EU:n tekoälyasetus – tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien turvallisuussäädös

Teknologiateollisuus ry

5.2.2025

Sisällys

Tiivistelmä

1. Soveltamisala

- Asetus koskee EU:ssa markkinoille saatettavia ja EU:ssa käyttöönotettavia tekoälyjärjestelmiä sekä yleiskäyttöisiä tekoälyämalleja, kuten suuria kielimalleja, joille monet tekoälyjärjestelmät pohjautuvat.
- Yksinkertaiset ohjelmistot ja ihmisen asettamia sääntöjä suoraviivaisesti seuraavat päätöksentekojärjestelmät eivät tule asetuksen piiriin.
- Markkinoille saatetut tai käyttöönotetut vapaat ja avoimeen lähdekoodiin perustuvat järjestelmät ja mallit tulevat pääosin säädöksen piiriin.
- Asetuksen ulkopuolelle jäävät tutkimus- ja kehitysvaiheessa olevat järjestelmät ja mallit sekä järjestelmät, jotka on tarkoitettu yksinomaan sotilaalliseen, puolustukselliseen tai kansallisen turvallisuuden käyttöön.

2. Turvallisuussäädös

- Asetuksen tavoitteena on suojata terveyttä, turvallisuutta ja perusoikeuksia tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien käytöstä aiheutuvilta riskeiltä ja haitoilta.
- Säädös pyrkii asettamaan tekoälyjärjestelmien ja -mallien vaatimukset riskiperusteisesti. Olennaista on tarjoajana tai käyttöönottajana tietää, mihin riskiluokkaan järjestelmä tai malli kuuluu, jotta voi täyttää velvoitteensa.

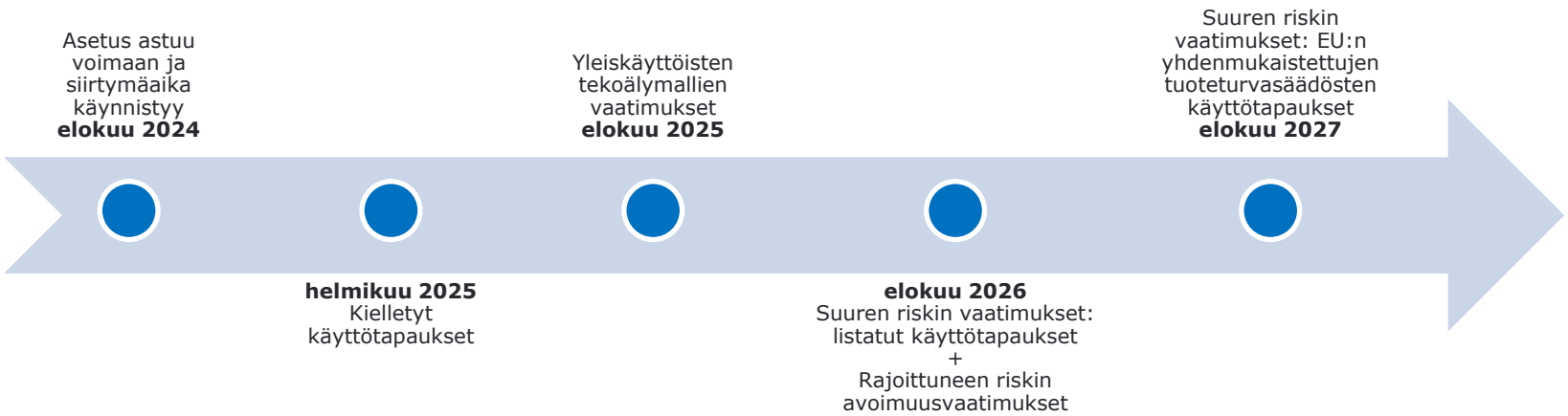
3. Tekoälyjärjestelmien riskiluokittelu

- Kestämättömiä riskejä sisältävien järjestelmien käyttö kielletään. Esimerkkinä voidaan mainita sosiaalinen pisteytys. Joidenkin kiellettyjen järjestelmien käyttö on sallittua tietyissä tarkkaan rajatuissa tapauksissa.
- Suuren riskin järjestelmien käyttö on sallittua, kunhan järjestelmä täyttää sille asetetut vaatimukset. Suuren riskin piiri kattaa tuotteita ja niiden turvakomponentteja, jotka ovat EU:n tuoteturvallisuuslainsäädännön piirissä, kuten koneet. Lisäksi suuren riskin piiriin luetaan muita määriteltyjä käyttötapauksia, kuten rekrytointi ja kriittisen digitaalisen infrastruktuurin hallinnointi. Suuren riskin vaatimuksista on mahdollisuus poiketa tietyissä määritellyissä tapauksissa.
- Rajoittuneita riskejä käsittävien generatiivisten ja muiden järjestelmien tarjoamiselle ja käytölle asetetaan tiettyjä avoimuusvaatimuksia. Ihmisen on esimerkiksi saatava tieto siitä, että hän kommunikoi tekoälyjärjestelmän kanssa.
- Vähäisen riskin järjestelmille ei aseteta vaatimuksia. Suurin osa järjestelmistä, mukaan lukien valtaosa teollisuustuotannon käyttötapauksista, lukeutuu tähän luokkaan.

4. Yleiskäyttöisten tekoälymallien riskiluokittelu

- Kaikkia malleja koskevat tietyt avoimuus- ja informointivaatimukset. Näitä ovat muun muassa mallin tekoälyjärjestelmäänsä integroivien jatkokehittäjien informoiminen mallin ominaisuuksista sekä riittävän yksityiskohtaisen tiivistelmän laatiminen mallin koulutukseen käytetyistä sisällöistä.
- Systeemisiä riskejä sisältävien mallien, jotka ovat tyypillisesti isoimpia perustamalleja, on lisäksi täytettävä tietyt lisävaatimukset, mukaan lukien mallin arviointi ja adversiaalinen testaus.

5. Vaiheittainen soveltamisaikataulu



Soveltamisala ja määritelmät

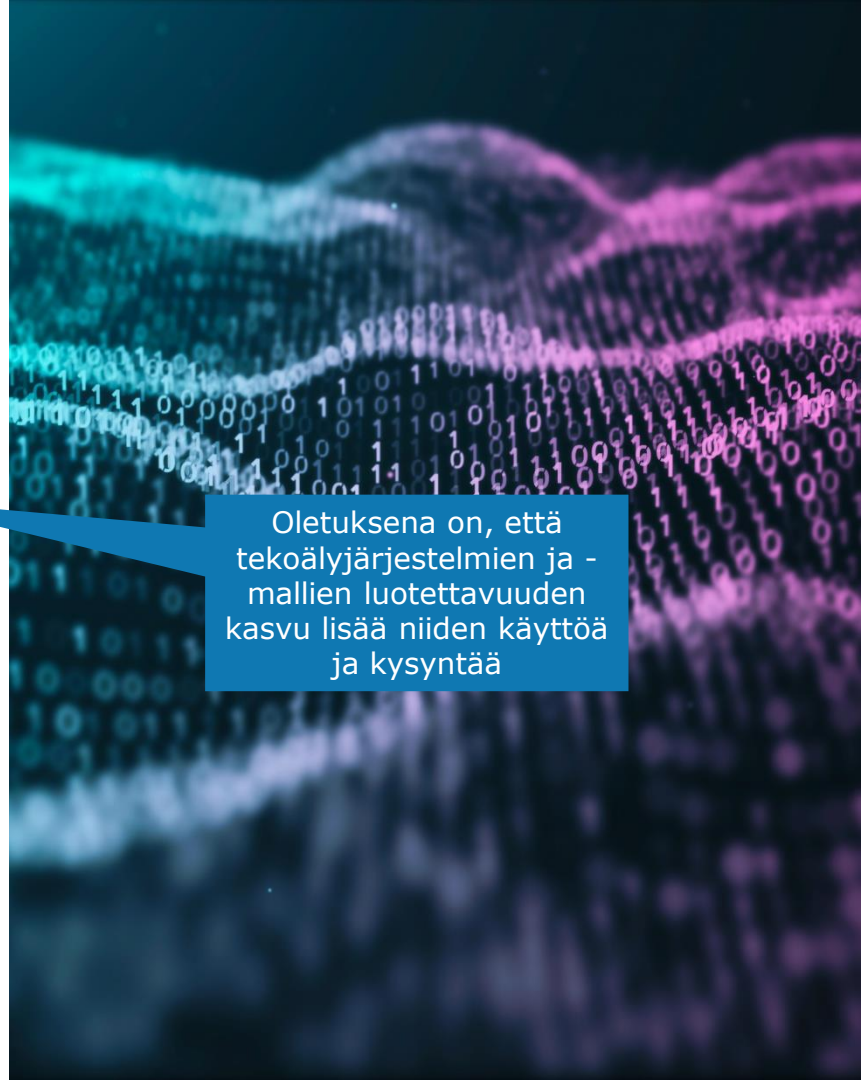
Mikä ihmeen tekoälyasetus?

Tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien turvallisuussäädös

- Tavoitteena on suojata terveyttä, turvallisuutta ja perusoikeuksia tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien käytöstä aiheutuvilta riskeiltä ja haitoilta.

- Sovelletaan sellaisenaan EU:ssa kaikilla sektoreilla ja toimialoilla.

- Säädös pyrkii asettamaan tekoälyjärjestelmien ja -mallien vaatimukset riskiperusteisesti.

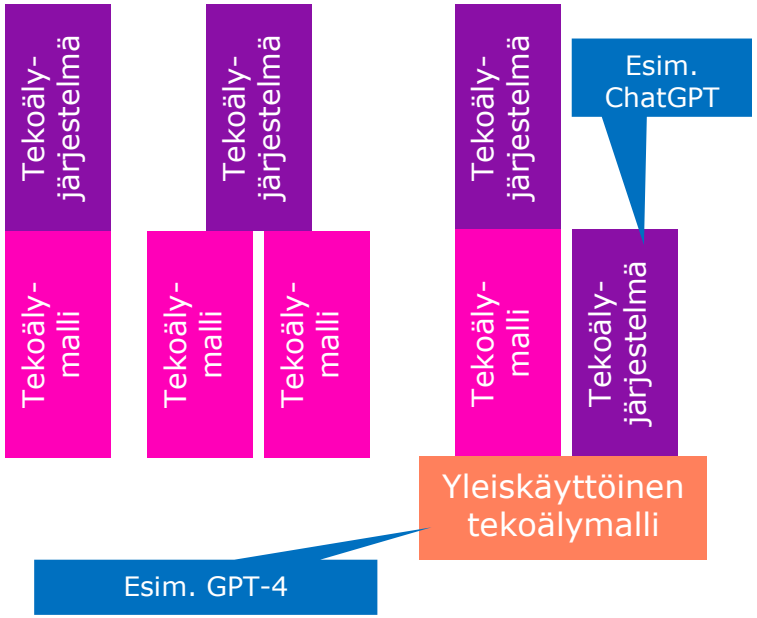


Asetuksen viitekehys:

Tekoälyjärjestelmät ja tekoälymallit

- Tekoälyjärjestelmä on sovellus, jolla on tietty käyttötarkoitus.
  - Järjestelmä voi rakentua yhden tai useamman yleiskäyttöisen tai kapean tekoälymallin varaan.

- Tekoälymalli on tekoälyjärjestelmän moottori, joka määrittää, miten järjestelmä käsittelee tietoa tietyissä tehtävissä, kuten kuvan tunnistuksessa tai kielen kääntämisessä.
  - On kapean tehtäväkentän omaavia malleja ja yleiskäyttöisiä malleja (esim. suuret kielimallit) joiden tehtäväkenttä on laaja.
  - Yleiskäyttöistä mallia voidaan jatkokehittää rajatummaksi malliksi.



