TIETOSUOJAVALTUUTETUN TOIMISTO

Dnro 3394/171/21

20.9.2021

Apulaistietosuojavaltuutetun huomautus ja määräykset tietoturvalouk-kausta koskevan ilmoituksen johdosta

Ilmoittaja

Poliisihallitus

Tietoturvaloukkauksen kuvaus

Tietoturvaloukkausta koskevaa alustava ilmoitus

Keskusrikospoliisi sai 31.3.2021 yhdysvaltalaiselta Buzzfeed News-verkkojulkaisulta kyselyn siitä, ovatko Suomen poliisiviranomaiset käyttäneet Clearview AI nimistä sovellusta. Keskusrikospoliisi on vastannut kyselyyn 1.4.2021, ettei tiedossa ole, että teknologia olisi Suomen poliisin käytössä. Buzzfeed News palasi kyselyyn 7.4.2021 kertoen, että heillä on tiedossaan noin 120 tehtyä hakua vuodelta 2020. Buzzfeed News myös kertoi aiempiin tietoihinsa perustuen, että monet viranomaiset muualla maailmassa ovat tehneet haut ilmaisen kokeilujakson aikana, jolloin järjestelmää ei varsinaisesti ollut otettu käyttöön ja sen käyttö ei näin ollen ole välttämättä päätynyt organisaatioiden johdon tietoon. Poliisihallitus ja Keskusrikospoliisi aloittivat välittömästi 7.4.2021 selvitystyön mahdollisesta kokeilujaksosta ja pyysivät myös lisätietoja Buzzfeediltä Newsiltä sovelluksen käytöstä.

Alkuvuodesta 2020 Keskusrikospoliisin CAM/CSE-ryhmässä on otettu Clearview AI ilmainen kokeilukäyttö testaukseen soveltuvuuden varmistamiseksi. CAM/CSE-ryhmä muun muassa esiseuloo kansainvälisiä, mahdollista lasten seksuaalista hyväksikäyttömateriaalia sisältäviä paketteja, jotka saapuvat NCMEC:ltä (National Center for Missing and Exploited Children). NCMEC on kansainvälinen organisaatio, joka tekee yhteistyötä sosiaalisen median palveluiden kanssa keräten niiltä materiaalia mahdollisista alaikäisten hyväksikäytöistä tai alaikäiseen liittyvän materiaalin jakamisesta.

Clearview AI -sovelluksen käyttö on rajoittunut NCMEC-tiedolla tehtyyn kokeiluun, jossa on pyritty hakemaan Clearview AI:lla mahdollisen uhrin julkista sosiaalisen median profiilia uhrin tunnistamiseksi ja suojelemiseksi ja selvittämään toimisiko työkalu jatkossa arvokkaana apuna tunnistamistyössä. Näin ollen henkilötietoja on käsitelty rikostorjuntatarkoituksessa. Kuvat sanitoitiin kokeilun aikana, jolla varmistuttiin siitä, etteivät ne sisällä muuta kuin haettavan mahdollisen uhrin kasvoprofiilin. NCMEC on kerännyt kuvat alun perin suurimmaksi osin sosiaalisesta mediasta. Kokeilun aikana löytyi yksi osuma, jossa lapsen seksuaalissävytteistä materiaalia yhdistettiin suomalaiseen profiiliin. Profiilin omistaja oli materiaalissa esiintyvä henkilö ja asia ohjattiin sosiaaliviranomaisten tietoon.

Saadun ennakkotiedon perusteella tuli käyttäjille käsitys, ettei palvelu tallenna hakuja. Tämänhetkisen selvityksen mukaan KRP:ssä on tehty noin 120 hakua vuonna 2020.

