Generatyvinio dirbtinio intelekto (GenDI) saugaus naudojimo organizacijoje gairės

Turinys

Tikslas

Šio dokumento tikslas yra pateikti rekomendacijas dėl generatyvinio dirbtinio intelekto (GenDI) naudojimo, ypač akcentuojant informacijos saugumą verslo sričiai ir sukurti struktūrą, kuri padėtų efektyviai ir saugiai integruoti GenDI technologijas į įmonės veiklą, kartu stiprinant jos konkurencingumą ir inovacijų potencialą.

Organizacija turi atsižvelgti ne tik į technologinius ir inovacinius GenDI diegimo aspektus, bet ir į saugumo, privatumo ir etinius aspektus. Siekiame užtikrinti, kad šios priemonės būtų naudojamos atsakingai ir saugiai, atitinkant įmonės ir reguliavimo institucijų reikalavimus.

Dokumente bus paaiškinta, kaip pritaikyti GenDI technologijas verslo procesuose, teikiant aiškias gaires, taisykles ir rekomendacijas. Tai apima skaidrumo principų laikymąsi, asmens duomenų apsaugą, konfidencialios informacijos saugojimą ir etišką naudojimąsi šiomis technologijomis. Siekiame ne tik aprašyti rizikas ir galimas problemas, bet ir pateikti sprendimus, kaip šias problemas spręsti ar išvengti, taip pat pateikti praktines rekomendacijas dėl technologijų naudojimo metodų ir įdiegimo praktikų.

Bendroji dalis

Išorinės sistemos ir vidiniai duomenys

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, 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.

Vidiniai duomenys yra informacija, kuri yra sukaupta, tvarkoma ir saugoma organizacijos vidaus sistemoje ar infrastruktūroje. Tai apima klientų duomenis, darbuotojų informaciją, finansinę informaciją, verslo operacijų duomenis ir bet kokius kitus duomenis, kurie yra sukurti ir valdomi pačios organizacijos. Vidiniai duomenys yra svarbūs organizacijos privatumo ir saugumo politikai, nes jie dažnai apima konfidencialią informaciją. Organizacija gali naudotis vidiniais duomenimis šiais atvejais:

1. Vidinius duomenis galima naudoti be papildomų leidimų, jei jie neapima asmeninių identifikatorių ar kitos jautrios informacijos, kuri gali būti reglamentuojama privatumo įstatymais (pvz., BDAR Europos Sąjungoje). Jei duomenys yra konfidencialūs, jų naudojimą turi reguliuoti vidaus privatumo politikos ir susiję teisiniai reikalavimai.

2. Vidiniai duomenys naudojami siekiant gerinti operacinį efektyvumą, tobulinti procesus ir priimti pagrįstus sprendimus, remiantis tikslia ir patikima informacija.

3. Vidiniai duomenys leidžia organizacijai geriau valdyti rizikas, nes duomenys yra kontroliuojami ir analizuojami pačios organizacijos, užtikrinant, kad bet kokie duomenų analizės ar naudojimo procesai atitiktų organizacijos saugumo standartus ir politikas.

4. Organizacijos gali naudoti savo vidinius duomenis moksliniams tyrimams ir produktų bei paslaugų inovacijoms kurti, neatskleidžiant jautrios informacijos išorinėms šalims.

Įvadas į generatyvinį dirbtinį intelektą

Dirbtinis intelektas (DI) (angl. artificial intelligence, AI) apibūdinamas kaip technologijų sritis, kurioje sukuriami kompiuteriniai algoritmai, galintys atlikti įvairias užduotis, tradiciškai reikalaujančias žmogaus intelekto, tokias kaip kalbos supratimas, mokymasis, problemų sprendimas, matymas ar sprendimų priėmimas. DI algoritmai mokomi naudojant didelius duomenų kiekius ir įvairias mokymo strategijas, leidžiančias jiems atpažinti raštus, kalbėti, vertinti ir kt.

