ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Åtgärdsprocedurer vid brott mot dataskyddet

Toimintamenettelyt tietosuojan rikkoutuessa

Informationstillfälle för privata social- och hälsovårds serviceproducenter
Yksityisten sote-palveluntuottajien infotapaaminen

Tietopalveluasiantuntija/tietosuojavastaava Anne Korpi
Tietosuojapäällikkö Tuija Viitala 23.4.2025

Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Definition av personuppgiftsincident:

- Som en följd av en personuppgiftsincident innebär det att de överförda, lagrade eller på annat sätt behandlade personuppgifterna
  - oavsiktligt eller olagligt förstörs,
  - förloras,
  - ändras,
  - obehörigt utlämnande eller

  obehörig åtkomst till uppgifter.

Henkilötietojen tietoturvaloukkauksen määritelmä

- tietoturvaloukkauksen seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen
  - vahingossa tapahtuva tai laiton tuhoaminen,
  - häviäminen,
  - muuttaminen,
  - luvaton luovuttaminen tai pääsy tietoihin

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Vad är ett dataskyddsbrott?

En avsiktlig eller oavsiktlig händelse som äventyrar säkerheten, integriteten eller konfidentialiteten hos de personuppgifter som är under organisationens ansvar.

Till exempel:

- Förlorad USB-enhet
- Stulen telefon eller dator
- Skicka ett dokument som innehåller personuppgifter via e-post eller post till fel mottagare
- Infektion med skadlig programvara
- Utlämning av personuppgifter till obehöriga
- Cyberattack

Mikä on tietosuojaloukkaus?

Tahallinen tai tahaton tapahtuma, joka vaarantaa organisaation vastuulla olevien henkilötietojen turvallisuuden, eheyden tai luottamuksellisuuden.

Esimerkiksi:

- Hävinnyt muistitikku
- Varastettu puhelin tai tietokone
- Henkilötietoja sisältävän dokumentin lähettäminen sähköpostilla tai postitse väärälle vastaanottajalle
- Haittaohjelmatartunta
- Henkilötietojen luovuttaminen ulkopuolisille
- Kyberhyökkäys

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Typer av personuppgiftsincidenter

Dataintrång kan klassificeras enligt tre säkerhetsprinciper:

• **Dataintrång som påverkar konfidentialiteten** – obehörig eller oavsiktlig utlämning av personuppgifter eller obehörig åtkomst till information.

• **Dataintrång som påverkar integriteten** – obehörig eller oavsiktlig ändring av personuppgifter.

• **Dataintrång som påverkar tillgängligheten** – förlust av åtkomst till personuppgifter eller förstörelse av personuppgifter av misstag eller obehörigt.

Henkilötietojen tietoturvaloukkausten tyypit

Tietoturvaloukkaukset voidaan luokitella kolmen tietoturvaperiaatteen mukaisesti:

• Tietojen **luottamuksellisuuteen** vaikuttava tietoturvaloukkaus – henkilötietojen luvaton tai vahingossa tapahtuva luovuttaminen tai pääsy tietoihin.

• Tietojen **eheyteen** vaikuttava tietoturvaloukkaus – henkilötietojen luvaton tai vahingossa tapahtuva muuttaminen.

• Tietojen **käytettävyyteen** vaikuttava tietoturvaloukkaus – vahingossa tapahtuva tai luvaton henkilötietoihin pääsy, häviäminen tai henkilötietojen tuhoaminen.

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Vad förväntas av personuppgiftsansvarig och personuppgiftsbiträde

- "Personuppgiftsincidenter skulle ofta kunna förebyggas med tillräckliga tekniska åtgärder, lämpliga rutiner inom organisationen och genom att säkerställa kunskap om dataskydd.
- Dataintrång orsakas ofta av gamla och icke uppdaterade system, särskilt bristande datasäkerhet. Dessutom har det observerats att sårbarheter i systemen utnyttjas snabbare än tidigare."

Mitä rekisterinpitäjältä ja henkilötietojen käsittelijältä odotetaan

- ”Henkilötietojen tietoturvaloukkaukset olisivat usein estettävissä riittävillä teknisillä toimenpiteillä, organisaation asianmukaisilla menettelytavoilla ja tietosuojaosaamisen varmistamisella.
- Tietoturvaloukkauksille altistavat vanhat ja päivittämättömät järjestelmät ja erityisesti puutteellinen tietoturva. Lisäksi on havaittu järjestelmien haavoittuvuuksien entistäkin nopeampaa hyödyntämistä.”
- TSV:n toimintakertomus 2023

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Förberedelse för avvikelsesituationer

Utan noggrann förberedelse är det svårt att hantera avvikelse-situationer på ett kontrollerat sätt.