Määritelmä:

Tekoälyjärjestelmä

- Suunniteltu toimimaan vaihtelevalla autonomian tasolla.
- Voi kyetä mukautumaan käyttöönoton jälkeen.
- Tavoitteitaan varten päättelee vastaanottamastaan syötteestä, kuinka luodaan tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä.
- Tuotokset vaikuttavat fyysiseen tai virtuaaliseen ympäristöön.

Tekoälyjärjestelmä *on konepohjainen järjestelmä, joka on suunniteltu toimimaan käyttöönoton jälkeen vaihtelevilla autonomian tasoilla ja jossa voi ilmetä mukautuvuutta käyttöönoton jälkeen ja joka päättelee vastaanottamastaan syötteestä eksplisiittisiä tai implisiittisiä tavoitteita varten, miten tuottaa tuotoksia, kuten ennusteita, sisältöä, suosituksia tai päätöksiä, jotka voivat vaikuttaa fyysisiin tai virtuaalisiin ympäristöihin.*

Määritelmä ei kata:
- Perinteiset yksinkertaiset ohjelmistojärjestelmät
- Automaattiset päätöksentekojärjestelmät, jotka noudattavat ihmisen asettamia sääntöjä

Määritelmä:

Yleiskäyttöinen tekoälymalli

Esim. suuret kielimallit ja multimodaaliset perustamallit

- Tyypillisesti koulutettu suurella määrällä dataa ja käsittää suuren määrän parametrejä.
- Kykenee suorittamaan pätevästi laajan määrän erilaisia tehtäviä.
- Voidaan integroida erilaisiin järjestelmiin tai sovelluksiin.

Yleiskäyttöinen tekoälymalli *on tekoälymalli, myös silloin, kun tällainen tekoälymalli on koulutettu suurella määrällä dataa käyttäen laajamittaista itsevalvontaa, joka on hyvin yleisluonteinen ja pystyy suorittamaan pätevästi monenlaisia erillisiä tehtäviä riippumatta siitä, miten malli saatetaan markkinoille, ja joka voidaan integroida erilaisiin ketjun loppupään järjestelmiin tai sovelluksiin.*

Voidaan saattaa markkinoille esimerkiksi:
- Kirjaston tai ohjelmointirajapinnan kautta
- Latauksena
- Fyysisenä kopiona

Keskeiset toimijat

Tarjoaja (Provider)

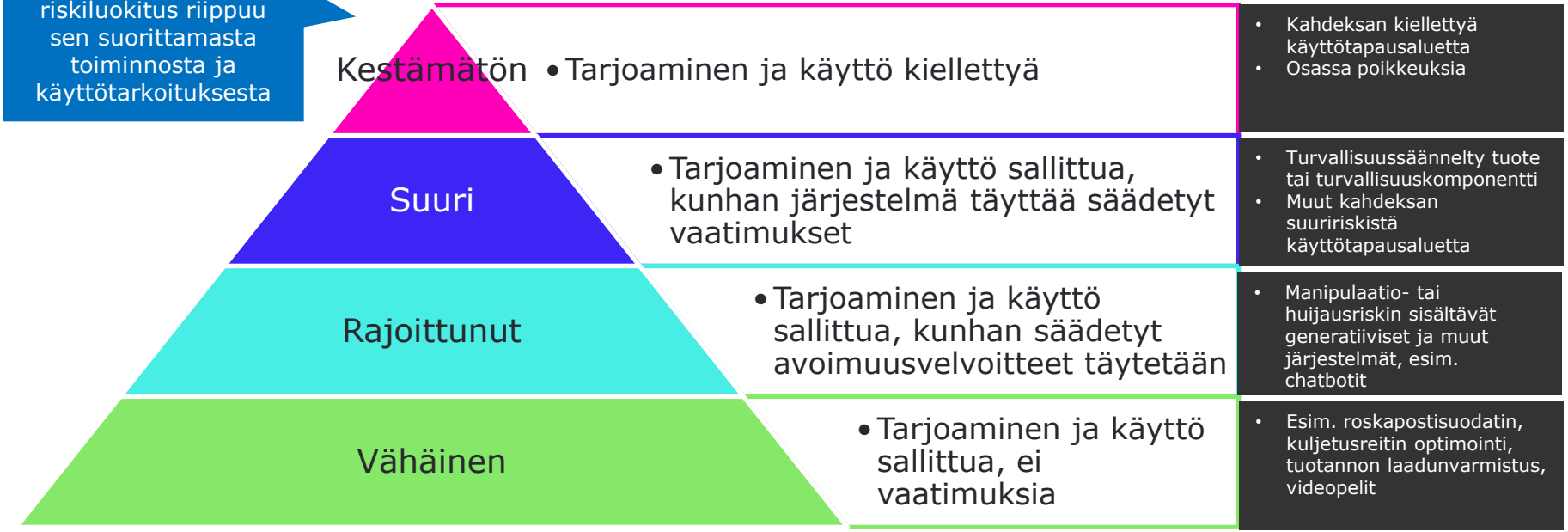
- Kehittää tai kehityttää tekoälyjärjestelmän tai yleiskäyttöisen tekoälymallin ja saattaa sen EU-markkinoille tai ottaa sen käyttöön omalla nimellä tai tavaramerkillä joko maksua vastaan tai ilmaiseksi
- Riippumaton sijoittautumispaikasta
- Yritys tai muu oikeushenkilö, viranomainen, virasto, luonnollinen henkilö

Käyttöönottaja (Deployer)

- Käyttää tekoälyjärjestelmää
- Sijoittautunut EU-alueelle tai käytetyn järjestelmän tuotos kohdistuu EU-alueelle
- Yritys tai muu oikeushenkilö, viranomainen, virasto, luonnollinen henkilö
- Luonnollisen henkilön henkilökohtainen, muu kuin ammattitoiminnassa tapahtuva käyttö ei lukeudu soveltamisalaan

Riskiluokittelu

Tekoälyjärjestelmän riskiluokitus riippuu sen suorittamasta toiminnosta ja käyttötarkoituksesta



Yleiskäyttöisille tekoälymalleille kaksitasoinen riskiluokittelu

Systeemisen riskin mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

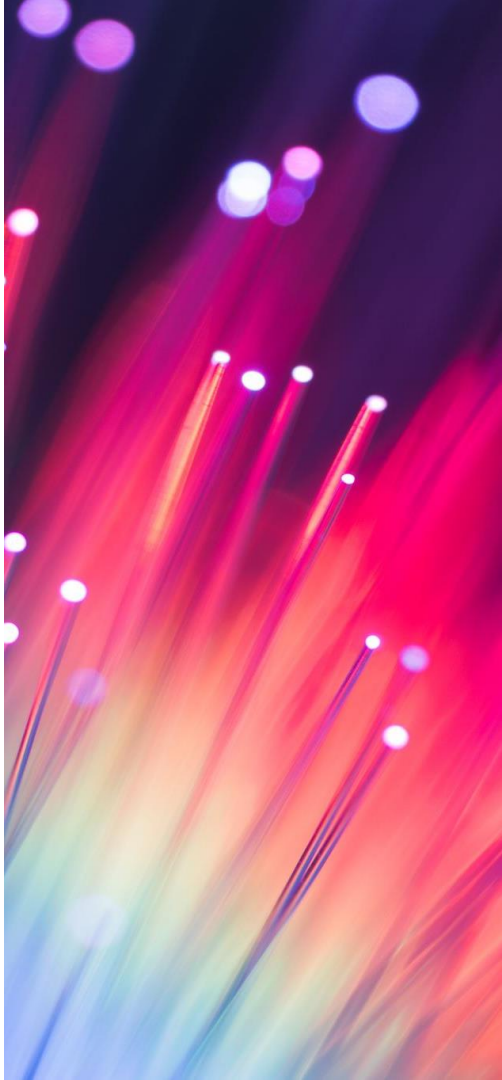
Asetuksen piiriin eivät tule

- Tieteelliseen tutkimus- ja kehityskäyttöön tarkoitetut tekoälyjärjestelmät ja -mallit.

- Tutkimus- ja kehitysvaiheessa olevat järjestelmät ja mallit, joita ei ole vielä saatettu markkinoille tai otettu käyttöön.
  - Tämä poikkeus ei kata järjestelmän tai mallin testausta tosielämän olosuhteissa.

- Yksinomaan sotilaalliseen, puolustukselliseen tai kansallisen turvallisuuden käyttöön tarkoitetut järjestelmät.

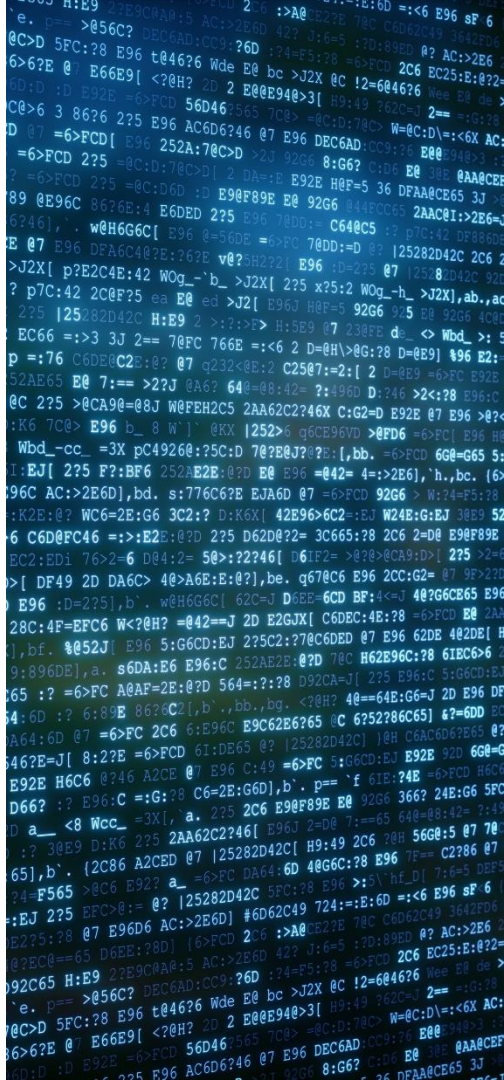
- Luonnolliset henkilöt, jotka käyttävät järjestelmää pelkästään henkilökohtaisessa ja muussa kuin ammattitoiminnassa.



