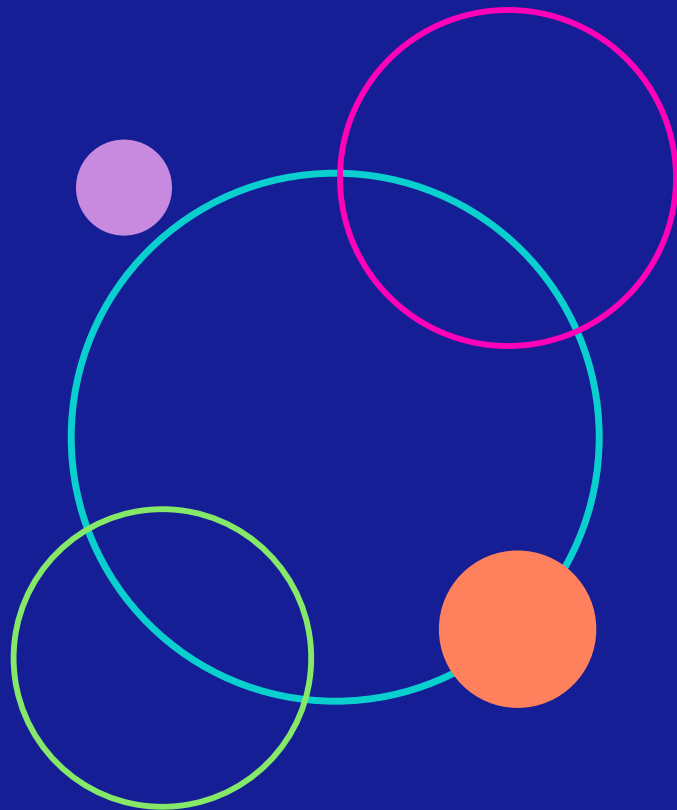


EU:n tekoälyasetus

Tekoälyjärjestelmien ja yleiskäyttöisten
tekoälymallien turvallisuussäädös

Asetus (EU) 2024/1689 – päivitetty tekoälyomnibusin muutoksilla

Teknolohiateollisuus ry · 3.8.2026





Sisällys



Tiivistelmä

3–8



Vähäinen riski ja käytäntesäännöt

51–52



Soveltamisala ja määritelmät

9–18



Yleiskäyttöisten tekoälymallien vaatimukset

53–58



Kielletyt käyttötapaukset

19–22



Innovointia tukevat toimet

59–63



Suuren riskin käyttötapaukset ja vaatimukset

23–44



Hallinnointi ja seuraamukset

64–67



Rajoittunut riski ja avoimuusvelvoitteet

45–50



Soveltamisaikataulu

68–69

Tiivistelmä





1. Soveltamisala



Mitä koskee: EU:ssa markkinoille saatettavia ja käyttöönotettavia tekoälyjärjestelmiä sekä yleiskäyttöisiä tekoälymalleja (esim. suuria kielimalleja).



Ei koske: yksinkertaisia ohjelmistoja eikä ihmisen sääntöjä suoraviivaisesti seuraavia päätöksentekojärjestelmiä.



Avoin lähdekoodi: vapaat ja avoimen lähdekoodin järjestelmät jäävät pääosin soveltamisalan ulkopuolelle; poikkeuksena suuririskiset, kielletyt ja avoimuusvelvoitteiden alaiset järjestelmät. Avoimille malleille kevennettyjä velvoitteita.



Rajaukset: tutkimus- ja kehitysvaihe sekä yksinomaan sotilas-, puolustus- ja kansallisen turvallisuuden käyttö jäävät ulkopuolelle.



2. Turvallisuussäädös



Tavoitteena suojata terveyttä, turvallisuutta ja perusoikeuksia tekoälyn käytöstä aiheutuvilta riskeiltä ja haitoilta.

Riskiperusteinen sääntely

Vaatimukset asetetaan järjestelmän tai mallin riskitason mukaan. Olennaista on tietää tarjoajana tai käyttöönottajana, mihin riskiluokkaan järjestelmä kuuluu – vasta se kertoo velvoitteet.



3. Tekoälyjärjestelmien riskiluokittelu



Kielletty: kestäättömiä riskejä sisältävät järjestelmät (esim. sosiaalinen pisteytys); osa kielloista sallii rajattuja poikkeuksia.



Suuri riski: sallittu, kun vaatimukset täytetään. Tuoteturvasäännellyt tuotteet ja turvakomponentit + erikseen määritellyt käyttötapaukset.



Rajoittunut riski: generatiivisille ja muille järjestelmille avoimuusvaatimuksia – esim. tieto asiointista tekoälyn kanssa.



Vähäinen riski: ei vaatimuksia. Suurin osa järjestelmistä, ml. valtaosa teollisuustuotannon käyttötapauksista.



4. Yleiskäyttöisten tekoälymallien riskiluokittelu



Kaikki mallit: avoimuus- ja informointivaatimukset – mm. jatkokehittäjien informointi ja tiivistelmä koulutusdatasta.



Systeemisen riskin mallit: tyypillisesti suurimmat perustamallit; lisävaatimukset, mm. mallin arviointi ja adversariaalinen testaus.



5. Vaiheittainen soveltamisaikataulu



2/2025

Kielletyt käytännöt; tekoälylukutaito

8/2025

Yleiskäyttöiset mallit; hallinto ja seuraamukset

8/2026

Avoimuusvelvoitteet (mm. tekoälyn kanssa asiointi, syvävääreennökset, synteettisen sisällön merkintä)

12/2026

Uudet kiellot (intiimimateriaali, CSAM); synteettisen sisällön merkintä ennen 8/2026 markkinoille saatetuissa järjestelmissä

8/2027

Sääntelyn testiympäristöt; ennen 8/2025 markkinoille tuodut yleiskäyttöiset mallit

12/2027

Suuririskiset järjestelmät – liite III (käyttötapaukset)

8/2028

Suuririskiset tuotteet ja turvakomponentit – liite I (tuoteturva)

8/2030

Ennen suuririskisäännösten soveltamista käyttöön otetut, viranomaiskäyttöön tarkoitetut suuririskiset järjestelmät

Soveltamisala ja määritelmät





Mikä ihmeen tekoälyasetus?