Generatyvinis dirbtinis intelektas (GenDI) yra tolesnis DI išplėtimas, apimantis sistemas ir algoritmus, gebančius savarankiškai generuoti turinį – tekstą, vaizdus ar kitų formų duomenis. GenDI pritaikymas versle suteikia galimybę integravimu įvairiais būdais, papildant tradicinius metodus ir skatinant veiklos efektyvumą.

Žemiau išvardinti įrankiai leidžia per kelias minutes sukurti pilnavertes pateiktis, nurodžius tik reikiamą temą ir (ar) atitinkamus raktažodžius, arba įkėlus turimą konspektą, paskaitos planą ir pan., su integruotu dizainu, grafika ir tekstu.

Pagrindinės GenDI technologijos ir platformos

1. **Tekstus generuojantys modeliai** (pvz., ChatGPT, Playground (OpenAI API), Gemini, Rytr), kurie versle naudojami įtraukiant naujas metodikas ir strategijas. Jie leidžia automatiškai generuoti tekstą, kuris gali praturtinti įmonės veiklą ir efektyvumą.

2. **Vaizdus generuojantys modeliai** (pvz., MidJourney, LeonardoAI, DALL-E, SoRa), suteikiantys galimybę įmonėms greitai ir nesudėtingai kurti originalius grafikos vaizdus, reikalingus skaidrėms, ataskaitoms ir kitoms vizualinėms medžiagoms.

3. **Vaizdo įrašus analizuojantys ir generuojantys modeliai** (pvz., Cockatoo, descript, 2short.AI), naudojami įvairioms verslo užduotims, tokioms kaip trumpų vaizdo įrašų kūrimas, įrašytų garso ar

vaizdo transkribavimas, efektų pridėjimas prie prezentacijų, situacijų analizė bei interaktyvių užduočių rengimas. Transkribavus vaizdo įrašus, galima greitai sukurti mokomąsias skaidres ar pristatymus.

4. **Tekstą analizuojantys modeliai** (pvz., Consesus, ChatPDF, AskPDF), naudingi versle siekiant pagerinti įvairius procesus, nuo einamųjų darbų automatinio vertinimo iki ilgų tekstų sutrumpinimo.

Strateginis planavimas ir analizė

Norint pradėti naudoti generatyvinį dirbtinį intelektą (GenDI), įmonei būtina nustatyti aiškius tikslus ir įvertinti jų atitikimą organizacijos strateginiam planavimui ir informacinių sistemų naudojimui. Tikslų nustatymui reikia apibrėžti metrikas ir svarbiausius veiklos rodiklius (KPI), kurie padės įvertinti investicijų į GenDI grąžą.

Vienas iš tikslų gali būti technologijos analizė, kuri nesiejama su tiesiogine finansine ar ekonomine nauda, tačiau gali atnešti vertingų įžvalgų dėl kitų inovatyvių produktų diegimo ir naudojimo. Šio tikslo metu, sistemos diegimas yra laikinai ribotas, o jo rezultatai ir analizė gali būti pateikiami nestruktūrizuota forma. Svarbiausias šio tipo diegimo rezultatas yra rekomendacijos dėl tolesnių žingsnių.

Kitas tikslas – konkrečių funkcijų ar jų efektyvumo bei produktyvumo didinimas. Šio tipo diegimams nustatomi konkretūs tikslai, o atsakomybė už projekto įgyvendinimą skiriama atitinkamos funkcijos vadovui. IT komandos dalyvauja projekte, bet nėra atsakingos už galutinį funkcijos efektyvumo rezultatą. Svarbu įvertinti įmonės galimybes automatizuoti kelias funkcijas vienu metu ir nustatyti, kurios funkcijų automatizavimas galėtų atnešti didžiausią naudą.

Trečiasis tikslas – sistemos diegimas darbuotojams. Šis diegimo tipas suteikia įmonės darbuotojams galimybę naudotis teikiama sistema ir individualiai ieškoti jos naudos. Čia svarbiausi kriterijai yra veiklos reglamentavimas, įskaitant duomenų apsaugą, teisių valdymą, ir vartotojų mokymai, siekiant užtikrinti, kad darbuotojai efektyviai ir saugiai naudotųsi sistemomis.

