PATVIRTINTA
Akcinės bendrovės Klaipėdos valstybinio jūrų uosto direkcijos stebėtojų tarybos
2026 m. birželio 25 d. sprendimu
(2026 m. liepos 13 d. posėdžio protokolo Nr. STP-8/2026)

AKCINĖS BENDROVĖS KLAIPĖDOS VALSTYBINIO JŪRŲ UOSTO DIREKCIJOS DIRBTINIO INTELEKTO TAIKYMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Akcinės bendrovės Klaipėdos valstybinio jūrų uosto direkcijos dirbtinio intelekto taikymo politika (toliau – Politika) nustato dirbtinio intelekto (toliau – DI) atsakingo naudojimo akcinės bendrovės Klaipėdos valstybinio jūrų uosto direkcijos (toliau – KVJUD) veikloje principus, užtikrinant informacijos saugumą, privatumą, etiką, atskaitomybę, skaidrumą ir teisėtumą.

2. Politikos tikslas – nustatyti pagrindines KVJUD DI taikymo sritis ir principus, užtikrinant KVJUD veiklos optimizavimą, atsižvelgiant į KVJUD veiklą, procesus, teisės aktais priskirtas ir kitas vykdomas KVJUD funkcijas, strateginius tikslus, teikiamas paslaugas bei teisės aktų, reglamentuojančių DI taikymą, reikalavimus.

3. Pagrindinės Politikoje vartojamos sąvokos:

3.1. DI sistema – mašininiu mokymusi grindžiama sistema, suprojektuota veikti įvairiais autonomijos lygiais, kuri po diegimo gali veikti prisitaikydama ir kuri, siekiant aiškių ar numanomų tikslų, naudodama gautos įvesties duomenis, pati daro išvadą, kaip generuoti rezultatus, pavyzdžiui: įžvalgas, 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.

3.2. Generatyvinis dirbtinis intelektas (toliau – turinį kuriantis DI) – tolesnis DI išplėtimas, apimantis sistemas ir algoritmus, gebančius savarankiškai generuoti turinį – tekstą, vaizdus ar kitų formų duomenis.

3.3. DI pareigūnas (toliau – DIP) – darbuotojas, atsakingas už DI taikymą KVJUD.

4. Kitos 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).

5. DI taikymo tikslai KVJUD:

5.1. optimizuoti KVJUD veiklą, procesus bei vidaus administravimą;

5.2. užtikrinti efektyvų ir kokybišką KVJUD tinklų ir informacinių sistemų bei duomenų valdymą;

5.3. padėti KVJUD darbuotojams efektyviai ir kokybiškai vykdyti priskirtas funkcijas, pavedimus, užduotis.

6. DI taikymo sritys KVJUD:

6.1. KVJUD veiklos organizavimas:

6.1.1. personalo valdymas;

6.1.2. biudžeto planavimas, finansų ir veiklos analizė, prognozavimas;

6.1.3. uosto paslaugų ir operacijų stebėsena, analizė ir prognozavimas;

6.1.4. laivybos planavimo rekomendacijos, infrastruktūros apkrovos, meteorologinių / hidrografinių duomenų, rizikų analizė ir incidentų prevencija;

6.1.5. darbotvarkių, posėdžių, susitikimų, pasitarimų planavimas ir jų eigos fiksavimas (protokolavimas);

6.2. KVJUD veikloje sudaromos dokumentacijos tvarkymas:

6.2.1. dokumentų rengimas, vertimas, analizė, klasifikavimas, santraukų kūrimas, paieška ir turinio tikrinimas;

6.2.2. teisinių rizikų analizė ar atitikties tikrinimas;

6.2.3. techninės dokumentacijos generavimas (pvz., informacinių technologijų sistemų aprašymų sudarymas, schemų rengimas ir kita);

6.3. KVJUD informacinių technologijų infrastruktūros, informacinių sistemų, duomenų ir teikiamų paslaugų priežiūra:

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

6.3.2. IT pagalba ir informacinių sistemų naudotojų konsultavimas;

6.3.3. informacinių sistemų pranešimų, užklausų, el. laiškų klasifikavimas, prioretizavimas, kategorizavimas ir kita;

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

6.3.5. duomenų kokybės, nuoseklumo, tikslumo tikrinimas;

6.4. kitų sričių, suderintų su DIP ir patvirtintų KVJUD generalinio direktoriaus, valdymas:

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

6.4.2. nauji procesai ir (ar) funkcijos;

6.4.3. kitos suderintos ir patvirtintos sritys.

II SKYRIUS
DI TAIKYMO PRINCIPAI

7. Pagrindiniai DI taikymo principai:

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

7.1.1. nepriimtina rizika (aukščiausio lygio rizika, kai yra draudžiami tokie DI naudojimo atvejai, kurie nesuderinami su ES vertybėmis ir pagrindinėmis žmogaus teisėmis, pvz., socialinis reitingavimas ar kenksminga manipuliacija ir kt.);

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

7.1.3. ribota rizika (vidutinės rizikos atvejai, kuriems taikomi skaidrumo reikalavimai);

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

7.1.5. nepriimtinos rizikos DI sistemos KVJUD 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 ir tinkamos stebėsenos priemonės, didelis sistemos patikimumas, saugumas ir tikslumas. Ribotos rizikos DI (pvz.: pokalbių robotai, turinį kuriantis DI) 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;

7.1.6. informacijos saugumas (kibernetinis saugumas ir asmens duomenų apsauga) – KVJUD darbuotojai gali naudoti tik KVJUD leidžiamas ir DI Politikos reikalavimus atitinkančias dirbtinio intelekto priemones bei paslaugas, siekiant užtikrinti informacijos saugumą (kibernetinį saugumą ir asmens duomenų apsaugą).

