



Tietotilinpäätös 2024

Creamailer Oy

Creamailer Oy

info@creamailer.fi

www.creamailer.fi

Y-tunnus: 2255533-0

Tietosuojavastaavan tervehdys

Vuosi 2024 on ollut Creamailerille merkittävä kehityksen ja turvallisuuden vuosi. Olemme siirtäneet palvelimemme Helsingin alueelle, Hetznerin moderniin datakeskukseen, mikä parantaa tietoturvaa ja varmistaa nopean pääsyn dataan kaikissa olosuhteissa. Lisäksi varmuuskopiot tallennetaan UpCloudin Helsingin datakeskukseen, mikä tuo lisävarmuutta ja takaa tietojen saatavuuden kaikissa tilanteissa.

Tietoturva on Creamailerille ensisijainen prioriteetti. Olemme päivittäneet käyttöjärjestelmän sekä keskeiset ohjelmistot vastaamaan nykypäivän tiukimpia tietoturvakäytänteitä.

Tekoälyn kehitys tuo mukanaan sekä uusia mahdollisuuksia että haasteita, minkä vuoksi pidämme erityistä huolta ohjelmistoversioiden ja tietoturvatarkistusten ajantasaisuudesta. Tämä koskee niin käyttöliittymäämme, ohjelmistoja kuin käytössä olevia kirjastoja, joiden määrän pidämme hallitusti minimissä.

Vuoden 2024 keskeisimpiä tavoitteita oli tietoturvarutiinien vakiinnuttaminen ja tukeminen monipuolisilla työkaluilla ja käytännöillä. Tämä kehitysprojekti eteni suunnitellusti ja jatkuu myös tulevaisuudessa tavoitteenaan luoda entistä turvallisempi ja luotettavampi ympäristö asiakkaillemme. Näin varmistamme, että Creamailer on aina proaktiivisesti valmiina vastaamaan digitaalisen maailman jatkuviin muutoksiin ja asiakkaidemme korkeisiin tietoturvavaatimuksiin.

Helsingissä 1.4.2025

tietosuojavastaava

Jami Pietilä

SISÄLLYSLUETTELO

TIETOSUOJAVASTAAVAN TERVEHDYS.....	2
KESKEISET KÄSITTEET	4
LAINSÄÄDÄNNÖN MUUTOKSET JA VAIKUTUKSET.....	5
REKISTERINPITÄJÄN VELVOITTEET JA VASTUUT.....	7
Tietosuojavastava	7
Riskipohjainen lähestymistapa ja vaikutustenarviointi	8
Henkilötietojen käsittelyn osoitusvelvollisuus	9
Henkilötietojen käsittelijä	9
Oletusarvoinen ja sisäänrakennettu tietosuoja.....	9
REKISTERÖIDYN OIKEUDET	11
Henkilötietojen käsittelyn läpinäkyvyys	11
Pääsy tietoihin ja tietojen siirto	11
Oikeus tietojen oikaisuun ja käsittelyn rajoittamiseen.....	12
Vastustamisoikeus ja oikeus tulla unohdetuksi.....	12
TIETOSUOJAN HALLINTA JA KEHITTÄMINEN.....	13
Tietosuoja ja osaamisen kehittäminen	13
Tietosuojan kokonaisuuden hallinta.....	13
TIETOVARANNOT JA TIETOARKKITEHTUURI.....	14
Creamailerin hallussa olevat tietovarannot	14
Asiakkaiden tuomat tietovarannot	14
TIETOTURVAN HALLINTA JA TEKNISET RATKAISUT	16
Palvelimien sijainti ja niihin pääsy	17
Creamailerin alihankkijat	17
Evästeet	18
Käyttöoikeuksien hallinta.....	19
Tietoturva osana kehitystyötämme	20
Tietoturvatapahtumat.....	20
Riskienhallinta ja jatkuvuus	20
API-rajapinta ja tietoturva.....	21
TIETOSUOJAKÄYTÄNTEET PÄHKINÄNKUORESSA	22

Keskeiset käsitteet

Rekisteri

Henkilötietoja sisältävä tietokokonaisuus, joka on koottu ja järjestetty tiettyä käyttötarkoitusta varten.

Rekisterinpitäjä

Organisaatio tai henkilö, joka määrittää henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä vastaa tietojen lainmukaisesta käsittelystä.

Rekisteröity

Luonnollinen henkilö, jonka henkilötietoja käsitellään rekisterissä, kuten asiakas, työntekijä tai muu rekisteröity henkilö.

Henkilötieto

Kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön, kuten nimi, osoite, sähköpostiosoite tai IP-osoite.

Henkilörekisteri

Henkilötietoja sisältävä tietojoukko, joka on järjestetty siten, että tiedot ovat helposti löydettävissä ja käytettävissä.

Käsittelijä

Henkilötietoja käsittelevä taho, joka käsittelee tietoa rekisterinpitäjän lukuun.

