PATVIRTINTA
Akcinės bendrovės „Regitra“
2026 m. birželio 19 d.
valdybos posėdžio
protokolu Nr. 2V-4704

AKCINĖS BENDROVĖS „REGITRA“ DIRBTINIO INTELEKTO POLITIKA

TURINYS:

1. PAGRINDINĖS SĄVOKOS

AB „Regitra“	Akcinė bendrovė „Regitra“, juridinio asmens kodas 110078991, registruotos buveinės adresas: Vilnius, Liepkalnio g. 97A, LT-02121.
Dirbtinis intelektas (DI)	Technologija, gebanti atlikti užduotis, kurios reikalauja žmogiškojo intelekto.
Politika	Ši AB „Regitra“ dirbtinio intelekto politika.

1.1. Politikoje vartojamos kitos sąvokos, įskaitant „DI sistema“, „tiekėjas“, yra suprantamos taip, kaip jos apibrėžtos 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamente (ES) 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) (toliau – DI aktas).

2. BENDROSIOS NUOSTATOS

2.1. Šios Politikos tikslas – nustatyti principus, reikalavimus ir atsakomybes, kuriomis vadovaujasi AB „Regitra“ naudodama DI sistemas savo veikloje ir jas diegdama.

2.2. Ši Politika apima ir numato:

2.2.1. DI naudojimo principus;

2.2.2. leidžiamą ir draudžiamą DI sistemų naudojimą;

2.2.3. atsakomybių paskirstymą bei rizikos valdyseną;

2.2.4. informacijos saugos bei asmens duomenų apsaugos reikalavimus DI sistemose;

2.2.5. su DI naudojimu susijusių incidentų valdymą;

2.2.6. trečiųjų šalių DI sistemų valdymo reikalavimus.

2.3. Ši Politika taikoma AB „Regitra“ darbuotojams (įskaitant kandidatus, laikinus darbuotojus ir praktikantus), paslaugų teikėjams, tretiesiems asmenims ir kitiems suinteresuotiems asmenims.

2.4. Esant poreikiui, konkrečios DI naudojimo ir diegimo procedūros ir praktikos apibrėžiamos atskiruose AB „Regitra“ valdymo dokumentuose.

2.5. Ši Politika parengta vadovaujantis:

2.5.1. DI aktu bei jį įgyvendinančiais, detalizuojančiais ir papildančiais teisės aktais;

2.5.2. Lietuvos Respublikos Seimo 2024 m. gegužės 9 d. rezoliucija Nr. XIV-2620 „Dėl dirbtinio intelekto technologijų naudojimo viešajame sektoriuje principų“;

2.5.3. Europos Tarybos parengta Dirbtinio intelekto ir žmogaus teisių, demokratijos ir teisinės valstybės pagrindų konvencija (Vilniaus konvencija), pasirašyta 2024 m. rugsėjo 5 d.;

2.5.4. 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) (toliau – BDAR);

2.5.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

2.5.6. Lietuvos Respublikos kibernetinio saugumo įstatymu.

3. DI NAUDOJIMO PRINCIPAI

3.1. AB „Regitra“ DI naudojimas yra paremtas šiais pagrindiniais principais, kuriais vadovaujasi AB „Regitra“ valdymo organai ir darbuotojai rengdami AB „Regitra“ vidaus dokumentus, priimdami sprendimus ir diegdami bei naudodami DI sistemas:

3.1.1. Žmogaus priežiūros – DI sistema naudojama kaip pagalbinė priemonė, siekiant efektyvinti AB „Regitra“ veiklos procesus ir pagerinti teikiamų paslaugų kokybę. DI sistemos sugeneruotas turinys negali būti tvirtinamas ir naudojamas kaip oficialus AB „Regitra“ dokumentas be kompetentingo darbuotojo peržiūros ir įvertinimo;

3.1.2. Atsakomybės – kiekvienas darbuotojas, naudojantis DI sistemą, yra asmeniškai atsakingas už DI sistemos sugeneruoto turinio tikslumą ir atitiktį AB „Regitra“ standartams bei taikytinų teisės aktų reikalavimams;