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

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

7.4. Skaidrumas, paaiškinamumas ir teisė paaiškinimui – DI sistemos veikimas turi būti skaidrus, suprantamas tiek darbuotojams, tiek trečiųjų asmenų atstovams.

7.5. Žmogaus kontrolė ir sprendimų priežiūra – DI sistemos turi būti suprojektuotos taip, kad žmogus galėtų veiksmingai prižiūrėti jų veikimą, suprasti ir, prireikus, įsikišti (pakoreguoti, sustabdyti ar ignoruoti), kad sumažintų riziką.

7.6. Etika (bendroji etika) – DI sistemos turi su visais elgtis teisingai, o galimybes, išteklius ir informaciją paskirstyti teisingai naudotojų atžvilgiu, vadovaujantis etikos principais:

7.6.1. nediskriminavimas ir sąžiningumas;

7.6.2. socialinė nauda ir žalos nedarymas;

7.6.3. atitiktis etikos standartams ir teisės viršenybė.

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

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

III SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

8. KVJUD vadovas atsako už bendrą DI taikymą ir už Politikos įgyvendinimą.

9. Už Politikos įgyvendinimo organizavimą, koordinavimą ir kontrolę atsako DIP, vadovaudamasis DI taikymo principais ir užtikrindamas rizikų valdymą, informacijos saugumą ir teisėtumą. DIP skiriamas KVJUD vadovo sprendimu, kartu nurodant ir DIP pavaduojantį asmenį. DIP atlieka savo funkcijas padedant kibernetinio saugumo vadovui.

10. DIP atlieka šias pagrindines funkcijas:

10.1. vertina ir prižiūri Politikos įgyvendinimą;

10.2. identifikuoja DI taikymo rizikas, apie jas informuoja KVJUD vadovą ir (ar) atsakingus darbuotojus – tinklų ir informacinių sistemų savininkus bei administratorius, taip pat siūlo technines ir (ar) organizacines priemones;

10.3. dalyvauja vertinant DI sistemų poveikį;

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

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

10.6. konsultuoja KVJUD darbuotojus DI taikymo klausimais;

10.7. organizuoja KVJUD darbuotojų DI mokymus;

10.8. informuoja KVJUD vadovą DI taikymo klausimais;

10.9. ne rečiau kaip vieną kartą per metus atsiskaito KVJUD vadovui apie DI taikymo veiklas, identifikuotas rizikas ir rizikos mažinimo priemones.

11. Kibernetinio saugumo vadovas atlieka šias funkcijas:

11.1. dalyvauja įgyvendinant Politiką;

11.2. dalyvauja sprendžiant įvykių, incidentų, susietų su DI taikymu, problemas (pažeidžiamumus);

11.3. dalyvauja diegiant su DI taikymu susietas technines ir (ar) organizacines priemones;

11.4. inicijuoja ir organizuoja KVJUD darbuotojų informacijos saugumo mokymus ir reguliarų instruktavimą;

11.5. inicijuoja Politikos pakeitimus.

12. Už DI sistemų taikymą, vadovaujantis Politika bei kitais DI taikymą reglamentuojančiais teisės aktais, tiesiogiai atsakingi KVJUD darbuotojai. KVJUD padalinių vadovai privalo imtis reikiamų priemonių, kad užtikrintų Politikos bei kitų DI taikymą reglamentuojančių teisės aktų nuostatų laikymąsi padalinio veikloje.

13. Už techninių ir organizacinių priemonių įgyvendinimą, įskaitant informacijos saugumo užtikrinimą, rizikų, poveikio asmens duomenų apsaugai vertinimą ir (ar), jei būtina, poveikio vertinimą (atliekamas didelės rizikos DI sistemoms, vadovaujantis Reglamento (ES) Nr. 2024/1689 nuostatomis), taikant DI sistemas, atsakingi tinklų ir informacinių sistemų savininkai ir administratoriai.

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

IV SKYRIUS
VIEŠIEJI PIRKIMAI, STEBĖSENA IR INFORMACIJOS SAUGUMAS

15. Vykdant pirkimus[1] dėl DI sistemų bei įgyvendinant DI sistemų pirkimų sutartis, turi būti:

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

15.2. užtikrinama sutartinių įsipareigojimų vykdymo priežiūra ir rizikų valdymas;

15.3. užtikrinamas bendradarbiavimas su DI sistemų tiekėjais.

16. Taikant DI sistemas, informacijos saugumas užtikrinamas vadovaujantis:

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

16.2. 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);

16.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

16.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

16.5. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

16.6. kitais informacijos saugumą reglamentuojančiais teisės aktais.

---

[1] Planuodama ir atlikdama pirkimus, vykdydama pirkimo sutartis ir nustatydama pirkimų kontrolės priemones, Uosto direkcija vadovaujasi Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Lietuvos Respublikos viešųjų pirkimų įstatymu, jo įgyvendinamaisiais teisės aktais, kitais įstatymais, Uosto direkcijos mažos vertės pirkimų taisyklėmis ir Uosto direkcijos priimtais vidaus dokumentais.

17. KVJUD 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.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

18. Politikos nuostatų privalo laikytis visi KVJUD darbuotojai.

19. Politika peržiūrima ne rečiau kaip vieną kartą per metus.

20. Už Politikos peržiūrą ir atnaujinimą atsakingas Politikos savininkas – DIP.

_____