AI Act ja MDR ne yhteen soppii, huomenna pannaan pussauskoppiin

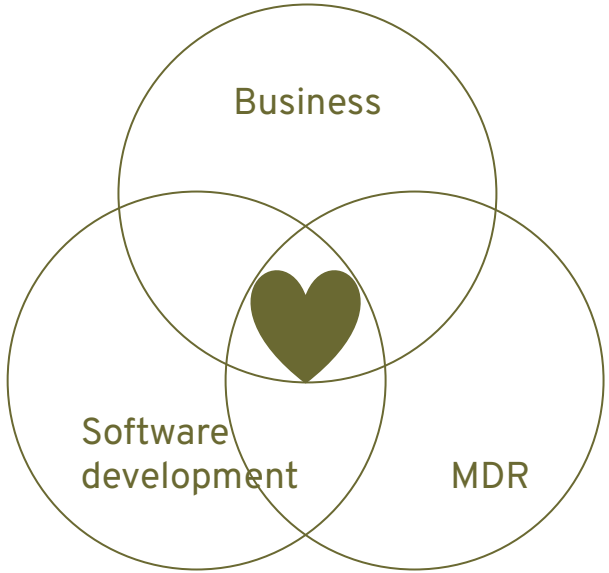
Business Tampere / Regulaatiowebinaari 13.12.2024

Kirsi Korhonen, Korsi Key Oy

Kuka puhuu?

Kirsi Korhonen - Yrittäjä, konsultti - Korsi Key Oy

- Ohjelmistot lääkinnällisinä laitteina
- SaMD-regulaatio
- Määrittelyt
- Projektinvetovastuut
- Prosessikehitys



kirsi.korhonen@korsikey.fi
+358 44 5466066
www.korsikey.fi
https://www.linkedin.com/in/kirsihkorhonen/

Hukummeko sääntelyyn?

MDR on ollut jo iso juttu, vyöryykö päälle vielä lisää vaatimuksia, työtä, kustannuksia?

Estääkö sääntely hienot ideat ja liiketoiminnan käytännössä?

Miten AI Actissa on huomioitu MDR ja lääkinnälliset laitteet, sopivatko ne yhteen ollenkaan?

Kuvan ideoinnissa ja luomisessa käytetty apuna ChatGPT 4o + DALL-E

Puhalletaan ensikellukkeet

- Tekoälyjärjestelmien luokittelu
- Millaisia vaatimuksia AI Act tuo suuririskisille tekoälyjärjestelmille?
- Mitä yhteistä ja mitä eroja löytyy MDR:stä ja AI Actista?
- Mitä ei vielä tiedetä?

Kuvan ideoinnissa ja luomisessa käytetty apuna ChatGPT 4o + DALL-E

Järjestelmien luokittelu

AI Act -riski	Mitä sisältää?	Vaatimukset	MDR
Ei-hyväksyttävä II luku 5 artikla	Mm. sosiaalinen pisteytys, kohdentamaton kasvojentunnistus, tunteentunnistus työ+oppilaitokset…	Käyttötapaukset kielletty (tietyin poikkeuksin)	
Suuririskinen	Tuote tai turvakomponentti tuotteessa, johon sovelletaan tiettyä lainsäädäntöä (mm. MDR, ks. AI Actin liite I) + Listatut soveltamisalat liite III	Erityisvaatimukset III luku	Luokat IIa, IIb, III Luokassa I eräs auditointipoikkeus
Muut	Muut, erityisesti luonnollisten henkilöiden kanssa suoraan vuorovaikutukseen tarkoitetut tekoälyjärjestelmät	Avoimuus (IV luku) Seuranta (IX luku)	

Järjestelmien luokittelu

- Erillinen ulottuvuus: yleiskäyttöiset tekoälyjärjestelmät
- MDR:n mukaisilla lääkinnällisillä laitteilla kuitenkin aina tietty käyttötarkoitus
- 25 artikla ei-suuririskisen järjestelmän muuttamisesta suuririskiseksi käyttötarkoitusta muuttamalla, eli esim. yleiskäyttöisen järjestelmän käyttö tiettyyn lääketieteelliseen tarkoitukseen
    - Alkuperäistä tarjoajaa ei pidetä uuden järjestelmän tarjoajana MUTTA
    - Velvollisuus antaa tarvittavat tiedot ja apu vaatimusten täyttämiseksi
    - PAITSI jos alkuperäinen tarjoaja täsmentänyt, että ei saa muuttaa tällä tavalla
    - **Uusimmat yleiskäyttöiset mallit eivät tule EU-markkinoille tai tulevat rajatuin käyttöehdoin?**

Suuririskisen järjestelmän dokumentaatio

Vaatimustenmukaisuus on dokumentoitava - MDR:ssä vastaava dokumentointi

AI Actin tavoite: Vaadittu **dokumentaatio yhdistetään muun sääntelyn mukaiseen dokumentaatioon** (mm. 8 ja 11 artiklat), myös yksi yhteinen vaatimustenmukaisuusvakuutus (47 artikla)

➜ **Ei pitäisi tarvita kahta erillistä dokumentaatiota MDR:ää ja AI Actia varten**

Miten hyvin toteutuu käytännössä?

