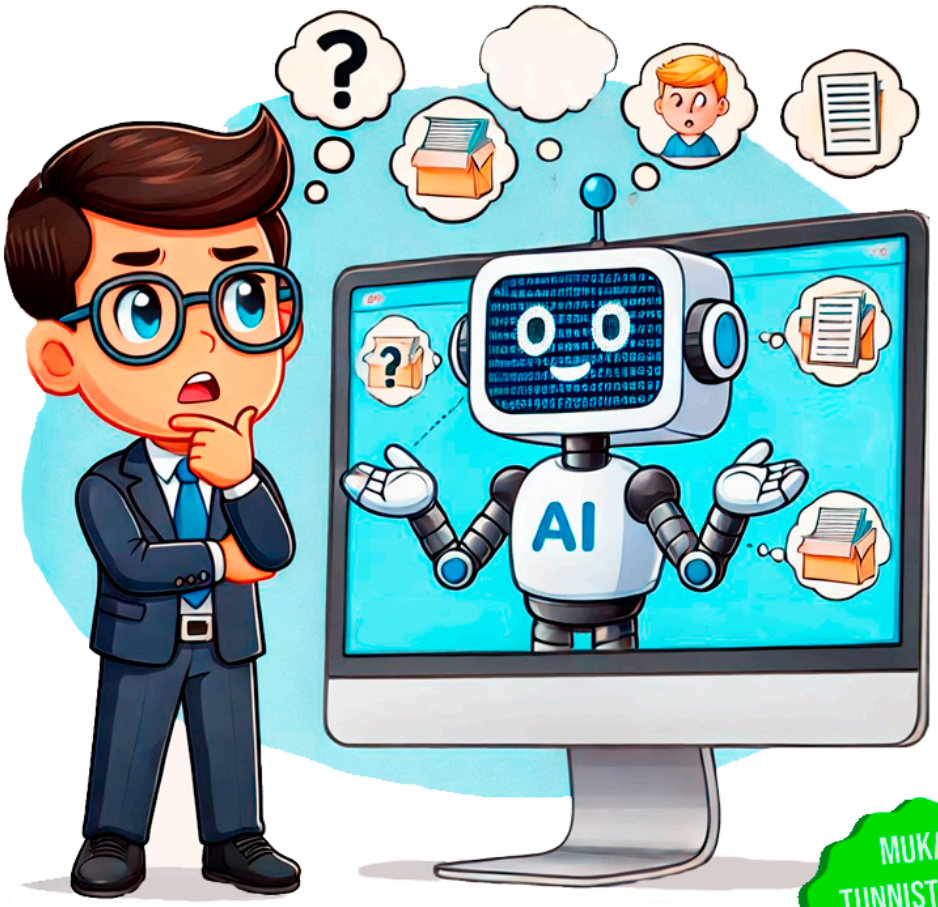
TEKOÄLYPALVELUN VAIKUTUKSENARVIOINTI



MUKANA: TUNNISTETTUJA RISKEJÄ TEKOÄLYN OPPILAITOS-KÄYTÖSSÄ!

Askel askeleelta -ohjeet

EDUKS

OTAVIA KUOPIO

OPETUSHALLITUS RAHOITTAA HANKETTA

JOHDANTO

Tekoälypalvelun käyttöönotto voi edellyttää laajoja arviointitoimia, kuten muutosvaikutusten arvoinnin, perusoikeuksien vaikutusten arvioinnin (FRIA), tietosuojan vaikutusten arvioinnin (DPIA) ja siirtovaikutusten arvioinnin (TIA). Opas keskittyy tietosuojanvaikutusten arvioinnin (DPIA) tekemiseen, mutta neuvoo myös muiden vaikutustenarviointien tarpeellisuudesta tekoälypalveluita käyttöönottaessa.

MUUTOSVAIKUTUSTEN ARVIOINTI

Muutosvaikutusten arviointi tarkoittaa etukäteen tehtävää selvitystä siitä, miten suunnitellut muutokset, kuten tekoälyjärjestelmän käyttöönotto, vaikuttavat organisaation tiedonhallintaan. Arvioinnin tavoitteena on tunnistaa ja ennakoida muutoksen vaikutuksia sekä riskejä, varmistaa, että tiedonhallinta toimii lainmukaisesti ja tehokkaasti myös muutoksen jälkeen. Muutosvaikutusten arvioinnista kaiken tarvittavan tiedot löydät valtioneuvoston oppaasta.

PERUSOIKEUKSIEN VAIKUTUSTENARVIOINTI (FRIA)

Euroopan unionin tekoälyasetus (AI Act) määrittelee, että suuririskisille tekoälypalveluille tehdään perusoikeuksien vaikutustenarviointi ennen niiden käyttöönottoa. Perusoikeuksien vaikutustenarvioinnin voi yhdistää tietosuojan vaikutustenarviointiin, kuten olemme tässä oppaassa tehneet. Tämän oppaan riskiosiossa käytämme **(FRIA)**-merkintää, jos riski koskee nimenomaisesti perusoikeuksien arviointia. Tämä opas ei kuitenkaan opasta FRIA:n tekoon, vaan se on tietosuojan vaikutustenarviointi (DPIA)-opas, jossa sivutaan hieman FRIA:a. Olemme lisäksi pohtineet erillisessä artikkelissa FRIA:n tarpeellisuutta tekoälypalveluiden käyttöönoton yhteydessä: Artikkeli.

SIIRTOVAIKUTUSTEN ARVIOINTI (TIA)

Kun henkilötietoja siirretään EU/ETA-alueen ulkopuolelle, on tärkeää arvioida siirtoon liittyvät riskit. Tätä kutsutaan siirtovaikutusten arvioinniksi (TIA). Asiaa helpottamaan on luotu Data Privacy Framework (DPF) -sopimus EU:n ja USA:n välillä. DPF mahdollistaa henkilötietojen siirron EU/ETA-alueelta sellaisille yhdysvaltalaisille yrityksille, jotka ovat sitoutuneet noudattamaan yhteisiä tietosuojaperiaatteita. Näissä tapauksissa tietosuojan tason katsotaan olevan riittävä (EU-komission riittävyyspäätös).

Jos arvioitava tekoälypalvelu siirtää tietoja EU/ETA-alueen ulkopuolelle (kuten Yhdysvaltoihin) tarkista onko palveluntarjoajalla Data Privacy Framework - sertifiointi (DPF). Tietojen siirto on yleensä hyväksyttävissä ilman erillistä siirtovaikutusten arviointia (TIA), mikäli DPF-sertifiointi on voimassa. Ilman DPF-sertifiointia siirtovaikutusten arviointi on tarpeen.

TIETOSUOJAN VAIKUTUSTENARVIOINTI (DPIA)

Tekoälypalvelun käyttöönotto edellyttää tietosuojan vaikutusten arviointia (TVA, eng. DPIA), josta on vastuussa rekisterinpitäjä (kunta, oppilaitos tai opetuksen järjestäjä). Arvioinnin tarkoituksena on tunnistaa ja vähentää henkilötietojen käsittelyyn liittyviä riskejä sekä tuottaa aineistoa tietosuojasääntelyn noudattamisen osoittamiseksi. TVA:ssa arvioidaan palvelun soveltuvuus, laillisuus ja turvallisuus. Kaikista eri vaikutusten arvioinneista tämä opas keskittyy tietosuojan vaikutustenarvioinnin toteuttamiseen.

Opas huomioi opetusalan erityispiirteet tekoälypalvelun käyttöönotossa ja ohjaa TVA-prosessin läpi askel askeleelta. Oppaamme sisältää paljon esimerkkivastauksia haastavimpiin osa-alueisiin. Emme ole vastanneet tietosuojan vaikutustenarvioinnin ohjeen kaikkiin apukysymyksiin pitääksemme oppaan kohtuullisen mittaisena.

Tarkoituksenamme on tehdä prosessista helposti ymmärrettävä. Pyrimme välttämään tietosuojajargonia, mutta tietyissä kohdissa viralliset termit ovat tarpeen. Sanaston löydät liitteestä 1.

TIETOLAATIKKO

Tarkemmat ohjeet vaikutustenarviointiin ja hyödyllinen arviointityökalu löytyvät Tietosuojavaltuutetun toimiston sivuilta:

- Tietosuojan vaikutusten arvioinnin alkukartoituslomake
- Tietosuojan vaikutustenarvioinnin ohje
- Tietosuojan vaikutustenarviointi rikosasioiden tietosuojalain mukaan
- Tietosuojavaltuutetun vaikutustenarvioinnin työkalu (.xls-tiedosto)

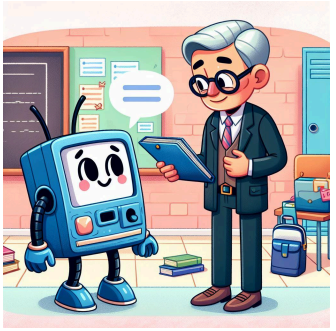
Seuraavat lait ja asetukset määrittelevät henkilötietojen käsittelyä ja tekoälyn hyödyntämistä:

- Tietosuojalaki 1050/2018
- Euroopan unionin yleinen tietosuoja-asetus: GDPR
- Euroopan unionin tekoälyasetus: AI Act

LISÄTIETOA: eduks.fi & bit.ly/totoppaat
TEKSTI: Heikki Laivamaa, Miika Miinin & Matti Kähkönen
TAITTO: Miika Miinin
ERITYISKIITOKSET: Harto Pönkä, Ilona Sidoroff, Kari A. Hintikka ja Anne Rongas.

I. VAIKUTUSTENARVIOINTIPROSESSI - ASKEL ASKELEELTA

Vaikutustenarviointia tehdessä tulee dokumentoida kaikki tehdyt vaiheet (osoittamisvelvoite). Tietosuojan vaikutustenarvioinnin (TVA) tekemiseen ja dokumentointiin on tarjolla paljon erilaisia (usein maksullisia) työkaluja. Tietosuojavaltuutetun toimisto tarjoaa ilmaista excel-pohjaista TVA-työkalua, jota käytetään oppaan esimerkeissä, mutta sekään ei ole edellytys arvioinnin tekemiselle.



VALMISTELUT ENNEN TIETOSUOJAN VAIKUTUSTENARVIOINTIA

Ennen tietosuojan vaikutustenarviointiprosessia tulee tehdä valmistelevat toimet, jotka esitellään seuraavaksi.