Strateginis GenDI planavimas ir analizė leidžia organizacijai maksimaliai išnaudoti šių technologijų teikiamas galimybes, atitinkant verslo tikslus ir optimizuojant veiklos procesus.

Teisinis reguliavimas ir etika

Vertinant dirbtinio intelekto (DI) naudojimo rizikas svarbu atsižvelgti į esamus teisinius reikalavimus, įskaitant ES Bendrojo duomenų apsaugos reglamento[1] (BDAR) ir ES Dirbtinio intelekto akto[2] nuostatas. Kaip duomenų valdytojai, organizacijos privalo laikytis BDAR nustatytų principų, susijusių su asmens duomenų tvarkymu. Tai reiškia, kad prieš pradedant tvarkyti asmens duomenis DI sistemų 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.

Organizacijos turi būti pasirengusios įgyvendinti procesus, kurie užtikrintų duomenų subjektų teisių įgyvendinimą pagal BDAR, ir pateikti savo privatumo politikoje aiškią informaciją apie DI sistemų naudojimą ir jų paskirtį. Svarbu paaiškinti dirbtinio intelekto pagrįstų automatizuotų sprendimų logiką ir pabrėžti galimas rizikas asmenims. Be to, organizacija atlieka DI sistemų atitikties vertinimą, vadovaudamasi Dirbtinio intelekto akte numatytomis procedūromis.

Kalbant apie generatyvinio dirbtinio intelekto (GenDI) naudojimo etinius aspektus, svarbu pabrėžti proporcingumą ir žalos nedarymą – GenDI naudojimas neturi viršyti to, kas būtina siekiant teisėto tikslo. Taip pat skatinamas skaidrus ir nediskriminuojantis naudojimas, užtikrinant, kad GenDI privalumai būtų prieinami visiems. Žmogiškoji peržiūra yra būtina prieš priimant galutinį sprendimą, siekiant užtikrinti, kad galutinio sprendimo priėmimas nebūtų paliktas vien algoritmų sprendimui. Prieš pradedant naudoti GenDI,

[1] Reglamentas - 2016/679 - EN - bendrasis duomenų apsaugos reglamentas - EUR-Lex (europa.eu)
[2] EUR-Lex - ST_7536_2024_INIT - EN - EUR-Lex (europa.eu)

atliekamas išsamus naudojimo ir su juo susijusių galimų rizikų vertinimas, kad būtų galima numatyti ir suvaldyti galimas neigiamas pasekmes.

Duomenų valdymas ir tvarkymas

Duomenų valdymo politikos sukūrimas, atnaujinimas ar išplėtimas yra būtinas, kad būtų užtikrintas saugus duomenų rinkimas, tvarkymas, jų gyvavimo ciklas, taip pat duomenų gavėjų, tiekėjų ir tvarkytojų nustatymas. Ši politika turėtų apimti visus duomenų tvarkymo aspektus, įskaitant duomenų rinkimą, saugojimą, tvarkymą, dalijimąsi ir ištrynimą.

Ypatingą dėmesį reikia skirti dirbtinio intelekto sistemų duomenų valdymui. Pagal ES Dirbtinio intelekto aktą, aukštos rizikos DI sistemoms taikomi skirtingi duomenų valdymo reikalavimai, o vidutinės ir žemos rizikos DI sistemoms – bendros gairės ir rekomendacijos. Svarbu laikytis etiškos duomenų praktikos, užtikrinant privatumą ir skaidrumą, naudojant sąžiningas ir teisėtas duomenų rinkimo priemones. Be to, duomenų kokybė yra gyvybiškai svarbi – duomenų rinkiniai turi būti tikslūs, patikimi, nešališki ir reprezentatyvūs numatytai taikymo sričiai.

