KEUSOTE
Keski-Uudenmaan hyvinvointialue

TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

-turvallisuusajattelu lähtee meistä itsestä-

Sote ihmisen kokoiseksi.

19.1.2024
Tietoturvapäällikkö Timo Pirtilä
Tietosuojavastaava Satu Jokinen

Sisällys

1. Johdanto

Tietoturva- ja tietosuojapolitiikan tarkoitus

Tietoturvan ensisijaisena tarkoituksena on hyvinvointialueen vastuulla olevien toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tarkoituksenmukainen ja tehokas tietoturva mahdollistaa hyvinvointialueen toimintoihin liittyvien ICT-ratkaisujen käytettävyyden, prosesseissa ja palveluissa käytettävien tietojen eheyden sekä luottamuksellisuuden kaikissa olosuhteissa. Tämän politiikka luo perustan hyvinvointialueen tietojärjestelmien ja tietojenkäsittelyn turvallisuuden varmistamiselle.

Hyvinvointialueella asiakastietojen ja muiden digitaalisten toimintojen tuottaman ja käsittelemän datan turvaaminen on olennainen osa vastuullista toimintaa, jota sekä asiakkaamme että yhteistyökumppanimme edellyttävät hyvinvointialueelta. Digitaalisuuden kasvu merkitsee sitä, että tietoturvallisuutta säännellään enenevässä määrin myös lainsäädännöillä.

Hyvinvointialueen strategiasta johdetut vaatimukset politiikalle

Keski-Uudenmaan hyvinvointialueen strategian ja palvelustrategian ytimessä on hyvinvoiva asukas. Uusi strategia ohjaa hyvinvointialueen toimintaa rohkeaksi uudistajaksi, jossa toimintamalleja kehitetään ja uudistetaan yhdessä asiakkaiden ja yhteistyökumppaneiden kanssa.

Kuva 1. Ote Keusoten strategiasta

Keusoten strategia antaa suuntaviivoja myös Tietoturva- ja tietosuojapolitiikalle erityisesti seuraavien kohtien osalta:

- **Meidät tunnetaan rohkeina uudistajina**: Uusien teknologioiden ja toimintatapojen käyttöönotto edellyttää nopeaa uusien asioiden omaksumista ja päätöksentekoa myös tietoturvan ja tietosuojan osalta. Riskienhallinta on ensisijaisen tärkeää, jossa sisäinen ja ulkoinen yhteistyö korostuu. Esimerkkejä uuden teknologian käytöstä ovat mm. tekoäly, some-palvelut sekä pilvipalvelut.

Kuva 2. Eräitä huomioitavia asioita pilvipalvelujen käyttöä harkittaessa

- **Tarjoamme tutkitusti vaikuttavat palvelut:** Tiedolla johtaminen nousee palvelujen tarjoamisessa ja kehittämisessä erittäin keskeiseksi tekijäksi.

Tietojen on oltava suojattuja, käytettävissä ja oikeita – eli kaikki tietoturvan osa-alueet huomioitu.

- **Lähellä ja läsnä – oikea-aikaisesti:** Palveluja tarjotaan yhä enemmän asiakkaiden luona. Myös palveluiden monikanavaisuus sekä omaisten huomioiminen kasvaa. Nämä tekijät tulee ottaa huomioon myös tietoturvan ja tietosuojan osalta.

Kuten sosiaali- ja terveydenhuollon, niin myös tietoturvan ja tietosuojan riskienhallinta on haastavaa, sillä yksinkertaisia ratkaisuja ei ole aina löydettävissä. Riskienhallinnan johtaminen, epävarmuuden sietäminen ja riittävä viestintä ovat avainasemassa varautumisessa. Visiomme ’Parasta jokaiselle’ edellyttää palveluidemme tietoturvan ja tietosuojan toteutumista kaikissa tiedon käsittelyvaiheissa.

Yleisesti toimialallamme, jossa käsitellään erittäin laajasti arkaluonteista ja salassa pidettävää sosiaali- ja terveydenhuollon tietoa, asettaa tietoturvalle ja tietosuojalle suuria haasteita.

