Yksinyrittäjän ja mikroyrityksen

KYBER- JA TIETOTURVA OPAS

Kyberturvan abc yrittäjille -hanke

Euroopan unioni
Euroopan sosiaalirahasto

Vipuvoimaa EU:lta 2014–2020

Elinkeino-, liikenne- ja ympäristökeskus

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Sisällys

Johdanto

Opas on tarkoitettu sosiaali- ja terveysalalla toimiville yrittäjille. Nimensä mukaan sen pääaiheena on tietoturvasuunnitelma. Kappaleissa käsitellään muun muassa sitä, mitä asioita tietoturvasuunnitelma sisältää ja minkä takia se tulee laatia. Oppaassa käsitellään myös aiheeseen tiiviisti liittyvää asiakastietolakia ja EU:n tietosuoja-asetusta, josta myöhemmin puhutaan GDPR:nä.

Oppaan tarkoituksena on antaa yleiskäsitys aiheista. Joidenkin osioiden loppuun on lisätty linkkejä, joista pääsee halutessaan lukemaan aiheesta lisää.

Kyberturvan abc yrittäjille -hanke on julkaissut myös yleisen oppaan, josta löytyy käytännön ohjeita esimerkiksi varmuuskopiointiin ja haittaohjelmilta suojautumiseen liittyen.

Yksinyrittäjän ja mikroyrityksen kyber- ja tietoturva oppaan löydät täältä: https://www.xamk.fi/wp-content/uploads/2022/09/kyberturvaopas_23.9.2022.pdf

Hanketta rahoittaa Hämeen ELY-keskus Euroopan sosiaalirahastosta (ESR).

Hanketiimi

Jenna Ruuska, kyber- ja tietoturvan asiantuntija (sote- ja hyvinvointiala)

Janine Klauenbösch, kyber- ja tietoturvan asiantuntija (sote- ja hyvinvointiala)

Heidi Ilmonen, SoteTraining (Salus Qualitas Consulting Oy), yritysneuvoja, kouluttaja, yrittäjä

Avainkäsitteitä

Kyberhygienia: Tarkoittaa hyviä kyberturvallisuuteen liittyviä toimintatapoja, jotka parantavat kyberturvaa. Näitä tapoja voivat olla esimerkiksi uniikkien salasanojen käyttö eri palveluissa tai se, että lukitsee tietokoneensa siltä poistuessaan.

Kyberturva: On turvallisuuden osa alue, jolla pyritään turvaamaan sähköiset laitteet sekä yhteydet laitteista ulos ja sisäänpäin. Näillä keinoilla pyritään edistämään laitteiden jatkuvuutta, jotta kaikki toimisi suunnitellusti ja laitteet pysyisivät toiminnassa häiriöistä riippumatta.

Rekisteröity: Henkilö, jota henkilötieto koskee.

Rekisterinpitäjä: Henkilö, yritys, viranomainen tai yhteisö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Tietosuoja: Turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen aina, kun henkilötietoja käsitellään. Osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tietoturva: Pyritään ylläpitämään tiedon saatavuutta, luottamuksellisuutta ja eheyttä. Nämä tiedot ilmentyvät digitaalisina tallenteina, fyysisinä tallenteina sekä ihmisten, kuten työntekijöiden, tietämyksenä. Tietoturva koskee tiedon suojaamista myös sen siirtämisen aikana.

EU:n yleinen tietosuoja-asetus

Suomen yrittäjät ovat kirjoittaneet hyvän oppaan tietosuojasta. Tältä sivulta voit tilata Yrittäjän tietosuojaoppaan: https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

GDPR:n on oman yrityksen etu pitää asiakkaiden tiedot turvassa ja sen perusteella saada luottamusta asiakkailta sekä säästää rahaa.

Mitä GDPR tarkoittaa?

GDPR on lyhenne sanoista **G**eneral **D**ata **P**rotection **R**egulations. Suomeksi se tarkoittaa EU:n yleistä tietosuoja-asetusta. GDPR on voimassa kaikissa EU-maissa ja sen tarkoitus on säädellä henkilötietojen käsittelyä. GDPR:n avulla EU on halunnut parantaa henkilötietojen suojaa ja tietosuojaoikeuksia. Laki kehitettiin vastaamaan uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin. Suomessa Tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädäntöä.

Mikä on henkilötieto?

Tiettyyn henkilöön (asiakkaaseen/työntekijään/yhteistyökumppaniin) liitettävissä oleva mikä tahansa tieto, kuten yhteystiedot. Ajattele henkilötietoja kuin palapeliä. Yksi pala ei välttämättä kerro paljon, mutta yhdistettynä ne paljastavat elävän kuvan elämästäsi.

Esimerkkejä henkilötiedoista:

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.fi
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot (esim. matkapuhelimen paikannustiedot)

Suorat tunnisteet sisältävät:

- henkilön koko nimi
- henkilötunnus
- henkilönimen mukainen sähköpostiosoite
- biometriset tunnisteet

Epäsuorat tunnisteet sisältävät:

- sukupuoli
- ikä
- ammatti

GDPR:n keskeiset säännöt

GDPR:n siirtymäaika loppui 25. toukokuuta 2018. GDPR käsittelee tietosuojaperiaatteita, vastuullisuutta, tietosuojaa, sitä milloin sinulla on lupa käsitellä tietoja, suostumusta, tietosuojavastaavia ja ihmisten yksityisyysoikeuksia.

Vaikka GDPR on EU direktiivi, se velvoittaa organisaatioita ja yrityksiä missä tahansa, kun ne keräävät tietoja EU:n alueella asuvista ihmisistä.

Kun käsittelet tietoja, sinun on tehtävä se GDPR:n seitsemän periaatteen mukaan.

1. Lainmukaisuus, asianmukaisuus ja läpinäkyvyys.
2. Käyttötarkoituksen vastattava rekisterissä ilmoitettua tarkoitusta.
3. Tietojen olennaisuus ja tarpeellisuus.
4. Tietojen käsittelyn oltava turvallista ja luottamuksellista.
5. Tietojen oltava täsmällisiä ja tarvittaessa päivitettyjä.
6. Tietojen säilytys ja käsittely vain niin kauan kuin on tarpeellista.
7. Näiden periaatteiden noudattaminen on voitava osoittaa dokumentaation avulla. Yleensä keskeinen henkilötietojen käsittelyä kuvaava dokumentti on tietosuojaseloste.

Milloin minulla on lupa käsitellä tietoja?

Artikkelista 6 löytyy tiedot siitä, milloin saat käsitellä tietoja. Alla olevassa listassa löytyy 6 esimerkkiä tietojen käsittelyyn liittyen.

1. Tietty henkilö on antanut sinulle nimenomaisen, yksiselitteisen suostumuksensa tietojen käsittelyyn (esim. markkinointisähköpostitilaus).

2. Käsittely on tarpeen sopimuksen toteuttamiseksi / valmistautumiseksi tietyn henkilön kanssa. (esim. vuokrasopimus).
3. Sinun on käsiteltävä tietoja noudattaaksesi lakisääteisiä velvoitteitasi (esim. tuomioistuimen määräys tai osakeyhtiölain edellyttämä osakasluettelo).
4. Sinun on käsiteltävä tietoja pelastaaksesi jonkun hengen. (esim. ensihoitajat)
5. Käsittely on tarpeen yleisen edun tai julkisen vallan edellyttämän tehtävän suorittamiseksi (esim. olet yksityinen jätehuoltoyritys).
6. Sinulla on oikeutettu etu käsitellä jonkun henkilötietoja. Esimerkiksi asiakas on halunnut tilata sinulta jotakin verkkokaupastasi tai työnantajavelvoitteista huolehtiminen.

