

ŽEMAITIJOS NACIONALINIO PARKO DIREKCIJOS DIRBTINIO INTELEKTO NAUDOJIMO POLITIKOS GAIRĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Žemaitijos nacionalinio parko direkcijos (toliau – Direkcija) dirbtinio intelekto naudojimo politikos gairės (toliau – Gairės) reglamentuoja pagrindines nuostatas dėl dirbtinio intelekto ir jo įrankių naudojimo Direkcijos veikloje.

2. Pagrindinės apibrėžtys:

2.1. **Asmens duomenys** – bet kokia informacija arba informacijos rinkinys, pagal kuriuos galima tiesiogiai arba netiesiogiai nustatyti fizinio asmens tapatybę, pavyzdžiui, pagal vardą, pavardę, el. pašto adresą, telefono numerį, gimimo datą, ar kitus požymius, kaip tai nustatyta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau - BDAR).

2.2. **Direkcijos darbuotojas** – Direkcijos valstybės tarnautojas arba darbuotojas, dirbantis Direkcijoje pagal darbo sutartį;

2.3. **Dirbtinis intelektas (DI)** – tai technologijos sritis, kurioje kuriami kompiuteriniai algoritmai, galintys atlikti užduotis, įprastai reikalaujančias žmogaus intelekto. Jie apima, bet neapsiriboja, kalbos supratimu, mokymusi, problemų sprendimu, matymu ar sprendimų priėmimu. DI algoritmai mokomi naudojant didelius duomenų kiekius ir įvairias mokymo strategijas, kad galėtų atpažinti raštus, kalbėti, vertinti ir kt;

2.4. **Dirbtinio intelekto aktas (DI aktas)** – tai Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas 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.

2.5. **DI įrankiai** – visiškai ar iš dalies dirbtiniu intelektu grįsti sprendimai, kurie, atsižvelgiant į tam tikrus žmogaus nustatytus tikslus, suformuluotas užduotis, kuria rezultatus, pavyzdžiui, turinį, prognozes, rekomendacijas ar sprendimus.

3. Gairių tikslas – nustatyti atsakingo ir etiško DI technologijų naudojimo gaires, įtvirtinančias Direkcijos darbuotojams privalomus laikytis ar rekomenduotinus pagrindinius DI ir jo įrankių naudojimo Direkcijos veikloje reikalavimus.

4. Technologinė pažanga leidžia generatyvinio DI modelius integruoti į įvairias aplikacijas – nuo mobiliųjų programėlių iki kompleksinių mokslinių tyrimų sistemų. DI įrankiai gali būti grindžiami vien tik programine įranga ir veikti virtualiajame pasaulyje (pvz., balso sintezatoriai, vaizdo analizės programinė įranga, paieškos sistemos, kalbos ir veido atpažinimo sistemos) arba gali būti integruoti techninėje įrangoje (pvz., pažangiuose robotuose, savaeigėse transporto priemonėse, bepiločiuose orlaiviuose). Dėl šios integracijos ne tik efektyviau veikia aplikacijos, tam tikri veiklos procesai iš dalies ar visai tampa automatizuoti, bet ir kyla įvairių su saugumu bei etika susijusių klausimų.

5. Išorinės sistemos apima bet kokius programinės įrangos įrankius, platformas ar technologijas, kurios priklauso arba yra valdomos išorės tiekėjų, partnerių ar kitų organizacijų. Tai gali būti įvairūs debesijos paslaugų teikėjai, trečiųjų šalių duomenų bazės, aplikacijų programavimo sąsajos (API) paslaugos, programinė įranga kaip paslauga (SaaS) produktai ir kiti išoriniai įrankiai. Šios sistemos suteikia papildomų funkcijų, kurios gali padidinti organizacijos efektyvumą ar prieinamumą, bet taip pat kelia papildomų saugumo ir duomenų privatumo iššūkių.

6. Direkcijos vidiniai duomenys yra informacija, kuri yra sukaupta, tvarkoma ir saugoma Direkcijos vidaus sistemoje ar infrastruktūroje. Tai apima klientų duomenis, darbuotojų informaciją, finansinę informaciją, operacijų duomenis ir bet kokius kitus duomenis, kurie yra sukurti ir valdomi pačios Direkcijos. Vidiniai duomenys yra svarbūs organizacijos privatumo ir saugumo politikai, nes jie dažnai apima konfidencialią informaciją.

7. Direkcijos veikloje naudojami DI įrankiai nėra taikomi automatizuotų sprendimų priėmimui ir automatizuotam subjektų profiliavimui.