3.1.3. Skaidrumo – asmenys turi būti informuojami, kai su jais tiesiogiai sąveikauja DI sistema ir kai jiems yra taikomas automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jiems kyla teisinės pasekmės arba kuris jiems panašiu būdu daro didelį poveikį. Taip pat užtikrinama, kad darbuotojai ir tretieji asmenys būtų aiškiai informuoti, kai jie sąveikauja su DI sistema (pvz., pokalbių robotu) arba kai jiems pateikiamas DI sugeneruotas turinys; DI sugeneruotas arba reikšmingai modifikuotas turinys (tekstas, vaizdas, garsas, vaizdo įrašas) būtų atitinkamai pažymėtas pagal DI akto 50 straipsnio reikalavimus;

3.1.4. Asmens duomenų apsaugos – DI sistema turi būti naudojama laikantis BDAR ir kitų asmens duomenų tvarkymą reglamentuojančių teisės aktų reikalavimų;

3.1.5. Nediskriminavimo – draudžiama naudoti DI sistemas, diskriminuojančias asmenis pagal lyties, amžiaus, tautybės, negalios ar kitus saugomus požymius;

3.1.6. Rizikų valdymo – visos AB „Regitra“ naudojamos ar planuojamos naudoti DI sistemos prieš jų diegimą ar esminį pakeitimą įvertinamos atsižvelgiant į galimą poveikį asmens duomenų apsaugai ir kitoms pagrindinėms teisėms, informacijos saugumui, AB „Regitra“ veiklos tęstinumui ir reputacijai. Šio vertinimo rezultatas dokumentuojamas;

3.1.7. Privatumo, žmogaus teisių ir socialinės naudos – DI sistemos taikomos gerbiant žmogaus teises, privatumą ir teisėtus asmenų lūkesčius. DI sistemos diegiamos tik tada, kai numatoma nauda AB „Regitra“ veiklai ir visuomenei yra didesnė už galimą žalą asmenų teisėms ir laisvėms, o nustačius neigiamo poveikio riziką imamasi rizikos mažinimo priemonių;

3.1.8. Paaiškinamumo – DI sistemų veikimo logika, paskirtis ir apribojimai turi būti suprantami tiek DI sistemas naudojantiems darbuotojams, tiek, kiek taikoma, asmenims, kurių teisėms ar pareigoms DI sistemų naudojimas gali turėti poveikį;

3.1.9. Atskaitomybės ir atsekamumo – už kiekvieną AB „Regitra“ naudojamą DI sistemą turi būti paskirtas atsakingas padalinys ir darbuotojas, o sprendimai dėl DI sistemų diegimo, reikšmingų pakeitimų, rizikos vertinimo ir incidentų turi būti dokumentuojami taip, kad būtų galima atsekti priimtus sprendimus;

3.1.10. Teisėtumo – DI sistemų taikymas AB „Regitra“ turi būti teisiškai pagrįstas ir atitikti Lietuvos Respublikos ir tiesiogiai taikytinus Europos Sąjungos teisės aktus.

4. LEIDŽIAMAS DI SISTEMOS NAUDOJIMAS

4.1. AB „Regitra“ gali naudoti tik patvirtintas ir DI sistemų sąraše registruotas DI sistemas, kurių paskirtis, rizikos, duomenų tvarkymas, atsakingi asmenys ir kontrolės priemonės yra dokumentuotos AB „Regitra“ vidaus teisės aktų nustatyta tvarka.

4.2. Asmeninių DI sistemų paskyrų, nepatvirtintų DI sistemų paskyrų bei nepatvirtintų ir neregistruotų DI sistemų naudojimas darbo metu AB „Regitra“ yra griežtai draudžiamas.

4.3. AB „Regitra“ darbuotojai darbo tikslais gali jungtis tik prie darbinių DI sistemų paskyrų ir šiais tikslais naudoti tik AB „Regitra“ generalinio direktoriaus nustatyta tvarka įvertintas, patvirtintas ir į DI sistemų sąrašą įtrauktas DI sistemas.