Kun olet määrittänyt tietojenkäsittelysi laillisen perustan, sinun on laadittava yrityksellesi tietosuojaseloste, joka sinun tulee saattaa niiden henkilöiden tietoon ja hyväksyttäväksi, joiden tietoja käsittelet.

Jos päätät muuttaa perustelujasi ja tietosuojaselostettasi myöhemmin, sinulla on oltava hyvä syy. Dokumentoi tämä syy ja ilmoita siitä henkilöille, joita muutos koskee. Näitä ilmoituksia ovat ne ilmoitukset, joita esimerkiksi ajoittain saat some-tileiltäsi (Voidaksesi jatkaa palvelun käyttämistä, sinun tulee hyväksyä uudet ehtomme tms.).

Suostumus

Suostumuksen suhteen on laadittu tiukat säännöt.

- Suostumuksen on oltava ”vapaasti annettu, täsmällinen, tietoinen ja yksiselitteinen”.
- Suostumuspyyntöjen on oltava selvästi erotettavissa muista asioista.
- Suostumuspyyntöjä on esiteltävä selkeällä muodolla ja selkeällä kielellä.
- Asiakkaat voivat peruuttaa antamansa suostumuksen, mikäli tietojen käsittelyyn ei ole perusteltua syytä.
- Sinun on kunnioitettava heidän päätöstään peruuttaa suostumuksensa. Et voi muuttaa käsittelyn oikeudellista perustetta johonkin muuhun perusteeseen.
- Alle 13-vuotiaat voivat antaa suostumuksen vain vanhemman luvalla.
- Sinun on säilytettävä suostumuksesta asiakirjatodiste.

Rekisteri, rekisterinpitäjä, henkilötietojen käsittelijä

Jokainen yritys, joka säilyttää henkilötietoja, on rekisterinpitäjä. Tämä tarkoittaa käytännössä jokaista yritystä, josta löytyy edes puhelin, jossa on asiakkaiden tietoja.

Rekisteri on mikä tahansa kokoelma henkilötietoja, vaikka ne sijaitsisivat eri paikoissa (esim. sähköpostissa, kännykkäsi yhteystiedoissa ja yrityksen työntekijöiden käytössä olevassa jaetussa Google-taulukossa sekä kaapin perukoille unohdetussa asiakkailta kerätyssä käyntikorttinivaskassa).

Henkilötietojen käsittelijä on yrityksen alihankkija/palveluntoimittaja, joka käsittelee yrityksen puolesta henkilötietoja (esim. työterveys ja tilitoimisto).

Ihmisten yksityisyysoikeudet

Ihmiset lainaavat tietojaan yrityksille. Organisaation on tärkeää ymmärtää heidän oikeutensa.

Asiakkaan (rekisteröidyn) oikeudet

- Saada läpinäkyvästi tietoa henkilötietojensa käsittelystä rekisterinpitäjän toimesta.
- Saada pääsy omiin henkilötietoihinsa. Varmista, että työntekijät ymmärtävät, että esimerkiksi haasteellista asiakasta ei voi kuvata värikkäästi asiakasrekisterissä.
- Oikeus saada virheelliset/puutteelliset korjattua.
- Oikeus tulla unohdetuksi. Tämä tarkoittaa, että organisaatio tai yritys poistaa heidän tietonsa kokonaan tietojärjestelmistä, niiltä osin kuin se on mahdollista (esimerkiksi lakisääteinen velvoite voi estää tämän joiltakin osin).
- Oikeus rajoittaa omien tietojensa käsittelyä.
- Oikeus saada omat tietojen siirretyksi järjestelmästä toiseen.
- Asiakkaalla on oikeus vastustaa henkilötietojensa käsittelyä.
- Asiakkaalla on oikeus olla joutumatta perusteetta automaattisen päätöksenteon kohteeksi.

Arkaluonteiset tiedot

Arkaluonteisia tietoja saa kerätä vain, mikäli

- rekisteröity on nimenomaisesti suostunut tähän;
- rekisterinpitäjän tulee tehdä näin lain vaatimuksesta (esim. sosiaalisen suojelun ala);
- se on tarpeen rekisteröidyn elintärkeiden etujen suojelemiseksi (esim. tiedottomuuden vuoksi);
- henkilö on itse tehnyt tiedoista nimenomaisesti julkisia;
- Käsittely tapahtuu asianmukaisin suojatoimin ammattiliiton tai poliittisen, filosofisen, uskonnollisen säätiön tai voittoa tavoittelemattoman yhteisön toimesta.

Arkaluonteisia tietoja ovat:

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettiset / biometriset tiedot, jotka on kerätty henkilön tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

Mitä minun pitää huomioida omassa yrityksessäni?

GDPR:n mukaan sinun tulee toimia seuraavasti:

- Henkilötietojen käsittelyn minimoiminen. Käsittele juuri niitä tietoja kun tarvitset, älä kerää liikaa tietoja.
- Henkilötietojen pseudonymisointi (tarkoittaa henkilötietojen käsittelyä siten, että niitä ei voi enää yhdistää tiettyyn henkilöön ilman lisätietoja) mahdollisimman pian.
- Läpinäkyvyys henkilötietojen käyttöön liittyen. Kerro asiakkaille, mihin tarkoitukseen keräät heidän tietojansa.
- Tietojenkäsittelyn seuranta.
- Antaa henkilötietojen käsittelijälle mahdollisuuden luoda ja parantaa suojausominaisuuksia.
- Tuotetta kehitettäessä on otettava huomioon tietosuojalait.
- Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olisi otettava huomioon myös julkisessa tarjouskilpailussa.
- Ylläpidä yksityiskohtaista dokumentaatiota keräämistäsi tiedoista.
- Mihin tarvitset niitä tietoja? Missä niitä säilytetään? Kuka on niistä vastuussa?
- Kouluttaa työntekijäsi siten, että he käyttävät hyvää kyberhygieniaa työskennelleessä.
- Tee tietojenkäsittelysopimuksia kolmansien osapuolten kanssa, jotka käsittelevät sinun kerättyjä asiakastietojasi.
- Jos laki vaatii (esim. SOTE-alalla tai muuten, kun yrityksessä tehdään laajaa henkilötietojen käsittelyä) nimitä tietosuojavastaava.
- Käytä hyvää suojausta (esim. ota kaksivaiheinen tunnistautuminen eli autentikointi käyttöön.)

- Seuraa säännöllisesti, onko kaikki tietosuojaan liittyvä toiminta ja dokumentaatio ajan tasalla.

Mitä rangaistuksia GDPR:n rikkomisesta määrätään?

Jos yritys tai organisaatio ei noudata yleistä tietosuoja-asetusta, voidaan rangaistuksesi antaa sakkoja, joiden suuruus voi olla jopa 20 miljoonaa euroa tai 4 % vuosittaisesta liikevaihdosta.

Esimerkkiä rangaistuksen saaneista yrityksistä Suomessa:

- Yksityishenkilö – 500 euroa

Yksityishenkilö oli asentanut kiinteistölleen valvontakamerat, jotka tallensivat myös naapurikiinteistöt.

- Matkatoimisto – 6 500 €

Asiakkaiden täyttämät viisumihakemuslomakkeet olivat julkisesti saatavilla matkatoimiston verkkopalvelimella. Tämä lomake sisälsi muun muassa rekisteröityjen nimet, passin numerot ja yhteystiedot.

