Dnro 2206/171/20

16.2.2023

Tietosuojavaltuutetun päätös

Asia Tietoturvaloukkaus ja tietojen minimointi

Rekisterinpitäjä Majoituspalvelu Forenom Oy

Asian tausta

Rekisterinpitäjään kohdistui tietoturvaloukkaus perjantaina 13.3.2020. Hyökkäys kohdistui rekisterinpitäjän extranet-palveluun (asiakkaiden itsepalveluportaali) ja sen käyttämään rajapintaan toiminnanohjausjärjestelmään. Hyökkäys havaittiin perjantaina 13.3.2020 sen vielä käynnissä ollessa poikkeavien lokitietojen perusteella.

Rekisterinpitäjän henkilökunta tunnisti käytetyn haavoittuvuuden ja korjasi sen välittömästi havainnon tehtyään. Tällöin hyökkäys keskeytyi ja hyökkääjän pääsy järjestelmiin estyi. Lokitietojen perusteella oli todennettavissa, että hyökkäys oli alkanut noin 12 tuntia ennen haavoittuvuuden korjausta. Lokitietojen ja tutkinnan perusteella kyse oli erilaisten haavoittuvuuksien automatisoidusta etsimisestä ja erityyppisten SQL-injektioiden automatisoiduista kokeiluista, joista valtaosa ei mahdollistanut hyökkääjälle pääsyä, mutta joista yhdellä hyökkääjä pystyi hyödyntämään rajapinnan haavoittuvuutta.

Samana päivänä toteutetun ensimmäisen vaiheen tutkinnan ja siinä havaittujen menetelmien ja löydösten perusteella alustava arvio oli, että hyökkääjä ei ehtinyt päästä käsiksi tietokannan sisältämään dataan (henkilötiedot mukaan lukien) rajapinnan haavoittuvuuden kautta. Tutkintaa jatkettiin maanantaina 16.3.2020, jolloin havaittiin, että hyökkääjällä oli ollut pääsy tietokantaan.

Vaikka järjestelmän haavoittuvuus saatiin korjattua, oli hyökkääjä saanut henkilötietoja käsiinsä eikä ole tietoa, mitä hyökkääjä on saamillaan tiedoilla tehnyt. Tietomurron seurauksena hyökkääjä sai pääsyn noin 165 000 henkilötietotietueeseen, joista osa on päällekkäisiä ja koskee samoja rekisteröityjä.

Tietomurrosta tehtiin tietosuojavaltuutetun toimistoon 14 kantelua[1]. Kantelijat eivät ole asiassa hallintolain (434/2003) 11 §:n tarkoittamalla tavalla tässä asiassa asianosaisia, sillä se ei koske heidän etujaan, oikeuksiaan tai velvollisuuksiaan.

Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on 3.7.2020 päivätyllä kirjeellä pyytänyt selvitystä koskien rekisterinpitäjän järjestelmään kohdistunutta verkkohyökkäystä ja tätä koskevaa tietoturvaloukkausilmoitusta. Rekisterinpitäjä on toimittanut selvityksen 14.8.2020 ja vastannut tietosuojavaltuutetun toimiston kysymyksiin seuraavasti:

1. Mitä henkilötietoja Forenom kerää asiakkaistaan?

Forenom toimii majoituspalveluiden tuottajana ja on Pohjoismaiden johtava kalustettujen asuntojen tarjoaja. Forenom keskittyy tarjoamaan palveluita yritysasiakkaille, mutta asiakkaina on myös yksityishenkilöitä. Kerättävät henkilötiedot riippuvat siitä, mihin rekisteröityjen ryhmään

[1] 2338/163/20, 2372/163/20, 2401/163/20, 2402/163/20, 2411/171/20, 2492/182/20, 2648/163/20, 2776/171/20, 3051/154/20, 3187/163/20, 3292/153/20, 3636/154/20, 4871/153/20 ja 6457/182/20

henkilöt kuuluvat ja mitkä tiedot ovat välttämättömän tarpeellisia käsittelytarkoitusten toteuttamiseksi. Forenomilla on esimerkiksi vuokralaisten, yritysyhteyshenkilöiden sekä vuokranantajien henkilötietoja.

Majoitus-/vuokrasopimukset: palvelun toimittaminen ja laskutus: yhteystiedot, syntymäaika, kieli, rekisteröintitiedot (käyttäjätunnus ja muut mahdolliset rekisteröinnin yhteydessä kerättävät yksilöivät tunnukset), luottoluokitustieto (laskutus), kameravalvonta, lokitiedot, koodilukkojen käyttölokitiedot, puhelutaltiointi, pikaviestihistoria.

Forenomin verkkokauppa: yhteystiedot (osoite, puhelinnumero, sähköposti), rekisteröintitiedot (käyttäjätunnus ja muut mahdolliset rekisteröinnin yhteydessä kerättävät yksilöivät tunnukset), osto-/käyttäytymishistoriatiedot.

Asiakaspalvelu ja -viestintä: yhteystiedot, asiakassuhdetiedot (tiedot uutiskirjetilauksista tai asiakkaiden yhteydenottopyyntöihin liittyvät tiedot).

Analysointi, tilastointi sekä liiketoiminnan, tuotteiden ja palveluiden kehittäminen: tiedot ostokäyttäytymisestä, asiakaspalautetiedot.

Suoramarkkinointi ja markkinointikampanjat: yhteystiedot (osoite, sähköpostiosoite ja puhelinnumero), tiedot uutiskirjeen tilauksesta, ostohistoriatiedot (markkinointiviestien kohdennus).

Verkkosivuston käytön analysointi: evästeiden keräämät tiedot.

Pääsynhallinta: tiedot asunnon tilasta (varattu, vapaa) ja avainten saatavuudesta vieraiden poistuessa ja saapuessa.

2. Millä perusteella Forenom käsittelee henkilötietoja?

Alla olevaan taulukkoon on eritelty Forenomin käyttämät oikeusperusteet kunkin henkilötietojen käsittelytarkoituksen osalta. Samaan käsittelykokonaisuuteen saattaa sisältyä useampia eri oikeusperusteita, joiden perusteella käsittelyä suoritetaan, mutta olemme lisänneet sulkeisiin kuvauksen tilanteista, joihin kutakin oikeusperustetta sovelletaan.

Käsittelytarkoitus ja oikeusperuste:

Majoitus-/vuokrasopimukset, palvelun toimittaminen ja laskutus

- Sopimus (sopimukset, palvelun toimittaminen)

- Suostumus (luottoluokitustieto)

- Oikeutettu etu (asiakassuhteen hoitaminen, asiakaspalvelu, väärinkäytösten ja vikojen selvittäminen, kameravalvonta, lokitiedot, koodilukkojen käyttölokitiedot)

Forenomin verkkokauppa

- Sopimus

Asiakaspalvelu ja -viestintä

- Oikeutettu etu

Analysointi, tilastointi sekä liiketoiminnan, tuotteiden ja palveluiden kehittäminen

- Oikeutettu etu

Suoramarkkinointi ja markkinointikampanjat

- Oikeutettu etu (yritysasiakkaat)

- Suostumus (yksityisasiakkaat, uutiskirjeen tilaus)

Verkkosivuston käytön analysointi

- Suostumus

Pääsynhallinta

- Oikeutettu etu

3a. Kuinka kauan asiakkaiden henkilötietoja säilytetään rekisterissä?

