



# Tietotilinpäätös 2020

Creamailer Oy

**Creamailer Oy**

info@creamailer.fi

www.creamailer.fi

Y-tunnus: 2255533-0



# Sisällysluettelo

<b>Tietosuojavastaavan tervehdys .....</b>	<b>4</b>
<b>Keskeiset käsitteet.....</b>	<b>5</b>
<b>Lainsäädännön muutokset .....</b>	<b>7</b>
<b>Rekisterinpitäjän velvoitteet ja vastuut.....</b>	<b>8</b>
Tietosuojavastaava .....	8
Riskipohjainen lähestymistapa ja vaikutustenarviointi .....	8
Henkilötietojen käsittelyn osoitusvelvollisuus.....	9
Henkilötietojen käsittelijä .....	9
Oletusarvoinen ja sisäänrakennettu tietosuojaja .....	10
Rekisteröidyn oikeudet .....	10
Henkilötietojen käsittelyn läpinäkyvyys .....	11
Pääsy tietoihin ja tietojen siirto .....	11
Oikeus tietojen oikaisuun ja käsittelyn rajoittamiseen.....	11
Vastustamisoikeus ja oikeus tulla unohdetuksi.....	12
<b>Tietosuojaja ja osaamisen kehittäminen .....</b>	<b>13</b>
<b>Tietosuojan kokonaisuuden hallinta .....</b>	<b>14</b>
<b>Creamailerin hallussa olevat tietovarannot.....</b>	<b>14</b>
Creamailerin omat tietovarannot .....	14
Asiakkaiden tuomat tietovarannot .....	15
<b>Creamailerin tietoarkkitehtuuri .....</b>	<b>15</b>
Tietoturvan hallinta, tekninen tietoturva ja tiedon suojaaminen.....	15
Palvelimien sijainti.....	16
Palvelimiin pääsy .....	16
Käyttöoikeuksien hallinta .....	16
Tietoturva mukana palvelujen kehittämisessä .....	17
Tietoturvatapahtumat.....	17
Riskienhallinta ja jatkuvuus.....	17
Asiakkaat ja kumppanit.....	18
<b>Creamailerin tietosuojakäytänteet pähkinänkuoressa .....</b>	<b>19</b>

# Tietosuojavastaavan tervehdys

Creamailer Oy:n tietotilinpäätöksessä kuvataan, kuinka tietosuojaa ja tietoturvaa on toteutettu. Tilinpäätöksellä vastataan EU:n tietosuoja-asetuksen (GDPR) edellytykseen siitä, että organisaatiot kertovat avoimesti tietojensa käsittelystä. Lisäksi luodaan katsaus siihen, miten toimintaa on kehitetty.

Kotimainen Creamailer on toimintansa alusta alkaen toiminut kansainvälisten hyvien käytänteiden ja vaatimusten mukaisesti ennakkoiden Euroopassa muuttuvat lait, jotka tulevat vaikuttamaan huomattavissa määrin sähköisen viestinnän toteuttamiseen Suomessa. Creamailer seuraa aktiivisesti lainsäädäntömuutoksia ja niiden kehittymistä sekä tiedottaa muutoksista myös asiakkaitaan.

Creamailerin toiminta ja arvot perustuvat lakien ja hyvien käytänteiden noudattamiseen, avoimuuteen, rehellisyyteen sekä kestäväen kehityksen ja yhteiskuntavastuun periaatteisiin. Toimintamme keskiössä on arvon tuottaminen asiakkaalle sekä vastavuoroiset ja pitkäkestoiset asiakassuhteet.

Toteutamme toimintaamme joustavasti, tehokkaasti ja tuloksellisesti asiakkaiden tarpeet huomioiden. Sitoudumme asiakassuhteisiimme ja olemme valmiita panostamaan jokaisen asiakkaan tyytyväisyyteen. Toimintamme peruspilarit rakentuvat asiakasarvolähtöisestä palvelukulttuurista, asiantuntijuudesta sekä kehittymis- ja kehittämishalusta.

