Tietoturva- ja tietosuojapolitiikka

Varkauden kaupunki

Versio 1.0

23.4.2018

Sisällysluettelo

1 Johdanto

Tietoturva ja tietosuoja ovat yhdessä tärkeä osa Varkauden kaupunkikonsernin (myöh. kaupunki) toiminnan ja palveluiden laatua. Niihin liittyvä työ kaupungissa on päivittäistä kaikille organisaatiotasoille, toimintoihin ja palveluihin sulautettua toimintaa.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista ja henkilötietojen oikeaoppista käsittelyä niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa.

Tietoturvatyö tarkoittaa tiedon suojaamiseksi tehtävien toimenpiteiden suunnittelua ja sen mukaista toteuttamista.

Tässä politiikassa ja sen liitteissä määritellään mitä tietoturva ja tietosuoja Varkauden kaupungissa tarkoittaa. Lisäksi politiikassa kuvataan kaupungin tietoturvan ja tietosuojan keskeiset periaatteet, tavoitteet, roolit ja vastuut.

Tämä politiikka katselmoidaan vuosittain ja on kokonaisuudessaan henkilöstön saatavilla intranetissä. Julkinen versio julkaistaan kaupungin kotisivuilla.

2 Tietoturva- ja tietosuojapolitiikan tarkoitus ja tausta

Tämä politiikka toimii kaupungin ylimpänä turvallisuusasiakirjana, sekä perustana toimialojen omille toimintaperiaatteille ja ohjeille, jotka tarkentavat tässä politiikassa annettuja määräyksiä.

Tämä politiikka kuvaa tietoturvan ja tietosuoja roolit kaupungin toiminnoissa ja palveluissa, perustuen tehtyihin riskiarvioihin ja toimintaa säätelevien lakien vaatimuksiin. Politiikassa on lisäksi huomioitu kaupunkistrategiassa (KV, 18.12.2017) määritellyt painopistealueet ja niiden asettamat vaatimukset. Tietoturvan ja tietosuojan kannalta yksi keskeisimpiä on poikkihallinnollinen kaupunkistrategian ohjelma ”Resurssitehokas digitalisaatio”.

3 Keitä tietoturva- ja tietosuojapolitiikka koskee

Tämä politiikka on kaupunginhallituksen hyväksymä ja koskee koko kaupunkiorganisaatiota sekä niitä sidosryhmiä (yhteistyö- ja sopimuskumppanit) jotka käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa.

Politiikassa esitetyt periaatteet ja käytännöt koskevat kaikissa tiedon elinkaaren vaiheissa (tuottaminen, kerääminen, säilytys, siirto, luovuttaminen, hävittäminen) ja kaikissa muodoissa (mm. paperi, sähköinen, optinen, puhuttu) olevaa tietoa.

4 Tietoturvallisuus

Tietoturvallisuus kattaa tietoturvaan ja tietosuojaan liittyvät toteutukset. Tietoturvalla kaupungissa tarkoitetaan kaikissa muodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen, palveluiden ja niiden käyttöympäristöjen) turvaamista siten, että tiedon alkuperäisyys, luottamuksellisuus, eheys, saatavuus ja käytettävyys kyetään varmistamaan.

Periaatteena on, että tietoturvallisuuskäytännöt kattavat kaikki kaupungin tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon ottaen huomioon toimialojen ja työyksiköiden perusluonteen ja tietoturvatarpeet. Tietoturvallisuus pyritään integroimaan kiinteästi kaupungin palveluihin ja toimintaan, sekä jokaisen käyttäjän työtapoihin.

Tietoturvallisuutta toteutetaan käytännössä seuraavilla:

- **Asenne**: Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoinut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja -määräyksiä.
- **Eheys:** Tieto, tietojärjestelmät ja arkistot ovat luotettavia, oikeellisia ja ajantasaisia. Toisin sanoen tieto ei ole muuttunut teknisen vian seurauksena tai tietoa ei ole muutettu ihmisen toimesta tahallisesti tai tahattomasti.
- **Kiistämättömyys:** Tiedonkäsittelytoimenpiteiden suorittamista siten, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen.
- **Luottamuksellisuus:** Tieto on vain siihen oikeutettujen saatavissa eikä sitä paljasteta tai muutoin saateta sivullisten tietoon. Tiedon käsittelyssä noudatetaan voimassa olevia lakeja sekä erikseen, toiminnoittain/järjestelmittäin, hyväksyttyjä tietojen turvaluokituksien mukaisia sääntöjä ja ohjeita.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa.
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kaupungin tietoturvatyön periaatteet ja toteutukset perustuvat ensisijassa julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeisiin ja suosituksiin, JHS-suosituksiin, tietoturvatasojen määrittelemiin Perustaso -vaatimuksiin (Tietoturvallisuusasetus 681/2010) ja tietosuojavaltuutetun toimiston antamiin ohjeisiin.