VAIHE 1: ÄLÄ TOIMI YKSIN

- Muodosta tiimi ja järjestä työpajoja.
- Tiimiin kannattaa kutsua: Tietosuojavastaava, IT-asiantuntijat, mahdollisesti juridinen neuvonantaja sekä käyttäjäryhmien edustajia.
- Varmista jatkuvuus ja vastuut: Milloin arviointia päivitetään: vuosittain, aina kun palveluun tehdään merkittäviä muutoksia? Kuka vastaa TVA:n ylläpidosta ja päivittämisestä? Kuka hyväksyy arvioinnin?
- Tarkista mikä on organisaatiosi prosessi tietosuojan vaikutustenarviointeihin - tämä opas on tukimateriaali eikä se ohita organisaation linjauksia.
- Dokumentoi ja kirjaa: Kirjaa milloin arvioinnin mikäkin vaihe on tehty. Milloin arviointia on päivitetty, mitä muutoksia on tehty ja kenen toimesta?

VAIHE 2: TUTUSTU PALVELUN DOKUMENTAATIOON

Tutustu palvelun käyttöehtoihin selvittääksesi, onko sen käyttö oppilaitoksessa mahdollista. Tarkista samalla palvelun ikärajat käyttöehdoista ja lainsäädännöstä, ja varmista, että kaikki käyttäjät täyttävät ne.

Samasta tuotteesta on usein maksullinen ja maksuton versio. Maksuttoman version ansaintalogiikka perustuu pääasiassa mainontaan ja/tai henkilötietojen kaupalliseen käyttöön. Ilmaispalvelut ovat yleensä tarkoitettu vain yksityiskäyttöön. Kokemuksemme mukaan maksulliset versiot ovat ilmaisversiota useammin EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisia.

Tutustu DPA-sopimukseen (sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välillä, jossa määritellään käsittelyn ehdot ja vastuut) sekä muuhun

dokumentaatioon, joissa kerrotaan kuinka palveluntarjoaja käsittelee henkilötietoja. DPA-sopimuksessa on usein linkit tarvittaviin dokumentteihin.

★ **Vinkki:** Googlen NotebookLM-tekoälypavelu on loistava työkalu tiedonetsintään suuresta tekstimassasta, esim. ikärajat käyttöehdoista.

VAIHE 3: ALUSTAVA RISKIKARTOITUS - TARVITAANKO VAIKUTUSTENARVIOINTI?

Alustavassa riskikartoituksessa tarkastellaan, kuinka merkittäviä riskejä palvelun käyttö aiheuttaa henkilötietojen suojan näkökulmasta ja selvitetään tarvitaanko *tietosuojan vaikutusten arviointi*.

Jos yksikin seuraavista kohdista täyttyy, tarvitaan TVA (DPIA):

- Käytetään uutta teknologiaa (esim. tekoälypohjainen chat-sovellus).
    - **Huom!** Jo tämä kohta varmistaa, että TVA tarvitaan tekoälypalveluiden käyttöönotossa.
- Käsitellään erityisiä henkilötietoja (esim. terveystiedot, oppimishistoria).
- Tehdään automaattisia päätöksiä tai profilointia.
- Henkilötietoja siirretään Euroopan talousalueen (ETA) ulkopuolelle.
- Oppilaat tai opiskelijat käyttävät palvelua ja heidän henkilötietojaan on palvelussa.

★ **Huom!** Tämä ei ole kaiken kattava lista, vaan opetuksen kannalta oleellisimpia esimerkkejä. Täyden listan löydät täältä ja vielä syvemmälle pääset täältä.
★ **Huom!** *Myös tämä vaihe tulee dokumentoida.*
★ **Vinkki:** *Voit hyödyntää Digi- ja väestötietoviraston* alkukartoituslomaketta.

★ **Päätös:** Ennen tekoälypalvelun käyttöönottoa tarvitaan tietosuojan vaikutusten arviointi (eli TVA/DPIA).

VARSINAINEN TIETOSUOJAN VAIKUTUSTENARVIOINTIPROSESSI

Tästä alkaa tietosuojan vaikutustenarviointi.

VAIHE 4: KUVAA HENKILÖTIETOJEN KÄSITTELY

Määrittele ja dokumentoi selkeästi miksi, miten ja mitä henkilötietoja käsitellään. Vastatkaa ainakin seuraaviin kohtiin:

1. Henkilötietojen käsittelyn tarkoitus ja tavoite
2. Henkilöt, joiden tietoja käsittely koskee (rekisteröidyt)
3. Roolit ja vastuut
4. Henkilötiedot
5. Käsiteltävien henkilötietojen määrä
6. Käsiteltävien tietojen maantieteellinen laajuus
7. Henkilötietojen elinkaari
8. Tekninen toteutus

★ **Vinkki:** Laajempi kuvaus löytyy TSV:n oppaasta sivulla 9.

Esimerkkejä:

- *Henkilötietojen käsittelyn tarkoitus ja tavoite*
  - Esim. Opetuksen järjestämiseen liittyvät tarkoitukset koulussa ja etäopetuksessa. Oppimisen tukeminen tekoälyavusteisesti.
- *Henkilöt, joiden tietoja käsittely koskee:*
  - Henkilökunta (30 henkilöä): opettajat, ohjaajat, hallinto
  - Lukion opiskelijat (350 henkilöä)
- *Roolit ja vastuut*
  - Esimerkit vaiheessa 5
- *Henkilötiedot*
  - Esim. oppilaan nimi, kirjautumistunnus, opiskelutiedot, henkilöön yhdistettävissä oleva viestihistoria chatissa.
- *Käsiteltävien henkilötietojen määrä*
  - Esim. opiskelijan etunimi, sukunimi, Primus-ID, osoite.
- *Käsiteltävien tietojen maantieteellinen laajuus*
  - Esimerkit vaiheessa 5
- *Henkilötietojen elinkaari*
  - Esim. Gemini-sovellusten käyttäytymistä koskevaa toimintatietoa (kehotteet ja vastaukset) säilytetään oletusarvoisesti 18kk käyttäjän Google-tilillä.
  - Esim. Opiskelijan Google-tunnus lukitaan välittömästi opiskelujen päätyttyä ja poistetaan 90 päivän kuluttua tästä.
- *Kuinka käsittely toteutetaan teknisesti?*

- “Tilejä käsitellään automaattisesti API-rajapintaa hyödyntäen oppilashallintaohjelmasta käsin.”
- “Järjestelmään luodaan erillinen tunnus.”
- “Järjestelmään kirjaudutaan erillisen palvelun kertakirjautumisella.”

★ **Tulos:** Dokumentaatio käsittelyn luonteesta

VAIHE 5: HENKILÖTIETOJEN KÄSITTELIJÄT JA SIIRROT ETA-ALUEEN ULKOPUOLELLE

Tämä osio on usein työläs. EU:n yleinen tietosuoja-asetus (GDPR) edellyttää, että henkilötietojen siirto Euroopan talousalueen (ETA) ulkopuolelle tapahtuu erityisten suojatoimien ja siirtoperusteiden mukaisesti.

★ **Vinkki:** Jos käytössä oleva tekoälypalvelu siirtää tietoja ETA:n ulkopuolelle (esim. Yhdysvaltoihin), on tärkeää varmistaa, että palveluntarjoajalla on **Data Privacy Framework** -sertifiointi.

★ **Vinkki:** Jos palveluntarjoajalta puuttuu DPF-sertifiointi, tulee tehdä siirtovaikutustenarviointi (TIA). Se on prosessi, jossa arvioidaan henkilötietojen siirron vaikutuksia erityisesti silloin, kun tietoja siirretään EU-/ETA-alueen ulkopuoliseen maahan.

Kirjaa tunnistetut henkilötiedon käsittelijät (tällä ei tarkoiteta henkilöitä, vaan organisaatioita ja yrityksiä) ja arvioi täyttävätkö he vaatimukset seuraavien apukysymysten avulla:

- Tunnista ja kirjaa henkilötietojen käsittelijät ja alikäsittelijät.
- Täyttävätkö käytetyt henkilötietojen käsittelijät heille asetetut kriteerit (TSA art.28.1)?
- Onko laadittu sopimus henkilötietojen käsittelystä (DPA)?
- Onko henkilötietojen käsittelijöille annettu muut tarpeelliset dokumentoidut ohjeet?
- Miten ohjeiden toimitustavasta ja muutoksista on sovittu osapuolten kesken?
- Siirretäänkö henkilötietoja EU:n / ETA:n ulkopuolelle tai kansainväliselle organisaatiolle?
  - Jos siirretään, mihin maihin ja/tai mille organisaatioille?
- Onko komissio tehnyt tietosuojan riittävyyttä koskevan päätöksen (art. 45) ko. maasta tai kansainvälisestä organisaatiosta?
- Takaako käytetty siirtomekanismi riittävän tietosuojan tason?
- Jos ei, mitä suojatoimia henkilötietojen siirroissa ETA:n ulkopuolelle käytetään (art. 46)?

★ **Vinkki:** Laajempi kuvaus löytyy TSV:n oppaasta sivulta 18 - 20.

Tietosuoja-asetuksen (TSA/GDPR) artikla 28.1 velvoittaa rekisterinpitäjän käyttämään vain sellaisia henkilötietojen käsittelijöitä, jotka antavat riittävät takeet

asianmukaisista teknisistä ja organisatorisista toimista. Tavoitteena on varmistaa GDPR:n noudattaminen ja rekisteröityjen oikeuksien suojelu.

Näin varmistat henkilötietojen oikeaoppisen käsittelyn (TSA art. 28.1):

- Valitse palveluntarjoaja huolella: vastuullasi on valita käsittelijä, joka osaa suojata tiedot ja noudattaa lakia.
- Sovi pelisäännöt kirjallisesti: Tehkää selkeä tietojenkäsittelysopimus (DPA), jossa määritellään, miten henkilötietoja käsitellään.
- Pyydä näyttöä osaamisesta: Käsittelijän sertifioinnit (esim. tietoturvatodistukset) ja muut selvitykset (kuten auditointiraportit) auttavat varmistamaan, että heillä on tarvittava osaaminen ja käytännöt kunnossa.
- Tarkista ja valvo: Varmista säännöllisesti (esim. tarkastuksilla tai pyytämällä uusia selvityksiä), että käsittelijä toimii edelleen sovitusti ja lainmukaisesti.