Käsittely

Kaikki henkilötietoihin kohdistuvat toimet, kuten kerääminen, tallentaminen, muokkaaminen, siirtäminen ja poistaminen.

Suostumus

Tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn.

Tietovaranto

Jäsennelty ja vastuullisesti hallintoitu tietokokonaisuus, joka on muodostettu organisaation toiminnan tarpeisiin. Tietovaranto koostuu yhteisesti hallituista tiedoista, jotka muodostavat loogisen kokonaisuuden ja helpottavat tiedonhallintaa.

Lainsäädännön muutokset ja vaikutukset

Viestinnän digitalisoituminen muuttaa jatkuvasti tietosuoja- ja tietoturvaa koskevaa lainsäädäntöä. Nämä muutokset vaikuttavat sekä meidän toimintaamme että asiakkaidemme arkeen. Vuoden 2024 aikana useat lainsäädännölliset uudistukset muokkasivat toimintaympäristöämme.

Euroopan unionin yleistä tietosuoja-asetusta (GDPR) on päivitetty vastaamaan teknologian kehityksestä syntyviä uusia vaatimuksia. Uudet säädökset ovat tiukentaneet henkilötietojen käsittelyn sääntelyä ja tarkentaneet rekisterinpitäjien vastuuta. Olemme reagoineet muutoksiin päivittämällä sisäisiä prosessejamme ja tietoturvakäytäntöjamme varmistaaksemme, että henkilötietoja käsitellään aina ajantasaisen lainsäädännön mukaisesti ja tietoturvallisesti.

Tekoälyn merkityksen kasvaessa sen sääntely on noussut entistä suurempaan rooliin. Vuonna 2024 Euroopan unioni otti käyttöön tekoälyä koskevia sääntelytoimia, jotka painottavat muun muassa läpinäkyvyyttä, vastuullisuutta ja tietoturvaa. Vastasimme näihin vaatimuksiin tarkentamalla tekoälyn käyttöön liittyviä toimintatapoja ja varmistamalla, että kaikki tekoälyä hyödyntävät ratkaisut täyttävät uusimmat sääntelyvaatimukset. Lainsäädäntömuutosten myötä olemme tehneet useita kehitysaskelleita varmistaaksemme palveluiden tietoturvallisuuden ja lainmukaisuuden:

- **Tietoturva- ja tietosuojakäytännöt on päivitetty** vastaamaan ajankohtaisia säädöksiä. Erityistä huomiota on kiinnitetty käyttöjärjestelmien ja ohjelmistojen ajantasaisuuteen, jotta kaikki käytössä olevat ratkaisut täyttävät uudet vaatimukset.
- **Ohjelmistoversioiden ja tietoturvatarkistusten hallintaa on tiukennettu.** Uudet rutiinit mahdollistavat nopean reagoinnin sekä tietoturvauhkien että sääntelymuutosten osalta.
- **Tekoälyn käyttöä ohjaavia periaatteita on selkeytetty ja vahvistettu.** Olemme panostaneet läpinäkyvyyteen ja vastuullisuuteen varmistaaksemme, että asiakkaidemme tietosuoja ja tietoturva toteutuvat korkealla tasolla myös tekoälyä hyödyntävissä ratkaisuissa.

Seuraamme aktiivisesti tietosuojan ja tietoturvan liittyvän lainsäädännön kehitystä ja pidämme asiakkaamme ajan tasalla muutoksista. Olemme sitoutuneet noudattamaan tiukimpia käytäntöjä ja varmistamaan, että palvelumme pysyvät turvallisina ja luotettavina myös tulevaisuudessa.

Rekisterinpitäjän velvoitteet ja vastuut

Tietosuojavastaava

Tietosuojavastaava on keskeinen toimija tietosuojaan ja tietoturvan varmistamisessa. Hänen tehtävänä on huolehtia siitä, että henkilötietojen käsittely noudattaa voimassa olevaa lainsäädäntöä ja parhaita käytänteitä. Creamailerin tietosuojavastaavana toimii ohjelmistokehittäjä Jami Pietilä.

Tietosuojavastaava varmistaa, että tietosuojakäytäntömme ovat ajan tasalla ja vastaavat voimassa olevaa lainsäädäntöä, kuten EU:n yleistä tietosuoja-asetusta (GDPR).

Tietosuojavastaava seuraa lainsäädännön muutoksia ja mukauttaa käytäntöjä niiden mukaisesti. Keskeisiä tehtäviä ovat:

1. Henkilöstön koulutus ja ohjeistus

Tietosuojavastaava vastaa henkilöstön tietosuojakoulutuksesta ja laatii ohjeistuksia, jotka tukevat tietosuojakäytäntöjen noudattamista arjen työssä. Tavoitteena on varmistaa, että jokainen työntekijä ymmärtää tietosuojaan liittyvät vastuut ja velvollisuudet.