On ratkaisevan tärkeää, että jokainen organisaation työntekijä kaikilla tasoilla omaksuu turvallisuuskulttuurin ja sitä kautta turvallisuusajattelun. Turvallisuusajattelua ei voi tilata ’avaimet käteen periaatteella’, vaan turvallisuusajattelu on sisäänrakennettua, tietoista toimintaa, mikä lähtee meistä jokaisesta itsestä.

2. Digitaalisen turvallisuuden osa-alueet

Digitaalinen turvallisuus koostuu seuraavista viidestä osa-alueesta:

1) **Johtaminen ja riskienhallinta**
2) **Jatkuvuudenhallinta**
3) **Kyberturvallisuus**
4) **Tietosuoja**
5) **Tietoturva**

Digitaalisen turvallisuuden toteutusalueet ulottuvat myös digitaalisen maailman ulkopuolelle.

Kuva 3 Digitaaliset turvallisuuden osa-alueet (Lähde: Digi- ja väestövirasto)

Keusoten tietoturva- ja tietosuojapolitiikka painottuu erityisesti kyberturvallisuuteen, tietoturvaan ja tietosuojaan. Johtaminen ja riskienhallinta sisältyy Keusoten turvallisuus- ja riskienhallintapolitiikkaan sekä jatkuvuudenhallinta valmiussuunnitelmaan. Seuraavassa on avattu nämä kolme keskeistä käsitettä:

Tietoturvalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.

Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua.

Tietosuojalla tarkoitetaan järjestelyjä, joilla varmistetaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

3. Uhkien tunnistaminen ja ennaltaehkäisy

Varautumisen kannalta on välttämätöntä tiedostaa tietoturvaan ja tietosuojaan kohdistuvat mahdolliset uhat sekä keinot niiltä suojautumiseen. Hyvinvointialueen **valmiussuunnitelma** tukee häiriöistä ja poikkeusoloista toipumista.

Uhkakartat ja yhteistyö
Keusote käyttää Euroopan Kyberturvallisuusviraston (ENISA) uhkakarttaa erilaisten kyberuhkien tunnistamiseen. Operatiiviset uhkatiedot saadaan lisäksi Kyberturvallisuuskeskukselta. Sote-sektorin tietoturvayhteistyöhön osallistutaan Kyberturvallisuuskeskuksen koordinoimissa verkostoissa.

Kuva 4. Euroopan kyberturvallisuusviraston uhkakartta

Yleisimmät Keusoten tietoturva- ja tietosuojapoikkeamat ovat huolimattomuudesta, tietämättömyydestä ja erilaisista laite/ohjelmistovioista sekä tietoverkko/sähkökatkoksista johtuvia. Näitä pyritään ennaltaehkäisemään henkilökunnan osaamistasoa nostamalla, kyvykkäiden yhteistyökumppanien valinnalla sekä kumppanien palvelutason valvonnalla.

Tietojenkalastelu on yleisin Keusoteen kohdistuva tietoturvauhka. Kalastelua suoritetaan monissa eri muodoissa kuten esimerkiksi sähköpostilla, tekstiviesteillä, sosiaalisessa mediassa, nettisivuilla, puhelimella sekä kasvokkain. Tietojenkalastelun kohteena ovat yleensä raha, luottokorttitiedot, salasanat sekä henkilötiedot.

Hyvinvointialueen tulee olla myös varautunut tietojärjestelmiin ja tietoverkkoihin kohdistuviin kyberiskuihin. Taustalla voi olla poliittisia, taloudellisia tai pelkkään vahingontekoon liittyviä vaikuttimia tai edellä mainittujen yhdistelmiä. Mikäli taustalla on valtiollisia toimijoita, niiden resurssit voivat olla lähes rajattomat mikä asettaa uhkien torjunnalle merkittäviä haasteita.