- Vastaamo – 608 000 €

Yritys rikkoi yleistä tietosuoja-asetusta laiminlyömällä henkilötietojen turvalliseen käsittelyyn sekä tietoturvaloukkauksesta ilmoittamiseen liittyviä velvollisuuksiaan. Rekisterinpitäjä ei ollut myöskään toteuttanut asianmukaisia toimenpiteitä henkilötietojen käsittelyn turvaamiseksi.

- Polar – 122 000 €

Yritys oli pyytänyt suostumuksen yleisesti terveyttä koskevien tietojen käsittelyyn, mutta ei ollut yksilöinyt tietoja, joita se keräsi ja käsitteli.

Pyydetty suostumus ei täyttänyt tietosuoja-asetuksen vaatimuksia, sillä se ei ollut yksilöity ja tietoinen.

- Alektum Oy – 750 000 €

Perintäyhtiö ei ollut vastannut rekisteröidyn oikeuksia koskeviin pyyntöihin. Yritys myös vaikeutti ja hidasti asian tutkintaa välttelemällä valvontaviranomaista.

Linkit

GDPR-tarkistuslista: https://gdpr.eu/checklist/ (englanniksi)

EU:n tietosuojaverkkosivu: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi

Finlex Tietosuojalaki: https://www.finlex.fi/fi/laki/alkup/2018/20181050

Yrittäjän tietosuojaopas: https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

Täältä pääset halutessasi itse katsomaan, millaisia sanktioita yleisen tietosuoja-asetuksen rikkomisesta on annettu: https://www.enforcementtracker.com/

Tietoturvasuunnitelma

Tietoturvasuunnitelma on dokumentti, joka kuvaa sosiaali- ja terveyspalvelujen tuottajan tietoturva- ja tietosuojakäytäntöjä. Tietoturvasuunnitelma perustuu asiakastietolakiin ja korvaa aiemman tietosuojan ja tietoturvan omavalvontasuunnitelman.

Tietoturvallisuus sosiaali- ja terveyspalveluissa käsittää kaikki ne toimenpiteet, joilla estetään asiakasta koskevien tietojen joutuminen ulkopuolisten tahojen tietoon tai hallintaan, sekä tietojen häviäminen tai hävittäminen.

Kenen pitää laatia tietoturvasuunnitelma?

- Sosiaalihuollon palvelut
- Terveydenhuollon palvelut
- Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat
- Apteekit
- Apteekkien tietojärjestelmien valmistajat
- Kansaneläkelaitos
- Kanta-välityspalveluiden tuottajat

Miksi laatia tietoturvasuunnitelma?

Tietoturvasuunnitelma korvaa entisen tietosuojan, tietoturvallisuuden ja tietojärjestelmien käytön omavalvontasuunnitelman. Sen avulla sosiaali-

ja terveydenhuollon toimijoita ohjataan riittäviin ja yhdenmukaisiin tietoturva- ja tietosuojakäytäntöihin.

Lisäksi tietojärjestelmiin ja hyvinvointisovelluksiin kohdistuvia olennaisia vaatimuksia yhdenmukaistetaan valtakunnallisesti. Olennaisten vaatimusten määräykset kohdistuvat ratkaisujen toiminnallisuuteen, yhteen toimivuuteen ja tietoturvallisuuteen.

Tietoturvasuunnitelma:

1. Edistää asiakas- ja potilastietojen turvallista käsittelyä
2. Parantaa sote-toimijoiden tietosuojaa ja tietoturvaa
3. Vahvistaa tietoturvallisuuden ja tietosuojan suunnittelun ja toteuttamisen käytäntöjä
4. Auttaa hallitsemaan erityisesti tietoturvallisuuteen liittyviä riskejä
5. Suunnitelma on dokumentti, joka yritykseltä tulee lain mukaan löytyä, jos yritys toimii sote-alalla ja käsittelee asiakas- tai potilastietoja

Tavoitteena on, että tietosuojaan ja tietoturvaan liittyvät turvalliset toimintatavat ja menettelyt otetaan huomioon kaikessa sosiaali- ja terveydenhuollon asiakastietojen ja potilastietojen käsittelyssä.

Suunnitelman on tarkoitus kasata näitä toimintatapoja saman dokumentin alle. Ohjeet voivat olla suoraan suunnitelmaan kirjattuja tai joissain tapauksissa tietoturvasuunnitelmassa voidaan viitata muihin yrityksen ohjeistuksiin.

Suunnitelmassa kuvattujen käytäntöjen tulee olla totuudenmukaisia. Sellaisia, että niitä pystytään toteuttamaan sillä henkilöstöllä ja niillä resursseilla, joita yrityksestä löytyy.

Valmiin suunnitelman olisi myös hyvä olla helposti saatavilla. Sen lisäksi, että suunnitelman tarkoituksena on varmistaa, että turvalliset toimintatavat on otettu huomioon yrityksessä, on sen tarkoituksena toimia käytännön työkaluna. Jos esimerkiksi jokin suunnitelmassa kuvattu poikkeustilanne tapahtuu, voi suunnitelmasta tarkastaa tilanteen varalle tehdyt toimintaohjeet tai sen, minne ohjeet on kirjattu.

Tietoturvasuunnitelma kuvaa miten palveluntuottaja järjestää toiminnassaan tietoturvan ja -suojan omavalvonnan.

Asiakastietolain vaatimukset tietoturvasuunnitelmalle:

- Tietojärjestelmien käyttäjillä on käytön vaatima koulutus
- Tietojärjestelmiä asentaa, ylläpitää ja päivittää vain henkilö, jolla on siihen tarvittava ammattitaito ja asiantuntemus
- Käyttöohjeet ovat saatavilla järjestelmän yhteydessä
- Käyttäjät noudattavat tietojärjestelmäpalvelun tuottajan ohjeita
- Tietojärjestelmiä ylläpidetään ja päivitetään tietojärjestelmäpalvelun tuottajan ohjeistuksen mukaisesti
- Käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen käyttöön ja varmistaa tietoturvan ja tietosuojan
- Tietojärjestelmiin liitetyt muut järjestelmät eivät vaaranna tietojärjestelmien suorituskykyä eivätkä niiden tietoturva- tai tietosuojaominaisuuksia
- Tietojärjestelmät täyttävät käyttötarkoituksensa mukaiset olennaiset vaatimukset

Ennen kuin palvelunantaja alkaa käyttää valtakunnallisia tietojärjestelmäpalveluja eli Kanta-palveluja, sen täytyy kuvata tietoturvasuunnitelmassa:

- Miten se varmistaa tietosuojan
- Miten se täyttää vaatimukset, joita valtakunnallisten palvelujen tietoturvallinen käyttö edellyttää

