TIETOSUOJAVALTUUTETUN TOIMISTO

23.03.2022

Dnro 2437/161/22

Apulaistietosuojavaltuutetun päätös

Asia

EU:n yleisen tietosuoja-asetuksen 33 ja 34 artiklojen mukaisten ilmoituksien myöhästyminen ja 34 artiklan mukaisen ilmoitusvelvollisuuden rajoitukset kansallisessa lainsäädännössä.

Rekisterinpitäjä

Ulkoministeriö

Asian taustaa

Tietosuojavaltuutetun toimisto vastaanotti ulkoministeriön (jäljempänä rekisterinpitäjä) ilmoituksen henkilötietoihin kohdistuneesta tietoturvaloukkauksesta 24.01.2022. Tietoturvaloukkaus on rekisterinpitäjän ilmoituksen mukaan johtunut NSO Groupin Pegasus -vakoiluhaittaohjelmasta.

Rekisterinpitäjä on tietosuojavaltuutetun toimistolle tekemänsä ilmoituksen mukaan selvittänyt tietoturvaloukkausta ja sen syitä eri viranomaisten ja sidosryhmien kanssa syksyn ja talven 2021–2022 aikana. Tietoturvaloukkaus on kohdistunut Suomen ulkomailla työskentelevään lähetettyyn henkilökuntaan. Rekisterinpitäjä on ilmoittanut tietoturvaloukkauksesta sen kohteena olleille rekisteröidyille.

Tietosuojavaltuutetun toimisto pyysi rekisterinpitäjältä 09.03.2022 tarkempaa selvitystä Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (jäljempänä yleinen tietosuoja-asetus) 33 ja 34 artiklojen mukaisten ilmoitusten tekemisen ajankohdista.

Rekisterinpitäjältä saatu selvitys

Rekisterinpitäjä antoi tietosuojavaltuutetun toimistolle selvityksen tietoturvaloukkausta koskevien ilmoituksien ajankohdasta 16.03.2022.

Rekisterinpitäjän antaman 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.

Oikeudellinen kysymys

Asiassa on ratkaistava:

1. Onko rekisterinpitäjä ylittänyt yleisen tietosuoja-asetuksen 33 artiklan mukaisen 72 tunnin aikarajan tehdä ilmoitus henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle?

2. Jos rekisterinpitäjä on ylittänyt yleisen tietosuoja-asetuksen mukaisen aikarajan, onko rekisterinpitäjän toimittanut valvontaviranomaiselle perustellun selityksen?

3. Onko rekisterinpitäjä noudattanut yleisen tietosuoja-asetuksen 34 artiklan 1 kohdan velvollisuutta ilmoittaa rekisteröidyille tietoturvaloukkauksesta ilman aiheetonta viivytystä?

4. Onko rekisterinpitäjälle annettava yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukainen huomautus?

Apulaistietosuojavaltuutetun päätös ja perustelut

1. Yleisen tietosuoja-asetuksen mukaisen 72 tunnin aikarajan ylittäminen

Apulaistietosuojavaltuutettu katsoo, ettei rekisterinpitäjä ole noudattanut yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan mukaista 72 tunnin aikarajaa.

Perustelut:

Sovellettavat säädökset ja oikeusohjeet

Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan 1 lauseen mukaan jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Yleisen tietosuoja-asetuksen johdanto-osan 85 kohdan mukaan jos henkilötietojen tietoturvaloukkaukseen ei puututa riittävän tehokkaasti ja nopeasti, siitä voi aiheutua luonnollisille henkilöille fyysisiä, aineellisia tai aineettomia vahinkoja, kuten omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintää, identiteettivarkaus tai petos, taloudellisia menetyksiä, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys tai muuta merkittävää taloudellista tai sosiaalista vahinkoa. Sen vuoksi rekisterinpitäjän olisi ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä heti, kun se on tullut rekisterinpitäjän tietoon, ja mahdollisuuksien mukaan 72 tunnin kuluessa, paitsi jos rekisterinpitäjä pystyy osoittamaan tilivelvollisuusperiaatteen mukaisesti, että henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos tällaista ilmoitusta ei voida tehdä 72 tunnin kuluessa, ilmoitukseen olisi liitettävä selvitys viivytyksen syistä, ja tietoa voidaan antaa vaiheittain ilman aiheetonta lisäviivytystä.

