

**EU:N UUSI
TIETOSUOJA-ASETUS**

**TIETOPAKETTI
CSI-ASIAKKAILLE**

9.5.2018

SISÄLLYSLUETTELO

1.	EU:n uusi tietosuoja-asetus ja osapuolten velvoitteet.....	3
1.1.	CSI-asiakkaiden velvoitteet	3
1.2.	CSI:n velvoitteet ohjelmistotoimittajana	3
2.	CSI-ohjelmistojen tuki tietosuoja-asetuksen vaatimusten täyttämiseen.....	4
2.1.	Rekisteröidyn oikeuksia tukeva toiminnallisuus	4
2.2.	Käyttäjien tunnistautuminen CSI-ohjelmistoon.....	5
2.3.	Käyttöoikeuksien rajaaminen.....	5
2.4.	Henkilötietojen muutos- ja katseluseuranta	6
3.	Tietosuoja-asetuksen huomiointi CSI:ssä	6
3.1.	Asiantuntemus ja resurssit	6
3.2.	Sopimukset tietojen käsittelystä.....	7
3.3.	Alihankkijoiden käyttö tiedon käsittelyssä	7
3.4.	Turvallisuus	7
3.5.	Tietojen siirto kansainvälisesti	8
4.	CSI:n toiminta tiedon käsittelijänä	8
4.1.	Tietojen käsittely	8
4.2.	Käytettävien yhteyksien tietoturvallisuus	8
4.3.	CSI:lle siirrettävät tietovarastot	9
4.4.	Tietovarastojen säilyttäminen	9
4.5.	Pilvipalveluasiakkaan tietovaraston poistaminen	9
4.6.	Ilmoittaminen tietoturvaloukkauksista	10
5.	CSI rekisterinpitäjänä.....	10
6.	CSI:n GDPR-tuki asiakkaille	10

1. EU:N UUSI TIETOSUOJA-ASETUS JA OSAPUOLTEN VELVOITTEET

EU:n uusi tietosuoja-asetus astuu voimaan 25.5.2018. Asetuksen tavoitteena on lisätä yksilön oikeuksia oman henkilötietonsa hallinnassa ja käsittelyssä sekä yhtenäistää lainsäädäntöä Euroopan Unionin sisällä.

CSI on sitoutunut noudattamaan uutta tietosuoja-asetusta omassa toiminnassaan ja kehittämään CSI-ohjelmistoja siten, että ne tukevat asiakkaita asetuksen noudattamisessa.

1.1.CSI-ASIAKKAIDEN VELVOITTEET

CSI:n asiakkaat toimivat rekisterinpitäjinä henkilörekistereille, joita he ylläpitävät ja käsittelevät CSI-ohjelmistoissa. Näissä tapauksissa CSI ei koskaan toimi rekisterinpitäjän roolissa, mutta saattaa toimia tietojen käsittelijänä.

Rekisterinpitäjä (asiakas) määrittää rekisterin käyttötarkoituksen (esim. asiakasrekisteri). Rekisterinpitäjä huolehtii siitä, että rekisteröityjen tietoja käsitellään asetuksen vaatimusten mukaan niin teknisesti kuin hallinnollisestikin.

Rekisterinpitäjän on huolehdittava toimintansa läpinäkyvyydestä rekisteröidyille. Käytännössä rekisterinpitäjällä on velvollisuus informoida rekisteröityä henkilötietojen käsittelystä, käsittelyn tarkoituksesta ja perusteesta, tietojen säilytysajasta sekä oikeussuojakeinoista. Tämä informaatio voidaan antaa tietosuojaselosteen avulla.

Lisäksi rekisterinpitäjän on huolehdittava rekisteröityjen tietojen oikeellisuudesta, henkilötiedon käytön rajoittamisesta sekä erityisesti tarpeettomien tietojen poistamisesta. Rekisterinpitäjän vastuulla on myös rekisteröidyn oikeuksien varmistaminen. Rekisteröidyillä on muun muassa oikeus pyytää nähtäväkseen rekisteröityjä tietojaan, pyytää virheellisten tietojen korjaamista ja vaatia myös tietojen poistamista, mikäli sille ei ole esteitä.

