Tietotilinpäätös 2025

Creamailer Oy

Creamailer Oy
info@creamailer.fi
www.creamailer.fi
Y-tunnus: 2255533-0
Päivitetty 1.12.2025

Tietosuojavastaavan tervehdys

Vuosi 2025 oli Creamailerille merkittävä tietoturvan ja tietosuojan kehityksen vuosi. Siirryimme vaiheeseen, jossa sisäisesti vakiinnutetut käytännöt vietiin seuraavalle tasolle: kohti ulkoista todentamista, systemaattisempaa dokumentointia ja entistä ennakoivampaa toimintamallia.

Toteutimme vuoden aikana riippumattoman asiantuntijan suorittaman tietoturva-auditoinnin, jossa arvioitiin palvelumme tekninen tietoturva. Auditointi vahvisti tekemäämme työtä ja oli tärkeä askel kohti läpinäkyvämpää tietoturvakulttuuria.

Samalla vahvistimme dokumentaatiotamme merkittävästi. Laadimme asiakkaille tarjottavan tietosuojaliitteen (DPA), päivitimme käsittelytoimien selosteen GDPR:n artikla 30:n mukaisesti ja selkeytimme asiakastileihin kirjautumisen käytänteet lokitusvaatimuksineen. Lisäksi määrittelimme kohtuullisen käytön politiikan palvelun käyttörajojen läpinäkyvyyden varmistamiseksi sekä loimme NDA-sopimuspohjat alihankkija- ja yhteistyösuhteita varten. Dokumentoinnin tavoitteena on ollut tehdä tietosuojasta entistä selkeämpää, johdonmukaisempaa ja todennettavaa.

EU:n NIS2-direktiivin voimaantulo vauhditti kehitystyötämme entisestään. Arvioimme ja vahvistimme tietoturvatoimenpiteitämme direktiivin vaatimusten mukaisesti. Riskienhallinta, poikkeamien hallinta, palvelun jatkuvuus, salaus ja pääsynhallinta ovat keskeisiä osa-alueita, joita kehitämme suunnitelmallisesti. Myös toimitusketjun tietoturvan arviointi ja vaatimustenmukaisuuden varmistaminen ovat jatkuva osa kehitystyötämme.

Tekoälyn rooli palvelukehityksessä kasvoi vuoden aikana merkittävästi. Varmistimme, että tekoälyn hyödyntäminen tapahtuu hallitusti ja tietosuojaperiaatteita noudattaen. Kaikki tekoälyn käyttö perustuukin selkeästi määriteltyihin ja dokumentoituihin periaatteisiin.

Palvelininfrastruktuurimme säilyi Suomessa ja EU:n alueella. Palvelimet sijaitsevat Hetznerin Helsingin datakeskuksessa, ja varmuuskopiot tallennetaan UpCloudin erilliseen, Suomessa sijaitsevaan datakeskukseen. Kahdennettu ratkaisu varmistaa tietojen saatavuuden ja palvelun jatkuvuuden myös mahdollisissa häiriötilanteissa.

Vuoden keskeisin saavutus oli siirtyminen reaktiivisesta tietoturvasta ennakoivaan ja jatkuvasti kehittyvään toimintamalliin. Ulkoiset auditoinnit, vahvistettu dokumentaatio ja systemaattinen NIS2-valmistautuminen osoittavat, että tietoturva on Creamailerille pysyvä ja strateginen investointi. Vuonna 2026 jatkamme tätä työtä määrätietoisesti ja kehitämme toimintaamme edelleen asiakkaidemme luottamuksen säilyttämiseksi ja vahvistamiseksi.

Helsingissä 20.2.2026

tietosuojavastaava
Eija Pietilä

Sisällysluettelo

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 hallinnoitu 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 tietosuojaa ja tietoturvaa koskevaa lainsäädäntöä. Nämä muutokset vaikuttavat sekä meidän toimintaamme että asiakkaidemme arkeen. Vuoden 2025 aikana useat lainsäädännölliset uudistukset muokkasivat toimintaympäristöämme.

