Hyvinvointiala HALI ry

Lausunto

21.06.2026

Asia: VN/10660/2026

Lausuntopyyntö yhteisötilaajasääntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista

1 Yleisiä kysymyksiä SVPL:n yhteisötilaajia ja sijaintitietojen käsittelyä koskevasta sääntelystä

1.1 Pidättekö SVPL:n yhteisötilaajia ja muita viestinnän välittäjiä sekä sijaintitietojen suojaa koskeva sääntelyä yleisesti ottaen sisällöltään ja soveltamisalaltaan asianmukaisena, kun otetaan huomioon nykyinen toimintaympäristö ja muu soveltuva kansallinen ja EU-lainsäädäntö?

Hyvinvointiala Hali ry kiittää mahdollisuudesta lauua yhteisötilaajasääntelystä ja muista sähköisen viestinnän tietosuojadirektiivin kansallisista laajennuksista.

Yhteenveto lausunnosta

Osana ministeriön selvityshanketta tulisi tehdä sote-toimialaan kohdistuvaa tarkempaa arviointia. Nykyinen sääntely ei vastaa yksityisen sote-toimialan tarpeita.

Toimialan erityispiirteenä on, että SVPL velvoittaa tallentamaan välitystietoja, mutta rajoittaa tiukasti niiden käyttöä — tavalla joka on ristiriidassa asiakastietolain selvitysvelvollisuuksien kanssa. Lisäksi sote-ala kuuluu NIS2-direktiivin piiriin kriittisenä toimialana, mikä velvoittaa aktiivisiin tietoturvatoimiin. Riskinä on, että tietoturvatoimenpiteet jäävät vajaiksi oikeudellisen epävarmuuden vuoksi.

Sääntelyn tulisi mahdollistaa tietoturvateknologian nykytason mukainen toiminta — automaattinen tietojen luokittelu, DLP-estot ja poikkeamahälytykset. Jos organisaatio käyttää etukäteen dokumentoituja, riskiperusteisia ja minimointiin perustuvia tietoturvamenettelyjä, niitä ei tulisi tulkita kielletyksi viestinnän seurannaksi. Sääntelyn toteuttamiseen liittyy tällä hetkellä merkittävää hallinnollista taakkaa.

1.1

Sote-alalla viestintä- ja lokitiedot eivät ole tavanomaista metatietoa. Ne voivat yhdessä muiden tietojen kanssa paljastaa potilaan, asiakkaan, yksikön, diagnoosin, palvelutarpeen tai työntekijän toiminnan. Tämä tekee sote-alan tilanteesta olennaisesti erilaisen kuin monella muulla alalla.

Nykyinen sääntely ei riittävästi erota toisistaan seuraavia tilanteita, jotka sote-alalla esiintyvät rinnakkain samassa organisaatiossa: potilas- ja asiakastietojen suoja, tietoturvalokitus ja tietovuotojen ehkäisy, työntekijöiden viestinnän yksityisyys, työnantajan normaali tekninen valvonta sekä asiakkaiden ja potilaiden turvallisuuteen liittyvä paikannus tai hälytysviestintä.

Epäselvyys koskee ennen kaikkea siitä, mitä saa tehdä normaalina tietoturvana, milloin mennään välitystietojen erityissääntelyn puolelle ja milloin käsittely tulkitaan työntekijän seurannaksi. Sote-alan erityispiirteet — asukasturvallisuus, viranomaisvalvonta, asiakastiedon salassapito, yksityisten palveluntuottajien monijärjestelmäympäristö ja ulkoiset ohjelmistotoimittajat — tekevät tilanteesta käytännössä monimutkaisemman kuin useimmilla muilla aloilla.

Sääntelyltä tulisi edellyttää, että se ei pakota rakentamaan erillisiä rinnakkaisia prosesseja, jos samat riskit voidaan hallita olemassa olevilla tietoturva-, loki-, DLP-, käyttöoikeus- ja tietosuojaprosesseilla.