5. DRAUDŽIAMA SU DI SISTEMOMIS SUSIJUSI PRAKTIKA

5.1. AB „Regitra“ draudžiama su DI sistemomis susijusi praktika, nurodyta DI akto 5 straipsnyje.

5.2. Draudžiama DI sistemas naudoti būdais ir tikslais, nesuderinamais su taikytinų teisės aktų, šios Politikos bei AB „Regitra“ vidaus teisės aktų reikalavimais.

6. TREČIŲJŲ ŠALIŲ TIEKIAMOS DI SISTEMOS

6.1. AB „Regitra“ vykdant viešuosius pirkimus dėl DI sistemų įgijimo ir diegimo bei įgyvendinant DI sistemų viešųjų pirkimų sutartis, atitinkamuose viešųjų pirkimų ir susijusiuose dokumentuose privalo būti įtraukti reikalavimai dėl DI sistemų atitikties DI akto bei šios Politikos reikalavimams, laikantis viešųjų pirkimų organizavimą bei taikymą nustatančių teisės aktų bei AB „Regitra“ vidaus teisės aktų reikalavimų.

6.2. Rengiant viešųjų pirkimų dokumentus DI sistemoms įsigyti, turi būti įtraukiami reikalavimai dėl atskaitomybės, skaidrumo, nediskriminavimo, saugumo, kibernetinės saugos ir asmens duomenų apsaugos reikalavimų laikymosi, atitikties DI akto nuostatoms.

6.3. Sutartyse su DI sistemų tiekėjais turi būti numatytos sąlygos, užtikrinančios šios Politikos bei taikytinų teisės aktų reikalavimų laikymąsi. Sutartys su DI sistemų tiekėjais privalo apimti bent: (i) asmens duomenų apsaugos, informacinės saugos bei kibernetinės saugos sąlygas; (ii) tiekėjo bei jo teikiamų DI sistemų patikros, vertinimo ir auditavimo sąlygas; (iii) tiekėjų pareigas, susijusias su poveikio duomenų apsaugai vertinimu, DI rizikos vertinimu, DI sistemų dokumentacija, įvesties bei išvesties duomenų panaudojimu apmokymo ir kitais tikslais, DI sistemų incidentų valdysena; (iv) DI sistemos tiekėjo atsakomybės sąlygas bei garantijas; (v) sutarties nutraukimo sąlygas.

7. ATSAKOMYBĖS

7.1. Pagrindinės organizacinės atsakomybės už šios Politikos įgyvendinimą:

Subjektas	Atsakomybės
Valdyba	– Tvirtina šią Politiką ir jos pakeitimus.
Generalinis direktorius	– Užtikrina šios Politikos įgyvendinimą.
Skaitmeninimo ir informacinių technologijų departamentas (SITD)	– Administruoja DI sistemas. – Prižiūri, atnaujina ir tvarko IT sistemų registrą, į kurį įtraukia DI sistemas. – Organizuoja darbuotojų mokymus, siekiant palaikyti pakankamą raštingumo DI srityje lygį. – Nagrinėja DI incidentus.
Duomenų apsaugos pareigūnas	– Padeda užtikrinti BDAR reikalavimų laikymąsi diegiant ir naudojant DI sistemas AB „Regitra“ veikloje. – Teikia konsultacijas, rekomendacijas ir išvadas atliekant rizikos ar poveikio duomenų apsaugai vertinimus, kai DI sistemos gyvavimo cikle yra tvarkomi asmens duomenys.
Padalinių vadovai	– Užtikrina, kad jų padalinyje būtų laikomasi Politikos. – Informuoja darbuotojus prieš pradėdami naudoti naują DI sistemą.
Darbuotojai	– Naudoja DI sistemas laikydamiesi šios Politikos reikalavimų. – Praneša apie incidentus.