5 Tietosuoja

Henkilötietoja kerätään vain siinä laajuudessa kuin kaupungin tarjoamien palveluiden tuottaminen edellyttää. Henkilötietojen käsittelijöillä on käyttöoikeus vain niihin tietoihin, joita palvelun tuottamisessa tarvitaan. Tietoja voidaan luovuttaa kolmansille osapuolille lakeihin perustuvien luovutustarpeiden nojalla. Tietoja ei luovuteta muihin tarkoituksiin ilman asiakkaalta pyydettyä käyttötarvekohtaista lupaa.

Toiminnassa muodostuvista henkilörekistereistä on julkisesti tarjolla tietosuojaselosteet, joista käy ilmi rekistereiden sisältämät tiedot ja käyttötarkoitus.

Rekisterinpitäjänä on se toimija, jonka käyttötarkoitusta varten henkilötiedot on kerätty.

Varkauden kaupungin toimiessa rekisterinpitäjänä palveluntarjoaja voi siirtää henkilötietoja Euroopan unionin, Euroopan talousalueen tai muiden maiden, joiden Euroopan Komissio on todennut takaavan riittävän tietosuojan tason, ulkopuolelle ainoastaan Varkauden kaupungin etukäteisellä kirjallisella suostumuksella.

Tietoturva- ja tietosuojaryhmän riskiarvion mukaisesti Varkauden kaupunki tekee sopimuksen kumppaneiden ja palveluntarjoajien kanssa henkilötietojen käsittelystä.

Varkauden kaupunki noudattaa laissa ja asetuksissa voimassa olevia velvollisuuksia rekisterinpitäjänä ja henkilötietojen käsittelijänä, sekä sitoutuu turvaamaan rekisteröidyn oikeudet. (Euroopan unionin yleinen tietosuoja-asetus (EU 679/2016), Tietosuojalaki (2018), Tiedonhallintalaki (2019).

Varkauden kaupunki edellyttää, että henkilöstö on osallistunut tietoturva- ja tietosuojakoulutuksiin ja todentaa osaamisen mm. verkko-oppimisympäristössä suoritetun testin avulla. Lisäksi henkilöstö allekirjoittaa tietoturva- ja tietosuojasitoumuksen (liite 3).

Varkauden kaupunki rekisterinpitäjänä vastaa siitä, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu (asetuksen mukainen osoitusvelvollisuus):

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus

5.1 Menettely tietosuojan vaarantuessa

Tietosuojaloukkaukseksi katsotaan kaikki henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kaupungin tarkempien periaatteiden ja ohjeistuksien vastainen toiminta.

Jo pelkkä epäily tietosuojaloukkauksesta johtaa asian selvittämiseen. Selvittäminen aloitetaan kaupungin sisäisenä toimintana. Jos tietosuojaloukkaus arvioidaan lainsäädännön perusteella rangaistavaksi toiminnaksi tai rangaistavuudesta on olemassa riittävä epäilys, asian käsittely annetaan viranomaiselle.

Jos henkilötietojen tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja valvontaviranomaiselle ilman aiheetonta viivytystä (72h).

Muu, ei lainsäädännöllisesti rangaistavaksi toiminnoksi luettava, mutta tietosuojaa vaarantava toiminta johtaa kaupungin sisäiseen seuraamusmenettelyyn, jossa tietosuojaloukkaus voi johtaa huomautukseen, varoitukseen tai työsuhteen päättämiseen. Tietoturva- ja tietosuojapolitiikan liitteessä 2 on Varkauden kaupungin tietoturva- ja tietosuojarikkomusten seuraamustaulukko.

Varkauden kaupungin nimetyt tietosuojavastaavat toimivat yhteyshenkilöinä valvontaviranomaiselle sekä rekisteröidyille, joita tietosuojaloukkaus koskee.

