27.5.2021

EOAK/6511/2020

Ratkaisija: Apulaisoikeusasiamies Pasi Pölönen

Esittelijä: Oikeusasiamiehensihteeri Anne Ilkka

HENKILÖTIETOJEN KÄSITTELY OIKEUSHALLINNON TURVAPOSTIA KÄYTETTÄESSÄ

1 KANTELU

Pyysitte tutkimaan Rovaniemen hovioikeuden menettelyn lainmukaisuutta tietopyynnön tekijän tietojen tallentamisessa.

Olitte pyytänyt Rovaniemen hovioikeudesta julkisuuslain nojalla asiakirjan, joka oli toimitettu Teille suojatulla sähköpostilla. Sähköpostin avaaminen edellytti suostumuksen antamista tietojen tallentamiseen. Sähköpostin ilmoituksen mukaan tallennettava tieto voi käsittää puhelinnumerot, sähköpostiosoitteet ja IP-osoitteet. Ilmoitus ei sisältänyt tietoja siitä, mihin rekisteriin tiedot kerätään, mihin niitä käytetään ja kuinka kauan niitä säilytetään.

Lisäksi piditte tarpeettomana julkisen asiakirjan lähettämistä suojatulla sähköpostilla, joka edellyttää vastaanottajan tietojen tallentamista.

2 SELVITYS

Käytettävissäni ovat olleet seuraavat asiakirjat:
- Rovaniemen hovioikeuden selvitys ja lausunto 15.12.2020
- Tuomioistuinviraston selvitys 11.12.2020
- Oikeusministeriön selvitys 13.11.2020
- Valtorin kuvaus henkilötietojen käsittelystä Turvaviesti-palvelussa
- Ohje oikeusministeriön hallinnonalan virastoille suojatun ja matkapuhelinnumerolla varmistetun sähköpostiviestin lähettämiseksi 14.2.2020 VN/15039/2019

3 VASTAUS

Olen tutkinut asianne, mutta en ole havainnut siinä oikeusasiamiehen toimenpiteitä edellyttävää lainvastaista menettelyä tai velvollisuuden laiminlyöntiä.

Perustelen ratkaisuani seuraavasti.

3.1 Tuomioistuinviraston selvitys

Tuomioistuinvirasto on toimittanut selvityksensä liitteenä oikeusministeriön selvityksen, koska kantelussa tarkoitettu turvasähköpostiratkaisu on oikeusministeriön tilaama ja laajasti käytössä koko oikeushallinnon alalla. Tuomioistuinvirasto yhtyy oikeusministeriön näkemykseen ja täydentää sitä seuraavasti.

Asiakirjapyynnön esittäminen viranomaiselle ja tietopyynnön käsittely

Kun asiakirjapyyntö tulee viranomaiselle sähköpostitse, tulee kyseisestä viestistä viranomaisen asiakirja, jota koskevat tiedot on käsiteltävä ja kirjattava siten, kuin laki viranomaisen toiminnan julkisuudesta 621/1999, julkisuuslaki) sekä laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) edellyttävät. Viranomaiselle toimitettu asiakirja on julkisuuslain 5 §:n 2 momentissa tarkoitettu viranomaisen asiakirja. Tiedonhallintalain 25 §:n mukaan viranomaisen on rekisteröitävä viipymättä sille saapunut tai sen laatima asiakirja asiarekisteriin. Sen lisäksi, mitä 26 §:ssä säädetään, asiakirjan rekisteröinnistä on käytävä ilmi asiakirjan saapumisajankohta. Tiedonhallintalain 26 §:ssä määritellään asiarekisteriin rekisteröitävät tiedot. Viranomaiselle saapuneesta asiakirjasta rekisteröidään ainakin asiakirjan lähettäjä tai asiamies.

Kansalaisen harkinnassa on se, käyttääkö hän esimerkiksi yhteystietona sellaista sähköpostisosoitetta, josta hänet voidaan suoraan tunnistaa esimerkiksi etu- ja sukunimitiedon perusteella. Keskeistä on kuitenkin havaita se, että asiakirjapyynnön esittämiseen sähköpostitse sisältyy jo itsessään sellaisia elementtejä, jotka velvoittavat viranomaista keräämään ja tallettamaan pyyntöä koskevia tietoja. Se, voidaanko tietojen perusteella todella päätellä kansalaisen henkilöllisyys, on osin riippuvainen myös siitä, mitä tietoja hän itsestään pyynnön yhteydessä toimittaa. Viranomainen on velvoitettu kirjaamaan ne tiedot, joita kansalainen toimittaa. Tietopyyntöjen käsittelyyn liittävästä henkilötietojen käsittelystä informoidaan myös rekisteröityjä avoimesti tuomioistuinten tietosuojaselosteissa. Tätä taustaa vasten on todettava, ettei kantelun vireille saattajan tietopyyntö ole ollut ”anonyymi” sen jälkeen, kun hän on sähköpostitse toimittanut asiakirjapyynnön Rovaniemen hovioikeuden kirjaamoon.