Creamailer Oy:n missiona on tarjota viestintäpalvelu, jonka avulla yritykset, järjestöt ja yhteisöt voivat toteuttaa viestintää helposti nopeasti sekä ympäristöystävällisesti. Tavoitteena on luoda asiakkaille lisäarvoa panostamalla tehokkaaseen kustannusrakenteeseen, palvelun laatuun sekä asiakaskokemukseen.

Helsingissä 17.2.2021

tietosuojavastaava

*Jami Pietilä*

# Keskeiset käsitteet

## **Rekisteri**

Tiettyä käyttötarkoitusta varten koottu ja järjestetty henkilötietoja sisältävä tietojoukko tai tietovaranto.

## **Rekisterinpitäjä**

Rekisterinpitäjällä on määräysvalta rekistereissä oleviin tietoihin ja niiden hyödyntämiseen. Rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään säädösten mukaisesti. Käsite ”rekisterinpitäjä” on määritelty henkilötietolaissa.

## **Rekisteröity**

Rekisteröity on luonnollinen henkilö, jota henkilötieto koskee.

## **Henkilörekisteri**

Henkilörekisteri määrittellään henkilötietolaissa (523/1999) henkilötietoja sisältäväksi tietojoukoksi, jota käsitellään automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia.

## **Tietovaranto**

Tietovarannon tietojenhallinta on organisoitu ja vastuutettu yhdelle toimijalle. Se on toiminnan tarpeista johdettu ja hallinnollisista syistä määritelty tietojen kokonaisuus, jotta tiedot olisivat paremmin hallittavissa. Tietovaranto kattaa yhteisesti hallinnoidun joukon tietoja, joista muodostuu looginen kokonaisuus.

## **Henkilötieto**

Luonnollista henkilöä koskeva tieto, joka on tunnistettua ja tunnistettavissa olevaa.

## **Käsittelijä**

Henkilötietoja käsittelevä taho, joka käsittelee tietoa rekisterinpitäjän lukuun.

**Käsittely**

Henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin kohdistettuja toimintoja. Kyseisiä toimintoja ovat esimerkiksi tietojen säilyttäminen, kerääminen, tallentaminen ja muokkaaminen.

**Suostumus**

Tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn.

# Lainsäädännön muutokset

Viestintätoimien digitalisoitumisen johdosta tietoon, tietosuojaan ja tietoturvaan liittyvät asetukset ja lainsäädäntö elävät muutoksessa. Muutokset vaikuttavat myös Creamailerin sekä asiakkaidemme toimintaan. Creamailer on käyttöehdoissaan huomionnut kansainvälisesti tiukentuvan tietosuojatrendin jo toimintansa alusta lähtien, joten tilanne muutosten kynnyksellä on lähtökohtaisesti vakaalla pohjalla.

Yksi keskeisistä meitä ja asiakkaitamme koskevista muutoksista on EU:n tietosuoja-asetusta, eli General Data Protection Regulationia (GDPR) koskeva uudistus. Tietosuoja-asetuksen soveltaminen alkoi 25.5.2018, jolloin henkilötietojen käsittelyn tuli olla toteutettu tietosuoja-asetuksen mukaisesti.

Uuden tietosuoja-asetuksen tarkoituksena oli yhdenmukaistaa EU:n jäsenvaltioiden tietosuoja koskevat säännökset ja ajantasaistaa tietosuoja teknologisen kehityksen ja globalisaation vaatimusten mukaiseksi. Asetuksen tarkoituksena oli myös lisätä henkilötietojen käsittelyn läpinäkyvyyttä, vahvistaa rekisteröityjen oikeuksia ja valvoa henkilötietojen käsittelyä.

Tietosuoja-asetus päivitti nykyistä, Suomessa henkilötietolakiin perustuvaa tietosuojasääntelyä, lisäämällä sääntelyn määrää. Vaikka tietosuoja-asetus rakentui henkilötietolaissa olevien tuttuun periaatteiden varaan, henkilötietoja käsittelevien tahojen vastuu kasvoi, yksilön oikeudet vahvistuivat ja tietosuojaviranomaisten toimivalta lisääntyi. Näin ollen uusi tietosuoja-asetus loi uusia velvoitteita rekisterinpitäjälle ja lisää oikeuksia rekisteröidylle.

