

Airiston Putkityö Oy

EU:n tietosuoja-asetuksen (EU 2016/943) mukainen

Seloste käsittelystä

Päivitetty 28.1.2019

1. Johdanto

EU:n tietosuoja-asetus 2016/679 (General Data Protection Regulation), myöhemmin ”tietosuoja-asetus” ja ”asetus”, parantaa luonnollisten henkilöiden yksityisyyttä ja oikeuksia omiin tietoihin. Samalla se lisää henkilötietoja käsittelevien tahojen velvoitteita. Asetus korvasi EU:n henkilötietodirektiivin 95/46/EY ja yhdenmukaisti henkilötietoja koskevan lainsäädännön EU:n jäsenmaissa ja ETA-alueella.

Asetuksen ”oletusarvoinen tietosuoja” (privacy by default) velvoittaa henkilötietoja käsittelevän yrityksen arvioimaan tietosuojaan ja tietoturvaan liittyvät käytäntönsä ja dokumentoimaan ne – Seloste käsittelystä. Asetus vaikuttaa yrityksen sisäisen toiminnan ohella yritystenvälisiin sopimuksiin.

Tämä Seloste käsittelystä korvaa aiemman version, ja kokoaa yhteen henkilötieto- ja tietoturvakäytännöt Airiston Putkityö Oy:ssä. Aineistoa täydennettiin ulkopuolisen asiantuntijan avulla. Päivitämme asiakirjaa, mikäli käytäntömme henkilötietojen käsittelyn osalta muuttuu tai lainsäädäntö sitä edellyttää. Pidämme myös yrityksemme kotisivuilla julkaistun Tietosuojaselosteen ja yhteistyösopimuksemme ajan tasalla.

Seloste käsittelystä on luottamuksellinen ja tarkoitettu tietosuojakäytäntöjen kehittämiseen Airiston Putkityö Oy:n sisällä (EU 2016/943 direktiivi, Rikoslaki 38 luku, Liikesalaisuuslaki 595/2018). Asiakirja täyttää osoitusvelvollisuuden valvontaviranomaisille (artikla 31 ja 41) ja on arviointiperusteena tulevalle, asetuksen mukaiselle tietosuojasertifiointille (artikla 42).

1.1 Lähtöarviointi

Alkuperäinen Seloste käsittelystä liitteineen perustui lähtöarviointiin (PIA – Privacy Impact Assessment), jossa huomioitiin Airiston Putkityö Oy:n toimiala sekä kumppani- ja sidosryhmien vaikutus henkilötietojen käsittelyyn. Kartoitimme mm. millaisia henkilötietoja yrityksessämme kerätään, mihin tarkoitukseen, kuka niitä käsittelee, millä tavalla ja millaisin valtuuksin. Otimme huomioon, että henkilötietojen minimointi, turvallinen käsittely ja läpinäkyvyys ovat tietosuoja-asetuksen keskeisiä vaatimuksia (artiklat 5-6 ja 12 sekä 25 ja 32).

Asetuksen toteutuminen tarkastettiin henkilöstömme, ohjelmistojen ja teknisten ratkaisujen osalta. Kartoituksen pohjalta paransimme yrityksen käytössä olevien laitteiden ja ohjelmistojen tietoturvaa, ja päivitimme sisäistä tietosuojaohjeistusta. Airiston Putkityö Oy:n johto varmistaa, että henkilöstö sitoutuu toimimaan ohjeiden mukaan. Lisäksi mietimme toimintamalleja sellaisen tilanteen varalle, että henkilötietoja päätyisi väärin käsiin inhimillisen tai teknisen virheen vuoksi (artikla 40).

1.2 Tietosuoja-asetuksen määritelmiä

”Henkilötiedoilla” tarkoitetaan mitä tahansa tietoa, kuten nimi, henkilötunnus, sähköpostiosoite muodossa etunimi.sukunimi@yritys.fi, sijaintitieto, verkkotunnistetieto ym., jotka voidaan yhdistää luonnolliseen henkilöön, ja jonka pohjalta henkilö voidaan suoraan tai epäsuorasti tunnistaa.

”Rekisteri” on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein.

”Rekisterinpitäjä” on luonnollinen henkilö, oikeushenkilö, viranomainen, jonka määräysvallassa rekisteri on.

”Käsittelijä” on luonnollinen henkilö, oikeushenkilö, viranomainen, joka käsittelee henkilötietoja Rekisterinpitäjän luvalla ja lukuun.

”Rekisteröity” on luonnollinen henkilö, jonka tietoja säilytetään rekisterissä ja käsitellään tiettyä tarkoitusta varten (artikla 4, kohdat 1-7).

2. Henkilötietojen käsittelyn lailliset periaatteet

Asetuksen nojalla henkilötietojen käsittelyn tulee olla lainmukaista, kohtuullista ja läpinäkyvää. Luonnollisista henkilöistä saa kerätä vain tarkoitukseen sopivia tietoja (artikla 5). Henkilötietojen käsittelyyn on oikeutettu etu, kun tietoja käytetään sopimusten tekoon, asiakassuhteiden ylläpitoon, markkinointiin tai perusteena on jokin muu, Rekisterinpitäjän tai kolmannen osapuolen, etu (artikla 6).

Airiston Putkityö Oy toimii B2B ja B2C sektorilla. Yksityisasiakkaiden osuus on 50 %. Henkilötietoja saamme nettilomakkeella ja puhelimitse. Näissä tapauksissa asiakkaat antavat tietonsa itse, eli henkilötietojen käsittely perustuu Rekisteröityjen suostumukseen. Käsittelemme henkilötietoja projektien läpiviemiseen sekä työ- ja liikesopimusten solmimiseen, joissa rekisteröity on osapuolena. Oikeutettuna etuna on asiakkuussuhteiden, yhteistyön, laskutuksen ja verotuksen kaltaisten velvoitteiden hoitaminen (artikla 6, kohdat 1a-1c). Lisäksi Airiston Putkityö Oy käsittelee henkilötietoja työnantajana.

Kummassakin tapauksessa Airiston Putkityö Oy toimii vastuullisena Rekisterinpitäjänä.

3. Rekistereiden muodot

Henkilörekisterit voivat sijaita fyysisesti toimistolla, palveluntarjoajan pilvipalvelussa, eri toimipaikoissa, toisessa maassa. Rekisteri voi olla digitaalinen, manuaalinen ja molemmissa muodoissa (artikla 4, kohta 6).

Airiston Putkityö Oy:ssä henkilötietoja sisältäviä aineistoja säilytetään yrityksen toimistossa, laitteissa ja ohjelmistoissa Paraisilla ja Kaarinassa. Molemmissa toimipaikoissamme käytämme samaa tuotannonohjausjärjestelmää asiakastietojen käsittelyyn. Toimintamme luonteesta johtuen osa asiakkaidemme ja kumppaniyritystemme edustajien henkilötietoja sisältävästä aineistosta on manuaalista. Myös työntekijöiden tietoja on sekä digitaalisessa että manuaalisessa muodossa.