Alla on avattuna esimerkein Google Gemini -palvelua koskevat vastaukset. Vastaukset kysymyksiin löytyvät palveluntarjoajan dokumentaatiosta ja ne tarjoavat tähän usein myös apua:

- Google
- Microsoft

Esimerkkivastaukset Google Gemini -palvelusta:

- *Rekisterinpitäjä(t):*
  - Kunta.
  - Google toimii rajoitetusti rekisterinpitäjänä palveludatan osalta.
- *Henkilötiedon käsittelijä(t):*
  - Alphabet (Google)
- *Alikäsittelijä(t):*
  - Googlen konserniin kuuluvia alikäsittelijöitä on 42 yhtiötä eri maissa. Googlen yhtiöt hoitavat Google Workspacesin ylläpitoa, datakeskuksia ja teknistä tukea. Täydellinen lista alikäsittelijöistä.
- *Täyttävätkö käytetyt henkilötietojen käsittelijät niille asetetut kriteerit?*
  - Kyllä.
  - ISO 27001- , ISO 27017- , ISO 27018- , SOC 2- ja SOC 3 -sertifioinnit
  - Googlen omat tiukat tietosuojakäytännöt
  - Data privacy framework -sertifiointi
  - ★ **Vinkki:** Yritykset tarjoavat usein sertifikaattinsa selkeästi esiteltynä. Sertifikaatit kannattaa käydä läpi ja listata oleelliset. Esimerkit:
    - Google
    - Microsoft
- *Sopimus (DPA) ja ohjeistus henkilötietojen käsittelystä:*
  - Kyllä (vakioehdoin)
  - Google Workspace for Education Terms of Service

        - Google Cloudin datankäsittelyä koskeva lisäys (henkilötietojen käsittelysopimus)
- *Onko henkilötietojen käsittelyn sopimus rekisterinpitäjän käsittelytarkoitusten mukainen?*
    - Ei.
    - Google on osassa palveludataa rekisterinpitäjä palveludatan osalta.
- *Maantieteellinen laajuus? Siirretäänkö henkilötietoja ETA-alueen ulkopuolelle?*
    - ETA-alueen ulkopuoliset maat tai kansainväliset organisaatiot, joihin tietoja siirretään: Australia, Brasilia, Chile, Hongkong, Intia, Singapore ja Taiwan.
    - Onko Euroopan komissio antanut päätöksen tietosuojan riittävyydestä koskien kyseistä maata tai organisaatiota?
        - Kyllä. Palvelun tarjoajalla (Google) on Data privacy framework-sertifikaatti.
    - Mitkä ovat henkilötietojen siirrossa käytettävät siirtoperusteet?
        - Henkilötietojen siirroissa käytettävät perusteet:
            1. EU-komission tekemät riittävyyspäätökset tiettyjen maiden osalta
            2. EU-komission vahvistamat vakiolausekkeet (SCC)
            3. EU:n ja Yhdysvaltojen välinen tietosuojakehys (Data privacy framework).
- *Täydentävät suojatoimet*
    - Opetuksen järjestäjän on suositeltavaa ottaa käyttöön maksullisiin palveluihin sisältyvä data-alueet -toiminto (Data Region) käyttöön siten, että sisältötietoja tallennetaan ja käsitellään vain EU/ETA-alueella.

★ **Tulos:** *Dokumentaatio henkilötietojen käsittelijöistä ja siirrot ETA-alueen ulkopuolelle.*

VAIHE 6: TARPEELLISUUS JA OIKEASUHTAISUUS

Henkilötietojen käsittely on sallittua vain, jos se on välttämätöntä määritellyn laillisen tarkoituksen toteuttamiseksi ja käsittelyn laajuus on suhteessa tähän tarkoitukseen.

Kirjaa arviot:

- Arvio suunnitellun käsittelyn tarpeellisuudesta.
- Arvio siitä, onko olemassa vähemmän henkilötietojen suojaan puuttuvia keinoja, joilla päästään samaan tavoitteeseen?

Arvio suunnitellun käsittelyn tarpeellisuudesta

★ **Esimerkkiarvio:** Rekisterinpitäjän arvion mukaan suunniteltu henkilötietojen käsittely on tarpeellista ja oikeasuhtaista laillisten tarkoitusten

saavuttamiseksi. Käsittely on tehokkain tapa toteuttaa nämä tarkoitukset ja vaikuttaa vähiten rekisteröityjen yksityisyyteen ja henkilötietojen suojaan verrattuna muihin käytettävissä oleviin vaihtoehtoihin. Tarkoituksia ei voida kohtuullisesti saavuttaa ilman henkilötietojen käsittelyä. Rekisterinpitäjä on varmistanut, että palvelusopimus ja henkilötietojen käsittelysopimus on laadittu sen lakisääteisten velvoitteiden mukaisesti.

Onko olemassa vähemmän henkilötietojen suojaan puuttuvia keinoja, joilla päästään samaan tavoitteeseen?

- **Esimerkkiarvio:** Rekisterinpitäjän arvion mukaan ei ole saatavilla vaihtoehtoisia keinoja, jotka rajoittaisivat rekisteröidyn oikeuksiin puuttumista ja samalla mahdollistaisivat samojen tavoitteiden saavuttamisen. Henkilötietojen käsittely on minimoitu ottaen huomioon suunnitellun käsittelyn tarkoitukset ja tavoitellut hyödyt. Rekisterinpitäjä on suunnitellut toimenpiteitä varmistaakseen, että henkilötietoja kerätään ja käsitellään vain siinä laajuudessa kuin on välttämätöntä käsittelytarkoitusten kannalta.

VAIHE 7: VARMISTA ETTÄ HENKILÖTIETOJEN KÄSITTELYLLE ON LAILLINEN KÄSITTELYPERUSTE.

Henkilötietojen käsittelyn tulee aina pohjautua johonkin kuudesta laillisesta *käsittelyperusteesta*. Oppilaitokset käsittelevät tietoja yleensä **lakisääteisten velvoitteidensa** tai **yleistä etua** koskevien tehtäviensä perusteella. Harvinaisissa tapauksissa peruste voi olla myös **rekisteröidyn suostumus**.

KÄSITTELYPERUSTE	SELITYS
Lakisääteinen velvoite	Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. • **Esim.** Tekoälyä hyödyntävän ohjelman käyttäminen työjärjestysten tekemiseen. • **Peruste:** Lakisääteinen velvoite, Lukiolaki (714/2018 luku 3), opetuksen järjestäminen.
Yleinen etu ja julkinen valta	Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. • **Esim.** Oppilaitos voi käsitellä henkilötietoja tilastollisiin ja tutkimustarkoituksiin, jos se palvelee yleistä etua.
(Rekisteröidyn suostumus)	Henkilötietoja voidaan käsitellä, jos rekisteröity on antanut suostumuksensa tiettyä tarkoitusta varten. • **Esim.** Valokuvien ja videoiden käyttö: Suostumusta voidaan pyytää, jos oppilaitos haluaa käyttää opiskelijoiden kuvia tai videoita esimerkiksi verkkosivuilla tai esitteissä. • **Huom!** Oppivelvollisuuteen perustuvassa koulutuksessa henkilötietojen käsittely ei yleensä voi perustua käyttäjän suostumukseen.

★ **Muut käsittelyperusteet:** Käsittelyperusteita ovat myös: *sopimus* ja *elintärkeiden etujen suojaaminen* mutta niiden soveltaminen opetuksessa on hyvin harvinaista. Viimeinen käsittelyperuste on *oikeutettu etu*, mutta sitä ei ole tarkoitettu käytettäväksi viranomaisten toiminnassa. Mikäli tätä käsittelyperustetta käytetään, on tehtävä lisäksi tasapainotesti.

★ **Tulos:** Tekoälypalvelun käsittelyperusteeksi valittiin **lakisääteinen velvoite**.

VAIHE 8: MÄÄRITTELE TIETOSUOJAPERIAATTEET

Riskien tunnistamisessa on tärkeää tunnistaa mihin tietosuojaperiaatteeseen riski liittyy. Alta löytyy selitys tietosuojaperiaatteista ja mitä ne tarkoittavat. Tietosuojaperiaatteet on määriteltävä, jotta voidaan aloittaa myöhemmässä vaiheessa riskien tunnistaminen. Määrittelyssä on suositeltavaa hyödyntää Tietosuojavaltuutetun julkaiseman vaikutustenarvioinnin työkalun tietosuojaperiaatteita käsittelevää **taulukkoa** (Tietosuojaperiaatteet-välilehti).

#	TIETOSUOJAPERIAATE	HUOMIOITAVAA

1.	**Lainmukaisuus ja kohtuullisuus**	• Mikä on *käsittelyperuste*?
		  ○ Arvioitu prosessin vaiheessa 7. (Lakisääteinen velvoite, opetuksen järjestäminen)
		  ○ Perusopetuslaki (628/1998)
		  ○ Lukiolaki (714/2018)
		• Kuinka käsittelyperusteen velvoitteet täytetään? (esim. suostumus tai oikeutettu etu)
		• Onko erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelylle olemassa poikkeusperustetta?
		• Jos käsittelet henkilötunnuksia, mitkä ovat perusteet näiden tietojen käsittelylle?
		• Jos käsittelet rikostuomioihin ja rikkomuksiin liittyviä tietoja, mitkä ovat perusteet näiden tietojen käsittelylle?
		• Kuinka henkilötietojen käsittelyn ennakoitavuus ja kohtuullisuus on huomioitu?

