TRINITI JUREX
TALLINN RIGA VILNIUS

Atsakingas DI naudojimas.
Ką sako teisė?

Aurelija Rutkauskaitė

DI AKTAS

DI akto veikimo principai

2024 m. rugpjūčio mėn. įsigaliojo ES dirbtinio intelekto aktas - pirmasis siekis išsamai reglamentuoti dirbtinio intelekto („DI“) sistemų kūrimą ir naudojimą.

Akte laikomasi rizika grindžiamo požiūrio, t. y. DI sistemos reguliuojamos skirtingai, atsižvelgiant į jų potencialą sukelti žalą.

Akto reikalavimai įsigalioja etapais.

Rizika grįstas reglamentavimas

Nepriimtina rizika: DI sistemos, keliančios nepriimtiną riziką, yra **draudžiamos.**.

Didelė rizika: leidžiamos, bet tokioms DI sistemoms taikomi griežti DI akto reikalavimai.

Skaidrumo rizika: leidžiamos, bet tokioms DI sistemoms keliami skaidrumo reikalavimai.

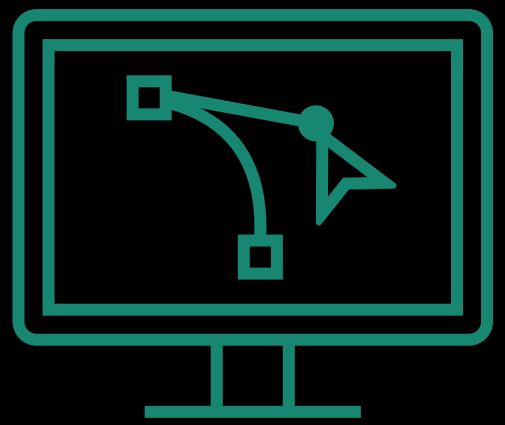
Minimali arba jokios rizikos: leidžiamos, nenumatant jokių konkrečių reikalavimų.

DI akto taikymo etapai

2024 m. rugpjūčio 1 d.	Įsigaliojo DI aktas.
2025 m. vasario 2 d.	• **Įsigalioja DI akto I skyrius, įskaitant DI raštingumo nuostata (4 straipsnis).** • **Įsigalioja draudžiamų praktikų draudimas (5 straipsnis).**
2025 m. gegužės 2 d.	Turi būti parengti bendros paskirties DI praktikos kodeksai (56 straipsnio 9 dalis).
2025 m. rugpjūčio 2 d.	• **Paskiriamos nacionalinės institucijos (III skyriaus 4 skirsnis).** • **Taikomi reikalavimai bendros paskirties DI modeliams (V skyrius).** • **Taikomos nuostatos dėl priežiūros ES ir nacionaliniu lygmeniu (VII skyrius).** • **Taikomos konfidencialumo ir sankcijų taisyklės (išskyrus susijusias su bendros paskirties DI modeliais) (XII skyrius).**
2026 m. rugpjūčio 2 d.	Pradedamos taikyti visos kitos DI akto nuostatos (nebent taikomos žemiau nurodytos vėlesnės datos).
2027 m. rugpjūčio 2 d.	• **Pradedamas taikyti I priede išvardytų didelės rizikos kategorijų sąrašas.** • **Bendros paskirties DI modeliai, pateikti rinkai iki 2025 m. rugpjūčio 2 d. (111 straipsnis), turi atitikti DI akto reikalavimus.**
2030 m. rugpjūčio 2 d.	**Didelės rizikos DI sistemos** (išskyrus toliau nurodytas), kurios buvo pateiktos rinkai arba pradėtos naudoti iki 2026 m. rugpjūčio 2 d. ir **kurios skirtos valdžios institucijoms** (111 straipsnis), turi atitikti DI akto reikalavimus.
2030 m. gruodžio 31 d.	**Didelio masto IT sistemų komponentai, išvardyti X priede (pvz., Šengeno informacinė sistema)**, kurie buvo pateikti rinkai arba pradėti naudoti iki 2027 m. rugpjūčio 2 d. (111 straipsnis), turi atitikti DI akto reikalavimus.

DI raštingumas

Taikoma nuo 2025 m. vasario 2 d.