• Tekniska kontroller och åtgärder för att förhindra datasäkerhetsincidenter:

• Styrmodeller och riktlinjer

• Roller och ansvar

• Vägledning, utbildning och regelbundna övningar

- Ändringar i behandlingen av personuppgifter och trender inom dataintrång.

Poikkeamatilanteeseen valmistautuminen

Ilman huolellista valmistautumista on hallittu toiminta poikkeama-tilanteessa vaikeaa.

• Tekniset kontrollit ja toimenpiteet, joilla tietoturvapoikkeamia pyritään torjumaan:

• Hallintamallit ja ohjeistukset

• Roolit ja vastuut

• Opastaminen, kouluttaminen ja säännöllinen harjoittelu

- Muutokset henkilötietojen käsittelyssä & tietoturvaloukkaus-trendit.

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Dokumentation av dataintrång

- Den personuppgiftsansvarige ska dokumentera alla dataintrång (enligt ansvarsskyldighets-principen).
- Övervakande myndighet ska kunna kontrollera genom dokumentationen att artikel 33 följs.
- Händelseloggar vid händelsetidpunkten ingår också i dokumentations-skyldigheten.

Tietoturvaloukkauksen dokumentoiminen

- Rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset. (Osoitusvelvollisuus periaatteen mukaisesti).
- Valvontaviranomaisen on voitava tarkistaa dokumentoinnin avulla, että artiklaa 33 noudatetaan.
- Tapahtuma-ajan lokitiedot kuuluvat myös dokumentointi-velvollisuuden piiriin.

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Dokumentationskrav

- Orsaker till dataintrånget
- Vad som hände och vilka personuppgifter som påverkades
- Effekter och konsekvenser av dataintrånget
- Bedömning av risker för de registrerades rättigheter och friheter
- De åtgärder som den personuppgiftsansvarige har vidtagit
- Tidslinje

Dokumentoitavat asiat

- Tietoturvaloukkauksen syyt
- Mitä tapahtui ja mihin henkilötietoihin se vaikutti
- Tietoturvaloukkauksen vaikutukset ja seuraukset
- Luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien arviointi
- Rekisterinpitäjän toteuttamat korjaavat toimet
- Aikajana

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Anmälningar registreras hos ÖVPH

- Alla anmälningar kan göras på HaiPro Integritet/ säkerhetssidan.
- Anmälningar om missförhållanden inom socialtjänsten kan också göras på SPro.

ÖVPH:lla ilmoitukset kirjataan

- Kaikki ilmoitukset voi tehdä HaiPro Tietosuoja/ tietoturvasivustolle
- Sosiaalihuollon epäkohtailmoitukset voi myös tehdä SPro

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

När ska ett dataintrång som rör personuppgifter anmälas?

