18.12.2023

Dnro 2106/03.04.04.04.01/2022

Asia Tietosuoja-asiaa koskeva valitus

Valittaja Ulkoministeriö

Päätös, josta valitetaan

Apulaistietosuojavaltuutettu 23.3.2022 dnro 2437/161/22

Apulaistietosuojavaltuutettu on valituksenalaisella päätöksellä antanut ulkoministeriölle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaisen huomautuksen, koska ulkoministeriö ei ole rekisterinpitäjänä noudattanut toiminnassaan yleisen tietosuoja-asetuksen 33 ja 34 artiklojen mukaisia määräaikoja henkilötietojen tietoturvaloukkauksen ilmoittamisessa.

Apulaistietosuojavaltuutettu on esittänyt päätöksessään ja sen perusteluissa muun ohella seuraavaa:

Tietosuojavaltuutetun toimisto on vastaanottanut 24.1.2022 ulkoministeriön ilmoituksen henkilötietoihin kohdistuneesta tietoturvaloukkauksesta, joka on ulkoministeriön ilmoituksen mukaan johtunut NSO Groupin Pegasus -vakoiluhaittaohjelmasta. Ilmoituksen mukaan ulkoministeriö on selvittänyt tietoturvaloukkausta ja sen syitä eri viranomaisten ja sidosryhmien kanssa syksyn ja talven 2021–2022 aikana. Tietoturvaloukkaus on kohdistunut Suomen ulkomailla työskentelevään lähetettyyn henkilökuntaan. Ulkoministeriö on ilmoittanut tietoturvaloukkauksesta sen kohteena olleille rekisteröidyille.

Ulkoministeriö on 16.3.2022 antanut tietosuojavaltuutetun toimistolle tarkemman selvityksen yleisen tietosuoja-asetuksen 33 ja 34 artiklojen mukaisten ilmoitusten ajankohdista. Selvityksen mukaan ilmoituksen myöhästymisen pääasialliset syyt ovat liittyneet tietoturvaloukkauksen selvittämiseen ja siihen liittyviin kansallisen turvallisuuden näkökohtiin. Osittain myöhästymisen syyt ovat liittyneet myös tietoturvaloukkaukseen liittyvien tiedotusvastuiden jakaantumiseen viranomaisten kesken ja rekisterinpitäjän toiminnan luonteeseen.

Saadun selvityksen perusteella ulkoministeriö on saanut kohtuullisen varmuuden tietoturvaloukkauksen tapahtumisesta huomattavasti ennen ilmoituksen tekemistä valvontaviranomaiselle. Ulkoministeriö ei ole noudattanut yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan mukaista velvollisuutta ilmoittaa valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta eikä ole esittänyt yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa tarkoitettua perusteltua selitystä henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle tehtävän ilmoituksen myöhästymisestä.

Vaikka yleisessä tietosuoja-asetuksessa jossakin määrin sallitaan ilmoittamisen viivästyminen, tätä ei tulisi pitää säännöllisenä käytäntönä. Selityksen antamista tietoturvaloukkauksen myöhästymisestä ei voida pitää vaihtoehtona tietoturvaloukkauksen ilmoittamiselle 72 tunnin aikarajassa, vaan sen on katsottava olevan rekisterinpitäjään kohdistuva velvoite, joka otetaan huomioon harkittaessa yleisen tietosuoja-asetuksen mukaisten toimivaltuuksien käyttöä. Jos rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta, mutta ei kykene toimittamaan kaikkia tietoturvaloukkausta koskevia tietoja 72 tunnin mukaisessa aikarajassa, sen on mahdollista toimittaa tiedot valvovalle viranomaiselle vaiheittain yleisen tietosuoja-asetuksen 33 artiklan 4 kohdan mukaisesti. Ulkoministeriö ei ole esittänyt sellaista selitystä, jonka perusteella vaiheittainen ilmoittaminen ei olisi ollut mahdollista. Ulkoministeriön esittämät selitykset tietoturvaloukkausta koskevan ilmoituksen myöhästymiselle eivät ole osoittaneet, ettei rekisterinpitäjällä olisi ollut mahdollisuutta noudattaa ilmoituksen tekemisessä yleisen tietosuoja-asetuksen mukaista 72 tunnin aikarajaa.

Ulkoministeriö ei ole noudattanut yleisen tietosuoja-asetuksen 34 artiklan 1 kohtaa, jonka mukaan rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä. Asiassa saadun selvityksen perusteella rekisterinpitäjä on ilmoittanut tietosuoja-asetuksen 34 artiklan mukaiset tiedot tietoturvaloukkauksen kohteena olleille rekisteröidyille. Ilmoitusta ei kuitenkaan ole tehty yleisen tietosuoja-asetuksen mukaisesti ilman aiheetonta viivästystä pääosin kansalliseen turvallisuuteen liittyvien seikkojen vuoksi.

Yleisen tietosuoja-asetuksen 23 artiklan mukaan tiettyjä rekisteröidyn oikeuksia voidaan rajoittaa jäsenvaltion lainsäädännössä artiklassa säädettyjen edellytysten täyttyessä silloin, kun rajoituksella pyritään takaamaan kansallinen turvallisuus. Rekisterinpitäjän esittämän kansallisen turvallisuuden perusteen voitaisiin siis katsoa olevan relevantti peruste rekisteröidylle tehtävän ilmoituksen lykkäämiselle, edellyttäen että rekisterinpitäjää koskevassa henkilötietojen käsittelyä koskevassa lainsäädännössä on asiasta säädetty. Yleistä tietosuoja-asetusta täydentävässä tietosuojalaissa (1050/2018) ei ole säädetty poikkeusta yleisen tietosuoja-asetuksen 34 artiklan mukaiseen velvollisuuteen ilmoittaa rekisteröidylle tietoturvaloukkauksesta kansallisen turvallisuuden takaamiseksi. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietinnön mukaan tällaisen rajoituksen säätäminen yleislailla ei ole mahdollista, vaan rajoituksista on säädettävä erityislailla. Henkilötietojen tietoturvaloukkauksesta ilmoittamiseen

rekisteröidylle ei ole säädetty rajoituksia kansallisen turvallisuuden takaamiseksi rekisterinpitäjää koskevassa erityislainsäädännössä. Rekisterinpitäjän olisi siis tullut tehdä rekisteröidylle ilmoitus henkilötietojen tietoturvaloukkauksesta yleisen tietosuoja-asetuksen 34 artiklan mukaisen pääsäännön mukaisesti ilman aiheetonta viivästystä.