Avoimen lähdekoodin tekoälyjärjestelmät

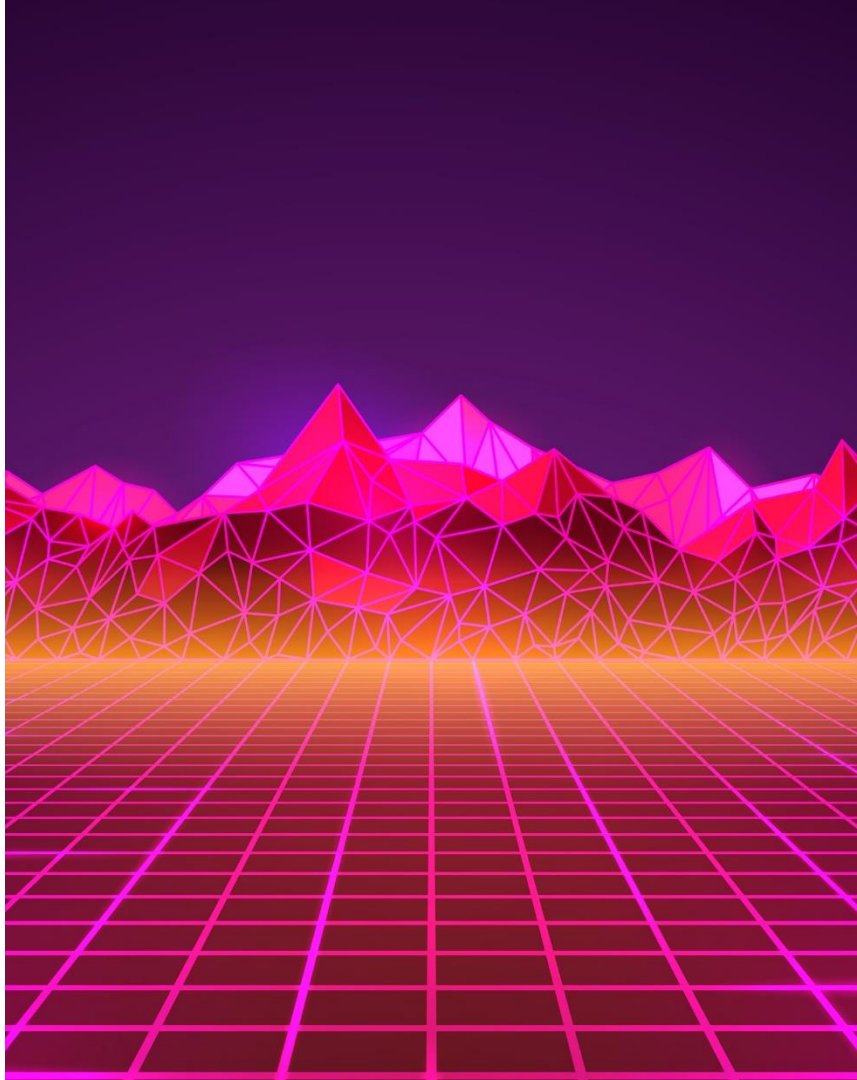
Asetusta ei sovelleta vapaisiin ja avoimeen lähdekoodiin perustuviin tekoälyjärjestelmiin, paitsi jos ne saatetaan markkinoille tai otetaan käyttöön

- suuririskisinä tekoälyjärjestelminä,
- tekoälyjärjestelminä, joiden käyttötapaukset ovat kiellettyjä tai
- tekoälyjärjestelminä, joihin sovelletaan avoimuusvelvoitteita.

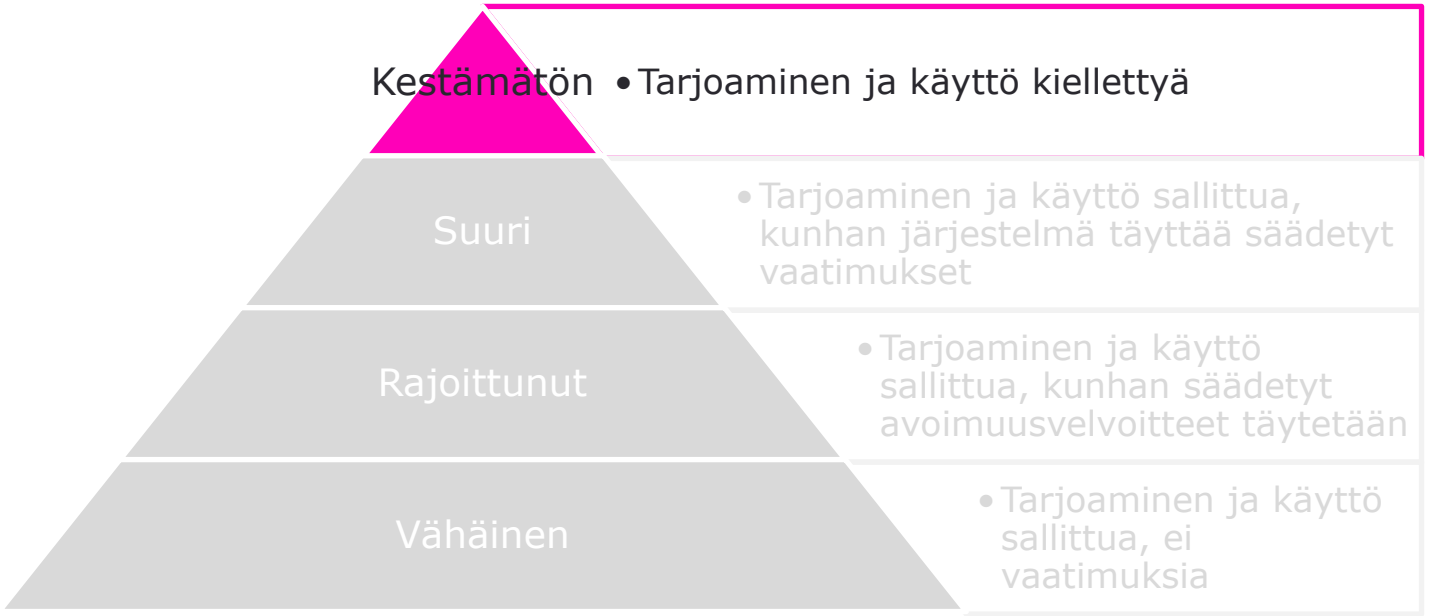


Tekoälylukutaito

- Tekoälyjärjestelmien tarjoajien ja käyttöönottajien on parhaansa mukaan varmistettava henkilöstönsä ja muiden niiden puolesta tekoälyjärjestelmien toiminnasta ja käytöstä vastaavien henkilöiden riittävä tekoälylukutaito.



Kielletyt käyttötapaukset



Systeemisen riskin mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

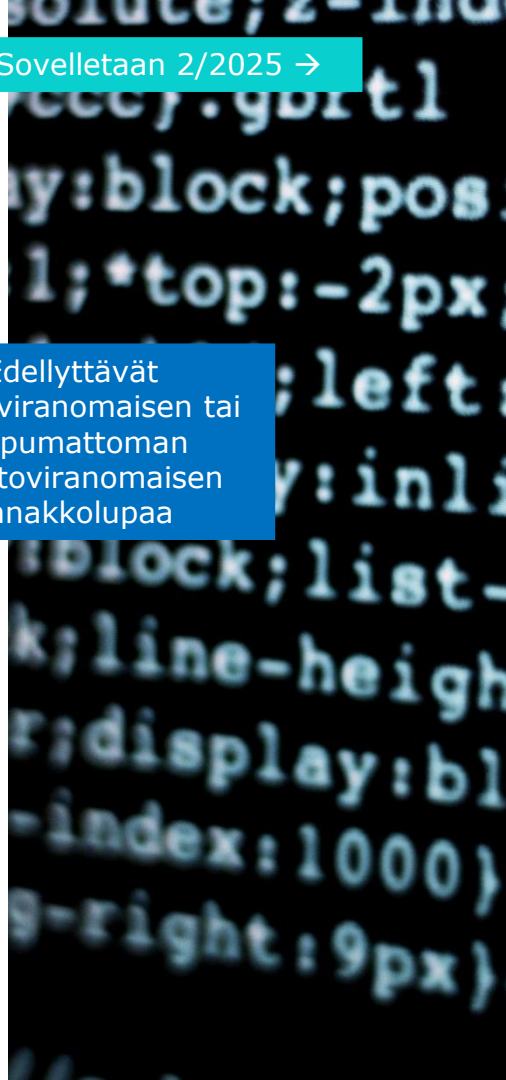
Kielletyt käyttötapaukset 1/2

Sovelletaan 2/2025 →

- Reaaliaikainen biometrinen etätunnistaminen julkisissa tiloissa lainvalvontatarkoituksessa
  - Ei kata:
    - Terrori-iskun ehkäisy tai siihen vastaaminen
    - Kadonneiden tai rikoksen uhrien etsintä
    - Tiettyihin vakaviin rikoksiin liittyvä lainvalvonta

Edellyttävät oikeusviranomaisen tai riippumattoman hallintoviranomaisen ennakkolupaa

- Haitalliset alitajuiset tekniikat
- Haavoittuvien ryhmien hyväksikäyttö
  - Ikä, vamma, sosiaalinen tai taloudellinen tilanne
- Sosiaalinen pisteytys, joka johtaa henkilöiden tai ryhmien haitalliseen tai epäedulliseen kohteluun



Kielletyt käyttötapaukset 2/2

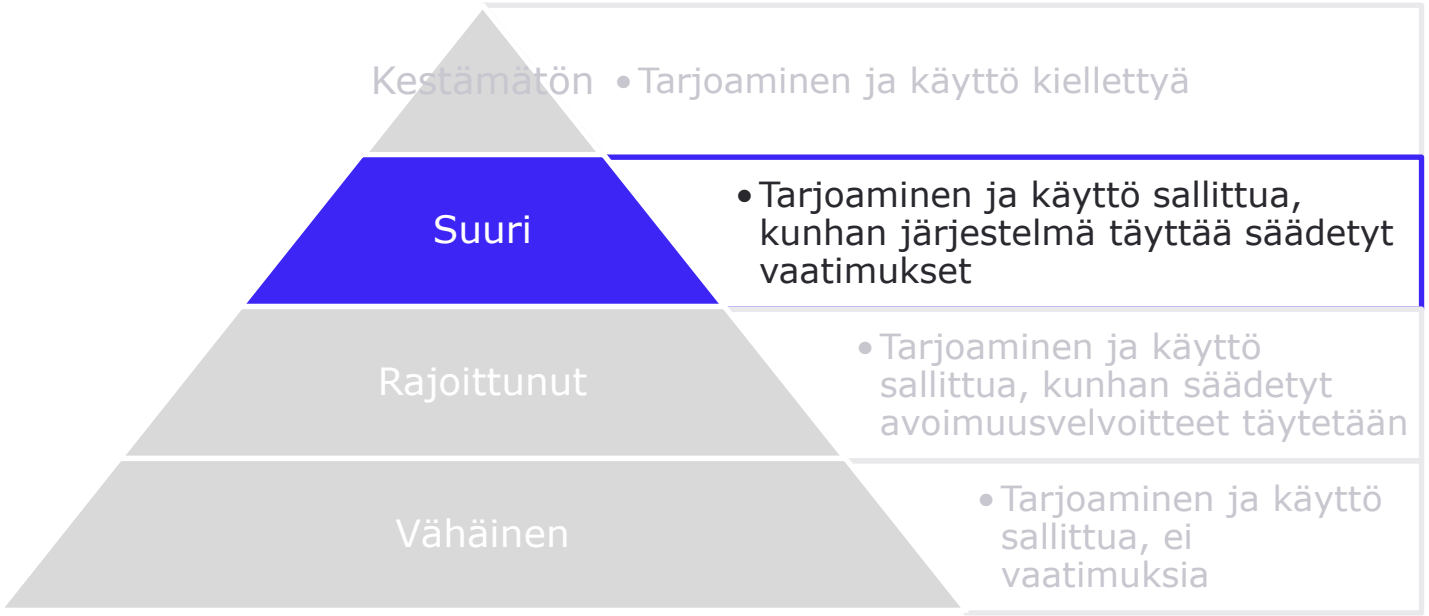
- Henkilön luokittelu tämän biometristen tietojen perusteella rodun, poliittisten mielipiteiden, ammattiliittojen jäsenyyden, uskonnollisen tai filosofisen vakaumuksen tai seksuaalisen suuntautumisen päättelemiseksi
  - Ei kata laillisesti hankittujen biometristen tietojoukkojen merkintöjä tai suodattamista esimerkiksi lainvalvontatarkoituksissa.