TIETOSUOJAVALTUUTETUN TOIMISTO

Tietosuojavaltuutetun toimiston pyytämä lisäselvitys

Rekisterinpitäjän 9.4.2021 tekemä tietoturvaloukkausta koskeva ilmoitus oli alustava. Rekisterinpitäjä ei oma-aloitteisesti täydentänyt ilmoitusta, jonka vuoksi tietosuojavaltuutetun toimisto pyysi 2.6.2021 asiassa lisäselvitystä rekisterinpitäjältä. Lisäselvitys saatiin 18.8.2021. Lisäselvityksessä todettiin seuraavaa:

Keskusrikospoliisin selvityksessä ilmeni 8.4.2021, että Europolin isännöimässä kokouksessa vuonna 2019 on esitelty ja suositeltu kyseistä Clearview AI-sovellusta seksuaalisen hyväksikäytön materiaalin (CAM/CSE) automaattiseen seulontaan. Esittelyssä annettiin ymmärtää osallistujille, että järjestelmä ei tallenna hakuja ja siten soveltuisi tähän käyttöön.

CAM/CSE-ryhmän keskeinen tehtävä on estää ja paljastaa lasten seksuaalista hyväksikäyttöä ja materiaalien levitystä. Loppuvuodesta 2019 Keskusrikospoliisin CAM/CSE-ryhmässä otettiin Clearview AI ilmaiseen kokeilukäyttöön ja testaukseen soveltuvuuden varmistamiseksi. Koekäyttö lopetettiin oma-aloitteisesti alkuvuodesta 2020. Ennen käyttöä keskusrikospoliisi sai rekisteröitymislinkkejä palveluun Ruotsista ja Latviasta. CAM/CSE-ryhmä muun muassa esikäsittelee kansainvälisiä, mahdollista lasten seksuaalista hyväksikäyttömateriaalia sisältäviä paketteja, jotka saapuvat NCMEC:ltä (National Center for Missing and Exploited Children). NCMEC on kansainvälinen organisaatio, joka tekee yhteistyötä sosiaalisen median palveluiden kanssa keräten niiltä materiaalia mahdollisista alaikäisten hyväksikäytöistä tai alaikäiseen liittyvän materiaalin jakamisesta.

Keskusrikospoliisissa Clearview AI sovelluksen koekäyttö rajoittui NCMEC-tiedolla tehtyyn kokeiluun, jossa pyrittiin hakemaan Clearview AI:lla mahdollisen uhrin julkista sosiaalisen median profiilia uhrin tunnistamiseksi ja suojelemiseksi rikostorjuntatarkoituksessa. Samalla selvitettiin, toimisiko työkalu jatkossa arvokkaana apuna tunnistamistyössä.

Keskusrikospoliisissa oli käytössä henkilökohtaisia koekäyttölisenssejä 4 kappaletta, jotka olivat voimassa yhden kuukauden. Koekäytön yhteydessä hakuja tehtiin pääasiallisesti testidatalla. CAM/CSE ryhmän nykyisen jäsenten toimesta ohjelmaa on testattu kahdessa tapauksessa oikeilla kuvilla. Kummassakaan tapauksessa ei ole käytetty kuvia, mitkä sisältäisivät mitään tietoa siitä, mikä asia on kyseessä tai mitään kuvaa täydentäviä tietoja, kuka kuvassa esiintyy. Kuvissa ei myöskään ole ollut sukupuolisiveellisyyttä loukkaavaa materiaalia. Hauissa on käytetty kasvokuvia, koska kyseessä on kasvojentunnistusohjelma.

Kokeilun aikana löytyi yksi osuma, jossa lapsen seksuaalissävytteistä materiaalia yhdistettiin suomalaiseen profiiliin. Profiilin omistaja oli materiaalissa esiintyvä henkilö ja asia ohjattiin sosiaaliviranomaisten tietoon. Tapauksesta ei käynnistetty esitutkintaa. Buzzfeed News -verkkojulkaisun antamaa lukumäärää hakujen määrästä ei ole saatu varmistettua selvityksessä. Täysin varmaa kuvaa ei myöskään ole selvityksessä saatu siitä, miten paljon ohjelmaa on kokeiltu oikeilla kuvilla henkilöpoistumista johtuen. Tehdyn testin perusteella Clearview AI todettiin soveltumattomaksi viranomaistyöhön tässä tarkoituksessa.