EU:n yleisen tietosuoja-asetuksen (GDPR) soveltamista täsmennettiin vuoden aikana viranomaisohjeistuksilla, oikeuskäytännöllä ja valvontamenettelyjä koskevilla tarkennuksilla. Muutokset eivät muuttaneet itse asetuksen ydinsisältöä, mutta ne selkeyttivät sen tulkintaa ja vahvistivat rekisterinpitäjien vastuita. Reagoimme tarkennuksiin päivittämällä sisäisiä prosessejamme ja tietoturvakäytäntöjämme varmistaaksemme, että henkilötietojen käsittely vastasi ajantasaista sääntelyä ja valvontakäytäntöä.

Euroopan unionin NIS2-direktiivi (Network and Information Security 2) asettaa aiempaa tiukemmat kyberturvallisuusvaatimukset keskeisille ja tärkeille toimijoille. Se edellyttää kattavaa riskienhallintaa, nopeaa poikkeamien ilmoittamista sekä toimitusketjun turvallisuuden varmistamista. Jäsenvaltioiden tuli saattaa direktiivi osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. Suomessa kansallinen toimeenpano toteutui kyberturvallisuuslailla, joka tuli voimaan huhtikuussa 2025.

Valmistauduimme NIS2-vaatimuksiin järjestelmällisesti vuoden 2025 aikana. Keskeisimmät toteutetut toimenpiteet:

- Riskienhallinta: Tietoturvariskien arviointi on vakiintunut käytäntö. Riskeille on nimetty vastuuhenkilöt ja seurantaprosessi.
- Poikkeamien hallinta: Tietoturvatapahtumien havaitsemis-, arviointi- ja ilmoitusprosessi on dokumentoitu. Vakavista poikkeamista ilmoitetaan viranomaisille 24 tunnin kuluessa.
- Palvelun jatkuvuus: Kriittiset toiminnot on kahdennettu ja palautumisprosessit testattu säännöllisesti.
- Pääsynhallinta ja salaus: Monivaiheinen tunnistautuminen, VPN-yhteydet ja vahva salaus (TLS 1.3, AES-256) ovat käytössä kaikissa kriittisissä järjestelmissä.

- Toimitusketjun turvallisuus: Alihankkijoiden ja kumppaneiden tietoturva-arviointia on tiivistetty osana NIS2-valmistautumista.

Seuraamme aktiivisesti NIS2-direktiivin kansallista toimeenpanoa ja mukautamme käytäntöjämme sitä mukaa kun viranomaisohjeistukset tarkentuvat.

Tekoälyn merkityksen kasvaessa myös sen sääntely on noussut entistä keskeisempään rooliin. Euroopan unionin tekoälyasetus (AI Act) hyväksyttiin vuonna 2024, ja se tuli voimaan elokuussa 2024. Asetus perustuu riskiperusteiseen lähestymistapaan, jossa velvoitteet määräytyvät tekoälyjärjestelmän riskitason mukaan, ja sen vaatimukset tulevat voimaan vaiheittain siirtymäaikojen mukaisesti. Sääntely korostaa muun muassa läpinäkyvyyttä, turvallisuutta, vastuullisuutta ja tietosuojan huomioimista.

Vastasimme sääntelyn kehitykseen tarkentamalla tekoälyn käyttöä koskevia toimintatapojamme ja varmistamalla, että tekoälyä hyödyntävät ratkaisumme ovat linjassa voimassa olevan ja voimaan tulevan sääntelyn kanssa. Lainsäädäntömuutosten myötä teimme useita kehitysaskeleita varmistaaksemme palveluidemme tietoturvallisuuden ja lainmukaisuuden:

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

Seuraamme aktiivisesti tietosuojaan ja tietoturvaan liittyvän lainsäädännön kehitystä ja pidämme asiakkaamme ajan tasalla muutoksista. Noudatamme tiukimpia käytäntöjä ja varmistamme, että palvelumme pysyvät turvallisina ja luotettavina.