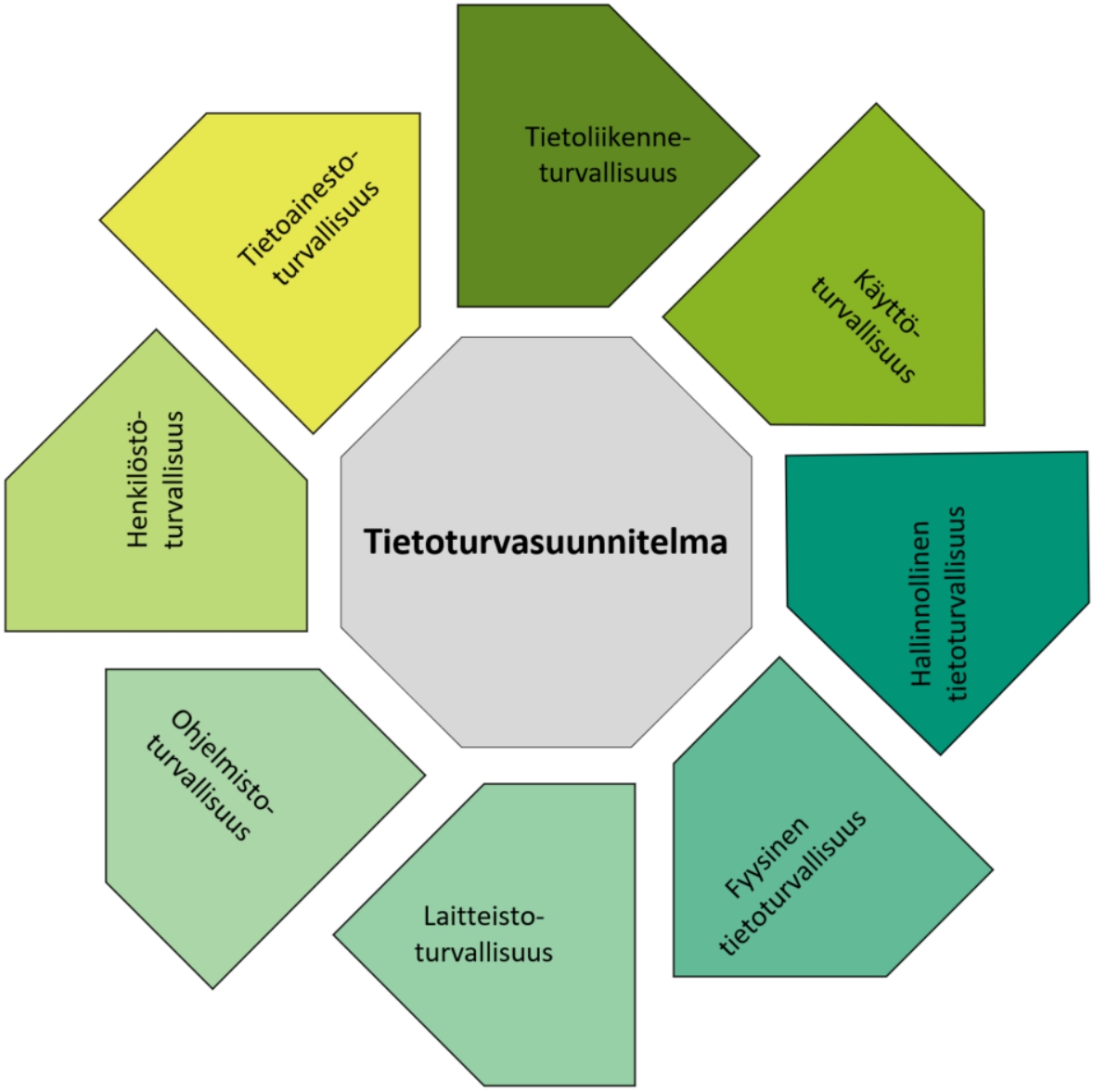
Valvontaviranomaisia ovat sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira), aluehallintovirasto (AVI), hyvinvointialueet ja tietosuojavaltuutettu. Heillä on oikeus tehdä tarkastuksia.

Riskien tunnistaminen

Tietosuoja-asetuksessa painotetaan riskiperusteista lähestymistapaa. Riskiperusteisella lähestymistavalla tarkoitetaan sitä, että henkilötietojen käsittelyyn liittyvät riskit pitää arvioida ja tarvittavat suojatoimet tulee suunnitella niiden perusteella. Riskin suuruus arvioidaan sen perusteella, kuinka suuri riski käsittelystä syntyy **rekisteröidyn** oikeuksille ja vapauksille.

Riskejä on tärkeä arvioida kattavasti. Kun riskejä kartoitetaan, tulee huomioon ottaa tiedon koko elinkaari. Myös erilaiset poikkeustilanteet on otettava huomioon. Tällaisia poikkeustilanteita voivat olla pandemian lisäksi esimerkiksi erilaiset kyberhyökkäykset.

Mitä tietoturvasuunnitelma sisältää?



Tietoliikenneturvallisuus

Tietoturvasuunnitelmassa pitää kuvata, mitkä asiat ovat yrityksen vastuulla ja mitkä puolestaan esimerkiksi tietoliikenneoperaattorin vastuulla. Tietoturvasuunnitelmaan tulee kuvata esimerkiksi kuinka on sovittu yhteydenotoista ja menettelyistä häiriötilanteissa. Nämä ovat asioita, jotka saattavat löytyä sopimuksista.

Tietoliikenneturvallisuus kattaa verkon tietoturvakäytänteet ja verkkolaitteiden turvallisuuden. Suunnitelmassa pitää kuvata kenen vastuulla on esimerkiksi laiteohjelmistojen päivittäminen ja miten verkon tai verkkojen turvallisuus on varmistettu (tähän liittyy esimerkiksi palomuuri, verkon suojaaminen salasanalla ja salasanan vaihtamiskäytännöt).

Jos yrityksessä tehdään etätöitä, liittyvät etäyhteyksiin liittyvät käytänteet myös tietoliikenneturvallisuuteen. Käytänteet voivat olla kuvattuna tietoturvasuunnitelmassa tai erillisissä etätyöohjeistuksissa, joihin tietoturvasuunnitelmassa viitataan. Etätyöohjeistuksessa pitää olla määritelty mm. se, mitä järjestelmiä on sallittua käyttää etänä ja millaisilla yhteyksillä (esimerkiksi VPN-yhteyden kautta).

Jos yrityksessä tarjotaan verkkoyhteys asiakkaille tai muille vierailijoille, tulee suunnitelmassa olla kuvattuna, kuinka se on toteutettu turvallisesti. Käytännössä tämä tarkoittaa sitä, että vierailijaverkko on erikseen yrityksen käyttämästä verkosta.

Käyttöturvallisuus

Käyttöturvallisuuteen kuuluu esimerkiksi salasanojen ja käyttöoikeuksien hallinnointi ja järjestelmien valvonta.

Tietoturvasuunnitelmassa täytyy kuvata se, kuinka työntekijät tunnistautuvat asiakastietojärjestelmiin. Potilas- ja asiakastietojärjestelmissä ei saa olla käytössä yhteiskäyttöisiä tunnuksia asiakastietojen muokkaamiseen, katseluun tai sähköiseen reseptiin liittyvien toiminnallisuuksien osalta. Yhteiskäyttöiset tunnukset on sallittu

vain silloin, kun niitä käytetään ei-tunnisteellisten tietojen tarkkailuun (esimerkiksi resursseihin ja prosesseihin liittyvät tiedot).

Suunnitelmassa tulee kuvata, missä tilanteissa edellytetään monivaiheista tunnistautumista ja missä toimikorttitunnistautumista. Myös muut kirjautumis- ja tunnistautumiskäytännöt, kuten työasemille ja mobiililaitteisiin kirjautuminen, pitää kuvata suunnitelmassa.

Yrityksessä tulee olla suunniteltuna, kuinka uudet työntekijät perehdytetään ja kuinka heille järjestetään tarvittavat käyttöoikeudet. Lisäksi tulee suunnitella, kuinka huolehditaan käyttöoikeuksien poistamisesta siinä tapauksessa, jos työntekijä irtisanoutuu tai irtisanotaan. Käyttöoikeuksia tulee seurata ja muuttuneisiin tilanteisiin tulee reagoida. Muutoksista täytyy pitää kirjaa.