Atitikties teisės aktams užtikrinimas, įskaitant vietinius ir tarptautinius duomenų apsaugos teisės aktus, yra būtinas. Organizacijos turi įtraukti nuostatas, susijusias su duomenų subjektų teisėmis, pavyzdžiui, teise susipažinti su duomenimis, teise reikalauti juos ištaisyti ar ištrinti ir reguliariai peržiūrėti atliktus PDAV.

Skaidrumas ir atskaitomybė yra būtini, reikia aiškiai dokumentuoti visus DI sistemų procesus ir sprendimus, siekiant didinti pasitikėjimą DI sistemomis ir užtikrinti, kad jų priimami sprendimai būtų suprantami vartotojams ar reguliuotojams. Taip pat svarbu užtikrinti, kad trečiųjų šalių teikiamos paslaugos laikytųsi atitinkamų duomenų apsaugos ir privatumo standartų.

Įmonė turi pasirengti papildomas gaires, kurios bus skirtos didelės rizikos dirbtinio intelekto sistemoms, apima šališkumo, turinčio įtakos saugumui ar lemiančio diskriminaciją, nustatymą ir mažinimą, kontekstinį aktualumą, kur duomenų rinkiniai turi atspindėti konkrečias geografines ir kontekstines ypatybes, ir išsamios dokumentacijos bei audito reikalavimus, siekiant užtikrinti visapusišką atskaitomybę ir atitiktį.

GenDI saugumo aspektai

Informacijos saugumo klausimai, susiję su generatyviniu dirbtiniu intelektu (GenDI), yra kritiškai svarbūs bet kurioje organizacijoje, kurioje šios technologijos yra taikomos. Rekomenduojama atkreipti dėmesį į:

1. **Atsakomybės ir atskaitomybės identifikavimas**. Būtina aiškiai nustatyti, kas yra atsakingas už GenDI saugumo užtikrinimą organizacijoje. Tai apima atsakomybių ir pareigų paskirstymą tarp komandų ir asmenų.
2. **Supratimas tarp lyderių**. Visi, pradedant valdybos nariais ir baigiant aukščiausio lygio vadovais, turėtų būti gerai informuoti apie GenDI sistemas, jų naudojimo rizikas ir naudą, kad galėtų priimti atsakingus sprendimus.
3. **Įgūdžių ir žinių spragų identifikavimas**. Jei organizacijoje yra žinių ar įgūdžių spragų, susijusių su GenDI sauga, būtina nustatyti strategijas, kaip šias spragas užpildyti.
4. **Dalyvavimas sprendimų priėmime**. Už kibernetinę ir asmens duomenų saugą atsakingi asmenys turėtų būti įtraukti į sprendimų priėmimo procesą dėl GenDI produktų naudojimo.
5. **Rizikos integravimas**. GenDI produktų naudojimo rizika turi būti integruota į esamus organizacijos valdymo procesus, siekiant užtikrinti veiksmingą rizikos valdymą.
6. **Kritinių elementų apsauga**. Svarbu nustatyti, kurie kritiniai infrastruktūros elementai yra ar bus susiję su GenDI, ir kaip šie elementai yra apsaugoti (elementai gali būti esminės sistemos, kritinės paslaugos).
7. **Galimi incidentai**. Organizacija turi suprasti, kas blogiausia gali nutikti, jei GenDI įrankis būtų paveiktas, ir kokios gali būti operacinės ar reputacinės pasekmės.
8. **Reagavimas į incidentus**. Būtina turėti aiškų planą, kaip bus reaguojama į rimtus saugumo incidentus, susijusius su GenDI įrankiu.

9. **Tiekimo grandinės supratimas**. Svarbu suprasti savo duomenų, modelių ir programinės įrangos tiekimo grandines ir galėti užduoti tinkamus klausimus tiekėjams apie jų saugumo praktikas.