3.1 Digitaaliset rekisterit

Xpaja

Airiston Putkityö Oy hyödyntää työnohjaukseen ja asiakkuushallintaan Xpaja-tietokantaohjelmistoa. Se on erityisesti talotekniikka- ja rakennusalan tuotannonohjaukseen suunniteltu, pilvipohjainen tietokantaohjelmisto

(SaaS), joka sisältää asiakasrekisterin osto- ja myyntireskontran muodossa sekä raportointityökaluja. Xpajaan on koottu suuri osa Airiston Putkityö Oy:n rekisteritiedoista.

Laskutuksemme on pääosin digitaalista (verkkolaskut) ja käytämme Xpajaa myös laskutukseen. Ohjelman käyttöoikeudet on rajattu useammalle tasolle henkilöstön tehtävien mukaan. Laajimmat käyttöoikeudet ovat toimitusjohtaja Mikko Kankareella ja projektipäällikkö Esa Jalosella.

Word, Outlook

Office-paketista käytämme eniten Word ja Outlook-ohjelmia. Office on sekä paikallisena (on-premises) että pilvipohjaisena (Office 365). Wordissa teemme tarjoukset ja sopimukset. Outlook -sähköpostiohjelmaan tallentuu henkilötietoja, hoidamme sillä asiakas- ja sidosryhmien välistä ja yrityksen sisäistä viestintää.

Mobiililaitteet: Outlook, tekstiviestiohjelmat

Työmme on liikkuvaa ja älypuhelimet tärkeimpiä viestintävälineitämme. Xpajan lisäksi käytämme älypuhelimilla Outlookia ja tekstiviestiohjelmia. Yrityksemme johdon, kuten toimitusjohtaja, työnjohtajat ja työpäälliköt, laitteisiin kertyy seuraavia henkilötietoja: etu ja sukunimi, puhelinnumero, sähköpostiosoite.

Joitakin asiakastietoja, kuten kumppaniyritysten puhelinnumeroita ja yhteyshenkilöiden nimiä tallentuu Airiston Putkityö Oy:n työntekijöiden puhelimiin ja toisinaan asiakas jättää viestin numerokohtaiseen vastaajaan. Jokainen puhelin on Airiston Putkityö Oy:n omistuksessa ja tietyn henkilön käytössä.

Puhelimiin liittyvät tietoturvaohjeet *9.1 Teknisten ja henkilöriskien vähentäminen – toimintaohjeet* alta.

Tarkemmat tiedot sähköisistä rekistereistämme ja niiden käyttöoikeuksista on koottu taulukkoon Ohjelmat ja Tietovarannot.

3.2 Manuaaliset rekisterit

Seuraavat Airiston Putkityö Oy:n manuaaliset aineistot sisältävät tai saattavat sisältää henkilötietoja:

- mapitetut tilaukset ja laskut
- projekteihin liittyvät kaavat, kuvat ja tekniset piirustukset, joissa on tekijän nimi

Henkilötietoja sisältävää manuaalista aineistoa kertyy väliaikaisesti Airiston Putkityö Oy:n Paraisten toimiston työpöydille. Kaarinan toimistolla käsittelemme digitaalisessa (tuotannonohjausjärjestelmä) rekisterissä olevia henkilötietoja. Henkilön nimen sisältävää manuaalista aineistoa (projekteihin liittyvät kuvat ja tekniset piirustukset) on projektien aikana mukana työmaalla.

4. Säännönmukaiset lähteet ja rekistereiden sisältö

Tietosuoja-asetukseen liittyy minimivaatimus – yritys voi asetuksen puitteissa kerätä ja käsitellä vain sen verran ja sellaisia henkilötietoja, joita toiminnassaan tarvitsee. Myös tietolähteet ja tietojenkeruumenetelmät tulee eritellä (artiklat 5–6 sekä johdannon kohdat 40–41, 44–50). Rekisteriä ylläpitävän tulee olla selvillä, mitä kautta ja millä tavalla henkilötiedot on saatu.

Airiston Putkityö Oy on sitoutunut asetuksen mukaiseen henkilötietojen minimointiin. Keräämme ainoastaan sellaisia tietoja, joita tarvitsemme sopimusten tekemiseen ja projektien läpiviemiseen. Jokainen työntekijämme kerää ja käsittelee henkilötietoja oman vastualueensa puitteissa. Päävastuu tietojen keräämisestä on toimitusjohtajalla, työnjohtajilla ja työpäälliköillä.

Suurin osa Airiston Putkityö Oy:n rekisterissä olevista henkilötiedoista on saatu asiakkailta itseltään tarjouspyyntöjen ja projektien yhteydessä tai kumppaneiden kautta. Yleisin henkilötietojen toimitustapa on puhelin. Suurin osa asiakastiedot tallennetaan sähköiseen rekisteriin (Xpaja).

Yrityksen kotisivut

Vuoden 2019 alussa Airiston Putkityö Oy:n sivusto uudistettiin – sivusto www.aptoy.fi sai SSL-suojauksen. Näin verkko-osoite ja lomakkeella lähetettävät henkilötiedot pysyvät turvassa. Lomaketiedot tallentuvat palveluntarjoajan sähköpostipalvelimelle, josta ne noudetaan yrityksemme paikalliseen sähköpostiin.

Tällä hetkellä yrityksemme sivuilla ei ole analytiikkaa eikä evästeitä. Sivut eivät kerää muita tietoja, kuin mitä lomakkeen kautta lähetetään. Kotisivujen lisäksi Airiston Putkityö Oy:llä ei ole muita verkkokanavia.

4.1 Asiakasrekisteri

Airiston Putkityö Oy:n henkilötietorekistereissä on kolmenlaisia henkilötietoryhmiä: asiakkaat ja sidosryhmät, kuten tavarantoimittajat, kumppanit, alihankkijat sekä työntekijät. Asiakkaista ja sidosryhmistä keräämme:

- yrityksen nimi
- yrityksen katuosoite, postinumero ja toimipaikka
- yhteyshenkilön etu- ja sukunimi
- yhteyshenkilön puhelinnumero
- yhteyshenkilön sähköpostiosoite (ei aina)
- toisinaan yhteyshenkilön henkilökohtainen matkapuhelinnumero
- yrityksen pankki- ja tilitiedot

Alihankkijoilta keräämme lisäksi:

- henkilötunnus
- veronumero

4.2 Työntekijärekisteri

Airiston Putkityö O:n työntekijärekisterissä olevat tiedot on saatu henkilöiltä itseltään työsuhteen alussa ja työsopimusten tekohetkellä. Työntekijärekisteriin, joka on henkilötietolomakkeen muodossa, kerätään:

- henkilön koko nimi
- syntymä-aika ja henkilötunnus
- lähiosoite, postinumero ja postitoimipaikka
- henkilökohtainen puhelinnumero
- henkilökohtainen sähköpostiosoite

- pankki ja tilinumero
- tiedot ammattiliittoon kuulumisesta

Työntekijärekisteri sisältää myös:

- työsopimukset ja työtehtävät
- tiedot työajasta (työtuntilistat) ja palkanmaksusta
- tiedot työsuhteen aikaisista koulutuksista ja sertifioinneista, kuten tulityö- ja työturvallisuuskortit, ja ensiapukurssit

5. Rekisterien suojausperiaatteet

Henkilötiedot kuuluvat tietosuojasetuksella oletusarvoisen suojauksen ja turvallisen käsittelyn piiriin. Tiedot tulee suojata luvattomalta käytöltä ja tämä on otettava huomioon tietojen käsittelyn kaikissa vaiheissa (artikla 32, johdannon kohta 83). Airiston Putkityö Oy:ssä henkilötietojen käyttö on rajattu tehtävien mukaan. Myös laitteiden ja yhteyksien tietoturvaan on panostettu.

5.1 Digitaalisten rekistereiden suojaus

Airiston Putkityö Oy:n digitaaliset rekisterit on suojattu asianmukaisesti. Käytämme sekä infratason että ohjelmallisia ratkaisuja:

- Osoitteenmuunnosta käytävä lähiverkko (NAT, Network Address Translation)
- päätelaitteissa laitekohtainen palomuri- ja virustorjuntaohjelmat
- palomuri-, virustorjunta- ja muiden ohjelmien automaattinen päivitys
- käyttöjärjestelmien automaattinen päivitys
- käyttöoikeudet rajattu, päätelaitteisiin kirjaututaan henkilökohtaisilla kirjautumistunnuksilla

Päätelaitteilla ajetaan virusskannaus joka päivä. Skannaus on ajoitettu käynnistyksen yhteyteen, joka viivyttaa laitteiden käyttöönottoa hieman, mutta on tehokkain pitämään ne turvallisina.

Kaikki Airiston Putkityö Oy:ssä käytettävät älypuhelimet on suojattu sormenjälki- tai iiristunnistuksella. Omia (BYOD) älypuhelimia ei työtehtävien yhteydessä käytetä. Henkilöstömme on sitoutunut siihen, ettei laitteiden sisältämiä tietoja päädy väärin käsiin. Ulkopuolinen IT-yritys tarkistaa säännöllisin väliajoin (auditointi), että Airiston Putkityö Oy:n lähiverkon ja laitteiden toiminnot ja suojaukset ovat ajanmukaisia.

Taulukosta Ohjelmat ja Tietovarannot löytyvät tietosuojakäytäntömme ohjelmisto- ja laitetyypeittäin.

5.2 Manuaalisten rekistereiden suojaus

Toimistomme työpöydille kertyy väliaikaisesti henkilötietoja sisältäviä aineistoja: laskuja, tilauksia, asiakaskortteja (työmääräin). Tietosuojasetuksen voimaantulon jälkeen olemme muuttaneet käytäntöämme: manuaalinen aineisto, joka voidaan digitoida, tallennetaan sähköiseen muotoon ja tuhoataan pysyvästi paperintuhoajalla. Säilytystä vaativa manuaalinen aineisto mapitetaan. Digitointi ei koske projekteihin liittyviä kuvia ja teknisiä piirustuksia, joita tarvitaan työvaiheiden hahmottamiseen.

Airiston Putkityö Oy:n manuaaliset aineistot on asianmukaisesti järjestetty ja mapitettu. Niitä säilytetään lukituissa, kulunvalvotuissa tiloissa. Manuaalista aineistoa varten on oma, lukittava kaappi.

5.3 Henkilötietojen käsittelyn valvonta Airiston Putkityö Oy:ssä

Jokainen henkilötietoja käsittelevä työntekijämme toimii yrityksessämme sovittujen ohjeiden mukaan. Yrityksessämme tapahtuvaa henkilötietojen käsittelyä valvotaan.

Toimistoissa olevien päätelaitteiden ja ohjelmistojen käyttöoikeudet on rajattu yrityksen johdolle tehtävien mukaan. Toimiston päätelaitteita käyttävät toimitusjohtaja (pääkäyttäjäoikeudet), työnjohtaja ja työpäällikkö, ja kukin näkee oman työhön liittyvät asiakirjat ja tiedostot. Sama pätee tiedostojen muokkaamiseen, muuttamiseen, tallentamiseen ja tuhoamiseen. Päätelaitteisiin kirjaudutaan henkilökohtaisilla salasanoilla. Salasanat ovat vähintään 12 merkkiä pitkiä ja niitä vaihdetaan 2-3 kertaa vuodessa

Laitteissa olevia tiedostoja tallennetaan toimistossa sijaitsevalle varmuuskopiointiasemalle. Varmuuskopiointiasema on salattu (7-Zip). Asiakirjoja tulostetaan verkkotulostuksella yrityksen sisäverkossa. Kun tulostettava aineisto kulkee yhden laitteen läpi, on helpompi seurata mitä milloinkin tulostetaan.

Airiston Putkityö Oy:n toimitusjohtaja valvoo henkilötietojen käsittelyä yrityksen kahdessa toimipaikassa, arvioi tietojenkäsittelyyn liittyvät käytännöt ja valtuudet, ja onko niitä tarvetta selkeyttää.

6. Henkilötietojen säännönmukainen luovutus

Rekisterinpitäjä, joka on kerännyt henkilötiedot ja jolla on määräysvalta niihin, voi luovuttaa tietoja toiselle tai kolmannelle osapuolelle esim. palvelun tai projektin toteuttamista vasten. Kun vastaanottajayritys tallentaa tiedot omiin järjestelmiin (puhelimet, ohjelmistot, pilvipalvelut, mukaan lukien manuaaliset asiakaskortit tai lomakkeet), vastaanottaja toimii henkilötietojen käsittelijänä tiedot luovuttaneen yrityksen (Rekisterinpitäjän) lukuun ja Rekisterinpitäjän kirjallisten ohjeiden mukaan (artiklat 4 ja 26–29).

6.1 Henkilötietojen luovutus Suomessa

Rekisterinpitäjänä Airiston Putkityö Oy:llä on oikeutettu etu luovuttaa, siirtää ja käsitellä henkilötietoja yrityksen sisällä, eri toimipaikkojen välillä. Siirto-oikeus koskee sekä asiakkaiden ja sidosryhmien että työntekijöiden henkilötietoja (artikla 4, kohta 19 ja johdanto, kohta 48). Siirto koskee yleensä tietoja, joita tarvitaan projektin, tai sen tietyn vaiheen toteuttamiseen.