- Profilointiin perustuva rikosriskin ennakointi tai arviointi

- Tunteiden päätteleminen työpaikalla tai oppilaitoksessa
  - Ei koske lääketieteellisiä tai turvallisuuteen liittyviä käyttötarkoituksia

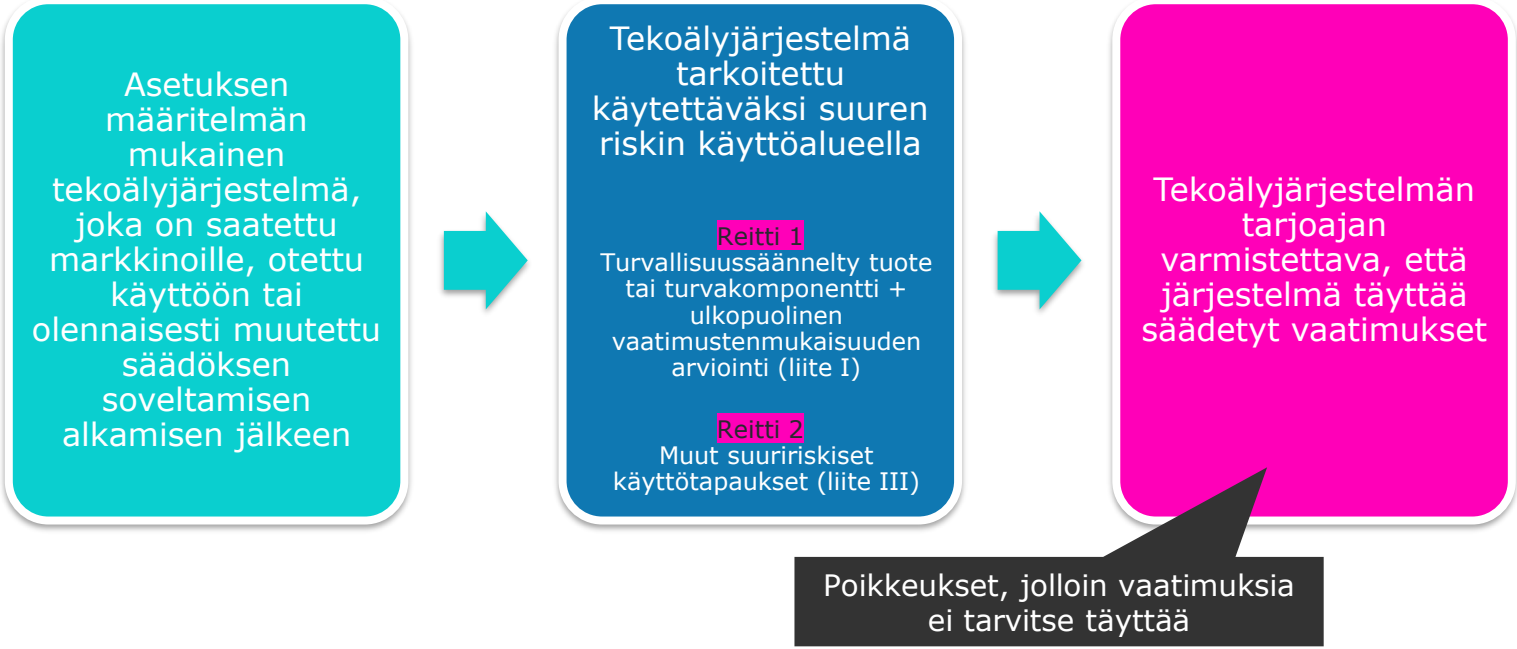
- Kasvojentunnistustietokantojen luominen tai laajentaminen kasvokuvien kohdistamattomalla haravoinnilla internetistä tai valvontakamera-aineistosta

Suuren riskin käyttötapaukset ja vaatimukset



Systeemisen riskin mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

Reitit suuren riskin vaatimusten piiriin



Reitti 1

Sovelletaan 8/2027 →

Suuririskiset käyttötapaukset:

Turvallisuussäännellyt tuotteet ja turvakomponentit

- Tekoälyjärjestelmä, joka

1. on tuote tai tuotteen turvakomponentti, joka kuuluu EU:n tuoteturvallisuuslainsäädännön piiriin

2. JA jolle on tuon sääntelyn perusteella suoritettava kolmannen osapuolen vaatimustenmukaisuuden arviointi.

Turvallisuussäädökset luetellaan asetuksen liitteessä I: NLF-mukautetut säädökset (osio A) + muut yhdenmukaistetut säädökset (osio B)

Reitti 1

Tuoteturvasäädösten kautta tekoälyasetuksen soveltamisalaan tulevia tuoteryhmiä

Nämä säädökset luetellaan asetuksen I liitteen jaksossa A

- Koneet
- Lelut
- Huviveneet ja vesiskootterit
- Hissit
- Räjähdysvaarallisissa tiloissa käytettäviksi tarkoitetut laitteet ja suojajärjestelmät
- Radiolaitteet
- Painelaitteet
- Köysiratalaitteet
- Henkilönsuojaimet
- Kaasumaisia polttoaineita polttavat laitteet
- Lääkinnälliset laitteet ja in vitro -diagnostiikkalaitteet

Reitti 1

Kulkuneuvoja koskevat säädökset

Nämä säädökset luetellaan asetuksen I liitteen jaksossa B

Kulkuneuvojen kohdalla tekoälyasetus soveltuu vain osin. Kulkuneuvojen suuririskisten tekoälyjärjestelmien vaatimuksista tullaan säätämään erikseen niiden sektorisäädöksissä.

- Siviililentokoneet ja miehittämättömät ilma-alukset
- Kaksi-, kolmi- ja nelipyöräiset ajoneuvot
- Maa- ja metsätalousajoneuvot
- Laivavarusteet
- Rautatiejärjestelmät
- Moottoriajoneuvot ja niiden perävaunut

Reitti 2

Muut suuririskiset käyttötapaukset 1/3

Sovelletaan 8/2026 →

- Biometrinen etätunnistaminen ja luokittelu sekä tunteiden tunnistaminen
  - Kiellettyjen käyttötarkoitusten ulkopuolelle jäävät tapaukset
  - Ei koske yksinomaan henkilöllisyyden todentamiseen ja laitteiden avaamiseen tarkoitettuja järjestelmiä

- Kriittinen infrastruktuuri
  - Kriittisen digitaalisen infrastruktuurin, tieliikenteen sekä vesi-, kaasu-, lämmitys- ja sähköhuollon hallinnan ja toiminnan turvakomponentit
  - Ei koske kyberturvakomponentteja

- Yleissivistävä ja ammatillinen koulutus
  - Oppilas- ja opiskelijavalinnat
  - Oppimisen arviointi ja ohjaaminen, tarjottavan koulutuksen tason arviointi
  - Koetilanteissa kielletyn käytöksen seuranta ja havaitseminen

Luetellaan asetuksen III liitteessä, jota komissio voi muokata tai täydentää

Reitti 2

Muut suuririskiset käyttötapaukset 2/3

- Työllistäminen, henkilöstöhallinto ja itsenäisen ammatinharjoittamisen mahdollistaminen
  - Rekrytoiminen ja työntekijävalinta
    - Työpaikkailmoitusten kohdentaminen
    - Työhakemusten suodattaminen ja analysointi ja hakijoiden arviointi
  - Työehtoihin ja sopimussuhteen päättämiseen ja uralla etenemiseen liittyvät päätökset
  - Työtehtävien jakamiseen yksilöllisen käytöksen tai personallisuuspiirteiden tai henkilön ominaisuuksien perusteella
  - Työsuhteessa olevien suorituksen ja käytöksen seuranta ja arviointi

- Välttämättömien yksityisten palvelujen ja välttämättömien julkisten palvelujen ja etuuksien saatavuus ja käyttö
  - Ihmisen kelpoisuuden arvioiminen liittyen välttämättömiin julkisiin etuisuuksiin ja palveluihin sekä näiden myöntäminen tai epääminen
  - Ihmisen luottoluokituksen arviointi, pois lukien talouspetosten havaitseminen
  - Sairaus- ja henkivakuutuksen riskien arviointi ja hinnoittelu
  - Hätäpuheluiden arviointi ja luokittelu

Reitti 2

Muut suuririskiset käyttötapaukset 3/3

- Lainvalvonta
  - Rikosuhririskin, rikosriskin tai rikoksen uusimisen riskin arviointi
  - Valheenpaljastus
  - Todistusaineiston luotettavuuden arviointi
  - Rikoksen tutkintaan tai syyttämiseen liittyvä profilointi
- Muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta
  - Valheenpaljastus
  - Maahantulijan turvallisuus-, terveys- ja muiden riskien arviointi
  - Turvapaikka-, viisumi- ja oleskelulupahakemusten arviointi
  - Maahantulijoiden havaitseminen tai tunnistaminen
- Oikeudenhoito ja demokraattiset prosessit
  - Tosiasioiden ja lain tutkiminen ja tulkitseminen sekä soveltaminen
  - Vaalien tai kansanäänestyksen tulokseen tai äänestäjiin vaikuttaminen

Reitti 2

Poikkeukset suuren riskin luokituksesta

Tekoälyjärjestelmää ei katsota suuririskiseksi, jos sen tarkoitus on joku seuraavista:

1. Suorittaa suppea menettelytehtävä
   - Esim. strukturoimattoman datan strukturoiminen

Poikkeusmahdollisuus koskee vain III liitteen käyttötapauksia

2. Parantaa aiemmin suoritettua ihmisen toiminnan tulosta
   - Esim. ihmisen tuottaman tekstin tyylin muokkaaminen

3. Havaita päätöksentekotavat tai poikkeamat aiemmista päätöksentekotavoista
   - Esim. opettajan tekemän oppilasarvioinnin poikkeamien tai epäjohdonmukaisuuksien merkitseminen

4. Suorittaa valmistelutehtävä, joka koskee suuririskisten käyttötapausten kannalta merkityksellistä arviointia
   - Esim. tiedostojen käsitteleminen

Poikkeukset eivät päde ihmisten profilointiin tarkoitettuihin järjestelmiin

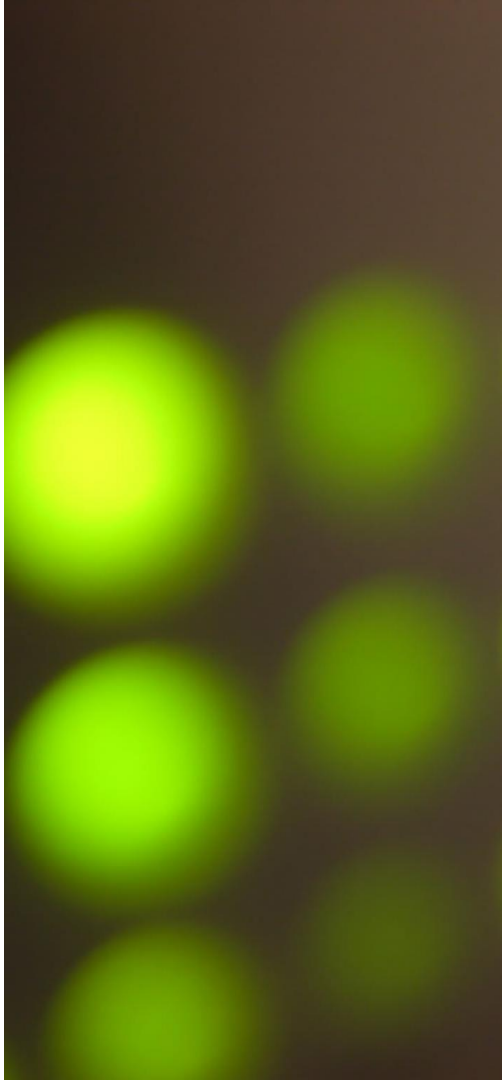
Reitti 2

Poikkeuksen dokumentointi ja rekisteröinti

- Tarjoajan, joka katsoo, että liitteessä III tarkoitettu tekoälyjärjestelmä ei ole suuririskinen, on dokumentoitava arvionsa ennen kuin järjestelmä saatetaan markkinoille tai otetaan käyttöön.

- Toimivaltaisten viranomaisten pyynnöstä tarjoajan on toimitettava arviointia koskevat asiakirjat.

- Tarjoajan on lisäksi noudatettava suuririskisten järjestelmien rekisteröintivelvoitetta.
  - Ks. dia 36.