Toliau išvardintos priemonės ir procesai yra gyvybiškai svarbūs užtikrinant, kad GenDI naudojimas organizacijoje būtų saugus ir atitiktų visus reglamentuojančius reikalavimus

Saugumo stebėjimas ir palaikymas

1. GenDI sistemų stebėjimas yra būtinas siekiant aptikti saugumo grėsmes.
2. Reguliarūs atnaujinimai užtikrina, kad taikomosios programos būtų saugios ir atnaujintos.
3. Incidentų valdymo planavimas ir vykdymas, reguliarūs saugumo vertinimai ir kodo peržiūros bei saugumo auditai ir atitikties patikros yra būtini, kad būtų išlaikytas aukštas saugumo lygis.
4. Prieigos kontrolės ir autentiškumo nustatymo mechanizmai turi būti įgyvendinti, siekiant užtikrinti, kad prieiga prie sistemų būtų kontroliuojama ir saugi.

GenDI įgyvendinimo etapai

Diegiant generatyvinį dirbtinį intelektą (GenDI) organizacijoje, būtina laikytis metodikos, kuri atitinka IT produktų diegimo etapus. Šie etapai apima technologijos ir platformos pasirinkimą, integravimą į esamą IT infrastruktūrą bei bendradarbiavimą su patikimais ir saugiais paslaugų teikėjais. Visi žemiau išvardinti etapai yra susiję su kruopščiu planavimu, rizikos valdymu ir nuolatiniu vertinimu, kad užtikrintų sklandų ir saugų GenDI įgyvendinimą organizacijoje. Svarbu reguliariai atnaujinti dokumentus, licencijas ir palaikyti nuolatinę komunikaciją su visomis suinteresuotomis šalimis per visą įgyvendinimo procesą.

Technologijos ir platformos pasirinkimas yra pirmasis ir vienas svarbiausių etapų, nes čia sprendžiama, kokios technologijos ar platformos bus naudojamos organizacijoje. Šiame etape atliekamas rinkos tyrimas, vertinamos skirtingos technologijos pagal jų funkcionalumą, saugumą, skaliamumą ir suderinamumą su organizacijos poreikiais. Svarbu įvertinti ne tik technologijos galimybes, bet ir gamintojo reputaciją bei palaikymą.

Integravimas į esamą IT infrastruktūrą yra kitas būtinas žingsnis, užtikrinantis, kad naujos GenDI sistemos veiksmingai bendradarbiautų su jau naudojamomis IT sistemomis. Tai apima techninį suderinamumą, duomenų mainus, našumo užtikrinimą ir saugos protokolų integravimą. Integravimo metu būtina atlikti išsamius testavimus ir koregavimus, kad naujoji sistema veiktų sklandžiai ir efektyviai, mažinant trukdžius esamai veiklai.

Bendradarbiavimas su patikimais ir saugiais paslaugų teikėjais yra gyvybiškai svarbus, kad užtikrintų sistemos patikimumą ir atitiktį visiems reglamentuojantiems reikalavimams. Renkantis trečiąsias šalis, svarbu atlikti išsamų jų patikimumo ir saugumo vertinimą. Taip pat būtina sudaryti sutartis, kurios apibrėžtų paslaugų lygio susitarimus (SLA), duomenų apsaugos ir privatumo reikalavimus, atsakomybę už paslaugų kokybę bei nuostatas susijusias su intelektinės nuosavybės teisėmis.

Mokymai ir komunikacija

Sėkmingas generatyvinio dirbtinio intelekto (GenDI) įdiegimas organizacijoje priklauso ne tik nuo technologijos, bet ir nuo darbuotojų mokymų ir efektyvios komunikacijos. Šiame skyriuje aptariami būtini mokymų ir komunikacijos aspektai, kurie užtikrina saugų ir etišką GenDI naudojimą.

Darbuotojų mokymai apie saugų GenDI naudojimą ir geriausias praktikas yra gyvybiškai svarbus. Mokymai turėtų apimti saugumo protokolus, duomenų tvarkymo etiką ir būdus, kaip išvengti neteisėto duomenų naudojimo. Taip pat svarbu, kad mokymo planai būtų reguliariai atnaujinami atsižvelgiant į technologijų pažangą, kad darbuotojai visada būtų informuoti apie naujausias praktikas ir įrankius.

