Valtori

Lausunto

18.06.2026 Valtori/1555/00 05 00/2026

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?

Kokonaisuutena pidämme sääntelyn tavoitteita tarkoituksenmukaisina. Sähköisen viestinnän luottamuksellisuus korostuu mm. palveluiden digitalisoituessa ja sähköisten viestintävälineiden yleistyessä.

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?

Kyberturvallisuuden valvontamenetelmät ovat kehittyneet yhä hienojakoisemmiksi ja laajemmiksi. Valvonta ei välttämättä kohdistu enää yksinkertaistettuna ”viestin välitykseen” vaan laajemmin käyttäjän toimintaan digitaalisessa toimintaympäristössä ja viestinnässä. On tärkeää, että SVPL sääntely mahdollistaisi asianmukaisen tietoturvallisuuden varmistamisen kehittyneillä tekniikoilla, turvaten kuitenkin heikommassa asemassa olevien rekisteröityjen (kuten työntekijöiden) yksityisyyden suojan. Uusi tietoturvaa koskeva sääntely (esim. NIS2) ja yhä kehittyneemmät hyökkäystekniikat edellyttävät, että tietoturvallisuutta voidaan varmistaa teknisesti.

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?

Sääntely on turvannut käyttäjien yksityisyyden suojaa siten, että viestinnän välittäjällä on mahdollisuus vedota säädöksiin, mikäli yhteisötilaaja pyytäisi esimerkiksi laajalti pääsyä käyttäjän viestintä- tai sijaintitietoihin. Käyttäjä on usein esimerkiksi työntekijän tai kansalaisen asemassa eli tietosuojalainsäädännön näkökulmasta ns. heikommassa asemassa. Kokonaisuutena suojaaminen on tarkoituksenmukaista. Muidenkin yksilöiden henkilötietojen suojaamiseksi olisi kuitenkin tarpeen

säännellä selkeästi, että välitystietoja voidaan hyödyntää asianmukaisen tietoturvatason varmistamiseen.

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?

Pääsääntöisesti sääntely on mahdollistanut kyberuhilta suojautumista. Mikäli sääntelyä uudistetaan, tulisi selkeästi mahdollistaa kyberturvallisuuteen liittyvä välitystietojen käsittely nykyistä laajemmassa merkityksessä. Myös tekoälyn hyödyntäminen ja muut nousevat teknologiat tulisi huomioida siinä, miten välitystietoja voidaan käsitellä nimenomaan tietoturvan varmistamisen tarkoituksiin. Tällä hetkellä on oikeudellista epävarmuutta, voidaanko tiettyjä edistyneitä teknologioita (esim. signaalianalyysi, tekoälyavusteinen uhka-analyysi) hyödyntää, mikäli ne analysoisivat myös viestintään yhdistettävää tietoa.

Nykysääntelyssä korostuu ulkoisten uhkien torjunta, mikä onkin tärkeä osa tietoturvallisuuden varmistamista. Sääntely puhuu ”viestintäverkon luvattomasta

käytöstä, esim. laitteen tai ohjelman asentamisesta tai sivulliselle pääsyn avaamisesta”. Kehittyneet tietoturvateknologiat tunnistavat kuitenkin myös sisäisiä uhkia ja riskikäyttäytymistä (insider threat), mikä tulisi mahdollistaa lainsäädännöllä nimenomaan tietoturvatarkoituksiin.

Pidämme tarkoituksenmukaisena, että manuaalinen välitystietojen tarkastelu olisi edelleen tiedonantovelvollisuuden alaista (152 §, 153 §). Tämä vahvistaisi rekisteröidyn oikeuksia ja käsittelyn läpinäkyvyyttä sekä ennaltaehkäisisi mahdollisen vallan epätasapainoon liittyvää välitystietojen väärinkäyttöä (esim. työntekijän epäasiallinen valvonta). Tiedonantovelvollisuuden muotoa tulisi kuitenkin modernisoida siten, että se voitaisiin antaa esimerkiksi digitaalisesti.

Manuaalisen välitystietojen käsittelyn osalta olisi tärkeää selkeyttää, kattaako se myös tilanteet, joissa viestinnän välittäjä tarkastaa ”rutiininomaisesti” hälytyksen pohjalta asiakkaan viestinnästä nousseen hälytyksen asiakkaan lukuun/puolesta. Eli tulisiko näistä, usein tietoturvaa sivuavista tai väärinkäytösepäilyyn liittyvistä tilanteista, laatia vastaava selvitys. Tällä hetkellä oikeudellinen tulkinta on hieman epäselvä.