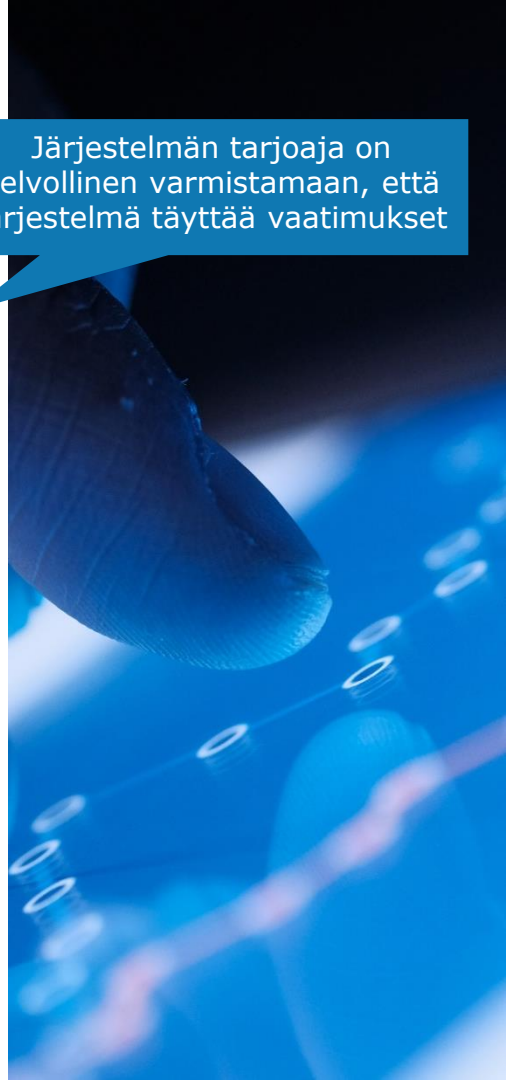


Suuririskisen tekoälyjärjestelmän vaatimukset

- Riskienhallintajärjestelmä
- Data ja datanhallinta
- Tekninen dokumentaatio
- Tietojen säilyttäminen
- Avoimuus ja tietojen antaminen käyttöönottajille
- Ihmisen suorittama valvonta
- Tarkkuus, vakaus ja kyberturvallisuus

Järjestelmän tarjoaja on velvollinen varmistamaan, että järjestelmä täyttää vaatimukset

Vaatimusten täyttämisen tueksi on tarkoitus tuottaa yhdenmukaistettuja standardeja



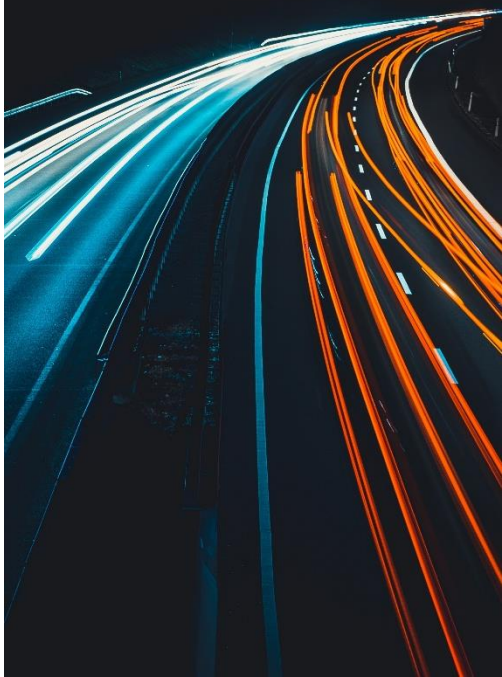
Tarjoajan velvollisuus:

Vaatimustenmukaisuuden arviointi

- Ennen kuin suuririskinen tekoälyjärjestelmä saatetaan EU:n markkinoille tai muulla tavoin otetaan käyttöön, järjestelmän tarjoajan on tehtävä sille vaatimustenmukaisuuden arviointi.
  - Arviointi on toistettava, jos järjestelmää tai sen tarkoitusta muutetaan olennaisesti.

- Liitteen III piiriin tulevan suuririskisen järjestelmän vaatimuksenmukaisuuden arviointi olisi pääsääntönä voitava tehdä tarjoajan itsensä toimesta.
  - Tuoteturvasäänneltyjen tuotteiden ja turvakomponenttien (liite I) kohdalla noudatetaan lähtökohtaisesti kyseisten tuoteturvasäädösten arviointimenettelyä, mukaan lukien kolmannen osapuolen arviointia.

Tarjoajat voivat hyödyntää yhdenmukaistettuja standardeja osoittaakseen, että järjestelmä täyttää asetetut vaatimukset

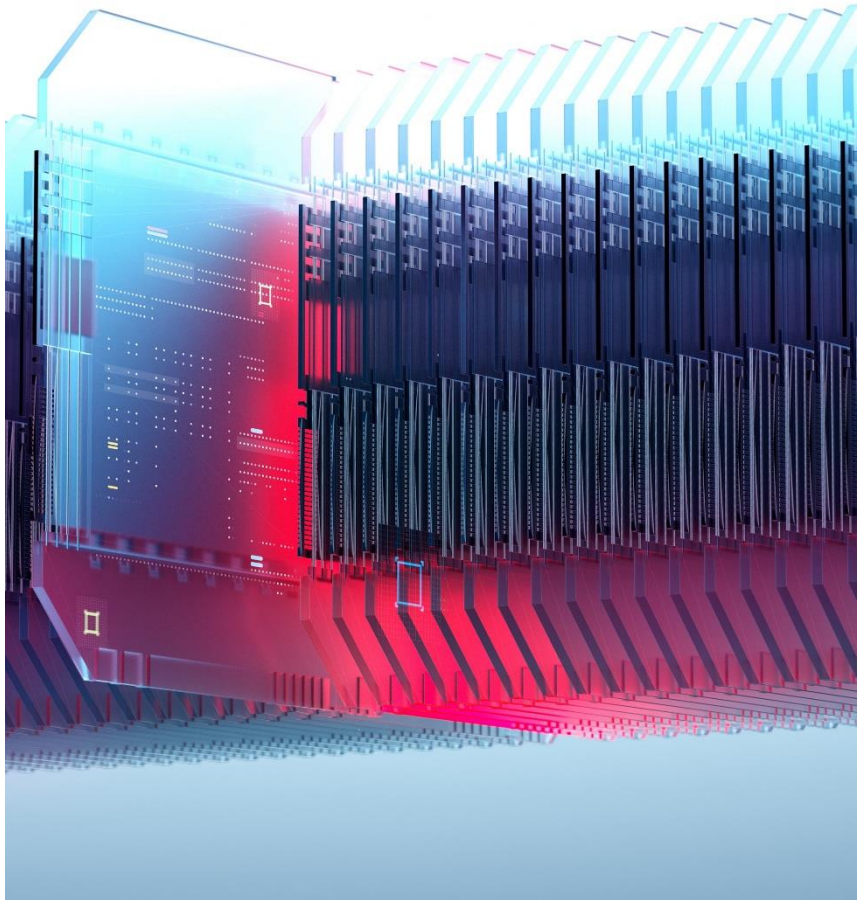


Tarjoajan velvollisuus:

Suuririskisen järjestelmän rekisteröinti

- Liitteen III mukaisen suuririskisen tekoälyjärjestelmän tarjoajan on rekisteröitävä itsensä ja järjestelmänsä EU:n tietokantaan.
  - Tämä on tehtävä ennen järjestelmän markkinoille saattamista tai käyttöönottamista.

- Velvollisuus koskee myös liitteen III piiriin tulevaa järjestelmää, joka ei tarjoajan arvion perusteella ole suuririskinen.



Suuririskisen järjestelmän tarjoajan muut velvollisuudet

- Laatujärjestelmä
- Dokumentaation säilyttäminen (10 vuotta)
- Automaattisesti luotujen lokitietojen säilyttäminen (6 kk)
- Korjaavat toimenpiteet ja tiedonantovelvollisuus
- Yhteistyö toimivaltaisten viranomaisten kanssa
- Valtuutetun EU-edustajan nimeäminen, ellei tarjoaja ole sijoittunut EU:hun
- Markkinoille saattamisen jälkeinen seurantajärjestelmä ja -suunnitelma
- Vakavista vaaratilanteista ilmoittaminen

Vastuut suuririskisen tekoälyjärjestelmän arvoketjussa:

Järjestelmien muokkaaminen

- Käyttöönottajaa, jakelijaa, maahantuojaa tai muuta kolmatta osapuolta pidetään suuririskisen tekoälyjärjestelmän tarjoajana, mikäli:
  - Laittaa nimensä tai tavaramerkkinsä suuririskiseen järjestelmään.
  - Tekee merkittävän muutoksen suuririskiseen järjestelmään siten, että se pysyy suuririskisenä järjestelmänä.
  - Muuttaa tekoälyjärjestelmän käyttötarkoitusta, jota ei ole luokiteltu suuririskiseksi, siten, että järjestelmästä tulee suuririskinen järjestelmä.

Näissä tilanteissa tarjoajaa, joka alun perin saattoi järjestelmän markkinoille tai otti sen käyttöön, ei enää pidetä kyseisen järjestelmän tarjoajana

Alkuperäisen tarjoajan on toimittava yhteistyössä ja asetettava saataville tarvittavat tiedot sekä annettava kohtuullinen tekninen pääsy ja muu apu, jota vaaditaan velvoitteiden täyttämiseksi, ellei tämä ole täsmentänyt, että sen järjestelmää ei saa muuttaa suuririskiseksi järjestelmäksi

Vastuut suuririskisen tekoälyjärjestelmän arvoketjussa:

Järjestelmien alihankkijat

- Kolmas osapuoli, joka toimittaa suuririskisessä järjestelmässä käytettäviä tai siihen integroitavia tekoälyjärjestelmiä, välineitä, palveluja, komponentteja tai prosesseja, on sovittava suuririskisen järjestelmän tarjoajan kanssa kirjallisesti toimitettavista tiedoista ja avusta, jotta tarjoaja voi noudattaa asetuksen velvoitteita.
  - Ei koske maksuttomin, avoimin lisenssein tarjottuja välineitä, palveluita ja komponentteja, jotka ovat muita kuin yleiskäyttöisiä tekoälymalleja.

Komission tekoälytoimisto voi kehittää ja suositella vapaaehtoisia mallisopimusehtoja suuririskisten tekoälyjärjestelmien tarjoajien ja kolmansien osapuolten välillä

Suuririskisen järjestelmän käyttöönottajan velvollisuudet

- Käytettävä ja valvottava järjestelmää käyttöohjeiden mukaisesti.
- Annettava järjestelmän valvonta henkilöille, joilla on tarvittava pätevyys, koulutus ja valtuudet sekä tarvittava tuki.
- Varmistettava, että syöttötiedot ovat merkityksellisiä ja riittävän edustavia järjestelmän käyttötarkoituksen kannalta – siltä osin kuin käyttöönottaja hallitsee syöttödataa.
- Informoitava järjestelmän tarjoajaa ja valvontaviranomaista havaitsemistaan riskeistä.
- Säilytettävä järjestelmän automaattisesti tuottamat lokitiedot vähintään 6 kk ajan – siltä osin kuin ne ovat käyttöönottajan hallinnassa.
- Työnantajana informoitava työntekijöitä työpaikalla käyttöön otettavasta järjestelmästä.
- Informoitava luonnollisia henkilöitä, jotka ovat päätöksiä tekevän tai niissä avustavan suuririskisen järjestelmän kohteina.
- Julkisen sektorin käyttöönottajien on lisäksi rekisteröidyttävä EU:n tietokantaan

Julkisen sektorin käyttöönottajan velvollisuus:

