Ekspert selgitab: levinud müüdid tehisaru kehtima hakkava määruse kohta

1 aasta tagasi - 24.07.2025 Autor: AM

Alates 2. augustist peavad üldotstarbelised tehisintellekti kasutavad süsteemid vastama tehisintellekti määruse läbipaistvusnõuetele. Andmekaitseidu GDPR Register tegevjuht Krete Paal tõi välja määrusega seotud levinumad hirmud ja müüdid ning selgitas, mida ettevõtjad peavad juba täna ära tegema.

Euroopa Liidu tehisintellekti määrus (AI Act) on maailma esimene terviklik regulatsioon, mille eesmärk on muuta tehisintellekti kasutamine turvaliseks, vastutustundlikuks ja inimese põhiõigusi austavaks. Kuigi eesmärk on õilis, on määrusega seotud palju teadmatust, mitmeid hirme ja müüte.

"Määruse vastuvõtmisest on möödunud aasta, kuid Euroopas ja ka Eestiski levivad jätkuvalt murelikud küsimused ja tugevalt liialdatud tõlgendused. On arutatud koguni, kas määrus keelab tehisintellekti ning kas innovatsiooni loomiseks tuleb ettevõtetel Euroopa Liidust lahkuda," sõnas ta.

Paal tõi välja viis põhilist määrusega seotud müüti, mille ta ümber lükkab.

Müüt 1: tehisaru määrus tapab innovatsiooni

Tehisintellekti määrus ei tapa innovatsiooni, vaid suunab seda targemaks, läbipaistvamaks ja inimkesksemaks. "Ma tooks näiteks GDPRi jõustumise 2018. aastal, sest ka siis oli Euroopas palju segadust ja hirme. Mõned ettevõtted panid oma veebilehed kinni "igaks juhuks", teised kulutasid üle juriidilistele audititele. Samal ajal nutikad ettevõtjad tegid andmekaitsest oma konkurentsieelise," tõi Paal näite.

Ka tehisintellekti määrus on nutikatele ja proaktiivsetele ettevõtjate jaoks võimalus, mitte takistus. Läbimõeldud lähenemine tehisintellekti kasutamisele, varajane riskianalüüs ja läbipaistvus võivad hoopis tugevdada ettevõtte usaldusväärsust ning kindlustavad õigust tegutseda ka tulevikus.

Müüt 2: tehisintellekti määrus keelab tehisintellekti

Andmekaitse ekspert rõhutas, et tehisintellekti määrus ei ole keeldude nimekiri ning kasutajatele tuttavad AI-süsteemid nagu näiteks juturobotid, turundustööriistad ja tootmisanalüütika kuuluvad määruse kohaselt madala või piiratud riskiga tehnoloogia hulka.

"See tähendab, et selliste tehnoloogiate kasutamine jääb lubatuks minimaalsete lisatingimustega. Näiteks muutub kohustuslikuks kasutajale märku andmine, et tegemist on AI-põhise tööriistaga," selgitas Paal.

Määrus keelab vaid väga väikest hulka rakendusi, nagu näiteks reaalajas biomeetriline massiline jälgimine avalikus ruumis ilma õigusliku aluseta või inimkäitumise manipuleerimine, mis kahjustab inimese vaba tahet. "Need süsteemid ongi äärmused, mitte igapäevane normaalsus," kinnitas Paal.

Müüt 3: tehisaru kasutavad tooted on kõrge riskiga

Määrus liigitab “kõrge riskiga” süsteemideks vaid väga konkreetsed valdkonnad. Nendeks on näiteks tehisintellekti kasutamine tööintervjuude eelvalikus, eksamitulemuste automaatne hindamine ning õiguskaitses ja piirivalves kasutatavad süsteemid.

Muud tooted, mis lubavad näiteks sotsiaalmeedia personaliseerimist, sisu genereerimist või tootmisliini optimeerimist ei kuulu kõrge riski alla.

Lisaks on määruses väga täpselt kirjeldatud, kuidas saab süsteemi seadusega kooskõlla viia, kasutades näiteks riskihindamist ning kirjeldades protsesse läbipaistvalt nõuetekohases dokumentatsioonis.

Müüt 4: generatiivne tehisintellekt kaob

GDPR Registri juht rõhutas, et kuigi tegemist on levinud müüdiga, siis generatiivne tehisintellekt ei kao, vaid muutub vastutustundlikumaks. Näiteks ChatGPT ja teised generatiivsed tehisintellekti süsteemid on määruses eraldi käsitletud kui "üldotstarbelised AI mudelid" ehk GPAI.

"Nende puhul kehtivad läbipaistvuse ja sisuloome märgistamise nõuded ehk kasutaja peab teadma, kui sisu on loodud tehisintellekti poolt ning võimalusel tuleb ka avalikustada, millised andmekogud olid mudeli treenimise aluseks," rõhutas Krete Paal ning lisas, et antud nõue kaitseb kasutajat ning suurendab tehisintellekti usaldust ajastul, mis süvavõltsingud ja valeinfo levivad kiiresti ning võivad olla vägagi usutavad.

Müüt 5: tehisaru on IT-osakonna vastutus

Levinud, ent ohtlik müüt on, et määrus puudutab ainult arendajaid, andmeteadlasi või tehnilisi juhte. Tegelikkuses ulatuvad aga selle mõjud palju kaugemale – määrus puudutab otseselt ka turundustiime, tootearendust, klienditeenindust, juriste ja tippjuhtkonda.

Näiteks turundusosakond peab teadma, millal tuleb avalikkusele teada anda, et sisu on loodud tehisintellekti abil. Tootearendajad peavad hindama, kas nende AI-põhised funktsioonid võivad kuuluda kõrge riski alla. Juhtkonnal lasub vastutus selle eest, et organisatsioonil oleks olemas riskijuhtimise süsteem ja sisemised protseduurid vastavuse tagamiseks.

"Tehisintellekti määrus ei ole pelgalt tehniline dokument – see on strateegiline raamistik, mis eeldab organisatsiooniülest koostööd ja teadlikkust. Tehisintellekt on meeskonnaspordiala, kus kõik peavad mängureegleid mõistma," rõhutas Paal.

Mida peaksid ettevõtted praegu tegema?

Siin on olulised tegevused, mis võiks kohe ette võtta:

- **Kaardista**, milliseid tehisintellekti rakendusi sa kasutad või arendad. Ära oota määruse täielikku jõustumist – esimesed osad rakendusid juba 2025. aasta alguses.
- **Uuri**, millisesse riskikategooriasse sinu poolt kasutatavad või arendatavad tehisintellekti süsteemid kuuluvad.
- **Ehita sisse läbipaistvus** ja kasutajateadlikkus juba täna. Seda hindavad nii kliendid kui investorid.
- **Ära lase hirmul otsustada** – ole kursis faktidega ja küsi vajadusel spetsialisti nõu.

Eesti iduettevõtte poolt loodud GDPR Register on arendatud koostöös IT ekspertidega.

- Tegijad
- Uudised

- Lahendused
- Tarkvara
- Tehisintellekt

Pilt

