Sam's Care Oy
Laadukasta kotihoitoa

Viimeksi päivitetty 04/03/2024

Tietosuojaohje

Käsitteet

Henkilörekisteri
Henkilörekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot on saatavilla tietyin perustein. Henkilörekisteri sisältää samaa käyttötarkoitusta varten henkilötietoja. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. esim. jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Henkilötieto
Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja: Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
Henkilötieto voi määritelmään mukaan olla esim. paikkatieto, joka kertoo jotakin tietystä henkilöstä; kuva, joka yhdistettynä esim. osoitetietoihin, IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään tai käyttäjätunnus.

Henkilötiedon käsittelijä
Henkilötietojen käsittelijä on se henkilö, viranomainen, virasto tai muu taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötiedon käsittely
Henkilötiedon käsittelyllä tarkoitetaan toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, esim. tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Rekisterinpitäjä
Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä on siis se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

Tietosuoja
Tietosuojalla tarkoitetaan kansalaisten yksityisyyden suojaamista sekä oikeuksien, etujen, vapauksien ja oikeusturvan turvaamista henkilötietoja käsiteltäessä.

Tietosuojavastaava
Henkilö, jonka tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Asema on itsenäinen ja riippumaton. Vastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle, joka on päävastuussa henkilötietojen käsittelyn lainmukaisuudesta.

Tietoturva
Tietoturvalla tarkoitetaan niitä teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen.

Käyttöoikeudet, vaitiolo- ja salassapitovelvollisuus

Henkilötietoja saavat käsitellä vain ne henkilöt, joilla on siihen tehtäviensä vuoksi oikeus. Yksiköiden esimiehet päättävät kenelle tietojärjestelmien käyttöoikeuksia annetaan. Käyttöoikeudet rajataan henkilön työtehtävien mukaisesti. Käyttöoikeuksia myöntäessä ja muuttaessa tulee jäädä merkintä (loki tai dokumentti), jolloin käyttöoikeuksia voidaan tarvittaessa selvittää myös jälkikäteen.

Mikä on henkilötietojen tietoturvaloukkaus?

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Tietosuojaloukkaus voi tapahtua esimerkiksi silloin, kun asiakkaiden henkilötietoja käsitellään tai jaetaan ilman asianmukaista suostumusta tai luvanvaraista käyttöä.

Tämä voisi olla esimerkiksi:

- Henkilötietojen väärinkäyttö: Henkilökunnan tai muiden tahojen väärinkäyttö voi johtaa henkilötietojen luvattomaan käyttöön, kuten asiakastietojen myyntiin tai jakeluun kolmansille osapuolille.

- Tietojen menetys tai varkaus: Kotihoidon asiakastietojen menetys tai varkaus voi tapahtua esimerkiksi silloin, kun paperitiedostoja hävitetään väärin tai kun tietoturvatoimia ei noudateta asianmukaisesti sähköisissä järjestelmissä.

- Luvattomat pääsytietoihin: Jos kotihoidon tietojärjestelmiin pääsee luvattomasti esimerkiksi heikon salasanasuojauksen tai tietoturva-aukkojen kautta, tämä voi johtaa tietojen luvattomaan käyttöön tai varkauteen.

- Virheellinen tietojen käsittely: Henkilötietojen virheellinen tallentaminen tai käsittely voi johtaa väärinkäsityksiin tai epätarkkoihin päätöksiin, mikä saattaa vaarantaa asiakkaiden turvallisuuden ja yksityisyyden.

Tietosuojaloukkaukset ovat vakava asia, ja yrityksemme pyrkii tulee varmistamaan, että meillä on pätevät ja asianmukaiset käytännöt ja tietoturvaratkaisut henkilötietojen suojaamiseksi. Lisäksi koulutamme henkilökuntaa tietosuojakäytäntöjen noudattamisessa ja reagoimme nopeasti ja asianmukaisesti, jos loukkauksia tapahtuu.

Ilmoitus viranomaiselle ja rekisteröidylle

Henkilötietojen tietoturvaloukkauksen sattuessa yrityksellä on velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista yrityksen tietosuojavastaavalle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan. Loukkausta koskeva ilmoitus tehdään valvontaviranomaiselle (tietosuojavaltuutetulle) mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Valvontaviranomaisena toimii tietosuojavaltuutetun toimisto.

Tietosuojavaltuutetun toimiston Ilmoitus tietoturvaloukkauksesta -lomake toimii Valtion tieto- ja viestintätekniikkakeskus Valtorin Turvalomake-palvelussa. Yrityksen

tietosuojavaltuutettu Samuel Tangoh täyttää lomakkeen ja lähettää suojatusti tietosuojavaltuutetun toimistoon.

Ilmoituksen lisäksi

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

Ilmoitukseen sisällytetään nämä tiedot:

- mitä on tapahtunut
- milloin tapahtunut
- millaista ryhmää tietoturvaloukkaus koskee
- millainen riski mahdollinen
- ehdotus haittojen lieventämiseksi
- selkeä kuvaus henkilötietojen tietoturvaloukkauksesta
- tietosuojavastaavan nimi ja yhteystiedot
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on jo toteuttanut; tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Tietosuojariskien arviointi

Rekisterinpitäjän eli yrityksen vastuu henkilötietojen tietoturvaloukkauksen tapahtuessa on suuri. Hänen on kyettävä arvioimaan muun muassa se millainen riski vuodosta aiheutuu rekisteröidylle. Tämän perusteella määräytyvät tehtävät jatkotoimet. Jos arvion tekeminen tuntuu vaikealta, otetaan yhteyttä tietosuojavaltuutetun toimistoon. Selvää on, että mitä arkaluonteisempaan tietoon loukkaus kohdistuu, sitä suurempi riski siitä aiheutuu rekisteröidylle.