Lisätietoja asetuksesta löytyy muun muassa Tietosuojavaltuutetun ohjeista <http://www.tietosuoja.fi/fi/index/euntietosuojaudistus/ohjeitarekisterinpitajalle.html>.

1.2.CSI:N VELVOITTEET OHJELMISTOTOIMITTAJANA

CSI tukee asiakkaitaan tietosuoja-asetuksen velvoitteiden täyttämässä kehittämällä CSI-ohjelmistoihin sitä helpottavia toiminnallisuksia.

Tämän lisäksi CSI saattaa rekisterinpitäjän pyynnöstä toimia henkilötietojen käsittelijän roolissa seuraavissa tilanteissa:

- käsitellessään konversiotietokantoja asiakkaan siirtyessä CSI-ohjelmiston käyttäjäksi
- käsitellessään testitietokantoja asiakkaan valmistautuessa uuden ohjelmistoversion käyttöönottoon
- tutkiessaan etäyhteyden tai tietokantayhteyden kautta asiakkaan ongelmatilannetta tai tehdäkseen asiakkaan pyytämiä muutoksia CSI-ohjelmistoon tai
- käsitellessään asiakkaan tietokantoja asiakkaan yritysjärjestelyjen yhteydessä.

CSI:n käsittelemät henkilötiedot voivat näissä tapauksissa olla

- asiakkaan ohjelmistonsa tallentamien asiakkaiden henkilötietoja tai muita toimeksiantoihin liittyviä henkilötietoja ja/tai
- asiakkaan työntekijöiden eli CSI-ohjelmiston käyttäjien henkilötietoja.

Olemme kuvanneet toimintamallimme asiakkaan tietokantojen käsittelijänä edellä mainituissa tilanteissa, ja tarkentaneet samassa yhteydessä toimintatapojamme tietosuojan maksimoimiseksi.

2. CSI-OHJELMISTOJEN TUKI TIETOSUOJA-ASETUksen VAATIMUSTEN TÄYTTÄMISEEN

2.1. REKISTERÖIDYN OIKEUKSIA TUKEVA TOIMINNALLISUUS

CSI-ohjelmistossa henkilö perustetaan vain kerran, mikä helpottaa tietosuoja-asetuksen vaatimuksien täyttämistä ja henkilötietojen hallintaa yleensäkin. Henkilön esimerkiksi vaihtaessa työpaikkaa tämän tietoihin päivitetään uusi työnantaja, jolloin vältetään duplikaatit.

CSI-ohjelmistot tarjoavat tukea rekisteröityjen oikeuksien täyttämiseen seuraavasti:

REKISTERÖIDYN OIKEUDET		CSI-OHJELMISTON TUKI
Pääsy tietoihin	Oikeus saada tieto siitä, onko rekisterissä rekisteröidyn henkilötietoja, ja jos on, lista tallennetuista henkilötiedoista.	CSI-ohjelmisto tuottaa raportin, joka listaa henkilöstä ohjelmistoon tallennetut henkilötiedot.
Tietojen oikaisu	Oikeus saada epätarkat ja virheelliset tiedot oikaistua.	Tietojen muokkaus kuuluu ohjelmiston perustoimintoihin.
Tietojen siirto	Oikeus saada tiedot siirretyksi toiselle rekisterinpitäjälle.	Tiedot saadaan CSI-ohjelmistosta ulos muodossa, joka on luettavissa sisään toiseen ohjelmistoon.
Profiloinnin vastustaminen	Oikeus vastustaa profilointiin perustuvaa päätöksentekoa.	Automaattista profilointia ei suoriteta. Esim. esteellisyys-tarkastus kerää tiedot, mutta päätös jää käyttäjälle.
Käsittelyn rajoittaminen	Oikeus estää henkilötietojen käsittely ilman, että tietoja poistetaan.	Markkinointikiellolla voidaan estää rekisteröidyn tiedon listautumisen markkinointitarkoituksiin käytettäville postituslistoille.
Unohdetuksi tuleminen	Oikeus saada henkilötiedot poistettua, ellei olemassa oleva palvelusopimus tai lainsäädäntö estä poistamista.	Henkilö voidaan poistaa, ellei CSI-ohjelmistosta löydy poistoa estäviä tapahtumia.