1.2 Liittyykö SVPL:n ePrivacy-direktiiviä täydentävään sääntelyyn mielestänne piirteitä, jotka eivät asianmukaisesti huomioi nykyistä kyberturvallisuuden toimintaympäristöä, uusien digitaalisten palveluiden käytön ja tarjonnan muotoja tai uudempaa muuta kansallista ja EU-sääntelyä?

Sote-organisaatiot kuuluvat NIS2-direktiivin piiriin kriittisenä toimialana, mikä velvoittaa niitä aktiivisiin tietoturvatoimiin — lokien seurantaan, poikkeamien havainnointiin ja verkkoliikenteen analysointiin. Nämä toimet edellyttävät käytännössä välitystietojen käsittelyä. SVPL rajoittaa kuitenkin juuri tätä käsittelyä.

Tilanne on ristiriitainen: kaksi EU-lähtöistä velvoitetta vetävät eri suuntiin, eikä lainsäädäntö anna selkeää vastausta siihen, kumpi menee edelle. Tähän tarvitaan selkeyttä.

1.3 Millaisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on käsityksenne mukaan ollut käyttäjien yksityisyyden suojalle? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla?

-

2 Kyberturvallisuuden riskienhallinta ja viestinnän ja välitystietojen käsittely

2.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää sääntelyä tarkoituksenmukaisena siltä osin kuin se sääntelee sellaista välitystietojen ja viestien käsittelyä, joka liittyy erilaisilta kyberuhkilta suojautumiseen? Millaisia vaikutuksia tällä sääntelyllä on ollut organisaatioiden ja käyttäjien kyberturvallisuuteen? Onko sääntely mielestänne mahdollistanut kyberturvallisuuden riskienhallinnan tarkoituksenmukaisella tavalla vai aiheuttanut sille rajoituksia?

Sääntelyn tulee mahdollistaa riittävä tekninen valvonta ilman, että jokainen tietoturvatoimi näyttää jälkikäteen työntekijän viestinnän tarkkailulta. Tietoturvan kehityssuunta painottaa nykyään enemmän estämistä kuin jälkikäteistä selvittämistä. Nykyinen sääntely ei kuitenkaan riittävästi tue tätä lähestymistapaa — automaattiset estomekanismit, DLP-järjestelmät ja poikkeamahälytykset edellyttävät välitystietojen käsittelyä, jonka laillisuus on SVPL:n nojalla epäselvää.

Käytännön tarve sote-alalla on estää esimerkiksi:

- asiakas- tai potilastietojen lähettäminen väärälle vastaanottajalle
- salassa pidettävien tietojen lähettäminen suojaamattomalla sähköpostilla
- tietojen siirtäminen henkilökohtaisiin pilvipalveluihin
- massalataukset ja epätyypillinen käyttö
- tunnusten väärinkäyttö
- ulkoisten sovellusten kautta tapahtuvat vuodot

Sääntelyn tulee sallia automaattinen tietojen luokittelu, DLP-estot, haitallisten liitteiden ja linkkien suodatus, epätyypillisten tietovirtojen hälytykset ja käyttöoikeuspoikkeamien havainnointi ilman raskasta erillistä menettelyä. Nämä ovat tietoturvateknologian normaalia nykytasoa.

2.2 SVPL 18 luvun (ns. Lex Nokia) mukaisia toimenpiteitä on käytetty vähemmän, kuin sääntelyn valmistelussa aikanaan ennakoitiin. Millaisia syitä arvioitte olevan sen taustalla, ettei toimenpiteitä ole otettu käyttöön? (SVPL 18 luvussa säädetään yhteisötilaajan oikeudesta käsitellä tietyin edellytyksin välitystietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi.)