Prieš pradedant naudotis GenDI sprendimais, būtina:

- Peržiūrėti įrankio privatumo politiką ir sąlygas, užtikrinant, kad jos atitinka organizacijos standartus.
- Atkreipti dėmesį į duomenų politiką, užtikrinant, kad duomenų tvarkymas būtų etiškas ir teisėtas.

- Nustatyti, kad informacija nebus naudojama kaip mokymosi šaltinis ar saugoma užklausų istorijoje, jei tai leidžiama nustatymais.
- Įsitikinti, kad sistema nebūtų klaidinanti ar diskriminuojanti.
- Atlikti IT saugos bei etikos vertinimą, kad užtikrinti, jog sprendimas atitinka nustatytas gaires ir politikas.

Mokymų turinys turėtų apimti tokia temas:

- Kaip teisingai pateikti užklausas, siekiant gauti kuo tikslesnius rezultatus.
- Kaip vertinti pateiktus rezultatus, atpažinti galimus nuokrypius ir juos interpretuoti.
- Supažindinimas su galimomis „AI haliucinacijomis“ ir jų atpažinimu.
- Instrukcijos, kaip naudoti gautą rezultatą darbe, ir kaip elgtis pastebėjus neetišką ar neteisingą GenDI veikimą.

Nuolatinis vertinimas yra svarbus norint užtikrinti, kad GenDI sistemų veikimas išlieka etiškas ir saugus. Organizacijoms rekomenduojama reguliariai atlikti saugumo auditus, etikos vertinimus ir naudotojų apmokymus, siekiant išlaikyti aukštą pasitikėjimo lygį ir kompetenciją naudojant šiuos sprendimus.

Komunikacija yra esminė įgyvendinant GenDI sprendimus. Būtina nuolat informuoti darbuotojus apie naujus atnaujinimus, mokymus ir keisti praktikas. Taip pat svarbu skaidriai komunikuoti su visais suinteresuotais asmenimis apie bet kokius GenDI naudojimo pokyčius, incidentus ar naujoves.

Tinkami mokymai ir komunikacija ne tik padeda užtikrinti saugų ir etišką GenDI naudojimą, bet ir skatina darbuotojų įsitraukimą ir inovacijų diegimą visoje organizacijoje.

PRIEDAI

Priedas Nr. 1
Kontrolinis sąrašas, apibendrinantis pagrindinius saugios GenDI diegimo žingsnius

Šis kontrolinis sąrašas suteikia pagrindines gaires ir rekomendacijas, kaip saugiai ir etiškai įdiegti GenDI technologijas organizacijoje, užtikrinant, kad jos būtų naudojamos atsakingai ir atitiktų visus reikalingus saugumo, privatumo ir etikos standartus.

1. Sukurti ar atnaujinti duomenų valdymo politiką, užtikrinti saugų duomenų rinkimą, tvarkymą, gyvavimo ciklą ir susijusius procesus.
2. Užtikrinti proporcingumą, nedaryti žalos, naudoti skaidriai ir nediskriminuojant.
3. Įtraukti žmogiškąją peržiūrą prieš priimant galutinį sprendimą.
4. Atsakyti į svarbius klausimus apie atsakomybę ir atskaitomybę už GenDI saugumą, įgūdžių ir žinių spragas, saugumo incidentų valdymą. Įtraukti kibernetinio ir asmens duomenų apsaugos specialistus į sprendimų priėmimo procesus.
5. Atlikti darbuotojų mokymus apie saugų GenDI naudojimą ir geriausias praktikas, informuoti apie etišką naudojimą ir nuolat atnaujinti mokymų planus.
6. Vykdyti reguliarius saugumo vertinimus, kodo peržiūras, saugumo auditus ir prieigos kontrolės peržiūras.
7. Atsakingai integruoti GenDI technologijas į organizacijos IT infrastruktūrą, bendradarbiaujant su patikimais paslaugų teikėjais.
8. Prieš pradedant naudoti GenDI sprendimus, rekomenduojama atlikti išsamų rizikos vertinimą ir numatyti rizikų mažinimo priemones.

