POHJOIS-SAVON
HYVINVOINTIALUE

# Tietoturvallisuuden osa-alueet ja lait

## Tietoturva- ja tietosuojapolitiikan liitteet 1 ja 2

POHJOIS-SAVON
HYVINVOINTIALUE

## Sisällys

POHJOIS-SAVON
HYVINVOINTIALUE

## LIITE 1 TIETOTURVALLISUUDEN OSA-ALUEET

**1** Hallinnollinen turvallisuus

Hallinnollisella tietoturvalla ja tietosuojalla tarkoitetaan tietoturvallisuuden ja tietosuojan hallintajärjestelmien, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Sen tarkoituksena on tuoda organisaatioon tietoturva- ja tietosuojapolitiikka ja tietoturvalliset toimintatavat luonnolliseksi osaksi kaikkea toimintaa. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvallisuuden ja tietosuojan kehittämiseksi ja ylläpitämiseksi. Tietoturvan ja tietosuojan kehittäminen ja ylläpito ovat puolestaan osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Hallinnollisen turvallisuuden perustaso edellyttää, että
- tietoturva- ja tietosuojaperiaatteet on hyväksytty.
- tietoturvakoulutus on organisaatiossa jatkuvaa ja systemaattista.
- tietoturvavastuut ja -tehtävät on määritelty.

Hallinnollinen tietoturva ja tietosuoja on kaikkien muiden tietoturvallisuuden ja tietosuojan osa-alueiden toteutuksen ja määrittelyn perusta. Sen avulla määritellään tietoturvallisuuden ja tietosuojan suuntaviivat ja turvallisuutta parantavat toimenpiteet.

Tietoturvan ja tietosuojan hallinnassa otetaan huomioon hyvinvointialueella sovellettavan laatujärjestelmän vaatimukset. Palveluja ulkoistettaessa palvelun toimittajia vaaditaan noudattamaan hyvinvointialueella tietosuoja- ja tietoturvapolitiikkaa, tähän liittyviä käytäntöjä, sopimusehtoja sekä ohjeita. Hankintoja varten on tehty yleiset tietoturva- ja tietosuojaehdot ja henkilötietojen käsittelytoimien kuvaus. Sopimuksissa turvataan ulkoistettujen palvelujen auditointimahdollisuus.

Hallinnollisessa tietoturvassa ja tietosuojassa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään hallitsemaan tietoturva- ja tietosuojariskit. Riskejä hallitaan erikseen kuvatun riskienhallintaprosessin avulla.

**2** Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varusohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistautumis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä (mm. versiointi, lisensointi ja muutoksenhallinta).

Hyvinvointialueelle hankittaville ja hyvinvointialueella valmistamille ohjelmistoille ja tietojärjestelmille on asetettu tietoturvallisuuteen, tietosuojaan ja yhteensopivuuteen liittyvät vaatimukset.

Ohjelmiston suunnittelijan, valmistajan ja myyjän vastuu ohjelmistotuotteista määräytyy hankinta- ja käyttöoikeussopimusten mukaan.

Hyvinvointialueella ohjelmistoturvallisuuden perustaso edellyttää, että

- mikäli kyse on A tai B-luokan sosiaali- ja terveydenhuollon tietojärjestelmästä, tulee sen täyttää Terveyden ja hyvinvoinnin laitoksen (THL) määräykset olennaisista toiminnallisista ja tietoturvavaatimuksista ja sen tulee olla kirjattuna Valviran rekisteriin ennen käyttöönottoa.
- terveydenhuollon laitteella on oltava CE-merkintä, jolla valmistaja osoittaa, että terveydenhuollon laite täyttää sitä koskevat olennaiset vaatimukset. Kun laite saatetaan markkinoille, se on varustettava CE-merkinnällä.
- järjestelmä on hyvinvointialueen tietoturva- ja tietosuojavaatimusten mukainen.
- järjestelmä täyttää yleiset tietoturva ja tietosuojaehdot, jotka ovat hankintasopimuksen liitteenä.
- tietojärjestelmien ylläpidosta huolehditaan toimittajien kanssa tehtyjen ylläpitosopimusten mukaisesti.
- toimittajilta vaaditaan tuotteelleen tietoturva- ja tietosuojaselvitys, tietoturvasuunnitelma/kuvaus sekä ICT-valmiussuunnitelma (toiminta poikkeusoloissa/sopimukset).
- toimittajat avustavat tietosuojaa koskevan riskiarvion ja vaikutustenarvioinnin laatimisessa.
- järjestelmämuutoksia varten järjestelmän omistaja kartoittaa käyttäjien tarpeet, vie muutokset muutoksenhallintakäsittelyyn sekä tekee testaussuunnitelman ja – aikataulun. Järjestelmän omistaja kuvaa testaussuunnitelmassa testaukseen valtuutetut (esim. pääkäyttäjät, ohjelmistotoimittajat, ICT – palveluntuottajat), testauksen tyypit ja vastuut (omistaja: toiminnallinen testaussuunnitelma, ohjelmistotoimittaja: tekninen testaussuunnitelma) sekä kriteerit, joilla testaus katsotaan hyväksytyksi.
- tietoturvapäivityksien kriittisyys arvioidaan riskianalyysin mukaisesti ja päivitykset toteutetaan hätä-, standardi- tai normaalimuutoksena.