Forenom on ennen tietosuoja-asetuksen voimanatuloa osana GDPR-projektiaan selvittänyt ja koonnut keräämänsä asiakastiedot sekä dokumentoineet tai määrittäneet puuttuvat henkilötietojen säilytysajat. Asiakkaita koskevien henkilötietojen pääsääntöiset säilytysajat on määritelty seuraavasti:

Vuokranantaja ja vuokralaistiedot: 10 vuotta vuokrasuhteen tai sopimuksen päättymisestä
CRM-tiedot: 5 vuotta viimeisestä aktiviteetista
Laskutukseen liittyvät tiedot: kirjanpitolainsäädännön mukaisesti (6 vuotta + kuluva vuosi)

Maaliskuussa 2020 tapahtuneen tietoturvaloukkauksen sekä siitä seuranneiden asiakaskyselyiden johdosta liittyen tietojen säilytysaikoihin, Forenom on kevään ja kesän aikana ottanut tehdyn tietoinventaarion ja tähän liittyneet henkilötietojen säilytysajat uudelleen tarkasteltaviksi sekä arvioi parhaimmillaan, onko tarvetta muuttaa säilytysaikoja kuitenkin siten, että liiketoiminta tai Forenomin lakisääteiset velvollisuudet eivät vaarannu.

3b. Mitä tiedoille tehdään säilytysajan päätyttyä?

Forenomin tai lainsäädännön määrittämän säilytysajan päätyttyä asiakastiedot joko poistetaan tai anonymisoidaan.

4a. Onko asiakkailla mahdollisuus poistaa omat tietonsa Forenomin asiakasrekisteristä?

Forenomin asiakkailla on mahdollisuus itse poistaa Forenom tilinsä (verkkokauppatunnukset) kirjautumalla sisään tiliinsä. Muiden poistopyyntöjen käsittelyyn Forenom on määritellyt vastuuhenkilöt sekä sisäisen prosessin, jonka perusteella rekisteröityjen henkilötietojen poistopyynnöt otetaan käsittelyyn. Forenomilla on lakisääteisiä velvollisuuksia tiettyjen henkilötietojen säilyttämiseksi (esimerkiksi matkustajailmoituksen tiedot), mutta lakisääteisen säilytysvelvollisuuden ulkopuoliset henkilötiedot poistetaan rekisteröidyn pyynnön perusteella Forenomin asiakasrekisteristä kuukauden kuluessa poistopyynnön vastaanottamisesta.

4b. Jos ei, niin miksi ei?

Forenomilla on rekisterinpitäjänä lakisääteisiä sekä liiketoimintaansa liittyviä velvollisuuksia tiettyjen asiakkaita koskevien henkilötietojen säilyttämiseen. Mikäli asiakkailla olisi mahdollisuus päästä poistamaan laajasti itseään koskevia tietoja, vaarantuisi Forenomin tietojen säilytysvelvoitteen toteutuminen. Forenom on arvioinut vaihtoehtoja ja tullut siihen tulokseen, että asiakkaille on annettu oikeus itsenäisesti hallinnoida verkkokauppatunnuksiaan, mutta majoitukseen ja vuokraustoimintaan sekä -sopimuksiin liittyvät tiedot tulee pyytää poistamaan Forenomin rekisteröityjen oikeuksien toteuttamisprosessin mukaisesti, jotta Forenom rekisterinpitäjänä voi arvioida tapauskohtaisesti, mitä tietoja on mahdollista poistaa.

5a. Kuinka kerätyt henkilötiedot on suojattu a) tietoja kerättäessä

Tiedot siirretään suojattua HTTP-yhteyttä käyttäen käyttäjältä palvelimillemme.

5b. Kuinka kerätyt henkilötiedot on suojattu b) säilytyksen ajan?

Tiedot säilytetään salatuissa tietokannoissa ja lokitiedostoissa, joihin pääsy on rajatulla määrällä henkilöitä.

6. Muita asiaan vaikuttavia seikkoja?

Tietoinventaarin päivitystyön johdosta myös Forenomin tietosuojaseloste on päivitettävänä ja sisäisesti hyväksytettävänä, eikä päivitettyä versiota ole ehditty toistaiseksi vielä julkaista. Päivitetty tietosuojaseloste löytyy tämän selvityspyynnön vastauksen liitteenä.

7. Mihin toimenpiteisiin tietomurtoa koskevassa asiassa on ryhdytty tai aiotaan ryhtyä?

Forenom on ottanut käyttöön lisäpalomuurikerroksen hyökkäyksiltä suojautumiseksi, rajannut järjestelmiin pääsyn tiettyihin maantieteellisiin sijainteihin, suorittanut turvallisuusauditoinnin järjestelmän lähdekoodille, ja ottanut käyttöön salauksen myös vähemmän merkityksellisille tiedoille.

Organisaationa Forenom on sitoutunut säännöllisiin kolmannen osapuolen suorittamiin tietoturva-auditointeihin Forenomin järjestelmiin.

Koko henkilöstö osallistuu pakolliseen verkkokoulutukseen henkilötietojen käsittelystä ja tietoturvasta. Niille rooleille ja tiimeille, jotka tarvitsevat syvempää osaamista (esimerkiksi myynti, asiakaspalvelu ja teknologiatiimi) otetaan käyttöön erilliset koulutusmateriaalit.

Rekisterinpitäjän kuuleminen

Rekisterinpitäjälle on annettu 16.4.2021 lähetetyllä kuulemispyynnöllä mahdollisuus lausua asiaa koskevasta alustavasta arviosta ja kuulemispyynnössä esitetyistä tosisekoista. Lisäksi tietosuojavaltuutetun toimisto on varannut rekisterinpitäjälle tilaisuuden tulla kuulluksi asiassa mahdollisesti määrättävästä seuraamuksesta. Rekisterinpitäjä on 18.5.2021 toimittamassaan vastauksessaan kertonut muun muassa seuraavaa:

[- -]

Todennettavissa oli, että osa hyökkääjän tekemistä tietokantakyselyistä oli palauttanut tietoja kannasta alla eriteltyjen rekisteröityjen ryhmien osalta seuraavasti:

• Asiakastiedot, 60 569 kpl

- nimi, osoite, postinumero, kaupunki, maa, sähköpostiosoite, puhelinnumero, kieli, tilinumero