Sovelletaan sellaisenaan
EU:ssa kaikilla sektoreilla ja
toimialoilla



Tavoitteena suojata terveyttä,
turvallisuutta ja
perusoikeuksia



Vaatimukset asetetaan
riskiperusteisesti

Oletuksena: tekoälyjärjestelmien ja -mallien luotettavuuden kasvu lisää
niiden käyttöä ja kysyntää.



Asetuksen viitekehys: tekoälyjärjestelmät ja -mallit



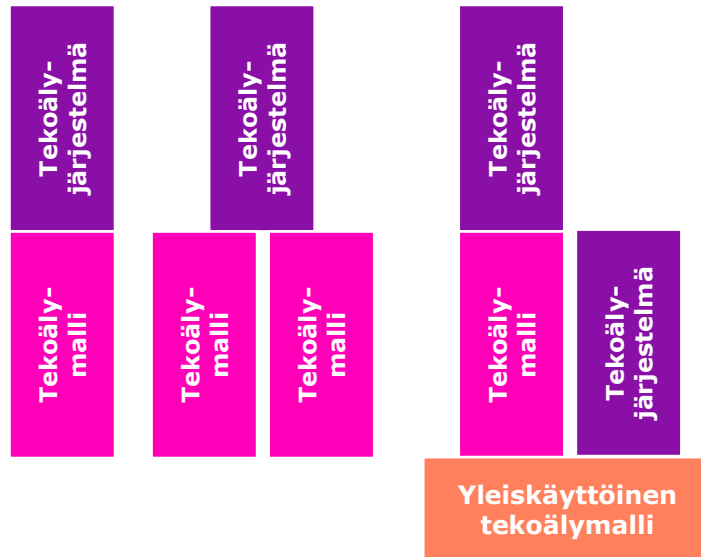
Tekoälyjärjestelmä

= sovellus, jolla on tietty käyttötarkoitus.

Tekoälymalli

= järjestelmän **moottori**, joka määrittää tiedon käsittelyn.

Yleiskäyttöistä mallia voidaan jatkokehittää rajatummaksi malliksi.





Määritelmä: tekoälyjärjestelmä



Konepohjainen järjestelmä, joka toimii vaihtelevilla autonomian tasoilla, voi mukautua käyttöönoton jälkeen ja päättelee syöttestä, miten tuottaa tuotoksia (ennusteita, sisältöä, suosituksia, päätöksiä), jotka voivat vaikuttaa fyysiseen tai virtuaaliseen ympäristöön.



Vaihteleva autonomia



Voi mukautua käytössä



Tuottaa ennusteita ja sisältöä



Vaikuttaa ympäristöön

Ei kata perinteisiä yksinkertaisia ohjelmistoja eikä ihmisen sääntöjä noudattavia automaattisia päätöksentekojärjestelmiä.



Määritelmä: yleiskäyttöinen tekoälymalli



Laaja koulutus: tyypillisesti koulutettu suurella määrällä dataa ja käsittää suuren määrän parametreja.



Monikäyttöisyys: kykenee suorittamaan pätevästi monenlaisia erillisiä tehtäviä riippumatta siitä, miten malli saatetaan markkinoille.



Integroitavuus: voidaan liittää erilaisiin loppupään järjestelmiin (kirjasto, pilvipalvelu, ohjelmointirajapinta, lataus, fyysinen kopio, chatbot).



Indikatiivinen kriteeri: koulutukseen laskentatehoa $\geq 10^{23}$ FLOP ja malli kykenee tuottamaan kieltä, kuvaa tai videota.



Keskeiset toimijat



Tarjoaja

Provider

Kehittää tai kehityttää tekoälyjärjestelmän tai yleiskäyttöisen mallin ja saattaa sen EU-markkinoille omalla nimellään – maksutta tai maksua vastaan.

Riippumaton sijoittautumispaikasta.

Yritys, oikeushenkilö, viranomainen tai luonnollinen henkilö.



Käyttönottaja

Deployer

Käyttää tekoälyjärjestelmää.

Sijoittautunut EU:hun tai järjestelmän tuotos kohdistuu EU-alueelle.

Yritys, oikeushenkilö, viranomainen tai luonnollinen henkilö.

Henkilökohtainen, muu kuin ammattikäyttö ei kuulu soveltamisalaan.



Riskiluokittelu



**Tekoälyjärjestelmät –
neljä riskiluokkaa:**

Kielletty

Suuri riski

Rajoittunut

Vähäinen

Tarjoaminen ja käyttö kiellettyä

Osassa poikkeuksia

Sallittu, kun vaatimukset täytetään

Tuoteturvasäännellyt tuotteet + muut käyttötapaukset

Sallittu, kun avoimuusvelvoitteet täytetään

Esim. chatbotit

Sallittu, ei vaatimuksia

Esim. roskapostisuodatin, reittioptimointi, laadunvarmistus

Yleiskäyttöiset mallit – oma kaksitasoinen luokittelu:

Systeemisen riskin mallit → lisävaatimukset

Kaikki mallit → avoimuus & informointi



Asetuksen piiriin eivät tule



Tutkimus ja kehitys: tieteelliseen T&K-käyttöön tarkoitetut sekä vielä markkinoille saattamattomat järjestelmät ja mallit.
– Poikkeus ei kata testausta tosielämän olosuhteissa.