Yleisen tietosuoja-asetuksen johdanto-osan 87 kohdan mukaan olisi tarkistettava, onko kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus, ja saattaa asia viipymättä valvontaviranomaisen ja rekisteröidyn tiedoksi. Se, että ilmoitus tehtiin ilman aiheetonta viivytystä, olisi selvitettävä ottaen huomioon erityisesti henkilötietojen tietoturvaloukkauksen luonne ja vakavuus sekä tästä rekisteröidylle aiheutuvat seuraukset ja haittavaikutukset. Kyseinen ilmoitus voi johtaa siihen, että valvontaviranomainen puuttuu asiaan sille tässä asetuksessa säädettyjen tehtävien ja toimivaltuuksien mukaisesti.

Euroopan tietosuojaneuvoston WP29-työryhmän suuntaviivoissa asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta todetaan, että rekisterinpitäjän olisi katsottava tulleen tietoiseksi tietoturvaloukkauksesta silloin, kun sillä on kohtuullinen varmuus siitä, että on tapahtunut henkilötietoja vaarantava turvapoikkeama. Se, milloin tarkalleen tietyn tietoturvaloukkauksen voidaan katsoa tulleen rekisterinpitäjälle ”ilmi”, riippuu kunkin tietoturvaloukkauksen olosuhteista.[1]

Suuntaviivojen mukaan kun rekisterinpitäjä on saanut tiedon mahdollisesta tietoturvaloukkauksesta yksityishenkilöltä, media-alan organisaatiolta tai muusta lähteestä tai jos se itse on havainnut turvapoikkeaman, se voi vähän aikaa tutkia, onko tietoturvaloukkaus todella tapahtunut. Tämän tutkinnan aikana ei voida katsoa, että tietoturvaloukkaus on tullut ”ilmi” rekisterinpitäjälle. Alustavan tutkinnan edellytetään kuitenkin alkavan mahdollisimman pian, ja sillä olisi selvitettävä kohtuullisen varmasti, onko tietoturvaloukkaus tapahtunut; tämän jälkeen voidaan suorittaa tarkempi tutkinta.[2]

Oikeudellinen arviointi ja perustelut

Saadun selvityksen perusteella rekisterinpitäjä on saanut kohtuullisen varmuuden tietoturvaloukkauksen tapahtumisesta huomattavasti ennen ilmoituksen tekemistä valvontaviranomaiselle.

Apulaistietosuojavaltuutettu katsoo, ettei rekisterinpitäjä ole noudattanut tietosuoja-asetuksen 33 artiklan 1 kohdan mukaista velvollisuutta ilmoittaa valvontaviranomaisen henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta.

2. Rekisterinpitäjän selitys tietoturvaloukkauksen ilmoittamatta jättämisestä

Apulaistietosuojavaltuutettu katsoo, ettei rekisterinpitäjä ole esittänyt yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa tarkoitettua perusteltua selitystä henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle tehtävän ilmoituksen myöhästymisestä.

Perustelut

Sovellettavat säädökset ja oikeusohjeet

Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan toisen lauseen mukaan jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys.

Mainitun artiklan 4 kohdan mukaan jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

Oikeudellinen arviointi ja perustelut

Vaikka yleisessä tietosuoja-asetuksessa jossakin määrin sallitaan ilmoittamisen viivästyminen, tätä ei tulisi pitää säännöllisenä käytäntönä. Selityksen antamista tietoturvaloukkauksen myöhästymisestä ei voida pitää vaihtoehtona

[1] WP29 ohje sivu 11
[2] WP29 ohje sivu 12

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. Nyt kyseessä olevassa tapauksessa rekisterinpitäjä ei ole esittänyt sellaista selitystä, jonka perusteella vaiheittainen ilmoittaminen ei olisi ollut mahdollista.