SVPL:n 18 luvun mukainen menettely on käytännössä raskas, juridisesti riskialtis, ja sen käyttö on mainehaittaakin aiheuttavaa. Työnantajalle järkevin malli on, että tietoturvan perustoimet saa tehdä normaalina riskienhallintana, kun ne ovat dokumentoituja, rajattuja, lokitettuja ja kohdistuvat ensisijaisesti järjestelmä- ja tietovirtoihin — ei yksittäisten työntekijöiden seuraamiseen.

Sote-alan näkökulmasta SVPL:n 18 luku on ainoa säännös, joka periaatteessa mahdollistaisi luvattoman potilastietokatsauksen tai tietovuodon jälkikäteisen selvittämisen. Asiakastietolaki velvoittaa tähän — mutta SVPL rajoittaa sen toteuttamista käytännössä. Sääntely tulisi tehdä käytännössä toimivaksi.

2.3 Voiko SVPL:n tietoturvatoimenpiteistä säätävän 272 §:n ja SVPL 18 luvun muun muassa liikesalaisuuksien paljastamisen selvittämistä koskevan sääntelyn (Lex Nokia) suhde aiheuttaa mielestänne soveltamishaasteita? Millaisia?

SVPL 272 § asettaa yleisen tietoturvavelvollisuuden — organisaation on huolehdittava verkkonsa tietoturvasta. SVPL:n 18 luku puolestaan antaa erityisen oikeuden käsitellä välitystietoja väärinkäytösten selvittämiseksi tietyin edellytyksin. Näiden kahden säännöksen soveltamisalat eivät täysin vastaa toisiaan, mikä aiheuttaa käytännön tulkintaepävarmuutta.

Sote-alalla tämä konkretisoituu esimerkiksi tilanteessa, jossa epäillään luvatonta potilastietojen katselua. Tietoturvavelvollisuus (272 §) edellyttää reagointia — mutta 18 luvun mukaiset edellytykset selvittämiselle voivat olla niin tiukat tai epäselvät, että toimenpiteeseen ei uskalleta ryhtyä. Organisaatio joutuu arvioimaan, onko kyse 272 §:n sallimasta tietoturvatoimesta vai 18 luvun edellyttämästä erillisestä menettelystä — ja tähän ei ole selkeää vastausta.

2.4 Voiko SVPL:n ePrivacy-direktiiviä täydentävä sääntely estää organisaatioita käyttämästä viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mistä SVPL:n vaatimuksesta tämä johtuu? Onko SVPL:n sääntely asettanut teille esteitä tai rajoituksia tällaisten toimenpiteiden käyttöön?

Työnantajalla tulisi olla oikeus käyttää normaaleja, dokumentoituja tietoturvatoimia — automaattinen tietojen luokittelu luottamuksellisuuden mukaan, DLP-estot, epätyypillisten tietovirtojen hälytykset, käyttöoikeuspoikkeamien havainnointi — ilman että ne tulkitaan kielletyksi viestinnän seurannaksi. Sote-alalla tämä on erityisen kriittistä, koska tietovuodon kohteena ovat potilastiedot. Nykyinen sääntely luo tilanteen, jossa organisaatio voi joutua valitsemaan: joko se jättää nämä toimet tekemättä oikeudellisen epävarmuuden takia, tai se ottaa ne käyttöön ja riskeeraa sääntelyn rikkomisen. Kumpikin vaihtoehto on huono.

3 Muu kuin kyberturvallisuuden riskienhallintaan liittyvä välitystietojen ja viestinnän käsittely

3.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen ja viestinnän käsittelyn sääntelyä tarkoituksenmukaisena siltä osin kuin tietojen käsittely liittyy muuhun kuin erilaisilta kyberuhkilta suojautumiseen? Onko sääntelyn mahdollistamat käsittelytilanteet määritelty tarkoituksenmukaisesti?

-

3.2 Onko ja millä tavoin SVPL:n sääntely edistänyt tai tukenut sellaisten muiden viestinnän tai välitystietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa, jotka eivät liity kyberuhkien torjumiseen? Millaisten toimenpiteiden?