Turvallisuus: yksinomaan sotilaalliseen, puolustukselliseen tai kansallisen turvallisuuden käyttöön tarkoitetut järjestelmät.



Henkilökohtainen käyttö: luonnolliset henkilöt, jotka käyttävät järjestelmää pelkästään muussa kuin ammattitoiminnassa.



Avoimen lähdekoodin tekoälyjärjestelmät



Asetusta ei pääsääntöisesti sovelleta vapaisiin ja avoimeen lähdekoodiin perustuviin tekoälyjärjestelmiin.

Poikkeus ei kuitenkaan koske järjestelmiä, jotka saatetaan markkinoille tai otetaan käyttöön:



Suuririskiset järjestelmät



Kielletyt käyttötapaukset



Avoimuusvelvoitteet



Tekoälylukutaito



Tarjoajien ja käyttöönottajien on toteutettava toimenpiteitä, jotka tukevat henkilöstön ja muiden niiden lukuun järjestelmiä käyttävien tekoälylukutaitoa.



Velvoite ei edellytä tietyn yksilökohtaisen osaamistason takaamista.



Komissio julkaisee käytännön esimerkkejä; tekoälyneuvosto antaa suosituksia.

Kielletyt käyttötapaukset





Kielletyt käyttötapaukset 1/3



Reaaliaikainen biometrinen etätunnistus julkisissa tiloissa lainvalvonnassa.

- Ei kata: terrori-iskun ehkäisy, kadonneiden/uhrien etsintä, tietyt vakavat rikokset.
- Edellyttää oikeus- tai hallintoviranomaisen ennakkolupaa.



Haitalliset alitajuiset, manipuloivat tekniikat.



Haavoittuvien ryhmien hyväksikäyttö (ikä, vamma, sosiaalinen tai taloudellinen tilanne).



Sosiaalinen pisteytys, joka johtaa haitalliseen tai epäedulliseen kohteluun.



Kielletyt käyttötapaukset 2/3



Biometrinen luokittelu rodun, poliittisten mielipiteiden, vakaumuksen, ammattiliiton jäsenyyden tai seksuaalisen suuntautumisen päättelemiseksi.
– Ei kata laillisten biometristen aineistojen merkintää/suodatusta.



Profilointiin perustuva rikosriskin ennakointi tai arviointi.



Tunteiden päätteleminen työpaikalla tai oppilaitoksessa.
– Ei koske lääketieteellisiä tai turvallisuuteen liittyviä tarkoituksia.



Kasvojentunnistustietokantojen luonti kuvien kohdistamattomalla haravoinnilla internetistä tai valvontakameroista.



Kielletyt käyttötapaukset 3/3



Ei-suostumuksellinen intiimimateriaali. Järjestelmä, joka tuottaa tai muokkaa realistista kuva-, video- tai äänimateriaalia tunnistettavan henkilön intiimialueista tai seksuaalisesta toiminnasta ilman tämän nimenomaista suostumusta.



Lapsen seksuaalista hyväksikäyttöä esittävä materiaali (CSAM). Tällaisen materiaalin tuottaminen tai muokkaaminen tekoälyjärjestelmällä (direktiivi 2011/93/EU).



Soveltamisala: kohdistuu tarjoajiin, kun tällaisen materiaalin tuottaminen on järjestelmän käyttötarkoitus tai kohtuudella ennakoitavissa eikä riittäviä suojakeinoja ole, sekä käyttöönottajiin, jotka käyttävät järjestelmää tähän.

Suuren riskin käyttötapaukset ja vaatimukset





Reitit suuren riskin vaatimusten piiriin



Reitti 1

Liite I

Tuote tai tuotteen turvakomponentti, joka kuuluu EU:n tuoteturvalainsäädäntöön ja edellyttää kolmannen osapuolen vaatimustenmukaisuuden arviointia.



Reitti 2

Liite III

Kuuluu johonkin liitteessä III lueteltuun käyttötapa-alueeseen (esim. työllistäminen, kriittinen infrastruktuuri, koulutus).