6 Kokonaisturvallisuus

Kaupungin kokonaisturvallisuus koostuu riskienhallintaan, varautumiseen ja turvallisuuteen liittyvistä prosesseista ja niiden toteutuksista. Tietoturva- ja tietosuojapolitiikka on osa kaupungin kokonaisturvallisuuden hallintaa.

7 Riskienhallinta

Riskienhallinta toimii kaupungin kokonaisturvallisuuden perustana. Riskienhallinnan avulla kaupungin palveluihin, toimintoihin ja tietoihin kohdistuvia riskejä hallitaan järjestelmällisesti ja koko organisaation laajuisesti. Riskienhallinta kuuluu jokaisen työntekijän vastuulle.

EU:n yleinen tietosuoja-asetus edellyttää vaikutuksen arvioinnin (DPIA) tekemistä. Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarviointi on tehtävä, kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski. Vaikutustenarvioinnin tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen vaatimusten noudattamisessa ja noudattamisen osoittamisessa.

8 Varautuminen ja jatkuvuudenhallinta

Kaupungin tavoitteena on varautua erilaisiin toimintaa häiritseviin tai toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen ennakolta. Tämä tapahtuu kehittämällä ja ylläpitämällä seuraavia varautumiseen ja jatkuvuudenhallintaan liittyviä suunnitelmia:

- Jatkuvuussuunnitelmat toiminnan kannalta kriittisille palveluille, toiminnoille ja tietojärjestelmille niiden jatkuvuuden turvaamiseksi
- Toipumissuunnitelmat kriittisille tietojärjestelmille ja -verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi
- Valmiussuunnitelma toiminnan, palveluiden ja järjestelmien hallinnoimiseksi häiriö- ja poikkeusoloissa
- Lakisääteiset pelastussuunnitelmat ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa

9 Turvallisuus

Tietoturvan ja tietosuojan ohella keskeisimpiä turvallisuuden osa-alueita kaupungissa ovat:

Turvallisuusjohtaminen on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla tietoturvaprosessin kuvaamilla osa-alueilla.

Henkilöstöturvallisuus on kaupungin ja sidosryhmien henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Periaatteena on, että tietoturva ja tietosuoja huomioidaan työ- / virkasuhteen kaikissa vaiheissa.

Fyysinen turvallisuus koostuu järjestelyistä joilla kaupungin tiloja, ihmisiä, tietoa ja muuta omaisuutta suojataan vahingoilta ja vahingoittamisyrityksiltä.

10 Roolit ja vastuut

Tietoturvan ja tietosuojan toteuttaminen on jatkuvaa, laaja-alaista ja kaikille toimijoille kuuluvaa toimintaa. Periaatteena on, että sen toteuttamiseen osallistuvat kaupungin ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan. Käytännössä tämä tarkoittaa hyvien periaatteiden ja ohjeiden noudattamista sekä tietoturvan- ja tietosuojan huomioimista kaikessa tekemisessä.

Ylin vastuu tietoturvasta, tietosuojasta, riskienhallinnasta ja varautumisesta on kaupunginhallituksella ja kaupunginjohtajalla. Ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan liitteessä 1.

11 Tietojärjestelmien käyttö

Kaupungin periaatteiden mukaisesti, käytettävät tietojärjestelmät on tarkoitettu työtehtävien hoitamiseen eikä niitä tule käyttää kaupungin omistaman tai hallinnoiman tiedon vaarantumiseen johtavaan toimintaan. Kaupungille tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensisijassa vaarantumisen aiheuttaja.

Käyttäjien toimintaa ohjataan tästä politiikasta johdetuilla periaatteilla ja ohjeilla. Tiedon ja tietojärjestelmien väärinkäyttöön puututaan kaupungin normaalein kurinpitomenettelyin.

12 Tietoturvan ja tietosuojan seuranta, ylläpito ja kehittäminen

Kaupungin tietoturva- ja tietosuojatavoitteiden toteutumista seurataan säännöllisesti laaditun vuosikellon mukaisesti. Seuranta perustuu tietoturva- ja tietosuojaprosessin mukaisiin mitattaviin tavoitteisiin ja raportointikäytäntöihin (mm. tietotilinpäätös), sekä yhteisesti sovittuihin teknisen valvonnan keinoihin.