- 24 315 rekisteröidyn osalta henkilötunnus

• Yritysasiakkaiden yhteyshenkilöt ja yritysten tiedot, 5 707 kpl

- arvonlisäverotunniste, yrityksen nimi, osoite, postinumero, kaupunki, maa, kieli,

puhelinnumero, sähköpostiosoite, luoton raja ja tieto Forenomin asiakasvastaavasta

• Forenomin ERP:n käyttäjien tiedot, 1 800 kpl

- nimi, sähköpostiosoite, puhelinnumero, kieli, salattu ja suolattu salasana, maa ja tiimi

• Kaupunkien/kuntien yhteyshenkilöiden tiedot, 1 383 kpl

- nimi, titteli, puhelinnumero, sähköpostiosoite

• Verkkokaupan käyttäjät, 96 196 kpl

- sähköpostiosoite, salattu ja suolattu salasana sekä joiltakin nimi, puhelinnumero ja viittaus asiakastietoihin

Tietosuojavaltuutetun toimiston kuulemispyynnössä todetaan, että "tietoturvaloukkauksen seurauksena noin 165 000 asiakkaan nimi, syntymäaika, henkilötunnus sekä yhteystiedot päätyivät ulkopuoliselle taholle". Tältä osin Forenom haluaa täsmentää, että edellä mainitut lukumäärät kuvaavat kuhunkin ryhmään kuuluvien rekisteröityjen määrää, ja ryhmissä on päällekkäisyyksiä. Sama rekisteröity voi kuulua useampaan ryhmään: esimerkiksi verkkokaupan käyttäjissä on henkilöitä, joiden tiedot ovat myös asiakastiedoissa. Tästä johtuen todellinen rekisteröityjen määrä on edellä mainittujen yhteenlaskettua määrää (165 655) pienempi. Myös henkilötietoryhmät vaihtelevat rekisteröityjen ryhmien mukaan. Tietoturvaloukkaus koski henkilötunnusten osalta 24 315 rekisteröityä.

Rekisterinpitäjä kertoo ryhtyneensä tietoturvaloukkauksen jälkeen toimenpiteisiin parantaakseen järjestelmiensä tietoturvaa sekä henkilöstönsä tietosuojaosaamista. Rekisterinpitäjä kertoo teettäneensä lokakuussa 2020 ulkopuolisella asiantuntijalla tietoturvatestauksen, joka sisälsi järjestelmien penetraatiotestauksen. Ulkopuolisen asiantuntijan arvio oli, että järjestelmistä ei löytynyt julkisesta verkosta hyödynnettävissä olevia haavoittuvuuksia ja testattavat kohteet ovat hyökkääjille vaikeita kohteita tehokkaan hyökkäysten torjunnan johdosta.

Rekisterinpitäjä on kommentoinut esittelijän alustavaa arviota muun muassa seuraavasti:

[- -]

Aiemman projektin yhteydessä vuokranantajien ja majoittujien tietojen säilytysajaksi on määritelty 10 vuotta sopimuksen päättymisestä. Tiedot ovat yhteys- ja tunnistetietoja (nimi, yhteystiedot, henkilötunnus, tilinumero). Forenom toteaa lisäksi, että hyökkääjällä ei ollut pääsyä majoittujatietoihin (majoittujien tiedot ja asiakkaiden tiedot ovat erillisiä, sillä majoittujana on aina yksittäinen henkilö, kun taas asiakkaana voi olla esimerkiksi henkilön työnantaja).

Kuulemispyynnön tosiseikastoa koskevassa osiossa (s. 5) tietosuojavaltuutetun toimisto toteaa, että rekisterinpitäjä ei ole osoittanut selkeää lakiin perustuvaa tarvetta säilyttää henkilötietoja 10 vuotta. Tältä osin Forenom toteaa, että lainsäädännössä erikseen määriteltyjen säilytysaikojen lisäksi säilytysaika voi perustua joko rinnakkain tai täydentävästi esimerkiksi liiketoiminnallisiin tarpeisiin. Näin on myös Forenomin osalta.

[- -]

Säilytysaikaa määriteltäessä säilytyksen rajoittamisen periaatteen käytännön sisältö oli osin täsmentymätön, ja Forenomin näkemyksen mukaan säilytettävien tietojen laatu, liiketoiminnalliset tarpeet, sopimusvelvoitteet sekä aiemmat kokemukset tarpeesta palata vanhoihin tietoihin huomioon ottaen 10 vuoden säilytysaikaa voitiin pitää perusteltuna. Säilytysajan määrittelyssä on otettu huomioon myös esimerkiksi vahingonkorvauslain mukaisen korvausoikeuden vanhentuminen. Forenom toteaa, että vanhoihin tietoihin on jouduttu palaamaan esimerkiksi vuokrasuhteiden päätyttyä riitatilanteiden selvittelyissä tuomioistuimessa tilanteissa, joissa vuokranantaja on vaatinut korvausta asunnon kunnon perusteella. Tällöin on ollut välttämätöntä palata asunnossa majoittuneiden henkilöiden tietoihin ja esimerkiksi selvittää heidän havaintojaan asunnon kunnosta vuokrasuhteen aikana (Forenom vuokraa asunnon sen

omistajalta ja luovuttaa sen asiakkaan käyttöön, ja majoittujat voivat olla esimerkiksi asiakkaan työntekijöitä).

Forenom on sittemmin täsmentänyt ja rajannut säilytysaikoja tietokohtaisesti tarkemmalla tasolla 14.8.2020 tietosuojavaltuutetun toimistolle toimitetussa vastauksessa viitatun uudelleentarkastelun myötä.

Tietojen minimoinnin periaatteen osalta kuulemispyynnössä ei ole eritelty, miltä osin tietosuojavaltuutetun toimisto katsoo, että käsiteltävät tiedot eivät ole asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista käsittelyn tarkoituksiin nähden. Forenomin näkemyksen mukaan sopimuksiin liittyvät tiedot ovat tarpeellisia käsittelyn tarkoituksiin (asuntojen vuokraaminen, majoituspalveluiden tarjoaminen, lakisääteisten velvoitteiden ja sopimusvelvoitteiden noudattaminen) nähden.

Tietosuoja-asetuksen 25 artiklan 2 kohdassa säädetyltä osin Forenom toteaa, että käsiteltävänä olevan henkilötietojen tietoturvaloukkauksen taustalla ei ole kuulemispyynnössä kuvatulla tavalla henkilötietojen oletusarvoinen saattaminen rajoittamattoman henkilömäärän saataville. Rekisterinpitäjän mukaan:

Hyökkääjä on saanut pääsyn henkilötietoihin tietomurrolla (ts. rikollisella toiminnalla) yksittäisen rajapinnan haavoittuvuutta hyödyntämällä. Tiedot eivät toisin sanoen ole olleet vapaasti saatavilla, vaan niihin pääsy on tapahtunut tietomurron seurauksena. Hyökkäysvektorina käytetty rajapinta on tietoturvaloukkauksen kuvauksen yhteydessä käsitellyllä tavalla liittynyt Forenomin asiakkaiden käyttämään ja tämän vuoksi myös julkiseen verkkoon auki olevaan extranet-palveluun.