Uusi tietosuoja-asetus koskee kaikkia julkisella ja yksityisellä sektorilla toimivia organisaatioita ja toimijoita, jotka käsittelevät henkilötietoja. Asetusta sovelletaan tietyissä tilanteissa myös EU:n ulkopuolelle sijoittuneisiin organisaatioihin. Tällaisia ovat esim. yritykset, jotka tarjoavat palveluita EU:ssa oleville kuluttajille.

# Rekisterinpitäjän velvoitteet ja vastuut

## Tietosuojavastaava

Creamailer Oy:n tietosuojavastaavana toimii ohjelmistokehittäjä Jami Pietilä.

Tietosuojavastaavan tehtäviin kuuluu esimerkiksi seurata organisaation tietojenkäsittelyyn liittyviä toimintatapoja ja huolehtia, että ne vastaavat asetuksessa tai muualla lainsäädännössä säädettyjä vaateita.

Tietosuojavastaava auttaa ja ohjaa organisaatiota tietosuojaperiaatteiden ja –vaatimusten toteuttamisessa. Lisäksi tietosuojavastaava toimii yhteyshenkilönä rekisteröityihin ja valvontaviranomaiseen. Creamailerissa tietosuojavastaava huolehtii myös tietoturvan mittaamisesta, todentamisesta ja kehittämisestä.

## Riskipohjainen lähestymistapa ja vaikutustenarviointi

Tietosuoja-asetus perustuu riskipohjaiseen lähestymistapaan, joka tarkoittaa sitä, että henkilötietojen käsittelyyn liittyvät riskit rekisteröidyn oikeuksille ja vapauksille on arvioitava etukäteen ennen henkilötietojen käsittelyn aloittamista (Privacy Impact Assessment, PIA). Riskejä ovat henkilötietojen käsittelytavat, jotka voivat aiheuttaa rekisteröidylle fyysisiä, aineellisia tai aineettomia vahinkoja kuten identiteettivarkauteen, petokseen, taloudellisiin menetyksiin tai syrjintään liittyviä vahinkoja.

Tietosuoja-asetus määrää myös tietosuojaa koskevasta vaikutustenarviointista (Data Protection Impact Assessment, DPIA) ja tähän mahdollisesti liittyvästä valvontaviranomaisen ennakkoluulemisesta.

Rekisterinpitäjän tulee tehdä vaikutustenarviointi tilanteissa, joissa henkilötietojen käsittelyyn liittyy korkea riski. Kyseisiä tilanteita ovat esimerkiksi tilanteet, joissa käsitellään mm. rekisterissä olevien terveydentilatietoja tai rikostuomioita. Käytännössä vaikutustenarviointi tarkastelee suunniteltuja henkilötietojen käsittelytoimia ja menettelytapoja, sillä varmistetaan henkilötietojen suoja sekä pienennetään käsittelyn riskejä.



Jos vaikutustenarviointi osoittaa riskin olevan korkea eikä rekisterinpitäjä ole tehnyt toimenpiteitä riskin pienentämiseksi, tulee rekisterinpitäjän kuulla valvontaviranomaisia ennen käsittelyn aloittamisesta. Kyse on tällöin riskiperustaisesta ilmoitusvelvollisuudesta.

Creamailer Oy:llä on räätälöity tietosuojariskien hallintaprosessi, joka arvio henkilötietojen käsittelyyn liittyviä riskejä sekä riskeihin liittyviä ja niiden vaativia toimenpiteitä. Vaikutustenarviointi määrittyy Creamailerissa esimerkiksi tietosuoja koskevien elementtien tietoturvatestauksena.