Projektien yhteydessä Airiston Putkityö Oy asiakkaiden tai työntekijöiden tietoja, kuten nimi, puhelinnumero, sähköpostiosoite, sijainti, jaetaan tarvittaessa Outlookin ryhmäkalenterin kautta. Usein tietoja välitetään tekstiviesteillä. Projektien läpivieminen saattaa vaatia, että Airiston Putkityö Oy:n asiakkaiden henkilötietoja jaetaan lain puitteissa myös rahoitusyhtiöille (luotottaja), vakuutusyhtiöille ja verottajalle.

Tiedot Airiston Putkityö Oy:n työntekijöiden sopimuksista, tehtävistä, työajoista ja palkanmaksusta jaamme tilitoimistolle. Näiltä osin, samoin työntekijöiden verotietojen osalta, tilitoimisto toimii henkilötietojen

käsittelijänä Airiston Putkityö Oy lukuun, jolloin henkilötietojen käsittely tapahtuu antamamme kirjallisten ohjeiden mukaisesti (artiklat 28- 29).

6.2 Henkilötietojen luovutus EU:n ja ETA-alueen ulkopuolelle

Henkilötietojen siirrosta EU:n ja ETA-maiden ulkopuolelle säädetään asetuksen V luvussa (artiklat 44–48). Ennen kuin henkilötietoja siirretään EU:n / ETA:n ulkopuolelle, tulisi tarkistaa, ovatko palveluntarjoajan turvatoimet riittävät, ja sijaitsevatko palveluntarjoajan serverit EU:n hyväksymissä maissa. EU-komission on listannut Euroopan talousalueen ulkopuoliset, turvalliset maat, joiden joukossa ovat Norja, Sveitsi, Islanti, Kanada, Mansaaret, Färssaaret, Argentiina, Uruguay, Andorra ja Israel. Yhdysvaltoihin voi siirtää henkilötietoja vain sellaisten palveluntarjoajien puitteissa, jotka kuuluvat EU:n ja Yhdysvaltain välisen *Privacy Shield*-sopimuksen piiriin. Lista löytyy osoitteesta www.privacyshield.gov

Airiston Putkityö Oy:llä ei ole toimintaa Suomen ulkopuolella. Palveluntarjoajamme sijaitsevat Suomessa, joten meillä ei ole tarvetta luovuttaa tietoja EU:n ja ETA-maiden ulkopuolelle.

Monilla Suomessa toimivilla verkko-ohjelmistojen (Software as a Service, SaaS) ja pilvipalvelujen tarjoajilla kuitenkin on palvelimia eri puolilla maailmaa. Kumppani- ja alihankkijasopimuksissa Airiston Putkityö Oy on ottanut huomioon, että nämä saattavat omien palveluntarjoajiensa puitteissa siirtää ja säilyttää henkilötietoja EU:n ja ETA-alueen ulkopuolella.

7. Tietojen linkaari ja tuhoaminen

Tietosuoja-asetuksen minimointivaatimusten mukaan (artiklat 5, ja 13–14 sekä 25) tunnistettavassa muodossa olevia henkilötietoja saa säilyttää vain sen ajan, kuin työ- tai muun sopimuksen, palvelun tuottamisen tai lainsäädännön nojalla tarpeen.

Airiston Putkityö Oy:n on vuosia tehnyt yhteistyötä tiettyjen kumppaneiden kanssa. Säilytämme kumppaneiden tietoja sopimusten voimassaolon ajan, ellei kirjanpitolaki toisin sano.

Puolet asiakkaistamme on yksityishenkilöitä. Rekistereissämme olevia yksityishenkilöiden tietoja säilytämme kirjanpito- ja muiden lakien määräämän ajan. Tarpeettomat tiedot poistamme rekistereistämme oma-aloitteisesti.

Tilinpäätöksiä, tili- sekä kirjanpito- ja aineistoluetteloja säilytämme lain vaatimat 10 vuotta, tilikauden tositteita 6 vuotta. Myös yksityisasiakkaiden tietoja säilytämme Kirjanpitolain (1336/1997) puitteissa. Työntekijöiden henkilötietojen osalta noudatamme Työsopimuslakia (55/2001) ja Työaikalakia (605/1996). Työtodistuksia säilytämme 10 vuotta, tietoja työtunneista ja niistä maksetuista korvauksista 2 vuotta.

Henkilötietoja sisältävät sähköpostiviestit (tilaukset, tarjouspyynnöt ym.), joiden tietoja on jo toisissa rekistereissä, tuhoamme sähköpostiohjelmasta. Vanhentuneen digitaalisen aineiston poistamme kaikista rekistereistä, manuaalisen aineiston tuhoamme paperinsilppurilla.

8. Rekisteröidyn oikeudet

Tietosuoja-asetuksen 3 luku antaa rekisteröidyille Henkilötietolakia (523/99) laajemmat oikeudet, joihin kuuluvat oikeus tarkistaa, oikaista, siirtää, poistaa tai rajata itseään koskevien tietojen käyttöä sekä tehdä valitus valvontaviranomaisille. Henkilötietojen poistamiselle on kuitenkin oltava perusteet. Sama koskee mahdollista valitusta valvontaviranomaiselle (artiklat 12–22).

Puolet Airiston Putkityö Oy:n rekisterissä olevista henkilötiedoista on saatu yksityisasiakkailta. Kun tietojen käsittelyn perusteena on rekisteröidyn suostumus (on antanut tietonsa puhelimitse tai nettilomakkeen kautta), rekisteröidyllä on oikeus muun muassa:

- saada Rekisterinpitäjältä itsestään koskevat tiedot tarkastettavaksi
- saada tietoa henkilötietojensa käsittelyn tarkoituksista
- oikaista, eli korjata itseään koskevia tietoja
- rajoittaa tietojensa käyttämistä esim. suoramarkkinointiin
- poistaa tiedot, esim. yhteistyön tai sopimuksen päätyttyä
- siirtää tiedot järjestelmästä (yrityksestä) toiseen

Rekisteröidyn oikeudet omiin tietoihin ovat samoja, kun tietojen käsittelyn perusteena on sopimus (suostumukseen perustuva yhteistyö tai toimeksianto). Kun tietoja ei ole saatu Rekisteröidyltä itseltään, eli ne on kerätty julkisista lähteistä, yrityksen tulee informoida Rekisteröityjä rekisterin sisällöstä kuukauden kuluessa tietojen saamisesta (artiklat 12 -14).

Rekisteröidyn oikeudet on otettu Airiston Putkityö Oy toiminnassa huomioon. Henkilötietojen käsittely yrityksessämme perustuu sekä suostumukseen että oikeutettuun etuun. Asetuksen käytäntöjen noudattaminen on tiivistetty Airiston Putkityö Oy:n kotisivuilla julkaistussa Tietosuojaselosteessa.

8.1 Rekisteröidyn oikeuksien toteuttaminen

Rekisteröidyn niin pyytäessä, hänelle tulee toimittaa kaikki hänestä rekisterissä olevat tiedot (artikla 12).