Se, että kansalainen pyytää viranomaiselta tietoja käyttötarkoitukseen, joka on rajattu tietosuojasäännösten soveltamisalan ulkopuolelle (eli tässä tapauksessa yksinomaan henkilökohtaiseen ja kotitaloutta koskevaan käyttötarkoitukseen), ei luo viranomaiselle oikeutta poiketa oman käsittelynsä osalta sille laissa säädetyistä vaatimuksista, mukaan lukien tietosuojasäännösten asettamista vaatimuksista rekisterinpitäjälle. Kun viranomainen käsittelee henkilötietoja tai henkilötietoja sisältäviä asiakirjoja tietopyynnön toteuttamiseksi, ei käsittely vielä tässä vaiheessa ole tietosuojasäännösten soveltamisalan ulkopuolella.

Rikostuomioiden ja rikkomuksia koskevien henkilötietojen luonne

Tuomioistuinvirasto kiinnittää tässä yhteydessä huomiota siihen, että rikostuomioita ja rikkomuksia koskevat tiedot, joita myös tuomioista ilmenee, ovat niin sanotun korotetun suojausvaatimuksen piirissä tietosuojalain 7 §:n 2 momentin mukaisesti ja niiden käsittelyn osalta edellytetään asianmukaisia ja erityisiä suojatoimia, jotka on määritetty tietosuojalain 6 §:n 2 momentissa. Tämän ohella tuomioistuinten on tietosuoja-asetuksessa omaksutun riskiperusteisen lähestymistavan mukaisesti noudatettava asianmukaisia suojatoimia siten, kuin tietosuoja-asetuksen 24, 25 ja 32 artiklassa säädetään. Rekisterinpitäjän on ensivaiheessa arvioitava, millaiset suojatoimenpiteet ovat käsittelytoimiin

nähden asianmukaiset. Yleisen tietosuoja-asetuksen 5 artiklan 2 kohdan osoitusvelvollisuudesta seuraa, että rekisterinpitäjän ja henkilötietojen käsittelijän on kyettävä osoittamaan valittujen suojatoimien asianmukaisuus ja oikeasuhtaisuus. Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen laajamittaiseen käsittelyyn liittyvä korkea riski on tunnistettu myös tietosuoja-asetuksen 35 artiklassa, jonka mukaan rikostuomioihin ja rikkomusten laajamittainen käsittely edellyttää vaikutustenarviointia sekä 37 artiklassa, joka koskee tietosuojavastaavan nimittämistä.

Riskiperusteisen lähestymistavan keskiössä on riskinarviointi nimenomaan rekisteröidyn näkökulmasta, eli mitä haittaa rekisteröidylle voi aiheutua henkilötietojen asiattomasta käsittelystä. Tietosuojasäännöksillä pyritään turvaamaan sitä, ettei henkilötietojen käsittelystä aiheutuisi haittavaikutuksia rekisteröidylle. On myös tunnistettava, että moni kansalainen pelkää joutuvansa identiteettivarkauden uhriksi.

Tietojen toimittaminen suojatun sähköpostiyhteyden kautta

Suojatun sähköpostin avaamisen yhteydessä tallentuu IP-osoite. Niin staattista kuin dynaamista IP-osoitetta pidetään ”välillisesti” tunnistettavina henkilötietoina, koska ne ovat lisätietojen avulla johdettavissa takaisiin yksittäiseen henkilöön (kts. Unionin tuomioistuimen tuomio asiassa C-582/14, Breyer vs. Saksan liittotasavalta).

Vaikka IP-osoite on henkilötieto, tulisi julkisuuslain mukaisten velvoitteiden toteutumisen näkökulmasta arvioida myös sitä, oliko viranomaisella tosiasiasiallisesti tarkoituksena pyytää suojatun sähköpostin yhteydessä selvitystä tietoa pyytävän henkilöllisyydestä, vaikka turvallinen viestintä ja henkilötietojen asianmukainen suojaaminen tässä yhteydessä edellyttivätkin IP-osoitteen käsittelyä. Suojatun sähköpostin yhteydessä IP-osoitteen tallentumisella turvataan sitä, ettei viestiä saa auki muulla laitteella kuin sillä, jolla se on ensin avattu.

Tuomioistuinviraston näkemyksen mukaan suojatun sähköpostin käyttö on perusteltua henkilötietosuojaan suojaan liittyvistä syistä silloin, kun luovutuksen kohteena ovat korotetun suojavaatimuksen piirissä olevat rikostuomioita ja rikkomuksia koskevat tiedot (tietosuojalain 7 §). Henkilötietojen (IP-osoite) käsittely perustuu rekisterinpitäjän lakisääteiseen velvoitteeseen. Informointia suojatun sähköpostin yhteydessä tapahtuvasta henkilötietojen käsittelystä on selkeytetty Oikeusministeriön toimesta.

3.2 Oikeusministeriön selvitys

Oikeusministeriö on tilannut Turvaviesti-palvelun hallinnonalan viranomaisten käyttöön valtion tieto- ja viestintätekniikkakeskus Valtorilta. Tietopyynnön esittäjälle sähköpostin avaamisen yhteydessä näytetyn informointitekstin oli tuottanut palvelun toimittaja.

