Tietosuoja ja henkilötietojen käsittely

Rakennusautomaatioliikkeiden
liitto

Sisällys

Johdanto

Rakennusautomaatioliikkeiden liitto, RALL ry on rakennusautomaatioalalla ja LVIS-säätöalalla toimivien liikkeiden, maahantuojien ja järjestelmävalmistajien yhteenliittymä, joita liitto edustaa suhteessa viranomaisiin, toisiin järjestöihin ja muihin ulkopuolisiin. Liiton tarkoituksena on valvoa jäsentensä yleisiä ja yhteisiä etuja alaa koskevissa ammatillisissa, teknillisissä, kaupallisissa ja liikkeenhoidollisissa sekä työmarkkinakysymyksissä. Liiton tarkoituksena on myös edistää jäsentensä ja koko alan korkean ammatillisen tason saavuttamista ja edelleen kehittämistä. Liitto valvoo hyvien liiketapojen noudattamista ja vastustaa kaikkea epätervettä toimintaa alalla.

25.5.2018 astuu voimaan EU:n uusi tietosuoja-asetus (General Data Protection Regulation, GDPR). Jo ennen näitä muutoksia olemme kiinnittäneet erityistä huomiota henkilötietojen käsittelyyn kulloisenkin lainsäädännön mukaisesti. Uusi tietosuoja-asetus tuo tullessaan muutamia tarkennuksia henkilötietojen käsittelyyn ja voit tästä dokumentista tutustua siihen, miten olemme asiat hoitaneet. Tietosuoja-asetuksen perustarkoitus on pitää yritysten hallussa olevat henkilötiedot ajan tasalla, turvassa ja saatavilla ja vain niille, jotka tietoa tarvitsevat.

Noudatamme tietosuoja-asetuksen ydinhengen mukaisesti sisäänrakennetun tietosuojan (Privacy by Design) periaatteita. Olemme uusineet sähköiset järjestelmämme toimintavarmoiksi ja turvallisiksi tätä henkeä silmällä pitäen.

Tietosuoja-asetus ja sen tarkennukset ovat uusi asia ja sitä mukaa kun viranomaistulkintoja saadaan lisää, meidän voi olla tarpeen päivittää toimintatapojamme ja siihen liittyvää ohjeistusta. Otamme mielellään vastaan tietosuojaan liittyvää palautetta ja kysymyksiä parantaaksemme toimintaamme.

Roolit

Ohessa on lyhyesti avattuna joitan keskeisiä tietosuoja-asetuksessa käytettyjä termejä.

Rekisterinpitäjä

Toimimme rekisterinpitäjänä. Rekisterinpitäjä tekee sisältöön, prosesseihin ja henkilötietoihin käyttöoikeuksiin liittyvät päätökset.

Yhteisrekisterin pitäjä

Jos eri rekisterinpitäjät yhteisesti määräävät henkilötietojen käsittelystä, voivat he toimia yhteisrekisterin pitäjänä. Yhteisrekisterin pitäjät voivat yhdessä määritellä mikä rekisterinpitäjä toimii yhteyspisteenä rekisteröidyille. RALL ry on ulkoistanut palvelusopimuksella jäsenrekisterin ylläpitämisen Sähkö- ja Teleurakoitsijaliitto STUL ry:lle. Sähkö- ja Teleurakoitsijaliitto STUL ry:n rekistereitä ylläpitää sen kustannusyhtiö Sähköinfo Oy. Sähköinfo Oy toimii yhteisrekisterin pitäjänä STUL ry:lle ja RALL ry:lle.

Henkilötietojen käsittelijä

Palveluntarjoajat, jotka tuottavat meille järjestelmiä toimivat henkilötietojen käsittelijöinä. Palveluntarjoajat käsittelevät tietoja ainoastaan tuottaakseen nimettyä järjestelmää. Palveluntarjoajat ovat vastuussa meille sopimusperusteisesti sekä tietysti suoraan viranomaisille. Käsittelemme eri palveluntarjoajat myöhemmin tässä dokumentissa.

Rekisteröity

Rekisteröity-termillä tarkoitetaan henkilöitä, joiden tietoja käsitellään.

Oikeus käsitellä henkilötietoja

Oikeus käsitellä tietoja voi perustua suostumukseen, sopimukseen tai oikeutettuun etuun.

Suostumuksella tarkoitetaan sitä, kun rekisteröity antaa suostumuksen tietojen käsittelyyn esim. tuoteoston yhteydessä.