Ks. kohdat 2.3 ja 2.4.

3.3 Voiko SVPL:n sääntely mielestänne estää ottamasta käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä toimenpiteitä, jotka eivät liity kyberuhkien torjumiseen mutta olisivat käsityksenne perusteltuja ja muun soveltuvan lainsäädännön mukaisia, tai rajoittaa niiden käyttöä? Mitä toimenpiteitä? Mikä lainsäädännön vaatimus voi muodostua esteeksi? Onko SVPL:n sääntely estänyt teitä ottamasta jotakin tällaista toimenpidettä käyttöön?

Sote-alalla käytetään työviestintään kaupallisia pikaviestimiä, vaikka asiakas- ja potilastietoja ei tule käsitellä epävirallisissa viestikanavissa. Näiden sovellusten ongelma ei ole vain viestin sisältö vaan myös metatieto: kuka viestii, milloin, kenen kanssa, mistä laitteesta. On lisäksi huomattava, että osa sovelluksista — kuten Signal — ei kerää metatietoja edes itse, jolloin tallennusvelvoitetta ei teknisesti voi täyttää vaikka se syntyisi.

Tarvitaan selkeä kansallinen ohje siitä, miten työnantajan hyväksymät hallitut viestintäkanavat erotetaan epävirallisista, ja milloin kaupallisen sovelluksen käyttö työviestintään synnyttää tallennusvelvoitteen.

4 Hallinnollinen taakka ja lisäkustannukset sekä rajat ylittävät tilanteet

4.1 Millaisia hallinnollisia vaikutuksia SVPL:n ePrivacy-direktiiviä täydentävällä sääntelyllä on ollut organisaatioiden ja käyttäjien kannalta? Pidättekö sääntelyä tarkoituksenmukaisena tältä kannalta vai onko sääntely aiheuttanut mielestänne tarpeetonta hallinnollista taakkaa?

Jokainen uusi sääntelyvelvoite lisää organisaation hallinnollista työtä käytännössä välittömästi. Kustannusten tarkka arviointi on sinänsä jo haasteellista, mutta ne ovat merkittäviä. Työmäärä kasvaa tietosuojavastaavalla ja tietosuojaryhmällä: DPIA-arvioinnit, DPA-sopimukset, käsittelytoimien kuvaukset sekä ulkoisten ohjelmistotoimittajien liittyminen organisaation omaan tietoarkkitehtuuriin edellyttävät jatkuvaa ylläpitoa ja päivittämistä.

Sote-alalla hallinnolliseen taakkaan liittyy lisäksi erityinen riski: mitä enemmän sensitiivistä tietoa kerätään ja käsitellään eri järjestelmissä, sitä suurempi on vahingon mittakaava tietovuodon sattuessa. Tietoaltaiden tulee siksi sisältää vain sellaista tietoa, jolla on perustelu myös toisiolain mukaisessa käytössä. Sensitiivinen tieto väärissä käsissä on myös potilaalle vaarallista.

4.2 Poikkeaako SVPL:n sääntely käsityksenne mukaan merkittävästi muiden EU-maiden sääntelystä? Millä tavoin?

-

4.3 Millaisia vaikutuksia mahdollisilla eroilla sääntelyssä voi olla tai on ollut organisaatioiden toiminnan kannalta tai sijoittautumis- ja investointipäätöksiä tehtäessä?

-

4.4 Voiko SVPL:n sääntely aiheuttaa lisäkustannuksia otettaessa käyttöön viestinnän tai välitystietojen käsittelyä edellyttäviä riskienhallintatoimenpiteitä tai muita toimenpiteitä (esim. tietojärjestelmien tai

prosessien muuttaminen Suomen lainsäädännön mukaiseksi)? Mistä syystä? Onko SVPL:n sääntely aiheuttanut teille tällaisia lisäkustannuksia?

