI sistemos, galinčios paveikti asmens saugumą, sveikatą ar teises);

8.1.3. vidutinė rizika (ribotos rizikos atvejai, kuriems taikomi skaidrumo reikalavimai);

8.1.4. maža (minimali rizika būdinga daugumai įprastų DI taikymų, pvz., el. laiškų šlamšto filtrai);

8.1.5. labai maža rizika (kai rizika nenustatyta arba jos poveikis yra nykstamai mažas);

8.1.6. labai didelės (nepriimtinos) rizikos DI sistemos administracijos veikloje negali būti naudojamos. Didelės rizikos DI sistemoms taikomi griežti reikalavimai: privalomas rizikos vertinimas ir valdymas, aukštos kokybės mokymo duomenys, veiklos žurnalų (angl. *log files*) kaupimas rezultatų atsekamumui užtikrinti, išsami techninė dokumentacija, aiški informacija naudotojams, teisėtos stebėsenos priemonės, tinkamos bei didelis sistemos patikimumas, saugumas ir tikslumas. Ribotos rizikos DI (pvz.: pokalbių robotai, generatyvinis DI turinys) atvejais turi būti užtikrinamas skaidrumas – naudotojai informuojami, kad sąveikauja su DI, o generuojamas turinys yra atitinkamai pažymėtas. Minimalios rizikos DI naudojimas nėra ribojamas, tačiau net ir tokie projektai turėtų vadovautis atsargumo ir gerosios praktikos principais.

8.2. Informacijos saugumas (kibernetinis saugumas ir asmens duomenų apsauga) – administracijos darbuotojai privalo naudoti tik administracijos leidžiamas ir DI politikos reikalavimus atitinkančias dirbtinio intelekto priemones bei paslaugas, siekiant užtikrinti informacijos saugumą (kibernetinį saugumą ir asmens duomenų apsaugą).

8.3. Pagrindinių žmogaus teisių apsauga – administracija užtikrina, kad DI sistemos būtų taikomos su pagarba pagrindinėms žmogaus teisėms ir nepažeidžiant pagrindinių žmogaus teisių ar laisvių.

8.4. Naudotojų privatumas – administracijos įgyvendinamos DI sistemos turi nepažeisti naudotojų privatumo, o naudotojai, taikydami DI savo veikloje, turi gerbti privatumą.

8.5. Skaidrumas (paaiškinamumas) – DI sistemos turi būti skaidrūs, suprantami tiek darbuotojams, tiek trečiųjų asmenų atstovams.

8.6. Administracijoje taikomi DI sprendimai grindžiami etiškumo principais – jie turi užtikrinti teisingą elgesį su visais asmenimis ir teisingą galimybių, išteklių bei informacijos paskirstymą naudotojų atžvilgiu, laikantis:

8.6.1. nediskriminavimas ir sąžiningumas;

8.6.2. žmogaus kontrolė ir sprendimų priežiūra;

8.6.3. paaiškinamumas ir teisė paaiškinimui;

8.6.4. socialinė nauda ir žalos nedarymas;

8.6.5. atitiktis etikos standartams ir teisės viršenybė.

8.7. Atskaitomybė (atsekamumas) – turi būti užtikrinama, kad už kiekvieną DI sistemų sukūrimą ir (ar) diegimą būtų aiškiai nustatyti atsakingi asmenys – tiek techniniu, tiek sprendimų priėmimo lygmeniu. DI sistemų priežiūra integruojama į administracijos valdymo struktūrą: paskiriami atsakingi darbuotojai, kurie prižiūri DI sistemų gyvavimo ciklą, rizikų valdymą ir atitikimą Politikoje nustatytiems principams.

8.8. Teisėtumas (pagrįstumas) – DI taikymas turi būti teisiškai pagrįstas, naudotojas taikydamas DI sistemas savo veikloje turi vadovautis tiek administracijos vidiniais teisės aktais, tiek kitais galiojančiais teisės aktais, nepažeidžiant nustatytų teisės aktų normų.

III SKYRIUS
ATSAKOMYBĖ

9. Administracijos direktorius atsako už bendrą DI taikymą ir už Politikos įgyvendinimą.

10. Už Politikos įgyvendinimo organizavimą, koordinavimą ir kontrolę atsako asmuo, atsakingas už administracijos DI taikymą – DIP, vadovaudamasis DI taikymo principais ir užtikrindamas rizikų valdymą, informacijos saugumą ir teisėtumą. DIP skiriamas administracijos direktoriaus įsakymu, kartu nurodant ir DIP pavaduojantį asmenį. DIP pavaduoja administracijos direktoriaus įgaliotas asmuo (toliau – DIP pavaduotojas), padedant administracijos saugos įgaliotiniui (-iams) (toliau – SĮ), duomenų apsaugos pareigūnui ir Kibernetinio saugumo vadovui.

11. DIP atlieka šias pagrindines funkcijas:

11.1. vertina ir prižiūri Politikos įgyvendinimą;

11.2. identifikuoja DI taikymo rizikas, apie jas informuoja administracijos direktorių ir (ar) atsakingus darbuotojus – administracijos IS ir (ar) aplikacijų (programinės įrangos) savininkus bei administratorius, taip pat siūlo technines ir (ar) organizacines priemones;

11.3. dalyvauja DI sistemų poveikio vertinime;

11.4. dalyvauja tiriant ir sprendžiant incidentus, susietus su DI taikymu;

11.5. komunikuoja su teisės aktais nustatytomis nacionalinėmis DI kompetentingomis institucijomis (notifikuojančioji, priežiūros, kitos);

11.6. konsultuoja administracijos darbuotojus DI taikymo klausimais;

11.7. organizuoja administracijos darbuotojų DI mokymus ir reguliarų instruktavimą;

11.8. informuoja administracijos direktorių klausimais, susietais su DI taikymu;

11.9. ne rečiau kaip vieną kartą per metus atsiskaito administracijos direktoriui apie DI taikymo veiklas, identifikuotas rizikas ir rizikos mažinimo priemones.

