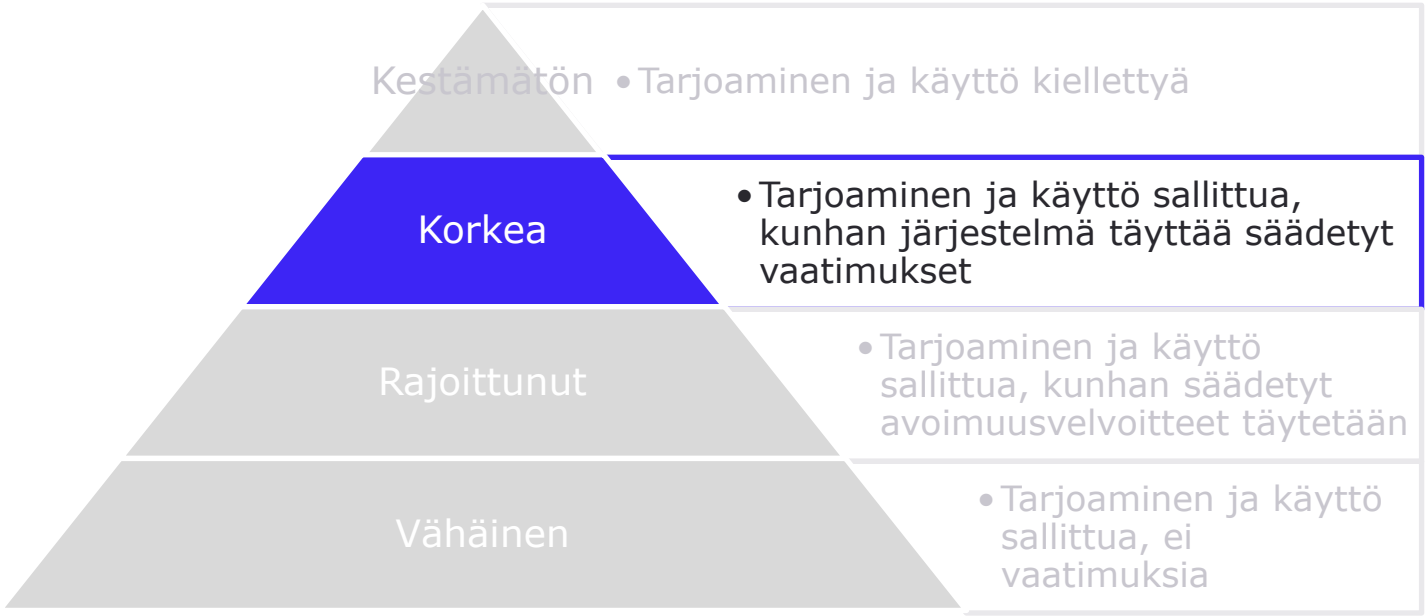
EU:n tekoälyasetus, osa II: korkean ja rajoittuneen riskin luokat tekoälyjärjestelmille