Henkilötiedot ovat hyökkäyksen myötä päätyneet yksittäisen hyökkääjän saataville. Forenomilla ei ole tietoa, että myöskään hyökkääjä olisi julkaissut tietoja rajoittamattoman henkilömäärän saataville. Näin ollen Forenom katsoo, että Forenom ei ole saattanut henkilötietoja tietosuoja-asetuksen 25 artiklan 2 kohdassa tarkoitetulla tavalla rajoittamattoman henkilömäärän saataville. Estääkseen kyseessä olevien tietojen päätymisen rajoittamattoman henkilömäärän saataville Forenom oli ennen tietoturvaloukkausta toteuttanut teknisiä ja organisatorisia toimenpiteitä järjestelmien ja niiden sisältämien tietojen suojaamiseksi.

Yleisessä tietosuoja-asetuksessa 32 artiklan 1 kohdan d alakohdassa ja 2 kohdassa säädettyn osalta Forenom toteaa, että nyt käsiteltävänä olevan tietoturvaloukkauksen aiheuttanut hyökkäys kohdistui Forenomin extranetiin (ts. Forenomin asiakkaille tarkoitettuun itsepalveluportaaliin) ja siihen liittyvään rajapintaan toiminnanohjausjärjestelmään. Rekisterinpitäjän mukaan:

Extranetiä käyttävät Forenomin asiakkaat, minkä vuoksi extranetin on välttämätöntä olla avoinna myös julkiseen internetiin. Toiminnanohjausjärjestelmään on myös muita julkisia rajapintoja esimerkiksi ulkopuolisiin palveluihin (mm. Oikotie). Järjestelmän muissa rajapinnoissa on syötteentarkistus SQL-injektioiden estämiseksi, mutta hyökkäyksessä käytetystä rajapinnasta syötteentarkistus oli jäänyt aiemman virheen vuoksi pois, mikä sai aikaan haavoittuvuuden.

Forenom on ennen nyt käsiteltävänä olevaa tietoturvaloukkausta toteuttanut useita teknisiä ja organisatorisia toimenpiteitä tietoturvan varmistamiseksi. Sovelluskehityksessä noudatetaan Forenomin sovelluskehitysprosessia ja Forenomin sisäänrakennetun ja oletusarvoisen tietosuojan politiikkaa (Privacy by Design Policy). Teknisissä suojatoimissa hyödynnetään Forenomin omien toimenpiteiden lisäksi Amazon Web Services (AWS) -alustan tarjoamia palveluita. Forenom on tietoturvatoimenpiteiden osalta jo ennen tietoturvaloukkausta hyödyntänyt myös ulkopuolisia palveluntarjoajia, esimerkiksi lähdekoodille vuonna 2018 teetetyn ulkopuolisen auditoinnin osalta. Organisatoriset suojatoimet (esimerkiksi lokitietojen säännöllinen katselmointi) auttoivat havaitsemaan hyökkäyksen sen vielä ollessa käynnissä ja keskeyttämään hyökkäyksen.

Forenom toteaa lopuksi, että tietoturvaloukkauksen taustalla oli yksittäinen julkiseen verkkoon käyttötarkoituksensa vuoksi avoinna olleeseen extranet-palveluun liittyvä haavoittuva rajapinta. Forenom on ennen tietoturvaloukkauksen tapahtumista pyrkinyt toteuttamaan riittävät tekniset ja organisatoriset suojatoimet henkilötietojen suojaamiseksi. Forenom on myös pyrkinyt varmistumaan näiden toimenpiteiden riittävyydestä tietosuojavaltuutetun toimiston kuulemispyynnössä viitatun tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohdan mukaisesti esimerkiksi edellä mainitulla ulkoisen asiantuntijan koodianalyysillä sekä sisäisellä sovelluskehitysprosessiin liittyvällä lähdekoodin katselmoinnilla. Toteutetuista tietoturvatoimenpiteistä kertoo myös tietoturvaloukkauksen jälkeen toteutetun ulkopuolisen asiantuntijan tekemän tietoturvatarkastuksen lopputulos, jossa ei löydetty vastaavanlaisia tai muita julkiseen verkkoon avoinna olevia hyödynnettävissä olevia haavoittuvuuksia. Näin ollen Forenom katsoo toteuttaneensa tietosuoja-asetuksen 32 artiklassa tarkoitetulla tavalla asianmukaiset tekniset ja organisatoriset toimenpiteet tietojen suojaamiseksi.

Henkilötietojen tietoturvaloukkausta on edellä käsitelty pääasiassa tietosuoja-asetuksen 83 artiklan 2 kohdan d alakohdan ja teknisten ja organisatoristen toimenpiteiden näkökulmasta. Muiden 83 artiklan 2 kohdan huomioon otettavien seikkojen osalta Forenom toteaa seuraavaa.

Forenom havaitsi tietoturvaloukkauksen itse ja korjasi haavoittuvuuden välittömästi, millä pystyttiin rajoittamaan tietoturvaloukkauksen laajuutta. Forenom ilmoitti tietoturvaloukkauksesta oma-aloitteisesti sekä tietosuojavaltuutetun toimistolle että rekisteröidyille ja on toiminut aktiivisesti yhteistyössä myös kyberturvallisuuskeskuksen ja poliisin kanssa hyökkäyksen tutkinnassa. Forenom on suunnannut tietoturvaloukkauksen jälkeiseen selvitys- ja tutkintatyöhön merkittävästi resursseja ja käynyt läpi koko ITinfrastruktuurin vastaavien ja muiden haavoittuvuuksien varalta edellä kuvatulla tavalla.

[--]

Asian rajat ylittävä luonne

Yleisessä tietosuoja-asetuksessa on säädetty sellaisten asioiden käsittelystä, jotka ovat yleisen tietosuoja-asetuksen 4 artiklan 23 kohdassa määritellyllä tavalla rajat ylittäviä. Tällaiset asiat on käsiteltävä yleisen tietosuoja-asetuksen 56 artiklassa ja VII luvussa säädetyllä tavalla.