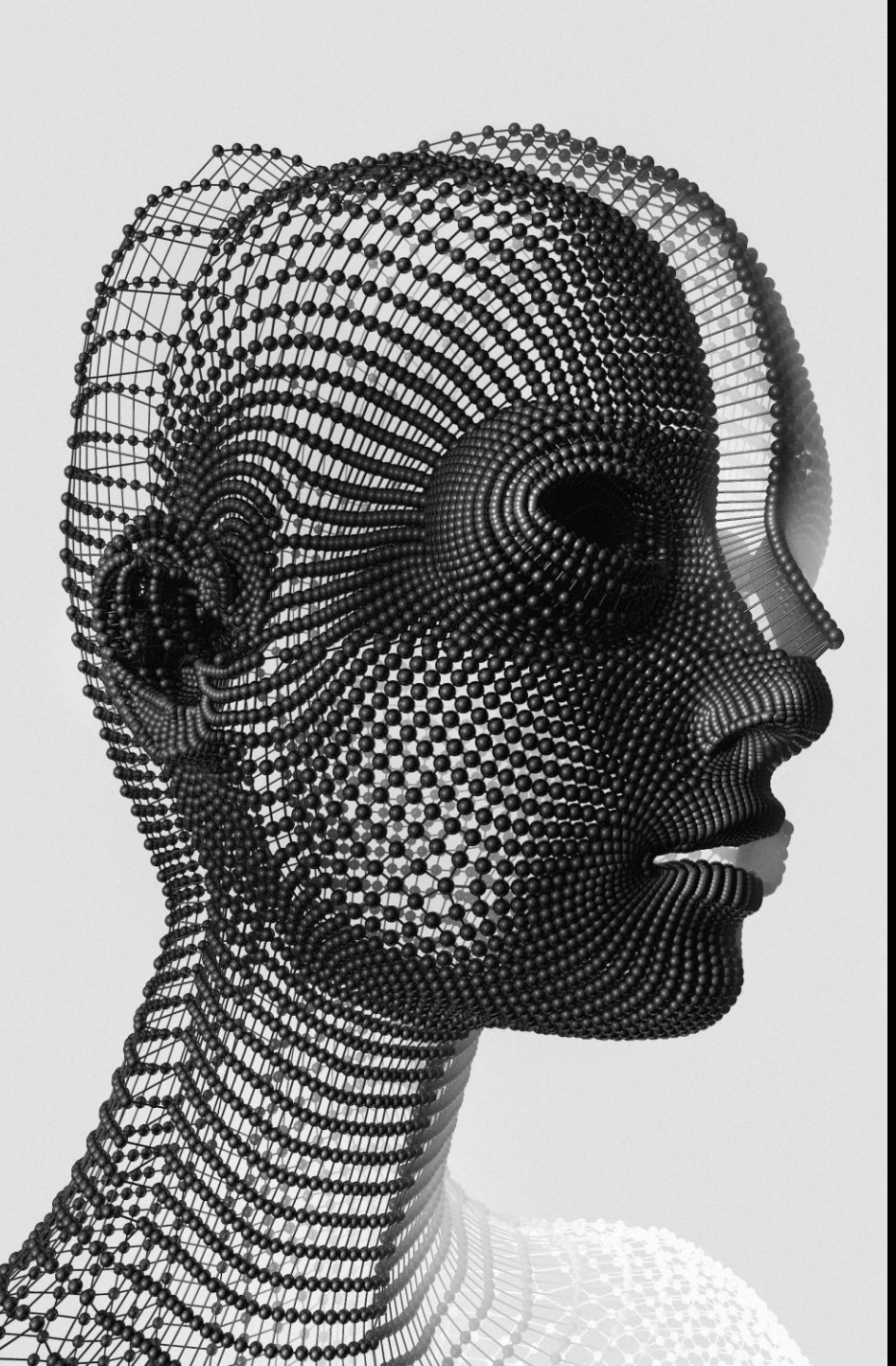


T**aikoma:** visiems DI sistemų teikėjams ir naudotojams.

Patenka į apimtį: darbuotojai ir kiti asmenys, naudojantys DI sistemas jų vardu.

Organizacijos turėtų:

- ✓ Užtikrinti bendrą supratimą apie DI ir jam taikomą reguliavimą (DI akto nuostatas) savo organizacijoje.
- ✓ Įsivertinti savo rolę (teikėjas ar naudotojas) ir atitinkamai pritaikyti DI mokymus.
- ✓ Įsivertinti rizikas ir atitinkamai pritaikyti mokymus:
  Ką darbuotojai turi žinoti, kai naudoja konkrečias DI sistemas? Kaip galima sumažinti rizikas? Ką darbuotojai turi žinoti, kai perka DI sistemas? Kokie reikalavimai taikomi DI sistemų vystymui? Kaip nepažeisti DI akto reikalavimų vystant ir naudojant DI sistemas?