## Henkilötietojen käsittelyn osoitusvelvollisuus

Creamailerin on osoitettava ja dokumentoitava henkilötietojen käsittelyyn liittyvät prosessit ja käytännön tietosuojatoimenpiteet, joilla Creamailer toteuttaa tietosuoja-asetuksen vaatimuksia henkilötietojen käsittelyssä. Kyseinen osoitusvelvollisuus lisää tietosuojatoimien suunnitelmallisuutta ja läpinäkyvyyttä sekä vahvistaa lainsäädännön edellyttämää henkilötietojen käsittelyn suunnitteluvastuuta. Kyseistä vastuuta voidaan näyttää toteen henkilötietojen käsittelyyn liittyvien prosessien dokumentoinnilla, henkilötietojen käsittelytoimista annettavalla selosteella ja eri käyttötarkoituksia ja käsittelytoimia koskevilla käytännesäännöillä. Creamailerin henkilörekistereiden rekisteriselosteet ja käytännesäännöt vastaavat tietosuoja-asetuksen vaatimuksia.

## Henkilötietojen käsittelijä

Henkilötietojen käsittelijällä tarkoitetaan henkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tietosuoja-asetus velvoittaa rekisterinpitäjän solmimaan sopimuksen henkilötietojen käsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Henkilötietojen käsittelijä on vastuussa siitä, että se noudattaa tietojen käsittelyssä tietosuoja-asetuksen vaatimuksia. Creamailerilla on nimetty asiakkuuksiin liittyvä henkilötietojen käsittelijä, joka

huolehtii tietosuojasetusten vaatimusten toteutumisesta. Creamailer Oy:llä ei ole ulkopuolisia henkilötietojen käsittelijöitä.

## Oletusarvoinen ja sisäänrakennettu tietosuojajaperiaate

Oletusarvoinen ja sisäänrakennettu tietosuojajaperiaate tarkoittaa, että tietosuojajaperiaatteet otetaan huomioon jo henkilötietojen käsittelyä suunniteltaessa. Henkilötietojen suojaamista koskevat suojaustoimet sisällytetään osaksi henkilötietojen käsittelyprosessia heti alkuvaiheessa. Tällöin huomioidaan henkilötietojen käsittelyn luonne, laajuus ja asiayhteydet sekä tarkoitukset. Lisäksi huomioidaan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvat riskit. Kyseinen velvoite koskee kerättyjen tietojen määrää, käsittelyn laajuutta, tietojen säilytysaikaa ja saatavilla oloa.

Creamailerissa tietosuojajaperiaate toteutuu sisäisten menettelykäytänteiden, ohjeistusten sekä koulutusten kautta. Creamailerissa on käytössä vahvat kehittämis- ja projektityön käytänteet, jotka sisältävät elinkaariajattelun mallin, joihin sisällytetään tietosuojajaperiaate- ja tietoturvamäärittelyt. Käytännössä tämä tarkoittaa sitä, että kehittämis- ja projektityön suunnitteluvaiheessa huomioidaan kunkin kohteen osalta käsiteltävät henkilötiedot ja määritellään niiden elinkaari. Creamailer huolehtii tietosuojajaperiaatteiden täyttymisestä omien asiakasrekisteriensä kohdalla. Tietosuojajaperiaatteet ovat kiinteä osa Creamailerin toimintaa ja vastaamme omalta osaltamme henkilötietolain mukaisista suunnittelu- ja huolellisuusvelvoitteista.

## Rekisteröidyn oikeudet

Rekisteröidyn oikeudet korostuvat osana Creamailerin velvollisuuksia. Rekisteröidyn oikeuksilla tarkoitetaan rekisteröidyn osallistamista tietojensa käsittelyyn, lisäämään käsittelytoimien läpinäkyvyyttä ja antaa rekisteröidylle mahdollisuus päättää tietojensa käsittelystä. Tietosuojajaperiaate täsmentää ja tiukentaa rekisteröidyn oikeuksia nykysääntelyä yksityiskohtaisemmin ja tuo Creamaileriin prosesseja, joilla oikeudet toteutetaan. Rekisteröidyillä on oikeus saada itseään koskevat tiedot ja muuttaa niitä milloin tahansa.

