tietosuojapolitiikka

**Luokitus**: Julkinen

Tätä asiakirjaa voidaan jakaa [Yrityksen] ulkopuolisille kiinnostuneille osapuolille.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versio | Päivitetty | Muokkaaja | Asiakirjan muutokset | Hyväksyjä | Omistaja |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Sisällysluettelo

[Tämän asiakirjan tarkoitus 3](#_Toc196732891)

[Määritelmät ja soveltamisala 3](#_Toc196732892)

[Tietosuojan periaatteet 3](#_Toc196732893)

[Yleiset säännökset 4](#_Toc196732894)

[Lainmukainen ja läpinäkyvä käsittely 4](#_Toc196732895)

[Käsittelyn lainmukainen tarkoitus 4](#_Toc196732896)

[Tietojen minimointi 5](#_Toc196732897)

[Tietojen täsmällisyys 5](#_Toc196732898)

[Arkistointi ja poistaminen 5](#_Toc196732899)

[Tietoturva 5](#_Toc196732900)

[Henkilötietojen tietoturvaloukkaukset 5](#_Toc196732901)

# Tämän asiakirjan tarkoitus

Tämä politiikka määrittelee, miten [Yritys]:

* Suojaa, käsittelee ja säilyttää hallussaan olevia henkilötietoja, jotka koskevat työntekijöitä, allekirjoittajia tai asiakkaita.
* Noudattaa tietosuojalainsäädäntöä, mukaan lukien Suomen tietosuojalakia ja EU:n yleistä tietosuoja-asetusta (GDPR), ja käyttää näitä vertailukohtana henkilötietojen suojaamisen ohjeistuksissa.

# Määritelmät ja soveltamisala

Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan elossa olevaan luonnolliseen henkilöön liittyviä tietoja, kuten:

* Henkilöiden nimet
* Postiosoitteet
* Sähköpostiosoitteet
* Puhelinnumerot
* Valokuvat
* Muut henkilöihin liittyvät tiedot

Tietosuojalaki tai GDPR ei koske anonymisoituja tietoja, jos niitä ei voida takaisinmallintaa henkilön tunnistamiseksi.

Jotkin tiedot ovat erityisen arkaluonteisia ja niille tulisi antaa vahvempi suoja, mukaan lukien:

* Terveystiedot
* Poliittiset mielipiteet
* Uskonnollinen tai filosofinen vakaumus
* Ammattiliiton jäsenyys
* Geneettiset tiedot
* Biometriset tunnistetiedot
* Rotu tai etninen alkuperä
* Seksuaalinen suuntautuminen
* Rikoksiin liittyvät tiedot (tuomiot ja rikkomukset)

Tässä politiikassa *Vastuuhenkilöllä* tarkoitetaan organisaation sisällä henkilöä, joka omistaa liiketoimintaprosessin ja käsittelee tietoja.

# Tietosuojan periaatteet

Henkilötietoja tulee:

1. käsitellä lainmukaisesti, asianmukaisesti ja läpinäkyvästi suhteessa rekisteröityihin.
2. kerätä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempi käsittely yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota yhteensopimattomaksi alkuperäisten tarkoitusten kanssa.
3. rajoittaa siihen, mikä on asianmukaista, olennaista ja tarpeellista suhteessa tarkoituksiin, joita varten niitä käsitellään.
4. pitää täsmällisinä ja tarvittaessa päivitettyinä; on toteutettava kaikki kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.
5. säilyttää muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten edellyttäen, että tietosuoja-asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on toteutettu rekisteröidyn oikeuksien ja vapauksien turvaamiseksi.
6. käsitellä tavalla, joka varmistaa henkilötietojen asianmukaisen turvallisuuden, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimenpiteitä.

# Yleiset säännökset

1. Tämä politiikka koskee kaikkia henkilötietoja, joita [Yritys] käsittelee, mukaan lukien henkilöstön, konsulttien, allekirjoittajien ja muiden tietoja.
2. [Yritys] tietojen omistajat vastaavat tämän politiikan jatkuvasta noudattamisesta.
3. Tämä politiikka on tarkistettava vähintään vuosittain.
4. [Yritys] rekisteröityy tietosuojavaltuutetun toimistoon henkilötietoja käsittelevänä organisaationa.
5. [Yritys] tarkistaa vuosittain tietosuojavastaavan tunnistamista ja nimittämistä koskevat vaatimukset.