2. Tietoturvan mittaaminen ja kehittäminen

Tietosuojavastaava valvoo tietoturvakäytäntöjen toteutumista ja osallistuu säännöllisiin tietoturvatestauksiin. Hän varmistaa, että prosessit, kuten tietosuojaan koskevat vaikutustenarviointit (DPIA), tehdään ajallaan ja että mahdolliset puutteet korjataan viipymättä.

3. Tietosuoja vaikutusten arviointi (DPIA)

Korkean riskin käsittelytoimissa tietosuoja vaikutusten arviointi on keskeinen työkalu riskien hallintaan. Tietosuojavastaava johtaa ja koordinoi näitä arviointeja varmistaakseen, että toimintamme on turvallista ja lainmukaista.

4. Rekisteröityjen oikeuksien toteuttaminen

Tietosuojavastaava toimii ensisijaisena yhteyshenkilönä rekisteröidyille. Hän käsittelee esimerkiksi tietopyyntöjä ja vastustamispyyntöjä, sekä varmistaa, että toimintamme on läpinäkyvää ja rekisteröityjen oikeudet toteutuvat käytännössä.

5. Yhteistyö valvontaviranomaisten kanssa

Tietosuojavastaava toimii yhteyshenkilönä viranomaisiin, kuten tietosuojavaltuutetun toimistoon. Hän vastaa mahdollisiin tietopyyntöihin ja raportoi tietoturvaloukkauksista tarvittavin toimin ja aikatauluin.

Riskipohjainen lähestymistapa ja vaikutustenarviointi

Tietosuojasetus perustuu riskipohjaiseen lähestymistapaan, mikä tarkoittaa, että meidän on arvioitava henkilötietojen käsittelyyn liittyvät riskit rekisteröidyn oikeuksille ja vapauksille jo ennen käsittelyn aloittamista. Arviointiprosessia kutsutaan tietosuojavaikutusten arvioinniksi (Data Protection Impact Assessment, DPIA).

Tällaisia riskejä voivat olla esimerkiksi henkilötietojen käsittelytavat, jotka saattavat aiheuttaa rekisteröidylle fyysisiä, taloudellisia tai henkisiä haittoja, kuten identiteettivarkauksia, petoksia, taloudellisia menetyksiä tai syrjintää.

Tietosuojasetus edellyttää, että vaikutustenarviointi tehdään aina, kun henkilötietojen käsittelyyn liittyy todennäköisesti korkea riski.

Vaikutustenarvioinnissa tarkastelemme suunniteltuja henkilötietojen käsittelytoimia ja käytäntöjä ennakoivasti. Tavoitteena on varmistaa tietojen suoja ja tunnistaa sekä pienentää mahdollisia riskejä ennen käsittelyn aloittamista. Mikäli arvioinnissa ilmenee, että riski jää edelleen korkeaksi, eikä käytössä ole riittäviä toimenpiteitä riskin pienentämiseksi, olemme velvollisia kuulemaan valvontaviranomaista ennen henkilötietojen käsittelyn aloittamista. Tämä on osa riskiperustaista ilmoitusvelvollisuutta.

Meillä on käytössämme oma, räätälöity tietosuojariskien hallintaprosessi, jonka avulla arvioimme henkilötietojen käsittelyyn liittyviä riskejä ja määrittelemme tarvittavat toimenpiteet niiden hallitsemiseksi. Käytännössä vaikutustenarviointi näkyy esimerkiksi tietosuojaan liittyvien teknisten ratkaisujen, kuten järjestelmien tietoturvatestauksen kautta.

Henkilötietojen käsittelyn osoitusvelvollisuus

Olemme velvollisia osoittamaan ja dokumentoimaan, miten henkilötietoja käsitellään palvelussamme. Tietosuojatoimenpiteet ja -prosessit suunnitellaan ja toteutetaan niin, että ne täyttävät EU:n yleisen tietosuoja-asetuksen (GDPR) vaatimukset.

Osoitusvelvollisuus lisää toiminnan suunnitelmallisuutta ja läpinäkyvyyttä sekä tukee henkilötietojen käsittelyn huolellista suunnittelua, kuten lainsäädäntö edellyttää.

Velvollisuuden täyttyminen osoitetaan dokumentoimalla henkilötietojen käsittelyprosessit, laatimalla käsittelytoimien selosteet sekä määrittelemällä selkeät käytäntesäännöt eri käyttötarkoituksia ja käsittelytilanteita varten.

Kaikki rekisteriselosteemme ja käytäntesääntömme on laadittu tietosuoja-asetuksen mukaisesti ja pidetään jatkuvasti ajan tasalla. Näin varmistamme, että henkilötietojen käsittely tapahtuu lainmukaisesti, vastuullisesti ja läpinäkyvästi.

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. Meillä on nimetty asiakkuuksiin liittyvä henkilötietojen käsittelijä, joka huolehtii tietosuoja-asetusten vaatimusten toteutumisesta.