Rekisterinpitäjän velvoitteet ja vastuut

Tietosuojavastaava

Tietosuojavastaava on keskeinen toimija tietosuojan ja tietoturvan varmistamisessa. Hänen tehtävänään on huolehtia siitä, että henkilötietojen käsittely noudattaa voimassa olevaa lainsäädäntöä ja parhaita käytänteitä. Creamailerin tietosuojavastaavana toimii viestintäpäällikkö Eija 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 tietosuojaa koskevat vaikutustenarvioinnit (DPIA), tehdään ajallaan ja että mahdolliset puutteet korjataan viipymättä.
3. **Tietosuojavaikutusten arviointi (DPIA)**
   Korkean riskin käsittelytoimissa tietosuojavaikutusten 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

Tietosuoja-asetus 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.

Tietosuoja-asetus 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 riskiperusteista 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 käytännesäännöt eri käyttötarkoituksia ja käsittelytilanteita varten.

Kaikki tietosuojaselosteemme ja käytännesääntömme 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 tahoa (organisaatiota tai henkilöä), joka käsittelee henkilötietoja rekisterinpitäjän lukuun tämän ohjeiden mukaisesti. 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 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 tietoturvavaatimukset. Käytännössä tämä tarkoittaa, että kehitys- ja projektityön suunnitteluvaiheessa kartoitamme käsiteltävät henkilötiedot, määrittelemme niiden käyttötarkoituksen ja elinkaaren, sekä arvioimme niihin liittyvät tietosuojariskit.

Näin varmistamme, että toimintamme täyttää EU:n yleisen tietosuoja-asetuksen (GDPR) sekä sitä täydentävän tietosuojalain (1050/2018) mukaiset suunnittelu-, huolellisuus- ja osoitusvelvollisuudet.

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 tietojenkäsittelystään tai esittää esimerkiksi korjaus- tai poistopyynnön.

Henkilötietojen käsittelyn läpinäkyvyys

Meille on tärkeää, että rekisteröidyn oikeuksien toteutuminen perustuu selkeään ja ymmärrettävään tiedottamiseen. Henkilötietojen käsittelymme on avointa, jotta rekisteröity ymmärtää, miten ja miksi hänen tietojaan käsitellään.

Olemme laatineet GDPR:n ja tietosuojalain (1050/2018) mukaiset tietosuojaselosteet kaikista ylläpitämistämme henkilötietojen käsittelykokonaisuuksista. Ajantasaiset tietosuojaselosteet sekä tiedot käsittelyn tarkoituksista ja tietosisällöistä ovat saatavilla verkkosivuillamme. Näin jokainen rekisteröity voi helposti tutustua omien tietojensa käsittelyyn.

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.

Rekisteröidyillä 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 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.

Tietosuojan hallinta ja kehittäminen

Tietosuoja ja osaamisen kehittäminen

Tietosuojan suunnittelussa, toteuttamisessa ja seurannassa keskeistä on tunnistaa ja määritellä 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 tietoturvatestaukseen tai teknisiin suojausratkaisuihin. Tietosuoja sisällytetään aina osaksi järjestelmä- ja sovelluskehitystä sekä projektinhallintaa. Analysoimme kehitystyön eri vaiheissa jokaisen palvelun osa-alueen tietosuojavaatimukset. Tekninen toteutus suunnitellaan niin, että se täyttää kaikki tarvittavat tietoturvavaatimukset.

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.

Tietosuojan 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.

Vuonna 2025 laajensimme dokumentaatiotamme. Laadimme tietosuojaliitteen (DPA) asiakassopimuksiin, käsittelytoimien selosteen GDPR:n artikla 30:n mukaisesti, salassapitosopimuspohjan (NDA) yhteistyökumppaneille sekä käytänteet asiakastileihin kirjautumiselle. Dokumentaatio vahvistaa tietosuojatoimintamme läpinäkyvyyttä ja jäljitettävyyttä.