Kyberiskuja suunnittelevat ovat voineet murtautua tietotekniseen ympäristöön paljon aikaisemmin kuin iskun tekoajankohta ja iskun tekijä voi olla eri taho kuin sinne alun perin murtautunut (eli tietoturva-aukkokin on kauppatavaraa). Kyberisku voi mm. estää tietojärjestelmän toiminnan, tietojärjestelmien tietoja voidaan muuttaa tai poistaa, tietojärjestelmät voidaan kryptata ja vaatia suuria rahasummia niiden palauttamiseen tai tietojärjestelmissä olevia arkaluonteisia henkilötietoja voidaan julkaista Internetissä tai ns. pimeässä netissä. Tietojärjestelmiin ja tietoliikenneverkkoihin voi kohdistua myös palvelunestohyökkäyksiä.

4. Tietoturva- ja tietosuojatavoitteet

Yksityisyydensuoja ja henkilötietojen suoja ovat jokaisen perusoikeus. Keusoten tavoitteena on edistää hyvää tietojenkäsittelytapaa ja varmistaa tietojenkäsittelyn turvallisuus, sekä tehtävien sujuva ja häiriötön toiminta. Tietoja käsitellään niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen.

Hyvän tietosuojan tason saavuttamiseksi jokaisen tietoa käsittelevän henkilön tulee ymmärtää tietojen käsittelyn periaatteet: mitä tietoa saa käsitellä, missä tarkoituksessa ja milloin tietoa saa käsitellä sekä mitkä ovat rekisteröidyn oikeudet.

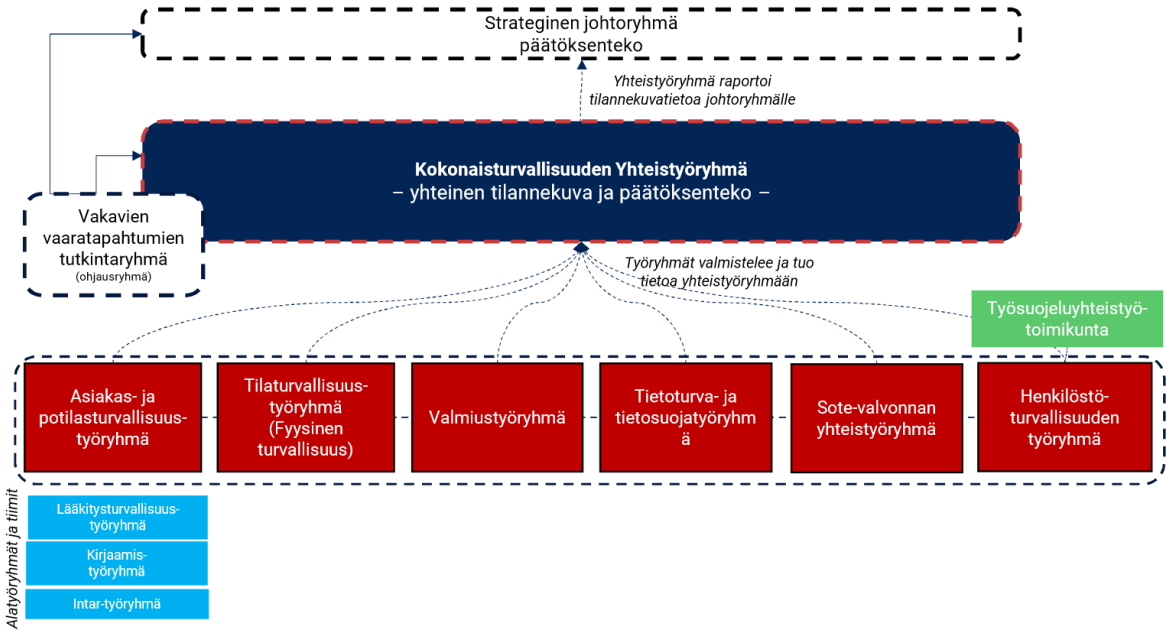
On ensiarvoisen tärkeää, että asiakas- ja potilastiedot ovat sekä suojattuina että käytettävissä kaikissa tiedon käsittelyvaiheissa. Myös tiedolla johtamisen kannalta tietoturva ja tietosuoja ovat elintärkeitä. Näiden seikkojen perusteella on määritelty tietoturvan ja tietosuojan tavoitteet.