II SKYRIUS

DI TAIKymo PRINCIPAI

8. Pagrindiniai DI taikymo principai:

8.1. **Žmogaus kontrolės.** Laikantis šio principo naudojant DI turi būti užtikrinta, kad DI technologijomis grindžiami sprendimai ir kiti veiklos rezultatai būtų nuolat kontroliuojami Direkcijos darbuotojų ir būtų peržiūrimi gavus suinteresuotų asmenų skundų. Direkcijos darbuotojai privalo atlikti DI įrankiais parengtos informacijos ar sprendimų projektų peržiūrą prieš priimdami galutinius sprendimus, ypač jei sprendimai gali turėti reikšmingos įtakos fizinių ar juridinių asmenų teisėms, teisėtiems interesams ar reputacijai. Sprendimų

priėmimas negali bŭti visiškai perduotas DI algoritmams. Naudodamiesi DI sistemomis, darbuotojai turi suprasti jŭ veikimo principus, priskiriamŭ rizikŭ, kaip tai apibrėžta Gairiŭ III skyriuje, vertinti funkcionalumŭ, ŭžinoti jŭ privalumus ir trŭkumus;

8.2. atsakomybės uŭ priimtus sprendimus. DI gali bŭti naudojamas kaip įrankis, kuris padeda vykdyti veiklas, atlikti uŭduotis, siŭlo alternatyvas ar didina darbo efektyvumŭ, taėiau DI turi bŭti naudojamas tik kaip pagalbinis įrankis darbuotojui, nepakeičiant atsakomybės, kompetencijos ar gebėjimo priimti sprendimus. Todėl laikydamiesi ŭio principo, Direkcijos darbuotojai prisiima atsakomybę uŭ savo veiklos padarinius, nepriklausomai nuo to, ar ŭie padariniai kyla dėl ŭmogiŭkujŭ veiksmŭ, ar dėl DI technologijŭ naudojimo;

8.3. atsekamumo. Laikantis ŭio principo uŭtikrinama, kad DI įtaka konkretiems veiklos rezultatams bŭtŭ atskirai nurodoma, kad bŭtŭ galima atsekti, kokie duomenys ir kokiais veiksmais lėmė tam tikrŭ rezultatŭ. Visi reikŭmingi DI veiksmai turi bŭti uŭregistruojami, kad vėliau iŭkilus klausimams ar vykstant tyrimams bŭtŭ galima perŭiŭrėti sprendimo keliŭ ir duomenis;

8.4. kokybės garantijos. Laikantis ŭio principo, turi bŭti uŭtikrinama vienodai aukŭta veiklos kokybė, nepriklausomai nuo to, ar rezultatai grindŭjami materialiais objektais, ŭmogaus veikla, ar skaitmenizuota informacija, robotizuotais procesais ir DI technologijomis. Naudodami DI sugeneruotŭ informacijŭ ar sprendimus, Direkcijos darbuotojai privalo įsitikinti jŭ tikslumu ir tinkamumu naudoti konkreėiu atveju;

8.5. lygiateisiŭkumo. Laikantis ŭio principo, Direkcijos darbuotojai uŭtikrina, kad naudojant DI technologijas visi asmenys bŭtŭ traktuojami lygiai – nevarŭžomos jŭ teisės, jiems neteikiamos privilegijos dėl jŭ lyties, rasės, tautybės, kalbos, kilmės, socialinės ir turtinės padėties, seksualinės orientacijos, iŭsilavinimo, religiniŭ ar politiniŭ paŭiŭrŭ, veiklos rŭšies ir pobŭdŭio, gyvenamosios vietos ir kitŭ aplinkybiŭ. Draudŭiama naudoti ar skleisti DI sugeneruotŭ turinį, kuris gali bŭti diskriminuojantis, ŭeidŭiantis, kitaip neatitinkantis ŭmogaus teisiŭ ir (ar) gali paŭzeisti lygiŭ galimybiŭ principus;

8.6. nepiktnaudŭiavimo. Laikydamiesi ŭio principo, Direkcijos darbuotojai uŭtikrina, kad DI technologijos bŭtŭ naudojamos tik pagal paskirtį ir Direkcijos veiklŭ reglamentuojanėius teisės aktus. DI sistemŭ taikymas galimas tik esant teisiniam pagrindui ir nepaŭeidŭiant DI reglamentuojanėiŭ teisės aktŭ;

8.7. skaidrumo. Laikantis ŭio principo, turi bŭti uŭtikrinamas skaidrus DI taikymas.

Naudotojai turi bŭti informuoti, kai sąveikauja su DI sistema (pvz., virtualiu asistentu ar pokalbiŭ robotu), o DI generuotas turinys privalo bŭti aiŭkiai paŭymėtas, kad bŭtŭ iŭvengta naudotojŭ klaidinimo.