Sopimuksen myötä syntyvä käsittelyoikeus edellyttää sopimuksen kautta syntyvää oikeutta sopimuksen ehtojen toimeenpanemiseksi.

Oikeutettuun etuun perustuva käsittelyoikeus muodostuu, kun tietojen käsittely on tarpeen etuuden tuottamiseksi, esimerkiksi jäsensopimukset.

Lakisääteinen oikeus muodostuu, kun rekisterinpitäjällä on velvoite käsitellä tietoja.

Miksi tietoa kerätään ja miten sitä säilytetään

Jäseneksi hakeutuminen

RALL ry:n jäsenet ovat yrityksiä. Yritykset ilmoittavat jäsenhakemuksella yhteyshenkilön yhteystiedot. Yhteystietoja käytetään jäsenviestintään ja jäsenetujen toimittamiseen.

RALL ry:n hallitus käsittelee kaikki jäsenhakemukset ja hyväksyy jäsenyyden ehdot täyttävät jäsenet. Hallituksella on pääsy jäsenhakemustietoihin. Hallituksen voimassa olevan kokoonpanon näet verkkosivuilta: http://www.rall.fi/index.php?k=224459

Jäsenhakemus voi saapua yhdistykselle paperisena tai sähköpostin liitteenä. Paperilla toimitetut hakemukset arkistoidaan yhdistyksen kansioon.

Kaikki sähköisesti saapuneet hakemukset arkistoidaan yhdistyksen verkkolevykansioon.

Sähköisesti tiedostot ovat tallennettuina Sähköinfon lukuun Chilit Oy:n ylläpitämillä tiedostopalvelimilla Helsingissä. Sähköposti tuotetaan Sähköinfon lukuun Microsoftin O365 -palvelulla Chilit Oy:n toimesta.

Jäsenrekisteri

RALL ry on ulkoistanut jäsenrekisterin ylläpidon palvelusopimuksella Sähkö- ja Teleurakoitsijaliitto STUL ry:lle. STUL ry:n jäsenrekisteriä ylläpitää yhteisrekisterinpitäjänä Sähköinfo Oy.

Jäsenrekisteri on sähköinen ja sitä tuottaa Sähköinfon lukuun Business Databases Oy.

Jäsensivuja ja siellä käytettäviä salasanoja hallinnoi Sigmatic Oy.

Jäsentiedotus

Eräs keskeisimmistä toiminnoistamme on tiedottaminen alaan liittyvistä asioista. Hoidamme tiedotusta verkkosivujen ja sähköpostin kautta. Jäsentiedotusta varten henkilöiden tietoja ylläpidetään jäsenrekisterissä ja viestit lähetetään O365 Outlook -sähköpostiohjelmistolla aina piilokopioina.

Tietojen edelleen luovutus

RALL ry on Sähkö- ja teleurakoitsijaliitto STUL ry jäsenjärjestö. Jäsenjärjestönä RALL ry:n jäsenet ovat oikeutettuja saamaan STUL ry:n jäsenetuja. Näiden etujen toimittamiseksi RALL ry luovuttaa jäsentietonsa Sähkö- ja teleurakoitsijaliitto STUL ry:lle.

RALL ry on ulkoistanut palvelusopimuksella toimistopalveluidensa ja järjestelmiensä hallinnan Sähkö- ja teleurakoitsijaliitto STUL ry:lle. Sähkö- ja teleurakoitsijaliitto STUL ry:lle näitä palveluita tuottaa Sähköinfo Oy, STUL:n 100 % omistusyhtiö.

RALL ry:n tilintarkastajana toimii BDO Oy tilintarkastusyhteisö (1893593-9), kotipaikka Helsinki. Vastuullisina tilintarkastajina toimivat BDO:sta Pertti Hiltunen ja Pekka Klemetti. Tilintarkastuksessa ja tarkastaessaan toiminnan vastuullisuutta voi tulla tilanne, jossa tilintarkastajalla on pääsy henkilötietoihin.

Riskit ja riskienhallinta

Tietoriskien hallinta muodostuu riskien tunnistamisesta ja olennaiset osat riskien hallinnasta liittyvät tekniseen suojaamiseen ja henkilöstön osaamisen varmistamiseen.

Tietoriskien kannalta tärkeätä on että,

- tiedot ovat oikeita, luotettavia ja ajan tasalla
- tiedot on oikeutettujen henkilöiden saatavilla
- tiedot eivät joudu asiaankuulumattomille henkilöille.