Priedas Nr. 2
Patvirtintų GenDI sistemų registras (įrankiai, pareigybės)

Eil. Nr.	Įrankio pavadinimas	Savininkas organizacijoje	Ar įrankis skirtas darbui su konfidencialia informacija?

Priedas Nr. 3
Atmintinė vartotojui

Darbuotojui pradėjus naudotis GenDI sprendimais, rekomenduojama:

1. Naudoti užklausas, kurios aiškiai apibrėžia, kokių rezultatų tiksliai siekiate ir pateikti papildomą informaciją, kuri yra reikalinga rezultatui gauti.
2. Naudoti tinkamą ir kokybišką duomenų rinkinį. Švarūs, struktūrizuoti duomenys leis GenDI geriau suprasti užduotį.
3. Dažnai GenDI leidžia nustatyti įvairius parametrus ir parinkti naudojamus AI modelius. Eksperimentuokite su skirtingais modeliais ir nustatymais, nes tai leis rasti geriausią sprendimą jūsų užduočiai ir gauti tikslesnius rezultatus.
4. Kiekvienas GenDI turi savo ribas, todėl stenkitės suprasti ir atpažinti, kada pasirinktas modelis gali būti netikslus ar netinkamas, tinkamai interpretuokite gautą rezultatą.
5. Jei yra tokia galimybė, įsitikinkite, kad GenDI naudojami informacijos šaltiniai jums yra priimtini ir naudoja patikimą informaciją.

6. Visada patikrinkite gautą rezultatą ir ekspertiškai vertinkite jo tikslumą ir galimą tolimesnį panaudojimą.
7. Būkite atidūs dalindamiesi informacija. Labai nerekomenduojama dalintis asmenine informacija, o konfidencialia ar neskelbtina informacija dalintis draudžiama, nebent tai leidžia įmonės politika ir esate įsitikinę, kad tai saugu.
8. Sekite jūsų naudojamo ar kitų GenDI įrankių naujienas. Šio tipo įrankiai intensyviai tobulinami, todėl būkite pasiruošę išbandyti naujas galimybes, kurios leis pasiekti dar geresnių rezultatų.
9. Pastebėję neetišką ar diskriminuojantį GenDI veikimą, informuokite organizacijos atsakingus asmenis.
10. Jei per klaidą pasidalinote neleistina informacija, būtinai nedelsdami informuokite organizacijos atsakingus asmenis.
11. Asmuo, skelbiantis ar naudojantis GenDI modelio sugeneruotus rezultatus, atsako už galutinio rezultato turinį ir kokybę. Atkreiptinas dėmesys, kad dirbtinio intelekto sugeneruotas turinys gali būti netikslus, klaidinantis arba neteisingas, pažeisti trečiųjų šalių intelektinės nuosavybės, asmens duomenų apsaugos ar kitas saugomas teises. Dėl šios priežasties, bet koks pagalbiniais įrankiais sugeneruotas rezultatas turi būti peržiūrėtas ir patikrintas, o skaidrumo principai reikalauja atskleisti GenDI panaudojimą.
12. Rekomenduojama išsaugoti GenDI modelių sugeneruotus rezultatus (jų gavimo kelią).

Priedas Nr. 4
Kontrolinis GenDI naudojimo organizacijoje veiksmų sąrašas

Šis kontrolinis sąrašas skirtas organizacijos vadovams ir IT specialistams, siekiantiems užtikrinti sklandų ir saugų GenDI technologijų įdiegimą ir naudojimą. Kiekvieno veiksmo pabaigoje pateikiamas tuščias langelis leidžia pažymėti atliktus veiksmus, užtikrinant efektyvų procesų stebėjimą ir valdymą.