Ulkoministeriölle on perusteltua antaa yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukainen huomautus, kun otetaan huomioon rikotut artiklat, tietoturvaloukkauksen syyt, rekisterinpitäjän mahdollisuudet ilmoittaa tietoturvaloukkauksesta ajoissa, tietoturvaloukkauksen merkitys rekisteröidyille ja ilmoituksen myöhästymisen vaikutukset rekisteröityjen mahdollisuuteen minimoida tietoturvaloukkauksesta aiheutuvia riskejä.

Valituksessa esitetyt vaatimukset

Apulaistietosuojavaltuutetun päätös on kumottava kokonaisuudessaan. Toissijaisesti päätös on kumottava ainakin väitettyä 34 artiklan vastaista menettelyä koskevin osin.

Ulkoministeriö sai eräiden lähteiden avulla vahvan indikaation siitä, että eräisiin sen työntekijöiden mobiililaitteisiin olisi asennettu NSO Groupin Pegasus -vakoiluhaittaohjelma. Ulkoministeriö ilmoitti lähes heti asianosaisille henkilöille tästä alustavien tietojensa perusteella (käytännössä seuraavan päivän aikana). Tämän jälkeen ulkoministeriö kävi kyseisten henkilöiden kanssa vielä henkilökohtaisesti tarkempia keskusteluja tapahtuneesta ja asiaan liittyvistä riskeistä. Nämä keskustelut käytiin noin kaksi viikkoa ensimmäisten asianomaisille työntekijöille tehtyjen ilmoitusten jälkeen. Tapahtuman kohteena ovat olleet eräät ulkoministeriössä työskentelevät henkilöt. Koska hyökkäys kohdistui heidän mobiililaitteisiinsa, on myös mahdollista, että vakoiluohjelma on käsitellyt laitteen tietosisällössä mainittujen muiden henkilöiden tietoja (esim. kontaktilistassa olleet nimet tai vaikkapa valokuvan taustalla olleiden henkilöiden kuvia). Tällaisille henkilöille ei ole ilmoitettu tapahtuneesta. Kansalliseen turvallisuuteen liittyvistä syistä ulkoministeriö ei voi valituksessaan kuvata tapahtumainkulkua tarkemmin.

Kyseessä on kuitenkin lähtökohtaisesti ollut sellainen tilanne, josta olisi voinut aiheutua yleisen tietosuoja-asetuksen 33 artiklan tarkoittama luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski ja/tai 34 artiklan tarkoittama korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille, joihin lähtökohtaisesti liittyy ilmoitusvelvollisuus tietosuojavaltuutetun toimistolle (33 artikla) ja rekisteröidyille itselleen (34 artikla). Käsillä olevassa asiassa tällaisia ilmoitusvelvollisuuksia ei kuitenkaan ole ollut, koska kyse on ollut kansallisen turvallisuuden ja/tai ulko- ja turvallisuuspolitiikan ylläpitämiseen liittyvästä toiminnasta.

Kysymys siitä, kuinka laajasti yleisen tietosuoja-asetuksen mukaisia ilmoitusvelvollisuuksia sovelletaan henkilötietoihin kohdistuviin ulko- ja turvallisuuspoliittisesti arkaluonteisiin kyberhyökkäyksiin, on periaatteellisesti hyvin merkittävä sekä Suomen että EU:n tasolla. Tällaisten hyökkäysten takana ovat usein vieraat valtiot tai niihin läheisesti kytkeytyvät toimijat. Tilanteet ovat siten usein hyvin arkaluontoisia. Suomen valtiolla voi

esimerkiksi olla intressi varmistaa, ettei hyökkäyksen tehnyt taho heti saa tietoa siitä, että hyökkäys on paljastunut tai että sen torjumiseen on ryhdytty. Valtioiden väliset diplomaattiset suhteet edellyttävät usein myös merkittävää hienovaraisuutta siinäkin tilanteessa, että yksi valtio (tai siihen kytkeytyvä toimija) on toiminut toisen valtion etujen vastaisella tavalla. Suomen viranomaisilla on siten usein merkittävä intressi varmistaa, ettei tieto kansallisen turvallisuuden tai ulko- ja turvallisuuspolitiikan kannalta arkaluonteisesta tapahtumasta heti lähde leviämään hallitsemattomasti.

Jos rekisteröidyille ilmoitettaisiin heti estetystä hyökkäyksestä, sen salassapito voisi osoittautua mahdottomaksi erityisesti silloin, jos rekisteröidyn käsitettä tulkitaan niin laajasti, että myös kaikille hyökkäyksen kohteena olleen henkilön puhelinkontakteissa olleille henkilöille tulisi ilmoittaa hyökkäyksestä. Koska tällaiset intressit ovat pakottavia, voisi liian laaja ilmoitusvelvollisuus myös helposti johtaa siihen, ettei esimerkiksi kyberhyökkäyksestä tiedon saanut viranomainen välttämättä ollenkaan ilmoittaisi asiasta eteenpäin. Yleisen tietosuoja-asetuksen tarkoituksena ei ole ohjata jäsenvaltioiden ulko- ja turvallisuuspoliittista toimintaa tai saattaa valtioiden välistä diplomatiaa tietosuojaviranomaisten toimi- ja määräysvaltaan.

Yleistä tietosuoja-asetusta ei sen 2 artiklan 2 kohdan a alakohdan mukaisesti sovelleta sellaiseen toimintaan, joka ei kuulu unionin lainsäädännön soveltamisalaan. Lisäksi asetuksen 2 artiklan 2 kohdan b alakohdan mukaan asetusta ei sovelleta jäsenvaltioiden toteuttaessa SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa eli EU:n yhteistä ulko- ja turvallisuuspolitiikkaa. Yleisen tietosuoja-asetuksen johdanto-osan 16 perustelukappaleessa tarkennetaan näiden poikkeusten tarkoittavan, ettei asetusta sovelleta kansallisen turvallisuuden ylläpitämiseen tai ulko- ja turvallisuuspolitiikkaan. Yleisen tietosuoja-asetuksen 2 artiklan 2 kohta ilmentää siten selvää yleistä periaatetta siitä, ettei asetusta sovelleta kansalliseen turvallisuuteen tai ulko- ja turvallisuuspolitiikkaan liittyvään toimintaan sekä sitä, ettei EU-lainsäätäjä ole asetuksella halunnut vaikuttaa jäsenvaltioiden toimintaan niiden turvatessa tällaisia etujaan.