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.)

Taustalla voi olla epäselvyys tulkinnasta siinä, milloin kyse on SVPL 18 mukaisesta välitystietojen käsittelystä. Monissa edistyneissä tietoturvajärjestelmissä analysoidaan käytännössä välitystietoa ja niiden pohjalta saatuja hälytyksiä. Yhteisötilaajilla ja viestinnän välittäjillä voi kuitenkin olla epäselvyyttä siitä, kuuluuko tällainen käsittely SVPL 18 luvun alaan.

Tärkeää olisi selkeyttää, kuuluuko yhteisötilaajan käyttämän tietoturvaohjelmiston suorittama analyysi ja sen pohjalta mahdollisesti suoritettava manuaalinen tarkastelu (esim. viestin linkin analyysi, kalastelukampanjan tunnistaminen) SVPL 18 luvun alaan, vaikka käytännössä tarkastelun suorittaisi viestinnän välittäjä. ks. selkeyttämistarpeista myös seuraava vastaus.

Viestinnän välittäjän ja yhteisötilaajan käsittelyoikeudet SVPL 18 luvun tilanteissa olisi hyvä ilmoittaa selkeämmin, jotta osapuolet uskaltaisivat luovuttaa tietoja toisilleen. SVPL 137 §:n taustatöissä voisi avata käsittelyoikeutta hieman laajemmin.

Esimerkki 1: voiko viestinnän välittäjä antaa yhteisötilaajalle tietoja 272 § perusteella tehtävästä selvityksestä?

Esimerkki. 2: Onko SVPL 18 luvun tilanteissa kyse pelkästään yhteisötilaajan yksinomaisesta käsittelyoikeudesta? Jos yhteisötilaajalla ei ole osaamista toteuttaa SVPL 18 mukaisia toimenpiteitä, voivatko viestinnän välittäjä ja lisäarvopalvelun tuottaja toimia yhteisötilaajan puolesta. Jos tämä on sallittua, niin tarvitaanko käsittelyyn joka kerta yhteisötilaajan lupa, vai voivatko muut osapuolet toimia aiemmin annetun mandaatin perusteella?

Esimerkki 3: pyytäisimme tarkentamaan 138 § 2 momentin taustakuvaukseen myös, että voiko yhteisötilaaja antaa tilaajalle tarkkoja henkilötietoja vai pitääkö

tietojen olla anonyymejä.

Esimerkki 4: Pitäisikö tarkentaa, että jos 137 § mukaan viestejä ja välitystietoja saa käsitellä vain tilaajan lukuun toimiva, niin tarkoittaako se sitä että tilaaja ei saa käsitellä ko. tietoja?

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?

Kyllä. Tämä on keskeisin soveltamishaaste tällä hetkellä SVPL alaisessa toiminnassa erityisesti silloin, kun asiakas (yhteisötilaaja) hankkii tietoturvatoiminnot ja viestintäpalvelut palveluntuottajalta (usein viestinnän välittäjä).

On epäselvää, miltä osin viestinnän välittäjän tietoturvatoiminnoissa suorittama välitystietojen käsittely kuuluu tietoturvatoimenpiteisiin ja milloin se muuttuu YTja tiedonantovelvollisuuden alaiseksi käsittelyksi (josta yhteisötilaajalla on velvoitteita).

Tyypillistä on, että tietoturvatarkoituksissa analysoidaan esim. sähköpostien tai muiden viestien kokoa, vastaanottajaa ja esimerkiksi tarkastetaan automaatioiden avulla linkkejä. Tietoturvallisuuteen liittyvät järjestelmät myös nostavat näiden signaalitietojen pohjalta hälytyksiä asiantuntijan tarkastettavaksi ja usein tarkastus tehdään manuaalisesti tietoihin, jotka voivat sisältää esim. lokitietoja, joista käy ilmi välitystietoa. Tältä osin on epäselvää, tuleeko käsittelystä tehdä selvitys a) silloin, jos käsittelyssä ei todeta poikkeavaa b) silloin, jos todetaan poikkeama ja siitä tiedotetaan yhteisötilaajaa tai c) molemmissa edellä mainituissa tilanteissa. Lisäksi epäselvää on, muuttuuko tulkinta, jos tarkastuksen tekee viestinnän välittäjän sijaan yhteisötilaaja itse viestinnän välittäjän toimittamaan tietoon.