Hyvinvointialueella on määritelty ohjelmistojen käyttöön liittyvät velvollisuudet:

- ohjelmiin kuuluvat alkuperäiset ohjeet, dokumentit ja/tai käsikirjat on talletettu huolellisesti ja niiden sijainti on tiedossa.
- kaikki ohjelmamuutokset/päivitykset käsitellään organisaation muutostenhallintaprosessin mukaisesti ja tiedotetaan viestintäsuunnitelmassa kuvatulla tavalla.
- ohjelmien kopioinnissa noudatetaan tekijänoikeuslakia ja lisensseistä pidetään kirjaa.

Ohjeet ohjelmistojen käytöstä päätelaitteilla, kuten työasemat, puhelimet ja tabletit:

- ohjelmistojen elinkaaren hallinta ja hankintojen koordinointi on keskitetty tietohallintoon. Työasemille ja muille päätelaitteille asennettavat ohjelmat vaativat tietohallinnon hyväksynnän.
- ohjelmien asennusmediat, samoin kuin niiden kopiot, säilytetään ohjeiden mukaisesti.
- käyttäjien tulee noudattaa tietojen käsittelystä annettuja ohjeistuksia.

- pilvipalveluiden käytöstä työhön liittyvien tiedostojen tallennuspaikkana päättää tietohallinto. Sallitut tallennuspaikat tiedotetaan käyttäjille ja kirjataan ohjeisiin.

Tavoitteena on varmistaa tietojärjestelmien saatavuus, eheys ja luottamuksellisuus.

**3** Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien tietojen suojaamista. Se koskee sekä paperiasiakirjoja että digitaalisessa muodossa olevia tallenteita, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä tai muita vastaavia teknisiä laitteita. Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa.

Tietoaineistoturvallisuuteen kuuluvat ne ulkoiset normit, jotka rajoittavat tai ohjaavat tietosisällön perusteella tehtävää tietojenkäsittelyä, kuten yleiset ja/tai erityisalan lait, asetukset, viranomaismääräykset ja Kansallisarkiston ohjeet. Lisäksi on annettu ohjeita tietoaineistojen käsittelystä, tietojärjestelmien käytöstä sekä tietojen ja asiakirjojen luokittelusta julkisuus- ja salassapitosäännösten mukaisesti.

Henkilötietojen käsittelyssä noudatetaan Tietosuoja-asetuksen mukaisia periaatteita. Käsittelyä arvioidaan riskilähtöisesti. Lähtökohtana on sisäänrakennetun ja oletusarvoisen tietosuojan varmistaminen.

Hyvinvointialueella on ajantasainen, kaikki tietoaineistot kattava arkistonmuodostussuunnitelma, josta ilmenee tietoaineiston käsittelysäännöt tietojen synnystä niiden tuhoamiseen asti, turvaluokitus sekä eheyden ja käytettävyyden varmistaminen aineiston elinkaaren kaikissa vaiheissa. Luokitellun tiedon käsittelyssä huomioidaan eri turvaluokkien edellyttämät suojaustoimenpiteet.

Organisaation tietoaineistoturvallisuuden perustason edellytyksenä on, että henkilöstö tuntee ja noudattaa toiminnassaan
- henkilötietojen käsittelyä koskevia yleisiä periaatteita ja ohjeita.
- yksikkönsä toimintaa ohjaavia ja/tai rajoittavia normeja.
- tietoaineiston käsittelyä koskevia sääntöjä.
- tietojen ja asiakirjojen luokittelusääntöjä.