12. Už Politikos įgyvendinimą atsako administracijos IS ir (ar) aplikacijų (programinės įrangos) savininkai ir administratoriai, padedant SĮ.

13. SĮ atlieka šias funkcijas:

13.1. dalyvauja šios Politikos įgyvendinime;

13.2. dalyvauja sprendžiant įvykius, incidentus ir problemas (pažeidžiamumus), susietus su DI taikymu;

13.3. dalyvauja su DI taikymu susietų techninių ir (ar) organizacinių priemonių diegime;

13.4. inicijuoja ir organizuoja administracijos darbuotojų informacijos saugumo mokymus ir reguliarų instruktavimą;

13.5. inicijuoja Politikos pakeitimus.

14. Už DI sistemų taikymą, vadovaujantis Politika bei kitais DI taikymą reglamentuojančiais teisės aktais, tiesiogiai atsakingi administracijos darbuotojai. Administracijos skyrių vedėjai privalo imtis reikiamų priemonių, kad užtikrintų Politikos bei kitų DI taikymą reglamentuojančių teisės aktų nuostatų laikymąsi skyrių veikloje.

15. Už techninių ir organizacinių priemonių įgyvendinimą, įskaitant informacijos saugumo užtikrinimą, rizikų, poveikio asmens duomenų apsaugai vertinimą ir (ar), esant būtinumui, poveikio vertinimą (atliekamas didelės rizikos DI sistemoms, vadovaujantis Reglamento (ES) Nr. 2024/1689 nuostatomis), taikant DI sistemas, atsakingi IT infrastruktūros, paslaugų, IS, aplikacijų (taikomųjų programų) savininkai ir administratoriai.

16. Administracijos darbuotojai privalo laikytis šios Politikos nuostatų ir informuoti atsakingus asmenis apie identifikuotus neatitikimus, rizikas bei informacijos saugumo incidentus (pažeidimus).

V SKYRIUS
VIEŠIEJI PIRKIMAI, STEBĖSENA IR INFORMACIJOS SAUGUMAS

17. Vykdant viešuosius pirkimus dėl DI sistemų bei įgyvendinant DI sistemų viešųjų pirkimų sutartis, turi būti:

17.1. viešųjų pirkimų dokumentuose nustatyti reikalavimai dėl DI, kartu numatant reikalavimus dėl DI sistemų atitikties Reglamento (ES) Nr. 2024/1689 nuostatų užtikrinimo;

17.2. sutartinių įsipareigojimų vykdymo priežiūra ir rizikų valdymas;

17.3. užtikrinamas bendradarbiavimas su DI sistemų tiekėjais.

18. DI informacijos saugumą, sprendimų atsekamumą, skaidrumą ir tobulinimą užtikrina:

18.1. DI sistemų inventorizacija;

18.2. reguliarios DI sistemų peržiūros ir (ar) auditai;

18.3. DI sistemų etikos vertinimai;

18.4. incidentų, susijusių su DI taikymu, valdymas.

19. Taikant DI sistemas, informacijos saugumas užtikrinamas vadovaujantis:

19.1. Reglamentu (ES) Nr. 2024/1689;

19.2. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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);

19.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

19.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

19.5. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

19.6. kitais informacijos saugumą reglamentuojančiais teisės aktais.

20. Administracija užtikrina tinkamą informacinių sistemų saugumo lygį, naudojant visas DI sistemas. Taikant DI, įgyvendinamos informacijos saugumui užtikrinti būtinos ir proporcingos techninės bei organizacinės priemonės, atsižvelgiant į galimas grėsmes (pvz.: duomenų nutekėjimą, modelio perėmimą ar klaidingų duomenų įdiegimą). Kiekvienai DI sistemai atliekamas atskiras informacijos saugumo rizikos vertinimas, įtraukiant informacijos saugumo specialistus. Minimalūs reikalavimai apima: prieigos kontrolę (tik įgalioti naudotojai gali pasiekti DI sistemas ir duomenis), duomenų šifravimą perdavimo ir saugojimo metu (ypač jautriems duomenims), reguliarų pažeidžiamumų testavimą, atnaujinimų diegimą, atsarginį kopijavimą.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

1. Politikos nuostatų privalo laikytis visi administracijos darbuotojai.
2. Politika peržiūrima ne rečiau kaip vieną kartą per metus.
3. Už Politikos peržiūrą ir atnaujinimą atsakingas Politikos savininkas – DIP.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Šakių rajono savivaldybės administracija
Dokumento pavadinimas (antraštė)	Įsakymas dėl Šakių rajono savivaldybės administracijos dirbtinio intelekto taikymo politikos patvirtinimo
Dokumento registracijos data ir numeris	2025-11-06 Nr. AT-699
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	2025-11-06 13:35
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
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_politika.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 (2025-11-06)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2025-11-06 nuorašą suformavo Irena Bacevičienė
Paieškos nuoroda	-
Papildomi metaduomenys	Nuorašą suformavo 2025-11-06 Dokumentų valdymo sistema „Kontora“