Raportti rekisteröidyn tiedoista ja tietojen siirto

CSI-ohjelmistoon on 7.0-versiosta lähtien mahdollista ladata raportti, joka listaa ohjelmistoon kirjatusta asiakkaasta tai käyttäjästä henkilötiedot: perustiedot, yhteystiedot ja rajoitukset (markkinointikielto, toimituskielto). Henkilötietoraportti on muodossa, joka voidaan sellaisenaan lähettää rekisteröidylle.

Henkilön tiedot saadaan ohjelmistosta ulos muodossa, joka mahdollistaa niiden siirtämisen toiseen ohjelmistoon.

Henkilötietojen käsittelyn rajoittaminen

CSI-ohjelmistojen 7.2-versio tuo Postituslistoihin mahdollisuuden rajoittaa yksityishenkilölle lähetettäviä markkinointiviestejä. Mikäli yksityishenkilön tiedoissa on valittuna ”Markkinointi kielletty” -kenttä, henkilön yhteystietoja ei tuoda markkinointitarkoituksiin käytettäville postituslistoille.

Henkilön poistaminen ohjelmistosta

Henkilön tiedot voidaan poistaa CSI-ohjelmistosta, mikäli tällä ei ole poistoa estäviä tapahtumia. Poistamisen estäviä tietoja ovat esimerkiksi toimeksiannot, tuntikirjaukset, aktiviteetit, fataljit, erilaiset laskut ja suoritukset.

Jos henkilöön liittyy poistamisen estäviä tietoja, häntä ei voida poistaa suoraan, vaan tiedot on ensin siirrettävä toiselle asiakkaalle (yksityishenkilölle tai yritysasiakkaalle). Tietojen siirtämisen jälkeen ohjelmisto poistaa henkilön kokonaan tietokannasta.

Käyttäjien (työntekijöiden) poistaminen CSI-ohjelmiston tietokannasta ei tällä hetkellä ole mahdollista. Sen sijaan esimerkiksi entisen käyttäjän tiedot voidaan pseudonymisoida eli muokata käyttäjän tunnus, nimi ja sähköpostiosoite siten, ettei niitä voida enää yhdistää henkilöön ilman lisätietoja, jotka säilytetään asianmukaisesti CSI-ohjelmistosta erillään.

2.2.KÄYTTÄJIEN TUNNISTAUTUMINEN CSI-OHJELMISTOON

Käyttäjät tunnistautuvat CSI-ohjelmistoon joko Active Directory –tunnuksella tai erikseen määriteltävällä käyttäjätunnus/salasana-yhdistelmällä. Nämä tiedot ovat CSI-ohjelmiston tietokannassa, johon ohjelmiston pääkäyttäjä voi lisätä tai muuttaa niitä. Salasana on kryptattu, joten sitä ei edes pääkäyttäjä pääse katsomaan.

Ohjelmistoon kirjautuminen edellyttää lisäksi, että käyttäjän Active Directory –tunnukselle on määritetty SOL Serveriin riittävät oikeudet. Vaihtoehtoisesti voidaan käyttää SQL-loginia, jolle SQL Serverin järjestelmävalvoja on antanut vastaavat oikeudet.

2.3.KÄYTTÖOIKEUKSIEN RAJAAMINEN

Myös CSI-ohjelmistojen käyttäjähallinta tarjoaa mahdollisuuksia tietojen näkyvyyden rajoittamiseen. Ohjelmiston pääkäyttäjillä on pääsy kaikkiin ohjelmiston tietoihin, mikä vuoksi suosittelemme pääkäyttäjien määrän pitämistä rajallisena.

