AUDITO, APSKAITOS, TURTO VERTINIMO IR NEMOKUMO VALDYMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS DIREKTORIUS

ĮSAKYMAS
DĖL AUDITO, APSKAITOS, TURTO VERTINIMO IR NEMOKUMO VALDYMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS DIRBTINIO INTELEKTO NAUDOJIMO POLITIKOS GAIRIŲ PATVIRTINIMO

2025 m. d. Nr. V1-
Vilnius

Vadovaudamasis Lietuvos Respublikos Seimo 2024 m. gegužės 9 d. rezoliucija Nr. XIV-2620 „Dėl dirbtinio intelekto technologijų naudojimo viešajame sektoriuje principų“, Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnybos prie Lietuvos Respublikos finansų ministerijos nuostatų 10 punktu,

t v i r t i n u pridedamas Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnybos prie Lietuvos Respublikos finansų ministerijos dirbtinio intelekto naudojimo politikos gaires.

Direktorius Audrius Linartas

PATVIRTINTA
Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnybos prie Lietuvos Respublikos finansų ministerijos direktoriaus 2025 m. d. įsakymu Nr. V1-

AUDITO, APSKAITOS, TURTO VERTINIMO IR NEMOKUMO VALDYMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS DIRBTINIO INTELEKTO NAUDOJIMO POLITIKOS GAIRĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Audito, apskaitos, turto vertinimo ir nemokumo valdymo tarnybos prie Lietuvos Respublikos finansų ministerijos (toliau – AVNT) dirbtinio intelekto naudojimo politikos gairės (toliau – Gairės) reglamentuoja pagrindines nuostatas dėl dirbtinio intelekto ir jo įrankių naudojimo AVNT 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. **AVNT darbuotojas** – AVNT valstybės tarnautojas arba darbuotojas, dirbantis AVNT 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 AVNT darbuotojams privalomus laikytis ar rekomenduotinus pagrindinius DI ir jo įrankių naudojimo AVNT 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. AVNT vidiniai duomenys yra informacija, kuri yra sukaupta, tvarkoma ir saugoma AVNT 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 AVNT. Vidiniai duomenys yra svarbūs organizacijos privatumo ir saugumo politikai, nes jie dažnai apima konfidencialią informaciją.

7. AVNT 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 AVNT darbuotojų ir būtų peržiūrimi gavus suinteresuotų asmenų skundų. AVNT 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 DI algoritmams. Naudodamiesi DI sistemomis, darbuotojai turi suprasti jų veikimo principus, priskiriamą riziką, kaip tai apibrėžta Gairių III skyriuje, vertinti funkcionalumą, žinoti jų privalumus ir trūkumus;

8.2. **atsakomybės už priimtus sprendimus**. DI gali būti naudojamas kaip įrankis, 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. Todėl laikydamiesi šio principo, AVNT darbuotojai prisiima atsakomybę už savo veiklos padarinius, nepriklausomai nuo to, ar šie padariniai kyla dėl žmogiškųjų veiksnių, ar dėl DI technologijų naudojimo;

8.3. **atsekamumo**. Laikantis šio principo užtikrinama, kad DI įtaka konkretiems veiklos rezultatams būtų atskirai nurodoma, 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 vykstant tyrimams būtų galima peržiūrėti sprendimo kelią ir duomenis;

8.4. **kokybės garantijos**. Laikantis šio principo, turi būti užtikrinama vienodai aukšta veiklos kokybė, nepriklausomai nuo to, ar rezultatai grindžiami materialiais objektais, žmogaus veikla, ar skaitmenizuota informacija, robotizuotais procesais ir DI technologijomis. Naudodami DI sugeneruotą informaciją ar sprendimus, AVNT darbuotojai privalo įsitikinti jų tikslumu ir tinkamumu naudoti konkrečiu atveju;

8.5. **lygiateisiškumo**. Laikantis šio principo, AVNT darbuotojai užtikrina, kad naudojant DI technologijas visi asmenys būtų traktuojami lygiai – nevaržomos jų teisės, jiems neteikiamos privilegijos dėl jų lyties, rasės, tautybės, kalbos, kilmės, socialinės ir turtinės padėties, seksualinės orientacijos, išsilavinimo, religinių ar politinių pažiūrų, veiklos rūšies ir pobūdžio, gyvenamosios vietos ir kitų aplinkybių. Draudžiama naudoti ar skleisti DI sugeneruotą turinį, kuris gali būti diskriminuojantis, žeidžiantis, kitaip neatitinkantis žmogaus teisių ir (ar) gali pažeisti lygių galimybių principus;

8.6. **nepiktnaudžiavimo**. Laikydamiesi šio principo, AVNT darbuotojai užtikrina, kad DI technologijos būtų naudojamos tik pagal paskirtį ir AVNT veiklą reglamentuojančius teisės aktus. DI sistemų taikymas galimas tik esant teisiniam pagrindui ir nepažeidžiant DI reglamentuojančių teisės aktų;

8.7. **skaidrumo.** Laikantis šio principo, turi būti užtikrinamas skaidrus DI taikymas. 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.