Joonas Mikkilä, johtava asiantuntija, Teknologiateollisuus ry

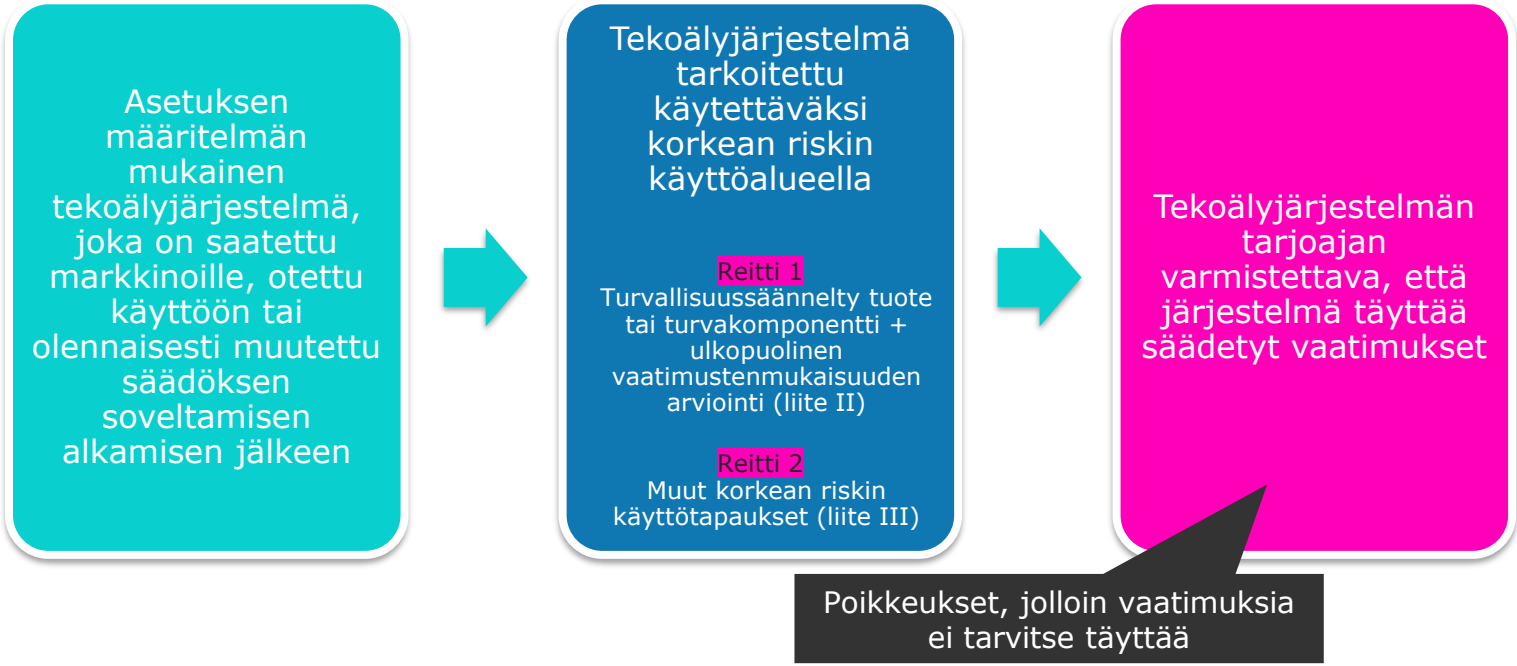
8.3.2024

Korkean riskin käyttötapaukset ja vaatimukset



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

Kaksi reittiä korkean riskin vaatimusten piiriin



Reitti 1

Sovelletaan 36 kk asetuksen voimaan astumisesta

Korkean riskin käyttötapaukset:

Turvallisuussäännellyt tuotteet ja turvakomponentit

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

- 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.

Reitti 1

Tuoteturvasääntelyn kautta tekoälyasetuksen piiriin tulevia tuoteryhmiä

- Koneet
- Hissit
- Lääkinnälliset laitteet
- Radiolaitteet
- Painelaitteet
- Veneet ja vesiskootterit
- Henkilösuojaimet
- Kaasumaisia polttoaineita polttavat laitteet
- Lelut
- Siviililentokoneet
- Kaksi-, kolmi- ja nelipyöräiset ajoneuvot
- Maa- ja metsätalousajoneuvot
- Laivavarusteet
- Moottoriajoneuvot ja niiden perävaunut