Rekisterinpitäjältä pyydettiin 13.8.2020 selvitystä asian mahdollisesta rajat ylittävästä luonteesta. Rekisterinpitäjä toimitti lisäselvityksen 30.8.2020. Rekisterinpitäjä on antamassaan selvityksessä ilmoittanut, että se toimii rekisterinpitäjänä nyt kysymyksessä olevan henkilötietojen käsittelyn osalta. Rekisterinpitäjä toimii Suomessa, Ruotsissa, Tanskassa ja Norjassa. Rekisterinpitäjän mukaan tietoja käsitellään konsernin yhteisessä asiakastietojärjestelmässä. Rekisterinpitäjä toteaa, että päätoimipaikka on Suomessa ja Suomen toimipaikka tekee päätökset nyt käsillä olevasta henkilötietojen käsittelystä. Näin ollen tietosuojavaltuutetun toimisto on katsottu toimivaltaiseksi käsittelemään asia johtavana valvontaviranomaisena. Tietosuojavaltuutetun toimisto on käsitellyt asian yleisen tietosuoja-asetuksen 60 artiklassa säädetyn menettelyn mukaisesti yhteistyössä osallistuvien jäsenvaltioiden valvontaviranomaisten kanssa.

Tietosuojavaltuutetun toimisto on 29.10.2020 toimittanut yleisen tietosuoja-asetuksen 56 artiklan ja 60 artiklan 3 kohdan mukaisesti asiaa koskevat olennaiset tiedot muille valvontaviranomaisille. Irlannin, Puolan, Norjan, Liettuan, Espanjan, Latvian, Belgian, Bulgarian, Ranskan, Luxemburgin, Tanskan, Unkarin, Slovakian, Ruotsin, Saksan Baijerin osavaltion ja Italian tietosuojavalvontaviranomaiset ovat ilmoittaneet olevansa osallistuvia valvontaviranomaisia sillä perusteella, että kysymyksessä oleva henkilötietojen käsittely vaikuttaa tai voi vaikuttaa rekisteröityihin kyseisessä jäsenvaltiossa.

Asian käsittely yhteistyömenettelyssä

Apulaistietosuojavaltuutetun päätösluonnos toimitettiin osallistuville valvontaviranomaisille tiedoksi 24.8.2021 yleisen tietosuoja-asetuksen 60 artiklan 3 kohdan mukaisesti. Tietosuojavaltuutettu vastaanotti luonnokseen vastalauseen Puolan valvontaviranomaiselta sekä kommentit Tanskan, Unkarin ja Ranskan valvontaviranomaisilta.

Puolan valvontaviranomaisen näkemyksen mukaan tietosuojavaltuutetun toimiston päätösluonnosta tulisi täydentää. Puolan valvontaviranomaisen mukaan päätöksessä tulisi todeta tietosuoja-asetuksen 6 artiklan 1 alakohdan rikkomus. Puolan valvontaviranomainen myös katsoi, että tietosuojavaltuutetun tulisi antaa rekisterinpitäjälle huomautus tietosuoja-asetuksen 6 artiklan sekä 25 artiklan 2 kohdan rikkomisesta. Se seikka, että rikkomus on sittemmin korjattu, ei Puolan valvontaviranomaisen näkemyksen mukaan vaikuta asiaan. Puolan valvontaviranomaisen näkemyksen mukaan huomautus on tarpeellinen seuraamus estämään mahdolliset jatkossa tapahtuvat rikkomukset. Puolan valvontaviranomaisen mukaan seuraamusmaksun määrääminen huomautuksen lisäksi olisi oikeasuhtainen, tehokas ja varoittava seuraamus. Oikeasuhtaisen ja tehokkaan korjaavan toimenpiteen soveltamatta jättäminen voisi Puolan valvontaviranomaisen näkemyksen mukaan johtaa siihen, että rekisterinpitäjää ei ole riittävällä tavalla varoitettu rikkomasta tietosuoja-asetusta uudelleen.

Tanskan valvontaviranomainen on kehottanut täydentämään arviota koskien rekisterinpitäjän toteuttamien teknisten ja organisatoriset suojatoimenpiteiden riittävyyttä ennen tietoturvaloukkauksen tapahtumista. Unkarin valvontaviranomainen on todennut, että seuraamusmaksun määrääminen ei olisi suhteeton seuraamus päätöksessä todettuihin rikkomuksiin nähden. Ranskan valvontaviranomainen on kommentoinut hyväksyvänsä päätösehdotuksen.

Tietosuojavaltuutetun toimisto on 27.5.2022 antanut rekisterinpitäjälle mahdollisuuden lausua osallistuvien valvontaviranomaisten kommenteista ja vastalauseista. Tässä yhteydessä rekisterinpitäjä on jo aikaisemmin mainittujen seikkojen lisäksi tuonut esille tehneensä erilaisia parannuksia ja tehostuksia tietoturvaan.

Rekisterinpitäjän mukaan pitkään säilytysaikaan oli päädytty erityisesti vahingonkorvauslain mukaisen korvausoikeuden vanhentumisen perusteella. Rekisterinpitäjän mukaan sen liiketoiminnassa merkittävässä roolissa ovat pitkäaikaiset huoneistovuokraukset, joissa vahingonkorvaustapaukset voivat ilmetä huomattavan pitkän aikavälin jälkeen, erotuksena normaaliin hotellitoimintaan liittyvät vahinkotapaukset. Rekisterinpitäjän mukaan se on sittemmin, tietosuojavaltuutetun kannanoton huomioiden, määritellyt asiakastietojen säilytysajan pituudeksi toiminnanohjausjärjestelmään kirjanpitolain mukaisen vähimmäissäilytysajan ja ottanut tietoisen liiketoimintariskin itselleen liittyen vahingonkorvaustapauksiin, joita ei voida käsitellä tässä määräajassa.

Rekisterinpitäjän mukaan tietoturvaloukkaus kohdistui pääosin verkkopalvelussa aktiivisena olleisiin asiakkaisiin ja murron kohteena oli vähäisessä määrin henkilötietoja, joiden osalta kirjanpitolain mukainen säilytysaika oli umpeutunut. Rekisterinpitäjä katsoo, ettei tietomurron kohteena olevien rekisteröityjen määrä olisi ollut oleellisesti pienempi, vaikka käytössä olisi ollut nykyisten määrittelyjen mukaiset säilytysajat.

Rekisterinpitäjän mukaan se havaitsi tietoturvaloukkauksen itse ja korjasi haavoittuvuuden välittömästi, millä pystyttiin rajoittamaan tietoturvaloukkauksen laajuutta. Rekisterinpitäjän mukaan se ilmoitti tietoturvaloukkauksesta oma-aloitteisesti sekä tietosuojavaltuutetun toimistolle että rekisteröidyille ja on toiminut aktiivisesti yhteistyössä myös kyberturvallisuuskeskuksen ja poliisin kanssa hyökkäyksen tutkinnassa. Rekisterinpitäjän mukaan se on suunnannut tietoturvaloukkauksen jälkeiseen selvitys- ja tutkintatyöhön merkittävästi resursseja ja käynyt läpi koko IT-infrastruktuurin vastaavien ja muiden haavoittuvuuksien varalta tässä ja edellisessä vastineessa kuvatulla tavalla. Rekisterinpitäjä katsoo, että seuraamusmaksun määrääminen olisi suhteeton seuraamus todettuihin rikkomuksiin nähden.