# Lainmukainen ja läpinäkyvä käsittely

1. Varmistaakseen, että tietojen käsittely on lainmukaista, oikeudenmukaista ja läpinäkyvää, [Yritys] ylläpitää henkilötietoja käsittelevien järjestelmien rekisteriä.
2. Järjestelmärekisteri tarkistetaan vähintään vuosittain.
3. Yksilöillä on oikeus päästä käsiksi omiin tietoihinsa, ja kaikki tulevat pyynnöt käsitellään viipymättä.

# Käsittelyn lainmukainen tarkoitus

1. Kaiken [Yritys] käsittelemän tiedon tulee perustua yhteen seuraavista lainmukaisista perusteista: suostumus, sopimus, lakisääteinen velvoite, elintärkeä etu, yleinen etu tai oikeutettu etu (lisätietoa tietosuojavaltuutetun ohjeistuksesta).
2. [Yritys] dokumentoi käsittelyn lainmukaisen perusteen tarvittaessa.
3. Kun suostumusta käytetään tietojenkäsittelyn lainmukaisena perusteena, todiste opt-in-suostumuksesta säilytetään henkilötietojen yhteydessä.
4. Kun viestintää lähetetään henkilöille heidän suostumuksensa perusteella, mahdollisuus suostumuksen peruuttamiseen tulee olla selkeästi saatavilla, ja käytössä tulee olla järjestelmät, jotka varmistavat, että tällainen peruutus näkyy asianmukaisesti [Yritys] järjestelmissä.

# Tietojen minimointi

1. [Yritys] varmistaa, että henkilötiedot ovat asianmukaisia, olennaisia ja rajoitettu siihen, mikä on tarpeellista suhteessa tarkoituksiin, joita varten niitä käsitellään.

# Tietojen täsmällisyys

1. [Yritys] toteuttaa asianmukaiset ja konkreettiset toimenpiteet varmistaakseen henkilötietojen täsmällisyyden.
2. Kun se on tarpeellista tietojen käsittelyn lainmukaisen perusteen kannalta, toteutetaan toimenpiteitä sen varmistamiseksi, että henkilötiedot pidetään ajan tasalla.

# Arkistointi ja poistaminen

1. Varmistaakseen, että henkilötietoja ei säilytetä pidempään kuin on tarpeen, [Yritys] ottaa käyttöön arkistointikäytännön kullekin henkilötietojen käsittelyalueelle ja tarkistaa tämän prosessin vuosittain.
2. Arkistointikäytännössä huomioidaan mitä tietoja tulisi/täytyy säilyttää, kuinka kauan ja miksi.

# Tietoturva

1. [Yritys] varmistaa, että henkilötiedot tallennetaan turvallisesti käyttäen nykyaikaisia, ajantasaisia ohjelmistoja.
2. Pääsy henkilötietoihin rajoitetaan henkilöstöön, joka tarvitsee pääsyn ja asianmukaiset turvatoimet toteutetaan luvattoman tietojen jakamisen välttämiseksi.
3. Kun henkilötietoja poistetaan, tämä tehdään turvallisesti niin, että tiedot eivät ole palautettavissa.
4. Asianmukaiset varmuuskopiointi- ja palautusratkaisut ovat käytössä.

# Henkilötietojen tietoturvaloukkaukset

Jos tapahtuu tietoturvaloukkaus, joka johtaa henkilötietojen tahattomaan tai lainvastaiseen tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai niihin pääsyyn, tulee viipymättä:

1. Ilmoittaa tietoturvaloukkauksesta IT-tukeen mahdollisimman nopeasti, jotta he voivat tukea tietoturvaloukkauksen hallinnassa.
2. Ilmoittaa tietoturvaloukkauksesta lähiesimiehelle, joka auttaa vaikutusten arvioinnissa ja valvonnassa.
3. Ilmoittaa tietoturvaloukkauksesta henkilöstöjohtajalle, jos loukkaus koskee henkilöstön tietoja.
4. Arvioida yhdessä esimiehen tai tietosuojavastaavan kanssa ihmisten oikeuksiin tai vapauksiin kohdistuva riski ja tehdä ilmoitus tietosuojavaltuutetulle 72 tunnin kuluessa (GDPR), jos todetaan ilmoitusvelvollisuuden täyttyvän (lisätietoja tietosuojavaltuutetun verkkosivuilta).