Lisäselvitysten myötä selvisi, että Keskusrikospoliisin CAM-ryhmällä on ollut käytössään 10.2.2020 - 3.3.2021 kanadalaisen NGO:n ylläpitämä Arachnid-palvelu, joka etsii verkossa CAM-materiaalia. Palvelua käytetään avoimessa verkossa web-selaimen

kautta. Kyseessä on ohjelma, joka etsii kaikkialta internetistä ns. lasten seksuaaliseen hyväksikäyttöön liittyvää materiaalia. Kyseisellä järjestöllä ja ohjelmalla on myös mahdollisuus edesauttaa laittoman materiaalin poistamista internetistä.

Portaalin kautta on mahdollista tehdä kyselyjä hash-luvuilla, kuvilla tai sitten kuvan voi tallentaa järjestelmään siten, että järjestelmä etsii kyseistä kuvaa automaattisesti tulevaisuudessakin. Palvelun käyttöönoton yhteydessä ohjeistettiin ryhmää tekemään kyselyjä vain sellaisilla valinnoilla, että tietoja ei tallenneta palveluun. Toiminnan kannalta kyseessä on ollut tiedon hankinta ei tiedon luovutus.

CAM/CSE ryhmä pyrkii torjumaan lasten seksuaalista hyväksikäyttöä ja ajoittain ilmenee tarvetta selvittää, onko jotain määrättyä kuvaa levitetty internetissä ja jos on niin, mistä se löytyy. Tätä ei varsinaisesti ole mahdollista tehdä ilman, että tavalla tai toisella internettiin kohdistetaan kuvahaku. Ei ollut ilmennyt mitään syytä epäillä kyseisen palveluntarjoajan luotettavuutta.

Keskusrikospoliisilta saatujen tietojen mukaan CAM/CSE nykyisestä ryhmästä palvelua oli käyttänyt 2 henkilöä, toinen kerran ja toinen kolme kertaa. Yhtään osumaa hakuihin ei ole tullut. Kyselyjen tarkat ajankohdat eivät ole tiedossa, mutta kyselyjä on tehty aikavälillä 10.2.2020 - 3.3.2021. Varsinaisesti palvelun käyttö lopetettiin selvityksen ajaksi 15.4.2021. Toisen tutkijan kysely liittyi yksittäiseen tiedustelutapaukseen, eikä kyselyssä käytetty cam-kuvaa ja toisen tutkijan kyselyt ovat olleet kyselyjä, joissa paikallispoliisi oli pyytänyt selvittämään, onko kuvia levitetty internetissä. Kuvien yhteyteen ei ole liitetty mitään tietoja, vaan palvelulla on pyritty tunnistamaan, onko tällaista kyseistä lasten seksuaalisen hyväksikäyttöön liittyvää kuvaa levitetty muualla verkossa.

Kuvissa esiintyvien henkilöiden määrä tai henkilöllisyys ei ole tiedossa. Kuvien tarkka sisältö ei ole valitettavasti tiedossa. On siis mahdollista, että kuvissa on useita henkilöitä, mutta on myös mahdollista, että henkilöt eivät ole tunnistettavissa ko. kuvista selkä kameraa kohti tyyppisistä syistä. Tiedossa ei ole, ovatko kuvat koskeneet samoja henkilöitä. Yhden arvion mukaan kuvissa on ollut 4–16 henkilön kuvia.

Kohteena olleet tiedot

Käsitellyt henkilötiedot ovat olleet henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018, jäljempänä rikosasioiden tietosuojalaki) 3 §:n 1 momentin 3 kohdan mukaisia biometrisiä henkilötietoja, joita koskee lain 11 §:ssä säädetyt käsittelyn edellytykset.