Navigointioikeuksien avulla voidaan rajata kansioiden näkyvyyttä eri käyttäjäryhmille. Näin voidaan määrittää esimerkiksi käyttäjäryhmä, jolle ei näytetä lainkaan henkilöasiakkaiden tietoja. Tällainen ryhmä pääsee ainoastaan yritysasiakkaiden kontaktihenkilöiden tietoihin.

Yksityishenkilön toimeksianto voidaan määrittää sisäpiiritoimeksiannoksi, jolloin sen näkyvyys rajataan vain toimeksiantotiimin jäsenille.

2.4. HENKILÖTIETOJEN MUUTOS- JA KATSELUSEURANTA

Henkilötietojen muutoksiin ja niiden katseluun CSI-ohjelmistoissa voidaan määrittää lokiseuranta. Muutosloki asetetaan päälle ohjelmiston Asetuksissa (Tietokannan hallinta > Muutoshistoria), jossa valitaan seurattavaksi kohteeksi yksityishenkilö, määritetään seurattavat kentät sekä liittyvät kohteet, esimerkiksi henkilön tietyt alikansiot. Seurantaan voidaan tarvittaessa tehdä myös lisärajoituksia.

Yksittäisen henkilön tietoihin tehtyjä muutoksia voidaan tämän jälkeen seurata henkilön historiatiedoissa. Ohjelmisto näyttää oletuksena, milloin henkilön tiedot on luotu ja milloin niihin on tehty muutoksia. Listalle saadaan näkyviin myös tieto siitä, milloin henkilön tietoja on käyty katsomassa ilman, että niitä on muutettu. Henkilön alikansioiden tietoihin tehdyt muutokset näkyvät kyseisen alikansion historiatiedoissa.

Toiminnallisuus löytyy jo tällä hetkellä kaikista CSI-ohjelmistoista lukuun ottamatta CSI LakiMies – ohjelmistoa, johon se tulee 7.2-versiossa.

HUOM! Koska henkilötietojen lokiseuranta koskee **kaikkia** ohjelmistoon tallennettuja henkilötietoja, sen käyttöönoton yhteydessä on varauduttava ohjelmiston mahdolliseen hidastumiseen.

3. TIETOSUOJA-ASETUKSEN HUOMIOINTI CSI:SSÄ

3.1. ASIAANTUNTEMUS JA RESURSSIT

Vastuu CSI:n tietosuojasta, tarvittavien muutosten tekemisestä sekä tietosuojaprosessien jalkauttamisesta osaksi yrityksen tuotteita ja palveluita on koko johtoryhmällä.

CSI:n koko henkilökunta on saanut peruskoulutuksen uuden tietosuoja-asetuksen vaatimuksista ja on sitoutunut noudattamaan niitä työssään. Täydentävä koulutus järjestetään vielä ennen tietosuoja-asetuksen voimaan astumista, ja jatkossa työntekijöille järjestetään tietosuojakoulutusta vähintään kerran vuodessa.

3.2.SOPIMUKSET TIETOJEN KÄSITTELYSTÄ

CSI ymmärtää roolinsa luottamuksellisten henkilötietojen käsittelijänä ja suhtautuu vakavasti sen tuomaan vastuuseen. Olemme laatineet pääsopimustamme täydentämään tietosuoja-asetuksen mukaisen henkilötietojen käsittelysopimuksen.

Edellytämme henkilötietojen käsittelysopimuksen allekirjoittamista kaikilta asiakkailtamme, jotta voimme varmistua tietoturvalisesta ja asetuksen mukaisesta henkilötietojen käsittelystä myös 25.5.2018 jälkeen.

Kaikkia työntekijöitämme sitoo salassapitosopimus, joka koskee myös asiakkaiden tietoja.