Tietosuojavaltuutettu on ottanut Puolan valvontaviranomaisen esittämän vastalauseen osittain huomioon päätöksessään ja lisännyt päätökseen 25 artiklan 2 kohdan, 32 artiklan 1 kohdan d alakohdan ja 2 kohdan rikkomuksen johdosta annettavat huomautukset. Tanskan valvontaviranomaisen kommentin johdosta tietosuojavaltuutetun päätöksessä on täydennetty suojatoimia koskevaa arviointia ja todettu, että suojatoimet eivät olleet 25 artiklan 2 kohdan, 32 artiklan 1 kohdan d alakohdan ja 2 kohdan edellyttämällä tavalla riittäviä. Tietosuojavaltuutetun toimisto on toimittanut yleisen tietosuoja-asetuksen 60 artiklan 5 kohdan mukaisesti tarkistetun päätösehdotuksen osallistuville valvontaviranomaisille.

Kukaan osallistuvista valvontaviranomaisista ei ole toimittanut merkityksellistä ja perusteltua vastalausetta tietosuojavaltuutetun toimiston korjattuun päätösehdotukseen 15.2.2023 mennessä. Lopullinen päätös annetaan tiedoksi rekisterinpitäjälle, kanteluiden tekijöille sekä osallistuville valvontaviranomaisille.

Sovellettava lainsäädäntö

Euroopan parlamentin ja neuvoston yleistä tietosuoja-asetusta (EU) 2016/679 (tietosuoja-asetus) on sovellettu 25.5.2018 alkaen. Säädös on asetuksena jäsenvaltioissa välittömästi sovellettavaa oikeutta. Yleistä tietosuoja-asetusta täsmentää kansallinen tietosuojalaki (1050/2018), jota on sovellettu 1.1.2019 alkaen. Tietosuojalailla kumottiin aiemmin voimassa ollut henkilötietolaki (523/1999).

Kyseisessä tapauksessa sovelletaan yleistä tietosuoja-asetusta.

Oikeudelliset kysymykset

Tietosuojavaltuutettu arvioi ja ratkaisee asian yleisen tietosuoja-asetuksen (EU) 2016/679 pohjalta. Asiassa on ratkaistavana:

1) Onko rekisterinpitäjä noudattanut yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdassa säädettyä tietojen minimoinnin periaatetta ja e alakohdassa säädettyä säilytyksen rajoittamisen periaatetta säilyttäessään rekisteröityjen henkilötietoja 10 vuotta?

2) Onko rekisterinpitäjä noudattanut yleisen tietosuoja-asetuksen 25 artiklan 2 kohdassa säädettyä velvoitetta toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla on varmistettava etenkin se, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ja että henkilötietojen säilytysaikaa rajoitetaan?

3) Onko rekisterinpitäjä noudattanut yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohdassa ja 2 kohdassa säädettyjä asianmukaisen turvallisuustason arviointia ja testausta koskevia velvoitteita?

Jos henkilötietojen käsittely ei ole ollut edellä mainittujen säännösten mukaista, asiassa on ratkaistavana se, mikä seuraamus toiminnasta on rekisterinpitäjälle määrättävä.

Tietosuojavaltuutetun päätös

Tietosuojavaltuutettu katsoo päätöksessään seuraavaa:

1) Tietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ole noudattanut yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdassa säädettyä tietojen minimoinnin periaatetta eikä saman artiklan e alakohdassa säädettyä säilytyksen rajoittamisen periaatetta säilyttäessään rekisteröityjen henkilötietoja lähtökohtaisesti 10 vuoden ajan. Niin ikään tietosuojavaltuutettu katsoo, ettei rekisterinpitäjä ole noudattanut yleisen tietosuoja-

asetuksen 25 artiklan 2 kohdan mukaista velvoitetta toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla on varmistettava, että tietoja säilytetään vain tarpeellinen säilytysaika.

2) Tietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ole kuvatun tietoturvaloukkauksen sattuessa noudattanut sille tietosuoja-asetuksen 25 artiklan 2 kohdassa säädettyä velvoitetta toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla on varmistettava etenkin se, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville.

3) Tietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ollut tietoturvaloukkauksen sattuessa noudattanut yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohdassa ja 2 kohdassa säädettyjä velvollisuuksia toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi.

Määräys

Tietosuojavaltuutettu antaa rekisterinpitäjälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d alakohdan mukaisen määräyksen arvioida käsittelemänsä henkilötietojen osalta mitkä henkilötiedot tulee säilyttää kirjanpitolaissa säädettyjen velvoitteiden noudattamiseksi. Siltä osin, kun tietoja ei tarvitse säilyttää kirjanpito- tai muiden lakisääteisten velvoitteiden noudattamiseksi, tietosuojavaltuutettu määrää rekisterinpitäjän lyhentämään käsittelemiensä henkilötietojen käsittelyaikaa.

Huomautus

Tietosuojavaltuutettu antaa rekisterinpitäjälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaisen huomautuksen. Tietosuojavaltuutettu huomauttaa, että rekisterinpitäjä ei ollut tietoturvaloukkauksen sattuessa noudattanut tietosuoja-asetuksen sisäänrakennettua ja oletusarvoista tietosuojaa koskevia velvoitteita (yleisen tietosuoja-asetuksen 25 artiklan 2 kohta), eikä henkilötietojen asianmukaista suojaamista koskevaa velvoitetta (yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohta ja 2 kohta).

Perustelut

Tietojen minimoinnin periaate

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdassa on säädetty tietojen minimoinnin periaatteesta. Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Käsiteltävien henkilötietojen on edellä mainitusti oltava määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia. Jo henkilötietolakia koskeneessa hallituksen esityksessä oli täsmennetty niin sanotun tarpeellisuusvaatimuksen sisältöä. Henkilötietoja voidaan pitää käsittelyn tarkoituksen kannalta tarpeellisina silloin, kun ne ovat asianmukaisia ja olennaisia, eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja mihin niitä myöhemmin käsitellään (HE 96/1998 vp, s.42). Yleisen tietosuoja-asetuksen johdanto-osan kappaleessa 39 on niin ikään todettu, että henkilötietojen olisi oltava riittäviä ja olennaisia ja rajoituttava siihen, mikä on välttämätöntä niiden käsittelyn tarkoitusten kannalta. Näin ollen voidaan todeta, että henkilötietoja saa käsitellä ainoastaan, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

Euroopan tietosuojaneuvosto on ohjeistanut minimointiperiaatteesta antamiensa suuntaviivojen yhteydessä[2]. Näiden ohjeiden mukaan ensin olisi selvitettävä, onko henkilötietojen käsittely ylipäänsä tarpeellista. Henkilötietojen käsittelyä kehotetaan nimenomaisesti välttämään silloin,

[2] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (annettu 13.11.2019).

kun se vain on mahdollista. Lisäksi erikseen on korostettu, että käsiteltävien henkilötietojen on oltava oleellisia kysymyksessä olevan käsittelyn tarkoituksen kannalta. Kaikkien käsiteltävien henkilötietojen olisi niin ikään oltava tarpeellisia erikseen määritellyn tarkoituksen saavuttamiseksi. Tietyn henkilötiedon käsittely olisi sallittua vain, jos käsittelyn tarkoitusta ei ole mahdollista saavuttaa muilla tavoin.[3] Käytännössä kussakin tilanteessa tulisi näin ollen kerätä mahdollisimman vähän henkilötietoja.