2.	**Läpinäkyvyys**	• Informointi rekisteröidylle: miten henkilötietojen käsittelystä kerrotaan ja missä yhteydessä? • Informoinnin yhteydessä annettavat tiedot • Kuinka tiedon ymmärrettävyys eri kohderyhmille on huomioitu (esim.lapset)? • Perustelut, jos informointia lykätään tai informointi jätetään tekemättä

#	TIETOSUOJAPERIAATE	HUOMIOITAVAA
3.	**Käyttötarkoitussidonnaisuus**	• Tarkoitukset, joita varten henkilötietoja käsitellään • Millaisin teknisin ja organisatorisin keinoin varmistutaan käsittelyn pysymisestä käyttötarkoituksen mukaisena? • Onko mahdollinen jatkokäsittely yhteensopiva alkuperäisen käsittelytarkoituksen kanssa?
4.	**Tietojen minimointi ja säilytyksen rajoittaminen**	• Kerättävien ja säilytettävien tietojen tarpeellisuus • Kuinka minimoidaan järjestelmien ja lomakkeiden keräämät tiedot? • Kuinka tietojen pääsyoikeuksia rajataan? • Onko tietoja mahdollista anonymisoida tai pseudonymisoida? • Mitkä ovat eri tietojen säilytysajat (ml. varmuuskopiot ja lokitiedot)? • Onko tiedoille mahdollisia lakisääteisiä säilytysaikoja? • Mikä on prosessi tietojen hävittämiselle (tai anonymisoinnille)? • Kuinka tietojen säilytysaikojen toteutumista seurataan?
5.	**Tietojen täsmällisyys**	• Kuinka huolehditaan käsiteltävien henkilötietojen täsmällisyydestä, päivittämisestä ja paikkansapitävyydestä? • Kuinka seurataan tietojen ajantasaisuutta?
6.	Henkilötietojen käsittelyn turvallisuus: **Luottamuksellisuus**, **eheys** ja **käytettävyys**	• Millaisilla toimenpiteillä edistetään tietojen luottamuksellisuutta? • Millaisilla toimenpiteillä edistetään tietojen eheyttä? • Millaisilla toimenpiteillä edistetään tietojen käytettävyyttä? • Toimintatavat tietoturvaloukkauksiin reagoimiseen

VAIHE 9: HUOLEHDI REKISTERÖIDYN OIKEUKSIEN TOTEUTUMISESTA

Oppilaitoksen tai opetuksen järjestäjän rekisterinpitäjänä tulee kunnioittaa toiveita niiltä henkilöiltä, joiden henkilötietoja käsitellään, ja tehdä heille muutosten tekeminen mahdollisimman helpoksi. Näistä henkilöistä käytetään nimitystä “rekisteröity”.

Rekisteröidyllä on oikeus:

- Saada tietää, miten hänen tietojaan käytetään.
- Nähdä, mitä tietoja hänestä on tallennettu.
- Korjata virheelliset tiedot.
- Poistaa tiedot ja tulla unohdetuksi.
- Estää tiettyä tietojen käyttöä.
- Siirtää tiedot järjestelmästä toiseen.
- Estää tietojen käsittelyä.
- Olla joutumatta automaattisen päätöksenteon kohteeksi.

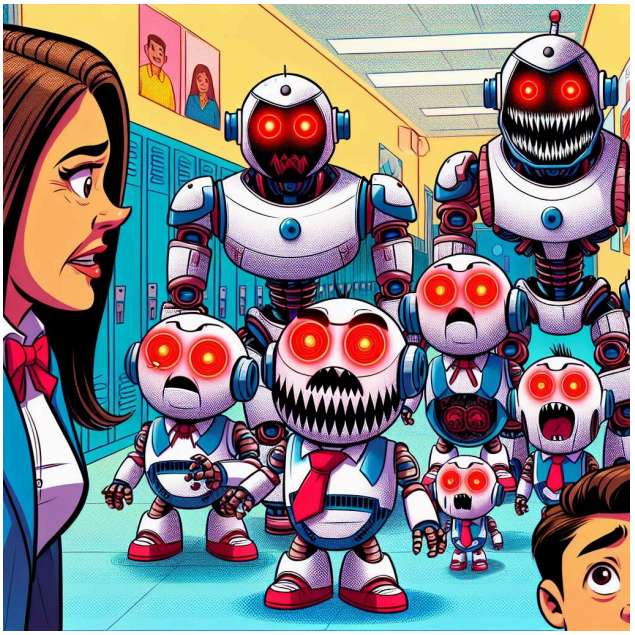
Rekisteröidyn oikeuksien turvaamiseksi tee seuraavat toimenpiteet:

- Tarjoa tietosuojaselosteessa selkeät ohjeet, joiden avulla rekisteröity voi tehdä henkilötietojaan koskevia pyyntöjä.
- Luo selkeä prosessi tietopyyntöjen käsittelyyn:
    - Tarjoa selkeät yhteydenottokanavat.
    - Varmista rekisteröityjen henkilöllisyyden varmistaminen tietoturvallisesti.
    - Nimeä vastuuhenkilöt.
    - Suunnittele pyyntöjen oikea-aikainen käsittely ja dokumentointi.
    - Huolehdi rekisteröityjen auttamisesta pyydettäessä.
    - Takaa tietojen turvallinen toimitus rekisteröidyille halutussa muodossa.

★ **Huom:** Rekisteröidyn oikeudet ovat riippuvaisia käsittelyperusteesta ja etenkin oikeus tulla unohdetuksi tulee hyvin harvoin kyseeseen opetuksessa.
★ **Vinkki:** Rekisteröidyn oikeudet eri tilanteissa.

VAIHE 10: TUNNISTA RISKIT

Palvelun arvioinnin edellytyksenä on siihen liittyvien riskien tunnistaminen. Riskien tunnistaminen ja niiden minimointi kuuluvat rekisterinpitäjän osoitusvelvollisuuteen mahdollisissa ongelmatilanteissa.



Riskiarviointi toteutetaan yhteistyössä käyttäjien kanssa. Heille on tärkeää selittää arvioinnin perusteet ja tavoitteet. Kokemuksemme mukaan käyttäjät saattavat joskus tulkita riskiarvioinnin henkilökohtaisena epäilynä heidän toimintaansa kohtaan - ole siis hienotunteinen!

Arvioi uhkaako jokin asia rekisteröidyn oikeuksia. Prosessi kannattaa aloittaa panemalla päähän “lasit”, joiden läpi palvelua katsotaan. “Laseina” voi käyttää Tietosuojavaltuutetun toimiston uhkataulukkoa (s.29).

- **Huom!** Tietosuojavaltuutettu käyttää kahta hieman eri asiaa tarkoittavaa termiä “uhat” ja “riskit”, mutta asian yksinkertaistamiseksi tässä oppaassa käytämme koko ajan termiä “riski”.

Hieman alempaa löydät taulukon, jonka täyttäminen on kuin pelaisi ristinollaa: jos tiedon *Tallentamiseen* liittyy *Täsmällisyyden* osalta riski, kirjataan se ko. ruutuun. Käytännössä tällainen riski voisi olla esimerkiksi: *Tekoälyjärjestelmä tallentaa kasvojen tunnistustiedot ilman päivitysmekanismia, jolloin tallennetut tiedot eivät ajan kuluessa ole täsmällisiä. Henkilön ulkonäkö voi muuttua ajan myötä, mikä voi johtaa virheellisiin tunnistuksiin.*

★ **Vinkki:** Yhtä riskiä kannattaa käsitellä vaikutustenarvioinnissa yhtenä kokonaisuutena, vaikka se osuisikin taulukossa useampaan ruutuun.

Alkuun pääset tutustumalla tämän oppaan kohtaan: Yleisiä tunnistettuja riskejä tekoälypalveluissa oppilaitoskäytössä. Tehdessäsi vaikutustenarviointia sinun tulee tunnistaa ja kirjata taulukkoon kaikki riskit, joita palvelun käyttöön liittyy. Esimerkin vuoksi olemme sijoittaneet mainitut riskit (pl. **FRIA**-riskit) alla olevaan taulukkoon. Esitäytetystä esimerkkitaulukosta löytyvät tietosuojaperiaatteet ja vasemmasta reunasta mihin vaiheeseen tiedon käsittelyä riski liittyy (ts. tiedon elinkaari).

	Tietosuojaperiaatteet							
Tietojen käsittelyn elinkaaren vaihe	Lainmukaisuus ja kohtuullisuus	Läpinäkyvyys	Käyttötarkoitus-sidonnaisuus	Minimointi ja säilytysaikojen rajoittaminen	Täsmällisyys	Eheys	Luottamuk-sellisuus	Käytettävyys
Kerääminen	12. Tietojenkäsittelysopimukset ovat suurilla yrityksillä määritelty kaikille samoiksi, eikä niihin ole mahdollista saada asiakaskohtaisia muutoksia: "Ota tai jätä".	7. Tekoälypalvelut käsittelevät usein henkilötietoja, esimerkiksi keskusteluhistorian tai käyttäjäprofiilien muodossa. On tärkeää, että käyttäjät ymmärtävät, miten näitä tietoja kerätään ja käytetään.	8. Lähes kaikki isot toimijat (Google, Microsoft jne.) keräävät diagnostiikkatietoja palvelun kehittämiseksi. Teknisesti ottaen palveluntarjoaja on näiden tietojen osalta rekisterinpitäjä eli henkilötietojen omistaja.					
Tallentaminen			4. Palveluntarjoajat voivat käyttää asiakaspalautetta tekoälyn toimintojen parantamiseen.				15. Alempien luokkien opettajilla saattaa huoltajan suostumuksella olla tiedossa oppilaan tunnus ja salasana käytön helpottamiseksi. Salasana saattaa päätyä ulkopuolisen tietoon tai opettaja käyttää pääsyä oppilaiden tietoihin muihin kuin opetustarkoituksiin. Salasanat voivat myös jäädä vaihtamatta alaluokkien jälkeen, jolloin opettajalla voi säilyä pääsy tietoihin.	
Yhdistäminen								
Käyttö ja muokkaaminen		10. Tekoälypalvelut eivät ole läpinäkyviä käytetyn koulutusdatan eikä datan prosessoinnin suhteen. Vastaukset voivat olla epätarkkoja, virheellisiä tai vanhentuneita.	1. Rehtori syöttää oppilaitoksen osoittamaan palveluun sisältöä, joka ei ole sinne tarkoitettu. 2. Useimmat ilmaiset tekoälypalvelut voivat käyttää käyttäjän kirjoittamia syötteitä tai palveluun syöttämää materiaalia tekoälyn kouluttamiseen. 13. Henkilötiedot on kerättävä tiettyä nimenomaista laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.		3. Sovelluskaupoissa on tarjolla lukuisia palveluita, joiden nimet ja logot ovat hyvin lähellä toisiaan.		9. Moni ympäristö mahdollistaa esim. työnjohdon näkökulmasta käyttäjän tarkkailun sekä teknisen valvonnan. Järjestelmänvalvojan voi olla mahdollista, asetuksista ja palvelusta riippuen, lukea käyttäjän tekoälyn kanssa käymät keskustelut.	
Luovutus ja saataville asettaminen			6. Tekoälypalvelut voivat tehdä verkkohakuja parantaakseen vastaustensa laatua. Nämä haut voivat tahattomasti paljastaa yksityisiä tietoja, jos tekoäly sisällyttää verkkohakusyötteeseen sellaisia asioita keskustelusta, joita ei ole tarkoitettu julkisiksi.					
Siirtäminen 3. maihin ja muut siirtotilanteet							11. EU:n yleinen tietosuoja-asetus (GDPR) edellyttää, että henkilötietojen siirto Euroopan talousalueen (ETA) ulkopuolelle tapahtuu erityisten suojatoimien ja siirtoperusteiden mukaisesti.	
Säilyttäminen				5. Kirjoitushetkellä Esim. Microsoft Copilotissa ja Google Gemini Advancedissa oletuksena chatin vuorovaikutushistoria on tallessa 18 kk. Jos keskusteluissa on käsiteltyhenkilötietoja, niin ne säilyvät poikkeuksellisen pitkään, ilman että käyttäjä välttämättä sitä edes tiedostaa.	14. Työntekijän vaihtaessa tehtävää, käyttöoikeudet eivät aina päivity, jolloin hänelle voi jäädä oikeuksia tietoihin, joihin hänellä ei enää tulisi olla pääsyä. Tämä mahdollistaa luvattoman pääsyn tietoihin ja jopa tietojen luvattoman käytön. Toimisto-ohjelmiin kytkeytyvä tekoäly pääsee käsiksi samoihin tietoihin, joihin työntekijällä on pääsy.			
Hävittäminen								