## Henkilötietojen käsittelyn läpinäkyvyys

Rekisteröidyn oikeuksien toteuttamisen lähtökohtana on oikeuksista informointi. Henkilötietojen käsittelyn tulee olla avointa ja ymmärrettävää. Informointivelvoite sisältyy myös henkilötietolakiin, mutta tietosuoja-asetus tarkentaa ja laajentaa henkilötietolaissa säädettyjä velvoitteita. Creamailerilla on olemassa henkilötietolain mukaiset rekisteriselosteet Creamailerin ylläpitämistä henkilörekistereistä. Creamailerin kotisivuilta löytyy ajantasainen rekisteriseloste ja tiedot sen tietosisällöstä ja käyttötarkoituksesta.

## Pääsy tietoihin ja tietojen siirto

Tietosuoja-asetuksen myötä rekisteröidyllä on tehostettu oikeus omiin tietoihin pääsyyn. Pyynnön voi asetuksen myötä tehdä muutoinkin kuin kirjallisella ja allekirjoitetulla pyynnöllä. Creamailerilla on kuitenkin velvollisuus tunnistaa tietojen pyytjä, jottei muiden rekisteröityjen oikeutta loukata. Creamailer pyytää tarvittaessa lisätietoja, jotta rekisteröidyn henkilöllisyys voidaan varmistaa. Creamailer toimittaa rekisteröidyn pyytämät tiedot joko sähköisessä tai muussa muodossa. Creamailer reagoi rekisteröidyn pyyntöön tietosuoja-asetuksen vaatiman ajan puitteissa.

Rekisteröidyllä on oikeus saada häntä koskevat tiedot ja siirtää ne toiselle rekisterinpitäjälle. Käytännössä Creamailer toteuttaa siirtoa vain, jos henkilötietojen käsittelyn oikeusperuste on sopimus- tai suostumusperustainen. Kyseinen oikeus ei saa vaikuttaa haitallisesti muiden rekisteröityjen oikeuksiin.

## Oikeus tietojen oikaisuun ja käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää oikaisemaan häntä koskeva virheellinen tieto tai täydentää puutteelliset tiedot. Creamailerilta voi pyytää tietojen oikaisua tai täydentämistä jatkossa samoin menettelykeinoin kuin aiemminkin. Pyynnöt käsitellään viipymättä.

Rekisteröidyillä on myös oikeus rajoittaa tietojensa käsittelyä. Käytännössä tämä tarkoittaa mahdollisuutta vastustaa ainakin väliaikaisesti henkilötietojen käsittelyä esimerkiksi ristiriitatilanteessa. Kyseisessä tilanteessa Creamailer kunnioittaa rekisteröidyn oikeuksia ja rajoittaa tietojen käsittelyä rekisteröidyn pyytämällä tavalla.

## Vastustamisoikeus ja oikeus tulla unohdetuksi

Rekisteröidyillä on oikeus perustellusti vastustaa henkilötietojen käsittelyä tietyissä käyttötarkoituksissa esimerkiksi suoramainontaa, etämyyntiä, suoramarkkinointia tai tutkimusta varten. Creamailerin asiakasrekisterissä olevia tietoja käytetään vain Creamailerin asiakasviestintää ja tiedottamista varten. Asiakastietoja käytetään asiakassuhteen hoitamiseen eikä Creamailer koskaan lainaa, vuokraa tai myy tietoja kolmansille osapuolille.

Sen lisäksi, että rekisteröidyillä on oikeus vastustaa henkilötietojen käsittelyä, hänellä on myös oikeus pyytää rekisterinpitäjää poistamaan häntä koskevat henkilötiedot. Creamailerissa kaikki asiakkaan tiedot poistetaan välittömästi palvelusta mikäli asiakas sitä pyytää. Asiakastiedot poistetaan myös asiakkaan päättäessä palvelusuhteen. Laskutusyhteystiedot säilytetään sopimuskauden ajan.

# Tietosuoja ja osaamisen kehittäminen

Tietosuojakysymyksissä, niiden suunnittelussa, toteuttamisessa ja seurannassa on keskeistä tunnistaa ja määritellä henkilötietojen käsittelytoimet sekä niiden prosessit. Creamailerilla tietosuoja käsitetään osana jokapäiväistä operatiivista toimintaa, johon on luotu vankat käytänteet.