Turvallisuus-säädökset luetellaan asetuksen liitteessä II

Reitti 2

Muut korkean riskin käyttötapaukset 1/3

Sovelletaan 24 kk asetuksen voimaan astumisesta

Luetellaan asetuksen liitteessä III, jota komissio voi muokata tai täydentää

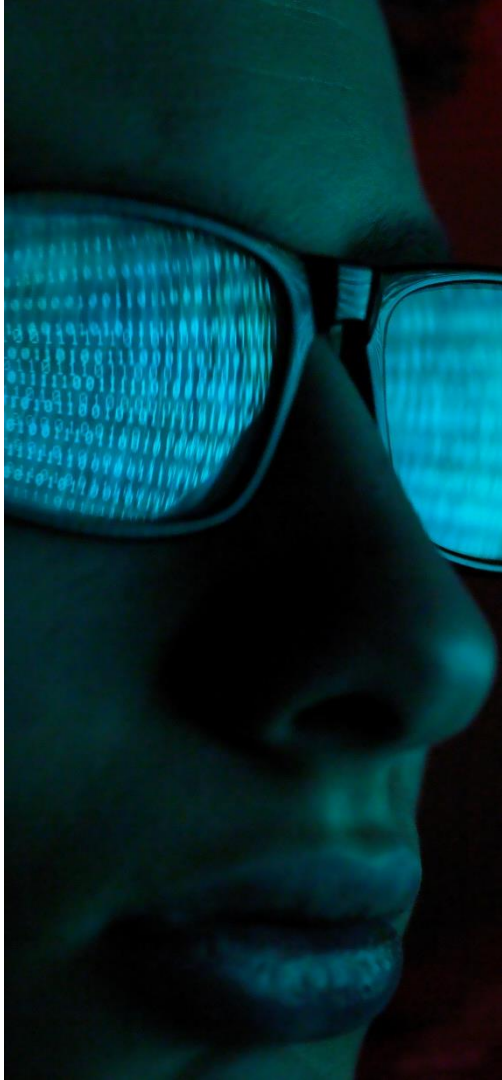
- Biometrinen etätunnistaminen ja luokittelu sekä tunteiden tunnistaminen
  - Kiellettyjen käyttötarkoitusten ulkopuolelle jäävät tapaukset
  - Ei koske yksinomaan henkilöllisyyden todentamiseen ja laitteiden avaamiseen tarkoitettuja järjestelmiä
- Kriittinen infrastruktuuri
  - Tieliikenteen ja kriittisen digitaalisen infrastruktuurin hallinnoinnin sekä veden, kaasun, lämmön ja sähkön jakelun turvakomponentit
  - Ei koske kyberturvakomponentteja
- Koulutus ja ammatillinen koulutus
  - Oppilas- ja opiskelijavalinnat
  - Oppimisen arviointi ja ohjaaminen, tarjottavan koulutuksen tason arviointi
  - Koetilanteissa kielletyn käytöksen seuranta ja havaitseminen

Reitti 2

Muut korkean riskin käyttötapaukset 2/3

- Työllisyys, työntekijöiden hallinta ja pääsy itsenäiseen ammatinharjoittamiseen
  - Rekrytoiminen ja työntekijävalinta
  - Työpaikkailmoitusten kohdentaminen
  - Työhakemusten suodattaminen ja analysointi ja hakijoiden arviointi
  - Työehtoihin ja työsuhteen päättämiseen ja ylennyksiin liittyvät päätökset
  - Työtehtävien jakaminen ja suorituksen ja käytöksen seuranta ja arviointi

- Pääsy välttämättömiin yksityisiin palveluihin ja olennaisiin julkisiin palveluihin ja etuihin
  - Ihmisen kelpoisuuden arvioiminen liittyen välttämättömiin etuisuuksiin ja palveluihin sekä näiden myöntäminen tai epääminen
  - Ihmisen luottoluokituksen arviointi, pois lukien talouspetosten havaitseminen
  - Hätäpuheluiden arviointi ja luokittelu
  - Henki- ja sairausvakuutuksen riskien arviointi ja hinnoittelu



Reitti 2

Muut korkean riskin käyttötapaukset 3/3

- Lainvalvonta
  - Rikosuhririskin, rikosriskin tai rikoksen uusimisen riskin arviointi
  - Valheenpaljastus
  - Todistusaineiston luotettavuuden arviointi
  - Rikoksen tutkintaan tai syyttämiseen liittyvä profilointi
- Maahanmuutto-, turvapaikka- ja rajavalvonnan hallinta
  - 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 korkean riskin luokituksesta