DRAUDŽIAMOS DI PRAKTIKOS

- **Manipuliatyvios arba apgaulingos praktikos**
- **Asmenų pažeidžiamumo išnaudojimas dėl jų amžiaus, negalios, socio-ekonominių aplinkybių**
- **Socialinis reitingavimas, lemiantis žalingą ar nepalankų elgesį su asmeniu**
- **Rizikos vertinimas polinkio nusikalsti prognozėms**
- **Veido atvaizdų betikslis rinkimas ir duomenų bazių kūrimas**
- **Biometrinė žmonių kategorizacija pagal rasę, politines pažiūras, religinius įsitikinimus ir pan.**
- **Emocijų atpažinimas darbo vietose ir švietimo įstaigose**
- **Realaus laiko biometrinė identifikacija, vykdoma teisėsaugos tikslais**

DI aktas taikomas

Nepriklausomai nuo to, ar jie yra įsteigti ar įsikūrę Europos Sąjungoje, ar trečiojoje šalyje

Turintiems įsisteigimo vietą arba įsikūrusiems Europos Sąjungoje

Jeigu DI sistemos sukurtas rezultatas naudojamas Europos Sąjungoje

Tai yra tas, kuris sukuria arba pateikia rinkai dirbtinio intelekto sistemą (DI system).

Pavyzdžiui, DI programinės įrangos kūrėjas ar pardavėjas.

Pagrindinės pareigos:

- **Atitikties užtikrinimas**: įsitikinti, kad sistema atitinka visus DI akto reikalavimus (ypač jei tai aukštos rizikos sistema).
- **Techninė dokumentacija ir įrašai**: parengti išsamią dokumentaciją apie DI sistemą, rizikų vertinimą, bandymų rezultatus.
- **Kokybės valdymo sistema**: turėti procesus, kaip kuriama, testuojama ir stebima DI sistema.
- **Vertinimas**: tam tikrais atvejais aukštos rizikos DI sistemai būtina atlikti atitikties vertinimą, gali kilti pareiga sistemą registruoti.
- **Incidentų pranešimas**: apie rimtus pažeidimus ar incidentus pranešti kompetentingoms institucijoms.
- **Duomenų valdymas**: užtikrinti tinkamus duomenų rinkinius, jų kokybę ir atitikimą nediskriminavimo reikalavimams.

Teikėjas
(Provider)

Diegėjas
(Deployer)

Esmė

Tai yra tas, kuris naudoja DI sistemą savo veikloje.

Pavyzdžiui, įmonė, kuri įsigijo DI sprendimą ir taiko jį personalo atrankai ar klientų aptarnavimui.

Pagrindinės pareigos:

- **Atsakingas naudojimas**: DI sistema turi būti naudojama pagal paskirtį ir laikantis teikėjo instrukcijų.
- **Rizikų valdymas**: įvertinti galimas rizikas (pvz., diskriminacijos, saugumo, klaidų) ir taikyti prevencines priemones.
- **Skaidrumo pareigos**: tam tikrais atvejais informuoti naudotojus, kad jie bendrauja su DI (pvz., pokalbių robotai).
- **Žmogiška priežiūra**: užtikrinti, kad sprendimus galima peržiūrėti, kad DI nebūtų vienintelis galutinis sprendėjas (ypač aukštos rizikos srityse).
- **Duomenų apsauga**: naudoti DI taip, kad būtų laikomasi BDAR ir kitų teisės aktų.
- **Pranešimas apie incidentus**: jei sistema kelia rimtą pavojų, turi būti informuotos kompetingos institucijos.

Teikėjas
(Provider)

Diegėjas
(Deployer)

Esmė

Teikėjas atsako už sistemos sukūrimą ir atitiktį.

Diegėjas atsako už tinkamą naudojimą praktikoje.

Jei įmonė pati kuria ir naudoja savo DI (in-house development), ji gali būti ir Teikėjas, ir Diegėjas vienu metu, tad turi abi pareigų grupes.

Teikėjas
(Provider)

Diegėjas
(Deployer)

Esmė

REGULIAVIMAS UŽ DI AKTO RIBŲ

3

Kokius DI įrankius naudojate?

Sudarykite išsamų savo organizacijoje naudojamų DI įrankių sąrašą.

01

Įtraukite pavadinimus ir versijas

Pvz., nemokama ar mokama.

02

Paskirkite atsakingą asmenį, kuris galės spręsti dėl naujų įrankių įtraukimo, esamų pašalinimo iš sąrašo.