Rekisterinpitäjän antamien selvitysten perusteella kuvissa esiintyvien henkilöiden määrää tai henkilöllisyyttä ei ole pysytty kattavasti selvittämään. Selvityksen mukaan testidataa käytettäessä tutkijat ovat mm. käyttäneet omia kuviaan sekä Internetistä satunnaisesti valikoituja mihinkään liittymättömiä kuvia. Rekisterinpitäjä ei ole selvityksessään saanut varmaa kuvaa siitä, miten paljon ohjelmaa on kokeiltu oikeilla kuvilla henkilöpoistumista johtuen. Keskusrikospoliisin CAM/CSE ryhmän nykyisen jäsenten toimesta ohjelmaa on testattu kahdessa tapauksessa oikeilla kuvilla. Kummassakaan tapauksessa ei ole käytetty kuvia, mitkä sisältäisivät mitään tietoa siitä, mikä asia on kyseessä tai mitään kuvaa täydentäviä tietoja, kuka kuvassa esiintyy. Kuvissa ei myöskään ole ollut sukupuolisiveellisyyttä loukkaavaa materiaalia. Hauissa on käytetty kasvokuvia, koska kyseessä on kasvojentunnistusohjelma.

Toteutetut toimenpiteet

Rekisterinpitäjä ilmoitti selvityksissään seuraavat toteutetut ja tulevat toimenpiteet:

Toteutetut toimenpiteet

Koekäytön jälkeen Clearview AI -palvelun käyttö on lopetettu. Lisäselvityksen myötä havaitun Arachnid-palvelun käyttö on lopetettu 15.4.2021.

Poliisissa on vuoden 2020 aikana annettu ohjeistusta ja koulutusta erityisesti biometristen tietojen käsittelystä ja välineistä, joita tähän tarkoitukseen voidaan käyttää. Poliisi on ottanut toukokuussa 2020 käyttöön oman tietosuoja- ja tietoturvavaatimukset täyttävän kasvojen tunnistusjärjestelmä KASTUn. KASTU-järjestelmän avulla poliisi voi tunnistaa rikoksesta epäiltyjä henkilöitä poliisin tuntomerkkirekisteristä.

Nyt kyseessä olevan tapauksen esiin tultua Poliisihallitus pyysi välittömästi selvityksen keskusrikospoliisilta asiasta. Poliisihallitus toimitti ennakkoilmoituksen henkilötietoihin kohdistuneesta tietoturvaloukkauksesta tietosuojavaltuutetulle 9.4.2021. Samalla keskusrikospoliisi julkaisi asiasta myös tiedotteen. Poliisissa lähdettiin viivytyksestä myös varmistamaan, ettei muualla organisaatiossa ole kyseistä Clearview AI-palvelua käytössä. Tietoon ei ole tullut, että jossakin muualla poliisin organisaatiossa olisi tätä tai vastaavia palveluja käytetty.

Vastausaineiston perusteella riskejä minimoitiin sanitoimalla käytetyt kuvat. Tällä varmistettiin, etteivät ne sisällä muuta kuin haettavan mahdollisen uhrin kasvoprofiilin. Kyselyjä oli mahdollista tehdä myös hash-luvuilla. Palveluntuottaja oli kerännyt kuvat alun perin suurimmaksi osin internetistä / sosiaalisesta mediasta. Tapauksissa ei ole käytetty kuvia, mitkä sisältäisivät mitään tietoa siitä, mikä asia on kyseessä tai kuka kuvassa esiintyy. Kuvissa ei myöskään ole ollut sukupuolisiveellisyyttä loukkaavaa materiaalia.

Clearview AI -palvelun käyttäjät oli minimoitu neljään käyttäjään. Koekäyttölisenssi oli voimassa kuukauden ajan. Pääasiallisesti palvelua testattiin testidatalla. Testidataa käytettäessä tutkijat olivat käyttäneet omia kuviaan sekä internetistä satunnaisesti valikoituja mihinkään liittymättömiä kasvokuvia. Arachnid-palvelun käyttäjät minimoitiin kahteen käyttäjään. Palvelun koekäyttöönoton yhteydessä oli ohjeistettu ryhmää tekemään kyselyjä vain sellaisilla valinnoilla, että tietoja ei tallenneta palveluun.