Kaikkia Pohjois-Savon hyvinvointialueella, ml. alihankkijoiden palveluksessa työskenteleviä, koskee vaitiolovelvollisuus ja salassapitosäännökset. Salassa pidettäviä tietoja saavat käsitellä vain henkilöt, joilla on välttämätön syy tietojenkäsittelyyn työtehtävien ja vastuiden perusteella.

Tietoja säilytetään ja vanhentuneet tiedot hävitetään arkistonmuodostussuunnitelman mukaisesti. ICT-palveluntuottaja (Istekki Oy) huolehtii, että huoltoon vietävästä, poistettavasta tai myyntiin luovutettavasta laitteesta poistetaan tai puhdistetaan tiedot aina ohjeen

mukaisesti. Kokeilukäytössä olleen tutkimus- tai hoitolaitteen palautuksen yhteydessä on huolehdittava tietojen poistamisesta laitteelta ohjeen mukaisesti. Käytettäessä pilvipalveluita on erityisesti huolehdittava sopimuksellisesti henkilötietojen käsittelyyn liittyvistä seikoista. Pilvipalveluita ei saa hankkia kuin tietohallinnon kautta ja niistä on aina tehtävä asianmukaiset tietojenkäsittely ja tietoturvasopimukset, ml. henkilötietojen käsittelytoimien kuvaus.

**4** Käyttöturvallisuus

Käyttöturvallisuus koostuu järjestelmien turvallisista käyttöperiaatteista, tiedonkäytön valvonnasta sekä jatkuvuuden turvaamisesta. Käyttöturvallisuuden avulla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojauskopioinnista sekä häiriöraportoinnista. Periaatteena on luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietojärjestelmien käytössä tietoturvallisuuden asianmukainen taso.

Käyttöturvallisuuden perustaso edellyttää, että organisaatiossa:

- on hyväksytyt sekä tietojenkäsittelyn toipumis- ja jatkuvuussuunnitelmat.
- on tietojärjestelmille nimetyt omistajat.
- päivittäin hoidettavien rutiinitehtävien ohjeistukset.
- on varasuunnitelmat käyttökatkoksia varten.
- noudatetaan tietoturvallisuudesta ja tietosuojasta annettuja ohjeita, sekä käyttöoikeuskäytäntöjä.
- tietojärjestelmiä käyttävät henkilöt tunnistetaan ja todennetaan.
- on käytössä vahvan tunnistautumisen menettelyt ja käyttäjätunnus-, salasana-, toimikortti- ja PIN-koodi –menettelyt.
- on ohjeistus haittaohjelmien torjuntaan.
- varmistetaan ja valvotaan suojausten riittävyys väärinkäytösten ennaltaehkäisemiseksi ja paljastamiseksi.
- varmistetaan tiedostojen sisältöjen käyttökelpoisuus ja tietojen saatavuus.
- varmistetaan huollon ja ylläpidon saatavuus.
- varmistetaan työasemien ja mahdollisuuksien mukaan muiden päätelaitteiden tietosisällön turvaaminen salausohjelmistolla.
- seurataan verkon tietoturvallisuustasoa säännöllisesti.
- suoritetaan tietoturvapäivitykset arvioinnin jälkeen hyödyntäen muutoshallintaa.
- seurataan verkon liikennettä, komponenttien tilaa ja verkkoon tunkeutumista ympärivuorokautisesti sekä toteutetaan poikkeuksellisen liikenteen vaatimat toimenpiteet viivytyksettä.

**5** Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja mahdollinen turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. Laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon myös kuuluvat asennuksen, takuun ja ylläpidon

lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.
Hyvinvointialueella laitteistoturvallisuuden perustasossa edellytetään, että:

- tietoverkot, ICT- ja tutkimuslaitteistot on dokumentoitu ja niistä on laadittu jatkuvuussuunnitelmat riskianalyysin pohjalta.
- varajärjestelmien käytettävyys poikkeusoloissa on varmistettu.
- laitteistojen fyysisen kunnon varmistamiseksi laadittuja ohjeita noudatetaan.
- huolto- ja ylläpitosopimukset ovat ajan tasalla ja vastaavat käytettävyysvaatimuksia.
- jokaisella laitteella on omistaja, joka vastaa laitteesta, jos kyseessä on henkilökohtaisessa käytössä oleva laite.
- yhteiskäytössä olevista laitteista vastaa yksikön hallinnollinen esimies.
- laitteista on laiterekisteri.
- tietojenkäsittelykapasiteettia seurataan, suunnitellaan ja ennakoidaan
- laitteistojen poistamisesta on kirjalliset ohjeet.
- laitteistoilla on ajantasainen suojaus haittaohjelmien torjumiseksi.
- laitteiden tietoturvapäivityksille on olemassa dokumentoitu prosessi.

