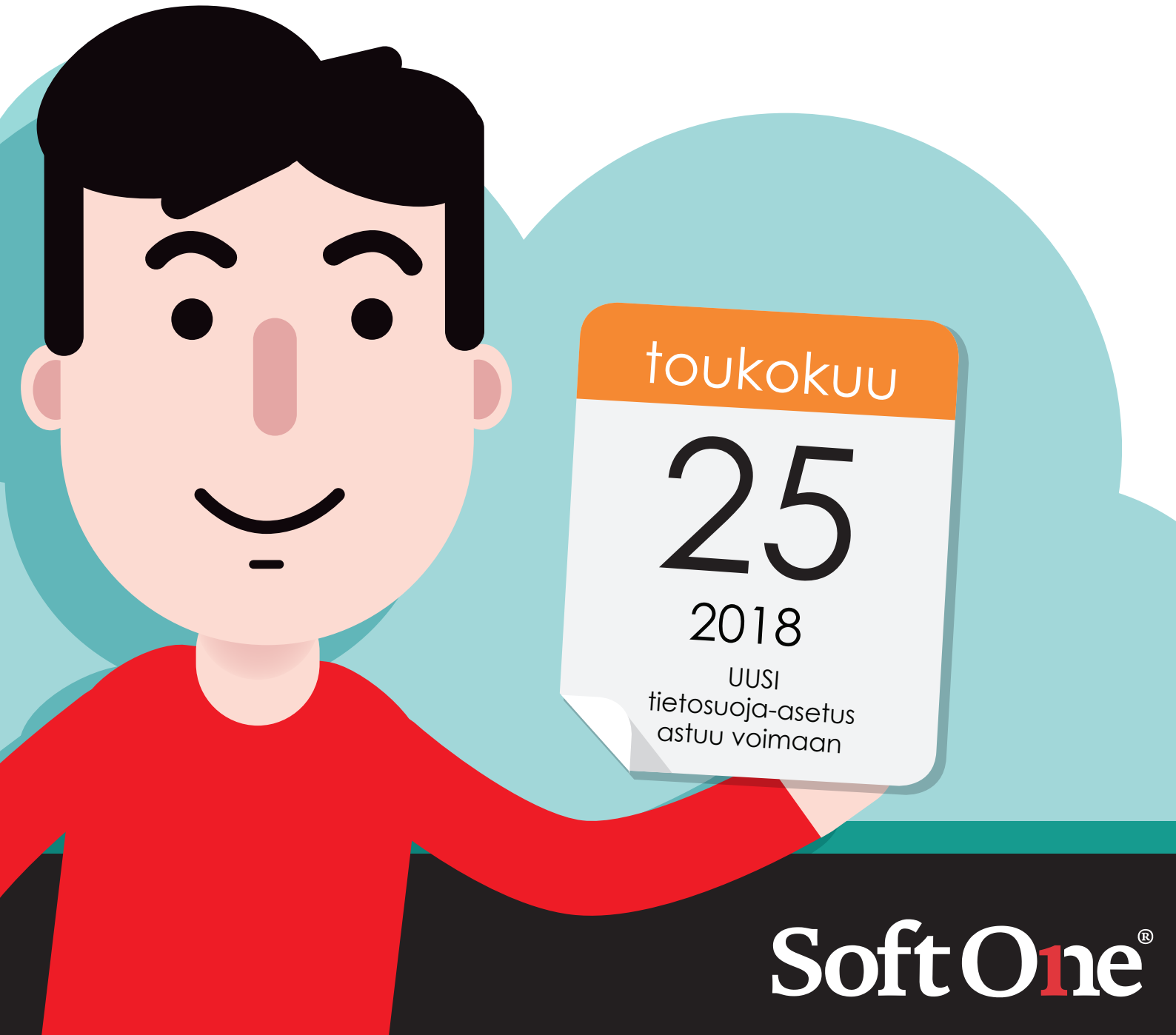
Hallitse uusi
TIETOSUOJA-ASETUS
GDPR

TIETOSUOJAN HELPOT ALKEET



SoftOne®

GDPR

Uusi tietosuoja-asetus GDPR astuu voimaan 25.5.2018 ja se korvaa henkilötietolain.

GDPR (General Data Protection Resolution) on EU-direktiivi, joka sisältyy niin sanottuun tietosuoja-asetukseen. Saamme yhteisen EU-lainsäädännön, joka säätelee henkilötietojen käsittelyä.

Suurin ero nykytilanteeseen tulee olemaan se, että yritykset eivät voi enää omistaa henkilötietoja vaan saada ne vain väliaikaisesti käyttöön tiettyä tarkoitusta varten.

Uusi laki voi vaikuttaa hieman sekavalta. Käytännöt alkavat muotoutua sitä mukaa kun lakia aletaan soveltaa. Suomessa tietosuojavaltuutettu on vastuussa lain noudattamisesta.

Yritys voidaan tuomita lain rikkomisesta sakkoihin, joiden suuruus on enintään 4 % liikevaihdosta. Tämä pakottaa yritykset pohtimaan, miten ne käsittelevät ja suojaavat henkilötietoja.

TUTUSTU HELPPOIHIN TIETOSUOJAN ALKEISIIN

Kolme perussääntöä yritysten arkipäivään

1.KERÄÄ TIETOJA VAIN MÄÄRÄTTYYN TARKOITUKSEEN
Kerää vain tarvittavat henkilötiedot ja vain erityiseen ja ennalta määrättyyn tarkoitukseen.

2. TIEDOTA ENEMMÄN
Kun keräätte henkilötietoja, henkilölle on kerrottava, mistä tiedoista on kyse ja miksi niitä kerätään. Jos luovutatte tietoja eteenpäin, asiasta on kerrottava.