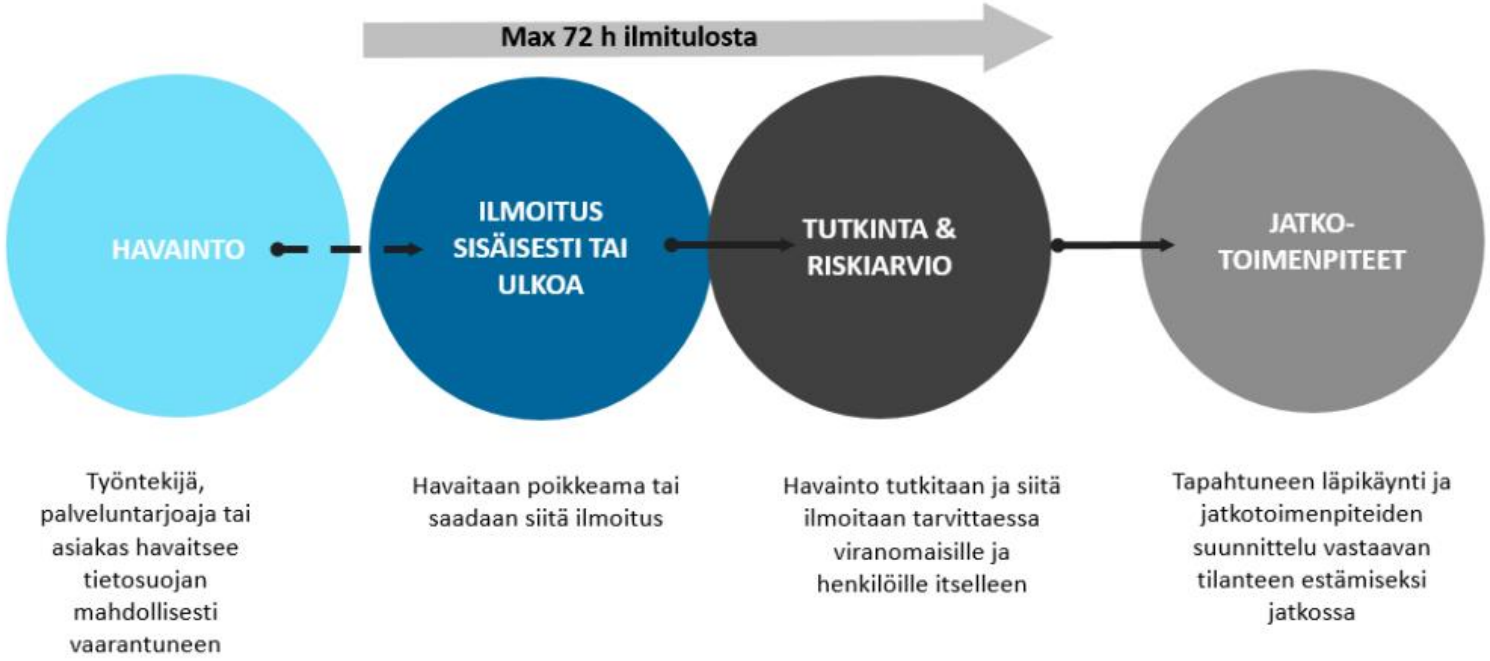
- Alltid när det finns en risk för fysiska personers rättigheter och friheter.

Milloin henkilötietojen tietoturvaloukkauksesta tulee ilmoittaa

- Aina kun on riski luonnollisten henkilöiden oikeuksille ja vapauksille.

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Åtgärder vid dataintrång
Toiminta tietoturvapoikkeamatilanteessa



ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Riskbedömning

- **Typ av dataintrång**
  • Till exempel läckage av känsliga personuppgifter vs. tillfällig förlust av åtkomst till personuppgifter
- **Personuppgifternas natur, känslighet och mängd**
  • Möjlighet att kombinera uppgifter, användningssammanhang
- **Lättheten att identifiera individer**
- **Allvarligheten av konsekvenserna för individerna**
- **Personens särskilda egenskaper** (t.ex. barn och andra sårbara grupper)
- **Personuppgiftsansvariges särskilda egenskaper** (t.ex. personuppgiftsansvariges verksamhet, såsom en sjukhuspatientregister)
- **Antalet personer som påverkas av dataintrånget**

Riskin arvioiminen

- **Tietoturvaloukkauksen tyyppi**

  • Esim. arkaluontoisten henkilötietojen vuotaminen vs. henkilötietojen käytön tilapäinen estyminen

- **Henkilötietojen luonne, arkaluonteisuus ja määrä**

  • Tietojen yhdisteltävyys, käyttöyhteys

- **Henkilöiden tunnistamisen helppous**
- **Henkilöille aiheutuvien seurausten vakavuus**
- **Henkilön erityiset ominaisuudet** (Esim. lapset ja muut heikommassa asemassa olevat)
- **Rekisterinpitäjän erityiset ominaisuudet** (esim. Rekisterinpitäjän toiminnan luonne – sairaalan potilasrekisteri)
- Niiden **henkilöiden määrä, joihin tietoturvaloukkaus vaikuttaa**.