8.8. **paaiškinamumo**. Laikantis šio principo turi būti užtikrinta, kad kiekvienas DI sistemos sprendimas, darantis įtaką asmeniui (pvz., piliečiui atsisakoma suteikti tam tikrą paslaugą remiantis DI įvertinimu), turi būti paaiškinamas suprantama forma to pageidaujanti asmeniui.

8.9. **teisės viršenybės, teisinio reguliavimo ekvivalentiškumo bei atitikties etikos standartams**. Laikantis šio principo, nepriklausomai nuo veiklos skaitmeninimo, robotizavimo ir DI technologijų įtakos, veikloje turi būti laikomasi atitikties ne tik teisės aktų reikalavimams, bet vadovaujamosi teisės principais bei bendromis etikos normomis – sąžiningumu, skaidrumu, pagarba asmens orumui;

8.10. **informacijos saugumo**. Laikantis šio principo, draudžiama DI įrankiuose naudoti slapta, konfidencialią (neskelbtiną), asmeninę informaciją arba specialių kategorijų asmens duomenis (informacija apie sveikatą, biometriniai duomenys, prisijungimo slaptažodžiai, religiniai ir politiniai įsitikinimai, lytinė orientacija ir pan.).

III SKYRIUS DI ĮRANKIŲ RIZIKOS LYGIAI

9. Prieš pradėdant Direkcijos veikloje naudoti DI technologijas turi būti įvertinta kuriam DI įrankių rizikos lygiui priskirtina DI technologija ir jos panaudojimo atvejai.

10. DI įrankiai skirstomi į 4 lygius:

10.1. **Nepriimtinos rizikos** - visi DI įrankiai, kurie laikomi keliančiais akivaizdžią grėsmę žmonių saugumui, pragyvenimo šaltiniams ir teisėms, yra uždrausti ir Direkcijos veikloje nenaudojami. DI aktu draudžiamos šios DI įrankių pagalba vykdomos ir kitos jai prilyginamos praktikos:

10.1.1. žalingas dirbtiniu intelektu grindžiamas manipuliavimas ir apgaulė;

10.1.2. žalingas dirbtiniu intelektu grindžiamas pažeidžiamumų išnaudojimas;

10.1.3. socialiniai reitingai;

10.1.4. atskiros nusikalstamos veikos rizikos vertinimas arba prognozė;

10.1.5. netikslinis interneto ar apsauginės vaizdo stebėjimo sistemos medžiagos nuskaitymas veido atpažinimo duomenų bazėms kurti ar plėsti;

10.1.6. emocijų atpažinimas darbo vietose ir švietimo įstaigose;

10.1.7. biometrinis skirstymas į kategorijas siekiant nustatyti tam tikras saugomas savybes;

10.1.8. tikralaikis nuotolinis biometrinis tapatybės nustatymas teisėsaugos tikslais viešosiose erdvėse.

10.2. **Didelės rizikos** - DI įrankiai, kurių naudojimas gali kelti didelę riziką sveikatai, saugai ar pagrindinėms teisėms bei teisėtiems interesams. Prie tokių gali būti priskirtini DI įrankiai, kuriuos naudojant būtų renkami ir vertinami į Direkciją besikreipiančių asmenų duomenys.

10.3. Prieš naudojant didelės rizikos DI įrankius Direkcijoje, turi būti laikomasi šių reikalavimų:

10.3.1. Įdiegtos tinkamos rizikos vertinimo ir mažinimo sistemos;

10.3.2. Užtikrinti aukštos kokybės duomenų rinkiniai, kuriais grindžiamas DI įrankis, siekiant kuo labiau sumažinti diskriminacinių rezultatų riziką;

10.3.3. Užtikrintas veiklos registravimas siekiant užtikrinti rezultatų atsekamumą;

10.3.4. Parengti išsamūs dokumentai, kuriuose pateikiama visa būtina informacija apie DI įrankį ir jo paskirtį, kad institucijos galėtų įvertinti jo atitiktį;

10.3.5. Pateikta aiški ir tinkama informacija diegėjui;

10.3.6. Sukurtos tinkamos žmogaus vykdomos priežiūros priemonės;

10.3.7. Užtikrintas aukštas patikimumo, kibernetinio saugumo ir tikslumo lygis.

10.4. **Ribotos rizikos** - tai DI įrankiai, susiję su DI naudojimo skaidrumo poreikiu. DI akte nustatytos konkrečios informacijos atskleidimo pareigos siekiant užtikrinti, kad žmonės būtų informuojami, kai to reikia pasitikėjimui išsaugoti. Pavyzdžiui, naudojant DI įrankius, pvz., pokalbių robotus, žmonės turėtų būti informuojami, kad sąveikauja su DI įrankiu, kad galėtų priimti atitinkama informacija pagrįstą sprendimą.