Apulaistietosuojavaltuutettu katsoo, etteivät rekisterinpitäjän esittämät selitykset tietoturvaloukkausta koskevan ilmoituksen myöhästymiselle ole osoittaneet, että rekisterinpitäjällä ei olisi ollut mahdollisuutta noudattaa ilmoituksen tekemisessä yleisen tietosuoja-asetuksen mukaista 72 tunnin aikarajaa.

3. Yleisen tietosuoja-asetuksen 34 artiklan 1 kohdan velvollisuus ilmoittaa rekisteröidyille tietoturvaloukkauksesta ilman aiheetonta viivytystä

Apulaistietosuojavaltuutettu katsoo, ettei rekisterinpitäjä ole noudattanut yleisen tietosuoja-asetuksen 34 artiklan 1 kohtaa, jonka mukaan rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

Perustelut

Sovellettavat säädökset ja oikeusohjeet

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.

Yleisen tietosuoja-asetuksen 23 artiklan 1 kohdan a kohdan 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.

Yleisen tietosuoja-asetuksen 73 kohdan mukaan rajoituksia, jotka koskevat erityisiä periaatteita ja oikeutta saada ilmoitus tietojenkäsittelystä, pääsyä tietoihin ja oikeutta oikaista tai poistaa henkilötietoja ja oikeutta siirtää tiedot järjestelmästä toiseen, oikeutta vastustaa tietojenkäsittelyä, profilointiin perustuvia päätöksiä sekä henkilötietojen tietoturvaloukkauksesta ilmoittamista rekisteröidylle sekä eräitä näihin liittyviä rekisterinpitäjän velvollisuuksia, voidaan asettaa unionin oikeudessa tai jäsenvaltion lainsäädännössä siltä osin kuin ne ovat välttämättömiä ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä yleisen turvallisuuden takaamiseksi, muun muassa ihmishenkien suojelemiseksi erityisesti ihmisen aiheuttaman tai luonnonkatastrofin yhteydessä taikka rikosten tai, säännellyn ammattitoiminnan yhteydessä, ammattietiikan rikkomisen ennaltaehkäisemistä, tutkintaa ja rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy, tai muiden unionin tai jäsenvaltion tärkeiden yleistä etua koskevien syiden vuoksi, erityisesti unionin tai jäsenvaltion tärkeiden taloudellisten tai rahoitusta koskevien etujen vuoksi, yleiseen etuun liittyvistä syistä pidettävien julkisten rekisterien pitämiseksi, arkistoitujen henkilötietojen myöhemmän käsittelyn vuoksi, jonka perusteena on yksittäisten tietojen hankkiminen poliittisesta toiminnasta entisten totalitaaristen valtioiden järjestelmissä, tai rekisteröidyn suojelemiseksi tai muille kuuluvien oikeuksien ja vapauksien, muun muassa sosiaaliturvan, kansanterveyden ja humanitaaristen tarkoitusten, turvaamiseksi. Näiden rajoitusten olisi oltava perusoikeuskirjassa ja ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä eurooppalaisessa yleissopimuksessa vahvistettujen vaatimusten mukaisia.

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietinnössä on tietosuoja-asetuksen sisältämää liikkumavaraa koskien todettu, että yleisen tietosuoja-asetuksen 23 artikla mahdollistaa 34 artiklan rajoittamisen kansallisella lailla. Johtuen 23 artiklassa säädetystä vaatimuksesta sääntelyn yksiselitteisyydestä ja tarkkarajaisuudesta, rajoituksesta 34 artiklaan ei ole mahdollista säätää yleislaissa.[3]

Oikeudellinen arviointi ja perustelut

Rekisterinpitäjä on saadun selvityksen perusteella ilmoittanut tietosuoja-asetuksen 34 artiklan mukaiset tiedot tietoturvaloukkauksen kohteena olleille rekisteröidyille. Ilmoitusta ei kuitenkaan saadun selvityksen perusteella 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.