Airiston Putkityö Oy:llä on henkilötietoja eri rekistereissä. Toteutamme rekisteröidyn oikeudet seuraavasti:

- Rekisteröity tekee kirjallisen pyynnön ja lähettää sen allekirjoitettuna Airiston Putkityö Oy:n rekisteriasioista vastaavalle henkilölle tai tuo paikan päälle yrityksemme Paraisten toimistoon.
- Rekisteristämme vastaava kokoa tiedot Exceliin, ja tallentaa ne rekisteröidyn toivomuksen mukaan CSV-Macintosh tai CSV-DOS muodossa.
- **Jos muissa rekistereissä olevat tiedot löytyvät kaikki Xpajasta, tiedot viedään sieltä CSV:nä**
- Tiedot luovutetaan pyynnön tehneelle Airiston Putkityö Oy:n toimistossa tai lähetetään liitteenä (CSV-tiedosto) sähköpostiin tai matkapuhelimeen. Rekisteriote voidaan luovuttaa myös tulosteena
- Ennen tietojen luovuttamista varmistamme pyynnön tehneen henkilöllisyyden

8.2 Suostumus tietojen käsittelyyn

Yritys- ja yhteisöasiakkaiden (rekisteröidyt) tiedot Airiston Putkityö Oy saa yleensä tarjouspyyntöjen kautta, projektien läpiviemiseksi, jolloin yritystä edustavan henkilön suostumus tietojensa käsittelyyn perustuu hänen kanssaan tekemämme sopimukseen (artikla 4, kohta 11).

8.3 Milloin on pyydettävä erillistä suostumusta

Airiston Putkityö Oy:n tulee pyytää erillinen suostumus henkilötietojen käsittelyyn (artiklat 13), mikäli henkilö antaa tiedot:

- a) liittyessään sähköpostilistalle yrityksen kotisivujen kautta*
- b) lähettäessään viestiä yrityksen kotisivujen lomakkeella
- c) messuilla, täyttäessään arvontalipukkeen

* Airiston Putkityö Oy:n kotisivuilta ei tällä hetkellä voi liittyä sähköpostilistalle

Se, että yksityinen tai yritystä edustava luonnollinen henkilö (rekisteröity) on vapaaehtoisesti antanut suostumuksensa tietojensa käsittelyyn, pitää pystyä osoittamaan (artiklat 4 ja 7 sekä johdannon kohdat 32–33 ja 42).

Suurimman osan yksityishenkilöiden (rekisteröidyt) tiedoista Airiston Putkityö Oy saa heiltä itseltään mm. tarjouskyselyjen yhteydessä puhelimitse. Jos puhelu ei johda kauppaan, eli jää vain tiedusteluksi, numero poistetaan eikä tietoja tallenneta.

Kun yhteydenotto tulee verkkolomakkeen tai sivuilla oleviin sähköpostiosoitteisiin Rekisteröity on lukenut Tietosuojaselosteen ja antanut suostumuksensa tietojen käsittelyyn (artikla 13).

Suostumusta pitää pyytää myös silloin, kun Airiston Putkityö Oy haluaa käyttää rekisterissään olevia henkilötietoja muuhun tarkoitukseen kuin mihin ne alun perin kerättiin. Lähetämme Rekisteröidyille suostumuspyynnön sähköpostitse ennen kuin tietojenkäsittely muuhun tarkoituksen alkaa (artikla 13, johdannon kohta 61).

Niissä tapauksissa, joissa henkilötietojen käsittely perustuu yksinomaan henkilön antamaan suostumukseen (lähetti tarjouspyynnön, mutta sopimusta ei syntynyt), poistamme tiedot rekistereistämme, mikäli henkilön niin toivoo.

Erillistä suostumusta ei tarvita, kun:

- a) Airiston Putkityön rekisteriin tallennetut tiedot on saatu julkisista lähteistä (yritysrekisterit, kotisivut)
- b) Airiston Putkityön rekisterissä jo oleville lähetetään joukkosähköpostia.*

* Joukkosähköpostin lopussa on linkki, jonka kautta Rekisteröity voi ilmoittaa halustaan poistua sähköpostilistalta (rekisteröidyn oikeudet).

9. Suunnitelma henkilötietojen käsittelyn turvaamiseksi (turvallisuuksuunnitelma)

Henkilötietojen käsittelyyn liittyy riskejä, jotka voivat johtua tietojen käsittelystä (henkilöstöriski), säilytyksestä sekä tietoturvan pettämisestä (tekniset riskit). Tietosuoja-asetuksen artikla 32 luettelee vähimmäiskeinot, joilla henkilötietojen luottamuksellisuus ja turvallinen käsittely tulisi varmistaa.

Henkilötietojen käsittely jakautuu Airiston Putkityö Oy:ssä usealle henkilölle ja tietojen käytön laajuus rajattu tehtävien perusteella. Jokainen henkilö käsittelee vain omaan vastuualueeseen kuuluvia tietoja, yrityksen tietosuojakäytäntöjen mukaan.

9.1 Teknisten ja henkilöriskien vähentäminen – toimintaohjeet

Useat henkilötietojen käsittelijät, liikkuva työ ja kaikkialla mukana seuraavat älypuhelimet kasvattavat tietoturvaloukkausten riskiä. Airiston Putkityö Oy ohjeistaa henkilöstöä, että aika ajoin:

- pyyhitään älypuhelimista soitettujen ja vastaanotettujen puhelujen historia
- pyyhitän numerokohtaisiin vastaajiin jätetyt ääniviestit
- pyyhitän tekstiviestihistoria
- yrityksen omistamiin älypuhelimiin on asennettu F-Securen VPN suojaamaan ja salamaan liikennettä
- yrityksen muihin, verkkoyhteyden mahdollistaviin päätelaitteisiin on asennettu VPN*

* Virtual Private Network (VPN) salaa laitteista lähtevän tietoliikenteen ja estää pääsyn haitallisille verkkosivuille. VPN-salaus toimii silloinkin kun älylaite käyttää mobiilidataa.

Muu laitteisiin liittyvä toiminta

Yrityksen hallussa olevat, ikääntyneet ja käytöstä poistuvat laitteet hävitämme asianmukaisesti. Näkyvät identiteettitiedot, kuten laitteen tilit, ja tiedostot poistetaan, yhteystiedot ja viestintä poistetaan, käytetyt ohjelmistot poistetaan ja laite toimitetaan alan asiantuntijalle tietojen lopullista tuhoamista varten. Mikäli edellinen ei onnistu (laite on rikki) laite toimitetaan alan asiantuntijalle, joka varmistaa tietojen asianmukaisen tuhoamisen.

