Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Automaation kyberturvallisuus

- 2- Tietosuoja, perusteet

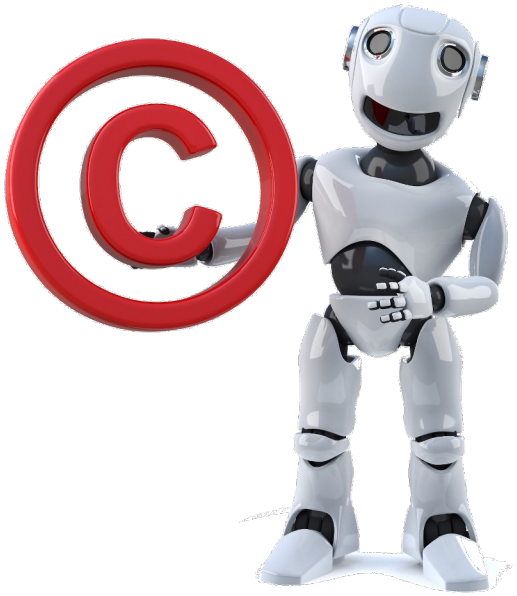
Kyy hanke
Mikko Korpela, Tampereen Ammattikorkeakoulu
Ville Haapakangas, Tampereen Ammattikorkeakoulu

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Materiaalin oikeudet

Kyy –hanke
TAMK

- Materiaali on tehty osana OKM hanketta: *Kyberturvallisuuden opintokokonaisuudet* (Kyy)
- Copyright © *Tampereen Ammattikorkeakoulu; Mikko Korpela, Ville Haapakangas 2025*
- Käytetyt lisenssit :
  - Adobe Stock, Education License, Käytössä TUNI:n kautta
  - MS Powerpoint, Office 365, Käytössä TUNI:n kautta
- Käyttöehto:
  - Materiaalin käyttö sallittu vain opetuskäyttöön
  - Alkuperä mainittava



Kuva: AdobeStock,

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

- Tietosuoja on yksityisyyden suojaa ja se koskee henkilötietoja
  - Tietosuoja koskee luonnollisten henkilöiden tietoja, ei esimerkiksi yrityksien tietoja
  - ! Mutta varsinkin pienten yrityksien kohdalla yrityksen tiedot voi paljastaa henkilötietoja
- Tietosuoja on juridinen termi ja siihen liittyviä vaatimuksia löytyy useista normeista
  - Tavoitteena on tarjota / taata henkilötietojen asiallinen käsittely ja tiedon vapaata liikkuvuutta
  - GDPR Euroopan yleiset tietosuojakäytänteet.
- Tietosuoja asettaa paljon vaatimuksia organisaatioille. Keskiössä on henkilörekisterin tai rekistereiden asianmukainen käsittely.
  - Henkilötietojen käsittelylle pitää aina olla syy.
  - Henkilötietojen kerääminen ja käsittely pitää olla suunnitelmallista ja läpinäkyvää
  - Henkilöllä on oikeus tarkistaa tietonsa tai tulla unohdetuksi
- Tietoturva tieto-omaisuuden hallintaa
  - Tietosuoja asettaa vaatimuksia tietoturvalle (Tietosuojavaatimukset)

Lähtökohta kaikelle on tarkoituksenmukaisuus. Kysytylle tiedolle pitää olla tarkoitus.
”Turhaa” tietoa ei tule kerätä.

Kuva: AdobeStock

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja, esimerkki

Kyy –hanke
TAMK

- Esimerkki: Oho… se lähti väärälle henkilölle
  (Tapahtui kerran…)
  - Mika kysyy opettajalta opintojakson arviointiin liittyvää asiaa. Opettaja lupaa tarkastaa asian ja lähettää tiedon sähköpostilla.

  → Opettaja tarkastaa asian ja kirjaan tiedot sovitusti sähköpostiin. Hän lisää sähköpostiin kuvakaappauksen arvioinnista, jossa näkyy opiskelijan nimi, opiskelijanumero ja osasuorituksen arviointi perusteineen.
  - Opettaja lähettää sähköpostin, mutta epähuomiossa lähetän sen väärällä henkilölle. (mika.virtanen ja miika virtanen meni sekaisin)

- Mitä tapahtui?
  - Kyseessä on **tietosuojaloukkaus**!
    - Viesti sisälsi henkilökohtaista tietoa, joka voidaan yksilöidä

    HUOM! Pelkkä opiskelijanumero olisi riittänyt! Tieto voidaan yksilöidä jo sen perusteella