3.3.ALIHANKKIJOIDEN KÄYTTÖ TIEDON KÄSITTELYSSÄ

CSI:n tavoitteena on tarjota asiakkaille mahdollisimman turvallista ja laadukasta palvelua. Palveluiden tuottamisessa käytämme alihankkijoita ja kumppaneita, jotka EU:n uuden tietosuoja-asetuksen mukaisesti luetaan myös henkilötietojen käsittelijöiksi. CSI:n alihankkijoiden rooli tietojen käsittelijöinä rajoittuu kuitenkin tietovarastojen tekniseen ylläpitoon, eikä alihankkijoilla missään tilanteessa ole oikeutta tietovarastojen sisältämien henkilötietojen katseluun tai muokkaamiseen.

Kaikki alihankkijamme täyttävät samat tietoturvan ja tietosuojan kriteerit, joihin olemme itsekin sitoutuneet.

CSI:n alihankkijoina toimivat:

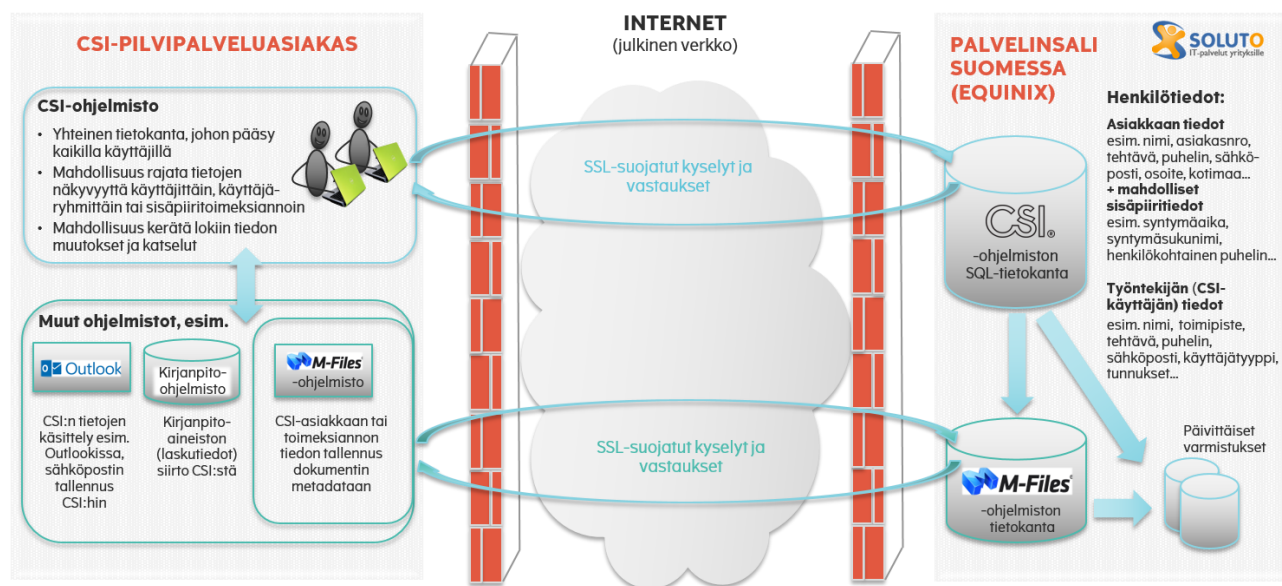
- Soluto Oy, 2084582-8 Pilvipalvelutoimittaja
- SoftAvenue Oy, 1761128-9 IT-palveluiden tuottaja

3.4.TURVALLISUUS

Henkilötietojen turvallisuus ja luottamuksellisuus on keskeinen osa uutta tietosuoja-asetusta. Varmistamme asiakkaidemme tietojen turvallisuuden noudattamalla alan parhaita käytäntöjä ja standardeja sekä kehittämällä jatkuvasti valmiuttamme uusien turvallisuuskäytäntöjen luomiseen.

Pilvipalvelun tietosuoja

Pilvipalvelussamme asiakkaiden tietovarastot ovat tietoturvalisessa, Helsingissä sijaitsevassa palvelinsalissa, joka on ISO9001-, ISO14001-, ISO27001-, ISO500001-, OHSAS18001- ja PCI-DCSS-auditoitu.