9.2. Suunnitelma kriisitilanteen varalle

Teknisestä suojaustasosta huolimatta päätelaitteisiin voi tulla virus tai haittaohjelma esim. aidon näköisten sähköpostiviestien (kalastusvietit) vastaanotettujen Word-dokumenttien (erityisesti doc ja docx), jopa kuvien kylkiäisinä. Haitakkeet kehittyvät nopeasti eivätkä virustorjuntaohjelmat välttämättä tunnista niitä.

Laitteen saastumisen huomaa yleensä siitä, että ohjelmat eivät enää toimi normaalisti. Vika saattaa olla tekninen, mutta haittaohjelmaa on ensimmäiseksi epäiltävä, kun tiedostoja ”särky” eli osia asiakirjassa alun perin olleista tiedoista katoaa tai koko asiakirja katoaa, tiedosto monistautuu (kopiot) tai tiedoston nimi on muuttunut. Airiston Putkityö Oy:n ohjeistuksen mukaan:

- mahdollisesti saastunut laite kytkentään ulos lähiverkosta
- laite sammutetaan
- asiasta informoidaan yrityksen johtoa

- paikalle kutsutaan IT-asioista vastaavaa kumppani

Toisinaan käyttöjärjestelmän tai tietyn ohjelman automaattinen päivitys (Patch Management) aiheuttaa haittaohjelmalle ominaisia ongelmia. Tällaista on havaittu Windows 10 käyttöjärjestelmän ja Avast-virustorjuntaohjelman päivitysten jälkeen. Tiedostojen häviäminen, verkkoyhteyksien katkeaminen tai laitteen jumiutuminen (sininen ikkuna) voi siis johtua myös kaupallisten tahojen huolimattomuudesta.

Tietoturva on noussut asetuksen myötä erityisen tärkeäksi tekijäksi henkilötietojen suojaamisessa. Airiston Putkityö Oy:n henkilöstö voisi hyötyä sellaisesta koulutuksesta, jossa harjoitetaan tietoturvaan liittyvissä kriisitilanteissa toimimista.

10. Toimiminen tietoturvaloukkausten sattuessa

Jos henkilötiedot vaarantuvat teknisen tai ohjelmistollisen vian takia, Rekisterinpitäjän tulee toimia niin, että tiedot saadaan nopeasti palautettu ja niiden eheys (tiedot eivät ole miltään osin muuttuneet, tuhoutuneet tai joutuneet väärin käsiin) voidaan varmistaa (artikla 32).

Tietoturvaloukkausten teknisiä syitä voivat olla (niihin kuitenkin rajoittumatta):

- laitteen saastuminen (haittaohjelma)
- tunkeutuminen tietojärjestelmiin (hakkerointi)
- kyberhyökkäys käyttämämme (palveluntarjoajan) sähköpostipalvelimelle tai tuotannonohjausjärjestelmää ylläpitävälle palvelimelle tai käyttämämme pankin järjestelmiin

Henkilötietoihin kohdistuvan uhan ei tarvitse olla tekninen. Tietoturvaloukkaus on mikä tahansa henkilötietojen luottamuksellisuutta vaarantava tilanne, kuten:

- henkilötietoja sisältävän asiakirjan tai sopimuksen kadottaminen
- laskun, tiliotteen tai muun henkilötietoja sisältävän asiakirjan postitus väärälle henkilölle
- luottamuksellisia tietoja sisältävän sähköpostiviestin välittäminen väärälle henkilölle
- hävinnyt tai varastettu laite (kannettava tietokone, älypuhelin)
- hävinnyt tai varastettu tallennusväline (ulkoinen kiintolevy, muistitikku)
- murtautuminen yrityksen ajoneuvoon, jossa on henkilötietoja sisältävää aineistoa
- murtautuminen yrityksen toimipaikkaan
- tulipalo yrityksen toimipaikassa

Airiston Putkityö Oy on ottanut nämä riskit huomioon. Pyrimme minimoimaan henkilötietoihin kohdistuvia uhkia, ja varmistamme, että tietoturvariskien uhatessa vika saadaan nopeasti paikannettu ja korjattua.

10.1 Tietoturvaloukkausten dokumentointi

Henkilötietoihin kohdistuvien riksien arvioinnista ja menettelystä tietoturvaloukkausten sattuessa säädetään artiklassa 4 ja 33 sekä johdannon kohdissa 85–88. Asetuksen mukaan riskien arvioinnin ja niiden mukaisen menettelyn pitää perustua dokumentointiin. Tietosuoja-asetus velvoittaa myös Rekisterinpitäjää kirjaamaan ylös

kaikki tietoturvaloukkaukset, arvioimaan luonnollisille henkilöille mahdollisesti aiheutuvat riskit sekä kuvaamaan millaisiin toimenpiteisiin yritys asian tiimoilta ryhtyi tai ryhtyy. Valvontaviranomaiset voivat tällaisen dokumentoinnin pohjalta tarkistaa, että tietosuoja-asetusta on noudatettu (artikla 33, kohta 5).

Airiston Putkityö Oy:ssä on sitä varten käytössä Tietoturvaloukkaukset -taulukko.

10.2 Tietoturvaloukkauksiin liittyvä ohjeistus

Teknisestä tai ohjelmallisesta viasta tulee viipymättä ilmoittaa Airiston Putkityö Oy:n rekisteristä vastaavalle henkilölle ja yrityksen johdolle. Samoin tulee toimia, mikäli epäillään tietoturva-avaaloukkausta kohdassa 10. luetelluista syistä. Lisäksi tietoturvaloukkaus kirjataan Tietoturvaloukkaukset -taulukkoon, johon merkitään:

- paikka, päivämäärä ja kellonaika, jolloin tietoturvaloukkaus havaittiin
- kuka havaitsi (henkilön nimi)
- mitä tapahtui (riittävän seikkaperäinen kuvaus)
- tietoturvaloukkauksen tyyppi (inhimillinen virhe: asiakirjan tai laitteen katoaminen; tekninen virhe: laitevika; ulkopuolinen uhka: virus, murto yrityksen laitteisiin tai tiloihin.)
- riskiluokitus: 1. riski rekisteröidylle on korkea, 2. riski on pieni, 3. rekisteröidylle ei aiheudu riskiä

sekä riskiluokituksen peruste (millaiset henkilötiedot mahdollisesti vaarantuivat)

- vaikutuksenarviointi (arvio rekisteröidylle aiheutuvasta haitasta)
- keitä yrityksen sisällä informoitiin
- mitä yrityksen sisällä asian eteen tehtiin tai aiotaan tehdä (toimenpiteet)
- vaatiiko tapahtuman laatu rekisteröidylle ilmoittamista, ja tehdäänkö niin
- vaatiiko tapahtuman laatu viranomaisille ilmoittamista, ja tehdäänkö niin

Airiston Putkityö Oy:llä on ulkoistettu IT-sopimus. Vakavimmassa ongelmatilanteessa IT-yritys selvittää tietoturvaloukkauksen syyt ja laajuuden, tekee kirjallisen vaikutuksenarvioinnin rekisteröidylle mahdollisesti aiheutuvasta vahingosta ja neuvoo toimenpiteet.