[3] EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö s. 55

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.

Apulaistietosuojavaltuutetun saaman selvityksen mukaan 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.

4. Seuraamusharkinta

Apulaistietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ole noudattanut toiminnassaan tietosuoja-asetuksen 33 ja 34 artikloja ilmoitusvelvollisuuksista ja antaa tälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaisen huomautuksen.

Perustelut

Sovellettavat säädökset ja oikeusohjeet

Yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaan jokaisella valvontaviranomaisella on kaikki seuraavat korjaavat toimivaltuudet:

b) antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet tämän asetuksen säännösten vastaisia.

Yleisen tietosuoja-asetuksen johdanto-osan 148 kohdan mukaan tämän asetuksen sääntöjen täytäntöönpanon vahvistamiseksi asetuksen säännösten rikkomisesta olisi määrättävä seuraamuksia, kuten hallinnollisia sakkoja, valvontaviranomaisen tämän asetuksen mukaisesti määräämien asianmukaisten toimenpiteiden lisäksi tai niiden sijasta. Jos kyseessä on vähäinen rikkominen tai jos määrättävä sakko olisi kohtuuton rasitus luonnolliselle henkilölle, voidaan sakon sijasta antaa huomautus. Rikkomisen luonteeseen, vakavuuteen ja kestoon, sen tahallisuuteen, aiheutuneen vahingon lieventämiseksi toteutettuihin toimiin, vastuun asteeseen tai mahdollisiin vastaaviin aiempiin rikkomisiin, tapaan, jolla rikkominen tuli valvontaviranomaisen tietoon, rekisterinpitäjälle tai henkilötietojen käsittelijälle määrättyjen toimenpiteiden noudattamiseen, käytännesääntöjen noudattamiseen ja mahdollisiin muihin raskauttaviin tai lieventäviin tekijöihin olisi kuitenkin kiinnitettävä asianmukaista huomiota. Seuraamusten, kuten hallinnollisten sakkojen, määräämiseen olisi sovellettava riittäviä menettelytakeita unionin lainsäädännön ja perusoikeuskirjan yleisten periaatteiden mukaisesti, tehokkaat oikeussuojakeinot ja asianmukainen prosessi mukaan luettuina.

Oikeudellinen arviointi ja perustelut

Apulaistietosuojavaltuutettu on edellä katsonut, ettei rekisterinpitäjä ole noudattanut yleisen tietosuoja-asetuksen 33 ja 34 artiklojen mukaisia määräaikoja henkilötietojen tietoturvaloukkauksen ilmoittamisessa.

Apulaistietosuojavaltuutettu katsoo, että huomioon ottaen huomioon rikotut artiklat, tietoturvaloukkauksen syyt, rekisterinpitäjän mahdollisuudet ilmoittaa tietoturvaloukkauksesta ajoissa, tietoturvaloukkauksen merkityksen rekisteröidyille ja ilmoituksen myöhästymisen vaikutukset rekisteröityjen mahdollisuuteen minimoida tietoturvaloukkauksesta aiheutuvia riskejä, rekisterinpitäjälle on perusteltua antaa yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukainen huomautus.

Sovelletut lainkohdat

Päätöksessä mainitut

Muutoksenhaku

Tietosuojalain (1050/2018) 25 §:n mukaan tähän päätökseen voi hakea muutosta valittamalla hallinto-oikeuteen noudattaen mitä laissa oikeudenkäynnistä hallintoasioissa (808/2019) säädetään. Valitus tehdään hallinto-oikeuteen.

Tiedoksianto

Päätös annetaan tiedoksi hallintolain (434/2003) 60 §:n mukaisesti postitse saantitodistusta vastaan.

Päätös saatetaan ulkoministeriön ja oikeusministeriön tietoon perustelujen kohdassa 3 ilmenevän mahdollisen sääntelytarpeen arvioimista varten.