Myös EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä (TATTI-työryhmä) on katsonut, ettei yleinen tietosuoja-asetus sovellu kansalliseen turvallisuuteen liittyvään henkilötietojen käsittelyyn ja unionin oikeuskäytännön osoittavan, että asialla tulee olla riittävä yhteys unionin lainsäädäntöön, jotta unionin lainsäädäntö soveltuisi. Mikäli riittävää yhteyttä ei voida osoittaa, jää kansalliseen turvallisuuteen liittyvä henkilötietojen käsittely yleisen tietosuoja-asetuksen soveltuvuuden ulkopuolelle. Kyseisessä tapauksessa tietosuojavaltuutetun toimisto ei ole kyennyt osoittamaan tällaista riittävää yhteyttä.

Ruotsissa yleistä tietosuoja-asetusta kansallisesti täydentävä laki sisältää nimenomaisen säännöksen siitä, ettei asetuksen 33 ja 34 artiklan mukaisia ilmoitusvelvollisuuksia sovelleta eräissä ulko- ja turvallisuuspoliittisesti arkaluonteisissa tilanteissa. Suomen kansallisessa tietosuojalaissa ei ole vastaavaa poikkeussääntöä. Ruotsissa on tietosuojalain 2 §:llä laajennettu yleisen tietosuoja-asetuksen soveltamisala koskemaan myös kansallista turvallisuutta sekä ulko- ja turvallisuuspolitiikkaa. Koska Ruotsi on

kansallisesti tehnyt tällaisen laajennuksen, Ruotsin on myös ollut tarpeellista säätää laajennukseen liittyvä poikkeus ilmoitusvelvollisuuksiin. Koska Suomessa ei ole mitään vastaavaa asetuksen soveltamisalan kansallista laajennusta, Suomessa ei myöskään ole tarvetta vastaavalle ilmoitusvelvollisuuksia koskevalle poikkeukselle. Suomessa asia ratkeaa suoraan asetuksen 2 artiklan 2 kohdan nojalla.

Tietosuojavaltuutetun toimiston viittaus TATTI-työryhmän kannanottoon, jonka mukaan ilmoitusvelvollisuuteen tehtävien poikkeusten tulisi olla yleisen tietosuoja-asetuksen 23 artiklan edellyttämällä tavalla tarkkarajaisia, perustuu edellä sanotun valossa väärinkäsitykseen. Vaikka sinänsä on totta, että 23 artiklan nojalla säädettävän poikkeuksen esimerkiksi ilmoitusvelvollisuuteen on noudatettava 23 artiklan vaatimuksia, tätä ei sovelleta silloin, kun yleistä tietosuoja-asetusta ei sovelleta ollenkaan. Arvioidessaan vain 23 artiklan valossa mahdollisuutta poiketa ilmoitusvelvollisuudesta kansalliseen turvallisuuteen tai ulko- ja turvallisuuspolitiikkaan liittyvistä syistä tietosuojavaltuutetun toimisto ja TATTI-työryhmä ovat siis jättäneet huomioimatta 2 artiklan 2 kohdan merkityksen kokonaisuudessa. Yleisen tietosuoja-asetuksen 23 artikla ei siten laajenna asetuksen soveltamisalaa yli sen, mitä seuraa asetuksen 2 artiklan 2 kohdasta. Asetuksen 23 artikla ei vastaavasti myöskään muodosta estettä sille, että ilmoitusvelvollisuutta ei tarvitse soveltaa silloin, kun on kyse kansallisen turvallisuuden tai ulko- ja turvallisuuspolitiikan soveltamisesta.

Ainakaan rekisteröidylle tehtävää ilmoitusta ei edellytetä joka tilanteessa, vaikka se tulisikin asetuksen 34 artiklan soveltamisalan piiriin. Yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan c alakohdassa on suoraan säädetty, ettei ilmoitusta rekisteröidyille edellytetä, jos se vaatisi kohtuutonta vaivaa. Kyseisen artiklan mukainen ilmoitusvelvollisuus ei siten ole ehdoton. Päinvastoin ilmoittamisen tarvetta on punnittava myös suhteessa ilmoittamisen haittoihin ja tällaiseksi ”kohtuuttomaksi vaivaksi” on katsottava myös Suomen kansallisen turvallisuuden tai Suomen ulko- ja turvallisuuspoliittisten intressien vaarantuminen. Suomen kansallista turvallisuutta on esimerkiksi pidettävä merkittävästi painavampana etuna kuin yksittäisen rekisterinpitäjän teknisiä haasteita tiedottamisessa. Vastaavasti näihin etuihin kohdistuvaa haittaa on pidettävä merkittävästi suurempana kuin tällaisia haasteita.

Lisäksi on huomioitava Ruotsin yllä selostetun sääntelyratkaisun edustavan pohjoismaisessa yhteiskunnassa yleisesti hyväksyttyjä arvopunnintoja eli joissain tilanteissa on hyväksyttävä se, että yhteiskunnan turvallisuus edellyttää, ettei yksittäisille rekisteröidyille ilmoiteta henkilötietoihin kohdistuvasta kyberhyökkäyksestä. Ei ole mitään syytä sille, että suomalaisen haittapunninnan tulisi lähtökohtaisesti merkittävästi poiketa Ruotsin tietosuojalain taustalla vaikuttavista punninnoista. Myös se, että EU-lainsäätäjä on sulkenut pois yleisen tietosuoja-asetuksen soveltamisen kansallisen turvallisuuden ja ulko- ja turvallisuuspolitiikan osalta, ilmentää arvovalintaa siitä, että jäsenvaltioille on haluttu turvata suuri harkintamarginaali ja liikkumavara tällä alueella. Tätä taustaa vasten myös yleisen tietosuoja-asetuksen 34 artiklan soveltamisalan piirissä voi olla tilanteita, joissa ilmoitusta ei edellytetä kansalliseen turvallisuuteen liittyvistä tai ulko- ja turvallisuuspoliittisista syistä. Sellaisesta tilanteesta on nyt kyse.