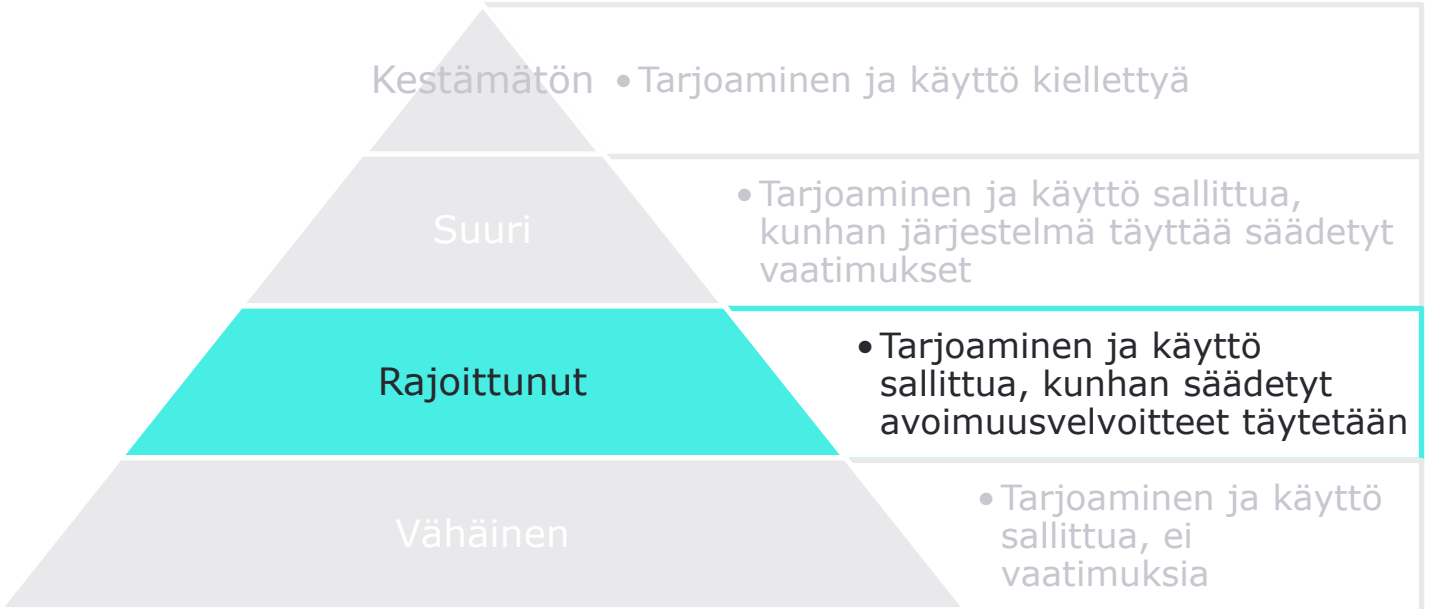
Perusoikeusvaikutusten arviointi

- Suuririskisen tekoälyjärjestelmän käyttöönottajan on suoritettava perusoikeusvaikutusten arviointi ennen järjestelmän käyttöönottoa.
  - Velvoite koskee julkisen sektorin elimiä sekä keskeisiä julkisia palveluita tuottavia yksityisiä yhteisöjä.

- Arvioinnin tulokset on ilmoitettava toimivaltaiselle viranomaiselle.

Voidaan suorittaa tietosuojavaikutusten arvioinnin yhteydessä

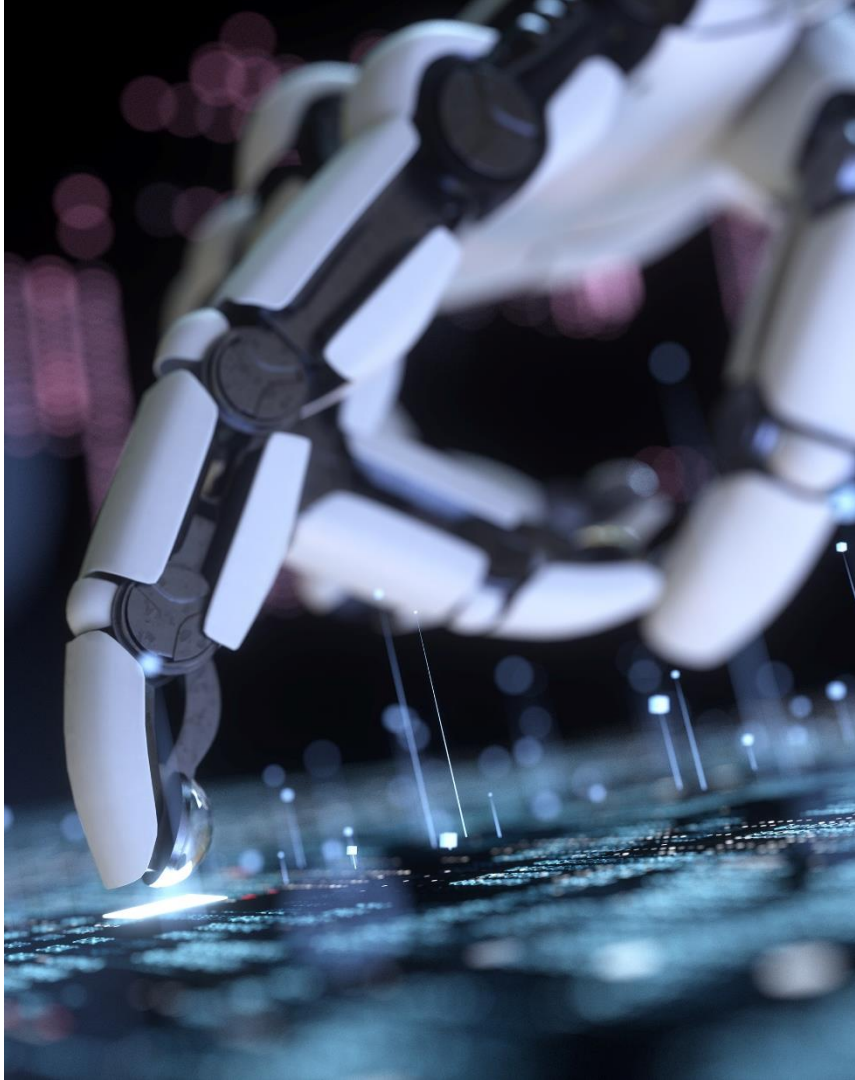
Rajoittuneen riskin käyttötapaukset ja avoimuusvelvoitteet



Systeemisen riskin mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

Ihmisen kanssa vuorovaikuttavat tekoälyjärjestelmät

- Tarjoajien on varmistettava, että tekoälyjärjestelmät, jotka on tarkoitettu vuorovaikuttamaan suoraan ihmisten kanssa, toteutetaan siten, että kyseisille henkilöille ilmoitetaan heidän asioivan tekoälyjärjestelmän kanssa.
  - Ei koske järjestelmiä, jotka on lailla valtuutettu rikoksentorjuntatarkoituksiin.



Generatiiviset tekoälyjärjestelmät:

Synteettisten tuotosten merkitseminen

- Synteettistä ääni-, kuva-, video- tai tekstisisältöä tuottavien tekoälyjärjestelmien tarjoajien on varmistettava, että järjestelmän tuotokset on merkitty koneellisesti luettavassa muodossa ja havaittavissa keinotekoisiksi tai manipuloiduiksi.
  - Käytettyjen tekniset ratkaisujen on oltava tehokkaita, yhteentoimivia, vakaita ja luotettavia siinä määrin kuin se on teknisesti mahdollista, ottaen huomioon monenlaisten sisältöjen erityispiirteet, toteutuskustannukset ja yleisesti tunnustettu uusin teknologia.
  - Ei koske järjestelmiä, jotka avustavat vakiomuokkaamista tai eivät olennaisesti muuta käyttöönottajan toimittamaa syöttödataa tai sen semantiikkaa.

Generatiiviset tekoälyjärjestelmät:

Syväväärennösten avoimuus

- Tekoälyjärjestelmän, joka tuottaa tai manipuloi syväväärennöksen muodostavaa kuva-, ääni- tai videosisältöä, käyttöönottajien on ilmoitettava, että sisältö on keinotekoisesti tuotettu tai että sitä on manipuloitu.
  - Jos syväväärennös on osa taiteellista, luovaa, satiirista tai fiktiivistä teosta, avoimuusvelvoite rajoittuu tällaisen sisällön paljastamiseen tavalla, joka ei haittaa teoksen esittämistä tai sen käyttöä.
  - Ei koske rikoksentorjuntatarkoituksiin tarkoitettua käyttöä.

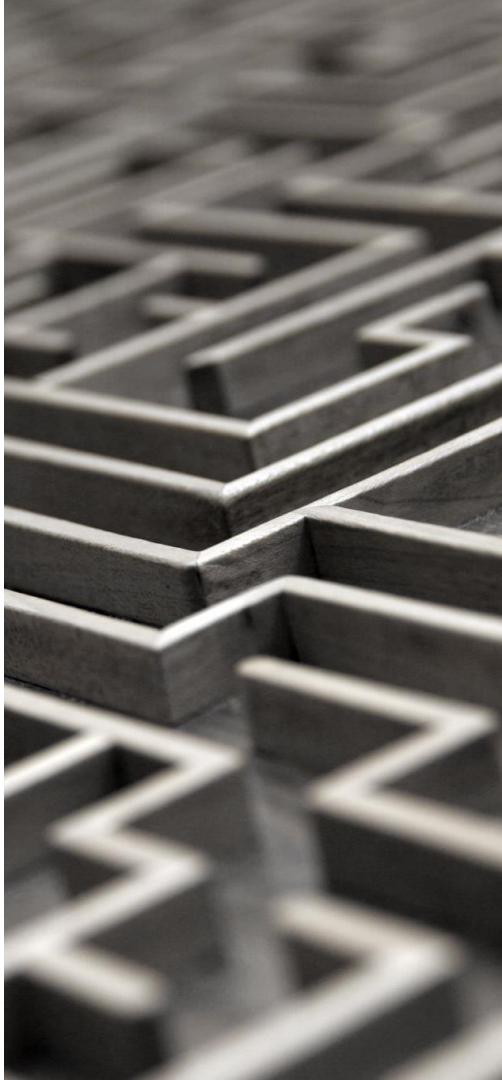
Generatiiviset tekoälyjärjestelmät:

Yleistä etua koskevan tekstin avoimuus

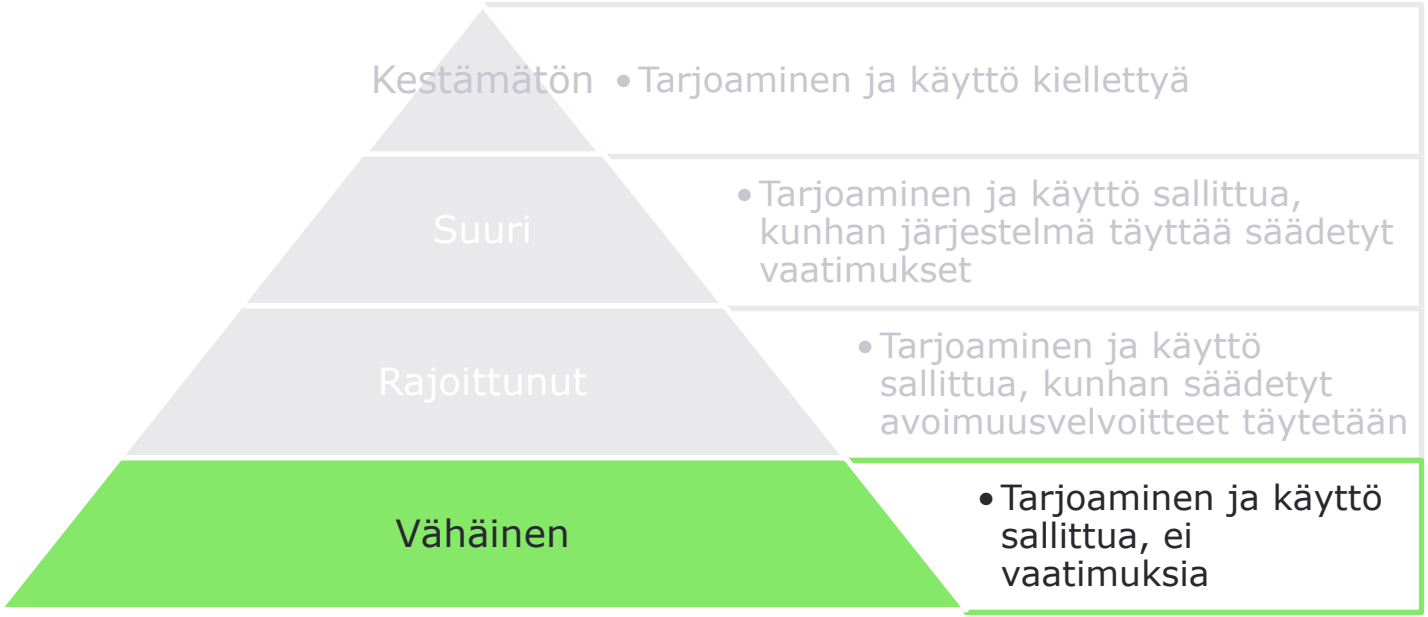
- Tekoälyjärjestelmän, joka tuottaa tai manipuloi tekstiä, jonka julkaisemisen tarkoituksena on tiedottaa yleisölle yleistä etua koskevista asioista, käyttöönottajien on ilmoitettava, että teksti on keinotekoisesti tuotettu tai sitä on manipuloitu.
  - Ei koske tilanteita, joissa järjestelmän tuottama sisältö on läpikäynyt ihmisen suorittaman arviointiprosessin tai toimituksellisen valvonnan ja jos luonnollisella henkilöllä tai oikeushenkilöllä on toimituksellinen vastuu sisällön julkaisemisesta.
  - Ei koske rikoksentorjuntatarkoituksiin tarkoitettua käyttöä.