-

4.5 Voiko SVPL:n sääntely mielestänne estää tai rajoittaa muissa EU-maissa hyödylliseksi havaittujen järjestelmien, niiden toimintojen tai menettelyjen käyttöä Suomessa? Voiko sääntely edellyttää niiden merkittävää muokkaamista Suomen lainsäädännön mukaiseksi toimittaessa monikansallisessa toimintaympäristössä? (Esim. valmisohjelmistot, pilvipalvelut ja monikansallisen konsernin yhteiset viestintäjärjestelmät.) Mistä vaatimuksesta tämä voi johtua? Onko näin tapahtunut kohdallanne ja miten ratkaisitte tilanteen?

-

5 Välitystietoja ja viestintää koskevien säännösten suhde yleiseen tietosuoja-asetukseen

5.1 Oletteko havainnut erityisiä haasteita SVPL:n välitystietoja ja viestintää koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

SVPL on yleiseen tietosuoja-asetukseen nähden erityislaki eli sitä sovelletaan ensisijaisesti silloin kun kyse on sähköisen viestinnän välitystiedoista. Sote-alalla tämä tarkoittaa, että SVPL:n rajoitukset voivat käytännössä estää sellaisen tietojen käsittelyn, joka GDPR:n nojalla muutoin olisi mahdollista esimerkiksi oikeutetun edun tai lakisääteisen velvoitteen perusteella. Lisäkerroksen tuo vielä GDPR:n artikla, joka asettaa terveystiedoille erityistä suojaa vaativan käsittelyperusteen. Sote-organisaatio joutuu siis navigoimaan kolmen päällekkäisen sääntelyn välillä samanaikaisesti.

Sote-organisaatiolla on käytännössä kaksi erillistä lokijärjestelmää: SVPL:n mukainen välitystietoloki, jota hallinnoi tyypillisesti IT, sekä asiakastietolain mukainen potilastietoloki, jota hallinnoi terveydenhuollon johto. Nämä ovat eri tarkoituksia varten eikä niitä saa sekoittaa — ensimmäinen koskee viestinnän teknisiä tunnistetietoja, jälkimmäinen potilastietojen käsittelyä. Käytännön riski syntyy erityisesti pilvipalveluissa, joissa järjestelmät saattavat teknisesti limittyä ilman että kukaan on tietoisesti suunnitellut niiden erillään pitämistä. Tarvitaan selkeä ohje siitä, miten nämä kaksi lokijärjestelmää pidetään erillään myös pilvipohjaisissa ympäristöissä.

6. Sijaintitietojen käsittely

6.1 Onko SVPL:n ePrivacy-direktiiviä täydentävä sääntely edistänyt tai tukenut sijaintitietojen käsittelyä edellyttävien toimenpiteiden käyttöönottoa? Onko sääntely toteuttanut yksityisyyden ja henkilötietojen suojaa mielestänne tarkoituksenmukaisella tavalla? Millä tavoin?

Sijaintitietojen käyttö sote-alalla voi olla perusteltua turvahälytyksissä, liikkuvassa työssä, yksintyöskentelyn turvallisuudessa tai asiakaskäyntien varmistamisessa. Työntekijän jatkuvaan paikantamiseen ei yleensä ole tarvetta.

Sote-alalla on tunnistettu tarve käyttää sijaintiteknologiaa myös asiakasturvallisuuden varmistamiseksi — esimerkiksi muistisairaan henkilön paikantamiseen, jos hän poistuu

asumisyksiköstä yksin. Tilanne jää useiden lakien — SVPL:n sijaintitietosääntely, sosiaalihuollon asiakaslaki, laki sosiaalihuollon asiakkaan itsemääräämisoikeudesta — väliin. Suostumusvaatimus on esimerkkitapauksessa erityisen ongelmallinen.