Kokonaisuuden arvioinnissa on lisäksi huomioitava myös tiedottamiseen liittyvä muu viranomaisohjeistus. Euroopan tietosuojaneuvoston edeltämä EU:n tietosuojatyöryhmä on ohjeistuksessaan todennut, ettei rekisteröityjä tarvitse informoida henkilötietojen käsittelystä, jos informointi todennäköisesti estäisi rekisterinpitäjän käsittelyn tarkoitusten saavuttamisen. Näin ollen informointiin liittyvät velvollisuudet eivät ole absoluuttisia, mikäli tiedottamatta jättämiselle on perustellut syyt. Ulkoministeriö on mahdollisuuksien mukaan tiedottanut tapahtuneesta julkisesti ja yleisellä tasolla. Ulkoministeriö on esimerkiksi julkaissut tiedotteen asiasta ja asiasta on myös uutisoitu mediassa, joten tietoturvaloukkauksen on katsottava tulleen myös rekisteröityjen tietoon tätä kautta. Ulkoministeriö on siten tiedottanut asiasta yleisen tietosuoja-asetuksen 34 artiklassa tarkoitetulla julkisella tiedonannolla tai vastaavalla toimenpiteellä.

Valituksenalaisessa päätöksessä on katsottu, ettei ulkoministeriö olisi ilmoittanut tapahtuneesta rekisteröidyille yleisen tietosuoja-asetuksen mukaisesti ilman aiheetonta viivästystä. Ulkoministeriö ilmoitti välittömästi tapahtumasta työntekijöilleen, joiden laitteisiin kyberhyökkäys kohdistui. Asian arkaluonteisuuden vuoksi tapahtumasta ilmoitettiin työntekijöille myös henkilökohtaisesti. Ulkoministeriöllä ei ole ollut velvollisuutta ilmoittaa ulkopuolisille rekisteröidyille, joiden henkilötietoja on saattanut olla kyseessä olevien edustajien laitteilla, sillä ilmoittaminen vaatisi yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan c alakohdan mukaista kohtuutonta vaivaa. Ulkoministeriö on asian luonteen salliessa tiedottanut julkisesti tapahtuneesta ja täten tuonut tapahtuneen myös ulkopuolisten rekisteröityjen tietoisuuteen.

Kyberhyökkäykset ovat nykyään osa valtioiden ulko- ja turvallisuuspoliittista keinovalikoimaa. Yleisen tietosuoja-asetuksen tarkoituksena ei ole ohjata jäsenvaltioiden ulko- ja turvallisuuspoliittista toimintaa tai saattaa valtioiden välistä diplomatiaa tietosuojaviranomaisten toimi- ja määräysvaltaan. Jos yleisen tietosuoja-asetuksen 34 artiklan soveltamisalaa tulkitaan liian laajasti, tarkoittaisi se samalla myös suomalaisen yhteiskunnan kyberresilienssin heikkenemistä.

Asian käsittely ja selvittäminen

Apulaistietosuojavaltuutettu on antanut lausunnon. Lausunnossa on esitetty muun ohella seuraavaa:

Toisin kuin ulkoministeriö on esittänyt valituksessaan, yleinen tietosuoja-asetus tulee sovellettavaksi myös yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a ja b alakohdissa tarkoitettuun käsittelyyn kansallisen tietosuojalain (1050/2018) 2 §:n 1 momentin nojalla.

Rekisteröidylle tehdyn ilmoituksen viivästymistä ei ulkoministeriön valituksessa ilmoitettujen seikkojen perusteella ole syytä arvioida toisin kuin päätöksessä on tehty. Rekisterinpitäjä on ollut tietoinen tietoturvaloukkauksesta ennen ilmoituksen tekemistä rekisteröidylle. Ulkoministeriöllä ei ole ollut asetukseen tai lakiin perustuvaa oikeutta viivyttää ilmoituksen tekemistä.

Ulkoministeriö esittää valituksessaan, että tietosuojavaltuutetun toimiston päätös on virheellinen niiltä osin kuin se koskee yleisen tietosuoja-asetuksen 34 artiklan mukaisen ilmoituksen tekemisen viivästymistä. Ulkoministeriön mukaan se on ilmoittanut rekisteröidylle ilman aiheetonta viivytystä. Ministeriö ei kuitenkaan ole esittänyt valituksensa yhteydessä tietoturvaloukkaukseen liittyviä ajankohtia tai tarkempaa perustetta sille, milloin se katsoo tietoturvaloukkauksen tulleen rekisterinpitäjän tietoon yleisen tietosuoja-asetuksen 34 artiklan mukaisesti.

Tietosuojavaltuutetun toimiston ulkoministeriöltä saaman suullisen selvityksen ja tietoturvaloukkausta koskevan ilmoituksen sekä ulkoministeriön kotisivuilla olevan tiedotteen mukaan loukkaus on tapahtunut jo vuoden 2021 aikana. Ilmoitus tietosuojavaltuutetulle on tehty 24.1.2022.

Tietosuojavaltuutetun toimiston päätös perustuu siihen, mitä ulkoministeriö on tietoturvaloukkausta koskevassa ilmoituksessaan ja 9.3.2022 suullisesti esittänyt.

Tietoturvaloukkauksesta tiedon saamisen ja rekisteröidylle tehtävän ilmoituksen välissä on ollut aika, jota voidaan pitää erityisesti tietoturvaloukkauksen syynä olevan haittaohjelman luonteen ja rekisteröityjen aseman ulkoministeriön ulkomailla työskentelevinä virkamiehinä huomioon ottaen liian pitkänä.

Käytetty haittaohjelma on NSO Groupin Pegasus -vakoiluhaittaohjelma, joka käyttää laitteiden nollapäivähaavoittuvuuksia hyväkseen päästäkseen käsiksi kaikkeen laitteella olevaan tietoon seuratakseen esimerkiksi laitteen kaikkea viestintää, lukeakseen tiedostoja ja seuratakseen sijaintia.

Julkisesti saatavilla olevan tiedon mukaan rekisteröityjen mahdollisuudet suojautua itse kyseiseltä haittaohjelmalta ovat hyvin rajalliset, sillä ohjelmisto ei viimeisen tiedon mukaan ole tarvinnut asentuakseen käyttäjän aktiivista toimintaa eikä se ole antanut laitteiden käyttäjille merkkejä olemassaolostaan. Käytännössä rekisteröidyn mahdollisuus minimoida haittaohjelmasta aiheutuvia seurauksia perustuu rekisterinpitäjän viivytyksettömään ilmoitukseen tietoturvaloukkauksen kohteeksi joutumisesta.