Keskusrikospoliisin näkemyksen mukaan asiassa on syytä korostaa, että testikäyttöjen kuvat ovat suurella todennäköisyydellä jo alkujaankin peräisin kolmannesta maasta, koska ne ovat olleet ladattuina internettiin ja palvelimet ovat mahdollisesti olleet kolmannessa maassa. Palveluntarjoaja on siten tullut tietoiseksi ainoastaan siitä, että haun tekijä on ollut jostain syystä kiinnostunut kyseisistä kuvista ja niiden löytymisestä internetistä.

Tulevat toimenpiteet

Poliisissa tullaan edelleen kiinnittämään erityistä huomiota yhtenäisten toimintatapojen ja välineiden kehittämiseen, jotta vastaavilta tapauksilta vältyttäisiin.

Poliisilla on käytössä tietojärjestelmien ja uusien palveluiden käyttöönottoprosessi. Poliisihallitus pyrkii varmistamaan, että läpi poliisihallinnon on riittävä tietoisuus tämän

prosessin mukaisista toimintatavoista ottamalla tämän asian esille mm. valtakunnallisessa poliisin tietosuojaverkostossa. Näin on toimittu myös keskusrikospoliisissa, jossa tietosuojan vastuuhenkilö nimitettiin viraston kehittämisryhmän jäseneksi, jotta tietosuojaa koskevat kysymykset huomioitaisiin heti kehittämistoimien alkuvaiheessa. Lisäksi keskusrikospoliisissa on asian sisäisessä käsittelyssä korostettu, että henkilötietojen käsittelyssä vastaavissa tilanteissa on varmistuttava tietosuojalainsäädännön noudattamisesta.

Osana muun muassa edellä mainittua käyttöönottoprosessia on myös tietosuojavaikutusten arviointiprosessi, jota parhaillaan entisestään kehitetään poliisissa. Vaikutustenarviointiprosessista pyritään saamaan niin kattava ja niin tunnettu prosessi läpi poliisin, ettei henkilötietojen käsittelyä käynnistetä ilman, että on vähintäänkin arvioitu tarve tietosuojavaikutusten arvioinnille.

Poliisihallitus on parhaillaan kehittämässä myös tiedonhallinnan seuranta- ja valvontatoimintaa, jonka yhtenä tavoitteena on osaltaan varmistaa, että henkilötietoja käsitellään vain sallituilla tavoilla.

Tapauksen johdosta Poliisihallitus päivittää vielä kasvojentunnistusjärjestelmää koskevan ohjeistuksensa ja koulutusmateriaalin. Poliisihallituksessa on valmistelussa myös Luotettavan tekoälyn periaatteet poliisille, jossa tultaneen korostamaan muun lisäksi juuri perusoikeuksien, kuten yksityisyyden suojan ja yhdenvertaisuuden, merkitystä ja lainsäädännön vaatimusten mukaisuuden varmistamista lähdettäessä ottamaan käyttöön ratkaisuja, joissa tekoälyavusteisuutta hyödynnetään toiminnan tukena.

Yhteydenotto rekisteröityihin

Rekisterinpitäjä on arvioinut rikosasioiden tietosuojalain 35 §:n edellyttämällä tavalla velvollisuutta ilmoittaa tapahtuneesta tietoturvaloukkauksesta rekisteröidyille. Tämänhetkisten tietojen mukaan tietoturvaloukkauksesta ei ole aiheutunut sellaista merkittävää riskiä rekisteröityjen oikeuksille, jotka edellyttäisivät henkilökohtaista ilmoittamista. Keskusrikospoliisi on julkaissut tiedotteen myös rekisteröityjen saataville.

Apulaistietosuojavaltuutetun toimenpiteet

Huomautus

Apulaistietosuojavaltuutettu antaa rekisterinpitäjälle rikosasioiden tietosuojalain 51 §:n 1 momentin 4 kohdan mukaisen huomautuksen, koska poliisi on käsitellyt henkilötietoja rikosasioiden tietosuojalain 4 ja 14 pykälien vastaisesti.

Rikosasioiden tietoasuojalain 14 §:n 1 momentin mukaan rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään lainmukaisesti. Sen on lisäksi kyettävä osoittamaan, että henkilötietoja on käsitelty lain 2 luvun mukaisesti. Rekisterinpitäjän on toteutettava tarvittavat 1 momentissa säädetyn vastuun edellyttämät tekniset ja organisatoriset toimenpiteet. Toimenpiteiden toteuttamisessa on otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin kohdistuvat riskit.