Oikeusministeriö toteaa, että sähköpostin avaamisen yhteydessä näytettävää viestiä on syytä täsmentää. Viestissä ei ole kyse hyväksynnän pyytämisestä, niin kuin tekstissä annetaan ymmärtää, vaan Turvaviesti-palvelusta viestin avaavan henkilön käyttämältä laitteelta

kerätään viranomaisen päätöksellä ne tiedot, jotka ovat tarpeen viestin tietoturvallisuuden varmistamiseksi.

Oikeusministeriö toteaa, että kantelija on oikeassa myös siinä, että nykyisistä teksteistä ei riittävällä tavalla käy ilmi EU:n yleisen tietosuoja-asetuksen 13 artiklassa edellytettyjä tietoja, kuten oikeusperustetta, jolla viranomainen tietoja kerää.

Oikeusministeriö on toimittanut Valtorille kuvaavamman tekstin ja tehnyt palvelupyynnön ilmoituksen muokkaamiseksi, jotta siinä jatkossa annetaan EU:n yleisen tietosuoja-asetuksen 13 artiklassa edellytetyt tiedot.

EU:n yleisen tietosuoja-asetuksen 32 artiklassa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 31 §:ssä säädetään rekisterinpitäjille velvollisuus käsitellä henkilötietoja tietoturvallisesti. Tämä tarkoittaa mm. tietojen suojaamista ulkopuolisten pääsyltä niihin. Sähköisen viestinnän palveluista annetun lain 138 §:ssä säädetään, että sähköisiä viestejä ja välitystietoja voi käsitellä siinä määrin kuin se on tarpeen viestinnän välittämiseksi ja sovitun palvelun toteuttamiseksi sekä 272 §:ssä säädetyllä tavalla tietoturvasta huolehtimiseksi.

Käytännössä kaikenlainen sähköisen viestin välittäminen edellyttää molempia osapuolia koskevien tietojen käsittelemistä. Turvaviesti-palvelussa tietoturvallisuudesta huolehtiminen on viety tavallista sähköpostia korkeammalle tasolle nimenomaan mm. sillä tavoin, että varmennetaan, että viestin voi avata vain yksi taho. Tämä edellyttää viestin avaajan laitetta ja selainta koskevien tietojen keräämistä. Kerättyjä tietoja käytetään ja säilytetään vain palvelun tietoturvallisen toteuttamisen tarkoituksiin sekä mahdollisten virhetilanteiden ja tietoturvapoikkeamien selvittämiseksi. Tähän liittyvä henkilötietojen käsittely on tarpeen rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseksi EU:n yleisen tietosuoja-asetuksen tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain mukaisesti, riippuen kumpaa säädöstä rekisterinpitäjän kyseisessä toiminnossa sovelletaan.

Viranomaisten toiminnan julkisuudesta annetun lain 13 §:ssä tietopyynnön tekijälle annettu lähtökohtainen oikeus olla selvittämättä henkilöllisyyttään ei ole ehdoton, vaan sitä sovellettaessa on otettava huomioon myös muita oikeuksia, kuten perustuslaissa säädetty oikeus henkilötietojen suojaan. Viranomaisella on velvollisuus suojata vastuulleen kuuluvat henkilötiedot asiattomalta pääsyltä. Tavallisessa suojaamattomassa sähköpostissa tiedot eivät ole sivullisilta suojattuja. Eduskunnan oikeusasiamies on ratkaisussaan EOAK/2455/2016 todennut, että on ”olemassa useita sinänsä julkisiksi katsottavia tietotyyppejä, jotka avoimessa tietoverkossa voivat altistaa henkilön erilaisille riskeille. Tällaisia tietoja voivat olla esimerkiksi henkilötunnus, osoite, puhelinnumero, sähköpostiosoite ja pankkitilin numero.”

Turvaviesti-palvelua käytettäessä noudatetaan viranomaisen lakisääteistä velvoitetta ja varmistetaan suoraan henkilötietojen suoja -perusoikeuden ydinalueen toteutumista. Turvaviesti-palvelua käytetään

salassa pidettävien tietojen lähettämisen ohella myös henkilötietojen lähettämiseen silloin, kun on syytä erityisesti varmentua, että tiedot eivät joudu ulkopuolisten saataville; esimerkiksi henkilötunnuksia lähetettäessä.

Turvaviesti-palvelua käyttävä viranomainen, Valtori tai sen alihankkija eivät pyri tunnistamaan viestin avannutta tahoa kerättyjen tietojen perusteella. Jos havaittaisiin tilanne, jossa olisi syytä epäillä välitetyn viestin tietoturvallisuuden vaarantuneen, mahdollisesti lainvastaisen menettelyn johdosta, Turvaviesti-palvelua käyttävä viranomainen tai Valtori pyytäisivät toimivaltaista viranomaista tutkimaan asiaa.

Oikeusministeriö on pyytänyt Valtoria muuttamaan rekisteröityjen informoinnin seuraavaksi:

”Henkilötietojen käsittely salattuna lähetetyn viestin lukemisen yhteydessä

Viestin lähettäneellä viranomaisella on velvollisuus suojata lähettämänsä tiedot asiattomalta pääsyltä. Viestin tietoturvallisuuden takaamiseksi viranomaisen on kerättävä muutamia tietoja, joista viestinnän osapuolet voivat olla tunnistettavissa. Näitä tietoja ovat lähettäjän ja vastaanottajan sähköpostiosoite, sen laitteen IP-osoite, jolta viesti on avattu, sekä käytetyn internet-selaimen asentaman evästeen tekniset tiedot. Jos viestin lähettämisessä on käytetty lisäksi puhelinnumerovarmennusta, vastaanottajan puhelinnumeroa säilytetään 30 päivän ajan viestin lähettämisestä.