10.5. **Minimalios rizikos arba jokios rizikos** - DI akte nenustatytos taisyklės dėl DI įrankių, kurie laikomi minimalią riziką ar jos nekeliančiais DI įrankiais (pavyzdžiui, darbo administravimo įrankiai tiek, kiek nenulemia reikšmingų sprendimų priėmimo, teksto koregavimo ar vertimo įrankiai, kiek jie naudojami kaip pagalbinė priemonė ir pan.).

IV SKYRIUS

DIREKCIJOS VEIKLOJE NAUDOJAMŲ DI ĮRANKIŲ NAUDOJIMAS IR ADMINISTRAVIMAS

11. Prieš pradėdant naudotis DI įrankį, būtina:

11.1. Peržiūrėti DI įrankio privatumo politiką ir sąlygas, užtikrinant, kad jos atitinka Direkcijos veiklą ir DI įrankių veikimą reglamentuojančius teisės aktus;

11.2. Esant galimybei, DI įrankio nustatymuose išjungti funkciją ir (arba) nepateikti sutikimo naudoti Direkcijos darbuotojo į DI įrankį įkeltus duomenis DI įrankio modelių (algoritimų) tobulinimui, pvz. ChatGPT duomenų valdiklių nustatymuose išjungti funkciją „Patobulinti modelį visiems“.

12. Naudoti tik tuos DI įrankius ir tokia apimtimi, kiek tai neprieštarauja šiose Gairėse bei kituose Direkcijos teisės aktuose nustatytoms sąlygoms.

13. Direkcijos veikloje naudojamų ir leistinų naudoti DI įrankių sąrašas (toliau – DI sąrašas) pateikiamas Direkcijos intranete ir (arba) kitoje Direkcijos darbuotojams prieinamoje vietoje (pvz. dokumentų valdymo sistemoje - DBSIS).

14. Konkrečių DI įrankių palaikymas, atnaujinimas, peržiūra ar atsisakymas remiasi periodiškai gaunamu grįžtamuju ryšiu.

V SKYRIUS DUOMENŲ SAUGA

15. Vertinant DI naudojimo rizikas svarbu atsižvelgti į esamus teisinius reikalavimus, įskaitant BDAR ir DI akto nuostatas. Prieš pradedant tvarkyti asmens duomenis DI įrankių pagalba, būtina atlikti poveikio duomenų apsaugai vertinimą (PDAV), konsultuojantis su duomenų apsaugos pareigūnu. Be to, duomenų tvarkymas turi atitikti BDAR 6 straipsnyje nurodytus teisinius pagrindus.

16. Direkcijos darbuotojams draudžiama DI įrankiuose numatyto funkcionalumo pagalba aktyvuoti prieigą (sąsają) su Direkcijos darbo paskyromis (pvz. Outlook, Sharepoint, Teams) ir (arba) Direkcijos infrastruktūra;

17. Gairių 8.10 ir 16 papunkčiuose nurodyti saugumo apribojimai netaikomi, jeigu DI sąrašė yra nurodytas leidimas konkretų DI įrankį naudoti su konfidencialia (nevieša), asmens duomenų informacija, arba nurodytas leidimas suteikti prieigą prie Direkcijos darbo paskyrų ir Direkcijos infrastruktūros.

VI SKYRIUS ATSAKOMYBĖ

18. Direkcijos darbuotojai prisiima visą su DI įrankių ir jų sukurtų rezultatų naudojimu susijusią atsakomybę tiek galutinio rezultato turinio, tiek jo kokybės prasme, todėl bet koks pagalbinais įrankiais sugeneruotas rezultatas turi būti išsamiai patikrintas.

19. Direkcijos darbuotojai už netinkamą DI įrankių ar jų pagalba sugeneruoto turinio panaudojimą atsako teisės aktų nustatyta tvarka.

VII SKYRIUS KVALIFIKACIJOS KĖLIMAS

20. Esant poreikiui, Direkcijos darbuotojams organizuojami kvalifikacijos kėlimo mokymai dėl DI įrankių naudojimo, DI rinkos tendencijų, taip pat organizuojami specializuoti mokymai konkrečių DI įrankių Direkcijoje savininkams.

VIII SKYRIUS BAIGIAMOSIOS NUOSTATOS

21. Šios Gairės peržiūrimos atsižvelgiant į DI naudojimo technologinius ar reglamentavimo pasikeitimus.

23. Gairės viešai skelbiamos Direkcijos interneto svetainėje www.zemaitijosnpd.lrv.lt.