HUOM! Esimerkki on kuvitteellinen

Kuva: AdobeStock

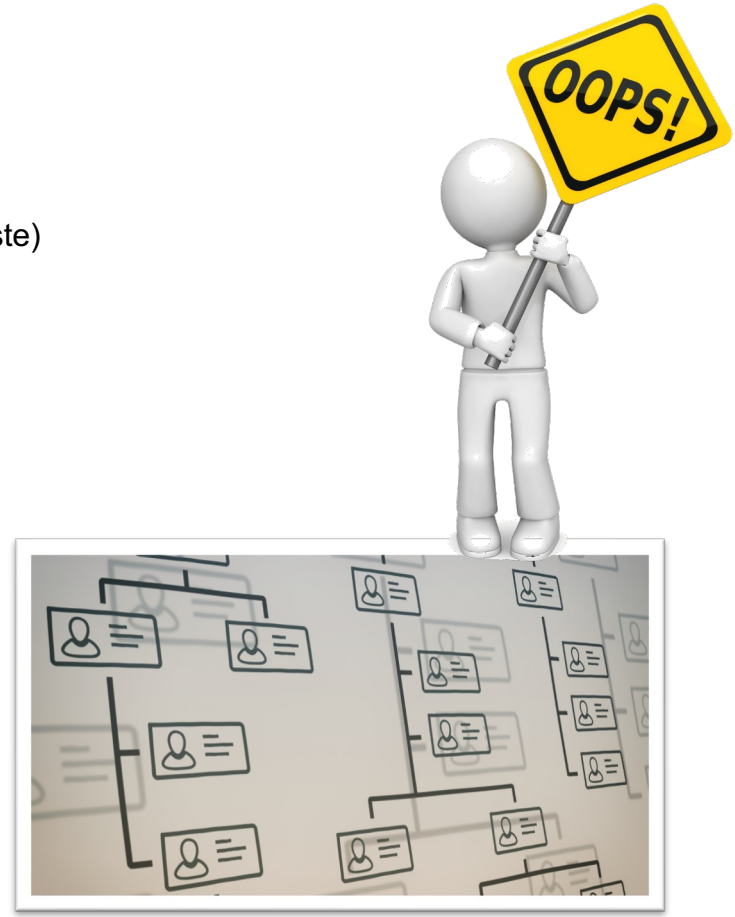
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

Tarkastellaan asiaa tietosuojasäädösten kannalta

- Oliko opettajalla lupa katsoa tieto?
  (Millä perusteella käsittelin henkilötietoja?)
  - Kyllä oli Opetuksen järjestäminen vaatii henkilötietojen käsittelyä (Lakisääteinen peruste)
- Mitä opettajan pitää tehdä? (prosessi)
  - Kun opettaja havaitsee asian pitää hänen tehdä:
    - ilmoittaa asiasta koulun (Organisaation) **tietosuojavastaavalla**
    - Pyytää opiskelijaa (Miika Virtasta) tuhoamaan saamansa viesti, joka sisältää hänelle kuulumatonta tietoa.
    - ! Kannattaa muistuttaa, että Miikalle kuulumattoman tiedon käyttö on rikos.
- Mitä organisaation pitää tehdä?
  (Rekisterin pitäjällä on velvollisuus tehdä seuraavat asiat)
    - Tietosuojavastaava arvioi tietosuojaloukkauksen aiheuttaman riskin opiskelijalle (**rekisteröidylle**), jonka tietoja joutui vääriin käsiin
    - Riskitason perusteella tietosuojavastaava määrittää toimenpiteet
      - Dokumentointi AINA: Mitä tapahtui, miksi ja milloin?
      - Ilmoitus **Tietosuojavaltuutetulle** harkinnan mukaan
      - Ilmoitus Rekisteröidylle, jos tapahtuma aiheuttaa korkean riskin rekisteröidylle



Kuva: AdobeStock

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

- Esimerkki: Oho… se lähti väärälle henkilölle
  (Riskien arviointi, ESIMERKKI!)
  - Rekisteröidylle (opiskelijalle) aiheutuva riski on pieni (ei aiheudu riskiä), koska
    - Viesti ei sisältänyt arkaluonteisia henkilötietoja, terveystietoja tai pankkitietoja
      (TUNI tietosuojaluokitus Henkilön perustieto)
    - Opiskelijanumeroa ei voi käyttää tunnistautumiseen koulun järjestelmissä
    - Opiskelijanumeroa ei käytetä koulun ulkopuolella.

    HUOM! Jos valtakunnallinen opiskelijarekisteri toteutuu, asia muuttuu!