AI Actin vaatiman dokumentaation sisältö kuvattu liitteessä IV

Suuririskisen järjestelmän vaatimukset 1/6

Riskienhallintajärjestelmä (9 artikla)

- Iteratiivisuus ja seuranta
- Riskit: terveys, *turvallisuus*, *perusoikeudet*
- Kohtuudella ennakoitavissa oleva väärinkäyttö huomioitava
- Poistaminen ja lieventäminen, 3 porrasta joista viimeinen informointi
- *Testaus* riskienhallintatoimenpiteiden määrittämiseksi (ennalta määritellyt mittarit ja todennäköisyyksien kynnykset)
- Jäännösriskin hyväksyttävyys

Mitäpä näistä MDR ei jo edellyttäisi?

Suuririskisen järjestelmän vaatimukset 2/6

Data ja sen hallinta (10 artikla)

- Tarvitaan erilliset koulutus-, validointi- ja testausdatajoukot - vaatimuksina mm. edustavuus, virheettömyys, täydellisyys
- Suunnitteluvalinnat, keräysprosessit, alkuperä, käsittely dokumentoitava
- Arvioitava mm. datan soveltuvuus, vinoumat, puutteet
- Erityiset henkilötietoryhmät vain suojatoimin (esim. terveystiedot) EU:n tietosuojasääntelyn mukaisesti

MDR:ssä vaatimuksia lähinnä kliinisille tutkimuksille ja datalle

Suuririskisen järjestelmän vaatimukset 3/6

Tietojen säilyttäminen

- Lokitusvaatimuksia: mitä vähintään kirjattava ja miten käsiteltävä (12 artikla)
- Tarjoajalle ja käyttöönottajalle vaatimus säilyttää lokitiedot sen mukaan kenen hallussa ne ovat (mm. artiklat 12, 19 ja 26)
    - Säilytettävä käyttötarkoitukseen nähden asianmukaisen ajanjakson ajan, kuitenkin vähintään 6 kuukautta, ellei muu lainsäädäntö vaadi toisin
- Dokumentaatio säilytettävä 10 vuotta markkinoille saattamisesta tai käyttöönotosta (18 artikla)

MDR ei määrittele lokeihin liittyen mitään, dokumentaation säilytysvelvollisuus sama kuin MDR:ssä (MDR 10 artikla)

Suuririskisen järjestelmän vaatimukset 4/6

Avoimuus ja tietojen antaminen (13 artikla)

- Käyttöönottajien suuntaan, jotta voivat tulkita ja käyttää asianmukaisesti
- Käyttöohjeet vaaditaan, **digitaalisessa** tai muussa muodossa
  - Varsin laajat taustatiedot ja tiedot tarvittavista resursseista, huoltotoimenpiteistä jne.
- Lisäksi yleiset avoimuusvaatimukset IV luku 50 artikla, mm.
  - Kun järjestelmä on tarkoitettu olemaan suoraan ihmisen kanssa vuorovaikutuksessa, ihmisen tiedettävä olevansa vuorovaikutuksessa tekoälyjärjestelmän kanssa
  - Synteettistä sisältöä tuottavien järjestelmien tuotokset merkittävä koneellisesti luettavasti niin, että ne voidaan tunnistaa tekoälyn tuottamiksi

MDR:n suhtautuminen sähköisiin käyttöohjeisiin epäluuloisempi, ja paperisetkin pitäisi olla saatavilla - ohjelmistolla saa kuitenkin sellaiset toimittaa

Suuririskisen järjestelmän vaatimukset 5/6

Ihmisen suorittama valvonta (14 artikla)

- Luonnollisten henkilöiden pitää pystyä valvomaan toimintaa
- Tarkoitus ehkäistä ja minimoida riskit
- Järjestelmän keinoin, tarjoajan tai käyttöönottajan tekemänä
- Valvojan pitää pystyä ymmärtämään toimintaa riittävästi
- Pidettävä yllä tietoisuutta automaatiovinoumasta eli inhimillisestä taipumuksesta luottaa liiallisesti järjestelmän tuloksiin!
    - Myös milloin ei pidä käyttää tai milloin korjata tai peruuttaa tuotokset

MDR vaatii markkinoille saattamisen jälkeistä valvontaa (kuten myös AI Act) sekä asettaa ylläpitovaatimuksia, mutta ei suoraan vastaavaa ihmisvalvontaa

Suuririskisen järjestelmän vaatimukset 6/6

Tarkkuus, vakaus ja kyberturvallisuus (15 artikla)

- Tarkkuudelle oltava mittareita
- Edellytyksenä vika- ja virhesietoisuus erityisesti jos luonnollisia henkilöitä vuorovaikutuksessa järjestelmän kanssa
- Oppivien järjestelmien vinoutumisen ehkäisy ja havaitseminen
- Järjestelmän on kestettävä ulkopuolisia hyökkäyksiä, ja teknisin toimin täytyy ehkäistä, havaita ja rajoittaa niitä
    - Myös koulutusdatajoukkoa, koulutusta edeltäviä komponentteja, syöttötietoja jne. vastaan (mm. data- ja mallimyrkytys)

Myös MDR:stä löytyy tietoturvavaatimuksia, mutta ei yhtä kootusti - aihe noususSa mm. standardoinnin kautta

Tarjoajan velvollisuudet

Paljon pieniä yksityiskohtia! Pääosin kuitenkin tuttuja MDR:stä.