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

1. Suorittaa kapea menettelytehtävä
   - Esim. strukturoimattoman datan strukturoiminen

Poikkeusmahdollisuus koskee vain liitteen III käyttötapauksia

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

3. Havaita päätöksentekomallit tai poikkeamat aiemmista päätöksentekomalleista
   - Esim. opettajan tekemän oppilasarvioinnin poikkeamien tai epäjohdonmukaisuuksien merkitseminen

4. Suorittaa valmisteleva tehtävä arviointiin, joka on olennainen korkean riskin käyttötapausten kannalta
   - Esim. tiedostojen käsitteleminen

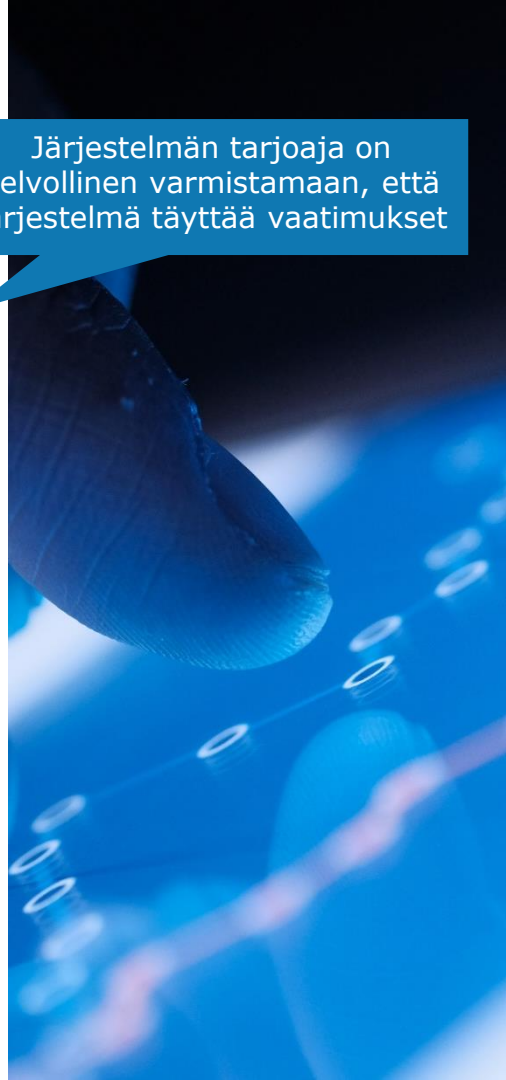
Poikkeukset eivät päde ihmisten profilointiin tarkoitettuihin järjestelmiin

Korkean riskin tekoälyjärjestelmien vaatimukset

- Riskienhallintajärjestelmä
- Data ja datan hallinnointi
- Tekninen dokumentaatio
- Arkistointi
- Avoimuus ja käyttäjien informointi
- Ihmisen suorittama valvonta
- Tarkkuus, toimintavarmuus ja kyberturvallisuus

Järjestelmän tarjoaja on velvollinen varmistamaan, että järjestelmä täyttää vaatimukset