Käyttöoikeuksien seurannassa voi käyttää apuna erillistä dokumenttia johon on kirjattu käyttäjäryhmät, -roolit, sekä -valtuudet eri järjestelmissä (kanta-palvelut, asiakas-/potilastietojärjestelmät, muut järjestelmät).

Asiakastietolaki velvoittaa palvelunantajaa keräämään lokitietoja kaikesta asiakastietojen käytöstä ja luovutuksesta. Lokitietojen avulla valvotaan, että tietoja voivat katsella ja käsitellä vain ne henkilöt, joilla on siihen oikeus. Lokitietoja käytetään myös tietojärjestelmien teknisten virheiden selvittämiseen.

Yrityksellä tulee olla suunnitelma siitä, kuinka yrityksessä tehdään säännöllisesti henkilötietojen käytön seurantaa ja miten toimitaan, jos väärinkäytöksiä ilmenee. Suunnitelma voi olla erillinen seuranta- ja valvontasuunnitelma, tai sitten käytänteet voidaan kirjata tietoturvasuunnitelmaan. Myös asiakkaiden ja viranomaisten tietopyyntöihin vastaaminen, lokiraporttien hallinta, sekä valvontatoimia

tekevien henkilöiden roolit tulee olla kuvattuna tietoturvasuunnitelmaan tai erilliseen suunnitelmaan, johon tietoturvasuunnitelmassa viitataan.

Hallinnollinen turvallisuus

Hallinnollinen tietoturvallisuus koostuu monista asioista, jotka mahdollistavat organisaation tietoturvallisuuden suunnittelun sekä asetettujen vaatimusten saavuttamisen. Keskeisin niistä on organisaation johdon hyväksymä tietoturvapolitiikka, jonka avulla määritellään tietoturvallisuuden vaatimukset lainsäädännön ja organisaation tarpeiden mukaisesti.

Tietoturvasuunnitelman laatiminen on keskeinen osa hallinnollista tietoturvaa.

Tietoturvaan liittyviä ohjeistuksia ja suunnitelmia tulee arvioida ja päivittää säännöllisesti. Näin varmistetaan, että ohjeet ovat yrityksen sen hetkiseen tilanteeseen sopivia.

Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa toimitilojen turvaamista ulkoisilta uhilta. Näitä ovat esimerkiksi tulipalo, luvattomat vierailijat, sekä vesivahingot.

Yrityksessä pitää huolehtia siitä, ettei ulkopuolisilla ole mahdollisuutta päästä käsiksi tietoaineistoihin. Tähän voi kuulua esimerkiksi joidenkin toimitilojen osien lukitseminen ulkopuolisilta. Fyysiseen turvallisuuteen kuuluvat myös mahdolliset kulunvalvonnan järjestelyt.

Myös laitteiden sijoittelu kuuluu fyysisen turvallisuuden alle. Esimerkiksi työasemat tulee sijoittaa niin, ettei sivullisilla ole näköyhteyttä tietokoneen ruudulle ja tulostimet niin, etteivät ulkopuoliset pääse niitä käyttämään. Tietokoneen ruutuja voidaan suojata myös näytönsuojakalvoilla.

Fyysinen turvallisuus koskee myös paperisia asiakirjoja. Arkistoitavat asiakirjat tulee säilyttää paloturvallisesti lukittuna. Hävitettäväksi tarkoitettuja asiakirjoja tulee myös käsitellä turvallisesti. Tähän voi liittyä esimerkiksi lukittavat säilytysastiat ja paperisilppurit.

Fyysisen turvallisuuden suojauskeinoja voivat olla esimerkiksi kameravalvonta, kulunvalvonta, toimitiloissa oleva rikosilmoitin- ja paloilmaisinjärjestelmä, sekä mahdolliset vartiointipalvelut.

Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa tietoverkon laitteiden, palvelinten, työasemien sekä muiden tietoteknisten laitteiden turvaamista. Näitä laitteita voivat olla työasemien lisäksi esimerkiksi verkkotulostimet ja älypuhelimet.

Jotta laitteistoturvallisuudesta voidaan huolehtia, täytyy yrityksen tietää mitä laitteitta sillä on käytössä. Laitteet on hyvä listata.

Tietoturvasuunnitelmassa tulee kuvata miten on varmistettu, etteivät ulkopuoliset henkilöt pääse käyttämään laitteita. Tähän kuuluu esimerkiksi niiden suojaaminen vahvalla salasanalla ja siitä huolehtiminen, että laitteet lukitaan, kun niiden luota poistutaan.

Laitteistoturvallisuuteen kuuluu myös omien laitteiden käyttöä koskevat ohjeet.

Laitteet tulee suojata virustorjuntaohjelmistolla. Myös virustorjuntaohjelmiston päivittämiseen liittyvät käytännöt pitää kuvata tietoturvasuunnitelmassa. Lisää tietoa virustorjuntaohjelmistoista löytyy kyber- ja tietoturvaoppaan kappaleesta 5.2.

Laitteistoturvallisuuteen liittyy myös päivityksistä huolehtiminen. Päivittämättömät laitteet ovat tietoturvariski. Tietoturvasuunnitelmaan tulee kirjata mahdolliset huolto- ja ylläpitosopimukset muiden toimijoiden kanssa.

Puhelimien suojauskäytäntöihin kuuluu esimerkiksi puhelimen lukitsemiseen liittyvät käytännöt, SIM-korttien hallinta ja kadonneiden mobiililaitteiden etälukitseminen tai -tyhjentäminen.

Myös käytöstä poistettujen laitteiden turvallinen käsittely pitää ottaa huomioon. Jos laite vielä toimii, pitää varmistaa, ettei sinne jää tietoja. Jos laite on rikki, tulee huolehtia sen tietoturvallisesta hävittämisestä. Vaikka esimerkiksi kannettava tietokone tai puhelin näyttäisikin käynnistettäessä mustaa ruutua ja vaikuttaisi käyttökelvottomalta, voi sieltä silti pystyä kaivamaan laitteelle tallennettuja tietoja.

Ohjelmistoturvallisuus

Ohjelmistoturvallisuus kattaa sen, että käytetyt ohjelmistot ovat turvallisia eivätkä vaaranna muita käytössä olevia ohjelmistoja ja järjestelmiä, sekä sen, että niitä käytetään turvallisesti.

Tietoturvasuunnitelmassa tai sen liitteissä pitää olla listaus kaikista yrityksen käytössä olevista tietojärjestelmistä ja muista ohjelmistoista, joita käytetään asiakastietojen käsittelyyn. Suunnitelmaan pitää myös kuvata vastuujako eli se, mitkä toimet ovat yrityksen vastuulla ja mitkä taas sopimuskumppanien vastuulla.

Ohjelmistojen ja sovellusten luokittelusta on kerrottu myöhemmin tässä oppaassa.

Suunnitelmassa tulee olla kuvattuna kuka saa asentaa ohjelmistoja yrityksen laitteille, sekä kenen vastuulla ohjelmistojen ylläpito ja päivittäminen ovat. Suunnitelmassa pitää kuvata myös se, kuinka varmistetaan, että ohjelmistoja asentavilla, ylläpitävillä ja päivittävillä henkilöillä on tehtävään tarvittava koulutus.