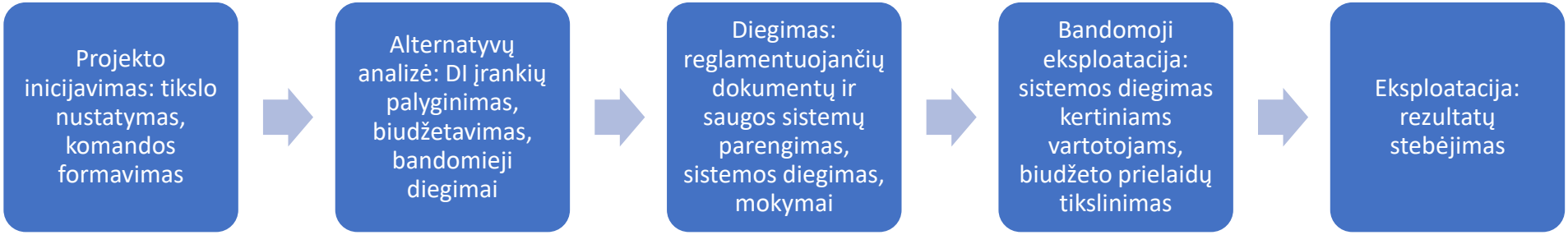
Kategorija	**Veiksmas**	**Atlikta (✓)**
1. Darbuotojų mokymai apie saugų GenDI naudojimą ir geriausią praktiką		
	Parengti mokymų planai	
	Parengtas mokymų turinys	
	Pateikti praktiniai pavyzdžiai	
2. Informavimas apie etišką GenDI naudojimą		
	Pravesti etikos mokymai	
	Parengtos praktinės gairės	
3. Mokymo planų atnaujinimas atsižvelgiant į technologijų pažangą		
	Įvardintos ir identifikuotos technologijų naujovės, kurios bus naudojamos	
	Dokumentuoti atnaujinimo ciklai	
4. Rekomendacijos prieš pradedant naudoti GenAI sprendimus		
	Atlikta privatumo politikos peržiūra	
	Atnaujinta duomenų apsaugos politika	
	Registruoti ir įvertinti GenDI apsimokymo šaltiniai ir jų kontrolės priemonės	
	Sukurtas ir dokumentuotas DI sistemų rezultatų validavimo vertinimas	

	Atliktas IT saugumo ir turinio etikos pateikimo vertinimas	
5. Darbuotojų veiksmai pradedant naudoti GenDI		
	Aiškios užklausos (prompts)	
	Duomenų rinkinių kokybė	
	Modelių eksperimentavimas ir tinkamiausio pasirinkimas	
	Modelių ribų supratimas	
	Informacijos šaltinių patikimumas	
	Atsakomybė ir etiškas deklaravimas apie gautus rezultatus	

Lentelė Nr. 1
Rekomendacijos dėl sistemos diegimo

Diegimo tipas	Tikslas	Reglamentavimo aspektai	IT padalinio rolė	Projekto savininkas
Technologijų analizė	Išbandyti technologiją	Naudotis inovacijų valdymo tvarkomis	Komandos narys, atsakingas už technologijos diegimą	Inovacijų padalinys
Funkcijos automatizavimas	Padidinti veiklos funkcijos efektyvumą ar produktyvumą	Veiklos procesų peržiūra	Komandos narys, atsakingas už technologijos diegimą	Funkcijos vadovas
Įrankis darbuotojams	Suteikti naujos kartos įrankį darbuotojams	IT įrankių naudojimo taisyklės	Komandos narys, atsakingas už technologijos diegimą. Stebėti sistemų naudojimo rezultatus, atidžiai stebėti duomenų naudojimą bei kitus saugos aspektus	IT padalinio vadovas

GenDI sistemų diegimo būdas yra panašus į kitų IT sistemų diegimo būdus, tačiau rekomenduojame numatyti žemiau pateiktus etapus:



Dokumentą parengė:

- EPSO-G, UAB – Nerijus Adomaitis, Titas Grincevičius, Lina Matukaitė
- Lietuvos geležinkeliai, AB – Vytautas Bitinas, Šarūnas Grigaliūnas
- Lietuvos bankas - Levaldas Zigmantas
- Registrų centras, VĮ – Jevgenij Tichonov
- Ignitis grupė, AB – Donatas Vitkus