Tietovarannot ja tietoarkkitehtuuri

Creamailerin hallussa olevat tietovarannot

Hallussamme olevat tietovarannot koostuvat omista asiakasrekistereistämme ja asiakkaiden palveluun tuomista rekistereistä. Tietovaranto käsittää toiminnan ja hallinnollisista syistä johdetut tietokokonaisuudet, joita tarvitaan toiminnan ylläpitämiseen. Omat asiakasrekisterimme sisältävät asiakkuussuhteiden ylläpitämiseen 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 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

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 Traficomin

määräyksen viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista (TRAFICOM/54045/03.04.05.00/2020).

Meillä on käytössä oma tietosuojariskien 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 palomuureja, 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 salasanalla 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. Monitoroimme tietoturvapoikkeamia ympäri vuorokauden. Henkilöstömme on koulutettu tunnistamaan ja käsittelemään poikkeamat nopeasti sekä estämään niiden mahdollinen leviäminen.

Ulkoinen tietoturva-auditointi

Vuonna 2025 toteutimme ulkopuolisen tietoturva-auditoinnin, jossa riippumaton kyberturvallisuuskumppani arvioi palvelumme teknisen tietoturvan tason. Auditointi kohdistui sekä sovellus- että palvelinympäristöön.

Auditoinnin tulokset olivat kokonaisuudessaan hyvät:

- Kriittisiä haavoittuvuuksia ei löytynyt. Palvelumme perusturvallisuus on vahvalla tasolla.

- Kolme korkean riskin löydöstä tunnistettiin, joista kaksi liittyi sovellustasoon ja yksi palvelinympäristöön. Nämä käsiteltiin ja korjattiin yhteistyössä kehitystiimin kanssa.
- Loput löydökset luokiteltiin kohtalaisen tai matalan riskin havainnoiksi, ja ne huomioitiin jatkokehityksessä.

Palvelimien sijainti ja niihin pääsy

Käytämme Hetznerin pilvipalvelinympäristöä, jonka palvelimet sijaitsevat Suomessa. Pääsy palvelimille on rajattu ainoastaan ohjelmistokehittäjillemme 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 toimii kolmantena osapuolena vastaten tiettyjen CRM- ja muiden järjestelmäintegraatioiden toteutuksesta ja ylläpidosta 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 soveltuvat EU:n tietosuoja- ja tietoturvavaatimukset. Hetznerin datakeskukset ovat sertifioituja ja varustettuja edistyneillä tietoturvateknologioilla, kuten palomuureilla, salauksella ja pääsynhallinnalla.
- **Nordic Server Management OÜ**
  Nordic Server Management OÜ vastaa Creamailerin palvelimien tietoturvasta ja skaalautuvuudesta. Heillä on tarkkaan valvottu pääsy Creamailerin palvelimille, ja tehtävänään 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 WordPress-integraatioiden toteuttamisesta. 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:n tietosuoja-asetuksen mukaisia, ja he tarjoavat nopean palautuksen hätätilanteissa.
- **AWS S3**
  Kyselytyökalun tiedostokysymysten kautta vastaanottajien lähettämät tiedostot tallennetaan AWS S3 -palveluun Tukholman datakeskuksessa (EU). Tiedostot ovat ainoastaan kyselyn luoneen asiakkaan saatavilla.

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- ja ALTCHA-evästeet**
  Evästeet auttavat estämään bottien häirintää ja roskapostia verkkolomakkeissa. Google reCAPTCHA analysoi käyttäjän toimintaa ja tunnistaa automaattiset toiminnot. ALTCHA puolestaan tarjoaa vaihtoehtoisen, kevyemmän botintunnistusratkaisun, joka ei perustu käyttäjän profilointiin. Näiden teknologioiden avulla suojaamme lomakkeita väärinkäytöksiltä ja parannamme palvelun

turvallisuutta. Evästeet ovat oletuksena käytössä, mutta käyttäjä voi halutessaan estää ne selaimensa asetuksista.