Tietotilinpäätös on raportti, joka syntyy organisaation sisäisen tarkastelun tuloksena. Se käsittää tilinpäätösluonteisen tarkastelun ulottamisen tietovarantoihin, tietojohtamiseen, tietojenkäsittelyyn ja tietoturvallisuuteen.

Tietoturvan ja tietosuojan ylläpidossa ja kehittämisessä keskeisessä roolissa on osaaminen, mitä toteutetaan säännöllisillä koulutus- ja viestintäkäytännöillä. Tämä politiikka sisällytetään koko kaupungin henkilöstön perehdytysprosessiin.

Tarvittavien ulkoisten sidosryhmien tietoturva- ja tietosuojaosaamisesta vastaa kyseisen toimialan johto. Periaate on, että kaikki, jotka käsittelevät kaupungin omistamaa tai hallinnoimaa tietoa saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

Liite 1 ROOLIT JA VASTUUT

Luottamushenkilöstö

- Vastaa tietoturvallisuuden toteuttamisesta omissa luottamustehtävissään

Kaupunginhallitus

- Toimii kaupungin ylimpänä kokonaisturvallisuudesta päättävänä tahona ja omistajana
- Politiikkatason asiakirjojen hyväksyntä
- Kokonaisturvallisuuden toteutumisen seuranta ja ohjaus

Kaupunginjohtaja

- Edellytysten luominen tietoturvallisuuden toteutumiselle
- Raportointi ja kehitysehdotukset kaupunginhallitukselle

Tietohallinnon johtoryhmä

- Tietoturvan ja tietosuojan tekniset linjaukset
- Yhteisten periaatteiden ja käytäntöjen hyväksyntä
- Tietoturva- ja tietosuojalinjausten tarkistaminen tietohallinnon vuosikellon mukaisesti
- Tietoturva- ja tietosuojapolitiikan ja ohjeistuksen kehittäminen
- Tietoturvatietouden edistäminen yhdessä toimialojen ja konsernin johdon kanssa
- Tietoturvallisuuden kehittäminen, sekä toteutumisen ohjaus ja valvonta kaupungin laajuisesti
- Tietoriskien ja tietoturvapoikkeamien hallinnan koordinointi
- Tietoturvallisuuteen liittyvän viestinnän tukeminen ja toteuttaminen yhdessä tietoturvapäällikön kanssa

Tietoturva- ja tietosuojaryhmä

- käsittelee, kommentoi, antaa lausuntoja ja kannanottoja tietosuojaan, tietoturvaan ja kyberturvallisuuteen liittyen
- tarkastaa henkilötietoja sisältävien sopimusten tietoturvan ja tietosuojan
- käsittelee tietosuojaan ja tietoturvaan liittyvät merkittävät poikkeamat
- käsittelee ja hyväksyy osaltaan projektit sovituissa tarkastuspisteissä
- kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista

Tietoturvapäällikkö

- Riskienhallinta- / tietoturvapolitiikan ja -periaatteiden määrittelyyn osallistuminen
- Tietoturvan kehittäminen tietoturvapolitiikan mukaisesti
- Henkilöstön tietoturvatietouden ylläpito ja tietoturvakoulutuksen järjestelyt
- Tietoturvaprosessin omistajuus ja prosessin mukaisen tietoturvan toteutuksen ohjaus
- Konsernijohdolle ja toimialajohdolle raportointi tietoturvan toteutumisesta, vuosikellon mukaisesti
- Yhteisten tietoturvaperiaatteiden ja käytäntöjen valmistelu, sekä tietoturvasuunnitelman omistajuus
- Yhteistyö ulkoisten sidosryhmien kanssa

Tietosuojavastaava

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja,

- antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti,
- tekee yhteistyötä valvontaviranomaisen kanssa ja toimii yhteyspisteenä käsittelyyn liittyvissä kysymyksissä,
- henkilötietojen käsittelyä koskeva suunnittelu- ja kehittämistoiminta, tietoturva- ja tietosuojaryhmän jäsenenä
- osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon,
- seuraa ja valvoo henkilötietojen käsittelyä ja niiden suojausmenetelmiä,
- raportoi suoraan organisaation johdolle tietosuojan (ja tietoturvallisuuden) tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta)

Toimialojen johto ja konsernijohto

- Tietoturvallisuuden toteuttaminen ja toteutumisen seuranta omassa organisaatiossaan ja kaikessa alaisessaan toiminnassa
- Tietoturva- ja tietosuojavastuiden toteuttaminen tytäryhtiöissä
- Tietoturvaa ja tietosuojaa säätelevien lakien, säädösten, direktiivien ja määräysten huomioiminen omassa organisaatiossaan
- Sisäisen valvonnan raportin tuottaminen vuosittain