★ **Linkki:** Taulukko löytyy sähköisessä muodossa täältä.
★ **Huom!** Tässä vaiheessa ei kannata huolehtia liikaa siitä, osuuko riski juuri oikeaan ruutuun. Tämä on vain työkalu, jolla tunnistetaan riskit - seuraavissa vaiheissa jokaista riskiä käsitellään yhtenä kokonaisuutena.
★ **Huom!** Taulukossa ei ole täydellinen lista, vaan muutamia esimerkkiriskejä.

★ **Tulos:** *Riskien tunnistaminen ja kirjaaminen.*

VAIHE 11: MÄÄRITÄ RISKITASOT

Riskien tunnistamisen jälkeen täytyy jokaiselle niistä arvioida **riskitaso**. Riskitaso saadaan määrittämällä (asteikolla 1-4) riskille **vakavuus** sekä **todennäköisyys riskin laukeamiselle** ja kertomalla nämä keskenään. Riskien arvioinnissa kannattaa hyödyntää tämän oppaan vakavuusluokitusta, joka esittelee luokittelun seikkaperäisesti.

VAKAVUUS		TODENNÄKÖISYYS RISKIN LAUKEAMISELLE	
Vähäinen	(1)	Epätodennäköinen	(1)
Kohtalainen	(2)	Mahdollinen	(2)
Merkittävä	(3)	Todennäköinen	(3)
Kriittinen	(4)	Lähes varma	(4)

*Jos riskin vakavuus on Kohtalainen (2) ja todennäköisyys sen laukeamiselle Lähes varma (4) on Riskitaso silloin 2 * 4 = **8**.*

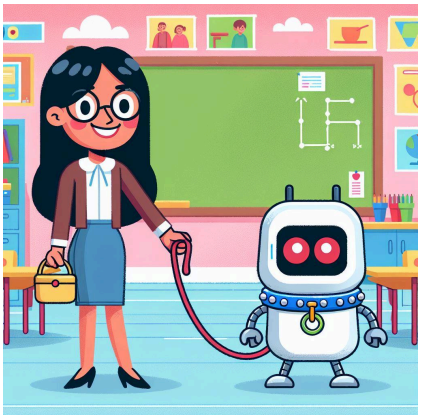
Riskit tulee dokumentoida ja tähän kannattaa käyttää Tietosuojavaltuutetun taulukkoa (lataa .xls-tiedosto ja avaa sieltä välilehti *Riskien arviointi*).

Jokainen riski kirjataan omalle rivilleen. Tässä vaiheessa taulukkoa täytetään jokaisen riskin osalta *Riskilukuun* asti:

	Uhan kuvaus	Uhan vaikutukset ja seuraukset rekisteröidylle	Vakavuus	Toden-näköisyys	Riskiluku	Suojatoimenpiteet riskin pienentämiseksi	Uusi vakavuus	Uusi toden-näköisyy	Uusi riskiluku
1	Esimerkki 1		2	2	4		2	1	2
2	Esimerkki 2		1	3	3		1	2	2
3	Esimerkki 3		3	3	9		3	1	3
4	Esimerkki 4		2	4	8		1	3	3
5					0				0

★ **Tulos:** *Ymmärrys siitä, mitkä riskit ovat kriittisiä.*

VAIHE 12: PIENENNÄ RISKEJÄ



Seuraavaksi pohditaan keinoja tunnistettujen riskien pienentämiseen ja kirjataan keinot ylös.

Yleisiä keinoja riskien vähentämiseksi:

- **Ohjeistus ja koulutus.** Käyttäjille annetaan selkeät ohjeet tekoälypalveluiden turvallisesta ja vastuullisesta käytöstä sekä koulutusta tietoturvariskeistä.
- **Sopimustekniset parannukset.** Palveluntarjoajan kanssa tehdään tarvittavat sopimusmuutokset, joilla varmistetaan tietosuojan toteutuminen ja palvelun turvallisuus, usein tämä tarkoittaa ilmaispalvelun päivittämistä maksulliseen versioon. **Huom!** Tämä tulee huomioida jo kilpailutusvaiheessa, jos hankitaan uusia palveluja.
- **Rajoitukset tietoihin pääsyyn.** Henkilöstön pääsyä (erityisesti arkaluonteisiin) tietoihin rajoitetaan vain niille, jotka niitä välttämättä tarvitsevat, jolloin henkilökunnan työtiedostojen säilytyksen turvallisuus paranee.
- **Salasanasuojaus ja pääsynhallinta.** Tekoälypalveluissa käytetään vahvoja salasanoja ja monivaiheista tunnistautumista sekä määritellään tarkat käyttöoikeudet eri käyttäjäryhmille.
- **Henkilötietojen poistaminen.** Henkilötiedot poistetaan säännöllisesti tai automatisoidusti heti kun niiden säilyttäminen ei enää ole välttämätöntä.
- **Käyttötarkoituksen varmistaminen.** Varmistetaan tiedottamisen ja koulutuksen kautta, että tekoälypalveluita käytetään vain niihin tarkoituksiin, joihin ne on hankittu, ja että tietoja ei käytetä muihin tarkoituksiin.

★ **Huom!** Aiemmin mainitusta osiossa: Yleisiä tunnistettuja riskejä tekoälyn oppilaitoskäytössä löydät riskien lisäksi myös mahdollisia toimia niiden pienentämiseksi.

Vaiheessa 5 taulukkoon kirjattujen riskien osalta kirjataan jokaiselle niistä keinot, joilla riskiä saadaan pienennettyä, ts: *Suojatoimenpiteet riskien pienentämiseksi*:

	Uhan kuvaus	Uhan vaikutukset ja seuraukset rekisteröidylle	Vakavuus	Toden-näköisyys	Riskiluku	Suojatoimenpiteet riskin pienentämiseksi	Uusi vakavuus	Uusi toden-näköisyy	Uusi riskiluku
1	Esimerkki 1		2	2	4		2	1	2
2	Esimerkki 2		1	3	3		1	2	2
3	Esimerkki 3		3	3	9		3	1	3
4	Esimerkki 4		2	4	8		1	3	3
5					0				0

VAIHE 13: ARVIOI JÄÄNNÖSRISKI

Arvioi, kuinka paljon kunkin riskin riskitaso pienenee vaiheessa 12 tehtyjen suojatoimenpiteiden myötä. Käy riskit uudelleen läpi, kuten kävit vaiheessa 11, mutta nyt arvioi tehtyjen toimien jälkeen jäävän **jäännösriskin** vakavuus ja todennäköisyys.

Taulukkoon täydennetään kohta:

	Uhan kuvaus	Uhan vaikutukset ja seuraukset rekisteröidylle	Vakavuus	Toden-näköisyys	Riskiluku	Suojatoimenpiteet riskin pienentämiseksi	Uusi vakavuus	Uusi toden-näköisyy	Uusi riskiluku
1	Esimerkki 1		2	2	4		2	1	2
2	Esimerkki 2		1	3	3		1	2	2
3	Esimerkki 3		3	3	9		3	1	3
4	Esimerkki 4		2	4	8		1	3	3
5					0				0

★ **Tulos:**

- *Jos jäännösriskitaso jää **kaikkien riskien** osalta riittävän matalaksi (7 tai alle) palvelu voidaan ottaa käyttöön ilman lisätoimia.*
- *Jos suojatoimista huolimatta riskitaso jää **yhdessäkin riskissä** korkeaksi (8 tai enemmän), ota yhteyttä tietosuojavaltuutettuun ennakkokuulemista varten.*

★ **Johtopäätös on jokin seuraavista:**

- Palvelu voidaan ottaa käyttöön ja määritellään ehdot.
- Palvelua ei voida ottaa käyttöön vielä, on tehtävä ennakkokuuleminen.
- Palvelua ei voida ottaa käyttöön.

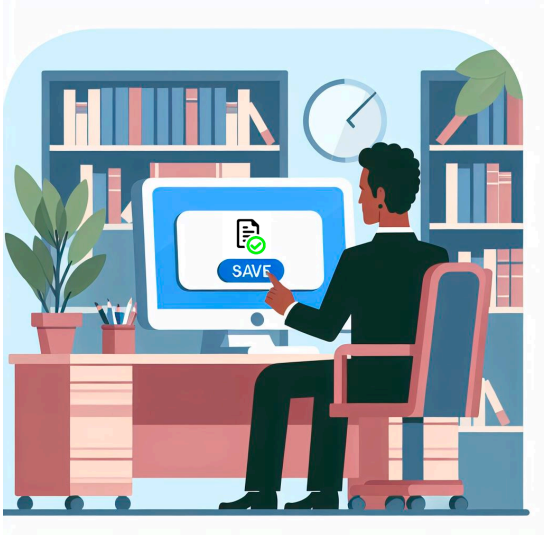
VAIHE 14: VIIMEISTELE DPA-SOPIMUS PALVELUNTARJOAJAN KANSSA

Tekoälypalvelun käyttöönotto edellyttää aina henkilötietojen käsittelysopimusta (DPA), kun palvelu käsittelee henkilötietoja, kuten käyttäjätunnuksia. Tämä sopimus on kuin pelisäännöt, jotka määrittelevät, miten tekoälypalvelun tarjoaja saa henkilötietoja käyttää ja miten niitä pitää suojata. DPA-sopimuksen tarkoituksena on varmistaa, että henkilötiedot pysyvät turvassa ja niitä käsitellään lainmukaisesti. Sopimus selventää, kuka on vastuussa tietojen suojaamisesta ja mitä tapahtuu, jos tietoturvaloukkauksen sattuessa. DPA-sopimus on tärkeä osa oppilaitoksen tietosuojakäytänteitä, jolla osoitetaan, että oppilaitos noudattaa tietosuojalainsäädännön vaatimuksia.