Työntekijöiden tulee myös tietää, miten toimitaan virhetilanteissa. Nämä asiat voivat olla kirjattuna tietoturvasuunnitelmaan. Ne voivat löytyä myös erillisestä suunnitelmasta, johon viitataan tietoturvasuunnitelmassa.

Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuus onkin yksi tietoturvan tärkeimpiä osa-alueita, sillä kaikki yrityksen tieto kulkee henkilöstön kautta.

Jotta turvalliset käytännöt pystytään suunnittelemaan, täytyy yrityksessä olla määritelty henkilöstölle heidän työnsä toimenkuvat. Toimenkuvan perusteella määritellään, mitä käyttöoikeuksia työntekijä tarvitsee ja millaista tietoa hänen on oikeus lukea ja käsitellä. Suunnitelmassa tulee

ottaa huomioon myös mahdolliset sijaisjärjestelyt ja sijaisille annettavat oikeudet.

Tärkeä osa henkilöstöturvallisuutta on myös henkilöstön perehdyttäminen ja tarvittavan koulutuksen varmistaminen.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuus tarkoittaa organisaatiossa olevan tiedon suojaamista. Tieto tulee suojata niin, että siihen pääsevät käsiksi vain henkilöt, joilla on siihen lupa. Etenkin kun kyse on tunnisteellisista asiakastiedoista, tulee varmistaa, että tietoja lukevat ja käsittelevät vain ne työntekijät, jotka tarvitsevat tietoja työtehtäviensä suorittamiseen.

Sähköisessä muodossa olevan tiedon suojaamiseksi on laitteissa tärkeää huolehtia laitteiden turvallisuudesta ja esimerkiksi käyttää virustorjuntaohjelmistoa.

Tiedon saatavuuden varmistaminen on tärkeä osa tietoaineistoturvallisuutta. Yrityksessä tulee määritellä, miten tärkeiden tietojen saatavuus on varmistettu ongelmatilanteiden varalta. Tähän kuuluu esimerkiksi se, että yrityksessä on suunniteltu mitä tietoja varmuuskopioidaan ja kuinka usein, sekä miten varmuuskopioita säilytetään turvallisesti. Lisätietoa varmuuskopioinnista löytyy kyber- ja tietoturvaoppaan kappaleesta 10.

Myös fyysisen tietoaineiston kuten paperisten asiakirjojen turvallisesta säilyttämisestä tulee huolehtia. Työntekijät täytyy kouluttaa fyysisten asiakirjojen turvalliseen käsittelyyn, säilyttämiseen ja hävittämiseen.

Tietoaineistoturvallisuus kattaa myös tarpeettoman tiedon turvallisen hävittämisen. Yrityksessä tulee olla mietitty, miten tietoaineistot hävitetään niin, etteivät ulkopuoliset pääse niihin käsiksi.

Työntekijöiden kouluttaminen

Heikoin lenkki hyvän tietoturvan toteutumisessa on ihminen. Siksi on erittäin tärkeää, että työntekijöitä koulutetaan **säännöllisesti** tietoturvaan ja kyberturvallisuuteen liittyvistä asioista. Työntekijöiden tulee tietää, miten ongelmatilanteissa toimitaan ja jos mahdollista, poikkeustilanteita olisi hyvä harjoitella säännöllisesti.

Uudet työntekijät tulee perehdyttää laitteiden ja ohjelmistojen turvalliseen käyttöön. Yrityksessä on myös tärkeä huolehtia siitä, että tarvittavat käyttöohjeet ja muut ohjeistukset ovat saatavilla ja ajan tasalla. Perehdytys on tärkeää myös silloin, kun yrityksessä otetaan käyttöön uusia laitteita tai ohjelmistoja.

Työntekijät on tärkeää opastaa henkilötietojen oikeanlaiseen käsittelyyn. Heidän tulee esimerkiksi tietää, että heillä on oikeus käsitellä asiakastietoja vain siinä laajuudessa, mitä heidän työtehtävänsä edellyttävät.

Työntekijöiden on hyvä olla tietoisia tilaajatahon vaatimuksista. Heidän on hyvä tietää, mihin yritys on sopimuksissa sitoutunut. Esimerkiksi kunnilla ja kuntayhtymillä saattaa olla sopimuksissa kirjattuna mahdollisia sanktioita tietoturvaan liittyvissä asioissa. On tärkeää, että työntekijät ovat näistä asioista tietoisia.

Työntekijöille annettavien ohjeiden tulee olla totuudenmukaisia. Jos tietoturvaan liittyvät ohjeet ovat liian vaikeita tai jopa mahdottomia

toteuttaa käytössä olevilla resursseilla, muodostuu päivittäisessä työnteossa usein ns. oikopolkuja, jotka helpottavat työntekoa mutta vaarantavat tietoturvan.

Tietojen luovutuksiin liittyvät käytännöt

Asiakkaasta kerättyä tietoa ei saa luvattomasti luovuttaa sivullisille. Sivullisiksi lasketaan kaikki ne tahot, jotka eivät osallistu asiakkaalle annettavan palvelun antamiseen ja jotka eivät tarvitse asiakkaan tietoja työtehtäviensä hoitamiseen. Kuten oppaassa on jo aiemmin mainittu, työntekijät saavat käsitellä asiakastietoja vain siinä laajuudessa, mitä heidän työtehtävänsä edellyttävät.

Tietoja voidaan luovuttaa sivullisille asiakkaan suostumuksella. Tällöin suostumuksen tulee olla vapaaehtoinen, yksilöity ja tietoinen tahdonilmaisu.

Tietoja voidaan luovuttaa myös siihen oikeuttavan lain nojalla. Esimerkiksi asiakaslaissa säädetään siitä, milloin salassa pidettäviä tietoja voidaan luovuttaa ilman asiakkaalta saatua suostumusta.

Asiakastietojen rekisterinpitäjällä on vastuu siitä, että tietoja luovutetaan lainmukaisesti. Rekisterinpitäjä arvioi, ovatko edellytykset tietojen luovuttamiseen olemassa ja päättää luovutetaanko tietoja. Tarvittaessa on syytä pyytää lisätietoja, miksi tietoja tarvitaan ja minkä lain perusteella niitä pyydetään.

Asiakkaalla ja hänen laillisella edustajallaan on oikeus tutustua asiakastietoihin. Oikeus perustuu yleiseen tietosuoja-asetukseen. Myös julkisuuslaissa on säännöksiä asianosaisen tiedonsaantioikeudesta.

Asiakas voi kieltää tietojensa luovuttamisen tai hankkimisen. Nämä kiellot on hyvä kirjata. Tietoja voidaan kuitenkin hankkia tai luovuttaa kiellosta huolimatta, jos siihen löytyy lain sallima syy.

Lisätietoa:

Tietosuojavaltuutetun toimiston ohje sosiaalihuollon asiakastietojen käsittelyyn: https://tietosuoja.fi/documents/6927448/10594424/Sosiaalihuollon+asiakatietojen+k%C3%A4sittely.pdf/fc9f4ce8-caee-3161-f3ae-8962a87007b6/Sosiaalihuollon+asiakatietojen+k%C3%A4sittely.pdf?t=1664534736382

Tietosuojavaltuutetun toimiston vastauksia usein kysyttyihin kysymyksiin potilastietojen käsittelystä:

https://tietosuoja.fi/usein-kysyttya-terveydenhuolto

Ohjelmistojen ja sovellusten luokittelu

Luokka A

Luokkaan A kuuluvat järjestelmät, jotka liittyvät suoraan tai välityspalvelun kautta Kanta-palveluihin tai tuottavat kansallisten määrittelyjen mukaisia rakenteisia asiakirjoja tai muita tietorakenteita, jotka välitetään tuotetussa muodossa Kanta-palveluihin.