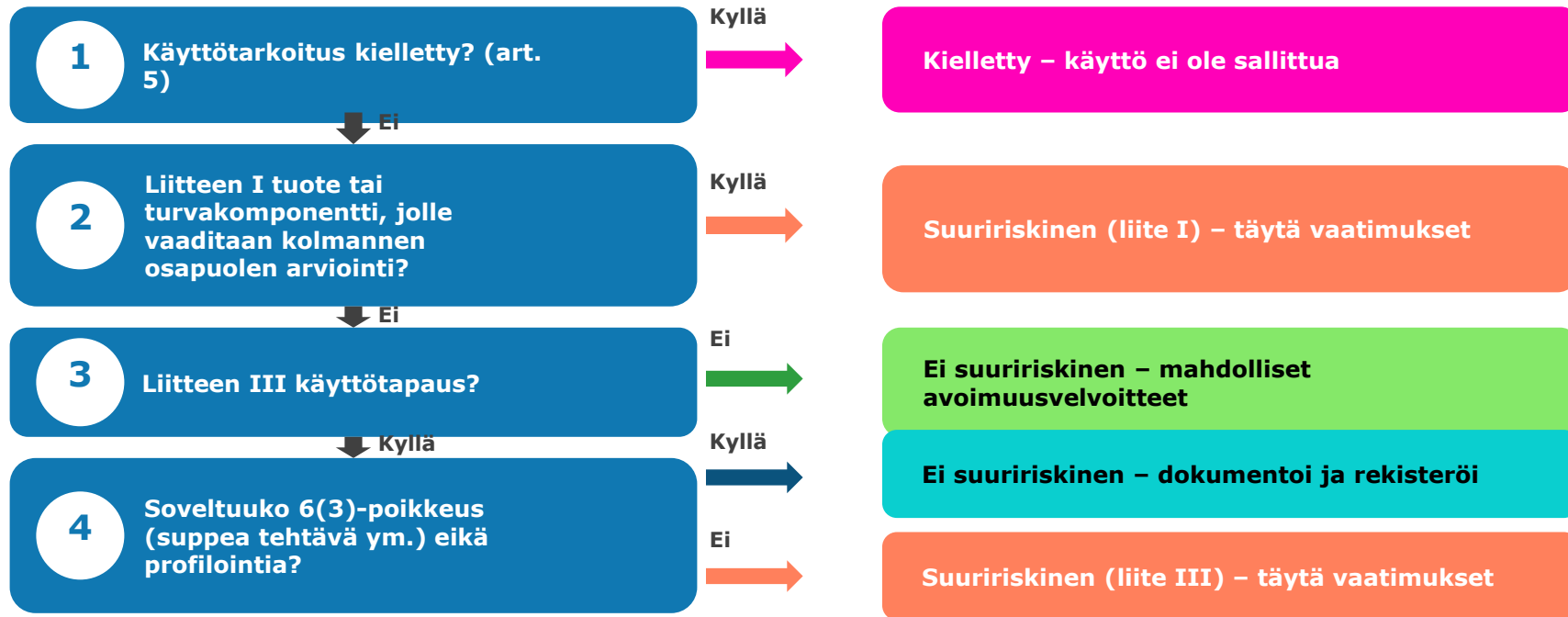


Suuren riskin vaatimukset

Poikkeukset



Onko järjestelmäsi suuririskinen? – pikatesti



6(3)-poikkeus koskee vain liitteen III käyttötapauksia; liitteen I tuotteet ovat aina suuririskisiä. Profilointi → aina suuririskinen.



Reitti 1: turvallisuussäännellyt tuotteet



Tekoälyjärjestelmä, joka on tuote tai tuotteen turvakomponentti ja kuuluu EU:n tuoteturvalainsäädäntöön ja jolle on sen perusteella tehtävä kolmannen osapuolen vaatimustenmukaisuuden arviointi.

Säädökset liitteessä I

Osio A: NLF-mukautetut säädökset · Osio B: muut yhdenmukaistetut säädökset

Sovelletaan

8/2028



Tuoteturvasäädösten kautta soveltamisalaan tulevia tuoteryhmiä (liite I, osio A)



Lelut · Huviveneet ja vesiskootterit · Hissit



Räjähdysvaarallisten tilojen laitteet · Radiolaitteet · Painelaitteet



Köysiratalaitteet · Henkilönsuojaimet · Kaasumaisia polttoaineita polttavat laitteet



Lääkinnälliset laitteet ja in vitro -diagnostiikkalaitteet



Koneet ja kulkuneuvot (liite I, osio B)



Koneet (koneasetus (EU) 2023/1230) – siirretty osioon B; suuririskisten järjestelmien vaatimuksista säädetään koneasetuksessa (sovelletaan 2.8.2028 alkaen).



Siviililentokoneet ja miehittämättömät ilma-alukset · maa- ja metsätalousajoneuvot



Kaksi-, kolmi- ja nelipyöräiset ajoneuvot · moottoriajoneuvot ja perävaunut



Laivavarusteet · rautatiejärjestelmät



Osio B: tekoälyasetus soveltuu vain osin – vaatimuksista säädetään pääosin sektorisäädöksissä.



Muut suuririskiset käyttötapaukset 1/3 (liite III)



Biometriikka: biometrinen etätunnistus ja luokittelu sekä tunteiden tunnistus (kiellettyjen ulkopuolella). Ei pelkkää todentamista/laitteen avaamista.



Kriittinen infrastruktuuri: digitaalisen infrastruktuurin, liikenteen sekä vesi-, kaasu-, lämmitys- ja sähköhuollon turvakomponentit. Ei kyberturvakomponentteja.



Koulutus: opiskelijavalinnat, oppimisen arviointi ja ohjaus, koulutustason arviointi, kokeissa kielletyn käytöksen havaitseminen.



Muut suuririskiset käyttötapaukset 2/3 (liite III)



Työllistäminen ja HR: rekrytointi ja valinta, ilmoitusten kohdentaminen, hakemusten suodatus ja hakija-arviointi, ylennys/irtisanominen, suorituksen ja käytöksen seuranta.



Välttämättömät palvelut ja etuudet: julkisten etuuksien kelpoisuus ja myöntäminen/epääminen, luottoluokitus (pl. petosten havaitseminen), sairaus-/henkivakuutuksen riskiarvio, hätäpuhelujen luokittelu.



Muut suuririskiset käyttötapaukset 3/3 (liite III)



Lainvalvonta: rikosriskin arviointi, valheenpaljastus, todistusaineiston luotettavuus, tutkintaan liittyvä profilointi.



Muuttoliike, turvapaikka, rajavalvonta: valheenpaljastus, riskien arviointi, hakemusten arviointi, maahantulijoiden havaitseminen.



Oikeudenhoito ja demokratia: tosiasioiden ja lain tutkiminen ja soveltaminen, vaalien tai äänestäjien tulokseen vaikuttaminen.



Milloin tekoälyjärjestelmä ei ole suuririskinen (liite I)



Ei turvakomponentti: pelkästään käyttäjän avustamiseen, suorituskyvyn tai palvelun optimointiin, automaatioon, käyttömukavuuteen tai laadunvalvontaan käytettävät järjestelmät.



Poikkeus: jos vikaantuminen tai virhetoiminta vaarantaisi terveyden tai turvallisuuden, järjestelmä on turvakomponentti.