Creamailerin kehitystyössä huomioidaan vaikutustenarviointi, joka kohdistuu esimerkiksi tietosuoja koskevien elementtien tietoturvatestaukseen. Tällaisia elementtejä ovat myös erilaiset tekniset suojaukset. Tietosuoja on palvelussa sisällytetty myös järjestelmä- ja sovelluskehitykseen sekä projektihallintaan. Kehitystyössä otetaan huomioon työvaiheet, jossa analysoidaan kunkin palvelun osa-alueen tietosuoja vaatimukset. Tekninen toteutus suunnitellaan niin, että se kattaa vaadittavat tietoturva vaatimukset.

Creamailerin henkilökunta koulutetaan jatkuvasti alan kehityksen mukaisesti, joten tietoturva-asiat kuten salaukset ja muut tietoturvaan liittyvät käytänteet, päivitetään aina ajan vaatimusten mukaiseksi. Tietosuoja lasketaan osaksi henkilöstön osaamispääomaa ja Creamailerissa onkin käytössä tieto-osaamisen malli, jolla osaamistarpeita tunnistetaan, kuvataan ja kehitetään Creamailerin strategisten tavoitteiden mukaisesti.

# Tietosuoja kokonaisuuden hallinta

Kansainvälistymisen, digitalisaation ja teknologisen kehittymisen myötä tietoturvan merkitys organisaatioiden suunnittelu, hallinta ja seurantaprosesseissa kasvaa entisestään. Organisaatioiden on pystyttävä tunnistamaan ja reagoimaan muutoksiin, mukautumaan ja mukauttamaan toimintansa muutosten vaatimalla tavalla sekä jopa toimimaan muutosten tekijöinä. Organisaatiokulttuurin ja arkkitehtuurin tulee olla suunniteltua ja täytettävä vaadittavat kriteerit. Näiden lisäksi organisaatiolla tulee olla kokonaisnäkemys ja hallinta omasta toiminnastaan.

## Creamailerin hallussa olevat tietovarannot

Creamailerin tietovarannot koostuvat Creamailerin omista asiakasrekistereistä sekä asiakkaiden palveluun tuomista rekistereistä. Tietovaranto käsittää toiminnan tarpeista määrittynyt ja hallinnollisista syistä johdetut tietojen kokonaisuudet, joita tarvitaan Creamailerin toiminnan ylläpitämisessä.

## Creamailerin omat tietovarannot

Creamailerin omat asiakasrekisterit sisältävät asiakkuussuhteiden ylläpitämisessä tarvittavia tietoja:

- Nimi (\*)
- Yritys (\*)
- Puhelinnumero (\*)
- Sähköpostiosoite (\*)
- Yritystiedot ja laskutustiedot (vain asiakkailta)
  - Y-tunnus \*
  - Laskutustiedot \*
    - Tilaustiedot (tuotteet)
    - Laskutustapa
    - Laskutuskausi
    - Laskutusosoite
    - Mahdolliset muut tiedot, esim. laskutusviite
- Asiakaskäyttäytymistiedot
- Suostumus sähköiseen suoramarkkinointiin

- Asiakkaalta saadut muut tiedot (esim. intressit, arvonta- ja kilpailuvastaukset, reklamaatiot)
- IP-osoite (uutiskirjeen tilaajat, kyselyihin vastanneet)

(\* Vain nämä tiedot ovat pakollisia)

## Asiakkaiden tuomat tietovarannot

Suurin osa Creamailerin tietovarannoista koostuu asiakkaiden tuomista tai keräämistä tietovarannoista kuten postituslistoista ja kyselyvastauksista. Asiakas vastaa itse tuomistaan tietovarannoista.

## Creamailerin tietoarkkitehtuuri

### Tietoturvan hallinta, tekninen tietoturva ja tiedon suojaaminen

Creamailerin tietoturvaan liittyvät toiminnot noudattavat Suomen ja EU:n lainsäädäntöä sekä viranomais määräyksiä. Creamailerin palvelun tiedot sijaitsevat EU:n sisäisillä turvallisilla palvelimilla. Palvelin keskuksen tilat täyttävät Viestintäviraston korkeimman tärkeysluokan 1 vaatimukset: Viestintävirasto 54 B/2014 M (Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista).