Palvelinarkkitehtuuri on rakennettu vikasietoiseksi, joten palvelut ovat käytössä myös yksittäisten laitteiden tai palveluiden vikaantumista. Asiakkaiden tietokannasta otetaan päivittäin varmuuskopiot, joita säilytetään eriytetyissä palveluissa. Näin voidaan varmistua tietojen palautuksesta ja eheydestä ongelmatilanteiden sattuessa.

3.5. TIETOJEN SIIRTO KANSAINVÄLISESTI

CSI tai CSI:n alihankkijat eivät siirrä käsittelysopimustemme alaista henkilötietoa Euroopan Unionin tai Euroopan talousalueen ulkopuolelle.

4. CSI:N TOIMINTA TIEDON KÄSITTELIJÄNÄ

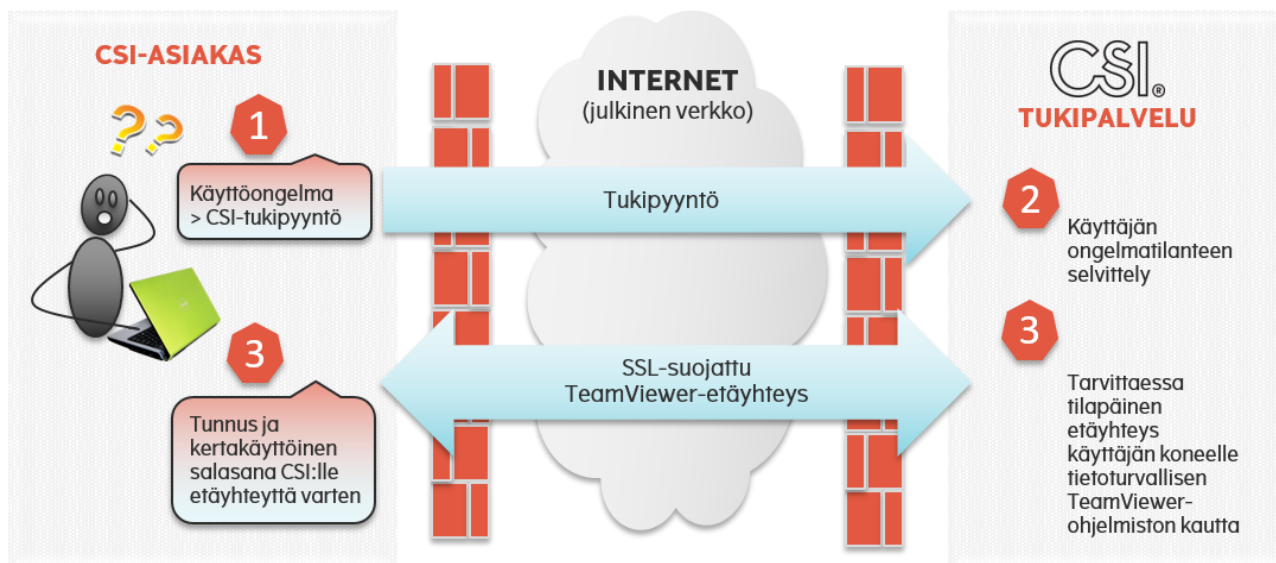
CSI noudattaa seuraavia periaatteita aina asiakkaan tietokantoja tai muita henkilötietoja käsitellessään:

4.1. TIETOJEN KÄSITTELY

CSI käsittelee asiakkaan tietokantoja ja tietoja ainoastaan asiakkaan pyynnöstä ja lukuun. Käsittelemme tietoja aina tietoturvallisesti ja huolellisesti, ja kiinnitämme erityistä huomiota asiakkaan tietojen oikeellisuuden säilymiseen. Asiakkaan tietoja käsittelevät ainoastaan henkilöt, jotka ovat saaneet riittävän koulutuksen tietosuojasta ja tietojen käsittelystä.