Tietosuojavaltuutetun toimisto on saanut rekisterinpitäjältä selvityksen siitä, että se on tunnistanut tietoturvaloukkauksen kohteena olevat rekisteröidyt ja ilmoittanut näille tietoturvaloukkauksesta. Valituksenalaisessa päätöksessä ei ole kyse siitä, onko rekisterinpitäjä tehnyt ilmoituksen rekisteröidylle, vaan siitä, onko kyseinen ilmoitus tehty yleisen tietosuoja-asetuksen 34 artiklan mukaisessa ajassa.

Ulkoministeriö on antanut vastaselityksen. Asiassa on järjestettävä suullinen käsittely, koska kansalliseen turvallisuuteen sekä ulko- ja turvallisuuspolitiikkaan liittyvät seikat estävät tapahtumainkulun tarkemman läpikäynnin kirjallisesti. Todistajina on kuultava ulkoministeriön tietoturvapäällikköä ja tietosuojavastaavaa tietoturvaloukkauksen ilmitulon ajankohdasta, asiassa tehdyistä selvityksistä, rekisteröidyille tehtyjen ilmoitusten ajankohdista sekä näihin liittyvästä tapahtumankulusta.

Nyt kyseessä olevassa tapauksessa yleisen tietosuoja-asetuksen soveltaminen perustuu siihen, että asetuksen soveltamisalaa on kansallisesti laajennettu. Kansallisella lainsäätäjällä on siten perusoikeussääntelyn puitteissa vapaa toimivalta itse päättää, missä laajuudessa asetusta sovelletaan tai ei sovelleta. Siksi kyseessä olevien ilmoitusvelvollisuuksien laajuutta on tulkittava kansallisten tulkintaperiaatteiden mukaisesti kansallisen lainsäätäjän tarkoituksen mukaisesti.

Lainsäätäjän tarkoituksena ei ole voinut olla edellyttää sellaista ilmoitusvelvollisuutta, joka käytännössä tarkoittaisi merkittäviä riskejä Suomen kansallisen turvallisuuden ja ulko- ja turvallisuuspolitiikan kannalta. Lainsäätäjän tarkoitusta ilmentää tietosuojalain 2 §:n 3 momentti, jonka mukaan lakia ei sovelleta sellaiseen henkilötietojen käsittelyyn, josta säädetään henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018). Mainitun lain 1 §:n 1 momentin mukaan lakia sovelletaan, kun on kyse rikosten ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta tai yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä toiminnan yhteydessä.

Nyt kyseessä olevassa tilanteessa on katsottava olleen kyse tietomurtoon tai siihen rinnastettavan rikoksen estämisestä, paljastamisesta tai selvittämisestä tai aivan vähintään yleiseen turvallisuuteen kohdistuvan uhan ehkäisemisestä tähän liittyen. Kokonaisuutena tarkastellen lainsäätäjän tahtona on siten ollut, ettei Suomen viranomaisten voida edellyttää tekevän tietosuojavaltuutetun toimistolle tai rekisteröidyille ilmoituksia tilanteessa, jossa tämä selvästi olisi haitaksi Suomen kansalliselle turvallisuudelle tai ulko- ja turvallisuuspolitiikalle. Tietosuojalain 2 §:n 1 momenttia on tulkittava tämän tahdon mukaisella tavalla.

Ulkoministeriön jo todisteeksi nimeämää tiedotetta ei ole tarvetta arvioida yleisen tietosuoja-asetuksen artiklan 34 kohdan c alakohdan tarkoittamana tiedonantona, koska rekisteröidyille on jo ilmoitettu suoraan. Ulkoministeriö tulkitsee tietosuojavaltuutetun toimiston katsovan, ettei ilmoitusvelvollisuuden henkilöllisen ulottuvuuden voida katsoa ulottuvan sellaisiin ei-työntekijöihin, joiden tietoja on mahdollisesti ollut hyökkäyksen kohteena olevalla tietolaitteella. Ulkoministeriön työntekijän hyökkäyksen kohteena olevaan puhelimeen tallennettu toisen henkilön puhelinnumero ei siten synnyttäisi velvoitetta ilmoittaa tälle toiselle henkilölle tapahtuneesta. Tämä on ulkoministeriön mielestä oikea tulkinta. Koska ulkoministeriön työntekijän puhelimeen voi olla tallennettuna kyberhyökkäystä suorittavan valtion edustajan puhelinnumero, tarkoittaisi vastakkainen tulkinta sitä, että Suomen katsottaisiin olevan oikeudellisesti velvoitettu paljastamaan kyberhyökkääjälle Suomen havainneen hyökkäyksen. Tulkinta olisi itsestään selvistä syistä äärimmäisen ongelmallinen Suomen kansallisen turvallisuuden ja ulko- ja turvallisuuspolitiikan kannalta.

Siltä osin kuin näihin tietoihin liittyen katsottaisiin sovellettavan jonkinlaista velvoitetta suorittaa julkinen tiedonanto, ulkoministeriö on täyttänyt tämän velvoitteen julkaisemalla tiedotteen.

Suullinen käsittely

Hallinto-oikeus on 6.9.2023 järjestänyt asiassa suullisen käsittelyn ulkoministeriön tiloissa. Käsittelystä laadittu pöytäkirja (23/S28/1) on liitetty asiakirjoihin. Suullisessa käsittelyssä on kuultu ulkoministeriötä ja ministeriön nimeämiä todistajia sekä tietosuojavaltuutettua valituksenalaisen päätöksen perusteena olevista seikoista. Suullisessa käsittelyssä ulkoministeriö on muun ohella esittänyt selvitystä siitä, milloin ulkoministeriö on saanut tiedon tietoturvaloukkauksesta sekä rekisteröidyistä, joita tietoturvaloukkaus on koskenut ja milloin ulkoministeriö on ilmoittanut tietoturvaloukkauksesta rekisteröidyille. Käsittely toimitettiin oikeudenkäynnin julkisuudesta hallintotuomioistuimissa annetun lain 11 §:n nojalla yleisön läsnä olematta.