Vaatimusten täyttämisen tueksi on tarkoitus tuottaa harmonisoituja standardeja



Korkean riskin järjestelmän tarjoajan muut velvollisuudet

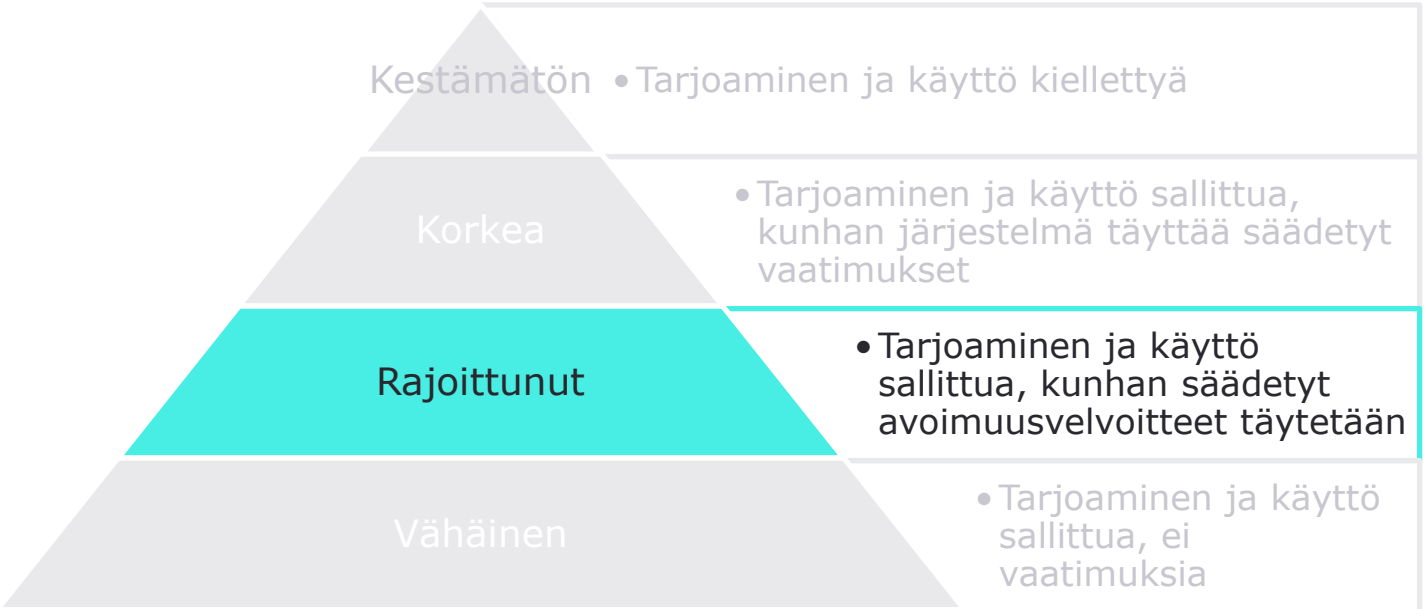
- Laatujärjestelmä
- Markkinoille saattamisen jälkeinen seurantajärjestelmä ja -suunnitelma
- Asiakirjojen säilyttäminen (10 vuotta)
- Automaattisesti luotujen lokien säilyttäminen (6 kk)
- Vakavien vaaratilanteiden ilmoittaminen markkinavalvontaviranomaisille
- Korjaavat toimet ja tiedonantovelvollisuus
- Yhteistyö toimivaltaisten viranomaisten kanssa
- Valtuutetun EU-edustajan nimeäminen, ellei tarjoaja ole sijoittunut EU:hun

Korkean riskin järjestelmän käyttöönottajan velvollisuudet

- Käytettävä ja valvottava järjestelmää käyttöohjeiden mukaisesti.
- Osoitettava järjestelmän valvonta henkilöille, joilla on tarvittava pätevyys, koulutus ja valtuudet sekä tarvittava tuki.
- Varmistettava, että syöttötiedot ovat merkityksellisiä ja riittävän edustavia järjestelmän käyttötarkoituksen kannalta – siinä määrin kuin käyttöönottaja hallitsee syöttödataa.
- Informoitava järjestelmän tarjoajaa ja valvontaviranomaista havaitsemistaan riskeistä.
- Säilytettävä järjestelmän automaattisesti luomat lokit vähintään 6 kk ajan – siltä osin kuin ne ovat käyttöönottajan hallinnassa.
- Informoitava työntekijöitä työpaikalla käyttöön otettavasta järjestelmästä.
- Informoitava luonnollisia henkilöitä, jotka ovat korkeariskisen päätöksiä tekevän tai niissä avustavan järjestelmän kohteina.