Tunteentunnistusjärjestelmät ja biometriset luokitusjärjestelmät

- Tunteentunnistusjärjestelmän tai biometrisen luokitusjärjestelmän käyttöönottajien on ilmoitettava järjestelmän toiminnasta niille luonnollisille henkilöille, jotka altistuvat järjestelmälle.
  - Ei koske rikoksentorjuntatarkoituksiin tarkoitettua käyttöä.



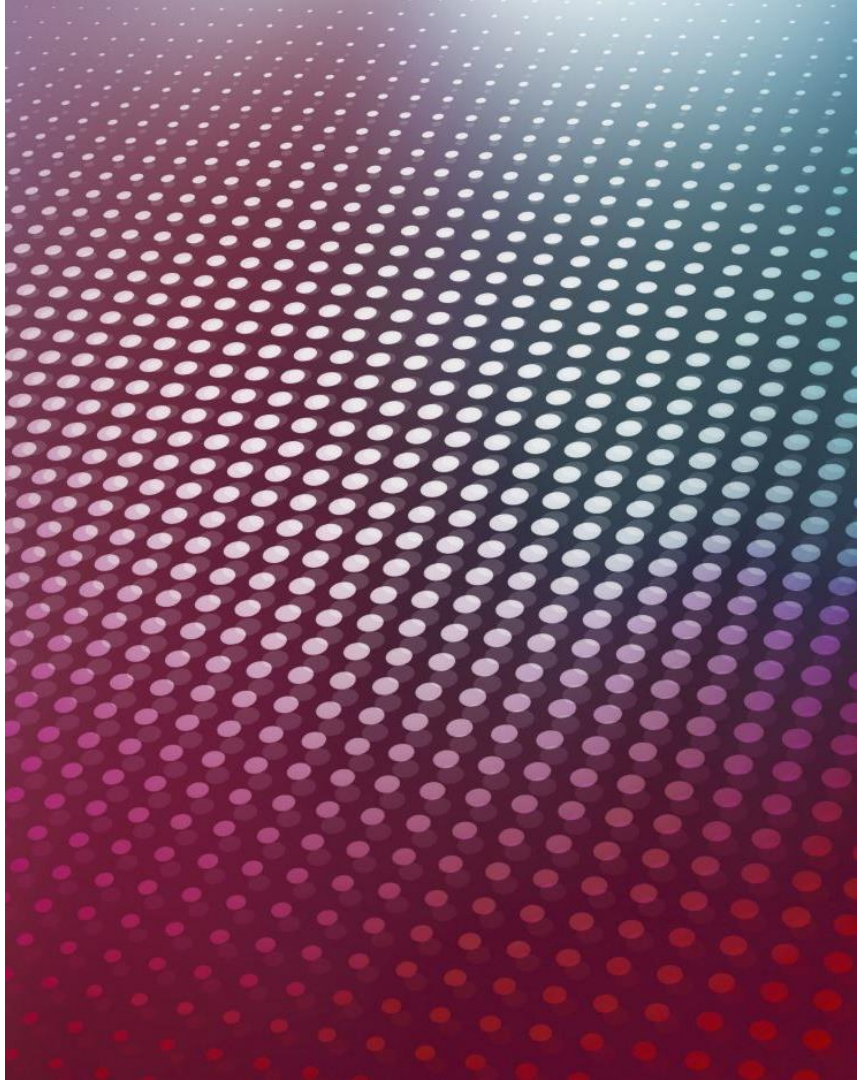
Vähäisen riskin käyttötapaukset ja vapaaehtoiset käytännesäännöt



Järjestelmäriskejä sisältävät mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

Vapaehtoiset käytännesäännöt

- Vähäisen riskin tekoälyjärjestelmien tarjoajat voivat varmistaa järjestelmänsä luotettavuuden kehittämällä omia vapaaehtoisia käytännesääntöjä tai noudattamalla muiden edustavien tahojen hyväksymiä käytännesääntöjä.



Yleiskäyttöisten tekoälymallien vaatimukset

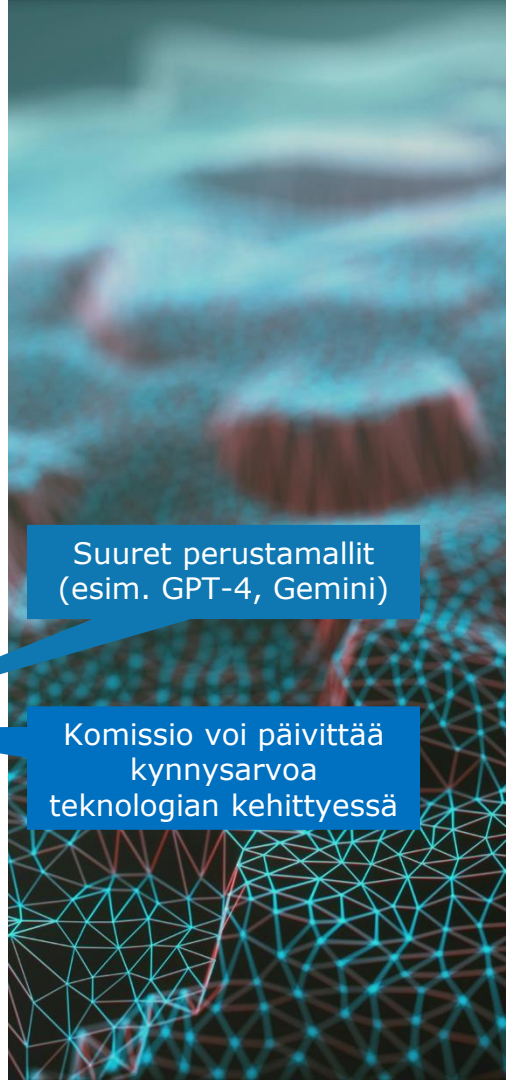
Systeemisen riskin mallit	• Lisävaatimukset
Kaikki yleiskäyttöiset mallit	• Avoimuus- ja informointivaatimukset

Yleiskäyttöiset tekoälymallit:

Kaksitasoinen riskiluokittelu

1. Kaikki yleiskäyttöiset tekoälymallit
   - Ks. määritelmä dialta 13.

2. Yleiskäyttöiset tekoälymallit, joihin liittyy systeeminen riski
   - Malli kuuluu tähän luokkaan,
     a) jos sen koulutuksessa on käytetty laskentatehoa vähintään 10^25 FLOPs
     b) TAI jos Euroopan komissio katsoo mallin muihin tekijöihin perustuen käsittävän systeemisiä riskejä (esim. parametrimäärä, käyttäjämäärä, autonomisuuden aste).



Kaikkia yleiskäyttöisiä malleja koskevat vaatimukset

- Dokumentaatio ja arviointi:
  - Laadittava ja pidettävä ajan tasalla mallin tekninen dokumentaatio, mukaan lukien sen koulutus- ja testausprosessi ja sen arvioinnin tulokset.
- Jatkotarjoajan informointi:
  - Laadittava, pidettävä ajan tasalla ja asetettava saataville tiedot ja dokumentaatio tekoälyjärjestelmien tarjoajille, jotka aikovat sisällyttää yleiskäyttöisen tekoälymallin tekoälyjärjestelmäänsä.
    - Tämän on annettava tekoälyjärjestelmien tarjoajille hyvä käsitys mallin ominaisuuksista ja rajoituksista, jotta nämä voivat noudattaa asetuksen velvoitteita.
- Tekijänoikeudet:
  - Otettava käyttöön toimintapolitiikka EU:n tekijänoikeusääntelyn noudattamiseksi.
  - Laadittava ja asetettava julkisesti saataville riittävän yksityiskohtainen tiivistelmä sisällöistä, joita on käytetty tekoälymallin koulutukseen.

Sovelletaan 8/2025 →

Vaatimukset täyttääkseen mallien tarjoajat voivat nojata alkuvaiheessa yleisiin käytännesääntöihin ja myöhemmin yhdenmukaistettuun standardiin

Immateriaalioikeuksia ja liikesalaisuuksia kunnioittaen ja suojaten

Avoimen lähdekoodin malleja, joihin ei liity systeemistä riskiä, koskevat vain tekijänoikeusvaatimukset

Systeemisen riskin mallien lisävaatimukset

- Mallin arviointi standardoitujen protokollien ja välineiden mukaisesti, mukaan lukien adversiaalisen testauksen suorittamisen ja tämän dokumentoinnin
- Systeemisten riskien arviointi ja lieventäminen
- Vakavien vaaratilanteiden seuranta, dokumentointi ja raportointi
- Riittävän kyberturvallisuuden varmistaminen mallille ja sen fyysiselle infrastruktuurille

Sovelletaan 8/2025 →

Vaatimukset täyttääkseen mallien tarjoajat voivat nojata alkuvaiheessa yleisiin käytännesääntöihin ja myöhemmin yhdenmukaistettuun standardiin

Lisävaatimukset koskevat myös avoimen lähdekoodin malleja, joihin liittyy systeeminen riski

Avoimen lähdekoodin yleiskäyttöiset tekoälymallit

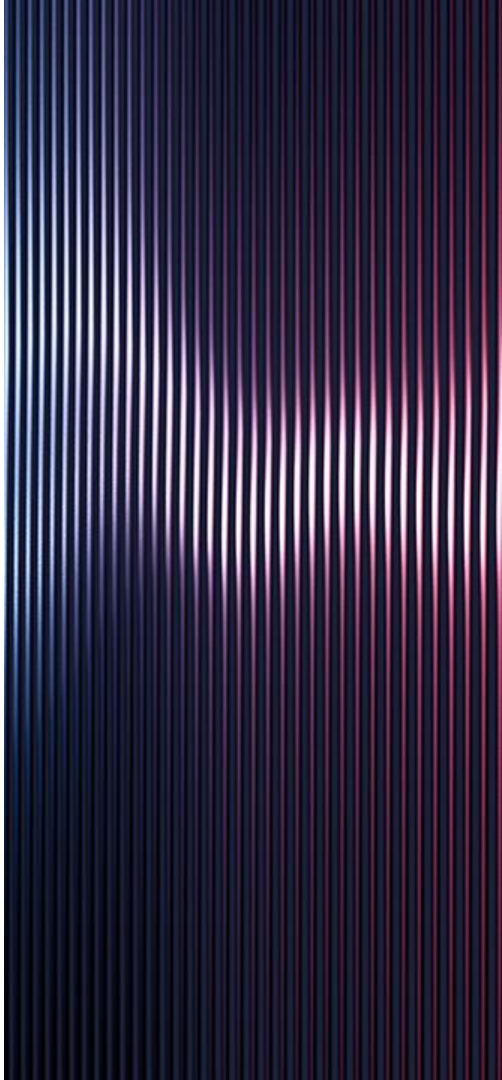
- Maksuttomalla ja avoimen lähdekoodin lisenssillä tarjotun yleiskäyttöisen tekoälymallin, jonka parametrit ja tiedot malliarkkitehtuurista ja käytöstä ovat julkisesti saatavilla, on noudatettava yleiskäyttöisten mallien tekijänoikeuksia koskevia vaatimuksia.