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Konsekvenser av dataintrång för individer

Dataintrång kan orsaka för individer:

- **Materiella konsekvenser,** t.ex. identitetsstöld eller bedrägeri
- **Icke-materiella konsekvenser**, t.ex. skada på rykte, förnedring, ångest, rädsla
- **Fysiska konsekvenser,** t.ex. hot mot hälsa eller liv

Henkilötietojen tietoturvaloukkauksen seuraukset henkilöille

Tietoturvaloukkauksista voi aiheuttaa henkilöille:

- **Aineellisia seurauksia**, esim. identiteettivarkaus tai petos
- **Aineettomia seurauksia**, esim. mainehaitat, nöyryytys, ahdistus, pelko
- **Fyysisiä seurauksia**, esim. terveyteen tai henkeen kohdistuvat uhat

ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

Anmälan till den registrerade och anmälan till dataskyddsmyndigheten

- Vägledning från ÖVPH
- ✓ Anmälan till den registrerade
  - Den aktuella enheten gör det.
- ✓ Anmälan till dataskyddsmyndigheten
  - ÖVPH:s dataskyddsansvarig gör anmälan.

Ilmoittaminen rekisteröidylle ja ilmoituksen tekeminen tietosuojaviranomaiselle

- ÖVPH:n ohjeistus
- ✓ Ilmoittaminen rekisteröidylle
  - Kyseinen yksikkö tekee
- ✓ Ilmoituksen tekeminen tietosuojaviranomaiselle
  - ÖVPH:n tietosuojavastaava tekee ilmoituksen

I enlighet med dataskyddsförordningens artikel 34 anmäls personuppgiftsincidenter till registrerade

Österbottens välfärdsområde är skyldigt att anmäla personuppgiftsincidenter till registrerade om de sannolikt orsakar en hög risk för de registrerades rättigheter och friheter. Säkerhetsincidenter dokumenteras i HaiPro-systemet (dataskyddsanmälan).

Enhetens chef (förman) informerar den registrerade/de registrerade. I anmälan till den registrerade ska man ge en klar beskrivning av personuppgiftsincidenten, de sannolika konsekvenserna av personuppgiftsincidensen samt de åtgärder som Österbottens välfärdsområde vidtagit eller avser vidta.

Anmälan ska inrymma åtminstone följande uppgifter:

- en klar beskrivning av personuppgiftsincidenten
- en begäran om ursäkt
- kontaktuppgifter eller något annat sätt för den registrerade att få mer information om ärendet, t.ex. namnet på dataskyddsombudet
- de sannolika konsekvenserna av personuppgiftsincidenten
- de åtgärder som den personuppgiftsansvarige föreslagit eller redan vidtagit; vid behov också åtgärder för att lindra eventuella olägenheter..

En anmälan krävs inte om

- Österbottens välfärdsområde vidtagit behöriga tekniska och organisatoriska skyddsåtgärder och dessa tillämpats på de personuppgifter som är föremål för personuppgiftsincidenten (i synnerhet åtgärder med vilka personuppgifterna ändras till obegriplig form för utomstående, såsom kryptering)
- Österbottens välfärdsområde har vidtagit fortsatta åtgärder, med vilka det säkerställs att det inte längre är sannolikt att en hög risk som riktar sig mot den registrerades rättigheter och friheter blir verklighet
- detta skulle kräva orimligt besvär, eftersom man till exempel inte vet vem de registrerade är. Ärendet bedöms enligt risk. Om det inte är möjligt att ta kontakt med de registrerade personligen, ska offentlig delgivning eller en motsvarande åtgärd användas, med vilken de registrerade informeras på ett lika effektivt sätt.

Om Österbottens välfärdsområdes personal inte ännu informerat en registrerad om personuppgiftsincidenten, kan tillsynsmyndigheten kräva att detta görs.

Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

Tietosuoja-asetuksen 34 artiklan mukaisesti henkilötietojen tietoturvaloukkauksesta ilmoitetaan rekisteröidylle

Pohjanmaan hyvinvointialue on velvollinen ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle, jos loukkaus todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja yksityisyydelle. Tietosuojaloukkaus dokumentoidaan Tietoturva HaiPro järjestelmään.

Yksikön esimies informoi rekisteröityä / rekisteröityjä. Rekisteröidyille tehtävässä ilmoituksessa on kuvattava selkeästi henkilötietojen tietoturvaloukkauksen luonne, tietoturvaloukkauksen todennäköiset seuraukset sekä toimenpiteet, joihin Pohjanmaan hyvinvointialue on ryhtynyt tai ryhtymässä.