Kerättyjä tietoja käytetään ja säilytetään vain palvelun tietoturvallisuuden toteuttamisen tarkoituksiin sekä mahdollisten virhetilanteiden ja tietoturvapoikkeamien selvittämiseksi. Henkilötietojen käsittely on tarpeen rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseksi (EU:n yleinen tietosuoja-asetus 32 artikla, laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 31 §).

Teknisenä palveluntarjoajina toimivat valtion tieto- ja viestintätekniikkakeskus Valtori sekä sen sopimuskumppani, Suomen valtion kokonaan omistama Erillisverkot Oy. Viestin lähettänyt viranomainen tai mainitut palveluntarjoajat eivät pyri tunnistamaan viestin avannutta tahoa kerättyjen tietojen perusteella. Jos havaittaisiin tilanne, jossa olisi syytä epäillä välitetyn viestin tietoturvallisuuden vaarantuneen, mahdollisesti lainvastaisen menettelyn johdosta, viestin lähettänyt viranomainen tai Valtori pyytäisivät toimivaltaista viranomaista tutkimaan asiaa.

Tarkempia tietoja Turvaviesti-palveluun liittyvästä henkilötietojen käsittelystä voi kysyä viestin lähettäneeltä viranomaiselta, joka toimii henkilötietojen käsittelystä vastaavana rekisterinpitäjänä. Viranomaisen yhteystiedot löytyvät sen internetsivuilta. Jokaisella on oikeus valittaa henkilötietojensa käsittelystä tietosuojavaltuutetulle, www.tietosuoja.fi.”

3.3 Rovaniemen hovioikeuden selvitys ja lausunto

Rovaniemen hovioikeus toteaa, että viranomaisella on velvollisuus suojata vastuulleen kuuluvat henkilötiedot asiattomalta pääsyltä. Tavallisessa suojaamattomassa sähköpostissa tiedot eivät ole sivullisilta suojattuja.

Oikeusministeriö on 14.2.2020 antamallaan päätöksellä ohjeistanut hallinnonalansa virastoja suojatun ja sähköpostilla varmistetun sähköpostiviestin lähettämisestä. Päätöksen mukaan .sec-suojatulla viestillä lähetetään viestit, jotka sisältävät henkilötietoja, arkaluonteisia tietoja, salassa pidettäviä tietoja sekä turvallisuusluokiteltuja tietoja. Tätä suojausta tulee käyttää lähettäessä sähköpostiviesti asiakkaille, ulkopuolisille toimijoille ja yhteistyökumppaneille. Suojausta ei tarvitse käyttää oikeusministeriön hallinnonalan sisällä eikä Valtorin yhteiseen verkkoon kuuluvien viranomaisten kesken.

Kantelija on 30.9.2020 lähettänyt hovioikeuteen sähköpostiviestin, jossa pyytänyt yksilöimäänsä kunnianloukkaustuomiota. Hän on allekirjoittanut viestin omalla nimellään ja lähettänyt viestin oman nimensä mukaisesta Gmail-sähköpostiosoitteesta.

Kantelijan pyytämä hovioikeuden tuomio ja siihen liittyvä käräjäoikeuden tuomio eivät sisällä salassa pidettäviä tai turvallisuusluokiteltuja tietoja. Tuomiot ovat julkisia, mutta ne kuitenkin sisältävät arkaluonteisia tietoja ja henkilötietoja, kuten esimerkiksi henkilötunnus.

Hovioikeus ei ole pyytänyt kantelijalta mitään lisäselvitystä esimerkiksi tietojen käyttötarkoituksesta. Tuomiot on lähetetty sähköpostitse ja sähköpostiviesti on suojattu oikeusministeriön ohjeistamalla tavalla käyttäen .sec-suojausta.

Hovioikeuden käytössä oleva turvaviesti-palvelu on oikeusministeriön Valtorilta tilaama palvelu. Kyseessä oleva viestin saajalle avautunut teksti on Valtorin tuottama. Oikeusministeriö on jo pyytänyt Valtoria muuttamaan tekstin aiempaa informatiivisemmaksi. Uusi teksti on jo palvelussa käytössä.

Palvelussa kerättyjä tietoja käytetään ja säilytetään vain palvelun tietoturvallisuuden varmistamiseksi sekä mahdollisten virhetilanteiden ja tietoturvapoikkeamien selvittämiseksi. Viestin avannutta tahoa ei pyritä tunnistamaan tietojen perusteella. Palveluun liittyvinä tietojenkäsittelijöinä toimivat Valtori ja Suomen Erillisverkot Oy. Tiedot eivät ole hovioikeuden hallussa.

3.4 Keskeiset oikeusohjeet

Perustuslain 10 §:n 1 momentissa turvataan yksityiselämän suoja. Henkilötietojen suojasta säädetään tarkemmin lailla.