- Jos avoimen lähdekoodin malliin liittyy systeeminen riski, on sen noudatettava kaikkia vaatimuksia.

Yleiskäyttöisen tekoälymallin muokkaaminen

- Jos yleiskäyttöistä tekoälymallia muutetaan tai hienosäädetään muun kuin alkuperäisen tarjoajan toimesta, tulee tästä toimijasta mallin tarjoaja, johon sovelletaan mallin tarjoajan velvoitteita.

- Tässä tapauksessa velvoitteet rajautuvat kyseiseen muutokseen tai hienosäätöön esimerkiksi täydentämällä jo olemassa olevia teknisiä asiakirjoja muutoksia koskevilla tiedoilla, mukaan lukien koulutukseen käytetyt uudet tietolähteet.



Innovointia tukevat toimet

Tekoälyn sääntelyn testiympäristöt

- Jäsenmaan toimivaltaisen viranomaisen on perustettava yksin tai muiden jäsenmaiden kanssa vähintään yksi riittävästi resursoitu kansallisen tason tekoälyn sääntelyn testiympäristö.

- Testiympäristö tarjoaa tekoälyjärjestelmien tarjoajille mahdollisuuden kehittää, kouluttaa, testata ja validoida innovatiivisia tekoälyjärjestelmiä ennen niiden markkinoille saattamista tai käyttöönottoa.
  - Testiympäristössä toimiminen on mahdollista rajatun ajan ja toimivaltaisten viranomaisten kanssa sovitun suunnitelman mukaisesti.
  - Viranomaisten on tarjottava ohjeistusta ja tukea asetuksen vaatimuksista ja velvoitteista ja niiden täyttämisestä.

”Sääntelyhiekkalaatikon” oltava toiminnassa viimeistään 8/2026

Maksutonta pk-yrityksille ja startupeille – poikkeuksellisia kustannuksia voidaan periä

Testiympäristöön osallistuvat tarjoajat eivät joudu hallinnollisten sakkojen kohteeksi asetuksen rikkomisesta, mutta ovat vastuussa kolmansille osapuolille aiheutuneista vahingoista

Testiympäristö ja asetuksen vaatimusten täyttäminen

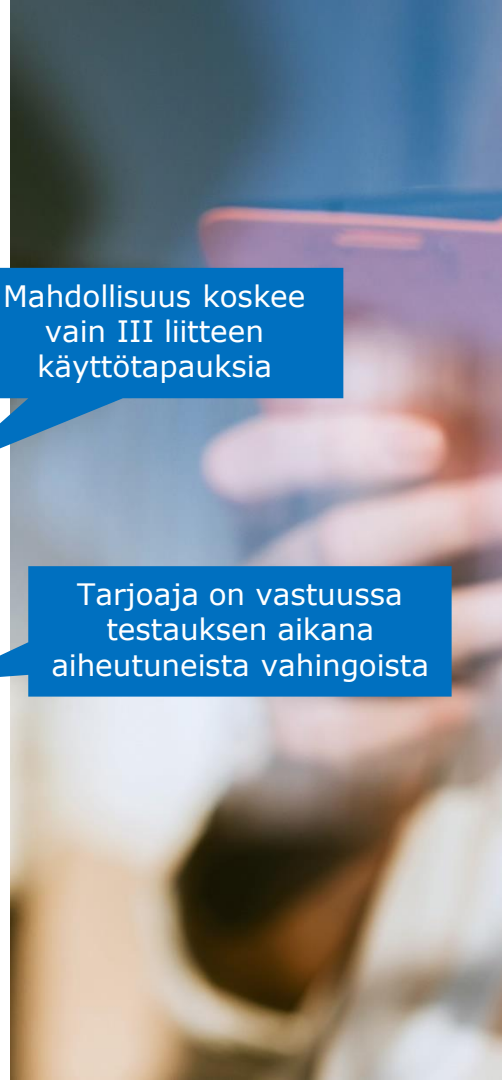
- Toimivaltaisen viranomaisen on esitettävä tekoälyjärjestelmän tarjoajan pyynnöstä kirjallinen todiste testiympäristössä onnistuneesti suoritetuista toimista.

- Toimivaltaisen viranomaisen on myös annettava loppuraportti, jossa eritellään testiympäristössä suoritetut toimet sekä niihin liittyvät tulokset ja oppimistulokset.

- Tarjoajat voivat käyttää näitä asiakirjoja osoittaakseen, että he noudattavat asetusta.
  - Valvontaviranomaisten ja ilmoitettujen arviointilaitosten on otettava myönteisesti huomioon nämä asiakirjat vaatimustenmukaisuuden arviointimenettelyjen nopeuttamiseksi.

Suuririskien tekoälyjärjestelmän testaaminen todellisissa olosuhteissa

- Suuririskisen tekoälyjärjestelmän tarjoaja voi suorittaa järjestelmän testauksen todellisissa olosuhteissa tekoälyn sääntelyn testiympäristön ulkopuolella enintään 12 kk ajan.
  - Tarjoajan on noudatettava tästä asetuksessa säädettyjä määräyksiä, mukaan lukien niiden mukaisesti laadittavaa, markkinavalvontaviranomaisen hyväksymää testaussuunnitelmaa.
  - Testaukseen osallistuvilta henkilöiltä on saatava tietoinen suostumus.



Muita innovointia tukevia toimia

- Jäsenmaat:
  - Järjestettävä asetuksen soveltamista koskevia tiedotus- ja koulutustoimia, jotka on räätälöity pk-yritysten, startupien, käyttöönottajien ja tarvittaessa paikallisten viranomaisten tarpeisiin.
  - Tarjottava pk-yrityksille, startupeille ja viranomaisille ohjeistusta ja vastattava näiden tiedusteluihin liittyen säädöksen toimeenpanoon.
  - Helpotettava pk-yritysten, startupien ja muiden sidosryhmien osallistumista standardointityöhön.
- Komission tekoälytoimisto:
  - Kehitettävä standardoituja malleja asetuksen soveltamisalaan kuuluville aloille.
  - Kehitettävä ja ylläpidettävä alustaa, joka tarjoaa helppokäyttöistä asetukseen liittyvää tietoa.
  - Järjestettävä tiedotuskampanjoita.

Hallinnointi ja seuraamukset

Hallinnointi:

Jäsenmaataso

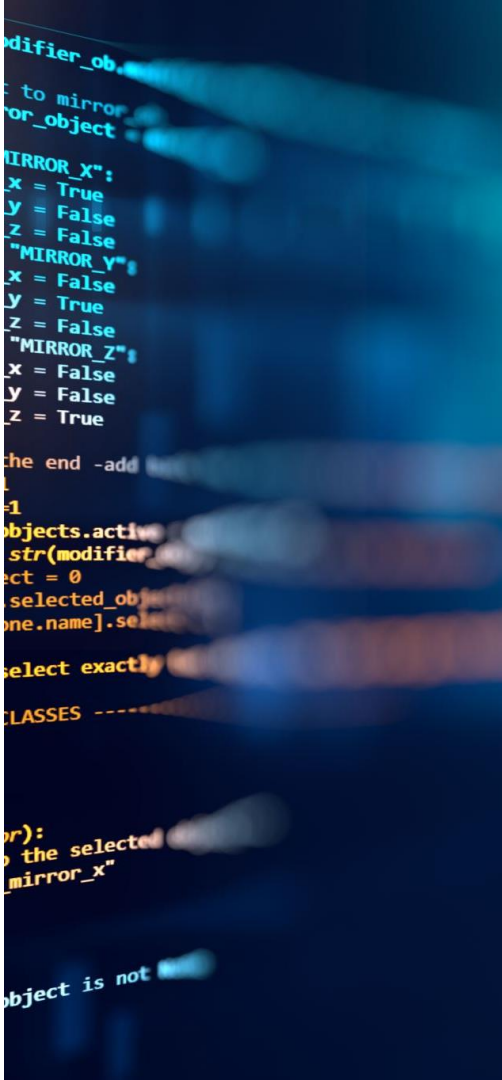
- Jäsenvaltion on perustettava tai nimettävä vähintään yksi ilmoittamisesta vastaava viranomainen ja vähintään yksi markkinavalvontaviranomainen kansallisiksi toimivaltaisiksi viranomaisiksi.

Hallinnointi:

EU-taso

- Euroopan tekoälyneuvosto:
  - Edustettuina jäsenmaat, komissio ja Euroopan tietosuojavaltuutettu.
  - Neuvoo ja avustaa komissiota ja jäsenvaltioita ja edistää näin asetuksen johdonmukaista ja vaikuttavaa soveltamista.
  - Teknistä asiantuntemusta lautakunnalle tarjoaa neuvoa-antava foorumi, joka edustaa toimialaa, startup- ja pk-yrityksiä, kansalaisyhteiskuntaa ja tiedeyhteisöä.

- Euroopan tekoälytoimisto:
  - Perustetaan komission yhteyteen.
  - Luokittelee ja valvoo yleiskäyttöisiä tekoälymalleja ja tekee yhteistyötä tekoälyneuvoston kanssa.
  - Toimistoa neuvoo ja tukee riippumattomista asiantuntijoista koostuva tiedelautakunta.



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 tuoteturvasääntelyyn (liite I) ja muuhun sääntelyyn
- Tekoälyjärjestelmän määritelmän soveltaminen

Seuraamukset

- Kiellettyjen käytäntöjen rikkominen:
  - Enintään 35 miljoona euroa tai 7 prosenttia edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta.

- Suuririskisten tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien säännösten sekä asetuksen muiden velvoitteiden rikkominen:
  - Enintään 15 miljoonaa euroa tai 3 prosenttia liikevaihdosta.

- Virheellisen, puutteellisen tai harhaanjohtavan tiedon toimittaminen arviointilaitokselle tai toimivaltaiselle viranomaiselle:
  - Enintään 7,5 miljoonaa euroa tai 1,5 prosenttia liikevaihdosta.

Jokaisessa rikkomusluokassa enimmäiskynnys on kahdesta summasta pienempi pk-yritysten osalta ja korkeampi muiden yritysten osalta

Soveltamisaikataulu

Aikataulu

Tekoälysopimus (AI Pact), jolla yritykset voivat vapaaehtoisesti sitoutua asetuksen vaatimuksiin etupainotteisesti

Ennen tätä markkinoille saatettujen yleiskäyttöisten mallien on täytettävä vaatimukset elokuussa 2027

Asetus astuu voimaan ja siirtymäaika käynnistyy **elokuu 2024**

helmikuu 2025
Kielletyt käyttötapaukset

Yleiskäyttöisten tekoälymallien vaatimukset **elokuu 2025**

elokuu 2026
Suuren riskin vaatimukset: listatut käyttötapaukset (liite III)
+
Rajoittuneen riskin avoimuusvaatimukset

Suuren riskin vaatimukset: EU:n yhdenmukaistettujen tuoteturvasäädösten käyttötapaukset (liite I) **elokuu 2027**

Standardointityö

Ennen tätä viranomaisten käyttöön ottamien suuririskisten järjestelmien on täytettävä vaatimukset elokuussa 2030