Muut riskit: kolmannen osapuolen arviointi yksin muista kuin terveys-/turvallisuussyistä (esim. radiotaajuudet, EMC) ei tee järjestelmästä suuririskistä.



Poikkeukset suuren riskin luokituksesta (liite III)



Suppea menettelytehtävä (esim. strukturoimattoman datan strukturoiminen).



Ihmisen tuloksen parantaminen (esim. tekstin tyylin muokkaaminen).



Poikkeamien havaitseminen aiemmasta päätöksenteosta (esim. arvioinnin poikkeamien merkitseminen).



Valmistelutehtävä liitteen III käyttötapauksen arvioinnille (esim. tiedostojen käsittely).



Rajaus: koskee vain liitteen III käyttötapauksia eikä päde ihmisten profilointiin.



Poikkeuksen dokumentointi ja rekisteröinti



Dokumentointi: jos tarjoaja katsoo, ettei liitteen III järjestelmä ole suuririskinen, arvio on dokumentoitava ennen markkinoille saattamista.



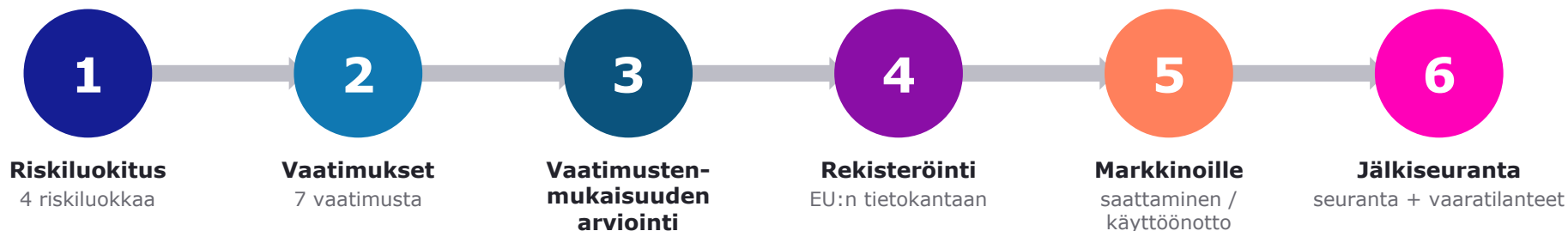
Viranomaispyyntö: toimivaltaisten viranomaisten pyynnöstä arviointiasiakirjat on toimitettava.



Rekisteröinti: rekisteröintivelvoitetta on noudatettava. Omnibus yksinkertaistaa ja keventää rekisteröintiä, mutta se säilyy markkinavalvonnan vuoksi.



Tarjoajan polku: suuririskisen järjestelmän elinkaari



Arviointi ja rekisteröinti uusitaan, jos järjestelmää tai sen käyttötarkoitusta muutetaan olennaisesti; markkinoille saattamisen jälkeinen seuranta jatkuu koko elinkaaren ajan.



Suuririskisen tekoälyjärjestelmän vaatimukset



Riskienhallinta



Data ja datanhallinta



Tekninen dokumentaatio



Lokitietojen säilytys



Avoimuus käyttäjille



Ihmisen valvonta



Tarkkuus, vakaus, kyberturva

Tueksi tuotetaan yhdenmukaistetut standardit. CRA-vaatimukset täyttävä järjestelmä täyttää myös 15 artiklan kyberturvan; tarjoaja vastaa vaatimusten täyttymisestä.



Data, datanhallinta ja vinoumien havaitseminen



Datan laatu: koulutus-, validointi- ja testausdatan on täytettävä laatukriteerit (relevanssi, edustavuus, virheettömyys mahdollisuuksien mukaan).



Vinoumien havaitseminen: erityisiä henkilötietoryhmiä voidaan poikkeuksellisesti käsitellä vinoumien havaitsemiseksi ja korjaamiseksi tiukoin suojatoimin (uudelleenkäytön rajat, pseudonymisointi, pääsynvalvonta, ei siirtoa, poisto).



Laajennus: oikeusperuste koskee myös muiden järjestelmien/mallien tarjoajia ja käyttöönottajia. Säännös ei velvoita tekemään vinoumien havaitsemista.



Tarjoajan velvollisuus: vaatimustenmukaisuuden arviointi



Ennen markkinoille saattamista: tarjoajan on tehtävä arviointi; toistettava, jos järjestelmää tai sen tarkoitusta muutetaan olennaisesti.



Liite III: arvioinnin voi pääsääntönä tehdä tarjoaja itse.



Liite I: noudatetaan tuoteturvasäädösten arviointimenettelyä, ml. tarvittaessa kolmannen osapuolen arviointi.



Standardit: tarjoaja voi hyödyntää yhdenmukaistettuja standardeja vaatimustenmukaisuuden osoittamiseen.



Tarjoajan velvollisuus: suuririskisen järjestelmän rekisteröinti



Liitteen III suuririskisen järjestelmän tarjoajan on rekisteröitävä itsensä ja järjestelmänsä EU:n tietokantaan ennen markkinoille saattamista tai käyttöönottoa.

Velvollisuus koskee myös sellaista liitteen III järjestelmää, jota tarjoaja ei arvionsa perusteella pidä suuririskisenä.



Suuririskisen järjestelmän tarjoajan muut velvollisuudet



Laatujärjestelmä



Dokumentaation säilyttäminen (10 vuotta) ja lokitietojen säilyttäminen (6 kk)



Korjaavat toimenpiteet ja tiedonantovelvollisuus



Yhteistyö viranomaisten kanssa; valtuutettu EU-edustaja, ellei tarjoaja ole EU:ssa



Markkinoille saattamisen jälkeinen seuranta ja vakavista vaaratilanteista ilmoittaminen



Vastuut arvoketjussa: järjestelmien muokkaaminen



Tarjoajaksi tulee taho, joka laittaa nimensä tai tavaramerkkinsä suuririskiseen järjestelmään,



tekee merkittävän muutoksen siten, että järjestelmä pysyy suuririskisenä, tai



muuttaa muun järjestelmän käyttötarkoitusta niin, että siitä tulee suuririskinen.