Täyttääkseen rikosasioiden 14 §:ssä säädetyt velvollisuudet, rekisterinpitäjän on huolehdittava koulutuksesta, joka liittyy uusien henkilötietojen käsittelytapojen suunnitte-

luun ja käyttöön. Rekisterinpitäjän on myös huolehdittava, että henkilötietojen käsittelyn osalta on voimassa olevat ajantasaiset ohjeet ja järjestettävä riittävä henkilötietojen käsittelyn valvonta. Rekisterinpitäjän velvollisuus on varmistua siitä, että poliisin työntekijät ovat tietoisia säännöksistä ja menettelytavoista, joita niiden on noudatettava toiminnassaan.

Rikosasioiden tietosuojalain 4 §:n 2 momentin mukaisesti henkilötietoja on käsiteltävä asianmukaisesti ja huolellisesti. Huolellisuuden vaatimus korostuu käsiteltäessä erityisiä henkilötietoryhmiä koskevia tietoja. Käyttäessään rikosasioiden tietosuojalain 11 §:n mukaan henkilön yksiselitteiseen tunnistamiseen tarkoitettujen biometristen tietojen käsittely on sallittu vain, jos se on välttämätöntä ja rekisteröidyn oikeuksien turvaamisen edellyttämät suojatoimet on toteutettu ja muut edellä mainitussa säännöksessä mainitut edellytykset täyttyvät.

Henkilötietojen käsittely on tapahtunut ilman rekisterinpitäjän hyväksyntää tai valvontaa. Poliisin työntekijät ovat käyttäneet Clearview AI- ja Arachnid-palveluja oman päätöksensä perusteella. Rekisterinpitäjä ei saadun selvityksen perusteella ole ollut tietoinen palvelujen käytöstä. Saadusta selvityksestä ei käy esille se, missä asemassa henkilötietojen käsittelyyn osallistuneet henkilöt ovat ja ovatko heidän esimiehensä olleet tietoisia toiminnasta.

Henkilötietojen käsittely on aloitettu hankkimatta tietoja siitä, miten kysymyksessä olevat palvelut käsittelevät henkilötietoja. Henkilötietojen käsittelyssä ei ole arvioitu tai toteutettu teknisiä tai organisatorisia toimenpiteitä, joita erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely olisi edellyttänyt, eikä selvitetty muun muassa sitä, kuinka kauan henkilötietoja säilytetään tai luovutetaanko niitä mahdollisesti kolmannen osapuolen käyttöön. Henkilötietojen käsittelyn välttämättömyys ja muut biometristen henkilötietojen käsittelyyn liittyvät edellytykset eivät ole täyttyneet.

Rekisterinpitäjän toimesta tapahtuva ohjaus, koulutus, sisäinen valvonta tai muut toimenpiteet eivät ole kyenneet estämään henkilötietojen lainvastaista käsittelyä. Edellä selostettu rekisterinpitäjän vastuu henkilötietojen käsittelystä ja henkilötietojen käsittelyn lainmukaisuusvaatimus eivät ole toteutuneet rikosasioiden tietosuojalain 4 ja 14 pykälissä tarkoitetulla tavalla.

Määräys

Apulaistietosuojavaltuutettu määrää rikosasioiden tietosuojalain 51 §:n 1 momentin 10 kohdanmukaisesti rekisterinpitäjän saattamaan käsittelytoimet rikosasioiden tietosuojalain mukaisiksi. Määräys on toteutettava siten, että rekisterinpitäjä 29.10.2021 mennessä pyytää Clearview AI- ja Arachnid-palvelujen ylläpitäjiä poistamaan poliisin näille palveluntarjoajille välittämät henkilötiedot.

Henkilötietojen käsittely on ollut lainvastaista. Koska henkilötietojen jääminen edellä mainittujen palveluntarjoajien haltuun aiheuttaa rekisteröidyille korkean riskin jäljempänä selostetulla tavalla, on rekisterinpitäjän pyrittävä siihen, että palveluntarjoajat poistavat poliisin heille välittämät tiedot tallennusalustoiltaan.