Säilytyksen rajoittamisen periaate

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa on säädetty henkilötietojen säilytyksen rajoittamisesta. Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Henkilötiedon säilytysajan on siis oltava mahdollisimman lyhyt. Yleisen tietosuoja-asetuksen johdanto-osan perustelukappaleen 39 mukaan henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin. Henkilötietoja ei näin ollen olisi säilytettävä pidempään kuin on tarpeen. Yleisen tietosuoja-asetuksen johdanto-osan perustelukappaleen 65 mukaan luonnollisella henkilöllä olisi puolestaan oltava oikeus ”tulla unohdetuksi”, jos tietojen säilyttäminen rikkoo tätä asetusta tai rekisterinpitäjään sovellettavaa unionin oikeutta tai jäsenvaltion lainsäädäntöä. Rekisteröidyllä olisi erityisesti oltava oikeus siihen, että hänen henkilötietonsa poistetaan ja ettei niitä käsitellä sen jälkeen, kun henkilötietoja ei enää tarvita niitä tarkoituksia varten, joita varten ne kerättiin tai jota varten niitä muutoin käsiteltiin, tai kun hän on vastustanut henkilötietojensa käsittelyä tai kun hänen henkilötietojensa käsittely ei muutoin ole tämän asetuksen säännösten mukaista.

Kyseisestä tapauksesta

Rekisterinpitäjä on todennut, että majoitus- ja vuokrasuhdetietoja säilytettiin kymmenen vuoden ajan vuokrasuhteen päättymisestä. Rekisterinpitäjä on perustellut säilytysajan pituutta mm. liiketoiminnallisella tarpeella; vanhoihin tietoihin on jouduttu palaamaan esimerkiksi vuokrasuhteiden päätyttyä riitatilanteiden selvittelyissä tuomioistuimessa tilanteissa, joissa vuokranantaja on vaatinut korvausta asunnon kunnon perusteella.

On kuitenkin ilmeistä, että esimerkiksi riitatilanteita aletaan pääsääntöisesti selvittää pian vuokrasuhteen päätyttyä ja tällöin kyseiseen tapaukseen liittyviä tietoja voidaan säilyttää tarvittaessa pidempi aika kuin riidattomiin asiakassuhteisiin liittyviä tietoja. Rekisterinpitäjä ei ollut esittänyt selkeää perustetta, miksi kaikkia asuntojen majoitus- ja vuokrasuhteeseen liittyviä henkilötietoja säilytettiin lähtökohtaisesti kymmenen vuoden ajan.

Rekisterinpitäjä on viimeisimmän kuulemisen yhteydessä todennut lyhentäneensä säilytysaikaa tietoturvaloukkauksen jälkeen. Rekisterinpitäjän mukaan se on määritellyt asiakastietojen säilytysajan pituudeksi toiminnanohjausjärjestelmään kirjanpitolain mukaisen vähimmäissäilytysajan ja ottanut tietoisen liiketoimintariskin itselleen liittyen vahingonkorvaustapauksiin, joita ei voida käsitellä tässä määräajassa.

Kirjanpitolain (1336/1997) 2 luvun 10 §:n 1 momentin mukaan tilinpäätös, toimintakertomus, kirjanpidot, tililuettelo sekä luettelo kirjanpidoista ja aineistoista on säilytettävä vähintään 10 vuotta tilikauden päättymisestä. Edelleen kirjanpitolain 2 luvun 10 §:n 2 momentin mukaan jollei muualla laissa ole säädetty pitempää määräaikaa säilyttämiselle, tilikauden tositteet, liiketapahtumia koskeva kirjeenvaihto sekä muu kuin 1 momentissa mainittu kirjanpitoaineisto on säilytettävä vähintään kuusi vuotta sen vuoden lopusta, jonka aikana tilikausi on päättynyt.

Kirjanpitolain 2 luvun 5 §:ssä on säädetty tositteesta. Tositteella tarkoitetaan päivättyä ja yksilöityä liiketapahtuman todentavaa kirjallista ilmaisua, kuten kuittia. Hallituksen esityksessä puolestaan on liiketapahtumia koskevan kirjeenvaihdon määrittelyn osalta viitattu

[3] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (annettu 13.11.2019), s. 19.

kirjanpitolautakunnan yleisohjeeseen 1.2.2011 kirjanpidon menetelmistä ja aineistoista, jonka kohdassa 4.2 on todettu, että liiketapahtumia koskevaa kirjeenvaihtoa ovat muut kirjanpitoaineistoon kuuluvat asiakirjat kuin tositteet. Tällaista aineistoa ovat esimerkiksi kirjanpidon perusteella tehdyt viranomaisilmoitukset (esimerkiksi veroilmoitukset) sekä eläkevakuutusta hoitaville yhteisöille tai muille yhteisöille annetut ilmoitukset ja muut lainsäädännön nojalla annettavat ilmoitukset (HE 89/2015 vp, s. 49).

Rekisterinpitäjä ei ole toimittanut tarkempaa selvitystä siitä, mitä majoitus- ja vuokrasuhdetietoja kirjanpitolain perusteella määritelty säilytysaika koskee. Edellä selostettuihin lainkohtiin perustuen on kuitenkin selvää, että kaikkia majoitus- ja vuokrasuhdetietoja ei voida katsoa kirjanpitolain 2 luvun 10 §:ssä tarkoitetuiksi tiedoiksi. [4] Rekisterinpitäjä ei ole esittänyt selkeää perustetta, miksi kaikille asuntojen majoitus- ja vuokrasuhteeseen liittyville henkilötiedoille on määritelty kirjanpitolakiin perustuva säilytysaika.

Edellä esitetyin perustein tietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ole tietojen säilyttämistä koskevissa käsittelytoimissaan noudattanut yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c ja e alakohdassa säädettyä.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksen 25 artiklan 2 kohdan mukaan rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Käsittelyn turvallisuus

Tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohdan 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, kuten
>
> [--]
>
> d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Tietosuoja-asetuksen 32 artiklan 2 kohdan mukaan 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.

Henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista. Rekisterinpitäjän on arvioitava mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä

[4] Ks. esimerkiksi apulaistietosuojavaltuutetun päätös dnro 4359/163/2018

henkilötietojen teknistä suojausta. Suojatoimien riittävyyttä on punnittava suhteessa olosuhteisiin ja riskeihin.