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?

Ei varsinaisesti estä mutta oikeudellinen epäselvyys aiheuttaa epävarmuutta kehittyneiden tietoturvaominaisuuksien käytölle.

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?

Kyllä, On tarkoituksenmukaista, että viestinnän välitystietojen käsittely on sallittua myös liikesalaisuuksien paljastamisen selvittämiseksi.

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?

SVPL ei ole varsinaisesti edistänyt kyseisten toimenpiteiden käyttöönottoa vaikkakin se mahdollistaa käsittelyn. Kyse on ehkä osin siitä, että liikesalaisuuksien paljastamisen selvittämisen mahdollisuutta ei ole laajalti tunnistettu tai haluttu ottaa käyttöön.

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?

Emme tunnista tällaisia tarkoituksia.

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?

Sääntely on nähdäksemme lisännyt välitystietojen käsittelyn läpinäkyvyyttä. Hallinnollista taakkaa liittyy epäselvyyksiin viestinnän välittäjän käsittelyoikeudesta sekä manuaalisen käsittelyn tulkinnasta, joita on käsitelty tarkemmin edellä. Sijaintitietojen käsittelyn osalta (erityisesti välitystietoihin sisältyvät epäsuorat tunnisteet, sovellusten käyttämät sijaintitiedot) tulisi selkeyttää oikeustilaa.

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?

Lisäkustannuksia voi aiheutua, jos tuotteeseen on tarpeen tehdä räätälöintiä. Toimittaja vastaa kuitenkin tuotteen soveltuvuudesta kyseisen markkinan sääntelyvaatimuksiin emmekä tunnista suoraa kustannusvaikutusta sen osalta. Välitystietojen käsittely teknisesti on melko tavanomaista ja lähinnä kustannukset liittyvät lisääntyneeseen työmäärään manuaalisen käsittelyn kirjaamisen osalta.

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?

Emme tunnista juridisesti, että EU:n markkinoilla soveltuva järjestelmä olisi ”vain” SVPL pohjalta yhteensopimaton. Tietyt USA:n tai muiden kolmansien maiden markkinoille soveltuvat järjestelmät eivät välitystietojen suojaamisen ja työnantajan valvonnan osalta ole yhteensopivia. Tämä liittyy kuitenkin laajempaan sääntelykehikkoon (mm. GDPR) sekä yksityisyyden vahvempaan suojaan perusoikeutena eikä vain SVPL:ään.

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?

Epäselvyyttä on erityisesti siinä, mikä katsotaan välitystiedoksi ja onko välitystieto myös henkilötietoa. Välitystiedon uusi määritelmä parantaa tätä tulkinnallista epäselvyyttä mutta olisi tärkeää saada käytännön esimerkkejä uuden määritelmän soveltamiseen.

Vastuunjako Traficomin ja Tietosuojavaltuutetun välillä on osin epäselvä. On vaikeaa erottaa, mikä on tosiasiassa välitystietoa tai sijaintitietoa (esim. viestin välityksessä IP-osoite). Erityisesti epäsuorat sijaintitiedot jäävät usein välitystiedon ja sijaintitiedon välimaastoon.

Tilanteissa, joissa Traficom ja Tietosuojavaltuutettu ovat molemmat vastuuviranomaisia tapauksissa, on viranomainen antanut itsenäisiä päätöksiä omalta osaltaan. Olisi suositeltavaa, että vastuuviranomaiset tekisivät yhteistyötä ja antaisivat lausuntonsa puolin ja toisin, taikka tekisivät yhteisen päätöksen, jossa molempien osuudet on huomioitu. Tällöin ratkaisun vastaanottaja sekä yleisö saisivat kokonaisen toimintaohjeen, eikä toisen viranomaisen osuuden ratkaisua tarvitsisi arvailla.

Tietosuojavaltuutetun osuuteen on suhteellisen vähän ohjeistusta. Ohjeistuksen määrää olisi hyvä lisätä, jotta tulkitseminen helpottuisi. Lisäksi olisi hyvä, jos tietosuojavaltuutetulla olisi lisää resursseja kysymyksiin vastaamisessa, sillä tulkintaongelmia tulee säännöllisesti ja niihin olisi hyvä saada nopeasti ohjeita.