Riskit

Henkilötietoihin liittyvät riskit ovat tietojen oikeellisuus, oikea-aikainen saatavuus oikeille henkilöille, tietojen väärinkäyttö tai tietojen katoaminen.

Henkilötietoja ylläpidetään säännöllisesti ja niihin tehdään tarkennuksia rekisteröidyn ilmoituksen perusteella tai ulkoisista lähteistä.

Tietojärjestelmiä varmistetaan niin, että ne ovat saatavilla oikeille henkilöille silloin, kun niitä tarvitaan. Järjestelmäkumppaneiden kanssa on sovittu erikseen sopimuksilla erillisistä palvelutasoista, milloin tietojen pitää olla käytettävissä häiriötilanteissa.

Tietojen väärinkäyttöä estetään käyttöä suojaamalla ja henkilöstöä opastamalla. Suurin tietoriski on henkilöiden toiminta, ja tätä hallitaan kouluttamalla ja ohjeistamalla henkilöstö tietojen oikeanlaiseen käsittelyyn.

Sellaisessa tilanteessa, jossa tietoja päätyisi vääriin käsiin, noudatetaan tietosuoja-asetuksen ilmoittamismenettelyä. Ilmoitusmenettelystä on sovittu ja dokumentoitu toimintamallit.

Johtaminen

Johto on tietoinen yrityksen hallussa olevista tietovarannoista ja siitä, miten niitä käytetään ja suojataan. Johto vastaa tietoturvapolitiikan ylläpitämisestä ja käytäntöön viemisestä. Johto vastaa siitä, että henkilöstöllä on riittävät mahdollisuudet tietoturvalliseen tietojen käsittelyyn.

Toimitilat

Yrityksen toimitilat on suojattu ulkopuolisilta. Mekaanisten lukitusten lisäksi käytössä on elektroninen kulunvalvonta. Arkaluontoista tietoa sisältävät fyysiset arkistot säilytetään lisäksi lukituissa tiloissa. Avainhallinta on keskitettyä ja henkilöstön ulkopuolelle annetut kulkuoikeudet on dokumentoitu.

Virustorjunta ja palomuurit ovat ajantasalla ja palomuuriavaukset dokumentoitu.

Arkaluontoisten dokumenttien tuhoamista varten on käytettävissä silppureita tai erillinen lukittu tietosuojasäiliö, jonka tietoturvallisesta tyhjennyksestä ja dokumenttien tuhoamisesta vastaa MTB Tietopalvelut Oy.

Tietojärjestelmien suojaus

Tietojärjestelmien hallinta on ulkoistettu ja konesalin turvallisuudesta vastaa Chilit Oy. Kunkin käytetyn järjestelmän kohdalla on kuvattu ko.tietoon liittyvä kumppani. Etäkäyttö on mahdollista vain suojatun VPN-yhteyden kautta. Käyttöä suojataan käyttöoikeuksin.

Henkilöstön toiminta

Jokainen työntekijä on koulutettu tietoturvalliseen tietojen käsittelyyn. Henkilöstön kanssa on käyty läpi tietoturvapolitiikka aina sen muututtua olennaisesti. Tietojen käsittelystä on selkeät toimintaohjeet. Henkilöstön kanssa on käyty läpi myös henkilötiedoista keskustelun periaatteet. Julkisissa tiloissa yrityksen asioista ja asiakkaista keskusteleminen on tietoturvaohjeessa kielletty.

Suhteet sidosryhmiin

Alihankkijoita valitessa ja kumppanuussopimuksia solmittaessa turvallisuuden hallintaan liittyvät asiat on käyty läpi. Sopimukset ovat ajantasalla ja niitä päivitetään säännöllisesti. Luottamushenkilöt ymmärtävät luottamusasemansa tuomat oikeudet tietovarantoihin ja niiden luottamukselliseen käsittelyyn.

Kehittäminen ja toiminnan jatkuvuus

Tietosuojakuvaukset ja tietovarannot on dokumentoitu, samoin tietotekniset järjestelmät. Tietoteknisestä ympäristöstä on tehty palautumis- ja jatkuvuussuunnitelma ja tiedot on varmistettu. Toiminnan jatkuvuuden kannalta avainhenkilöt on tunnistettu.

GDPR tarkentaa tiettyjä rekisteröidyn oikeuksia. Esitämme seuraavassa, miten olemme huomioineet nämä muutokset.