Voimme tarvittaessa käyttää ulkopuolisia henkilötietojen käsittelijöitä, esimerkiksi palveluntarjoajia, jotka tukevat teknisiä tai toiminnallisia prosessejamme. Tällaisissa tilanteissa varmistamme, että henkilötiedot pysyvät turvassa. Solmimme aina kirjallisen sopimuksen ulkopuolisen käsittelijän kanssa, joka varmistaa, että käsittely tapahtuu ainoastaan sovittuun tarkoitukseen ja tietosuoja-asetuksen vaatimuksia noudattaen.

Oletusarvoinen ja sisäänrakennettu tietosuoja

Oletusarvoinen ja sisäänrakennettu tietosuoja tarkoittavat meille sitä, että tietosuojaperiaatteet huomioidaan jo henkilötietojen käsittelyn suunnitteluvaiheessa.

Tietosuoja ei ole meille erillinen osa järjestelmää tai prosessia, vaan se sisällytetään toimintaamme heti alusta alkaen.

Suunnittelussa otamme huomioon henkilötietojen käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen. Arvioimme myös mahdolliset riskit, joita käsittely voi aiheuttaa rekisteröidyn oikeuksille ja vapauksille. Velvoitteet koskevat esimerkiksi kerättävien tietojen määrää, käsittelyn laajuutta, säilytysaikaa ja tietojen saatavuutta.

Toteutamme tietosuojan osana sisäisiä toimintamallejamme, ohjeistuksia ja henkilöstön säännöllistä koulutusta. Käytössämme on vahvat kehittämis- ja projektityön käytännöt, jotka perustuvat elinkaariajatteluun. Sisällytämme näihin systemaattisesti tietosuoja- ja tietoturva-vaatimukset. Käytännössä tämä tarkoittaa, että kehitys- ja projektityön suunnitteluvaiheessa kartoitamme käsiteltävät henkilötiedot, määrittelemme niiden käyttötarkoituksen ja elinkaaren, sekä arvioimme niihin liittyvät tietosuojariskit.

Varmistamme tietosuojavaatimusten toteutumisen kaikissa omissa asiakasrekistereissämme ja huolehdimme siitä, että tietosuojaperiaatteet ovat kiinteä osa kaikkea toimintaamme. Näin täytämme myös henkilötietolain ja EU:n tietosuoja-asetuksen mukaiset suunnittelu- ja huolellisuusvelvoitteet.

Rekisteröidyn oikeudet

Rekisteröidyn oikeudet ovat keskeinen osa tietosuojavastuutamme. Niiden avulla lisäämme henkilötietojen käsittelyn läpinäkyvyyttä, vahvistamme rekisteröidyn asemaa ja mahdollistamme osallistumisen omien tietojensa käsittelyyn.

EU:n yleinen tietosuoja-asetus (GDPR) täsmentää ja vahvistaa rekisteröidyn oikeuksia yksityiskohtaisemmin kuin aiempi lainsäädäntö. Näiden oikeuksien toteuttaminen on olennainen osa vastuullista tietosuojatyötämme. Rekisteröidyllä on oikeus saada tietoa siitä, mitä henkilötietoja hänestä käsittelemme, tarkastella, oikaista ja täydentää tietojaan, pyytää tietojen poistamista tai rajoittaa niiden käsittelyä. Lisäksi rekisteröity voi tietyissä tilanteissa vastustaa tietojensa käsittelyä.

Käytössämme on selkeät ja toimivat prosessit, joiden avulla varmistamme rekisteröidyn oikeuksien toteutumisen. Rekisteröity voi koska tahansa olla meihin yhteydessä ja pyytää tietoa omasta tietojenkäsittelystä tai esittää esimerkiksi korjaus- tai poistopyynnön.

Henkilötietojen käsittelyn läpinäkyvyys

Meille on tärkeää, että rekisteröidyn oikeuksien toteutuminen alkaa selkeästä ja ymmärrettävästä informoinnista. Henkilötietojen käsittelymme on avointa, jotta rekisteröity ymmärtää, miten ja miksi hänen tietojaan käsitellään.

Olemme laatineet henkilötietolain ja GDPR:n mukaiset rekisteriselosteet kaikista ylläpitämistämme henkilörekistereistä. Ajantasainen tietosuojaseloste sekä tiedot rekistereiden sisällöstä ja käyttötarkoituksista ovat saatavilla verkkosivuillamme. Näin varmistamme, että jokainen rekisteröity voi helposti tutustua siihen, miten hänen tietojaan käsitellään.

Pääsy tietoihin ja tietojen siirto

EU:n yleinen tietosuoja-asetus (GDPR) vahvistaa rekisteröidyn oikeuden saada pääsy omiin henkilötietoihinsa. Mahdollistamme tietopyynnön tekemisen vapaamuotoisesti, eli sen ei tarvitse olla erikseen kirjallinen tai allekirjoitettu. Meillä on kuitenkin velvollisuus varmistaa, että tietopyynnön esittäjä on rekisteröity itse. Tämä tehdään suojataksemme

muiden henkilöiden tietosuojaa. Tarvittaessa pyydämme lisätietoja henkilöllisyyden varmentamiseksi ennen tietojen luovuttamista. Toimitamme pyydetyt tiedot rekisteröidylle joko sähköisessä tai muussa asianmukaisessa muodossa.