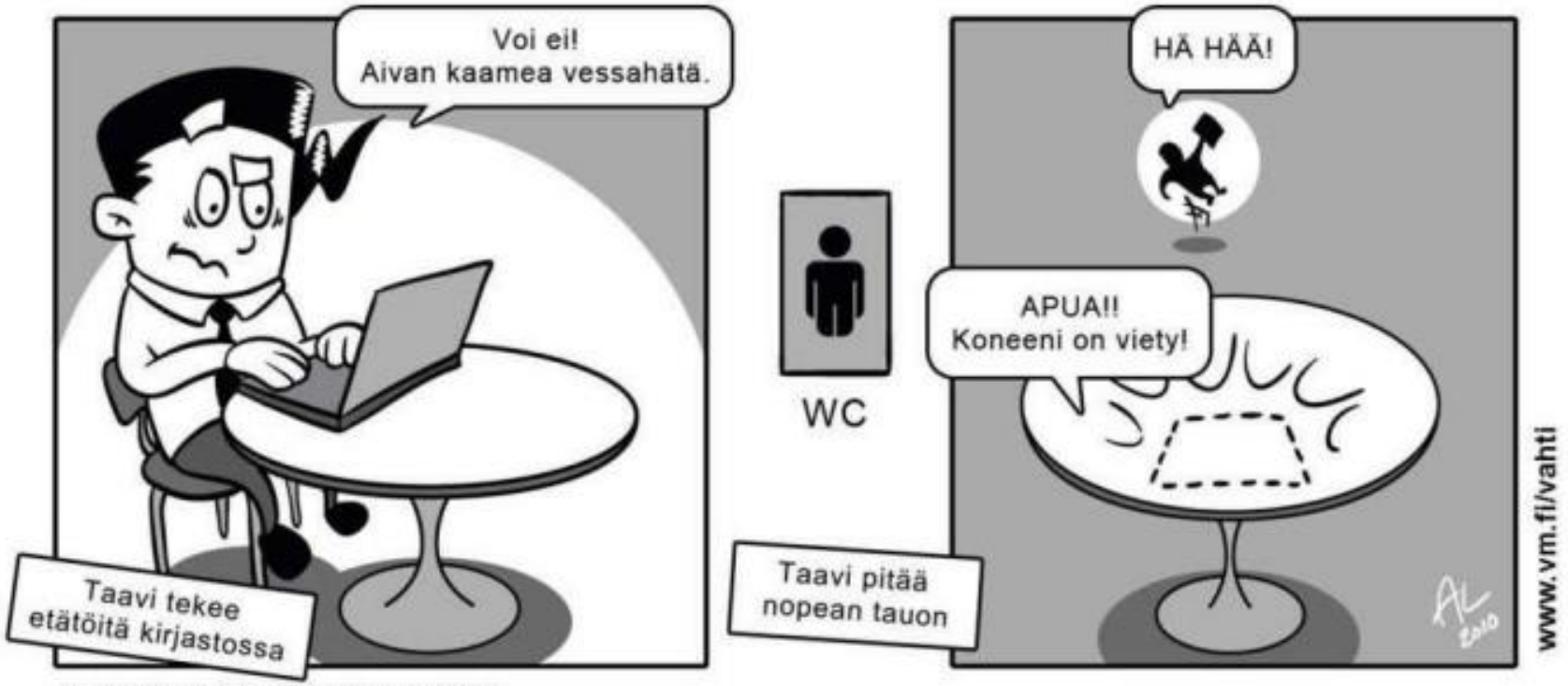
Sisällytä ilmoitukseen ainakin seuraavat tiedot:

- selkeä kuvaus henkilötietojen tietoturvaloukkauksesta
- anteeksi pyyntö
- yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa asiasta esim. tietosuojavastaavan nimi
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on jo toteuttanut; tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Ilmoitusta ei vaadita, jos

- Pohjanmaan hyvinvointialue on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja niitä on sovellettu henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin (erityisesti niitä, joiden avulla henkilötiedot muutetaan ulkopuolisille mahdottomiksi ymmärtää, kuten salausta)
- Pohjanmaan hyvinvointialue on tehnyt jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu
- Ilmoituksen tekeminen vaatisi kohtuutonta vaivaa, koska ei esimerkiksi tiedetä, keitä rekisteröidyt ovat. Asiaa arvioidaan riskien mukaan. Jos rekisteröityihin ei voida ottaa yhteyttä henkilökohtaisesti, on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröityjä informoidaan yhtä tehokkaalla tavalla.

Jos Pohjanmaan hyvinvointialueen henkilökunta ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä.



ÖSTERBOTTENS VÄLFÄRDSOMRÅDE | POHJANMAAN HYVINVOINTIALUE

TACK
KIITOS