Esimies

- vastaavaa oman yksikkönsä osalta annettujen määräysten ja ohjeistusten noudattamisesta. Tähän sisältyy niin työntekijöiden perehdyttäminen kuin toteutumisen seuranta.
- raportoi mahdollisista poikkeamista toimialan tietosuojavastaavalle
- tietojärjestelmien käyttöoikeuksien hakeminen, hyväksyminen, muuttaminen ja poisto- ja passivointipyyntöjen tekeminen

Tiedon tai tietojärjestelmän omistaja

- Omistamansa tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen, sekä käyttöoikeuksien hyväksyntä ja säännöllinen katselmointi
- Omistamansa henkilörekisterin tietosuojaselosteen hyväksyntä
- Riskienhallinta omistuksensa puitteissa
- Kriittisten järjestelmien turvajärjestelyjen testauksen toteuttaminen

Henkilöstöhallinto

- Henkilöstöturvallisuuden toteuttaminen virka- / työsuhteen kaikissa vaiheissa

Asiakirjahallinnosta vastaava

- Osallistuu asiakirjallisen tietoaineiston käsittelyn kehittämiseen ja tietoturvallisuuden toteuttamiseen
- Ohjaa toimialoja asiakirjahallinnon hoidossa, jotta arkistolain 7§ toteutuu oikeusturva ja tietosuoja huomioiden
- Hyväksyy asiakirjallisten tietoaineistojen hallinnan edellyttämät arkistonmuodostus- ja tiedonohjaussuunnitelmat
- Vastaa päätearkistoon luovutetusta pysyvästi säilytettävästä tietoaineistosta ja niiden tietoturvallisuudesta ja tietosuojasta

Toimialojen arkistovastaavat

- Vastaa asiakirjallisen tietoaineiston käsittelyn kehittämisestä ja tietoturvallisuuden toteuttamisesta arkistovastaavan tehtävissä
- Ohjaa omalla vastuualueellaan asiakirjahallinnon hoitoa arkistolain 7 § huomioiden
- Vastaa omalla vastuualueellaan arkistonmuodostus- ja tiedonohjaussuunnitelman ajantasaisuudesta myös tietoturvallisuuden toteutumiseksi
- Vastaa omalla vastuualueellaan päätearkistoon ja käsiarkistoihin luovutetun tietoaineiston säilyttämisestä ja tietoturvallisuudesta ja tietosuojasta

Tietotekniikan tukihenkilöstö

- Tietoturva- ja tietosuojapolitiikan soveltaminen ja toteuttaminen omaa erikoisasiantuntemusta hyödyntäen
- Tietoturvatoimenpiteiden huomioiminen omalla vastuualueellaan
- Teknisen valvonnan toteuttaminen tietoturvapäällikön ohjauksessa ja valvonnassa, yhteistyömenettelyssä sovittujen toteutusten mukaisesti

Tietojärjestelmän pää- ja varapääkäyttäjä

- Tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen ja toteuttaminen, yhdessä tiedon tai tietojärjestelmän omistajan kanssa
- Tietojärjestelmäkuvauksien ylläpito, yhdessä tiedon tai tietojärjestelmän omistajan kanssa (tietojärjestelmä- ja tietosuojaselosteet)
- Käyttöoikeuksien hallinta tietojärjestelmän omistajan valtuuttamana

Henkilöstö

- Käsittelee tietoja annettujen ohjeiden ja määräysten mukaisesti
- Havaitsemiensa tietoturvaan ja tietosuojaan liittyvien ongelmien, uhkien, poikkeamien tai ohjeiden vastaisen menettelyn raportointi

Rekisteröidyt

- ovat tietoisia oikeuksistaan sekä vastuussa antamiensa tietojen oikeellisuudesta

Ulkoiset palveluntuottajat

- Sitoutuvat noudattamaan kaupungin tietoturva- ja tietosuojapolitiikkaa
- Palveluntuottajien vastuut henkilötietojen käsittelyssä sovitaan palvelukohtaisissa sopimuksissa
- Palveluntuottajien tulee nimetä tietoturva- ja tietosuoja-asioihin yhteyshenkilö