Rekisteröidyllä on myös oikeus siirtää häntä koskevat henkilötiedot toiselle rekisterinpitäjälle. Toteutamme tietojen siirron silloin, kun käsittely perustuu suostumukseen tai sopimukseen, eikä siirto vaaranna muiden rekisteröityjen oikeuksia tai vapauksia.

Oikeus tietojen oikaisuun ja käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus pyytää virheellisten tai puutteellisten henkilötietojen oikaisua sekä oikeus rajoittaa tietojensa käsittelyä. Varmistamme, että nämä oikeudet toteutuvat nopeasti ja asianmukaisesti.

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

Vastustamisoikeus ja oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus perustellusti vastustaa henkilötietojensa käsittelyä tietyissä tarkoituksissa, kuten suoramainontaa, etämyyntiä, suoramarkkinointia tai tutkimustoimintaa varten. Käytämme asiakasrekisterissä olevia tietoja ainoastaan omaan asiakasviestintäämme ja tiedottamiseen. Hyödynnämme tietoja asiakassuhteen hoitamiseen, emmekä koskaan lainaa, vuokraa tai myy asiakastietoja kolmansille osapuolille.

Rekisteröidyllä on myös oikeus pyytää omien henkilötietojensa poistamista rekisteristämme. Poistamme kaikki asiakasta koskevat tiedot viipymättä, jos asiakas sitä pyytää. Tiedot poistetaan myös automaattisesti asiakassuhteen päättyessä. Poikkeuksena ovat laskutukseen liittyvät yhteystiedot, joita säilytämme sopimuskauden ajan kirjanpitolain ja muun sovellettavan lainsäädännön mukaisesti.

Tietosuojaan hallinta ja kehittäminen

Tietosuoja ja osaamisen kehittäminen

Tietosuojaan suunnittelussa, toteuttamisessa ja seurannassa keskeistä on tunnistaa ja määrittää kaikki henkilötietojen käsittelytoimet ja niihin liittyvät prosessit. Tietosuoja on meillä olennainen osa jokapäiväistä operatiivista toimintaamme, ja sitä tukevat selkeät ja vakiintuneet käytännöt.

Kehitystyössämme otamme järjestelmällisesti huomioon vaikutustenarvioinnit, jotka voivat kohdistua esimerkiksi tietosuojaan liittyvien elementtien tietoturvatarkastukseen tai teknisiin suojausratkaisuihin. Tietosuoja sisällytetään aina osaksi järjestelmä- ja sovelluskehitystä sekä projektinhallintaa. Analysoimme kehitystyön eri vaiheissa jokaisen palvelun osa-alueen tietosuoja-vaatimukset. Tekninen toteutus suunnitellaan niin, että se täyttää kaikki tarvittavat tietoturva-vaatimukset.

Henkilöstön osaamisen pidämme ajan tasalla koulutusten ja ohjeistusten avulla. Seuraamme aktiivisesti alan kehitystä, ja päivitämme käytössämme olevat tietoturvakäytänteet, kuten salaukset ja suojaustavat, vastaamaan kulloinkin voimassa olevia vaatimuksia. Meille tietosuoja on osa henkilöstön osaamispääomaa. Käytössämme on tieto-osaamisen malli, jonka avulla tunnistamme, kuvaamme ja kehitämme osaamistarpeita strategisten tavoitteidemme mukaisesti.

Tietosuojaan kokonaisuuden hallinta

Kansainvälistymisen, digitalisaation ja teknologian nopean kehityksen myötä tietoturvan merkitys kasvaa jatkuvasti suunnittelu-, hallinta- ja seurantaprosesseissamme. Meidän on kyettävä tunnistamaan ja ennakoimaan muutoksia, reagoimaan niihin ketterästi, mukauttamaan toimintaamme tilanteen vaatimalla tavalla sekä tarvittaessa toimimaan aktiivisesti muutosten mahdollistajina.

Organisaatiokulttuurimme ja arkkitehtuurimme perustuvat suunnitelmallisuuteen ja vaatimustenmukaisuuteen. Näiden lisäksi meillä on selkeä kokonaiskuva toiminnastamme ja kyky hallita sitä systemaattisesti.

Tietovarannot ja tietoarkkitehtuuri

Creamailerin hallussa olevat tietovarannot

Hallussamme olevat tietovarannot koostuvat omista asiakasrekistereistämme sekä asiakkaiden palveluun tuomista rekistereistä. Tietovaranto käsittää toiminnan tarpeista määrittyneet ja hallinnollisista syistä johdetut tietojen kokonaisuudet, joita tarvitaan toimintamme ylläpitämisessä.