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki) 5 §:n 2 momentissa on määritelty viranomaisen asiakirja. Viranomaisen asiakirjalla tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa. Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta, ja viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten.

Julkisuuslain 9 §:n 1 momentin mukaan jokaisella on oikeus saada tieto viranomaisen asiakirjasta, joka on julkinen.

Julkisuuslain 13 §:n 1 momentin mukaan pyyntö saada tieto viranomaisen asiakirjan sisällöstä on yksilöitävä riittävästi siten, että viranomainen voi selvittää, mitä asiakirjaa pyyntö koskee. Tiedon pyytäjää on diaarin ja muiden hakemistojen avulla avustettava yksilöimään asiakirja, josta hän haluaa tiedon. Tiedon pyytäjän ei tarvitse selvittää henkilöllisyyttään eikä perustella pyyntöään, ellei tämä ole tarpeen viranomaiselle säädetyn harkintavallan käyttämiseksi tai sen selvittämiseksi, onko pyytäjällä oikeus saada tieto asiakirjan sisällöstä.

Julkisuuslain 16 §:ssä säädetään asiakirjan antamistavoista. Sen 1 momentin mukaan viranomaisen asiakirjan sisällöstä annetaan tieto suullisesti taikka antamalla asiakirja viranomaisen luona nähtäväksi ja jäljennettäväksi tai kuunneltavaksi tai antamalla siitä kopio tai tuloste. Tieto asiakirjan julkisesta sisällöstä on annettava pyydetyllä tavalla, jollei pyynnön noudattaminen asiakirjojen suuren määrän tai asiakirjan kopioinnin vaikeuden tai muun niihin verrattavan syyn vuoksi aiheuta kohtuutonta haittaa virkatoiminnalle.

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) 25 §:n mukaan tiedonhallintayksikön on ylläpidettävä viranomaisen käsittelyssä olevista ja olleista asioista asiarekisteriä, johon rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Viranomaisen on rekisteröitävä viipymättä sille saapunut tai sen laatima asiakirja asiarekisteriin. Sen lisäksi, mitä 26 §:ssä säädetään, asiakirjan rekisteröinnistä on käytävä ilmi asiakirjan saapumisajankohta.

Tiedonhallintayksikön on huolehdittava siitä, että asiarekisterin tai sen osan julkisista merkinnöistä on mahdollista tuottaa tiedot tiedonsaantia koskevien pyyntöjen yksilöimiseksi.

Tiedonhallintalain 26 §:ssä säädetään asiarekisteriin rekisteröitävistä tiedoista. Tiedonhallintayksikön on muodostettava viranomaisen käsiteltäväksi otetun tai annetun asian yksilöivä asiatunnus, jonka avulla asiaan liittyvät tiedot yksilöidään.

Viranomaisen on rekisteröitävä asialle ainakin seuraavat yksilöintitiedot:
1) tiedonhallintayksikön yritys- ja yhteisötunnus;
2) viranomaisen yksilöivä tieto;

3) toimintaprosessin yksilöivä tieto;
4) asian vireilletuloajankohta.

Viranomaiselle saapuneesta asiakirjasta rekisteröidään ainakin:
1) asiakirjan yksilöivä tieto;
2) asiakirjan saapumistapa;
3) asiakirjan lähettäjä tai asiamies.

Viranomaisen laatimista asiakirjoista rekisteröidään ainakin:
1) asiakirjan yksilöivä tieto;
2) asiakirjan laatija;
3) laatimisajankohta.

Asiarekisteriin rekisteröidään lisäksi asiasta ainakin:
1) asian vireillepanija ja tarvittaessa muut asianosaiset;
2) asian käsittelyn tila;
3) viranomaisen toimenpiteet ja niissä käsitellyt asiakirjat käsittelyvaiheittain.

Sähköisen viestinnän palveluista annetun lain (917/2014) 138 §:ssä säädetään, että sähköisiä viestejä ja välitystietoja voi käsitellä siinä määrin kuin se on tarpeen viestinnän välittämiseksi ja sovitun palvelun toteuttamiseksi sekä 272 §:ssä säädetyllä tavalla tietoturvasta huolehtimiseksi.

Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) 13 artiklassa määritellään rekisteröidylle toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä. Kyseessä olevia tietoja ovat muun muassa tieto rekisterinpitäjästä, henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste ja henkilötietojen vastaanottajat tai vastaanottajaryhmät. Lisäksi tulee ilmoittaa muun muassa henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit, rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen sekä oikeus tehdä valitus valvontaviranomaiselle.

Tietosuoja-asetuksen 24 artiklan mukaan ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Kun se on oikeasuhteista käsittelytoimiin nähden, edellä tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.

Tietosuoja-asetuksen 25 artiklassa säädetään rekisterinpitäjän velvoitteesta toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet,

jotta käsittely vastaisi tämän asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin.

Tietosuoja-asetuksen 32 artiklan mukaan ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

Tietosuojalain (1050/2018) 7 §:n mukaan tietosuoja-asetuksen 10 artiklassa tarkoitettuihin rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja saa käsitellä, jos:
1) käsittely on tarpeen oikeusvaateen selvittämiseksi, laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi; tai
2) tietoja käsitellään 6 §:n 1 momentin 1, 2 tai 7 kohdassa säädetyssä tarkoituksessa.