DPA-sopimuksen tarkoituksena on, että rekisterinpitäjä (esim. kunta) määrittää henkilötietojen käsittelyn pelisäännöt, mutta todellisuudessa tämä on isojen toimijoiden kanssa usein mahdotonta. Suurten yritysten DPA-sopimukset ovat samanlaisia kaikille: “Ota tai jätä”. Myös nämä sopimukset tulee lukea, hyväksyä tai hylätä ja dokumentoida. DPA-sopimuksen arviointi on keskeinen osa vaikutustenarviointiprosessia.

VAIHE 15: DOKUMENTOI JA PÄIVITÄ TVA TARVITTAESSA

Säilytä kaikki vaikutustenarvioinnit ja DPA-sopimukset sekä mahdolliset viranhaltijapäätökset kootusti kunnan asiakirjahallinnon ohjeistuksen mukaisesti.



- **Vinkki:** Kirjaamiseen tehokas väline on alussa mainittu: Tietosuojan vaikutustenarvioinnin työkalu (ladattava .xls-tiedosto)

Seuraa palvelun kehitystä sekä käyttäjien tapaa sen hyödyntämiseen. Päivitä TVA aina, kun tulee muutoksia (esim. uusi ominaisuus tai käyttöehdot muuttuvat).

★ **Lopputulos:** *Oppilaitos pystyy perustelemaan ja todentamaan, että palvelun käyttöönotto on tietosuojan kannalta turvallista.*

II. TIETOSUOJARISKIEN VAKAVUUDEN LUOKITTELU OPPILAITOKSESSA

Tietosuojariskien luokittelua hyödynnetään arvioitaessa ja hallittaessa henkilötietojen käsittelyyn liittyviä riskejä oppilaitoksessa. Tietosuojalainsäädäntö vaatii, että rekisterinpitäjä (esim. opetuksen järjestäjä) pystyy osoittamaan, miten riskit on arvioitu ja miten niitä hallitaan.

Luokittelun avulla voidaan **priorisoida toimenpiteet**: Korkeamman riskiluokan (3–4) tilanteisiin on puututtava välittömästi ja varmistettava suojatoimenpiteet, kun taas matalamman riskiluokan (1–2) tapauksissa voidaan keskittyä ennaltaehkäiseviin käytäntöihin.

1. VÄHÄINEN VAKAVUUS

Rekisteröidyille ei aiheudu merkittäviä seurauksia, vaikka he voivat kohdata pieniä ongelmia.

- ★ **Yleisiä esimerkkejä:** Ajanhukka asian selvittämisessä, roskapostin vastaanottaminen, yksityisyyden loukkaamisen tunne ilman todellista haittaa.
- ★ **Kouluesimerkki:** Opiskelija saa arvioitavasta tekoälypalvelusta virheellistä tietoa, mutta tämä ei vaikuta merkittävästi hänen opiskeluunsa.
- ★ **Haitta:** Opiskelija saattaa joutua tarkistamaan tiedon muualta, mikä aiheuttaa ylimääräistä vaivaa, mutta tietosuoja ei vaarannu.
- ★ **Ennaltaehkäisy:** Opettaja ohjeistaa tarkistamaan vastaukset luotettavista lähteistä.

2. KOHTALAINEN VAKAVUUS

Rekisteröidyt voivat kohdata merkittäviä vaikutuksia, mutta selviytyvät niistä joitakin vaikeuksia kohdaten.

- ★ **Yleisiä esimerkkejä:** Ylimääräiset maksut (esim. sakot), pääsyn estyminen hallinnollisiin tai kaupallisiin palveluihin, mainehaitta, uhkailu verkossa.
- ★ **Kouluesimerkki:** Opiskelija kirjoittaa arvioitavan tekoälypalvelun chattiin oman nimensä sekä koulunsa ja palvelu tallentaa tiedot, vaikkei se ole palvelun tarkoitus.
- ★ **Haitta:** Tietojen jakaminen voi lisätä riskiä, että opiskelijan henkilöllisyys yhdistyy käytettyyn nimimerkkiin.
- ★ **Ennaltaehkäisy:** Opiskelijoita ohjeistetaan olemaan jakamatta henkilökohtaisia tietoja chatissa.

3. MERKITTÄVÄ VAKAVUUS

Rekisteröidyt voivat kohdata huomattavia vaikeuksia, jotka voivat vaikuttaa heidän elämäänsä pitkällä aikavälillä.

- ★ **Yleisiä *esimerkkejä:*** taloudelliset tappiot, työpaikan tai asunnon menettäminen, vakavat psykologiset haitat (esim. masennus), nettikiusaaminen.
- ★ **Kouluesimerkki:** Opiskelija jakaa arvioitavassa tekoälypalvelussa arkaluontoisia tietoja, kuten terveyteen tai perhesuhteisiin liittyviä asioita ja palveluntarjoaja käyttää niitä hyväkseen.
- ★ **Haitta:** Opiskelijan yksityisyys voi vaarantua ja tietoja voidaan käyttää markkinointiin, analytiikkaan tai päätöksentekoon.
- ★ **Ennaltaehkäisy:** Oppilaitos käyttää vain oppilaitoskäyttöön tarkoitettuja, tietoturvallisia tekoälypalveluita, joissa tietoja ei käytetä muihin tarkoituksiin.

4. KRIITTINEN VAKAVUUS

Rekisteröidyille voi aiheutua pysyviä ja vakavia vaikutuksia, joista he eivät välttämättä selviydy.

- ★ **Yleisiä esimerkkejä:** Kuolemaan johtava tapahtuma (esim. itsemurha), vakava velkaantuminen, työkyvyttömyys, pitkäaikainen psykologinen haitta kuten identiteetin menetys tai perhesiteiden katkeaminen
- ★ **Kouluesimerkki:** Arvioitavassa tekoäly-chat-palvelussa tapahtuu tietomurto ja opiskelijan kirjoittamat viestit, mukaan lukien henkilökohtaiset sekä arkaluontoiset tiedot, päätyvät vääriin käsiin.
- ★ **Haitta:** Opiskelijat voivat joutua kiusaamisen, identiteettivarkauden tai muun väärinkäytön kohteeksi.
- ★ **Ennaltaehkäisy:** Oppilaitos käyttää vain tietosuoja-asetuksen mukaisia koulukäyttöön tarkoitettuja palveluita, joissa asetukset on määritelty tietoturvallisiksi. Opettajille ja opiskelijoille järjestetään koulutusta tietosuojakäytännöistä.

III. YLEISIÄ TUNNISTETTUJA RISKEJÄ TEKOÄLYN OPPILAITOSKÄYTÖSSÄ

Selvitystyömme perusteella olemme havainneet yleisiä toistuvia tietosuojariskejä tekoälypalveluissa. Näitä havaintoja voi hyödyntää osana vaikutustenarviointia. Kohtien jälkeen löytyviä vinkkejä voi hyödyntää riskien pienentämisessä.. Kaikki riskit tulee kartoittaa oppilaitoksessa palvelukohtaisesti!

1. KÄYTTÄJÄRISKIT

- Rehtori syöttää oppilaitoksen osoittamaan palveluun sisältöä, joka ei ole sinne tarkoitettu.
- Opiskelija tai opettaja käyttää tekoälypalvelua huolimattomasti ja syöttää sinne henkilötietoja tai tekijänoikeuden alaista materiaalia.
- Opettaja antaa opiskelijoille tehtävän, jossa tämän tulee käyttää tekoälypalvelua. Opiskelijan ei olisi käyttöehtojen mukaan sallittua käyttää tekoälypalvelua (esim. ikäraja).

★ **Vinkki:** *Ottakaa tekoälypalvelut käyttöön hallitusti ja tietosuojatusti.*

2. TEKOÄLY HYÖDYNTÄÄ DATAA LAAJEMMIN KUIN KÄYTTÄJÄ HALUAA

- Useimmat ilmaiset tekoälypalvelut käyttävät käyttäjän kirjoittamia syötteitä tai palveluun syötettyä materiaalia tekoälyn kouluttamiseen. Esimerkiksi henkilötietoja tai kustantajan tekijänoikeuden alaista materiaalia voi päätyä luvattomaan jatkokäyttöön.

★ **Vinkki:** *Kouluta henkilökuntaa ja opiskelijoita tietosuoja- ja tekijänoikeusasioissa.*

3. LUOTETTAVAN PALVELUN TUNNISTAMINEN

- Sovelluskaupoissa on tarjolla lukuisia palveluita, joiden nimet ja logot muistuttavat toisiaan.
- Luottavien toimijoiden tuotenimet: onko käytössä tietosuojattu yrityspalvelu vai yksityiskäyttöön suunnattu palvelu?
- Microsoft on nimennyt suuren joukon palveluitaan nimellä “Copilot”, ja Google nimellä “Gemini”, eikä käyttäjä tunnista helposti nimen tai ulkoasun perusteella onko käytössä tietosuojattu yrityspalvelu vai tietosuojattomampi yksityiskäyttöön suunnattu palvelu.

★ **Vinkki:** *Varmista palvelun käyttöehdoista, että se on digiturvan näkökulmasta riittävän laadukas oppilaitoskäyttöön: syötteitä ei käytetä kielimallin kouluttamiseen, käyttäjän chat-historia on suojattu ja säilytysaika rajattu.*

4. PALAUTTEEN ANTAMINEN PALVELUNTUOTTAJALLE

- Palveluntarjoajat voivat käyttää **asiakaspalautetta** tekoälyn toimintojen parantamiseen.
- Jos opiskelijat saavat antaa asiakaspalautetta, palveluntarjoaja saa tietoa, jota heille ei saa luovuttaa.