Tähän luokkaan kuuluvat myös ne järjestelmät, joiden on todennettava tietoturvavaatimusten täyttäminen, koska järjestelmässä käsiteltävät tiedot muodostavat merkittävän ja laajamittaisen asiakastietojen

keskittymän, jonka suojaaminen edellyttää vaatimusten todentamista laajan asiakasjoukon tietosuoja tai sosiaali- ja terveyspalvelujen saatavuuden varmistamisen ja varautumisen näkökulmasta.

Luokka B

Asiakas- tai potilastietojen käsittelyyn käytetyt järjestelmät, jotka eivät liittyy suoraan Kanta-palveluihin ja joihin ei kohdistu luokan A1 mukaisia tarpeita olennaisten tietoturvavaatimusten todentamiseen.

Luokittelemattomat ohjelmistot ja sovellukset

Myös näitä ohjelmistoja käytettäessä asiakastietojen tietosuojasta ja tietoturvallisuudesta on huolehdittava henkilö- ja asiakastietojen käsittelyä koskevien ja muiden lakien mukaisesti.

Esimerkkejä:

- Tekstinkäsittelyyn tarkoitettu ohjelmisto, jota käytetään myös asiakas- ja potilastietojen käsittelyyn (esimerkiksi Microsoft Word)
- Ateriatilausjärjestelmät
- Asiakaslaskutusjärjestelmät
- Verkko- ja pilvipalvelut
- Viestintään käytetyt järjestelmät tai sovellukset (esimerkiksi WhatsApp)
- Tietojärjestelmät tai tietojärjestelmäpalvelut, jotka käsittelevät anonymisoitua tai ei-tunnisteellista käsiteltävää asiakas- tai potilastietoa

- Yleiset asianhallintajärjestelmät, joita ei ole tarkoitettu asiakas- ja potilastietojen käsittelyyn.

Asiakastietolaki 784/2021

Ketä uusi asiakastietolaki koskee?

- Sosiaali- ja terveydenhuollon palvelunantajat
- Tietojärjestelmäpalveluiden tuottajat
- Apteekit
- Kansaneläkelaitos

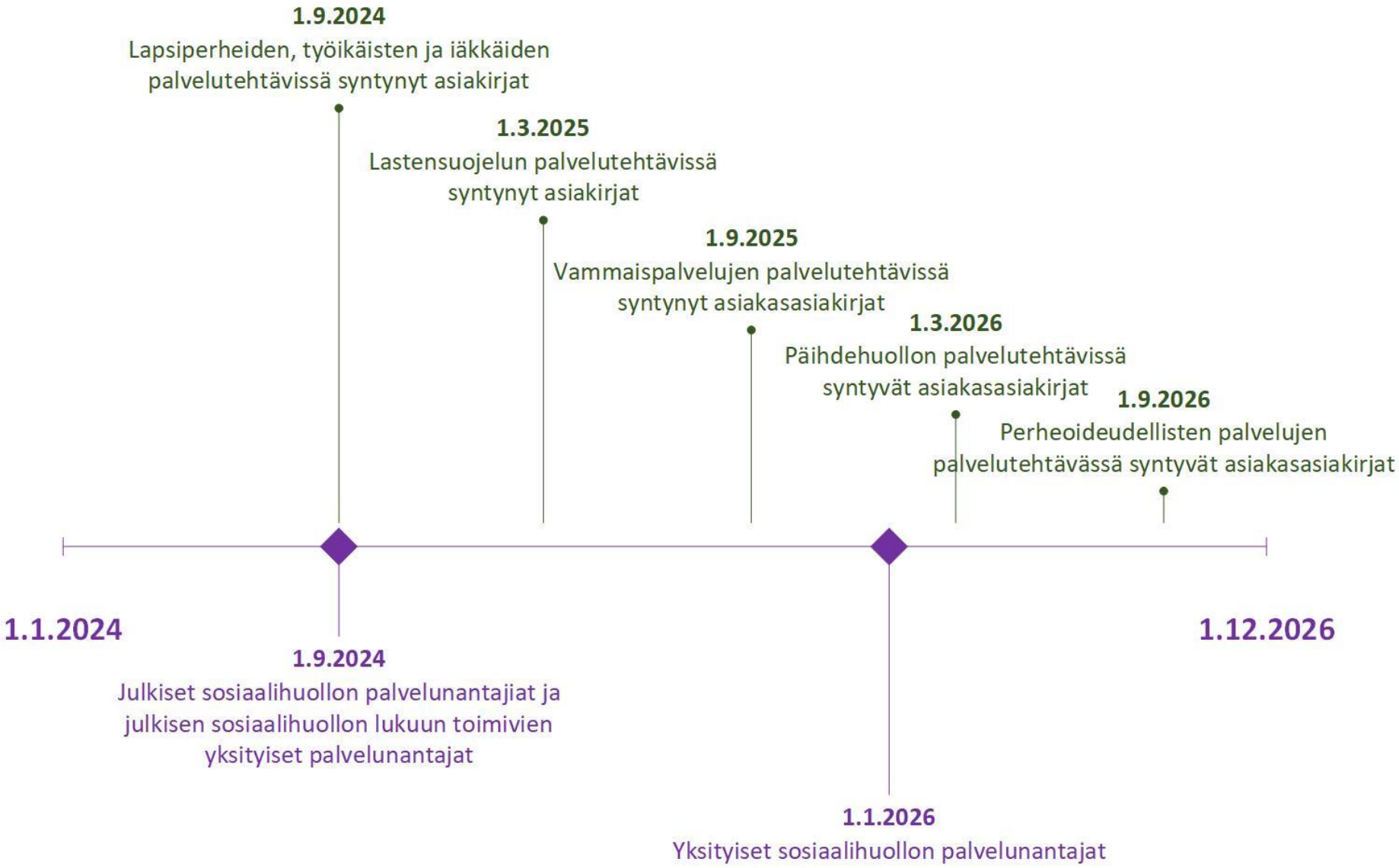
Mitä uusi laki tarkoittaa SOTE-alalle?

- Lain tavoitteena on parantaa tietoturvallisuutta asiakastietojen käsittelyssä
- Lain myötä useampi toimija on velvoitettu liittymään Kanta-palveluihin
- Laki velvoittaa laatimaan tietoturvasuunnitelman
    - Mahdollinen jo olemassa oleva omavalvonnan suunnitelma voidaan myös päivittää tietoturvasuunnitelmaksi
- Asiakastietolaki velvoittaa palvelunantajaa keräämään lokitietoja kaikesta asiakastietojen käytöstä ja luovutuksesta

Kenen pitää liittyä Kanta-palveluun?

- Apteekit
- Julkiset terveyden- ja sosiaalihuollon palvelunantajat
- Yksityiset terveyden- ja sosiaalihuollon palvelunantajat, joilla on käytössään potilas- tai asiakastietojen käsittelyyn tarkoitettu järjestelmä

Sosiaalihuollon siirtymäajat



Terveydenhuoltoa koskevat muutokset

Terveydenhuolto, Potilastiedon arkisto viimeistään 1.10.2026

- Ajanvarausasiakirja asiakkaalle varatuista ja hänelle ilmoitettavista terveydenhuollon ajanvarauksista
- Seulontatutkimuksista syntyvät kuvantamistutkimukseen liittyvät asiakirjat ja laboratoriotulokset
- Ajoterveyteen liittyvät todistukset ja lomakkeet
- Tapaturmiin ja ammattitauti-ilmoituksiin liittyvät todistukset ja lomakkeet
- Lääkärinlausunto terveydentilasta (T-todistus)
- Lääkärintodistus (TOD)
- Lääkärintodistus C
- Kuolintodistus. (Uusi 8 mom.)