Ilmoittaminen rekisteröidyille

Apulaistietosuojavaltuutettu määrää rekisterinpitäjän rikosasioiden tietosuojalain 51 §:n 1 momentin 6 kohdan mukaisesti ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidyille. Ilmoituksessa on noudatettava rikosasioiden tietosuojalain 37 §:n säännöksiä. Ilmoitus on tehtävä niille rekisteröidyille, joiden henkilöllisyys on rekisterinpitäjän tiedossa.

Rikosasioiden tietousojalain 35 §:n 3 momentin mukaan rekisteröidylle ilmoittamista voidaan kuitenkin lykätä tai rajoittaa tai se voidaan jättää tekemättä, jos lain 28 §:n mukaiset edellytykset täyttyvät. Jos rikosasioiden tietosuojalain 35 §:n 3 momenttia sovelletaan, tulee siitä tehdä ilmoitus perusteluineen tietosuojavaltuutetun toimistolle.

Rekisterinpitäjä ei ole kyennyt yksilöimään kaikkia henkilöitä, joiden henkilötietoja on käsitelty. Tämä ei kuitenkaan tarkoita sitä, ettei ilmoitusvelvollisuus voisi koskea niitä henkilöitä, joiden henkilöllisyys on rekisterin pitäjän tiedossa.

Saadun selvityksen mukaan toiminnassa ei ole käytetty kuvia, mitkä sisältävät tietoa siitä, mikä asia on kyseessä tai kuka kuvassa esiintyy. Biometriset kasvokuvat kuitenkin rikosasioiden henkilötietolain 3 §:n 1 momentin 13 kohdan mukaisia biometrisiä henkilötietojatietoja, joista henkilö voidaan kasvojentunnistustekniikkaa hyväksikäyttäen tunnistaa.

Kun tietoturvaloukkauksen aiheuttamaa riskiä arvioidaan, tulee huomioida tietoturvaloukkauksesta mahdollisesti aiheutuvan seurauksen vakavuus ja todennäköisyys. Riski on sitä suurempi, mitä vakavampi seuraus on yksilön kannalta ja mitä todennäköisemmin se toteutuu. Silloin kun on kysymys poliisin toimesta tapahtuneesta biometristen henkilötietojen käsittelystä rikosasiain tietosuojalain vastaisesti, voidaan lähtökohtaisesti arvioida, että tietoturvaloukkauksesta on aiheutunut rekisteröidyille korkea riski. Kysymyksessä olevassa tapauksessa rekisterinpitäjällä ei ole tietoja siitä, millä tavalla kysymyksessä olevat palveluntarjoajat ovat käsitelleet henkilötietoja tai miten kauan niitä säilytetään tai mahdollisesti edelleen käsitellään. Tästä syystä rekisteröityjen biometrisiset henkilötiedot ovat joutunet rekisterinpitäjän määräysvallan ja valvonnan ulkopuolelle. Edellä mainitun perusteella henkilötietojen käsittelystä on aiheutunut rekisteröidyille merkittävä riski.

Asiassa on otettu huomioon se, että tällä hetkellä käytettävissä olevien tietojen perusteella tietoturvaloukkauksesta aiheutunut riski ei ole konkretisoitunut. Keskusrikospoliisi on aiemmin kerrotulla tavalla julkaissut tiedotteen myös rekisteröityjen saataville. Tästä syystä ilmoitusvelvollisuutta koskeva määräys on rajattu koskemaan vain niitä henkilöitä, joiden henkilöllisyys on rekisterinpitäjän tiedossa.

Muutoksenhaku

Tietosuojavaltuutetun päätökseen tyytymätön saa hakea siihen muutosta hallinto-oikeudelta kirjallisella valituksella, noudattaen mitä hallintolainkäyttölaissa (586/1996) säädetään. Valitus tehdä Helsingin hallinto-oikeuteen.

Tiedoksianto

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