Omat asiakasrekisterimme 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
- Asiakaskäyttämistiedot
- 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 tietovarannoistamme koostuu asiakkaiden tuomista tai keräämistä tiedoista kuten postituslistoista, kyselyvastauksista ja tapahtumailmoittautumisista.

Asiakkaamme ovat itse vastuussa siitä, että tiedot ovat lainmukaisesti kerättyjä ja käsiteltyjä. Me taas varmistamme, että nämä tiedot säilytetään ja käsitellään turvallisesti palvelun käytön aikana.

Tietoturvan hallinta ja tekniset ratkaisut

Me Creamailerilla noudatamme kaikessa tietoturvaan liittyvässä toiminnassamme Suomen ja EU:n lainsäädäntöä sekä viranomaisten määräyksiä. Palvelumme tiedot sijaitsevat turvallisilla palvelimilla EU:n sisällä. Palvelinkeskukset täyttävät Liikenne- ja viestintävirasto Traficomien määräyksen viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (TRAFICOM/54045/03.04.05.00/2020).

Meillä on käytössä oma tietosuoja-riskien hallintaprosessi, jolla arvioimme henkilötietojen käsittelyyn liittyviä riskejä sekä suunnittelemme tarvittavat tekniset ja organisatoriset toimenpiteet niiden hallitsemiseksi. Hyödynnämme alan parhaita toimijoita sekä uusinta teknologiaa varmistaaksemme korkeatasoisen tietoturvan ja toimintavarmuuden. Seuraamme jatkuvasti alan kehitystä ja mahdollisia uhkia ja reagoimme niihin viipymättä.

Tietovälineemme huolletaan ja hävitetään hallitusti ja turvallisesti niin, ettei tallennettua tietoa päädy ulkopuolisille. Käytämme muun muassa vahvoja palomuuureja, verkkojen loogista eriyttämistä ja tiedonsiirron salausta suojataksemme palveluidemme sisäistä ja ulkoista liikennettä. Palveluidemme jatkuvuus on varmistettu kriittisten toimintojen kahdentamisella, jolloin mahdolliset käyttökatkot pysyvät minimissä.

Käyttäjät kirjautuvat palveluun aina salasanaalla suojatun yhteyden kautta. Kirjautuminen on mahdollista myös Google- tai Microsoft-tilin avulla. Meillä on käytössä myös kaksivaiheinen todennus, joka tuo lisäturvaa käyttäjien tunnistautumiseen. Kaksivaiheinen todennus voidaan haluttaessa ottaa käyttöön koko organisaation tasolla, mikä lisää palvelun tietoturvaa.

Pääsy palvelimille ja hallintapaneeleihin on suojattu useilla varmenteilla, jotka yhdessä muodostavat vahvan suojakerroksen. Tietoturvapoikkeamia monitoroimme ympäri vuorokauden. Henkilöstömme on koulutettu tunnistamaan ja käsittelemään poikkeamat nopeasti sekä estämään niiden mahdollinen leviäminen.

Palvelimien sijainti ja niihin pääsy

Käytämme Hetznerin pilvipalvelinympäristöä, jonka palvelimet sijaitsevat Suomessa. Pääsy palvelimille on rajattu ainoastaan ohjelmistokehittäjillämme sekä tietoturvasta ja skaalautuvuudesta vastaavalle yhteistyökumppanille, Nordic Server Management OÜ:lle. Hetznerin työntekijöillä ei ole pääsyä palvelimien sisältöön.

Creamailerin alihankkijat

Käytämme tiettyjen palvelujen tuottamiseen tarkoin valittuja, luotettavia alihankkijoita, jotka sitoutuvat noudattamaan tiukkoja tietosuoja- ja tietoturvakäytäntöjä. Kaikkien alihankkijoiden kanssa on solmittu sopimukset, joilla varmistamme henkilötietojen lainmukaisen ja turvallisen käsittelyn.

- **Gurumedia Oy**

Gurumedia Oy toteuttaa integraatioita ja WordPress-lisäosia käyttäen Creamailerin julkista API-rajapintaa. Heidän vastuullaan on varmistaa, että nämä integraatiot toimivat sujuvasti ja turvallisesti, täyttäen kaikki tietoturvavaatimukset.

- **Hetzner**

Hetzner tarjoaa Creamailerille palvelinympäristön, jossa palvelut ja tiedot sijaitsevat. Palvelimet sijaitsevat Suomessa, ja ne täyttävät kaikki EU tietosuoja- ja tietoturvastandardit. Hetznerin datakeskukset ovat sertifioituja ja varustettuja edistyneillä tietoturvateknologioilla, kuten palomureilla, salauksella ja pääsynhallinnalla.

- **Janne Vuori (Makasoft Oy)**

Creamailerin entinen työntekijä Janne Vuori toimii nyt alihankkijana, ja hänen vastuullaan on erityisesti kyselytyökalun kehitystyö. Jannella on pääsy Creamailerin palvelimille, ja hän vastaa myös palveluiden kehityksestä ja ylläpidosta, varmistaen, että ne täyttävät kaikki tietoturvavaatimukset.