Vastuuviranomaiset voisivat tarjota esimerkiksi kerran vuodessa yhdessä koulutusta alan toimijoille, sillä SVPL tulkinnassa ja rajanvedoissa on paljon haasteita.

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?

Osittain. Kuten edellä on todettu, sijaintitiedon käsite suhteessa välitystietoon on osittain epäselvä. Selkeytys on hyvä, mutta epäsuoran sijaintitiedon osalta olisi tärkeää selventää oikeustilaa ja toimivaltaa. Välitystietoa, joka voi osin paljastaa sijaintia, käsitellään myös tietoturvan varmistamiseksi.

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?

Ei. On epäselvää, missä tilanteessa käyttäjältä tulee pyytää suostumus ja kattaako suostumuksen pyytäminen esimerkiksi työlaitteisiin tarjottavat sovellukset.

Kuten edellä on todettu, sijaintitiedon käsite on hieman tulkinnanvarainen. On erityisen epäselvää, millä edellytyksillä välitystietoja (jotka voivat sisältää sijaintitietoa) voidaan käsitellä tietoturvatarkoituksiin tai muihin lakisääteisiin tarkoituksiin. Tulisi täsmentää, koskeeko sääntely vain GPS- ja satelliittipaikannusta mutta ei esim. IP-osoitteeseen liittyvää käsittelyä.

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?

Emme näe, että sääntely suoraan estäisi esim. tietoturvatoimien toteuttamista. Kokonaisuutena on hyvä, että sijaintitietojen käsittelyä säännellään erikseen niiden erityisen luonteen vuoksi. On kuitenkin epäselvää, vaatiiko esim. tietoturvatoimien vuoksi tapahtuva käsittely nimenomaisen suostumuksen.

Mikäli suostumusedellytystä muokataan tai se ei koske tietoturvakäsittelyä, pidämme tärkeänä, että sijaintitiedon käyttöä koskevat käyttötarkoitukset olisi määritelty siten, että heikommassa asemassa olevia rekisteröityjä kuten työntekijöitä suojataan.

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?

-

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

Sijaintitiedon käsittelyn reunaehdot ovat epäselvät erityisesti, kun tulkitaan SVPL, työelämän tietosuojalakia ja yleistä tietosuoja-asetusta yhdessä.

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?

Kyllä. Sijaintitiedon käsittelyä ja valvovien viranomaisten suhdetta tulisi täsmentää. Välitystietojen (ja epäsuorien sijaintietojen) käsittely viestinnän välittäjän toimesta tietoturvatarkoituksiin henkilötietojen asianmukaiseksi suojaamiseksi tulisi mahdollistaa.

Manuaalisen käsittelyn ilmoitusvelvollisuuden alaa tulisi selkeyttää (ks. esimerkit yllä) ja modernisoida ilmoituksen muotoa kaksi allekirjoitusta edellyttävästä muodosta.

Samalla on kuitenkin huomioitava, ettei sääntely laajennu tarpeettomasti sallimaan työntekijöiden epäasiallista seurantaa. Läpinäkyvyyden varmistamiseksi olisi hyvä, että yhteistoiminta- ja informointivelvoitteet säilytetään.

Lisäksi voi olla tarpeen säätää selkeyttävästi perusteita, joilla esim. viranomaiselle voidaan luovuttaa välitystietoja (esim. viittaus pakkokeinolakiin).

Selkeytysten vaikutuksena hallinnollinen taakka epäselvän lainsäädännön ohjauspyynnöistä vähenee, tietoturvallisuuden edistyneitä toimintoja voidaan ottaa käyttöön ja silti välitys- ja sijaintitietojen käsittely pysyy läpinäkyvänä.

8 Muut huomiot

8.1 Tässä voitte esittää mahdolliset muut huomionne selvitystä varten.

Kokonaisuutena välitystietojen määritelmä on uudistetussa ehdotuksessa kattavampi ja vastaa paremmin nykymuotoista käsittelyä. Soveltamisen ohjauksessa on tarpeen saada konkreettisia esimerkkejä.

Lisäksi voi olla tarpeen säätää selkeyttävästi perusteita, joilla esim. viranomaiselle voidaan luovuttaa välitystietoja (esim. viittaus pakkokeinolakiin).

Saira Antti
Valtori