Hallinto-oikeuden ratkaisu

Hallinto-oikeus hylkää valituksen.

Perustelut

Kysymyksenasettelu

Tietosuojavaltuutetun toimisto on 24.1.2022 vastaanottanut ulkoministeriön ilmoituksen henkilötietoihin kohdistuneesta tietoturvaloukkauksesta, joka on aiheutunut NSO Groupin Pegasus -vakoiluhaittaohjelmasta ja kohdistunut Suomen ulkomailla työskentelevään lähetettyyn henkilökuntaan. Kyseessä on ollut erittäin kehittynyt haittaohjelma, joka on pystytty tuomaan käyttäjän puhelimeen (Apple/Android) Suomen ulkomaan edustustossa hänen huomaamattaan ja ilman käyttäjän toimenpiteitä. Vakoiluohjelma on voinut mahdollistaa hyvin laajasti puhelimessa olevan tiedon ja sen ominaisuuksien hyväksikäytön.

Asiassa on valituksen johdosta ratkaistavana, sovelletaanko edellä mainittuun tietoturvaloukkaukseen yleistä tietosuoja-asetusta ja sen tietoturvaloukkauksesta ilmoittamista koskevia 33 ja 34 artikloja. Ulkoministeriö on vedonnut siihen, että yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a alakohdan mukaan asetusta ei sovelleta henkilötietojen käsittelyyn, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan, ja että asetuksen johdanto-osan 16 perustelukappaleessa on tarkennettu, että kansallista turvallisuutta koskevat toimet on rajattu asetuksen soveltamisalan ulkopuolelle.

Mikäli asetus tulee sovellettavaksi, asiassa on arvioitavana, onko ulkoministeriö ilmoittanut tietoturvaloukkauksesta rekisteröidyille asetuksen 34 artiklan 1 kohdan edellyttämässä määräajassa. Arvioitavaksi tulee sen jälkeen vielä, onko apulaistietosuojavaltuutetulla ollut edellytykset antaa asetuksen 58 artiklan 2 kohdan b alakohdan mukainen huomautus 33 ja 34 artiklojen rikkomisen vuoksi. Artiklan 33 osalta hallinto-oikeus toteaa, että ulkoministeriö ei ole väittänyt, että se olisi ilmoittanut tietoturvaloukkauksesta asetuksen 33 artiklan 1 kohdan edellyttämässä määräajassa tietosuojavaltuutetulle.

Yleisen tietosuoja-asetuksen soveltaminen

Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) 2 artiklan 1 kohdan mukaan asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan mukaan asetusta ei sovelleta henkilötietojen käsittelyyn:

a) jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan;

b) jota suorittavat jäsenvaltiot toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa.

Yleisen tietosuoja-asetuksen johdanto-osan 16 perustelukappaleen mukaan asetus ei koske unionin oikeuden soveltamisalaan kuulumattomia perusoikeuksien ja -vapauksien suojeluun tai henkilötietojen vapaaseen liikkuvuuteen liittyviä kysymyksiä, kuten kansallista turvallisuutta koskevia toimia. Tämä asetus ei koske henkilötietojen käsittelyä jäsenvaltioissa niiden toteuttaessa unionin yhteiseen ulko- ja turvallisuuspolitiikkaan liittyvää toimia.

Yleisen tietosuoja-asetuksen 23 artiklan 1 kohdan a, c ja d alakohtien mukaan rekisterinpitäjään tai henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan lainsäädäntötoimenpiteellä rajoittaa 12–22 artiklassa ja 34 artiklassa sekä 5 artiklassa, siltä osin kuin sen säännökset vastaavat 12–22 artiklassa säädettyjä oikeuksia ja velvollisuuksia, säädettyjen velvollisuuksien ja oikeuksien soveltamisalaa, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide, jotta voidaan taata kansallinen turvallisuus, yleinen turvallisuus ja rikosten ennalta estäminen, tutkinta, paljastaminen tai rikoksiin liittyvät syytetoimet taikka rikosoikeudellisten seuraamusten täytäntöönpano, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu tai tällaisten uhkien ehkäisy. Asetuksen 23 artiklan 2 kohdan c alakohdan mukaan edellä 1 kohdassa tarkoitettujen lainsäädäntötoimenpiteiden on sisällettävä tarpeen mukaan erityisiä säännöksiä, jotka koskevat ainakin käyttöön otettujen rajoitusten soveltamisalaa.

Tietosuojalain 1 §:n mukaan tällä lailla täsmennetään ja täydennetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 (yleinen tietosuoja-asetus) ja sen kansallista soveltamista.

Tietosuojalain 2 §:n 1 momentin mukaan tätä lakia sovelletaan tietosuoja-asetuksen 2 artiklan soveltamisalan mukaisesti. Tätä lakia ja tietosuoja-asetusta sovelletaan lisäksi, lukuun ottamatta asetuksen 56 artiklaa ja VII lukua, sellaiseen henkilötietojen käsittelyyn, jota suoritetaan mainitun 2 artiklan 2 kohdan a ja b alakohdassa tarkoitetun toiminnan yhteydessä, jollei muualla laissa toisin säädetä. Pykälän 3 momentin mukaan tätä lakia ei sovelleta sellaiseen henkilötietojen käsittelyyn, josta säädetään henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018).

Tietosuojalain esitöissä (HE 9/2018 vp) on 2 §:n 1 momenttia koskevissa yksityiskohtaisissa perusteluissa todettu, että pykälän 1 momentissa ilmaistaisiin lain soveltamisala. Soveltamisalaa koskevan pykälän 1 momentissa todettaisiin, että lakia sovelletaan tietosuoja-asetuksen 2 artiklan soveltamisalan mukaisesti. Yleisen tietosuoja-asetuksen 2 artiklan mukaan asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdassa rajataan asetuksen soveltamisalan ulkopuolelle henkilötietojen käsittely, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan ja käsittely, jota suorittavat jäsenvaltiot toteuttaessaan erityismääräyksiä yhteisestä ulko- ja turvallisuuspolitiikasta koskevan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa. Lisäksi rikosasioiden tietosuojadirektiivin soveltamisalaan kuuluva henkilötietojen käsittely on rajattu yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle.