Tietoturvan ja tietosuojan tavoitteina:

- suojata kaikki Keusoten käsittelemät luottamukselliset tiedot
- tiedon saatavuus ja oikeellisuus
- vakavien tietoturva- ja tietosuojapoikkeamien minimointi
- tietosuojan osoitusvelvollisuuden toteutuminen
- riittävä käyttölokivalvonta
- valvottu ja raportoitu tietotekninen ympäristö
- kattavat tietoturvaan, tietosuojaan sekä tiedonhallintaan liittyvät lakisääteiset arvioinnit (DPIA eli vaikutustenarvioinnit, muutosvaikutukset, riskit, auditoinnit)
- henkilöstön tietoturva- ja tietosuojaosaamisen varmistaminen
- lakien ja määräysten noudattaminen
- varmistaa rekisteröityjen oikeuksien toteutuminen

5. Tietoturvan ja tietosuojan organisointi

Tietoturvan- ja tietosuojan varmistaminen on osa Keusoten kokonaisturvallisuuden hallintaa. Kokonaisturvallisuuttaa johtaa Keusoten johto kokonaisturvallisuuden yhteistyöryhmän tuottaman informaation avulla. Yhdeksi alatyöryhmäksi on nimetty tietoturva- ja tietosuojatyöryhmä, jonka puheenjohtajana toimii tällä hetkellä tietoturvapäällikkö.



Kuva 5. Turvallisuuden työryhmät Keusotessa

Tietoturva- ja tietosuojatyöryhmän asema sekä tehtävät on asetettu ryhmän perustamisen yhteydessä seuraavasti:

Tietoturva- ja tietosuojatyöryhmä toimii valmistelevana työryhmänä tietosuoja ja tietoturva-asioille. Päätöstä vaativat asiat viedään asiasta riippuen kokonaisturvallisuuden yhteistyöryhmälle, rekisterinpitäjälle tai hyvinvointialuehallitukselle.

Tietoturva- ja tietosuojatyöryhmän tehtävänä on mm:

- Tietosuojaan ja tietoturvaan liittyvien asioiden käsittely, kommentointi ja lausuntojen antaminen
- Organisaation tietosuojan- ja tietoturvallisuuden edistäminen ja kehittäminen
- Poikkeamien/riskien käsittely (HaiPro)
- Vaikutustenarvioinnit (DPIA)
- Valmistelee tietosuojaan ja tietoturvaan liittyviä organisaation ohjeita ja linjauksia.
- Reagoi ajankohtaisiin tietosuojaan ja tietoturvaan liittyviin asioihin, erityisesti uuteen lainsäädäntöön.
- Tietosuojan/-turvan koulutusten ja koulutusohjelman laadinta
- Työryhmä viestii monikanavaisesti omasta toiminnastaan henkilöstölle

Tietosuojan ja tietoturvan hallinnassa toteutetaan **sisäänrakennettua ja oletusarvoista tietosuojan periaatetta**. Tämä tarkoittaa sitä, että tietosuojaan ja tietoturvaan liittyvät näkökohdat otetaan jo varhaisessa vaiheessa huomioon, esimerkiksi hankinnoissa sekä henkilötietojen käsittelyyn liittyvien toimintaprosessien ja siihen liittyvien teknologioiden esikartoituksessa, suunnittelussa, kehittämisessä ja toteuttamisessa.

Hyvinvointialueen tietoturva- ja tietosuojatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- hyvinvointialuetta velvoittavat lait ja asetukset
- viranomaismääräykset, ohjeet ja suositukset
- ISO 27001 -tietoturvan hallintamalli
- ISO 27002 -tietoturvakontrollit
- tiedonhallintalautakunnan suositukset
- tietosuojavaltuutetun toimiston ohjeet
- hyvinvointialueen omat strategiat ja niistä johdetut vaatimukset

Valitsemalla **ISO 27001 -hallintamallin** sovellettavaksi hyvinvointialueellamme voidaan mahdollisimman hyvin varmistaa tietoturvan ja tietosuojan toteutuminen.