10.3 Ilmoitusvelvollisuus rekisteröidylle

Rekisterinpitäjän on informoitava rekisteröityjä, mikäli heidän yksityisyytensä vaarantuu teknisen vian, inhimillisen virheen taikka tietomurron takia. Esim. tapauksessa, jossa henkilötietojen turvallista säilyttämistä ei pystytä takamaan tai on vaarana, että ne joutuvat / ovat joutuneet väärin käsiin (artiklat 33–34).

Ilmoitus pitää tehdä 72 tunnin sisällä. Aikaraja on sama riippumatta siitä, onko kyseessä pyhä tai vapaapäivä. Ilmoitus perustuu joko Airiston Putkityö Oy:n omaan riskiarvioon tai ulkopuolisen IT-asiantuntijan antamaan kirjalliseen lausuntoon.

Yrityksessämme on varauduttu siihen, että ilmoitus tehdään mahdollisimman pian yrityksen kotisivuilla (tiedote), sähköpostitse tai muulla luotettavalla tavalla niille henkilöille, joiden tiedot ovat vaarantuneet. Airiston Putkityö Oy:ssä ilmoituksen tekee rekisteristä vastaava henkilö.

Ilmoitusta rekisteröidylle ei vaadita (artikla 34), jos:

- a) tekninen vika on korjattu ja / tai haittaohjelma poistettu, vahingot havaittu sen verran pieniksi, ettei niistä ole rekisteröidyille merkittävää haittaa
- b) henkilötiedot on salattu tai muutettu niin (anonymisointi), etteivät ulkopuoliset, joilla ei ole oikeutta tietoihin, joko ymmärrä niitä tai pääse yksityiskohtaisiin tietoihin käsiksi
- c) Rekisterinpitäjä on jo toteuttanut sellaiset jatkotoimenpiteet, ettei arvioitu henkilötietoihin kohdistuva korea riski toteudukaan

10.4 Ilmoitusvelvollisuus viranomaisille

Airiston Putkityö Oy voi olla velvollinen ilmoittamaan tietoturvaloukkauksesta Tietosuojavaltuutetulle (tuleva Tietosuojavirasto). Esimerkiksi tapauksessa, jossa olemme lähettäneet joukkoviestiä asiakkaille ja huomaamme, että jokaisen vastaanottajan sähköpostiosoite etunimi.sukunimi@yritys.fi onkin kaikkien muiden vastaanottajien nähtävissä. Ilmoitus täytyy tehdä 72 tunnin sisällä.

Ilmoituksen tietoturvaloukkauksesta voi jättää verkkolomakkeella:

<https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta>

Neuvoja saa Tietosuojavaltuutetun toimistosta, Helsinki, puhelinvaihe 029 566 6700 (arkisin) tai (ma-ke) klo 9-16.00 erillisestä puhelinneuvonnasta 029 56 66777.

Meillä voi olla ilmoitusvelvollisuus myös Liikenne- ja viestintäviraston (Traficom) Kyberturvallisuuskeskukselle. Tällainen tilanne voi olla silloin, kun yrityksemme omiin tai palveluntarjoajan (sähköpostipalvelin, tilitoimisto, pankki) tietojärjestelmiin tehdään tietomurto (hakkerointi) ja on aihetta epäillä, että rekisterissämme olevien luonnollisten henkilöiden yksityisyys on vakavasti uhattuna tai tietoturvaloukkaus voi aiheuttaa heille taloudellista vahinkoa. Tämäkin ilmoitus pitää tehdä 72 tunnin sisällä.

I

Ilmoituksen tietoturvaloukkauksesta voi jättää verkkolomakkeella:

<https://kyberturvallisuuskeskus.fi/fi/ilmoita>

Neuvoja saa Liikenne- ja viestintävirastosta (Traficom), Helsinki, puhelinvaihe 029 534 5000 (arkisin).

Kummassakin ilmoituksessa on (artikla 33):

- a) kuvataan tietoturvaloukkaus, mahdollisuuksien mukaan myös rekisteröityjen ryhmät (asiakkaat, työntekijät, alihankkijat ym.) ja arvioit vaarantuneiden henkilötietojen lukumäärästä
- b) ilmoitetaan rekisteristä vastaavan henkilö nimi ja yhteystiedot lisätietojen saamista varten
- c) kuvataan henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- d) kuvataan toimenpiteet, joita rekisterinpitäjä on ehdottanut tai toteuttanut

Ilmoitusvelvoitteen täyttämistä helpottaa se, että tapahtuma on kirjattu Tietosuojaloukkaukset -taulukoon. Viranomaisilmoituksen tekee Airiston Putkityö Oy:n rekisteristä vastaava henkilö.

11. Tietosuoja / Rekisteriseloste

Tietosuoja-asetuksen läpinäkyvyysperikaateen ja rekisteröidyn oikeuksien nojalla Rekisterinpitäjä on velvollinen ilmoittamaan Rekisteröidyille tiiviissä, helposti ymmärrettävässä muodossa, millaista tietoa heistä kerätään ja mihin tarkoitukseen, samoin tuoda selvästi esiin Rekisteröityjen oikeudet. Rekisteriä ylläpitävän yrityksen on nimettävä rekisteriasioista vastaava henkilö, johon asiakkaita, kumppaneita ja sidosryhmiä edustavat luonnolliset henkilöt voivat olla yhteydessä (artiklat 12–14).

Airiston Putkityö Oy:n kotisivuilla julkaistu Tietosuojaseloste täyttää informoinnin velvoitteet. Tietosuojaseloste sisältää mm. seuraavia tietoja (tiivistelmä):

- rekisteriä pitävän yrityksen nimi: Airiston Putkityö Oy
- Y-tunnus: 1863243-6
- rekisterinpitäjän osoite: Teollisuuskatu 18, 21600 Parainen
- rekisterin nimi: Airiston Putkityö Oy:n asiakasrekisteri
- rekisteristä vastaava henkilö: Jani Jalonen
- rekisteristä vastaavan henkilön sähköpostiosoite: jani.jalonen(at)aptoy.fi
- rekisterin käyttötarkoitus: sopimukseen ja asiakassuhteiden ylläpitoon
- henkilötietojen käsittelyn ja suojauksen käytännöt yrityksessämme
- rekisteröidyn oikeudet

Tietosuojaselosteessa kerrotaan lisäksi, että Rekisteröidyn on lähetettävä pyyntö itseään koskevien tietojen tarkastamiseksi kirjallisesti ja missä ajassa Airiston Putkityö Oy toteuttaa pyynnön. Samoin, että Airiston Putkityö Oy varmistaa aina pyynnön tehneen henkilöllisyyden.