Creamailerilla on oma tietosuojariskien hallintaprosessi, joka arvio henkilötietojen tms. käsittelyyn liittyviä riskejä sekä riskeihin liittyviä ja niiden vaativia toimenpiteitä. Toiminnassa käytetään alan parhaita toimijoita niin tietoturvan kuin toimintavarmuudenkin suhteen. Toiminnassa hyödynnetään uusinta tekniikkaa ja seurataan alalla tapahtuvia muutoksia sekä tietoturvarikkomuksia, joihin vastataan aina vaadittavin toimenpitein. Tietovälineet huolletaan ja hävitetään siten, ettei tietoja päädy kolmansille osapuolille. Creamailerilla on käytössään mm. turvalliset palomuurit, verkkojen eriyttäminen sekä siirtoväylien salaus.

Creamailerissa on käytössä palvelujen kahdentaminen käyttökatkojen minimoimiseksi. Palveluun kirjaututaan aina suojatun yhteyden kautta salasanalla. Pääsy Creamailerin palvelimille ja niiden hallinta-paneeliin on turvattu useilla eri varmenteilla, jotka yhdessä takaavat erittäin vahvan tietoturvan. Tietoturvallisuuteen vaikuttavia poikkeamia monitoroidaan ympäristössä 24/7. Creamailerin henkilökunta on koulutettu selvittämään poikkeaman syyt, seuraukset ja vaikutukset sekä estämään poikkeaman leviäminen.

## Palvelimien sijainti

Creamailer käyttää vuodesta 1997 toiminutta Hetzner-pilvipalvelinympäristöä. Palvelimet sijaitsevat Suomessa.

Creamailer käyttää myös Linode-pilvipalvelinympäristöä, jolla on yli 400 000 asiakasta. Linoden palvelimet sijaitsevat Frankfurtissa.

## Palvelimiin pääsy

Palvelimiin on pääsy ainoastaan Creamailerin ohjelmistokehittäjillä ja palvelimien tietoturvasta sekä skaalautuvuudesta vastaavalla Nordic Server Management OÜ:lla. Linoden tai Hetznerin työntekijöillä ei ole pääsyä palvelimien sisältöön.

## Käyttöoikeuksien hallinta

Creamaileriin tuotujen tietojen käsittely on turvattua teknisin ja organisatorisin toimenpitein. Asiakkaan tietoja käytetään vain asiakassuhteen hoitamiseen eikä Creamailer käytä itse, lainaa, vuokraa tai myy tietoja kolmansille osapuolille. Palveluun tuodut tiedot on turvattu ja suojattu muun muassa siirron, tallennuksen ja käsittelyn aikana tuhoamiselta, muuttamiselta, luovuttamiselta sekä pääsylvä.

Asiakkaan Creamaileriin lisäämä data on ainoastaan asiakkaan käytettävissä, eikä Creamailer käytä itse, lainaa, vuokraa tai myy tietoja kolmansille



osapuolille. Tämä ei kuitenkaan koske sähköpostiosoitteiden virheellisyyden, viestinnän perumisen ja roskapostimerkkauksien kautta kertyvää tietoa, jota Creamailer voi käyttää käyttöehtojen vastaisen toiminnan seuraamisen ja sekä palvelun laadun takaamiseen.

## Tietoturva mukana palvelujen kehittämisessä

Tietosuoja on Creamailerissa sisällytetty järjestelmä- ja sovelluskehitykseen sekä projektihallintaan. Tietoturvaan liittyvät vaatimukset sisällytetään Creamailerissa myös uusiin ja päivitettäviin ominaisuuksiin ja järjestelmiin. Tietoturva arvioidaan aina järjestelmää kehitettäessä läpikäyden suunnittelu, toteutus, valvonta- ja arviointiprosessit. Jokaisen kehittämistyön kohdalla arvioidaan vaikutukset Creamailerin toimintoihin, prosesseihin ja turvallisuuteen.