Mitä 6 §:n 2 momentissa säädetään toimenpiteistä rekisteröidyn oikeuksien suojaamiseksi, sovelletaan myös käsiteltäessä tämän pykälän 1 momentissa tarkoitettuja henkilötietoja.

Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetulla lailla (1054/2018) on pantu täytäntöön luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 (rikosasioiden tietosuojadirektiivi).

Lain 1 §:n 1 momentin 3 kohdan mukaan lakia sovelletaan toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kyse on rikosasian käsittelemisestä tuomioistuimessa.

Lain 2 §:n mukaan, jos muussa laissa on tästä laista poikkeavia säännöksiä, niitä sovelletaan tämän lain asemesta. Oikeuteen saada tieto ja muuhun henkilötietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan, mitä viranomaisten toiminnan julkisuudesta säädetään.

Lain 31 §:n mukaan rekisterinpitäjän ja henkilötietojen käsittelijän tulee teknisin ja organisatorisin toimenpitein huolehtia henkilötietojen riittävästä suojaamisesta ottaen huomioon käsittelystä rekisteröidyn oikeuksille aiheutuva riski. Henkilötiedot on erityisesti suojattava oikeudettomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä,

tuhoutumiselta ja vahingoittumiselta. Toimenpiteitä suunniteltaessa ja toteutettaessa tulee ottaa huomioon:
1) uusin tekniikka;
2) toimenpiteiden toteuttamiskustannukset;
3) käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset;
4) luonnollisen henkilön oikeuksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain (370/2007) 22 §:n 1 momentin mukaan tuomioistuimen ratkaisu on julkinen, jollei tuomioistuin 24 §:n nojalla määrää sitä pidettäväksi salassa.

3.5 Asian arviointi

3.5.1 Tietopyynnön käsittely ja asiakirjan toimittaminen

Julkisuuslaissa ei säännellä eikä anneta tarkempia ohjeita tietopyynnön tekemisen muodosta. Laissa ei esimerkiksi edellytetä, että tietopyyntö tulisi tehdä kirjallisesti. Julkisuuslaissa tietopyynnön sisällön ainoa vaatimus on, että se tulee yksilöidä riittävästi, jotta viranomainen pystyy löytämään asiakirjan. Näin ollen asiakirjapyynnön voi tehdä vapaamuotoisesti kirjallisesti tai suullisesti.

Julkisuuslain mukaan julkisen tiedon pyytäjän ei tarvitse selvittää henkilöllisyyttään tai perustella pyyntöään, ellei tämä ole tarpeen viranomaiselle säädetyn harkintavallan käyttämiseksi tai sen selvittämiseksi, onko pyytäjällä oikeus saada tieto asiakirjan sisällöstä. Pääperiaate on siis se, että pyydettäessä tietoa julkisesta asiakirjasta, josta kenellä hyvänsä on oikeus saada tieto, tietopyynnön voi tehdä anonyymisti eikä tietopyynnön tekijällä ole velvollisuutta kertoa nimeään.

Viranomaisella on tiedonhallintalain mukaan velvollisuus merkitä saapunut tietopyyntö asiarekisteriinsä ja sitä käsitellään julkisuuslain 5 §:n 2 momentissa tarkoitettuna viranomaisen asiakirjana. Asiarekisteriin rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Asiarekisteriin kirjataan ainakin asiakirjan yksilöivä tieto, asiakirjan saapumistapa ja asiakirjan lähettäjä tai asiamies sekä asiakirjan saapumisajankohta. Kirjallisesti saapuneen tietopyynnön osalta viranomainen rekisteröi tietopyynnön esittäjän ilmoittamat tiedot.

Rikosasian käsittelemiseen tuomioistuimessa sovelletaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018), jolla on toimeenpantu rikosasioiden tietosuojadirektiivi. Kyseistä lakia sovelletaan toimivaltaisiin viranomaisiin, kuten esimerkiksi tuomioistuimiin, ainoastaan siltä osin, kuin ne suorittavat henkilötietojen käsittelyä lain soveltamisalaan kuuluvissa tehtävissä. Muita tarkoituksia varten suoritettavaan henkilötietojen käsittelyyn tuomioistuimessa sovelletaan yleistä tietosuoja-asetusta. Molemmat säännökset edellyttävät henkilötietoja käsittelevältä viranomaiselta henkilötietojen turvallista käsittelyä.

Tuomioistuinvirasto on selvityksessään kuvannut henkilötietojen käsittelyä tuomioistuimissa ja rikostuomioiden korotettua suojausvaatimusta koskevia säädöksiä seuraavasti.

Kun viranomainen käsittelee henkilötietoja tai henkilötietoja sisältäviä asiakirjoja tietopyynnön toteuttamiseksi, viranomaisella on velvollisuus noudattaa sille tietosuojalainsäädännössä säädettyjä vaatimuksia muun muassa tietojen tietosuoja-asetuksen 32 artiklassa edellytetystä turvallisesta käsittelystä. Se, että kansalainen pyytää viranomaiselta tietoja käyttötarkoitukseen, joka on rajattu tietosuojasäännösten soveltamisalan ulkopuolelle (yksinomaan henkilökohtaiseen ja kotitaloutta koskevaan käyttötarkoitukseen) ei luo viranomaiselle oikeutta poiketa oman käsittelynsä osalta sille laissa säädetyistä vaatimuksista, mukaan lukien tietosuojasäännösten asettamista vaatimuksista rekisterinpitäjälle.

Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 31 §:ssä edellytetään, että rekisterinpitäjän ja henkilötietojen käsittelijän tulee teknisin ja organisatorisin toimenpitein huolehtia henkilötietojen riittävästä suojaamisesta ottaen huomioon käsittelystä rekisteröidyn oikeuksille aiheutuva riski. Henkilötiedot on erityisesti suojattava oikeudettomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta.

Rikostuomioita ja rikkomuksia koskevat tiedot, joita myös tuomioista ilmenee, ovat niin sanotun korotetun suojausvaatimuksen piirissä tietosuojalain 7 §:n 2 momentin mukaisesti ja niiden käsittelyn osalta edellytetään asianmukaisia ja erityisiä suojatoimia, jotka on määritetty tietosuojalain 6 §:n 2 momentissa. Tämän ohella tuomioistuinten on tietosuoja-asetuksessa omaksutun riskiperusteisen lähestymistavan mukaisesti noudatettava asianmukaisia suojatoimia siten, kuin tietosuoja-asetuksen 24, 25 ja 32 artiklassa säädetään. Rekisterinpitäjän on ensivaiheessa arvioitava, millaiset suojatoimenpiteet ovat käsittelytoimiin nähden asianmukaiset ja kyettävä osoittamaan valittujen suojatoimien asianmukaisuus ja oikeasuhtaisuus. Käsittelyyn liittyvien riskien vuoksi on tärkeää huomata myös se, että rikostuomioiden ja rikkomusten osalta käsittelyperusteita on kavennettu tietosuojalain 7 §:n 1 momentin mukaisesti.

Yhdyn Tuomioistuinviraston näkemyksiin henkilötietojen turvallista käsittelyä edellyttävistä säädöksistä.

Yleisessä tuomioistuimessa annetut tuomioistuimen ratkaisut ovat julkisia, jollei tuomioistuin ole määrännyt ratkaisua pidettäväksi salassa. Julkiset asiakirjat saattavat sisältää henkilötietoja. Lähes kaikki rikosasioiden tuomiot sisältävät henkilötietoja ja esim. henkilötunnuksia. Apulaisoikeusasiamies on ratkaisussaan EOAK/2455/2016 todennut, että on ”olemassa useita sinänsä julkisiksi katsottavia tietotyyppejä, jotka avoimessa tietoverkossa voivat altistaa henkilön erilaisille riskeille. Tällaisia tietoja voivat olla esimerkiksi henkilötunnus, osoite, puhelinnumero, sähköpostiosoite ja pankkitilin numero.”

Riskiperusteisen lähestymistavan keskiössä on riskinarviointi nimenomaan rekisteröidyn näkökulmasta, eli mitä haittaa rekisteröidylle voi aiheutua henkilötietojen asiattomasta käsittelystä. Tietosuojasäännöksillä pyritään turvaamaan sitä, ettei henkilötietojen käsittelystä aiheutuisi haittavaikutuksia rekisteröidylle.

Oikeusministeriö on ohjeessaan edellyttänyt, että sen hallinnonalan virastot käyttävät suojattua sähköpostiyhteyttä lähettäessään henkilötietoja asiakkaille, ulkopuolisille toimijoille ja yhteistyökumppaneille. Ottaen huomioon rekisterinpitäjän velvollisuuden henkilötietojen turvalliseen käsittelyyn, pidän oikeusministeriön antamaa ohjeistusta henkilötietojen lähettämisestä suojatulla sähköpostiyhteydellä asianmukaisena.

Asiassa saadun selvityksen mukaan kantelija oli pyytänyt tiettyä rikostuomiota sähköpostitse, maininnut sähköpostissaan oman nimensä sekä käyttänyt sähköpostiosoitetta, josta käy ilmi hänen nimensä. Rovaniemen hovioikeus ei ole pyytänyt kantelijalta mitään lisäselvitystä tietopyyntöön vastatessaan. Hovioikeus vastasi asiakirjapyyntöön erittäin nopeasti, alle puolessa tunnissa.

Kantelija oli tietopyynnössään pyytänyt lähettämään asiakirjan sähköpostilla. Koska lähetetyt asiakirjat sisälsivät henkilötietoja, joiden oikeudettomasta käsittelystä saattaa aiheutua rekisteröidylle haittavaikutuksia, pidän Rovaniemen hovioikeuden menettelytapaa lähettää asiakirjat salatulla sähköpostilla asianmukaisena.