Tietosuojalakia sovellettaisiin yleisen tietosuoja-asetukseen nähden täydentävästi. Pykälässä säädettäisiin, että yleistä tietosuoja-asetusta sovellettaisiin sellaiseen henkilötietojen käsittelyyn, joka ei kuulu unionin lainsäädännön soveltamisalaan sekä henkilötietojen käsittelyyn, joka tapahtuisi SEU V osaston 2 jaksossa tarkoitettuun yhteisen ulko- ja turvallisuuspolitiikkaan liittyen. Yleisen tietosuoja-asetuksen soveltamisalan laajentaminen ei koskisi tilanteita, joissa unionin lainsäädännön soveltamisalan ulkopuolelle jäävässä asiassa olisi kansallisella lailla toisin säädetty.

Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (rikosasioiden tietosuojalaki) 1 §:n 1 momentin 1 ja 5 kohtien mukaan tätä lakia sovelletaan toimivaltaisten viranomaisten käsitellessä henkilötietoja, kun kyse on rikosten ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta ja yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä 1–4 kohdassa tarkoitetun toiminnan yhteydessä.

Hallinto-oikeus toteaa, että yleinen tietosuoja-asetus ei lähtökohtaisesti tule sen 2 artiklan 2 kohdan a alakohdan ja johdanto-osan perustelukappaleen 16 perusteella sovellettavaksi kansalliseen ulko- ja turvallisuuspolitiikkaan liittyvään henkilötietojen käsittelyyn. Tietosuojalain 2 §:n 1 momentissa on kuitenkin laajennettu yleisen tietosuoja-asetuksen soveltamista siten, että asetusta sovelletaan myös sellaiseen henkilötietojen käsittelyyn, joka jää asetuksen 2 artiklan 2 kohdan a alakohdan perusteella asetuksen soveltamisen

ulkopuolelle. Tietosuojalain esitöiden mukaan edellä mainittu yleisen tietosuoja-asetuksen soveltamisalan laajentaminen ei koskisi tilanteita, joissa unionin lainsäädännön soveltamisalan ulkopuolelle jäävässä asiassa olisi kansallisella lailla toisin säädetty.

Hallinto-oikeus katsoo, että koska yleisen tietosuoja-asetuksen soveltamisalaa on kansallisesti laajennettu, Suomi voisi unionin oikeuden estämättä kansallisessa lainsäädännössä säätää, ettei yleisen tietosuoja-asetuksen 33 ja 34 artiklan tietoturvaloukkauksen ilmoittamisvelvollisuuksia ja määräaikoja sovelleta kansalliseen ulko- ja turvallisuuspolitiikkaan ja kansalliseen turvallisuuteen liittyvien henkilötietojen käsittelyyn. Suomessa ei kuitenkaan ole säädetty tällaista poikkeamaa. Näin ollen hallinto-oikeus katsoo, että asiassa sovelletaan yleistä tietosuoja-asetusta tietosuojalain 2 §:n 1 momentin nojalla ja myös asetuksen 33 ja 34 artiklat tulevat siten tässä asiassa sellaisinaan sovellettavaksi. Lainsäätäjän tarkoituksen on ilmettävä laista ja lainvalmisteluaineistosta eikä tietosuojalain valmisteluaineisto sisällä kansalliseen turvallisuuteen liittyviä näkökohtia tai varauksia koskien yleisen tietosuoja-asetuksen soveltamisalan laajennusta sen varsinaisen soveltamisalan ulkopuolelle. Hallinto-oikeus katsoo sen vuoksi, ettei valituksessa, vastaselityksessä ja suullisessa käsittelyssä esitettyjä näkökohtia liittyen muun ohella rikosasioiden tietosuojalakiin voida käyttää tulkinta-apuna arvioitaessa lainsäätäjän tarkoitusta sen suhteen, missä laajuudessa yleistä tietosuoja-asetusta sovelletaan tai ei sovelleta kansalliseen ulko- ja turvallisuuspolitiikkaan liittyviin asioihin.

Tietoturvaloukkauksesta ilmoittaminen rekisteröidyille

Yleisen tietosuoja-asetuksen 4 artiklan 12 kohdan mukaan asetuksessa tarkoitetaan ’henkilötietojen tietoturvaloukkauksella’ tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Yleisen tietosuoja-asetuksen 34 artiklan 1 kohdan mukaan, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

Yleisen tietosuoja-asetuksen johdanto-osan 86 kohdan mukaan rekisterinpitäjän olisi ilmoitettava henkilötietojen tietosuojaloukkauksesta rekisteröidylle viipymättä, jos tämä tietosuojaloukkaus todennäköisesti aiheuttaa luonnollisen henkilön oikeuksia ja vapauksia koskevan suuren riskin, jotta rekisteröity voi toteuttaa tarvittavat varotoimet. Ilmoituksessa olisi kuvattava henkilötietojen tietoturvaloukkauksen luonne ja esitettävä suosituksia siitä, miten asianomainen luonnollinen henkilö voi lieventää sen mahdollisia haittavaikutuksia. Tällainen ilmoitus rekisteröidylle olisi tehtävä niin pian kuin se on kohtuudella mahdollista ja tiiviissä yhteistyössä valvontaviranomaisen kanssa noudattaen valvontaviranomaisen tai muiden asiaankuuluvien viranomaisten (kuten lainvalvontaviranomaisten) antamia ohjeita. Esimerkiksi tarve lieventää välittömien haittojen riskiä edellyttää sitä, että rekisteröidyille ilmoitetaan viipymättä, kun taas tarve toteuttaa asianmukaiset toimenpiteet tietoturvaloukkauksen jatkumisen tai vastaavien

henkilötietojen tietoturvaloukkausten estämiseksi voivat olla perusteena pidemmälle ilmoitusajalle.

Euroopan unionin neuvoa-antavan elimen tietosuojatyöryhmän antamissa suuntaviivoissa asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta (WP250rev.01, annettu 3.10.2017, viimeksi tarkistettu ja hyväksytty 6.2.2018) todetaan, että arvioitaessa tietoturvaloukkauksen aiheuttamaa riskiä henkilöiden oikeuksille ja vapauksille keskitytään eri asioihin kuin tietosuojaa koskevassa vaikutustenarvioinnissa. Tietosuojaa koskevassa vaikutustenarvioinnissa otetaan huomioon sekä riskit, jotka aiheutuvat, kun tiedonkäsittely suoritetaan suunnitellusti, että tietoturvaloukkauksen aiheuttamat riskit. Mahdollisen tietoturvaloukkauksen yhteydessä siinä tarkastellaan yleisesti tietoturvaloukkauksen todennäköisyyttä ja siitä rekisteröidylle mahdollisesti aiheutuvia vahinkoja; toisin sanoen siinä arvioidaan hypoteettista tapahtumaa. Todellisen tietoturvaloukkauksen kohdalla tapahtuma on jo tapahtunut, ja näin ollen painopiste on siitä aiheutuvassa henkilöihin kohdistuvien vaikutusten riskissä.