Sääntelyn tulisi erottaa selkeästi toisistaan:

- asiakkaan tai potilaan turvallisuuteen perustuva paikannus
- työntekijän työturvallisuuteen perustuva paikannus
- työtehtävän suorittamiseen välttämätön sijaintitieto
- työntekijän seurantaan tai tehokkuusvalvontaan liittyvä paikannus

Paras malli on minimointi: paikannusta vain jos se on välttämätöntä, käyttötarkoitus on ennalta määritelty, tieto säilytetään lyhyen ajan ja pääsy on rajattu.

6.2 Pidättekö SVPL 20 luvun sijaintitietojen käsittelyä koskevan lainsäädännön soveltamisalaa selvänä suhteessa esimerkiksi työnantajien toteuttamaan työntekijöiden tai ajoneuvojen paikantamiseen? Minkälaisia haasteita sääntelyn soveltamisalan tulkintaan voi liittyä?

-

6.3 Voiko sijaintitietojen käsittelyä koskeva SVPL:n ePrivacy-direktiiviä täydentävä sääntely (kuten siihen liittyvä käyttäjän suostumuksen vaatimus) estää tai rajoittaa työpaikoilla toimenpiteitä, jotka olisivat käsityksenne mukaan perusteltuja ja muun soveltuvan lainsäädännön mukaisia? Mitä toimenpiteitä?

Ks. 6.1. Sijaintitietojen käsittelyä koskevan sääntelyn soveltamisala ja käsittelyperusteet ovat tulkinnanvaraisia erityisesti turvallisuuskriittisissä tilanteissa. Kotihoidossa, ensihoidossa ja päivystyksessä sijaintitiedon hyödyntäminen on suoraan yhteydessä potilasturvallisuuteen. Lisäksi turvallisuustilanteet — yksin työskentelevä hoitaja kotikäynnillä tai droonihavainto sairaalakiinteistön läheisyydessä — voivat edellyttää henkilöstön sijaintitiedon hyödyntämistä nopeasti. Sääntelyn epäselvyys siitä, milloin käsittely on perusteltua ja millä perusteella, voi muodostua esteeksi juuri näissä tilanteissa.

6.4 Voiko sijaintitietojen käsittelyä koskevan sääntelyn soveltamisala ja tulkinta aiheuttaa haasteita paikannettaessa muita kuin työntekijöitä, esimerkiksi tarjottaessa mobiililaitteen paikannusta hyödyntäviä palveluita yleisölle? Millaisia haasteita? Onko sääntelyn suhde evästeiden ja muiden päätelaitteiden tietojen käyttöä sääntelevään SVPL 205 §:ään mielestänne selvä?

Sote-alalla toimii organisaatioita, jotka tarjoavat palveluja joissa sijaintitietoa hyödynnetään osana palvelun sisältöä — esim. turvarannekkeet, hälytysjärjestelmät ja etämonitorointipalvelut. Tällöin organisaatio toimii SVPL:n tarkoittamana lisäarvopalvelun tarjoajana, ja sääntely koskee sitä tässä roolissa. Moni toimija ei kuitenkaan välttämättä tunnista olevansa tässä asemassa, eikä sääntelyn soveltamisala ole näiltä osin riittävän selkeä. Tarvitaan ohjeistus siitä, milloin sijaintitietoa hyödyntävä palvelu synnyttää lisäarvopalvelun tarjoajan velvoitteet.

6.5 Oletteko havainnut erityisiä haasteita SVPL:n sijaintitietoja koskevan sääntelyn soveltamisessa yhdessä yleisen tietosuoja-asetuksen kanssa? Millaisia?

SVPL:n suostumusvaatimus sijaintitietojen käsittelyssä voi olla tiukempi kuin GDPR edellyttäisi. GDPR sallii henkilötietojen käsittelyn myös muilla perusteilla — kuten oikeutettu etu tai lakisääteisen velvoitteen täyttäminen. Sote-alalla tämä on erityisen ongelmallista tilanteissa, joissa käsittelyn peruste on selkeästi oikeutettu mutta suostumuksen hankkiminen on käytännössä hankalaa tai tilanteen luonteen takia mahdotonta.