Alkuperäinen tarjoaja antaa tarvittavat tiedot, teknisen pääsyn ja avun – ellei ole kieltänyt muuttamista suuririskiseksi.



Vastuut arvoketjussa: järjestelmien alihankkijat



Kirjallinen sopimus: kolmannen osapuolen, joka toimittaa suuririskiseen järjestelmään käytettäviä tai siihen integroitavia välineitä, palveluja, komponentteja tai prosesseja, on sovittava tarjoajan kanssa tarvittavista tiedoista ja avusta.



Rajaus: ei koske maksuttomin, avoimin lisenssein tarjottuja komponentteja, jotka ovat muita kuin yleiskäyttöisiä tekoälymalleja.



Mallisopimusehdot: tekoälytoimisto voi kehittää ja suositella vapaaehtoisia mallisopimusehtoja.



Suuririskisen järjestelmän käyttöönottaajan velvollisuudet



Käyttö ja valvonta käyttöohjeiden mukaisesti



Valvonta päteville, koulutetuille ja valtuutetuille henkilöille



Syöttötietojen merkityksellisyys ja edustavuus (omilta osin)



Riskeistä ilmoittaminen tarjoajalle ja viranomaiselle; lokien säilytys ≥ 6 kk



Työntekijöiden ja päätösten kohteena olevien informointi; julkinen sektori rekisteröityy EU:n tietokantaan



Käyttöönottajajan velvollisuus: perusoikeusvaikutusten arviointi



FRIA ennen käyttöönottoa: suuririskisen järjestelmän käyttöönottajajan on arvioitava vaikutukset perusoikeuksiin.

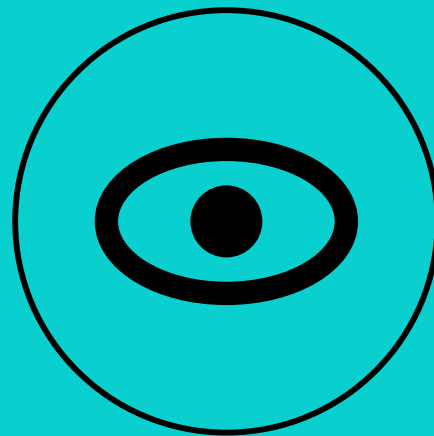


Kenelle: julkisen sektorin elimet sekä keskeisiä julkisia palveluita tuottavat yksityiset yhteisöt. Tulokset ilmoitetaan viranomaiselle.



Keventäjät: voidaan tehdä DPIA:n yhteydessä ristiviittauksin; tekoälytoimisto tarjoaa kyselylomakkeen (myös automatisoituna työkaluna).

Rajoittuneen riskin käyttötapaukset ja avoimuusvelvoitteet





Ihmisen kanssa vuorovaikuttavat tekoälyjärjestelmät



Ilmoitusvelvoite: suoraan ihmisten kanssa vuorovaikuttavat järjestelmät on toteutettava niin, että henkilölle ilmoitetaan hänen asioivan tekoälyjärjestelmän kanssa.



Poikkeus: ei koske järjestelmiä, jotka on lailla valtuutettu rikoksantorjuntaan.



Generatiiviset järjestelmät: synteettisten tuotosten merkitseminen



Merkintä: synteettistä ääni-, kuva-, video- tai tekstisisältöä tuottavan järjestelmän tarjoajan on varmistettava, että tuotokset merkitään koneluettavasti keinotekoisiksi tai manipuloiduiksi.



Tekniset ratkaisut: tehokkaita, yhteentoimivia, vakaita ja luotettavia teknisesti mahdollisissa rajoissa.



Poikkeus: ei koske vakioimuokkausta avustavia tai syöttödataa olennaisesti muuttamattomia järjestelmiä.



Siirtymäaika: ennen 2.8.2026 markkinoille saatettujen järjestelmien on noudatettava merkintää viimeistään 2.12.2026.



Generatiiviset järjestelmät: syvävääreännösten avoimuus



Ilmoitus: syvävääreännöksen muodostavaa kuva-, ääni- tai videosisältöä tuottavan/muokkaavan järjestelmän käyttöönottajana on ilmoitettava sisällön keinotekoisuudesta.



Taide ja satiiri: osana taiteellista, luovaa, satiirista tai fiktiivistä teosta avoimuus rajoittuu paljastamiseen, joka ei haittaa teoksen esittämistä.



Poikkeus: ei koske rikoksentorjuntatarkoituksia.



Generatiiviset järjestelmät: yleistä etua koskevan tekstin avoimuus



Ilmoitus: kun tekstiä tuotetaan/muokataan yleisölle tiedottamiseksi yleistä etua koskevista asioista, on ilmoitettava sisällön keinotekoisuudesta.



Poikkeus: ei koske sisältöä, joka on käynyt läpi ihmisen toimituksellisen valvonnan ja jolla on toimituksellinen vastuuhenkilö.



Poikkeus: ei koske rikoksentorjuntatarkoituksia.



Tunteentunnistus- ja biometriset luokitusjärjestelmät



Ilmoitus: tunteentunnistus- tai biometrisen luokitusjärjestelmän käyttöönottajana on ilmoitettava järjestelmän toiminnasta sille altistuville henkilöille.



Poikkeus: ei koske rikoksentorjuntatarkoituksia.