Hyvinvointialueen tietoturvaan ja tietosuojaan sovellettavasta lainsäädännöstä, viranomaismääräyksistä, ohjeista, suosituksista sekä hyödyllisistä linkeistä pidetään yllä erillistä listausta.

Tietoturvan ja tietosuojan toteuttaminen varmistetaan käyttämällä tarvittavia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi koko niiden elinkaaren ajan.

Teknisiä ja organisatorisia toimia ovat mm:

- tietosuojavastaavan ja tietoturvapäällikön nimeäminen
- tietosuojan ja tietoturvan dokumentointi
- henkilöstön kouluttaminen
- ohjeiden, linjausten ja määräysten laatiminen
- ostopalveluita koskevan tietosuojan ja tietoturvan hallinta (tietosuojasopimus, henkilötietojen käsittelyohje, henkilötietojen käsittelytoimien kuvaus, sopimuksen tietoturvaliite)

Keusote (hyvinvointialue) on linjannut tietoturvan ja tietosuojan vastuut seuraavasti hallintosäännössä:

- **Aluehallitus** vastaa tiedonhallinnasta ja toimii rekisterinpitäjänä sekä vastaa että hyvinvointialue täyttää tietosuojavelvoitteet ja valvoo niiden toteuttamista.

- **Tiedonhallintaa johtava viranhaltija (hyvinvointialueen johtaja)** vastaa tietoturvasta

Delegointisäännön mukaan:

- **Tieto- ja digijohtaja** vastaa tietoturvasta
- **Tietoturvapäällikkö** vastaa tietoturvan hallinnasta sekä tietoturva- ja tietosuojapolitiikan laatimisesta
- **Hallintojohtaja** vastaa tietosuojasta
- **Hallintopäällikkö** vastaa tietosuojan kehittämisestä ja koordinoinnista

EU:n tietosuoja-asetus määrittää tietosuojavastavan tehtävät:

Tietosuojavastaava

- opastaa henkilökuntaa henkilötietojen käsittelyssä
- seuraa organisaation henkilötietojen lainmukaista käsittelyä
- neuvoo ja valvoo henkilötietojen tietosuojan vaikutustenarviointeja (DPIA)
- tekee yhteistyötä valvontaviranomaisten ja sidosryhmien välillä
- on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa
- tehtävässään riippumaton toimija

6. Henkilöstön osaaminen ja tietoisuuden ylläpito

Osaaminen muodostaa pohjan hyvälle työn hallinnalle, myös tietoturvan ja tietosuojan osa-alueilla. Jokainen uudessa tehtävässä aloittava työtekijä tulee esihenkilön vastuulla perehdyttää kuntayhtymän perehdytyskäytäntöjen mukaisesti myös tietoturvan ja tietosuojan perusteisiin sekä niiden toteuttamiseen hänen omissa työtehtävissään.

Jokaisen työntekijän tulee sitoutua organisaation tietosuoja- ja tietoturvaperiaatteisiin. Tämä osoitetaan salassapito- ja tietoturvallisuussitoumuksella. Esihenkilöiden vastuulla on, että työntekijät suorittavat tietoturvan ja tietosuojan perusteista verkkokoulutuksen ja –testin sekä osallistuvat vuosittaisiin tietosuojakoulutuksiin. Lisäksi tietoturva- ja tietosuojaohjeet ovat kaikkien työntekijöiden saatavilla verkkosivuilla, intrassa (Keunetissa) sekä Navisec Flex -portaalissa.

Tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

7. Rekisterinpitäjän velvollisuudet ja käsittelijän vastuut

Keusoten rekisterinpitäjänä toimii aluehallitus. Rekisterinpitäjällä on ylin vastuu rekistereissään olevista henkilötiedoista, sekä niiden käsittelyn suunnittelusta ja toteutuksesta. Rekisterinpitäjällä on mm. velvollisuus määritellä henkilötietojen käsittelyperusteet sekä informoida rekisteröityjä heidän henkilötietojensa käsittelystä. Lisäksi rekisterinpitäjän on pystyttävä osoittamaan, että henkilötietojen käsittelyssä noudatetaan tietosuojalainsäädäntöä. Rekisterit tulee dokumentoida Selosteeseen käsittelytoimista. Lisäksi asiakkaiden informointia varten on laadittu tietosuojaselosteita, jotka ovat nähtävillä verkkosivuilla.

Tietosuoja tulee huomioida rekisterinpitäjän ja käsittelijän (esim. järjestelmän toimittajat, muut ostopalvelut) välisissä sopimuksissa EU-yleisen tietosuoja-asetuksen (GDPR) mukaisesti. Henkilötietojen käsittelyä ulkoistettaessa henkilötietojen käsittelijän vastuu tulee määritellä kirjallisella sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään. Sopimuksessa on määriteltävä vähintään käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä rekisterinpitäjän velvollisuudet ja oikeudet.

Keusote on laatinut ostopalveluita varten henkilötietojen käsittelysopimuksen, palvelukuvauksen sekä ohjeen henkilötietojen käsittelystä. Näihin tulee perehtyä jo kilpailutusvaiheessa. Katso Keunetista: https://keusote.sharepoint.com/sites/keunet-turvallisuus/sitepages/Hankinnat-ja-kilpailutukset.aspx

8. Tietoturvan ja tietosuojan ilmoitusvelvollisuus

Tietoturvaloukkaus on oikeudeton puuttuminen tietoon tai tietojärjestelmiin. Yleisempiä tietoturvaloukkauksia on käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palveluestohyökkäys, tietojenkalastelu, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

Henkilötietojen tietoturvaloukkauksella (tietosuojaloukkaus) tarkoitetaan tapahtumaa, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka oikeudeton pääsy tietoihin.

Henkilötietojen tietoturvaloukkauksen tapahtuessa rekisterinpitäjä, kuten Keusote, on velvollinen ilmoittamaan poikkeamasta ilmoituskynnyksen ylittyessä valvontaviranomaiselle ja tarvittaessa rekisteröidylle. Ilmoituskynnys viranomaiselle täyttyy tilanteissa, jossa loukkaus todennäköisesti aiheuttaa riskin henkilön oikeuksiin ja vapauksiin ja rekisteröidylle, jos loukkaus aiheuttaa todennäköisesti korkean riskin henkilöiden oikeuksille ja vapauksille.

Ilmoitus tietosuojavaltuutetulle tulee tehdä 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle loukkaus tulee ilmoittaa ilman aiheetonta viivytystä.

Myös henkilötietojen käsittelijän (sopimussuhteessa olevat) on ilmoitettava Keusotelle havaitsemastaan henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä.

Riippumatta siitä, onko tietoturvaloukkauksesta ilmoitettava, on rekisterinpitäjän dokumentoitava kaikki tietoturvaloukkaukset. Jokainen on velvollinen viipymättä ilmoittamaan epäilemistään tai havaitsemistaan tietoturvaloukkauksista erillisen ohjeistuksen mukaisesti.

Keusote on ohjeistanut loukkausten tekemisen HaiPro tietosuoja/turvailmoitusten kautta (tarkemmin asiasta Tietoturvaohjeessa).

Viranomaisille ilmoittamisessa tulee huomioida Keusoten ohje rikosilmoituksen tekemisestä poliisille. Poliisin lisäksi tapauksesta riippuen voidaan tehdä ilmoituksia mm. Tietosuojavaltuutetun toimistolle, Kyberturvallisuuskeskukselle, Aluehallintovirastolle (AVI) ja/tai Sosiaali- ja terveysalan lupa- ja valvontavirastolle (Valvira).