Kehitystyössä huomioidaan myös vaikutustenarviointi, joka kohdistuu esimerkiksi tietosuojaan koskevien elementtien tietoturvatestaukseen. Tällaisia elementtejä ovat myös erilaiset tekniset suojaukset. Tekninen toteutus suunnitellaan niin, että se kattaa vaadittavat tietoturvavaatimukset.

## Tietoturvatapahtumat

Mahdolliset Creamaileriin kohdistuvat tietoturvatapahtumat raportoidaan Creamailerin toimintamallien mukaisesti Creamailerin omaan toimintajärjestelmään. Tapahtumien arvioinnista vastaavat tietoturvavastaava ja ohjelmistokehittäjä, jotka raportoivat ja käsittelevät tapahtumat Creamailerin toimintaprosessien mukaisesti.

## Riskienhallinta ja jatkuvuus

Creamailerin tietoturvariskit kartoitetaan osana Creamailerin riskienhallintaprosessia. Arvioinnin lisäksi riskeille nimetään vastuu ja seurantatahot. Tietojärjestelmiin kohdistuvia riskejä seuraavat ohjelmistokehittäjät. Creamailerilla on oma riskienhallintaprosessi, jota päivitetään ja kehitetään jatkuvasti alan vaatimien muutosten mukaisesti.

## Asiakkaat ja kumppanit

Creamailerista löytyvän API-rajapinnan avulla Creamailer voidaan liittää mihin tahansa järjestelmään. API:n käyttäminen onnistuu ainoastaan salatun HTTPS-yhteyden kautta. Lisäksi jokaisen kutsun yhteydessä lähetetään yhteisen tunnisteen avulla laskettu tarkistussumma. Tämä takaa erittäin hyvän tietoturvan. API-avaimelle voidaan määritellä luku ja/tai kirjoitusoikeus. Avain voidaan myös poistaa suoraan ylläpidosta niin haluttaessa. Asiakas on vastuussa avaimen luovuttamisesta kolmannelle osapuolelle.

# Creamailerin tietosuojakäytänteet pähkinänkuoressa

- Alan parhaiden toimijoiden käyttäminen niin tietoturvan kuin toimintavarmuudenkin suhteen.
- Uusimman tekniikan käyttäminen ja alalla tapahtuvien muutosten ja tietoturvarikkomusten seuraaminen.
- Tietovälineiden turvallinen huolto ja hävittäminen.
- Turvalliset palomuurit, verkkojen eriyttäminen sekä siirtoväylien salaus.
- palvelun tiedot sijaitsevat EU:n sisäisillä, turvallisilla palvelimilla. Toiminnassa noudatetaan Suomen ja EU:n lakeja ja asetuksia. Palvelinkeskuksen tilat täyttävät Viestintäviraston korkeimman tärkeysluokan 1 vaatimukset: Viestintävirasto 54 B/2014 M (Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista).
- Tietoturvallisuudesta huolehtiminen ja muutosten hallinta järjestelmien päivitysten yhteydessä.
- Palvelujen kahdentaminen käyttökatkojen minimoimiseksi.
- Palveluun kirjaututaan salasanalla, suojatun yhteyden kautta.
- Pääsy Creamailerin palvelimille ja niiden hallintapaneeliin on turvattu useilla eri varmenteilla, jotka yhdessä takaavat erittäin vahvan tietoturvan.
- Henkilöstön osaaminen pidetään ajan tasalla erilaisin koulutuksin ja ohjeistuksin. Henkilökunnalla on vaitiolo- ja salassapitovelvollisuus.
- Tietoturvallisuuteen vaikuttavia poikkeamia monitoroidaan. Henkilökunta on koulutettu selvittämään poikkeaman syyt, seuraukset ja vaikutukset sekä estämään poikkeaman leviäminen.
- Creamailerilla on nimetty tietosuojavastaava, joka huolehtii tietoturvan hallintatehtävistä. Tietosuojavastaava huolehtii myös tietoturvan mittaamisesta, todentamisesta ja kehittämisestä yhdessä muiden työntekijöiden kanssa.