★ **Vinkki:** *Järjestelmänhaltija voi usein estää palautteen antamisen.*

5. SÄILYTYSAJAT LIIAN PITKIÄ

- Kirjoitushetkellä esim. Microsoft Copilotissa ja Google Gemini Advancedissa oletuksena chatin vuorovaikutushistoria on tallessa 18 kk. Jos keskusteluissa on käsitelty henkilötietoja, niin ne säilyvät poikkeuksellisen pitkään, ilman että käyttäjä välttämättä sitä edes tiedostaa.
- Opettaja säilyttää liian pitkään opiskelijatöitä ja tekoäly pääsee käyttämään niitä. Tekoäly saa pääsyn käyttäjän pilvitallennuksiin, jos käyttöön otetaan integroidut tekoälypalvelut (esim. maksullinen Google Gemini tai Microsoft Copilot)

★ **Vinkki:** *Säilytysaikaa voi usein järjestelmänhallinnan kautta lyhentää.*
★ **Vinkki:** *Tarkista mahdollistaako palvelu tietojen merkitsemisen tunnisteilla (label), jolla voidaan rajata tekoälyn pääsy vain haluttuihin tiedostoihin.*
★ **Vinkki:** *Pidä huolta, että opettajat poistavat tarpeettomat tiedot säännöllisesti (esim. vuosittain)*

6. TEKOÄLYN LUPA HYÖDYNTÄÄ HAKUKONETTA VASTAUSTA PROSESSOIDESSAAN

- Tekoälypalvelut voivat tehdä verkkohakuja parantaakseen vastaustensa laatua. Nämä haut voivat tahattomasti paljastaa yksityisiä tietoja, jos tekoäly sisällyttää verkkohakusyötteeseen sellaisia asioita keskustelusta, joita ei ole tarkoitettu julkisiksi.

★ **Vinkki:** *Tarkasta palveluntarjoajalta onko kuvatun tyyppinen vuoto palvelussa mahdollinen.*
★ **Vinkki:** *Toiminnon voi mahdollisesti järjestelmähallinnasta estää. Tämä vaikuttaa negatiivisesti vastausten laatuun ja ajantasaisuuteen.*

7. KÄSITTELYN LÄPINÄKYVYYS (FRIA)

- Käsittelyn läpinäkyvyys tarkoittaa, että on kerrottava selkeästi ja ymmärrettävästi, mitä tietoja kerätään, mihin niitä käytetään, kuinka pitkään niitä säilytetään ja miten niitä suojataan.
- Tekoälypalvelut käsittelevät usein henkilötietoja, esimerkiksi keskusteluhistorian tai käyttäjäprofiilien muodossa. On tärkeää, että käyttäjät ymmärtävät, miten näitä tietoja kerätään ja käytetään.

★ **Vinkki:** *Suosittelemme selkokielistä, käyttäjän ikätasolle sopivaa erillisviestintää läpinäkyvyyden varmistamiseksi.*
★ **Vinkki:** *Kerro selkeästi opiskelijoille, kuinka tekoälyä hyödynnetään arviointipalautteen monipuolistamiseksi, korostaen opettajan roolia lopullisena arvioijana.*
★ **Vinkki:** *Varmistetaan, että opiskelijoilla on selkeä prosessi, jonka kautta he voivat kyseenalaistaa arviointipalautteen.*

8. DIAGNOSTIIKKATIEDOT

- Lähes kaikki isot toimijat (Google, Microsoft jne.) keräävät diagnostiikkatietoja palvelun kehittämiseksi. Teknisesti ottaen palveluntarjoaja on näiden tietojen osalta rekisterinpitäjä eli henkilötietojen omistaja.

★ **Huomio:** *Käytännössä diagnostiikkatietojen keräämiseen ei käyttäjänä voi vaikuttaa. Järjestelmätasolla voidaan joissakin tilanteessa tehdä rajoituksia.*
★ **Huomio:** *Diagnostiikkatietojen sisältö on usein vähäisen vakavuuden tasolla (1).*

9. YKSITYISYYDENSUOJAN TAI SÄHKÖISEN VIESTINNÄN LUOTTAMUKSELLISUUDEN VAARANTUMINEN

- Moni ympäristö mahdollistaa esim. työnjohdon näkökulmasta käyttäjän tarkkailun sekä teknisen valvonnan. Järjestelmänvalvojan voi olla mahdollista, asetuksista ja palvelusta riippuen, lukea käyttäjän tekoälyn kanssa käymät keskustelut.

★ **Vinkki:** *Pienennä riskiä tarkalla tunnushallinnalla, eli rajaamalla turhat oikeudet pois. Oletusarvoisesti järjestelmänvalvojan pääsy käyttäjien vuorovaikutushistoriaan tulee kytkeä pois päältä.*

10. "VÄÄRÄT VASTAUKSET"

- Tekoälypalvelut eivät ole läpinäkyviä käytetyn koulutusdatan eikä datan prosessoinnin suhteen. Vastaukset voivat olla epätarkkoja, virheellisiä tai vanhentuneita.

★ **Vinkki:** *Riskiä voidaan pienentää käyttäjien kouluttamisella.*
★ **Vinkki:** *Muodosta tekoälyn käyttöön pilottiryhmä ja tue pilottiryhmän aktiivista sisäistä dialogia.*

11. HENKILÖTIETOJEN SIIRTYMINEN ETA-ALUEEN ULKOPUOLELLE

- EU:n yleinen tietosuoja-asetus (GDPR) edellyttää, että henkilötietojen siirto Euroopan talousalueen (ETA) ulkopuolelle tapahtuu erityisten suojatoimien ja siirtoperusteiden mukaisesti.

★ **Vinkki:** *Jos käytössä oleva tekoälypalvelu siirtää tietoja ETA:n ulkopuolelle (esim. Yhdysvaltoihin), on tärkeää varmistaa, että palveluntarjoajalla on* ***Data Privacy Framework*** *-sertifiointi.*
★ **Vinkki:** *Jos palveluntarjoajalta puuttuu DPF-sertifiointi, tulee tehdä siirtovaikutustenarviointi (TIA). Se on prosessi, jossa arvioidaan henkilötietojen siirron vaikutuksia erityisesti silloin, kun tietoja siirretään EU-/ETA-alueen ulkopuoliseen maahan.*

12. SUURTEN YHTIÖIDEN VAKIOEHDOT

- Jos kunta käyttää palvelua, joka käsittelee henkilötietoja (esim. nimet, osoitteet, sähköpostit), sen on tehtävä palveluntarjoajan kanssa tietojenkäsittelysopimus (DPA). Sopimuksessa määritellään tietojenkäsittelyn laajuus ja ehdot.
- Lähes kaikki tekoälypalvelut käsittelevät henkilötietoja, joten kunnan tulee tehdä sopimus palveluntarjoajan kanssa (esim. Google/Alphabet tai Microsoft).
- Suurten yritysten tietojenkäsittelysopimukset ovat kaikille samat, eikä niihin ole mahdollista saada asiakaskohtaisia muutoksia: "Ota tai jätä".

13. KÄYTTÖTARKOITUSSIDONNAISUUS EI TOTEUDU

- Henkilötiedot on kerättävä tiettyä nimenomaista laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.
- Esimerkki: Opiskelija on palauttanut aineen Classroomiin. Tiedosto tallentuu automaattisesti opettajan Drive-kansioon. Opettajalla on käytössä Driveen integroitu tekoälypalvelu Gemini for Google Workspace. Tekoäly voi hyödyntää opiskelijan palauttamaa aineistoa esimerkiksi uuden opetusmateriaalin tekemiseen.

★ **Vinkki:** *Opettaja pienentää riskiä poistamalla omat kopiot opiskelijatöistä.*
★ **Vinkki:** *Selvitä voiko järjestelmätasolla estää tekoälyä käsittelemästä tiettyjä kansioita.*
★ **Vinkki:** *Selvitä voiko järjestelmätasolla automatisoida vanhentuneiden tiedostojen arkistointi tai poisto, jolloin tekoälyllä ei ole pääsyä tietoihin.*

14. KÄYTTÖOIKEUSHALLINNAN AJANTASAISUUS

- Työntekijän vaihtaessa tehtävää, käyttöoikeudet eivät aina päivity, jolloin hänelle voi jäädä oikeuksia tietoihin, joihin hänellä ei enää tulisi olla pääsyä. Tämä mahdollistaa luvattoman pääsyn tietoihin ja jopa tietojen luvattoman käytön. Toimisto-ohjelmiin kytkeytyvä tekoäly voi päästä käsiksi samoihin tietoihin, joihin työntekijällä on pääsy.

★ **Vinkki:** *Ota käyttöön automaattinen käyttöoikeuksien hallintajärjestelmä. Järjestelmä päivittää työntekijöiden käyttöoikeudet* automaattisesti heidän vaihtaessaan tehtävää tai roolia.
★ **Vinkki:** *Tarkista ja auditoi käyttöoikeuksia, jotta luvattomat pääsyt voidaan havaita ja estää ajoissa.*
★ **Vinkki:** *Tarkista onko palvelussa tiedostojen luokittelumahdollisuus (Label), jonka avulla voidaan määrittää tekoälyn oikeuden tietoihin.*

15. PIENTEN OPPILAIDEN TUNNUKSET JA SALASANAT

- Alaluokkien opettajilla voi olla tiedossa oppilaan tunnus ja salasana käytön helpottamiseksi. Salasana saattaa päätyä ulkopuolisen tietoon tai opettaja käyttää pääsyä oppilaiden tietoihin muihin kuin opetustarkoituksiin. Salasanat voivat myös jäädä vaihtamatta alaluokkien jälkeen, jolloin opettajalla voi säilyä pääsy tietoihin.

★ **Vinkki:** *Opettaja opettaa hyvät salasanakäytännöt heti, kun tunnukset otetaan käyttöön. Opettaja ei säilytä oppilaiden salasanoja itsellään.*

16. PALVELUIDEN KÄYTTÖ HENKILÖKOHTAISILTA LAITTEILTA

- Opiskelijat voivat käyttää pilvipohjaisia tekoälypalveluita omilla laitteilla ja kotiverkolla etäopiskelussa sekä kotitehtävien teossa. Hallitsemattomilla laitteilla ja tuntemattomilla verkoilla palvelun käytön tietoturva voi vaarantua.