Sisäänrakennettu tietosuoja

Henkilötietojen yksityisyys ja tietoturva ovat prosessiemme perusteissa. Toimintaamme sisältyy henkilötietojen käsittelyä, ja sekä yksityisyys että tietosuojan noudattaminen ovat olennainen osa palveluamme, niin palvelun kehityksessä, ylläpidossa, tuessa kuin myynnissä ja markkinoinnissakin. Yksityisyys on tärkeä osa myös kaikkia kehityshankkeitamme. Tietojen käsittelyjärjestelmämme on tehty mahdollisimman turvalliseksi. Käytämme turvallisuutta ja hallintaa kumppanien valintaperusteissa ja kehitämme sekä teknisiä että omia toimintatapojamme taataksemme henkilötietojen turvallisen käsittelyn.

Oikeus saada tietoa henkilötietojen keräämisestä ja käsittelystä

Rekisteröidyllä on oikeus saada tietää, milloin ja mitä heitä koskevia henkilötietoja käsitellään ja mitä tallennetaan.

- Keräämme vain tietoa, joka on tarpeen palveluiden tuottamiseksi.
- Säilytämme henkilötietoja huolellisesti. Säilytämme tietoja ainoastaan sähköisesti poislukien paperiversiona tulleet jäsenhakemukset. Sähköisiä tietoja säilytämme tietojärjestelmissä, joissa tietojen käsittelyä suojataan käyttöoikeuksin.
- Tietosuoja- ja rekisteriselosteemme ovat jatkuvasti nähtävillä verkkopalvelussamme.
- Jos jokin tietojen käsittelyyn vaikuttava lainsäädäntö muuttuu olennaisesti, tiedotamme muutoksista.

Oikeus päästä omiin tietoihin ja tietojen oikaisuun

Rekisteröidyillä on oikeus saada pääsy omiin tietoihinsa ja saada epätarkat ja virheelliset tiedot korjattua.

- Rekisteröidyllä on oikeus saada jäljennös hallussamme olevista tiedoista. Pyynnöstä toimitamme jäljennöksen tiedoista sähköisesti. Jäljennöksen voi pyytää sähköpostitse osoitteesta ville.reinikainen@sahkoinfo.fi
- Toimitamme pyynnöt viivyttelemättä ja tietosuoja-asetuksen mukaisessa määräajassa 1 kk.
- Ylläpidämme tietoja ja päivitämme yhteystietoja ilmoituksesta.

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada tietonsa poistetuksi, kun tiedon käsittely ei ole enää aiheellista.

- Unohdetuksi tulemisen vaihtoehtoina voi käyttää postikieltoa, passivointia tai rajoitetusti poistoa.
- Tuotteiden myyntiin ja toimittamiseen liittyen tietoja voidaan pyynnöstä poistaa, ei kuitenkaan niiltä osin, kun niihin liittyy lakisääteisiä säilytysaikoja esim. laskuttamiseen liittyen.

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada omat tietonsa helposti luettavassa muodossa sekä siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

- Tallennetut tiedot voidaan pyynnöstä toimittaa asiakkaalle sähköisessä muodossa tietojen siirtämistä varten.
- Paperimuotoiset tiedot toimitetaan sähköisenä PDF-muodossa.
- Muut henkilötiedot toimitetaan sähköisenä CSV-tiedostona.

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Tietoturvaloukkaukset tulee raportoida viranomaisille 72 tunnin kuluessa.

- Olemme valinneet järjestelmätoimittajat tarkasti ja luotamme suomalaisiin kumppaneihimme, joten tietojasi säilytetään huolellisesti ja valvotusti.
- Tietokanta- ja tiedostopalvelimet ovat asiantuntevien kumppaneidemme hallinnassa ja niitä säilytetään Chilit Oy:n lukuun Telecityn tiloissa Helsingin Suvilahdessa ja Uspenskissa Katajanokalla. Ne täyttävät seuraavat standardit: TIA-942, ISO/IEC 27001:2005, ISO 9001:2008, ISO 14001:2004. Salit ovat Tier 3 -tason tiloja.
- Olemme sopineet kumppaneiden kanssa menettelystä, jolla tietoturvaloukkauksista informoidaan.
- Henkilökuntamme on koulutettu luottamuksellisen tiedon käsittelyyn.
- Epätodennäköisessä tilanteessa, jossa tietoturvaloukkaus tapahtuisi, ilmoitamme rekisteröidylle ja viranomaiselle.