7 Sääntelyn kehittämistä koskevat ehdotukset

7.1 Pidättekö SVPL:n ePrivacy-direktiiviä täydentävää välitystietojen, viestinnän ja sijaintitietojen käsittelyä koskevien sääntelyn kehittämistä tarpeellisena? Jos kyllä, millä tavoin havaitsemanne haasteet SVPL:n säännösten soveltamisessa tulisi mielestänne ratkaista? Tulisiko sääntelyn soveltamisala määrittää toisin kuin nykyisin tai sääntelyä muuttaa jollakin muulla tavoin? Mitkä arvioitte ehdotuksenne merkittävimmiksi vaikutuksiksi?

Kansallisia lisävelvoitteita tulisi keventää, jos ne eivät tuota selkeää lisäsuojaa EU-tasoon nähden. Lakiin tai viranomaisohjeeseen tarvitaan sote-alan esimerkit hyväksytyistä käsittelytilanteista, kuten:

- väärään osoitteeseen lähetetyn potilastiedon käsittely
- epäilty massalataus
- epävirallinen pikaviestiryhmä työasioissa
- kotihoidon paikannus
- DLP-järjestelmän hälytys
- ulkoisen järjestelmätoimittajan lokien käsittely
- viranomaisen tietopyyntö

Tavoitteena tulisi olla eräänlainen turvasatama työnantajalle: jos organisaatio käyttää etukäteen dokumentoituja, riskiperusteisia ja minimointiin perustuvia tietoturvamenettelyjä, niitä ei tulisi tulkita kielletyksi viestinnän seurannaksi. Automaattinen tietojen luokittelu, DLP, lokivalvonta ja poikkeamahälytykset tulisi nimenomaisesti sallia salassa pidettävän tiedon suojaamiseksi.

Sääntelyn tulee olla teknologianeutraalia eikä se saa sitoa organisaatiota johonkin yksittäiseen järjestelmä- tai dokumentointimalliin. Hallinnollista taakkaa voidaan vähentää hyväksymällä olemassa olevat tietosuoja-, tietoturva-, käyttöoikeus- ja lokienhallintaprosessit, jos ne täyttävät vaatimukset — ilman erillisiä päällekkäisiä raportteja.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

Tässä lausunnossa esitetyt havainnot perustuvat rajalliseen otokseen alan toimijoilta kerättyihin kokemuksiin. Lausunnonantaja katsoo, että sote-toimialan ja yksityisen sote-alan erityispiirteet — potilasturvallisuusvelvoitteet, arkaluonteiset tiedot, monijärjestelmäympäristö ja digitaalisten palvelujen nopea kehitys — edellyttävät omaa toimialakohtaista arviointia osana lainsäädäntöuudistusta. Tätä arviointia ei voida korvata yleisellä työnantaja- tai ICT-alan näkökulmalla.

Vastaamo-tapaus osoittaa, että sote-alalla tietovuodon vaikutus ei ole vain tekninen tai taloudellinen, vaan myös inhimillinen, maineeseen vaikuttava ja asukasturvallisuuteen liittyvä. Toisaalta sääntely ei saa johtaa siihen, että kaikki mahdollinen tieto kerätään varmuuden vuoksi — sote-alalla liiallinen tietojen kerääminen kasvattaa vahingon määrää, jos tieto myöhemmin vuotaa.

Tavoitteena tulisi olla vähemmän päällekkäistä sääntelyä, enemmän selkeitä sallittuja käyttötapauksia ja parempi mahdollisuus suojata salassa pidettävää tietoa ilman juridista epävarmuutta.

Jokinen Esa
Hyvinvointiala HALI ry