- **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
- **Evästeet: cmailer, creamailer_session**
    - Evästeen käyttötarkoitus: Muistaa käyttäjän kirjautumistiedot Creamailerin järjestelmässä.
    - Asettava domain: creamailer.fi
    - Voimassaoloaika: 1 päivä
    - Evästeen/tunnisteen tyyppi: HTTP Cookie
- **Eväste: CMLBSTICKY**
    - Evästeen käyttötarkoitus: Varmistaa palvelun toimivuuden ohjaamalla käyttäjän samalle palvelimelle istunnon aikana.
    - Asettava domain: creamailer.fi
    - Voimassaoloaika: Selainistunnon ajan
    - 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 roskapostimerkinnät. 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 omaan toimintajärjestelmäämme. Tapahtumien arvioinnista vastaavat tietosuojavastaava ja kehitystiimi, jotka raportoivat ja käsittelevät tapahtumat toimintaprosessiemme mukaisesti.

Vuoden 2025 aikana automaattisten roskapostibottien lisääntynyt toiminta ohjasi meitä tiukentamaan ja kehittämään useita palvelumme perustoimintoja. Vahvistimme muun muassa tilien aktivointiprosessia, lisäsimme automaattisia tarkistuksia väärinkäytösten

tunnistamiseksi sekä paransimme kokeiluversioiden hallintaa. Nämä toimenpiteet vähensivät merkittävästi palvelun väärinkäytön mahdollisuuksia ja samalla paransivat palvelun luotettavuutta kaikille asiakkaillemme.

Riskienhallinta ja jatkuvuus

Tietoturvariskit kartoitetaan osana riskienhallintaprosessia. Arvioinnin lisäksi riskeille nimetään vastuu ja seurantatahot. Kehitystiimimme seuraa tietojärjestelmiin kohdistuvia riskejä. 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 lasketaan yhteisen tunnisteen perusteella. Tämä mekanismi vahvistaa rajapinnan tietoturvaa.

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.

Tietosuojakäytänteet pähkinänkuoressa

1. Käytämme alan johtavia palveluntarjoajia, jotka takaavat korkean tietoturvan ja toimintavarmuuden.
2. Hyödynnämme uusinta teknologiaa ja seuraamme aktiivisesti tietoturva-alaa sekä mahdollisia uhkia ja rikkomuksia.
3. Huollamme ja hävitämme tietovälineet turvallisesti, jotta tiedot eivät päädy ulkopuolisille.
4. Suojaamme järjestelmät muun muassa vahvoilla palomuureilla, verkkojen eriyttämisellä ja tiedonsiirron salauksella.
5. Säilytämme kaikki tiedot turvallisilla palvelimilla EU:n sisällä. Palvelinkeskusten tilat täyttävät Traficomin määräykset viestintäverkkojen ja -palvelujen varmistamisesta sekä synkronoinnista.
6. Otamme tietoturvan huomioon järjestelmien ylläpidossa ja päivityksissä varmistaen hallitun muutoksen ja järjestelmien eheyden.
7. Varmistamme palveluidemme jatkuvuuden kahdentamalla kriittiset toiminnot käyttökatkosten minimoimiseksi.
8. Kirjautuminen Creamaileriin tapahtuu aina suojatun yhteyden kautta henkilökohtaisella salasanalla.
9. Pääsy palvelimille ja hallintapaneeleihin on suojattu useilla varmenteilla, jotka yhdessä muodostavat vahvan suojakerroksen.
10. Huolehdimme henkilöstömme osaamisesta jatkuvalla koulutuksella ja ajantasaisilla ohjeistuksilla. Kaikkia työntekijöitämme sitoo vaitiolo- ja salassapitovelvollisuus.
11. Monitoroimme tietoturvapoikkeamia 24/7. Henkilöstömme on koulutettu tunnistamaan poikkeamat, selvittämään niiden syyt ja vaikutukset sekä estämään niiden leviäminen.
12. Meillä on nimetty tietosuojavastaava, joka vastaa tietosuojan ja tietoturvan kokonaisvaltaisesta hallinnasta, mittaamisesta, kehittämisestä ja seurannasta yhteistyössä muun tiimin kanssa.