Oikeusasiamies useissa ratkaisuissaan ottanut kantaa julkisuuslain uudistamistarpeeseen, muun muassa oikeusasiamiehen vuosikertomuksessa vuodelta 2017. Oikeusasiamies on myös lausunnossaan oikeusministeriölle julkisuuslain toimivuudesta ja julkisuusperiaatteen toteutumisesta 10.5.2021 (EOAK/2808/2021) todennut, että julkisuuslain ja henkilötietojen suojaa koskevan lainsäädännön välinen tulkinnallisuus nousee kanteluasioissa usein esiin muun muassa niin, että lainsäädäntöjen suhdetta ei tunneta, mikä voi johtua myös tämän suhteen epäselvyydestä. Edellä mainittuihin oikeusasiamiehen kannanottoihin viitaten korostan myös omasta puolestani oikeusministeriön käynnistämän julkisuuslain ajantasaistamista koskevan hankkeen tarpeellisuutta.

3.5.2 Salatun sähköpostin vastaanottamisessa kerättävät tiedot

Saadun selvityksen mukaan kyseessä oleva Turvaviesti-palvelu on oikeusministeriön Valtorilta tilaama palvelu ja laajasti käytössä valtionhallinnossa. Palvelussa kerättyjä tietoja käytetään ja säilytetään vain palvelun tietoturvallisuuden varmistamiseksi sekä mahdollisten virhetilanteiden ja tietoturvapoikkeamien selvittämiseksi. Turvaviesti-palvelusta viestin avaavan henkilön käyttämältä laitteelta kerätään viranomaisen päätöksellä ne tiedot, jotka ovat tarpeen viestin tietoturvallisuuden varmistamiseksi. Käytännössä kaikenlainen sähköisen viestin välittäminen edellyttää molempia osapuolia koskevien tietojen käsittelemistä. Salatun sähköpostin toimittamisen yhteydessä IP-osoitteen tallentumisella turvataan sitä, ettei viestiä saa auki muulla laitteella kuin sillä, jolla se on ensin avattu. Puhelinnumero on tarpeen tallentaa, jos

viestin lähettämisessä on käytetty lisäksi puhelinnumerovarmennusta.

Niin staattista kuin dynaamista IP-osoitetta pidetään ”välillisesti” tunnistettavina henkilötietoina, koska ne ovat lisätietojen avulla johdettavissa takaisiin yksittäiseen henkilöön (kts. Unionin tuomioistuimen tuomio asiassa C-582/14, Breyer vs. Saksan liittotasavalta).

Viestin välittämiseen liittyvä henkilötietojen käsittely on tarpeen rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseksi EU:n yleisen tietosuoja-asetuksen tai henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain mukaisesti. EU:n yleisen tietosuoja-asetuksen 32 artiklassa sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 31 §:ssä säädetään rekisterinpitäjille velvollisuus käsitellä henkilötietoja tietoturvallisesti. Tämä tarkoittaa mm. tietojen suojaamista ulkopuolisten pääsyltä niihin.

Sähköisen viestinnän palveluista annetun lain (917/2014) 138 §:ssä säädetään, että sähköisiä viestejä ja välitystietoja voi käsitellä siinä määrin kuin se on tarpeen viestinnän välittämiseksi ja sovitun palvelun toteuttamiseksi sekä 272 §:ssä säädetyllä tavalla tietoturvasta huolehtimiseksi.

Asiassa saadun selvityksen mukaan kerättyjä tietoja käytetään ja säilytetään vain palvelun tietoturvallisen toteuttamisen tarkoituksiin sekä mahdollisten virhetilanteiden ja tietoturvapoikkeamien selvittämiseksi. Viestin avannutta tahoa ei pyritä tunnistamaan tietojen perusteella. Palveluun liittyvinä tietojenkäsittelijöinä toimivat Valtori ja Suomen Erillisverkot Oy. Tiedot eivät ole salatun sähköpostiviestin lähettäneen organisaation hallussa.

Asiassa saadun selvityksen perusteella olen voinut todeta, että salatun sähköpostiviestin avaamisen yhteydessä tallentuvia tietoja käytetään vain siinä määrin kuin on tarpeen viestinnän välittämiseksi, sovitun palvelun toteuttamiseksi ja tietoturvasta huolehtimiseksi. Turvaviestin avaamisen yhteydessä tallennettavien tietojen käyttötarkoitus ei ole tietopyynnön tekijän tunnistaminen. Näin ollen menettelyä ei ole pidettävä lainvastaisena.

Yleisen tietosuoja-asetuksen 13 artiklassa säädetään rekisteröidylle toimitettavista tiedoista silloin kun henkilötietoja kerätään rekisteröidyltä. Näitä tietoja ovat muun muassa rekisterinpitäjän yhteystiedot, henkilötietojen käsittelyn tarkoitukset ja oikeusperuste ja henkilötietojen vastaanottajat.

Yhdyn oikeusministeriön näkemykseen siitä, että turvaviestin avaajalle näkyvä teksti on ollut epäselvä. Totean, että tekstistä ei ole käynyt ilmi tietosuoja-asetuksen 13 artiklassa tarkoitetut tiedot. Oikeusministeriö on toimittanut Turvaposti-palvelun tuottavalle Valtorille korjatun muotoilun viestistä, joka näkyy vastaanottajalla salattua sähköpostia avattaessa. Uusi teksti on käytössä Turvaposti-palvelussa. Tämän johdosta katson, että asia ei anna aihetta enempiin laillisuusvalvonnan toimiin.

Lähetän tämän ratkaisun tiedoksi Rovaniemen hovioikeudelle, Tuomioistuinvirastolle ja oikeusministeriölle.