Suojatoimien tarkoituksena on varmistaa järjestelmien, palvelujen ja tietojen luottamuksellisuus, eheys ja saatavuus. Henkilötietoja suojataan luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta hävittämiseltä, tuhoutumiselta tai vahingoittumiselta. Tietoturvaloukkaukset voivat aiheuttaa vakavia riskejä rekisteröidyille, kuten identiteettivarkauden tai petoksen kohteeksi joutumisen. Henkilötietoja on suojattava kaikissa niihin kohdistuvissa käsittelytoiminnoissa sekä koko henkilötietojen käsittelyn elinkaaren ajan.

Rekisterinpitäjän on testattava suojatoimien toimivuutta säännöllisesti ja tehtävä tarvittavia parannuksia.

Kyseistä tapauksesta

Annetun selvityksen perusteella rekisterinpitäjä katsoo toteuttaneensa asianmukaiset tekniset ja organisatoriset toimenpiteet tietojen suojaamiseksi tietosuoja-asetuksen 32 artiklassa tarkoitetulla tavalla. Rekisterinpitäjän antaman selvityksen mukaan sillä oli ollut käytössään muun muassa seuraavia suojatoimia

- Tiedot siirretään suojattua HTTP-yhteyttä käyttäen käyttäjältä rekisterinpitäjän palvelimille.
- Tiedot säilytetään salatuissa tietokannoissa ja lokitiedostoissa, joihin pääsy on rajatulla määrällä henkilöitä.
- Teknisissä suojatoimissa hyödynnetään rekisterinpitäjän omien toimenpiteiden lisäksi Amazon Web Services (AWS) -alustan tarjoamia palveluita.
- Järjestelmän muissa rajapinnoissa on syötteentarkistus SQL-injektioiden estämiseksi (hyökkäyksessä käytetystä rajapinnasta syötteentarkistus oli jäänyt aiemman virheen vuoksi pois, mikä sai aikaan haavoittuvuuden).
- Rekisterinpitäjä noudattaa sovelluskehityksessään sovelluskehitysprosessia ja sisäänrakennetun ja oletusarvoisen tietosuojan politiikkaa (Privacy by Design Policy).
- Sovelluskehitysprosessiin kuuluu lähdekoodin katselmointi.
- Rekisterinpitäjä on ennen tietoturvaloukkausta hyödyntänyt ulkopuolisia asiantuntijoita, esimerkiksi lähdekoodille vuonna 2018 teetetyn ulkopuolisen auditoinnin osalta.

Rekisterinpitäjän mukaan se teetti tietoturvaloukkauksen jälkeen ulkopuolisella asiantuntijalla tietoturvatarkastuksen, jossa ei löydetty vastaavanlaisia tai muita julkiseen verkkoon avoinna olevia hyödynnettävissä olevia haavoittuvuuksia.

Tietoturvaloukkaus on toteutettu kyseisessä tapauksessa SQL-injektion avulla. SQL-injektio tarkoittaa käytössä olevan tietokantaympäristön sisältöön vaikuttamista mielivaltaisella komennolla, joka saadaan suorittumaan kohdejärjestelmässä. Hyökkäys voi onnistua esimerkiksi puuttuvan tai väärin toteutetun syöttötiedon tarkistuksen kautta, ja joissain tapauksissa myös itse tietokantarajapinnassa tapahtuvan tiedon väärästä käsittelystä. Tietomurrossa hyökkääjä oli suorittanut automaation avulla useita erilaisia komentoja, joista ainakin yksi on haavoittuvuutta hyödyntäen palauttanut hyökkääjälle yllä mainittuja henkilötietoja.

Koska SQL-injektiot ovat laajalti tiedostettu tietoturvariski, on tärkeää, että verkkopalveluiden ja tietokantapalvelinten ylläpitäjät suojautuvat niiltä asianmukaisin tietoturvatoimin[5]. SQL-injektioiden torjunnassa on huolehdittava ainakin siitä, että järjestelmää on testattu riittävästi, ja verkkoapplikaatioissa injektioita voi estää myös kattavin palomuuritoiminnoin. Koska tietomurron kohteena oleva järjestelmä on ns. extranet, eli asiakkaiden itsepalveluportaali, ei ole

[5]Esim. verkkopalveluiden kehitysyhteisö OWASP listaa injektiot yhdeksi kriittisimmistä riskeistä verkkoapplikaatioille. OWASP Top 10 edustaa laajaa yksimielisyyttä verkkosovellusten kriittisimmistä tietoturvariskeistä, ks. https://owasp.org/www-project-top-ten/ vierailtu 21.12.2022

tarkoituksenmukaista estää sen toimintaa julkisen internetin kautta; muutoin asiakkaat eivät voisi palvelua käyttää.

Rekisterinpitäjän mukaan lähdekoodi oli auditoitu vuonna 2018. Tietosuojavaltuutettu on ottanut huomioon, että auditoinnista oli tietoturvaloukkauksen tapahtuessa kulunut kaksi vuotta, eikä rekisterinpitäjä ole tuonut esille, että se olisi vuoden 2018 jälkeen suorittanut penetraatiotestausta tai auditointeja ennen tietoturvaloukkauksen tapahtumista.

Rekisterinpitäjä on todennut selvityksessään, että se on tietoturvaloukkauksen jälkeen teettänyt järjestelmilleen ulkopuolisella asiantuntijalla penetraatiotestauksen. Tässä testauksessa ei löytynyt julkisesta verkosta hyödynnettävissä olevia haavoittuvuuksia. Jos rekisterinpitäjä olisi tehnyt penetraatiotestauksen ennen tietoturvaloukkauksen tapahtumista, tietoturvaloukkauksessa hyödynnetty haavoittuvuus olisi voitu mahdollisesti havaita. Kuten edellä on todettu, SQL injektiot ovat yksi kriittisimmistä verkkoapplikaatioiden tietoturvariskeistä. Rekisterinpitäjä olisi voinut suorittaa säännöllisempää testausta haavoittuvuuksien havaitsemiseksi ja korjaamiseksi. Näin ollen tietosuojavaltuutettu katsoo, että rekisterinpitäjä ei ollut toteuttanut riittäviä toimenpiteitä riskiä vastaavan turvallisuustason varmistamiseksi yleisen tietosuoja-asetuksen 25 artiklan 2 kohdan, 32 artiklan 1 kohdan d alakohdan ja 32 artiklan 2 kohdan edellyttämällä tavalla.

Sovelletut lainkohdat

Perusteluissa 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 Helsingin hallinto-oikeuteen.

Valitusosoitus on liitteenä.

Tiedoksianto

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

Tietosuojavaltuutetun toimiston yhteystiedot

Postiosoite: PL 800, 00531 Helsinki

Sähköposti: tietosuoja@om.fi

Puhelinvaihde: 029 566 6700

Verkkosivut: www.tietosuoja.fi