★ **Vinkki:** *Laadi palveluiden käyttöön selvät pelisäännöt ja tee tarvittavat rajaukset järjestelmätasolla.*

17. OPISKELIJA KÄYTTÄÄ TEKOÄLYPALVELUA, JOKA EI OLE DPA-SOPIMUKSEN PIIRISSÄ

- Sekä Microsoft että Google tarjoavat omia tekoälyratkaisujaan ilmaiskäyttöön, mutta solmitut DPA-sopimukset eivät välttämättä kata tätä käyttöä. Lisäksi on olennaista huomioida palvelukohtaiset ikärajat: esimerkiksi Google Geminin käyttö edellyttää 13 vuoden ikää ja erillistä suostumusta, kun taas Microsoft Copilotilla ikäraja on 18 vuotta. Näin ollen merkittävänä riskinä on palveluiden käyttö ilman vaadittavaa suostumusta tai alle käyttöehtojen sallitun iän.

★ **Vinkki:** *Laadi palveluiden käyttöön selvät pelisäännöt ja tee tarvittavat rajaukset järjestelmätasolla.*

18. TEKOÄLY VAIKUTTAA JATKOKOULUTUKSEEN PÄÄSYYN (FRIA)

- Tekoälyn virheellinen tai syrjivä arviointi voi vaikuttaa opiskelijan pääsyyn tiettyihin koulutusohjelmiin tai vaikuttaa olennaisesti hänen saamaansa koulutuksen tasoon tai jatkokoulutukseen pääsyyn.

★ **Vinkki:** *Varmistetaan opettajan arviointivastuu ohjeistuksella ja koulutuksella.*
★ **Vinkki:** *Anonymisointi/pseudonymisointi: Mahdollisuuksien mukaan käytetään anonymisoitua tai pseudonymisoitua dataa.*

19. TEKOÄLY KORVAA OPETTAJAN ARVIOINNIN (FRIA)

- Tekoälypalvelut osaavat tuottaa laadukkaalta näyttävää arviointimateriaalia. Se pystyy teknisesti tuottamaan formatiivista ja summatiivista arviointimateriaalia. Tekoäly ei kuitenkaan saa toimia automaattisen arvioinnin työkaluna.

★ **Vinkki:** *Varmista opettajan arviointivastuu ohjeistuksella ja koulutuksella.*
★ **Vinkki:** *Anonymisointi/pseudonymisointi: Mahdollisuuksien mukaan käytetään anonymisoitua tai pseudonymisoitua dataa.*

20. SYRJINTÄ (FRIA)

- Tekoälyjärjestelmät voivat ylläpitää ja jopa voimistaa olemassa olevia syrjiviä rakenteita, jos ne on koulutettu vinoutuneella datalla.

★ **Vinkki:** *Käytä vain luotettaviksi todennettuja tekoälypalveluita.*
★ **Vinkki:** *Varmista kielimallin laatu (jatkuva seuranta ja testaus): Varmista, että tekoälyn koulutusdata on mahdollisimman vapaata tunnetuista vinoumista (sukupuoli, rotu, ihonväri…).*

LIITE 1: TIETOSUOJASANASTO

AI Act: ts. EU:n tekoälyasetus on Euroopan unionin asetus, joka säätelee tekoälyjärjestelmien käyttöä ja kehittämistä EU:ssa. Linkki: AI Act

Alikäsittelijä: Henkilötietojen käsittelijän käyttämä kolmas osapuoli, joka käsittelee tai säilyttää henkilötietoja rekisterinpitäjän ohjeiden mukaisesti ja määritellyissä rajoissa. Esimerkiksi kaupungilla on sopimus Wisman kanssa henkilötietojen käsittelystä Wilma-järjestelmässä. Wisma tallentaa tiedot Amazon Web Services -palvelimelle, jolloin Amazon on alikäsittelijä.

Anonymisointi: Henkilötietojen käsittely siten, että tietoja ei voida enää yhdistää tiettyyn henkilöön

DPIA (Data Protection Impact Assessment): Englanninkielinen termi TVA:lle

DPA-sopimus (Data Processing Agreement): Sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välillä, jossa määritellään käsittelyn ehdot ja vastuut. Se on pakollinen, kun joku muu kuin rekisterinpitäjä käsittelee henkilötietoja. Esim. Google Classroomin käyttöön opiskelijoiden henkilötietoja käsittelee Google (Alphabet), jolloin tarvitaan DPA-sopimus kunnan/oppilaitoksen ja Googlen välille.

Ennakkokuuleminen: Prosessi, jossa rekisterinpitäjä kuulee tietosuojaviranomaista ennen henkilötietojen käsittelyn aloittamista, jos vaikutustenarviointi osoittaa korkean riskin (riskitaso 8-16), jota ei ole saatu alennettua omilla toimenpiteillä.

EU:n yleinen tietosuoja-asetus: Euroopan unionin asetus, joka säätelee henkilötietojen suojaa ja käsittelyä Euroopan unionissa (EU) ja Euroopan talousalueella (ETA). GDPR:n tavoitteena on parantaa yksilöiden oikeuksia ja hallintaa omiin henkilötietoihinsa.

FRIA: Perusoikeuksien vaikutustenarviointi suuririskisille tekoälypalveluille.

GDPR: Englanninkielinen lyhenne EU:n yleiselle tietosuoja-asetukselle.

Henkilötieto: Kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön, esim. nimi osoite, terveystiedot.

Henkilötietojenkäsittelijä: Yritys tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän ohjeiden mukaisesti ja määritellyissä rajoissa. Esimerkiksi kaupungilla on sopimus Wisman kanssa henkilötietojen käsittelystä Wilma-järjestelmässä, jolloin Wisma on tietojenkäsittelijä.

Jäännösriski: Riski, joka jää jäljelle sen jälkeen, kun riskinhallintatoimenpiteet on toteutettu. Jäännösriski on usein hyväksyttävä osa riskienhallintaa.

Käsittelyperuste: Laillinen peruste, jonka perusteella henkilötietoja voidaan käsitellä. GDPR:n mukaan käsittelyperusteita ovat: suostumus, sopimus, lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleinen etu ja oikeutettu etu.

Oletusarvoinen tietosuoja: Henkilötietojen käsittelyn oletusasetukset ovat mahdollisimman tietosuoja-ystävällisiä: ilman käyttäjän erillistä toimintaa käsitellään vain välttämättömät tiedot, niiden käyttö on rajattua ja pääsy niihin on vain välttämättömille henkilöille.

Pseudonymisointi: Henkilötietojen käsittely siten, että tietoja ei voida yhdistää tiettyyn henkilöön ilman lisätietoja. Ero anonymisointiin tulee siitä, että lisätietojen avulla tiedot on yhdistettävissä henkilöön.

Rekisterinpitäjä: Opetuksenjärjestäjä tai muu organisaatio, joka kerää henkilötiedot ja vastaa siitä kuinka niitä käsitellään. Esim. kaupunki kerää opiskelijoiden tiedot opetuksen järjestämiseksi. Kaupunki on rekisterinpitäjä.

Rekisteröity: Henkilö, jonka tietoja käsitellään.

Riski: Tarkoittaa todennäköisyyttä, että *uhka* toteutuu ja aiheuttaa haittaa tai vahinkoa. Tässä oppaassa *uhka* ja *riski* termeistä käytetään koko ajan nimitystä *riski*. Katso myös *uhka*.

Riskitaso: Tietosuojan vaikutustenarvioinnissa riskitaso kertoo, kuinka todennäköisesti ja vakavasti henkilötietojen käsittely voi aiheuttaa haittaa rekisteröidylle. Riskin vakavuus x riskin todennäköisyys = riskitaso. Riskitaso auttaa priorisoimaan riskienhallintatoimenpiteitä.

- Riskien todennäköisyys:
    - 1 = epätodennäköinen
    - 2 = mahdollinen
    - 3 = todennäköinen
    - 4 = lähes varma
- Riskien vakavuus:
    - 1 = vähäinen
    - 2 = kohtalainen
    - 3 = merkittävä
    - 4 = kriittinen

Siirtovaikutustenarviointi: Prosessi, jossa arvioidaan henkilötietojen siirron vaikutuksia erityisesti silloin, kun tietoja siirretään EU-/ETA-alueen ulkopuoliseen maahan.

Sisäänrakennettu tietosuoja: Tietosuojan huomioiminen järjestelmien ja prosessien suunnittelun alkuvaiheesta alkaen.

Suostumus: Rekisteröidyn vapaaehtoinen, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn.

TIA (Transfer Impact Assessment): Englanninkielinen termi siirtovaikutustenarvioinnille.

Tietojen minimointi: Periaate, jonka mukaan henkilötietoja saa kerätä vain siinä määrin kuin on tarpeen käsittelyn tarkoitusten kannalta.

Tietosuojailmoitus: Asiakirja, jossa kerrotaan, miten organisaatio käsittelee henkilötietoja.

Tietosuojaperiaatteet: Tietosuojaperiaatteet muodostavat henkilötietojen käsittelyn perustan. Ne varmistavat, että henkilötietoja käsitellään vastuullisesti ja yksilöiden oikeuksia kunnioittaen. Yleisen tietosuoja-asetuksen (GDPR) mukaan niitä ovat: Lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus, osoitusvelvollisuus.

Tietosuojaseloste: Asiakirja, jossa kerrotaan, miten organisaatio käsittelee henkilötietoja. Se sisältää tiedot käsittelijästä, käsiteltävistä tiedoista, käsittelyn tarkoituksesta ja rekisteröidyn oikeuksista.

Tietosuojavastaava: Organisaation riippumaton asiantuntija, joka varmistaa tietosuojalainsäädännön noudattamisen, neuvoo henkilöstöä tietosuoja-asioissa ja valvoo organisaation tietosuojakäytäntöjä.

Tietosuojavaltuutettu: Viranomainen, joka valvoo tietosuojalainsäädännön noudattamista.

Tietoturvaloukkaus: Tapahtuma, joka johtaa henkilötietojen vahingossa tapahtuvaan tai luvattomaan tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai pääsyyn tietoihin.

TVA (Tietosuojan vaikutustenarviointi): Prosessi, jossa arvioidaan henkilötietojen käsittelyn vaikutuksia rekisteröidyn oikeuksiin ja vapauksiin. Se on tehtävä, kun käsittely todennäköisesti aiheuttaa korkean riskin. (eng. DPIA).

Uhka: Viittaa mahdolliseen tapahtumaan tai tilanteeseen, joka voi aiheuttaa haittaa tai vahinkoa. Tässä oppaassa uhka ja riski termeistä käytetään koko ajan nimitystä *riski*. Katso myös *riski*.

Vakavuusluokitus: Arvio henkilötietojen käsittelyyn liittyvän riskin vakavuudesta. Se auttaa määrittämään, kuinka merkittävä riski on ja millaisia toimenpiteitä tarvitaan riskin hallitsemiseksi.