Rekisterinpitäjän tulee arvioida loukkauksen kohteeksi joutuneiden henkilötietojen luonne, arkaluonteisuus ja määrä, ja pohdittava seurauksia. Ne voivat olla erilaisia riippuen siitä, mihin henkilötietoja on vuotanut: On eri asia, ovatko tiedot joutuneet esimerkiksi internetiin tai jos niitä ei päästä käsittelemään tietojärjestelmävian vuoksi.

Tärkeää on myös arvioida se, kuinka helposti henkilöt ovat tunnistettavissa tietosuojaloukkauksen kohteena olevasta materiaalista ja miettiä myös sitä, miten tätä materiaalia voidaan mahdollisesti käyttää hyväksi muiden saatavilla olevien tietojen kanssa.

Mitä tietoturva tarkoittaa

Tietoturvalla tarkoitetaan niitä käytännön toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen. Tietoturvatoimilla estetään tietojen luvaton käyttö ja haltuunotto. Tietoturvajärjestelyillä varmistetaan, että poikkeuksellisissakin olosuhteissa tietoaineistojen, tietojärjestelmien ja palveluiden saatavuus, eheys ja luottamuksellisuus säilyvät. Tiedot eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muidenkaan vahinkojen ja tapahtumien seurauksena. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin, kun niitä tarvitaan.

Sähköpostin ja verkon kautta leviävät haittaohjelmat eli virukset ovat vakava uhka tietoturvallisuudelle, koska ne voivat tuhota, varastaa ja välittää tiedostoja, tunnuksia ja salasanoja sekä hidastaa tietoverkon toimintaa. Kuitenkin myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat tietoturvallisuuteen. Suurimmat tietoturvallisuuden ongelmat liittyvätkin yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin.

Jokaisen työntekijän tulee omalla toiminnallaan varmistaa, ettei kukaan ulkopuolinen pääse tietoihin käsiksi.

Käytännön ohjeita tietoturvalliseen työhön

Salasanat

- Käytä palveluissa vahvoja salasanoja ja älä luovuta salasanaasi kenellekään toiselle.
- Vahva salasana on riittävän pitkä, vähintään kahdeksan merkkiä ja sen tulee sisältää isoja (A, B, C…) ja pieniä kirjaimia (a, b, c…), numeroita (0,1,2..) sekä mielellään erikoismerkkejä (näppäimistön symbolit). Erityisen vahva salasana sisältää 20–30 merkkiä, joka on joukko sanoja, joista muodostuu lause.
- Salasana ei saa sisältää käyttäjänimeäsi, oikeaa nimeäsi tai yrityksen nimeä.
- Älä käytä samaa salasanaa yrityksen ulkopuolisessa palvelussa.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.

Sähköpostin käyttö

Sähköposti on hyvä työväline yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa ei ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Yrityksen antama sähköpostiosoite on tarkoitettu käytettäväksi työasioissa.

Sähköpostiviestit liikkuvat verkossa yleensä salaamattomina ilman mitään suojausta, joten suojaamista edellyttäviä tietoja ja aineistoja ei saa lähettää sähköpostitse ilman suojausta.

- Sähköpostiviestit voivat sisältää haittaohjelmia tai linkkejä, jotka vievät haittaohjelmia sisältävälle sivustolle. Älä avaa epäilyttäviä sähköpostiviestejä, joiden alkuperästä et ole varma. Tarkista linkin kohdeosoite ennen klikkaamista.
- Varo kalasteluviestejä, joissa pyydetään tunnuksiasi ja salasanojasi, luottokortin numeroa tai muita henkilötietojasi. Ylläpitäjät missään yhteisössä eivät koskaan kysy salasanaasi, pankkitunnuksia tai luottokortin tietoja.
- Tarkista saamasi laskut huolella. Huijarit voivat yrittää hyödyntää esimerkiksi lomakautta, jolloin henkilöstöä yritetään saada maksamaan valheellisia maksuja kiireellisyyteen vedoten.
- Poista roskapostit, älä vastaa niihin. Roskapostia ovat mm. mainokset ja ketjukirjeet, jotka on lähetetty ilman vastaanottajan lupaa.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin. Vältä turhien sähköpostien lähettämistä. Ennen viestin lähettämistä varmista, että vastaanottaja (To:) ja mahdollisissa kopio (Cc:) sekä piilokopio (Bcc:) –kentissä olevat vastaanottajat ovat juuri ne henkilöt, joille tarkoituksesi on viesti lähettää.
- Älä kirjaudu yrityksen sähköpostiosoitteella sosiaalisen median palveluihin.

Toimintaohjeet ongelmatilanteiden varalle

Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

- Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista (esim. henkilötietojen vahingossa tapahtunut tai tahallinen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin) tietosuojavastaavalle ja esimiehelle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan.
- Ilmoita myös vakavat läheltä-piti-tilanteet tietosuojavastaavalle ja/tai esimiehellesi. Läheltäpiti-tilanteet tilastoimalla voidaan kehittää tietoturvaa.
- Mikäli hallussasi oleva laite tms. katoaa tai varastetaan, ilmoita siitä välittömästi esimiehelle ja tietosuojavastaavalle.
- Ilmoita aina haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi omalle esimiehellesi
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista esimiehellesi.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa

- Älä hätiköi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota kännykkäkameralla kuva. Kirjoita muistiin tekemisesi.
- Ota yhteyttä tietosuojavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

Lisätietoja kaikkiin tietosuojaa koskeviin asioihin voit tiedustella Sam’s care Oy:n tietosuojavastaavalta Samuel Tangoh p. 044 986 9221 tai sähköposti samuel.tangoh@samscare.fi