Kuvantamistutkimuksiin liittyvien asiakirjojen tallentaminen viimeistään 1.10.2029

- Säteilyrasitustiedot
- Video- ja äänitallenteet sekä valokuvat
- Patologian kuva-aineistot
- Biosignaalit
- Suun terveydenhuollon yksiköiden tallentamat kuvat
- Muut kuvat: piirustukset ja havainnekuvat

Lue lisää asiakastietolain myötä tulevista muutoksista ja siirtymäajoista täältä: https://www.kanta.fi/ammattilaiset/asiakastietolain-siirtymaajat-ja-vaiheistus

Mitä muita asiakirjoja olisi hyvä laatia?

Tietosuojaseloste

Yleinen tietosuoja-asetus velvoittaa rekisterinpitäjiä kertomaan henkilötietojen käsittelystä rekisteröidylle. Rekisteröidyn tulee saada kattava kuva henkilötietojen käsittelyn kokonaisuudesta selkeässä muodossa.

Tiedon voi antaa esimerkiksi verkkosivuilla. Tietosuoja-asetus ei määrää tietystä muodosta, mutta yksi yleisesti käytetyistä nimistä on tietosuojaseloste.

Seloste tulee päivittää säännöllisesti. Näin varmistutaan siitä, että informointi vastaa sitä, miten yrityksessä toimitaan. Muista, että mahdollisista muutoksista pitää viestiä rekisteröidyille selkeästi.

Voit lukea tarkemmin rekisteröidyn informoinnista ja selosteeseen sisällytettävistä tiedoista tietosuojavaltuutetun toimiston sivuilta: https://tietosuoja.fi/rekisteroidyn-informointi

Seloste käsittelytoimista

Asiakirja tulee laatia mm. silloin, kun henkilötietojen käsittely aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille, jos henkilötietojen käsittely ei ole satunnaista, tai jos henkilötiedot sisältävät erityisiä tietoryhmiä.

Seloste on yrityksen sisäinen asiakirja, mikä auttaa hahmottamaan henkilötietojen käsittelyn ja osoittaa, että tietoja käsitellään

tietosuojalainsäädännön mukaisesti. Se on pyydettäessä toimitettava valvontaviranomaiselle.

Selosteesta määrätään tietosuoja-asetuksen artiklassa 30: https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

Tietosuojavaltuutetun toimiston mallipohjat:

Rekisterinpitäjälle: https://tietosuoja.fi/documents/6927448/8323207/Mallipohja+rekisterinpit%C3%A4j%C3%A4lle+seloste+k%C3%A4sittelytoimista/bf9167e3-3f89-4a40-a284-9f438f3b6476?t=1544175233000

Henkilötietojen käsittelijälle: https://tietosuoja.fi/documents/6927448/8323207/Mallipohja+henkil%C3%B6tietojen+k%C3%A4sittelij%C3%A4lle+seloste+k%C3%A4sittelytoimista/f3bfa0a6-81e0-48b6-b26d-f907d9a1c805?t=1527077342000

Liiketoiminnan jatkuvuussuunnitelma

Jatkuvuussuunnitelman tavoite on tarjota väline hätätilanteeseen/poikkeamaan, joka uhkaa häiritä normaalia liiketoimintaa. Suunnitelma auttaa pienentämään poikkeamien riskit.

Täältä löydät pohjan yksinyrittäjälle:

https://www.xamk.fi/wp-content/uploads/2022/07/liiketoiminnan-jatkuvuussuunnitelma-yksinyrittajille.docx

Täältä löydät pohjan mikroyritykselle:

https://www.xamk.fi/wp-content/uploads/2022/07/liiketoiminnan-jatkuvuussuunnitelma-mikroyrittajille.docx

Arkistonmuodostussuunnitelma

Suunnitelman tarkoituksena on auttaa hahmottamaan ja suunnittelemaan asiakirjojen säilytystä, käsittelyä ja käyttöä. Sen avulla pyritään varmistamaan tiedon turvallinen käsittely koko sen elinkaaren ajan.

Suunnitelmaan on hyvä kirjata:

- Yrityksessä syntyvät asiakirjat
- Niiden säilytysajat
- Säilytysmuodot ja -paikat

Yksinkertainen esimerkki arkistonmuodostussuunnitelmasta:

Asiakirja/ rekisteri	**Säilytysaika**	**Muuta huomioita**
Koulutustiedot	Palveluksessa oloaika	Säilytetään lukitussa tilassa
Lääkärintodistus	2.v	Tallennetaan sähköiseen henkilöstörekisteriin
Päiväraha-anomus / Kela	2.v	
Tapaturmailmoitusjäljennös ja päätös	10.v	

Irtisanominen / irtisanoutuminen	10.v	
Työpaikkaterveyden huoltoon liittyvät asiakirjat: toimintasuunnitelmat	Voimassaoloaika + 2.v	

Lokiseurantadokumentti

Asiakastietolaki velvoittaa palvelunantajaa keräämään lokitietoja asiakasrekisterikohtaisesti, jos tietojärjestelmän käyttö edellyttää tunnistautumista. Lokitietoja on myös seurattava ja poikkeamiin on reagoitava. Erillinen dokumentti lokien seurannasta on siihen hyvä työkalu.

Dokumenttiin on hyvä kirjata:

- Päivämäärä ja kellonaika
- Kuka seurantaa on tehnyt
- Mitä on löytynyt
- Mihin toimenpiteisiin löydökset ovat johtaneet

Henkilötietojen tarkastuspyynnöt kasaava dokumentti

Rekisteröidyillä on oikeus esittää omiin tietoihinsa liittyviä tarkastuspyyntöjä. Pyynnöistä on hyvä pitää kirjaa.

Dokumenttiin on hyvä kirjata:

- Kuka pyynnön on tehnyt ja kuka sen on vastaanottanut
- Mitä tietoja henkilö on pyytänyt tarkastettavaksi

- Milloin pyyntö on tehty
- Miten ja milloin pyyntöön on vastattu ja kuka siihen on vastannut
- Jos pyyntö on johtanut toimiin, kuten rekisteröidyn tietojen oikaisuun, poistamiseen, siirtoon tai tietojen käsittelyn rajoittamiseen
- Kirjaa ylös myös, jos korjattavaa ei löytynyt

Lisätietoja rekisteröidyn oikeuksista tutustua omiin tietoihinsa:

https://tietosuoja.fi/oikeus-saada-tutustua-tietoihin

Käyttöoikeusdokumentti

Palvelunantajan on varmistettava, että asiakastietoja voivat katsella vain ne henkilöt, joilla on siihen oikeus. Työntekijöiden käyttöoikeuksien tulee vastata heidän työtehtäviään ja niiden tulee olla ajan tasalla. Käyttöoikeuksien seuraamisessa auttaa dokumentti, johon ne on kirjattu.

Dokumenttiin on hyvä kirjata:

- Kanta-palvelujen käyttöoikeudet
- Asiakas- ja potilastietojärjestelmien käyttöoikeudet
- Muut käyttöoikeudet
- Samaan dokumenttiin voi kerätä myös luettelon yrityksen käytössä olevista laitteista