- **Nordic Server Management OÜ**

Nordic Server Management OÜ vastaa Creamailerin palvelimien tietoturvasta ja skaalautuvuudesta. Heillä on tarkkaan valvottu pääsy Creamailerin palvelimille, ja

heidän tehtävänä on varmistaa, että palvelimet toimivat tehokkaasti ja turvallisesti. He hoitavat myös palvelimien ylläpitoa ja päivityksiä sekä varmistavat, että tietoturvakäytännöt pysyvät ajan tasalla.

- **Sakari Laine**

Sakari Laine toimii yksityishenkilönä ja vastaa integraatioiden toteuttamisesta samalla tavalla kuin Gurumedia. Hän käyttää Creamailerin julkista API-rajapintaa varmistaakseen, että integraatiot toimivat tehokkaasti ja turvallisesti.

- **UpCloud**

UpCloud tarjoaa Creamailerille varmuuskopiointipalvelut, jotka sijaitsevat Helsingin datakeskuksessa. Heidän vastuullaan on varmistaa, että kaikki Creamailerin tiedot varmuuskopioidaan säännöllisesti ja turvallisesti. UpCloudin palvelimet ovat myös EU tietosuoja-asetuksen mukaisia, ja he tarjoavat nopean palautuksen hätätilanteissa.

Evästeet

Evästeet ovat pieniä tiedostoja, jotka tallentuvat käyttäjän selaimeen hänen vieraillessaan verkkosivustolla. Käytämme evästeitä parantaaksemme palveluidemme turvallisuutta, sujuvoittaaksemme käyttäjäkokemusta ja suojataksemme lomakkeiden käyttöä haitallisilta toiminnoilta, kuten bottien häirinnältä. Evästeiden käyttö on linjassa EU:n yleisen tietosuoja-asetuksen (GDPR) vaatimusten kanssa. Evästeitä ovat esimerkiksi:

- **Cross-site request forgery (CSRF) -eväste**

Eväste estää lomakkeiden väärinkäytön eri verkkotunnuksista tulevien pyyntöjen kautta. Se on pakollinen eväste, joka suojaa käyttäjiä CSRF-hyökkäyksiltä.

- **Google reCAPTCHA -eväste**

Eväste auttaa estämään bottien häirintää ja roskapostia verkkolomakkeissa. Google reCAPTCHA analysoi käyttäjän toiminnan ja tunnistaa automaattiset toiminnot. Tämä eväste on oletuksena päällä, mutta sen voi halutessaan poistaa käytöstä.

- **Eväste: XSRF-TOKEN**

- **Evästeen käyttötarkoitus:** Suojaa Creamailerin lomakkeita häirinnältä.
- **Asettava domain:** creamailer.fi
- Voimassaoloaika: 1 päivä
- Evästeen/tunnisteen tyyppi: HTTP Cookie

- Eväste: _GRECAPTCHA
 - **Evästeen käyttötarkoitus:** Estää bottihäirintää Creamailerin lomakkeilla.
 - **Asettava domain:** recaptcha.net (3. osapuolen eväste)
 - Voimassaoloaika: 60 päivää
 - Evästeen/tunnisteen tyyppi: HTTP Cookie

- Eväste: creamailer_session
 - **Evästeen käyttötarkoitus:** Muistaa käyttäjän kirjautumistiedot Creamailerin järjestelmässä.
 - **Asettava domain:** creamailer.fi
 - Voimassaoloaika: 1 päivä
 - Evästeen/tunnisteen tyyppi: HTTP Cookie

Käyttöoikeuksien hallinta

Suojaamme kaikki palveluumme tuodut tiedot huolellisesti teknisin ja organisatorisin toimenpitein. Asiakastietoja käytämme ainoastaan asiakassuhteen hoitamiseen: emme koskaan käytä, lainaa, vuokraa tai myy asiakkaidemme tietoja kolmansille osapuolille.

Tallennamme tiedot turvallisesti ja huolehdimme niiden suojauksesta koko käsittelyn ajan. Takaamme tietojen eheyden, luottamuksellisuuden ja saatavuuden estämällä asiattomat muutokset, tuhoamisen, luovutuksen tai luvattoman pääsyn.

Asiakkaan itse lisäämä data on yksinomaan hänen omassa käytössään. Emme käytä näitä tietoja omiin tarkoituksiimme emmekä luovuta niitä ulkopuolisille tahoille. Poikkeuksen muodostavat tekniset ja laadunvalvontaan liittyvät tilanteet, kuten virheelliset sähköpostiosoitteet, viestien peruminen ja roskapostimerkinnot. Näistä syntyvää dataa

voimme hyödyntää palvelun väärinkäytösten ehkäisemiseksi ja laadun varmistamiseksi, käyttöehtojemme mukaisesti.