**Vähäisen riskin
käyttötapaukset ja
vapaaehtoiset
käytännესäännöt**





Vapaaehtoiset käytäntesäännöt



Vähäisen riskin järjestelmille ei aseteta erityisiä vaatimuksia – tähän kuuluu suurin osa järjestelmistä, ml. valtaosa teollisuustuotannon käyttötapauksista.

Vapaaehtoiset käytäntesäännöt

Tarjoajat voivat varmistaa luotettavuuden kehittämällä omia tai noudattamalla muiden edustavien tahojen hyväksymiä käytäntesääntöjä.

Yleiskäyttöisten tekoälymallien vaatimukset





Yleiskäyttöiset tekoälymallit: kaksitasoinen riskiluokittelu



Systemisen riskin mallit

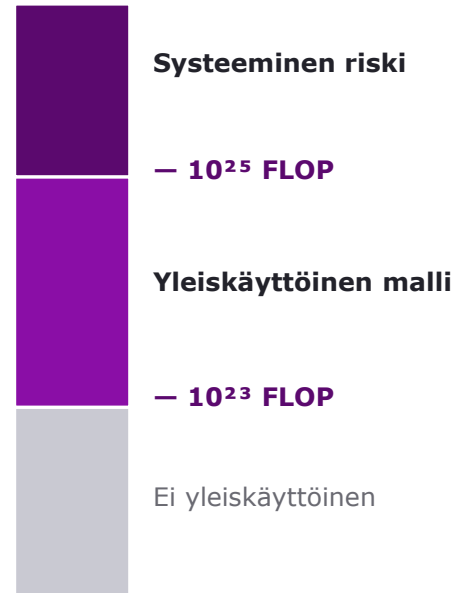
Laskentatehoa $\geq 10^{25}$ FLOP
tai komission arvio. →
Lisävaatimukset.



Kaikki yleiskäyttöiset tekoälymallit

Laskentatehoa $\geq 10^{23}$ FLOP ja malli
tuottaa kieltä, kuvaa tai videota. →
Avoimuus- ja informointivaatimukset.

Laskentateho (FLOP) ↑



Komissio voi päivittää kynnyksarvoja teknologian kehittyessä.



Kaikkia yleiskäyttöisiä malleja koskevat vaatimukset



Dokumentaatio ja arviointi: tekninen dokumentaatio ajan tasalla, ml. koulutus- ja testausprosessi sekä arvioinnin tulokset.



Jatkotarjoajan informointi: tiedot ja dokumentaatio järjestelmätarjoajille mallin ominaisuuksista ja rajoituksista.



Tekijänoikeudet: toimintapolitiikka EU:n tekijänoikeussäätelyyn sekä julkinen tiivistelmä koulutusdatasta.



Sovelletaan 2.8.2025. Avoimen lähdekoodin malleja (ei systeemistä riskiä) koskevat vain tekijänoikeusvaatimukset; tukena käytännesäännöt (komissio arvioi riittävyyden).



Systemisen riskin mallien lisävaatimukset



Mallin arviointi standardoiduin protokollin, ml. adversariaalinen testaus ja sen dokumentointi.



Systemisten riskien arviointi ja lieventäminen.



Vakavat vaaratilanteet: seuranta, dokumentointi ja raportointi.



Kyberturvallisuus mallille ja sen fyysiselle infrastruktuurille. Koskee myös avoimen lähdekoodin malleja, joihin liittyy systeminen riski. Sovelletaan 2.8.2025.



Avoimen lähdekoodin yleiskäyttöiset tekoälymallit



Avoin malli: maksuttomalla avoimen lähdekoodin lisenssillä tarjottu malli, jonka parametrit ja tiedot arkkitehtuurista ja käytöstä ovat julkisia, noudattaa tekijänoikeusvaatimuksia.



Systeeminen riski: jos avoimeen malliin liittyy systeeminen riski, sen on noudatettava kaikkia vaatimuksia.



Yleiskäyttöisen mallin muuttaminen tai hienosäätäminen



Jatkokehittäjästä tarjoaja: jos mallia merkittävästi muutetaan/hienosäädetään muun kuin alkuperäisen tarjoajan toimesta, jatkokehittäjään sovelletaan mallin tarjoajan velvoitteita.



Merkittävä muutos: käytetty laskentateho $\geq 1/3$ alkuperäisen mallin koulutustehosta.

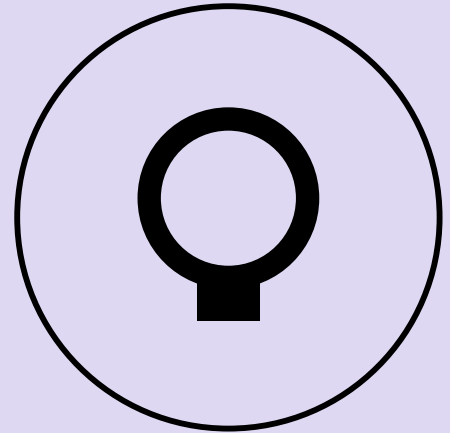


Kynnysarvot: jos alkuperäistä tehoa ei tiedetä: 10^{25} FLOP (systeminen riski) ja 10^{23} FLOP (ei systeemistä riskiä).



Rajaus: velvoitteet rajautuvat kyseiseen muutokseen, esim. täydentämällä teknisiä asiakirjoja uusilla tietolähteillä.

Innovointia tukevat toimet





Tekoälyn sääntelyn testiympäristöt



Kansallinen testiympäristö: kunkin jäsenmaan on perustettava vähintään yksi riittävästi resursoitu sääntelyn testiympäristö – toiminnassa viimeistään 2.8.2027.



Mitä tarjoaa: mahdollisuus kehittää, kouluttaa, testata ja validoida järjestelmiä ennen markkinoille saattamista viranomaisten kanssa sovitun suunnitelman mukaan.