- Tämän perusteella toimenpiteet (mitä opittiin)
  - Dokumentointi: KYLLÄ Muistin avuksi ja tilastointia varten. Poikkeuksien käsittely on osa organisaation jatkuvaa parantamista. Virheistä pitää oppia!
  - Ilmoitus tietosuojavaltuutetulle: EI tarvitse. Tapahtuneesta ei aiheudu riskiä
  - Ilmoitus rekisteröidylle: EI tarvitse. Tapahtuneesta ei aiheudu riskiä

- Pohdin tilannetta, jossa tilauslomake jää kopiokoneeseen

HUOM! Arvio on vain esimerkki.

- Todelliset tapaukset pitää aina käsitellä organisaatiossa yksittäistapauksina!
  - Riskienarviointi vaatii kokonaisvaltaisen tarkastelun ja ymmärryksen. Esimerkiksi puhelinnumero aiheuttaa huomattavasti suuremman riskin, koska sen avulla voidaan yhdistää rekistereitä.
  - Jokainen tapaus on yksittäinen. Esimerkiksi arvioinnin perustelu! ”…lukihäiriö huomioitu” kommentti vaarantaa henkilön kannalta arkaluonteista tietoa.

Kuva: AdobeStock

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

- Esimerkki: Oho… se lähti väärälle henkilölle
  (Viestin saajan kannalta)
  - Opiskelija, joka on saanut haltuunsa hänelle kuulumatonta tietoa, ei saa saa käyttää tätä tietoa eikä ilmaista sen olemassaoloa
    (laki sähköisen viestinnän palveluista 136 §)
  - Käytännössä opiskelijan pitää tuhota viesti

- Pääsy henkilötietoihin ei tee tiedon käytöstä hyväksyttävää
  - Henkilötietojen käyttöön pitää olla perusteltu syy!
  - Esimerkiksi Vastaamon tapauksessa. Henkilöt, jotka latasivat varastettuja tietoja voivat syyllistyä tietosuojarikokseen.

Sairaalan työntekijä urkki 200 potilaan tietoja – hovioikeus tuomitsi ehdolliseen vankeuteen

Etelä-Karjalan sosiaali- ja terveyspiiri Eksoten entinen työntekijä sai Itä-Suomen hovioikeudessa ehdollisen vankeustuomion luvattomasta potilastietojen katselusta.

Lähde: YLE
12.7.2019

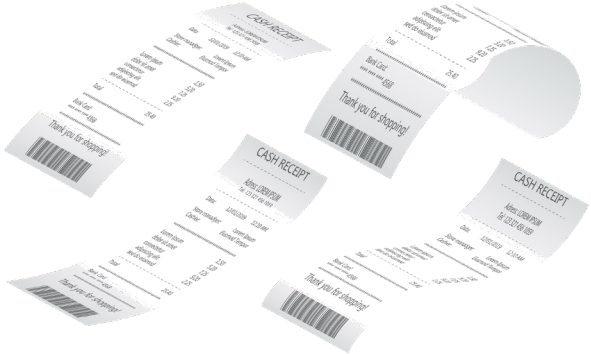
Kuva: AdobeStock

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

- Tietoa vai henkilötietoa?
  (Esimerkki: kauppa kuitti)
  - Yksittäisestä kauppalapusta tai ostokuitista ei vielä paljoa voida päätellä, mutta…
    - kuitti ei ole henkilötietoa, **jos sen sisältävää tietoa ei voi yksilöidä henkilöön.**
    - jos kuitissa on bonuskortin numero, voidaan kuitti yhdistetään numeron avulla henkilöön. Tällöin kuitin tiedoista henkilötietoa
    - Esimerkiksi apteekin kuitti voi sisältää terveystietoja!
  - Ostohistoriasta voidaan päätellä paljon
    - jos huomioidaan muiden asiakkaiden käyttäytyminen, voidaan oppia ”ennustamaan” tulevaa.
    - Rekisteröityjä voidaan profiloida tai ryhmitellä
  - Muista! Tiedon keräämiseen pitää olla aina peruste, joka pitää määrittää ennen tiedon keräämistä
    - Henkilölle kuulumatonta tietoa, ei saa saa käyttää eikä ilmaista sen olemassaoloa