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 pageidaujančiam 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 vadovaujamasi teisės principais bei bendromis etikos normomis – sąžiningumu, skaidrumu, pagarba asmens orumui;

8.10. **informacijos saugumo**. Laikantis šio principo, draudžiama DI įrankiuose naudoti 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.).

III SKYRIUS
DI ĮRANKIŲ RIZIKOS LYGIAI

9. Prieš pradedant AVNT 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 AVNT 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 duomenys dėl AVNT prižiūrimų profesijų atstovų veiklos kokybės.

10.3. Prieš naudojant didelės rizikos DI įrankius AVNT, turi būti 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
AVNT VEIKLOJE NAUDOJAMŲ DI ĮRANKIŲ NAUDOJIMAS IR ADMINISTRAVIMAS

11. Prieš pradedant naudotis DI įrankį, būtina:

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

11.2. Esant galimybei, DI įrankio nustatymuose išjungti funkciją ir (arba) nepateikti sutikimo naudoti AVNT darbuotojo į DI įrankį įkeltus duomenis DI įrankio modelių (algoritmų) 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 AVNT teisės aktuose nustatytoms sąlygoms.

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

14. Konkrečių DI įrankių palaikymas, atnaujinimas, peržiūra ar atsisakymas remiasi periodiškai gaunamu grįžtamuoju 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. AVNT darbuotojams draudžiama DI įrankiuose numatyto funkcionalumo pagalba aktyvuoti prieigą (sąsają) su AVNT darbo paskyromis (pvz. Outlook, Sharepoint, Teams) ir (arba) AVNT infrastruktūra;

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

VI SKYRIUS
ATSAKOMYBĖ

18. AVNT darbuotojai prisiima visą su DI įrankių ir jų sukurtų rezultatų naudojimu susijusią

atsakomybę tiek galutinio rezultato turinio, tiek jo kokybės prasme, todėl bet koks pagalbiniais įrankiais sugeneruotas rezultatas turi būti išsamiai patikrintas.

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

VII SKYRIUS
KVALIFIKACIJOS KĖLIMAS

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

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. AVNT darbuotojai turi būti supažindinti su šiomis Gairėmis.

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

23. Gairės viešai skelbiamos AVNT interneto svetainėje www.avnt.lrv.lt.

1 Priedas

AVNT VEIKLOJE NAUDOJAMŲ IR (ARBA) LEISTINŲ NAUDOTI DI ĮRANKIŲ SĄRAŠAS

Eil. Nr.	Pavadinimas	Šaltinis[1]	Tipas[2]	Paskirtis[3]	Konfidenciali /neviešinama informacija[4]	Fizinių asmenų duomenys[5]	Prieiga prie AVNT infrastruktūros[6]	Naudotojai[7]	Savininkas[8]

1 – Nurodoma DI įrankio interneto svetainė, AVNT infrastruktūra ar kitas sprendimas, kuriame yra įdiegtas DI įrankis.

2 – Nurodoma ar DI įrankis yra išorinis, vidinis arba mišrus.

3 – Nurodoma DI įrankio paskirtis – dokumentų analizė, informacijos santraukų parengimas, teksto vertimas, vaizdinės medžiagos generavimas ir pan.

4 – Nurodoma, ar leidžiama dirbti su konfidencialia ir (arba) viešai neprieinama (neviešinama) informacija.

5 – Nurodoma, ar leidžiama dirbti su fizinių asmenų duomenimis.

6 – Nurodoma, ar DI įrankio naudotojui leidžiama DI įrankiui suteikti prieigą prie AVNT darbo paskyrų ir (arba) AVNT infrastruktūros.

7 – Nurodomi DI įrankio naudotojai. Tai gali būti AVNT kolektyvas, konkretus AVNT skyrius arba darbuotojas, taip pat išorės naudotojai.

8 – Nurodomas konkretus AVNT skyrius ar darbuotojas, kuris yra atsakingas už DI įrankio sukūrimą, modernizavimą ir (arba) administravimą. Konkretus savininkas organizacijoje nenurodomas, jeigu tai yra išorinis DI įrankis (pvz. OpenAI ChatGPT).