Tietoturva osana kehitystyötämme

Tietosuoja ja tietoturva ovat kiinteä osa järjestelmä- ja sovelluskehitystämme sekä projektinhallintaa. Otamme tietoturvavaatimukset järjestelmällisesti huomioon aina, kun kehitämme uusia ominaisuuksia tai päivitämme järjestelmiämme.

Arvioimme tietoturvaa jokaisen kehitysprosessin vaiheessa, aina suunnittelusta toteutukseen, valvontaan ja lopulliseen arviointiin asti. Kehitystyön aikana tarkastelemme jatkuvasti vaikutuksia palveluidemme turvallisuuteen, toiminnallisuuteen ja prosesseihin.

Otamme huomioon myös vaikutustenarvioinnit (DPIA), jotka voivat kohdistua esimerkiksi tietosuojaa edellyttäviin toimintoihin, kuten arkaluontoisten tietojen käsittelyyn, tietoturvatestaukseen tai teknisiin suojausratkaisuihin.

Suunnittelemme tekniset ratkaisut aina niin, että ne täyttävät kaikki voimassa olevat tietoturvavaatimukset varmistaen sekä asiakastietojen suojan että järjestelmän luotettavuuden.

Tietoturvatapahtumat

Mahdolliset meihin kohdistuvat tietoturvatapahtumat raportoidaan toimintamalliemme mukaisesti esimerkiksi omaan toimintajärjestelmäämme. Tapahtumien arvioinnista vastaavat tietoturvavastaava ja ohjelmistokehittäjä, jotka raportoivat ja käsittelevät tapahtumat toimintaprosessiemme mukaisesti.

Riskienhallinta ja jatkuvuus

Tietoturvariskit kartoitetaan osana riskienhallintaprosessia. Arvioinnin lisäksi riskeille nimetään vastuu ja seurantatahot. Tietojärjestelmiin kohdistuvia riskejä seuraavat ohjelmistokehittäjät. Meillä on oma riskienhallintaprosessimme, jota päivitetään ja kehitetään jatkuvasti alan vaatimien muutosten mukaisesti.

API-rajapinta ja tietoturva

Meiltä löytyvän API-rajapinnan avulla palvelumme voidaan liittää mihin tahansa ulkoiseen järjestelmään. Rajapinnan käyttö tapahtuu aina salatun HTTPS-yhteyden kautta, mikä varmistaa turvallisen tiedonsiirron. Jokaisen API-kutsun yhteydessä lähetämme tarkistussumman, joka on laskettu yhteisen tunnisteen avulla. Tämä mekanismi takaa erittäin vahvan tietoturvan.

API-avaimelle voidaan määritellä erikseen luku- ja/tai kirjoitusoikeudet tarpeen mukaan. Avaimen voi halutessaan poistaa milloin tahansa suoraan ylläpidosta. Asiakas on vastuussa API-avaimen luovuttamisesta kolmansille osapuolille.

Tietosuojakäytännöt pähkinäkuoressa

- Käytämme alan johtavia palveluntarjoajia, jotka takaavat korkean tietoturvan ja toimintavarmuuden.
- Hyödynnämme uusinta teknologiaa ja seuraamme aktiivisesti tietoturva-alaa sekä mahdollisia uhkia ja rikkomuksia.
- Huollamme ja hävitämme tietovälineet turvallisesti, jotta tiedot eivät koskaan päädy ulkopuolisille.
- Suojaamme järjestelmät muun muassa vahvoilla palomuuereilla, verkkojen eriyttämisellä ja tiedonsiirron salauksella.
- Säilytämme kaikki tiedot turvallisilla palvelimilla EU:n sisällä. Palvelinkeskusten tilat täyttävät Traficomin määräykset viestintäverkkojen ja -palvelujen varmistamisesta sekä synkronoinnista.
- Otamme tietoturvan huomioon järjestelmien ylläpidossa ja päivityksissä varmistaen hallitun muutoksen ja järjestelmien eheyden.
- Varmistamme palveluidemme jatkuvuuden kahdentamalla kriittiset toiminnot käyttökatkosten minimoimiseksi.
- Kirjautuminen Creamaileriin tapahtuu aina suojatun yhteyden kautta henkilökohtaisella salasanalla.
- Pääsy palvelimille ja hallintapaneeleihin on suojattu useilla varmenteilla, jotka yhdessä muodostavat vahvan suojakerroksen.
- Huolehdimme henkilöstömme osaamisesta jatkuvalla koulutuksella ja ajantasaisilla ohjeistuksilla. Kaikkia työntekijöitämme sitoo vaitiolo- ja salassapitovelvollisuus.

- Monitoroimme tietoturvapoikkeamia 24/7. Henkilöstömme on koulutettu tunnistamaan poikkeamat, selvittämään niiden syyt ja vaikutukset sekä estämään niiden leviäminen.
- Meillä on nimetty tietosuojavastaava, joka vastaa tietosuojaan ja tietoturvan kokonaisvaltaisesta hallinnasta, mittaamisesta, kehittämisestä ja seurannasta yhteistyössä muun tiimin kanssa.