- **Laadunhallintajärjestelmä** (17 artikla), keskeisiä kohtia esimerkiksi
  - Strategia säännösten noudattamista varten!
  - Periaatteet, menettelyt, ohjeet mm. suunnitteluun, kehitykseen, testaukseen, validointiin
  - *Datanhallintajärjestelmä*
  - Markkinoille saattamisen jälkeisen seurannan järjestelmä
  - **Osaksi alakohtaista laadunhallintajärjestelmää!**
- Edellä esitettyjen ja muiden vaatimusten täyttämisestä huolehtiminen
- Vaatimustenmukaisuuden arviointimenettelyn teettäminen

HUOM! Velvollisuuksia myös käyttöönottajalle!

Ulkopuolinen arviointi pakollista, Fimea valvoo

- Ulkopuolisen tahon on arvioitava, täyttyvätkö suuririskiselle tekoälyjärjestelmälle asetetut vaatimukset
- Vaatimustenmukaisuuden arviointilaitos eli ns. ilmoitettu laitos
  - Laitoksen täytettävä tietyt vaatimukset
  - Tekee vaatimuksenmukaisuusarviointeja ja antaa todistukset niistä
- **Jos MDR:n mukainen ilmoitettu laitos täyttää myös AI Actin edellytykset ilmoitetulle laitokselle, sama laitos voi arvioida myös AI Actin näkökulmasta**
- Poikkeustapaus: MDR:n mukaiselle luokan I laitteelle ei tarvita ulkopuolista arviointia, jos noudatettu kaikkia standardeja ja muita yhteisiä eritelmiä JA ne kattavat kaikki vaatimukset - käytännössä tällaisia AI-laitteita ei ole

Standardit ja “yhteiset eritelmät”

40 ja 41 artiklat, vastaava käytäntö kuin MDR:ssä (jossa 8 ja 9 artiklat):

- Yhdenmukaistettuja standardeja pidettävä vaatimusten mukaisina
- Jos ja kun standardeja ei ole, voidaan käyttää täytäntöönpanosäädöksillä annettuja yhteisiä eritelmiä (common specifications)

→ Käytännön soveltamisohjeita tulossa vielä

Muutamia eroavaisuuksia ja erityisnostoja

- MDR vaatii yritykseltä PRRC:n (person responsible for regulatory compliance, 15 artikla), AI Actissa ei tällaista vaatimusta ole
- AI Act tuo markkinoille saattamisen jälkeiseen valvontaan mukaan eksplisiittisesti ihmisen suorittaman valvonnan
- Dataan kiinnitettävä entistä enemmän huomiota niin kehitysvaiheessa kuin verifioinnissa ja validoinnissakin
  - Ohjelmistojen tapauksessa testausdatan laatu on voinut olla käytännössä vaihtelevaa
- AI Actissa haluttu tukea innovointia
  - Tekoälyn sääntelyn testiympäristöt ja tietyt helpotukset pk-yrityksille
- Sanktiot
  - MDR jättää enemmän asioita kansallisen sääntelyn varaan
  - AI Actin mukaiset summat varsin suuria

Mitä kysymysmerkkejä?

Vaikka AI Act on periaatteessa varsin tutunoloinen MDR:ään perehtyneelle, käytännön asioissa on kuitenkin vielä ratkaistavaa, esimerkiksi:

- Pystyvätkö nykyiset ilmoitetut laitokset toimimaan myös AI Actin mukaisina arvioijina?
- Mistä kaikki kompetenssit yrityksiin, ilmoitettuihin laitoksiin ja valvoville viranomaisille (MDR:n piiriin kuuluville Fimea)?
- Miten soveltaminen konkretisoituu standardeiksi ja ohjeistuksiksi?
- Millaisia käytännön tapoja yritykset lopulta keksivät ja omaksuvat, jaetaanko tietoa ja parhaita käytäntöjä eri tahojen kesken?
- Miten yhden dokumentaation periaate toimii käytännössä?

Yhteenveto

AI Actissa on paljon samaa kuin MDR:ssä!

- Perusasiat paikoilleen molemmista ensin: strategia, laadunhallinta, riskienhallinta, data, kehitysprosessit jne.
- Seuraa standardointityötä, tarkista ohjeistukset
- Ajoissa yhteistyöhön ilmoitetun laitoksen kanssa
- Hanki apua ajoissa

Lähde surffaamaan tsunamin harjalla!

Kuvan “Lovechild of MDR and AI Act” ideoinnissa ja luomisessa käytetty apuna ChatGPT 4o + DALL-E

Kiitos!

Kuvan ottamisessa on hyödynnetty lapsityövoimaa, mutta ei tekoälyä tai kuvankäsittelyä