03

Tokiu būdu užtikrinama, kad visi komandos nariai aiškiai žinotų, kas yra leistina, o kas ne.

DI sprendmų naudojimas Jūsų organizacijoje

Aiškiai nurodykite, kur (kokiose srityse) naudojate DI sprendimus

- Pavyzdžiui:
  - Rinkodara
  - Duomenų analizė
  - Klientų aptarnavimas
- Apibrėžkite, kam ir kokiomis aplinkybėmis organizacijoje leidžiama naudoti DI.
- Nurodykite bet kokius DI sprendimų naudojimo apribojimus, nurodykite jų priežastis.

Konfidencialumas

Venkite dalytis privačia organizacijos ar klientų informacija, jei tai nėra būtina ir saugu.

Asmens duomenų ir privatumo apsauga

Kai įmanoma, naudokite anoniminius arba pseudonimizuotus duomenis.

Pateikite komandos nariams gaires, kuriomis užtikrinama atitiktis duomenų apsaugos reikalavimams, visų pirma - BDAR, vidinėms politikoms.

Intelektinė nuosavybė (IN)

Rizika pažeisti trečiųjų IN asmenų teises.

Gali būti sunkiau ap(si)saugoti savo pačių IN teises.

Žmonės yra atsakingi už DI rezultatus

Žmonės (ne DI sprendimas) yra atsakingi už DI pagalba sukurtus rezultatus.

- Privalu patikrinti gautą rezultatą, kad būtų išvengta šališkumo, klaidų ar haliucinacijų.
- Ši pareiga turėtų būti pagrindiniu Jūsų darbo su DI sprendimais principu.

Kibernetinis saugumas:

Saugokite prisijungimo duomenis

01

Nesidalykite prisijungimo duomenimis arba prieiga su DI sistemomis.

02

Naudokite tvirtus slaptažodžius ir užtikrinkite šifravimą.

03

Už(si)fiksuokite šias pareigas vidiniuose dokumentuise.

Laikykitės DI taisyklių ir sąlygų

Įsitikinkite, kad jūsų komanda laikosi naudojamų DI įrankių naudojimo sąlygų.

- Į šias sąlygas dažnai įtraukiamos svarbios privatumo ir saugumo nuostatos.
- Dažnu atveju DI sprendimų vystytojai stipriai apsiriboja savo atsakomybe, numato sprendimo naudojimo versle sąlygas.

Apmokykite savo komandą

Investuokite į komandos mokymus, kaip teisingai naudoti DI įrankius, daug dėmesio skirdami privatumui ir duomenų apsaugai.

Darbuotojai turėtų suprasti tiek DI suteikiamas galimybes, tiek ribojimus, galimas rizikas dirbant su juo.

Užtikrinkite, kad į Jūsų DI politiką būtų įtrauktas įsipareigojimas nuolat rengti mokymus apie DI,konfidencialumo reikalavimus, duomenų apsaugą ir kitas rizikas – tai privalomas reikalavimas pagal DI aktą.

Reguliariai peržiūrėkite naudojamus DI sprendimus

Planuokite reguliarias DI įrankių peržiūras.

Įsitikinkite, kad jie tebėra veiksmingi, saugūs ir atitinka naujas duomenų apsaugos taisykles.

Šis peržiūros procesas turėtų būti aiškiai aprašytas Jūsų DI politikoje.

3

Kas atsakingas?

Paskirkite atsakingą asmenį arba komandą, kuri prižiūrėtų DI sprendimų naudojimo praktiką Jūsų organizacijoje.

Pranešimų apie DI incidentus teikimas

Sukurkite sistemą, skirtą pranešti apie DI naudojimo incidentus, pavyzdžiui, duomenų saugumo pažeidimus, galimas klaidas, nešališkumo atvejus.

Užtikrinkite, kad visi darbuotojai žinotų šią procedūrą ir suprastų, kam pranešti.

Apsirašykite šį procesą savo DI naudojimo politikoje.

Ar būtina informuoti apie DI naudojimą?

Jei paslaugoms teikti naudojate DI, skaidriai komunikuokite apie tai su klientais.

- Iš anksto informuokite juos apie tai, kaip paslaugų teikimui bus naudojamas DI, ir užtikrinkite privatumo apsaugą.
- Intruktuokite savo komandą, kaip ir kada informuoti klientus apie DI naudojimą.

TRINITI JUREX
TALLINN RIGA VILNIUS

Ačiū!

Aurelija Rutkauskaitė

Partnerė ir advokatė | TRINITI JUREX