FORBES > TECH

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Former Staff

Welcome to The Not-So Private Parts where technology & privacy collide

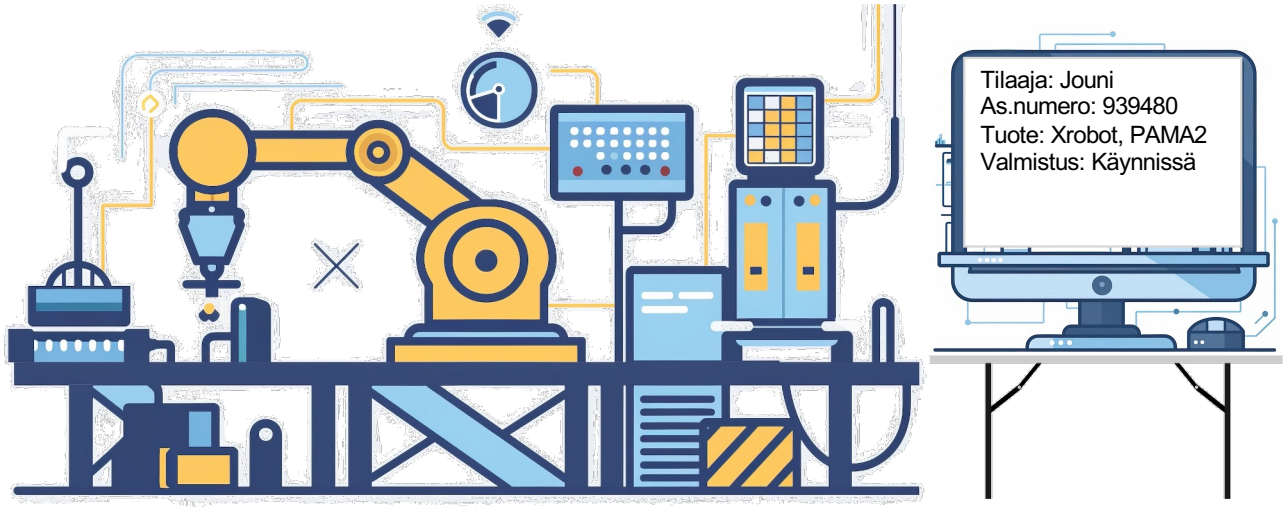
Feb 16, 2012, 11:02am EST

Lähde: Forbes 16.2.2012 www.forbes.com

Kuva: AdobeStock

Tietosuoja

- Tietosuoja tuotannossa
  - Tuotantoympäristöjä koskee samat vaatimukset, kuin tietojärjestelmien vaatimukset
  - Tuotantotieto ei ole henkilötietoja, jos sitä ei yhdistetä tilaajaan
- Esimerkki: Tilaajan tiedot tuotannossa
  - Tilausjärjestelmä välittää tuotantoon tuotetietojen lisäksi tilaajan tiedot
  - Tuotantosolun näyttö näyttää tuote- ja prosessitietojen lisäksi tilaajan tiedot
  - Ongelma saattaa syntyä, jos tehtaalla on vierailijoita.
    - Tuotteen tiedon on yhdistettävissä henkilöön, jolloin ne ovat henkilötietoja
- Oleellista, että tiedon laatu ja tiedon kulku (tietovirta) on suunniteltu
  - Välitetään tuotantoon vain tieto, joka on oleellista



Kuva: AdobeStock (Muokattu)

Tietosuoja

- Harjoitus: Rekisteröidyn oikeus
  - Valitse jokin organisaatio (rekisterinpitäjä), jonka rekisterissä on henkilötietojasi
  - Esim:
    - S-kauppa: https://rekisteriotepyynto.s-kanava.fi/#/start
    - Kesko (K-kaupat): https://tietosuoja.kesko.fi
    - Google: https://policies.google.com/privacy?hl=fi
  - Tee organisaatiolle tietopyyntö
  - Tarkastele tietopyynnön sisältöä
    - Missä muodossa tiedot toimitettiin
    - Mitä tiedoista on päätelty (profiloitu)
  - Vertaa tuloksia organisaation tietosuojaselostukseen.
  - Pohdi oliko tiedoissa jotain, jota et haluaisi toimittaa

Kuva: AdobeStock

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

Tietosuoja

Kyy –hanke
TAMK

- Muista tavoitteet!
  - Tietosuoja on perusoikeus. Henkilötietojen käsittely pitää olla suunnitelmallista, läpinäkyvää ja sille pitää olla peruste.
  - Tietoturva on tieto-omaisuuden hallintaa. Sen avulla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys.
  - Hyvä tietoturva ja tietosuoja lähtee organisaation työkulttuurista ja se näkyy organisaation kaikilla tasoilla ja kaikessa toiminnassa.
    - Sitä ei voi suoraan ostaa.
  - Kaikkien organisaation henkilöiden pitää osaltaan huolehtia tietoturvasta ja tietosuojasta
    - Varmista, että tiedät organisaatiosi tietosuoja ja tietoturva käytänteet.

- Hyödyllisiä linkkejä
  - Tietosuojavaltuutetun toimisto: https://tietosuoja.fi/etusivu
  - GDPR2DSM- hankkeen sivusto (PK- yrityksien tietosuojatyökalu) https://www.tietosuojaapkyrityksille.fi
  - Lainsäädäntö (Yleinen sivusto) https://finlex.fi/fi/

Kuva: AdobeStock