Maksuttoman tietopyynnön voi tehdä kerran vuodessa. Jos Rekisteröity esittää pyyntöjä toistuvasti, Airiston Putkityö Oy voi periä ylimääräisestä vaivasta maksun. Jos pyynnöt ovat kohtuuttomia ja perusteettomia, Airiston Putkityö Oy voi kieltäytyä tietojen luovuttamisesta. Tietopyynnön perusteettomuus tai kohtuuttomuus tulee pystyä osoittamaan (siksi pyynnöt tehdään kirjallisesti).

Airiston Putkityö Oy vastaa siitä, että julkinen Tietosuojaseloste, samoin kuin tämä Seloste käsittelystä, pidetään ajan tasalla.

12. Tietojenkäsittelysopimus

Asetuksen mukaan yritysten välillä tulee sopia kirjallisesti henkilötietojen luovutuksesta, luovutuksen kestosta, tietojen käyttötarkoituksesta, tietosuojakäytännöistä sekä rekisterinpitäjän ja henkilötietojen käsittelijän keskinäisistä vastuista ja millä tavalla rekisteröityjen oikeudet toteutetaan (artiklat 28, 42–43).

Yritys voi määritellä vastualueet erillisellä Tietojenkäsittelysopimuksella (sopimus henkilötietojen käsittelystä) tai tehdä sellaisen voimassa olevien (YSE) pääsopimusten liitteeksi. Tärkeintä on, että kaikki henkilötietojen käsittelyyn liittyvät käytännöt voidaan yksilöidä.

Tietojenkäsittelysopimuksessa Airiston Putkityö Oy määrittelee kenelle ja mitä varten henkilötietoja luovuttaa (esim. ulkoistettu IT-sopimus, tavarantoimitukset, alihankintaprojektin läpivieminen). Sopimuksilla varmistamme, että luovuttaessa hallussamme olevia henkilötietoja, niitä käsitellään ja säilytetään asianmukaisesti. Samoin toimimme meille luovutettujen henkilötietojen säilyttämisessä käsittelyssä ja siirroissa.

13. Sertifiointit

Tietosuoja-asetus vaikutti kaikkien EU- maiden lainsäädäntöön. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi uudisti useita lakeja, ja on mahdollista, että Tietosuojavaltuutetun toimisto muuttuu ehdotuksen nojalla (jossain vaiheessa) Tietosuojavirastoksi.

Lakimuutosten myötä otetaan käyttöön sinetit, merkit ja sertifikaatit, joilla Rekisterinpitäjät voivat osoittaa tietosuoja-asetuksen noudattamista (artiklat 42 ja 43). Mikä niistä sopii Airiston Putkityö Oy:lle, riippuu siitä, millainen tulee olemaan toimialaamme yleinen käytäntö.

Sertifiointi on vapaaehtoista ja sen pitää tapahtua läpinäkyvällä menettelyllä. Sertifiointi ei kuitenkaan vähennä Rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta asetuksen noudattamisesta. Sertifiointi ei myöskään rajoita valvontaviranomaisten valtuuksia (artikla 42, kohdat 3 ja 4).

Sertifiointia tekevän on voitava arvioida yrityksen tietosuojakäytännöt (artikla 43, kohta 6). Tämä tarkoittaa, että luovutamme Airiston Putkityö Oy:n sisäinen tietosuojadokumentaation ja yhteistyösopimusten tietosuoja koskevat litteet sertifioijan tarkastettavaksi. Tarvittaessa sertifioija voi tulla paikan päälle varmistamaan, että yrityksen tietosuojakäytäntö vastaa asiakirjoissa kuvattua.

Sertifiointeja tulevat tekemään Traficomien hyväksymät tahot. Airiston Putkityö Oy arvioi sertifiointin tarpeen ja tavan yhteistyökumppaneiden ja toimeksiantajien vaatimusten perusteella.

14. Tietosuoja-asetukseen liittyvää sanastoa

Henkilötietoryhmä

Rekisterissä olevien tietojen luokittelu ja / tai alaluokittelu, esim. työntekijät, alihankkijat, toimeksiantajat, asiakkaat, tavarantoimittajat, ym.

Henkilötietojen käsittely

Kun mitä tahansa luonnollisia henkilöitä koskevia tietoja kerätään, tallennetaan, säilytetään, muokataan, muutetaan, ryhmitellään, haetaan tietokannasta, siirretään tietokannasta (paikasta) toiseen, jaetaan sovittujen osapuolten kanssa.

Henkilötietojen käsittelijä

Luonnollinen henkilö, oikeushenkilö tai viranomainen tai kolmas taho, joka käsittelee henkilötietoja Rekisterinpitäjän lukuun.

Henkilötietojen vastaanottaja

Luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai kolmas osapuoli, jolle luovutetaan henkilötietoja. Henkilötietoja voidaan luovuttaa säilyttämistä, tilastointia, raportointia tai käsittelyä varten.

Kolmas osapuoli

On luonnollinen henkilö (ei kuitenkaan Rekisteröity), oikeushenkilö, viranomainen tai virasto, rekisterinpitäjä, henkilötietojen käsittelijä, joilla on oikeus käsitellä henkilötietoja suoraan Rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.

Yhteisrekisterinpitäjä

Useampi rekisterinpitäjä päättää yhdessä (sopimus) millaisia henkilötietoja ja mihin tarkoitukseen käsitellään: Yritys A ja Yritys B toteuttavat projekteja, joissa on tarkoitus yhteisen hyödyn saaminen esim. lisäpalveluja tarjoamalla, ja siinä hyödynnetään kummankin yrityksen asiakastietoja. Yhteisrekisterinpitäjät voivat käyttää yhteistä tietokantaa tai vaihtaa henkilötietoja keskenään ja toimia samalla käsittelijöinä toistensa lukuun.

"Yrityksesi/organisaatiosi on yhteisrekisterinpitäjä, jos se päättää yhdessä yhden tai useamman organisaation kanssa, "miksi" ja "miten" henkilötietoja käsitellään. Yhteisrekisterinpitäjien pitää sopia jokaisen osapuolen vastuista yleisen tietosuojasetuksen sääntöjen noudattamiseksi. Sopimuksen tärkeimmistä seikoista pitää ilmoittaa yksilöille, joiden tietoja käsitellään."

Ks. esimerkki: *Mikä on rekisterinpitäjä tai tietojen käsittelijä? Euroopan komission Tietosuojasetusta koskeva kysymys-vastaussivusto*

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi

Tietoturvaloukkaus

On tapahtuma, jossa rekisterissä olevia henkilötietoja vahingon tai lainvastaisen toiminnan seurauksena muutetaan, hävitetään, tuhoetaan tai luovutetaan luvattomasti; luvaton pääsy tietoihin.

Valvontaviranomainen

Tietosuojasetuksen noudattamista valvova viranomainen, Suomessa Tietosuojavaltuutetun toimisto.