4.2. KÄYTETTÄVIEN YHTEYKSIEN TIETOTURVALLISUUS

Ottaessaan yhteyden asiakkaan koneelle tai palvelimelle, CSI käyttää ensisijaisesti käytössään olevaa tietoturvallista yhteyttä, jonka asiakas avaa aina erikseen CSI:n asiantuntijan käyttöön.



Mikäli asiakas haluaa käyttää muuta yhteyttä, asiakas vastaa siitä, että yhteys on tietoturvallinen ja kirjoittaa yhteydestä tarvittavat tiedot lokiin.

Toimittaessaan uusia käyttäjätunnuksia esimerkiksi pilvipalveluasiakkaalle CSI lähettää tunnuksiin liittyvät salasanat aina erillisenä viestinä.

4.3.CSI:LLE SIIRRETTÄVÄT TIETOVARASTOT

Mikäli asiakkaan tietovarasto on siirrettävä CSI:lle esimerkiksi konversiota tai ongelmatilanteen selvittelyä varten, tietojen siirtoon sovitaan aina erikseen tietoturallinen tapa.

Kaikki asiakkaan CSI:lle siirtämät tietovarastot tallennetaan erilliseen tietoturvalliseen palvelinympäristöön, johon on pääsy vain nimetyillä henkilöillä.

4.4.TIETOVARASTOJEN SÄILYTTÄMINEN

CSI ei säilytä mitään asiakkaan tietoja tarpeettomasti. Ellei asiakkaan kanssa sovita muuta, CSI tuhoaa hallussaan olevat tietovarastot viimeistään kolme kuukautta sen jälkeen, kun sovitut tai tarvittavat toimenpiteet on suoritettu ja tiedot käyneet tarpeettomiksi.

CSI voi asiakkaan erillisestä pyynnöstä säilyttää asiakkaan tietovarastoa pidempään esimerkiksi asiakkaan puolesta tehtävää testausta varten. Tässä tapauksessa asiakkaan tietovaraston henkilötiedot voidaan pseudonymisoida tietosuojan varmistamiseksi.

CSI:n hallussa olevista asiakkaan tietovarastoista ei oteta varmuuskopioita.

4.5.PILVIPALVELUASIAKKAAN TIETOVARASTON POISTAMINEN

Mikäli CSI-ohjelmistoa pilvipalveluna käyttänyt asiakas irtisanoo CSI-sopimuksen, CSI pyrkii toimittamaan pilvipalveluun tallennetun tietokannan asiakkaalle. CSI tuhoaa asiakkaan tiedot tietokannan toimittamisen jälkeen tai viimeistään kolme kuukautta sopimuksen irtisanomisen jälkeen.

4.6.ILMOITTAMINEN TIETOTURVALOUKKAUKSISTA

Mikäli CSI havaitsee asiakkaan henkilötietoihin kohdistuneita tietoturvaloukkauksia tai muita henkilötietojen tietoturvallisuutta vaarantavia tapahtumia, CSI ilmoittaa niistä asiakkaalle kirjallisesti ilman aiheetonta viivettä.

5. CSI REKISTERINPITÄJÄNÄ

CSI:n toimintaperiaatteet rekisterinpitäjänä on kuvattu tietosuojaselosteessa, joka löytyy sekä erillisenä dokumenttina että kotisivuiltamme <http://www.csihelsinki.fi/csi-helsinki/tietosuojaseloste/>.

6. CSI:N GDPR-TUKI ASIAKKAILLE

CSI tukee asiakkaita tietosuoja-asetuksen CSI-ohjelmistoihin liittyvissä kysymyksissä sekä CSI:n tietosuoja-ominaisuuksien käytössä.

Tämä dokumentti täydentyy asiakkailta saamiemme kysymysten pohjalta. Tietosuoja-asetukseen liittyvien käytäntöjen tarkentuessa kehitämme CSI-ohjelmistoa asiakkaiden tarpeiden mukaisesti.

Tietosuoja-asetusta koskevia kysymyksiä ja CSI-ohjelmiston kehittämistoiveita voi lähettää CSI-tukeen, tuki@csihelsinki.fi.