Julkisen sektorin käyttöönottajien on lisäksi rekisteröidyttävä EU:n tietokantaan

Rajoittuneen riskin käyttötapaukset ja avoimuusvelvoitteet



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

Avoimuusvelvoitteet koskevat

1. Ihmisen kanssa vuorovaikuttavia tekoälyjärjestelmiä
2. Synteettisiä tuotoksia generoivia järjestelmiä
3. Deep fake -väärennösten generointia
4. Yleistä etua koskevan tekstin generointia
5. Tunteidentunnistusjärjestelmiä ja biometrisiä luokittelujärjestelmiä

Rangaistukset

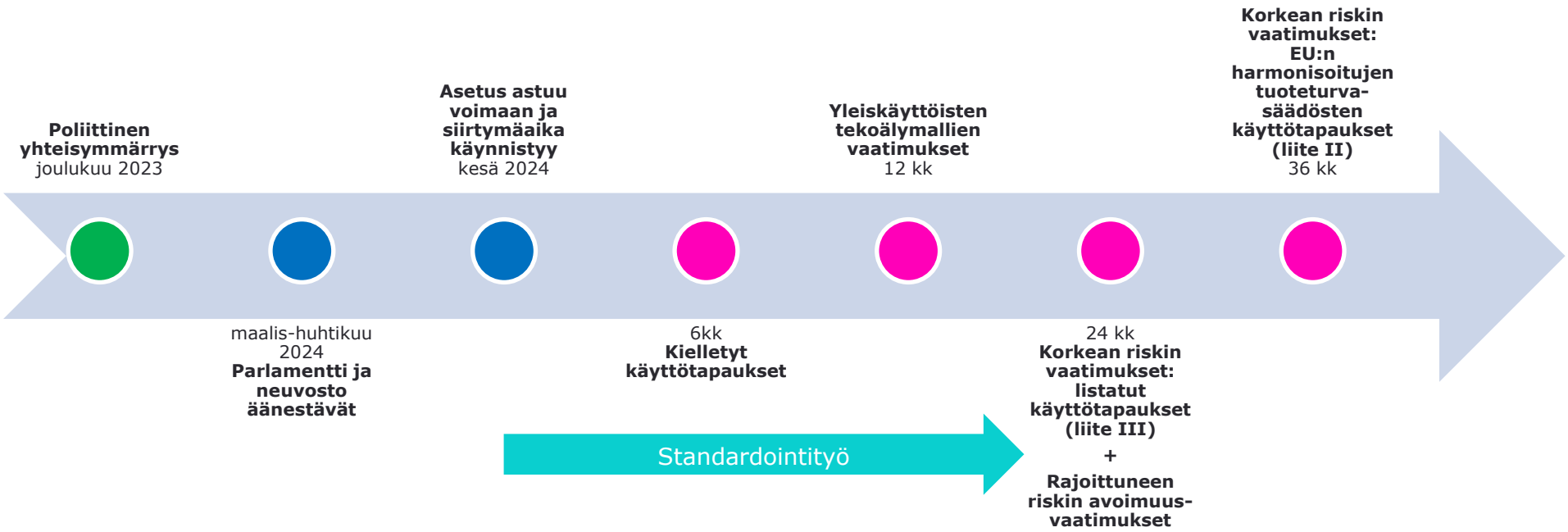
Rangaistukset

- Kiellettyjen käyttötapausten rikkominen:
  - Enintään 35 miljoona euroa tai 7 prosenttia edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta.
- Yleiskäyttöisten tekoälymallien sääntöjen ja asetuksen muiden vaatimusten tai velvoitteiden rikkominen:
  - Enintään 15 miljoonaa euroa tai 3 prosenttia liikevaihdosta.
- Epätäydellisen tai harhaanjohtavan tiedon toimittaminen:
  - 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


Poliittinen yhteisymmärrys
joulukuu 2023
maalis-huhtikuu 2024
Parlamentti ja neuvosto äänestävät
Asetus astuu voimaan ja siirtymäaika käynnistyy
kesä 2024
6kk
Kielletyt käyttötapaukset
Standardointityö
Yleiskäyttöisten tekoälymallien vaatimukset
12 kk
24 kk
Korkean riskin vaatimukset: listatut käyttötapaukset (liite III)
+
Rajoittuneen riskin avoimuus-vaatimukset
Korkean riskin vaatimukset: EU:n harmonisoitujen tuoteturva-säädösten käyttötapaukset (liite II)
36 kk

Kiitos!

joonas.mikkila@teknologiateollisuus.fi

+358 45 129 6791

@joonasmikkila