Unionin taso: tekoälytoimisto voi perustaa unionin tason testiympäristön, jossa pk-, startup- ja pienillä keskisuurilla yrityksillä (small mid-cap) on etusija.



Edut: ei hallinnollisia sakkoja rikkomuksista (vastuu kolmansille säilyy); maksutonta pk- ja startup-yrityksille.



Testiympäristö ja asetuksen vaatimusten täyttäminen



Kirjallinen todiste: viranomaisen on tarjoajan pyynnöstä annettava todiste onnistuneesti suoritetuista toimista.



Loppuraportti: viranomainen antaa raportin suoritetuista toimista, tuloksista ja oppimistuloksista.



Hyödyntäminen: asiakirjoilla voi osoittaa asetuksen noudattamista; valvojien ja ilmoitettujen laitosten on otettava ne myönteisesti huomioon.



Suuririskisen järjestelmän testaaminen todellisissa olosuhteissa



Kesto: suuririskistä järjestelmää voi testata todellisissa olosuhteissa testiympäristön ulkopuolella enintään 12 kk.



Ehdot: markkinavalvontaviranomaisen hyväksymä testaussuunnitelma; osallistujilta tietoinen suostumus; tarjoaja vastaa vahingoista.



Laajuus: liitteen III käyttötapaukset ja liitteen I osion A tuotteet; osion B tuotteille jäsenvaltiot voivat sallia testauksen erillisin puittein.



Muita innovointia tukevia toimia



Jäsenmaat: räätälöity tiedotus ja koulutus pk- ja startup-yrityksille; ohjeistus ja tuki; osallistumisen helpottaminen standardointiin.



Tekoälytoimisto: standardoidut mallit eri aloille, helppokäyttöinen tietoausta ja tiedotuskampanjat.



Pk- ja keskisuurten kevennykset: yksinkertaistettu tekninen dokumentaatio (komission lomake) ja yksinkertaistettu laatujärjestelmä kaikille pk-yrityksille.

Hallinnointi ja seuraamukset





Hallinnointi: jäsenmaa- ja EU-taso



Jäsenmaatase

Viranomaiset: nimeää kansalliset toimivaltaiset viranomaiset – vähintään yksi ilmoittamisesta vastaava ja yksi markkinavalvontaviranomainen.

Valvonta ja toimeenpano: valvoo tekoälyjärjestelmiä omalla alueellaan, käsittelee vaaratilanneilmoitukset ja määrää seuraamukset.

Testiympäristö: perustaa ja ylläpitää kansallista sääntelyn testiympäristöä.



EU-tase

Euroopan tekoälyneuvosto: jäsenmaat, komissio ja Euroopan tietosuojavaltuutettu; yhdenmukaistaa soveltamista ja antaa suosituksia.

Euroopan tekoälytoimisto: valvoo ja luokittelee yleiskäyttöisiä tekoälymalleja koko EU:ssa; omnibus laajentaa toimivaltaa myös yleiskäyttöisiin malleihin perustuviin järjestelmiin (sama tarjoaja) ja erittäin suuriin verkkoalustoisiin ja -hakukoneisiin – tutkinta- ja tarkastusvaltuudet, sakot ja uhkasakot.

Ero: jäsenmaat valvovat yksittäisiä tekoälyjärjestelmiä kansallisesti; EU-tason tekoälytoimisto valvoo yleiskäyttöisiä malleja keskitetysti ja koordinoi asetuksen yhtenäistä soveltamista.



Komission suuntaviivat



Komissio on velvollinen tuottamaan seuraavat suuntaviivat säädöksen käytännön täytäntöönpanosta:



Suuririskisten järjestelmien vaatimukset ja arvoketjun velvollisuudet



Kielletyt käytännöt



Merkittävää muutosta koskevien säännösten täytäntöönpano



Avoimuusvelvoitteiden täytäntöönpano



Tekoälyasetuksen suhde tuoteturvasäätelyyn (liite I) ja muuhun säätelyyn



Tekoälyjärjestelmän määritelmän soveltaminen



Seuraamukset



Kiellettyjen käytäntöjen rikkominen — enintään 7 % liikevaihdosta tai

35 M€

Suuririskisten järjestelmien ja yleiskäyttöisten mallien säännösten sekä muiden velvoitteiden rikkominen — enintään 3 % liikevaihdosta tai

15 M€

Virheellisen, puutteellisen tai harhaanjohtavan tiedon toimittaminen — enintään 1 % liikevaihdosta tai

7,5 M€

Suurilla yrityksillä sakon enimmäismäärä on euromäärästä ja %-osuudesta suurempi, pk-, startup- ja small mid-cap -yrityksillä pienempi. Uhkasakko enintään 5 % päivittäisestä liikevaihdosta.

Soveltamisaikataulu





Soveltamisaikataulu



2/2025



Kielletyt käytännöt; tekoälylukutaito

8/2025



Yleiskäyttöiset mallit; hallinto ja seuraamukset

8/2026



Avoimuusvelvoitteet (mm. tekoälyn kanssa asiointi, syvävääreennökset, synteettisen sisällön merkintä)

12/2026



Uudet kiellot (intiimimateriaali, CSAM); synteettisen sisällön merkintä ennen 8/2026 markkinoille saatetuissa järjestelmissä

8/2027



Säätelyn testiympäristöt; ennen 8/2025 markkinoille tuodut yleiskäyttöiset mallit

12/2027



Suuririskiset järjestelmät – liite III (käyttötapauskset)

8/2028



Suuririskiset tuotteet ja turvakomponentit – liite I (tuoteturva)

8/2030



Ennen suuririskisäännösten soveltamista käyttöön otetut, viranomaiskäyttöön tarkoitetut suuririskiset järjestelmät