**6** Fyysinen turvallisuus

Fyysisin turvallisuustoimenpitein luodaan ja ylläpidetään tietotekniikan vaatiman
käyttöympäristön toimintaolosuhteet ja suojataan ja valvotaan kiinteistö, sekä varmistetaan teknisten järjestelmien toiminta. Fyysinen turvallisuus käsittää kiinteistöjen
rakenteellisen turvallisuuden, valvontatekniikan kuten kulunvalvonta-
, hälytys-
ja videovalvontajärjestelmät sekä valvonnan ja vartioinnin. Fyysisen turvallisuuden lähtökohta on organisaation laatima riskianalyysi.

Hyvinvointialueella fyysisen turvallisuuden perustaso edellyttää, että:

- fyysisten tilojen suunnittelussa otetaan huomioon tietosuoja-, tietoturva- ja työturvallisuusnäkökohdat.
- tietoturvan kannalta oleelliset tilat pidetään lukittuna.
- toimitilojen turvallisuus on hoidettu vartioinnilla, kameravalvonnalla, teknisillä hälytysjärjestelmillä tai vastaavilla toimenpiteillä soveltuvin osin.
- korotetun suojaustason tiloissa tulee olla kulunvalvonta ja kulkuoikeudettomilla henkilöillä saattaja.
- palvelinlaitteistot on keskitetty erityisiin ICT-tiloihin, joiden rakentamisessa on noudatettu em. tiloja koskevia ohjeita.
- tutkimuslaitteistot, verkon komponentit, kytkentätilat, työasemat ja muut automaattista tietojenkäsittelyä suorittavat laitteet on sijoitettu ja suojattu luokituksensa mukaisesti.
- kriittiset laitteistot on merkitty yksilöidysti.
- kriittisille laitteistoille on tehty jatkuvuussuunnitelma ja se testataan säännöllisesti.
- varmuuskopiot on sijoitettu fyysisesti eri palotiloihin.
- kaapeloinnit suoritetaan voimassa olevan yleiskaapelointiohjeen mukaisesti
- paikallisverkon käytönvalvonta on järjestetty.

- paikallisverkolle on tehty jatkuvuussuunnitelmat.

## **7** Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron
suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvät turvallisuustoimenpiteet. Tietoliikenneturvallisuus voidaan jakaa kolmeen osa-alueeseen, joita ovat; järjestelmänhallinta, verkonhallinta sekä siirtoteidenhallinta. Tavoitteena on estää luvaton tunkeutuminen järjestelmiin tietoverkon kautta, paljastaa tunkeutumisyritykset, estää siirrettävän tiedon joutuminen sivullisten haltuun ja tarvittaessa estää sen käyttö sekä estää väärän tiedon syöttö tietojärjestelmiin.
Hyvinvointialueella tietoliikenneturvallisuuden perustaso edellyttää, että:

- tietoverkot on dokumentoitu ja niiden muutokset tapahtuvat muutoksenhallintamenettelyn mukaisesti.
- tietoihin ja tietojärjestelmiin pääsy on tarkoin määritelty.
- käyttöoikeudet tarkistetaan säännöllisesti ja käyttöoikeustasot on määritelty.
- luvaton käyttö on estetty teknisesti.
- tietoliikennelokia ja käyttöhäiriöitä seurataan säännöllisesti.
- noudatetaan työasemiin asennettavien varus-, sovellus- ja tietoliikenneohjelmien osalta annettuja ohjeita.
- varmistetaan tietoliikenneohjelmien ja -laitteiden turvallisuus ja tietoliikenneviestiensisällön muuttumattomuus.
- luottamuksellisten viestien lähettäjä ja vastaanottaja todennetaan.
- tietosuoja- ja vastuukysymykset omassa verkossa sekä eri tietoliikenneoperaattoreiden ja huollon välillä on sovittu kirjallisesti.
- langaton (WLAN) – tietoverkko suojataan käyttäen riittävän vahvaa salausta.
- verkon komponenttien tietoturvapäivitykset suoritetaan arvioinnin jälkeen hyödyntäen muutoshallintaa.
- eri turvatasojen ja eri käyttötarkoitusten verkot on tunnistettu ja verkot ovat eriytetty palomuurein ja segmentoinnin avulla.
- kiinteistönvalvontaverkko on eriytetty muista tietoverkoista.
- verkon aktiivilaitteet on suojattu ja konfiguroitu suojaustason mukaisesti.
- kriittiset tietoliikenneyhteydet on kahdennettu.
- tietoverkoissa on mekanismi tunkeutumisen estoa ja havainnointia varten.
- etäkäyttöyhteyksien tietoturvan taso pitää olla käytettyjen järjestelmien luokituksen mukainen.
- käyttöoikeuksien valtuuttamiseen, muutoksiin ja poistamisiin on dokumentoitu prosessi.

## **8** Henkilöstöturvallisuus

Henkilöstöön liittyvien riskien hallintaa kutsutaan henkilöstöturvallisuudeksi. Sen tavoitteena on ehkäistä henkilökuntaan suuntautuvia ja henkilökunnasta

tulevia uhkia. Näitä riskejä voidaan torjua sitouttamalla henkilö tietoturvalliseen toimintaan, turvallisuusselvityksillä, salassapitositoumuksilla, vastuiden ja velvollisuuksien selkeällä määrittämisellä. Lisäksi tulee olla selkeät ohjeet toimenpiteistä, kun työsuhde päättyy.

Lain yhteistoimintamenettelystä yrityksissä (334/2007) tavoitteena on edistää yrityksen ja sen henkilöstön välistä vuorovaikutusta. Yhteistyötoimikunta muodostuu työntekijöiden ja työnantajan edustajista. Tietoturvaan ja tietosuojaan liittyvät ohjeet, sopimukset ja sanktiosäännökset on hyvä saattaa yhteistyötoimikunnan tiedoksi ja myös hyväksyttää ne siellä.

LIITE 2 LAINSÄÄDÄNTÖ

## Tietoturvan ja tietosuojan lainsäädännöllinen perusta

Lainsäädäntö velvoittaa turvaamaan riittävän tietosuojan ja tietoturvan tason julkisen organisaation toiminnassa. Oikeus yksityiselämän suojaan on perusoikeus, joka on turvattu myös perustuslaissa ja EU:n perusoikeuskirjassa. Toisaalta viranomaisen toiminnassa sovelletaan myös julkisuuslakia, jonka lähtökohtana on viranomaisen asiakirjojen julkisuus, ellei salassapito rajoita julkisuutta. Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Perustuslaki (731/1999)
  - 2:10 § (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus)
  - 2:12 § (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)

- Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

- Tietosuojalaki (1050/2018)
  - 4 § (yleisen edun ja julkisen vallan käytön perusteen täsmentäminen)
  - 6 § (erityisiä henkilötietoryhmiä koskevan käsittely)
  - 28- 29 § (julkisuuslain soveltaminen, henkilötunnuksen käsittely)
  - 31-34 § (tieteellinen tutkimus, rekisteröidyn oikeudet)
  - 35 § (vaitiolovelvollisuus)

- Terveydenhuoltolaki (1326/2010)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)
- Laki sosiaalihuollon ammattihenkilöistä (817/2015)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (94/2022)
- Laki sosiaalihuollon asiakasasiakirjoista (254/2015)
- Laki sähköisestä lääkemääräyksestä (61/2007)

- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki potilaan asemasta ja oikeuksista (785/1992) (Potilasasiakirjojen salassapito)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Arkistolaki (831/1994) (Asiakirjojen laatiminen, säilyttäminen ja käyttö.)
- Työsopimuslaki (55/2001)
- Vahingonkorvauslaki (41/1974)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
- Laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista (629/2010)
- Laki lääkinnällisistä laitteista (719/2021)
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Rikoslaki 38 § (39/1889) Tieto- ja viestintärikoksista
- Laki kunnan ja hyvinvointialueen viranhaltijasta (2003/304)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki hyvinvointialueesta (611/2021)
- Laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021)