7.2. AB „Regitra“ valdymo organai ir darbuotojai, Audito komitetas, veikdami savo kompetencijos ribose, vadovaujasi Politikos nuostatomis priimdami sprendimus ir (ar) tvirtindami atitinkamus vidaus dokumentus, kai tai reikalinga ir kiek taikoma.

7.3. Detalesnė asmenų kompetencija gali būti nustatoma Lietuvos Respublikos teisės aktuose ir (ar) AB „Regitra“ vidaus teisės aktuose.

8. RIZIKOS VALDYSENA

8.1. AB „Regitra“ taiko rizika grįstą požiūrį į DI sistemų diegimą, taikymą ir naudojimą. Visos AB „Regitra“ naudojamos ar planuojamos diegti DI sistemos yra inventorizuojamos, klasifikuojamos bei vertinamos pagal DI aktą, taikant AB „Regitra“ vidinius rizikos valdysenos dokumentus.

8.2. Didelės rizikos DI sistema gali būti diegiama, taikoma ir naudojama AB „Regitra“ veikloje tik jeigu yra priimtas išankstinis AB „Regitra“ valdybos sprendimas, patvirtinantis atitinkamos didelės rizikos DI sistemos diegimą, taikymą ir naudojimą AB „Regitra“ veikloje.

8.3. Nustačius, kad planuojama naudoti / diegti DI sistema yra didelės rizikos DI sistema DI akto tikslais, DI diegimui, naudojimui ir taikymui yra taikomi reikalavimai, kylantys iš DI akto 26 ir 27 straipsnių.

9. DI SISTEMŲ SĄRAŠAS

9.1. AB „Regitra“ veikloje gali būti naudojamos tik AB „Regitra“ generalinio direktoriaus nustatyta tvarka įvertintos, patvirtintos ir į DI sistemų sąrašą įtrauktos DI sistemos.

10. INFORMACIJOS SAUGUMO ASPEKTAI IR KONFIDENCIALUMO APSAUGA. ASMENS DUOMENŲ APSAUGA

10.1. DI sistemos, įrankiai ir sprendimai yra diegiami, taikomi ir naudojami griežtai laikantis AB „Regitra“ informacijos saugumo politikos, komercinės (gamybinės) paslapties ir konfidencialios, įslaptintos informacijos naudojimo reikalavimų, kitų kibernetinę saugą reglamentuojančių teisės aktų ir vidaus teisės aktų reikalavimų.

10.2. DI sistemų, įrankių ir sprendimų diegimas, taikymas ir naudojimas, kai tvarkomi asmens duomenys, vykdomas griežtai laikantis BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, AB „Regitra“ asmens duomenų apsaugos politikos bei kitų asmens duomenų apsaugą reglamentuojančių teisės aktų ir AB „Regitra“ vidaus teisės aktų reikalavimų.

11. INCIDENTŲ VALDYMAS

11.1. Su DI sistemomis susiję incidentai turi būti nustatomi, registruojami, vertinami ir valdomi. Detalią incidentų valdymo tvarką nustato AB „Regitra“ generalinis direktorius.

12. BAIGIAMOSIOS NUOSTATOS

12.1. Politika įsigalioja ją patvirtinus.

12.2. Politika ir jos pakeitimai tvirtinami AB „Regitra“ valdybos sprendimu.

12.3. Su Politika supažindinami priimami ir esami AB „Regitra“ darbuotojai bei trečiosios šalys, kurioms suteikiama prieiga prie AB „Regitra“ tvarkomos informacijos.

12.4. Už Politikos parengimą, peržiūrą, kontrolę ir įgyvendinimą yra atsakingas AB „Regitra“ Skaitmeninimo ir informacinių technologijų vystymo departamento direktorius.

12.5. Politika bei jos pakeitimai yra skelbiami viešai AB „Regitra“ interneto svetainėje.

12.6. Politika ir jos įgyvendinimą reglamentuojantys vidaus teisės aktai yra peržiūrimi ne rečiau kaip kartą per metus ir atnaujinami pagal poreikį.