Hallinto-oikeus katsoo, että kysymyksessä oleva henkilötietojen tietoturvaloukkaus, joka on kohdistunut Suomen ulkomailla olevan edustuston käytössä oleviin mobiililaitteisiin, aiheuttaa yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa tarkoitetulla tavalla todennäköisesti korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Ulkoministeriö on suullisessa käsittelyssä tarkemmin esittämällään tavalla ilmoittanut tietoturvaloukkauksesta henkilökohtaisesti verkkovakoilun kohteena olevalle kohdehenkilölle ja tämän henkilön lähipiirille sekä edustuston työntekijöille.

Hyökkäyksen kohdistuessa henkilöiden mobiililaitteisiin kyseinen vakoiluohjelma on voinut käsitellä myös laitteen tietosisällössä mainittujen muiden henkilöiden tietoja. Tällaisille henkilöille ei saadun selvityksen perusteella ole henkilökohtaisesti ilmoitettu tapahtuneesta, vaan ulkoministeriö on 28.1.2022 julkaissut verkkosivuillaan tiedotteen asiasta.

Apulaistietosuojavaltuutettu on katsonut, ettei ulkoministeriö ole noudattanut yleisen tietosuoja-asetuksen 34 artiklan 1 kohtaa, jonka mukaan rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä. Apulaistietosuojavaltuutettu on lausunnossaan tuonut esiin, että tietosuojavaltuutetun toimiston ulkoministeriöltä saaman suullisen selvityksen ja tietoturvaloukkausta koskevan ilmoituksen sekä ulkoministeriön kotisivuilla olevan tiedotteen mukaan loukkaus on tapahtunut jo vuoden 2021 aikana. Tietoturvaloukkauksesta tiedon saamisen ja rekisteröidylle tehtävän ilmoituksen välissä on lausunnon mukaan ollut aika, jota voidaan pitää erityisesti tietoturvaloukkauksen syynä olevan haittaohjelman luonteen ja rekisteröityjen aseman ulkoministeriön ulkomailla työskentelevinä virkamiehinä huomioon ottaen liian pitkänä.

Hallinto-oikeus katsoo saadun selvityksen perusteella, että ulkoministeriö on tietoturvaloukkauksesta riittävän varmuuden saatuaan ilmoittanut siitä asetuksen 34 artiklan 1 kohdan tarkoittamalla tavalla ilman aiheetonta viivästystä niille rekisteröidyille, joiden mobiililaitteisiin verkkovakoilu on kohdistunut. Ilmoittamisen tietoturvaloukkauksesta kaikille mobiililaitteiden

tietosisällössä mainituille rekisteröidyille on katsottava tapahtuneen ulkoministeriön 28.1.2022 verkkosivuilla julkaistulla tiedotteella. Asiassa saadun selvityksen perusteella ulkoministeriöllä on kuitenkin ollut riittävä varmuus tietoturvaloukkauksesta jo selvästi ennen tätä ajankohtaa. Kun otetaan huomioon tietoturvaloukkauksen laatu ja rekisteröidyille siitä aiheutuvien mahdollisten vaikutusten vakavuus sekä toisaalta ulkoministeriön suorittamat toimet ja se, ettei Suomessa ole säädetty yleisen tietosuoja-asetuksen 23 artiklassa sinänsä sallittuja rajoituksia 34 artiklan soveltamiselle kansallisen turvallisuuden takaamisen perusteella, hallinto-oikeus katsoo, ettei ulkoministeriö ole ilmoittanut loukkauksesta viimeksi mainituille tahoille ilman aiheetonta viivästystä.

Huomautus

Yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaan jokaisella valvontaviranomaisella on toimivaltuudet antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet tämän asetuksen säännösten vastaisia.

Hallinto-oikeus toteaa, ettei ulkoministeriö ole ilmoittanut tietoturvaloukkauksesta yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa edellytetyllä tavalla 72 tunnin kuluessa valvontaviranomaiselle eli tietosuojavaltuutetulle eikä myöskään ole esittänyt sellaista selitystä, jonka perusteella artiklassa mahdollistettu vaiheittainen ilmoittaminen ei olisi ollut mahdollista. Ilmoitus on tehty vasta 24.1.2022. Hallinto-oikeus on myös edellä todetulla tavalla katsonut, ettei kaikille rekisteröidyille ole ilmoitettu tietoturvaloukkauksesta yleisen tietosuoja-asetuksen 34 artiklassa edellyttämässä määräajassa. Näin ollen hallinto-oikeus katsoo, että apulaistietosuojavaltuutetulla on ollut edellytykset antaa ulkoministeriölle asetuksen 58 artiklan 2 kohdan b alakohdan mukainen huomautus 33 ja 34 artikloiden rikkomisen vuoksi.

Sovelletut oikeusohjeet

Perusteluissa mainitut

Muutoksenhaku

Tähän päätökseen saa hakea muutosta valittamalla korkeimpaan hallinto-oikeuteen, jos korkein hallinto-oikeus myöntää valitusluvan.

Valitusosoitus on liitteenä (HOL valituslupa 30).

Hallinto-oikeuden kokoonpano

Asian ovat ratkaisseet hallinto-oikeuden jäsenet
[redacted].

Esittelijäjäsen [redacted]

Tämä päätös on sähköisesti varmennettu ja tulostettu hallinto-oikeuden asianhallintajärjestelmästä.

Jakelu ja oikeudenkäyntimaksu

Päätös	Valittajan asiamiehille sähköpostitse tavallisena tiedoksiantona
	Oikeudenkäyntimaksu 270 euroa
	Tiedote oikeudenkäyntimaksusta korkeimmassa hallinto-oikeudessa
Jäljennös	Apulaistietosuojavaltuutettu