3. SÄILYTÄ VÄHEMMÄN
Kun henkilötietoja ei enää tarvita siihen tarkoitukseen, mihin ne kerättiin, tiedot on poistettava. Tämä tarkoittaa sitä, että esimerkiksi tiedot henkilöistä, jotka eivät ole enää asiakkaita tai toimittajia, on poistettava tietojärjestelmästä.

Aiemmin käytäntönä oli, että entisen asiakkaan henkilötietoja voitiin käyttää markkinointiin vuoden verran asiakassuhteen päättymisen jälkeen. Näin ei siis ole enää.

Joitakin henkilötietoja voi kuitenkin olla tarpeen säilyttää, jotta esimerkiksi myyjä voi täyttää takuuvelvoitteen. Tiedot tallennetaan tällöin uutta tarkoitusta varten.

HUOM!

MUISTA!

Muu lainsäädäntö saattaa velvoittaa säilyttämään tiedot tietyn ajan. Lainsäädäntö voi koskea esimerkiksi kirjanpitoa, eläke- ja valvontatietoja.

Henkilötietoja ovat

KAIKKI TIEDOT, JOTKA VOIDAAN YHDISTÄÄ LUONNOLLISEEN HENKILÖÖN:

- Henkilötunnus, nimi ja osoite
- Kuva henkilöstä
- Sähköisessä muodossa säilytettävät äänitteet voivat sisältää henkilötietoja, vaikka niissä ei mainittaisi nimiä
- Yhteisötunnus, kun kyseessä on yksityinen elinkeinotoiminta
- Auton rekisterinumero voi olla henkilö- tieto, jos se voidaan yhdistää luonnollisen henkilön kanssa. Useiden henkilöiden käyttämän yritysauton rekisterinumero ei välttämättä ole henkilötieto.

SAAKO ASIAKKAAN KIINNOSTUKSEN KOHTEISTA SÄILYTTÄÄ TIETOJA?

Pelaako asiakas golfia? Onko asiakkaalla allergioita, joista on hyvä tietää ennen liikelounasta? Jotta voitte rekisteröidä tällaiset tiedot, asiakkaalle on kerrottava, miksi säilytätte tiedot ja hänen on annettava suostumus tietojen rekisteröintiin. Tietojen on oltava asiakassuhteen kannalta olennaisia. Muutoin niitä ei saa rekisteröidä.

HUOM!

MUISTA!

Henkilötietoja voi sisältyä sähköpostiin, sosiaalisiin medioihin jne. GDPR käsittää myös arkistoidut tiedot.

MITEN TOIMIMME KOTISIVUN JA UUTISKIRJEEN SUHTEEN?

GDPR:n mukaan sinun on hankittava yrityksen kotisivulla ja uutiskirjeessä nimettyjen henkilöiden suostumus.

Kuka vastaa mistäkin pilvipalveluiden osalta?

KAIKKIEN YRITYSTEN TULEE KARTOITTAA, KUINKA HE KÄSITTELEVÄT HENKILÖTIETOJA

Tässä yhteydessä kerrotaan kuka vastaa tietystä rekisteristä tai tietojärjestelmästä, mihin sitä käytetään, mitä henkilötietoja järjestelmässä esiintyy sekä millaisia tietoja ja millä oikeudellisella perusteella tietoja käsitellään.

UUDET ROOLIT JA KÄSITTEET:

REKISTERINPITÄJÄ

Organisaatiota, jonka hallussa on henkilötietoja ja joka käyttää pilvipalvelua, kutsutaan rekisterinpitäjäksi. Organisaatio itse vastaa siitä, että lakeja noudatetaan.

TIETOSUOJAVASTAAVA

Tietosuojavastaava on organisaation sisällä tai ulkopuolella toimiva henkilö, joka voi puuttua havaitsemiinsa epäkohtiin (sisäisenä tarkastajana). Nimetyn tietosuojavastaavan tiedot on ilmoitettava valvontaviranomaiselle.

HENKILÖTIETOJEN KÄSITTELYSOPIMUS

Rekisteripitäjien on käytännössä huolehdittava henkilötietojen käsittelyä koskevasta sopimuksesta.

PILVIPALVELUN TARJOAJA

Pilvipalvelun tarjoaja (esim. SoftOne) avustaa henkilötietojen käsittelyssä rekisterinpitäjää.

Rekisterinpitäjän on nimitettävä tietosuojavastaava, jos:

- henkilötietojen käsittely tapahtuu viranomaisen tai julkisen elimen toimesta (mutta ei tuomioistuinten toimesta lainkäyttötehtävissä)
- ydintehtävät muodostuvat henkilötietojen käsittelystä, joka edellyttää laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- ydintehtävät muodostuvat luottamuksellisten henkilötietojen tai rikoksia koskevien tietojen laajamittaisesta käsittelystä.

Huom! Halutessaan organisaatio voi nimittää tietosuojavastaavan muutenkin.

Pilvipalvelu SoftOne GO antaa vahvan suojan

SUOJAA PALVELIMIA TIETOMURROILTA

SoftOne GO toimii omilla Ruotsissa toimivilla palvelimilla, joita valvotaan ympäri vuorokauden. Palvelimia säilytetään turvallisissa tietokonehalleissa ja niitä suojaavat muun muassa palomuurit ja virustentorjuntaohjelmat. Vain muutamilla toimivaltaisilla henkilöillä on pääsy henkilötietoihin. Käyttöoikeuksia hallinnoidaan käyttäjäroolien kautta, jotka ovat mm. salasanasuojattuja.

POISTA JA ANONYMISOI

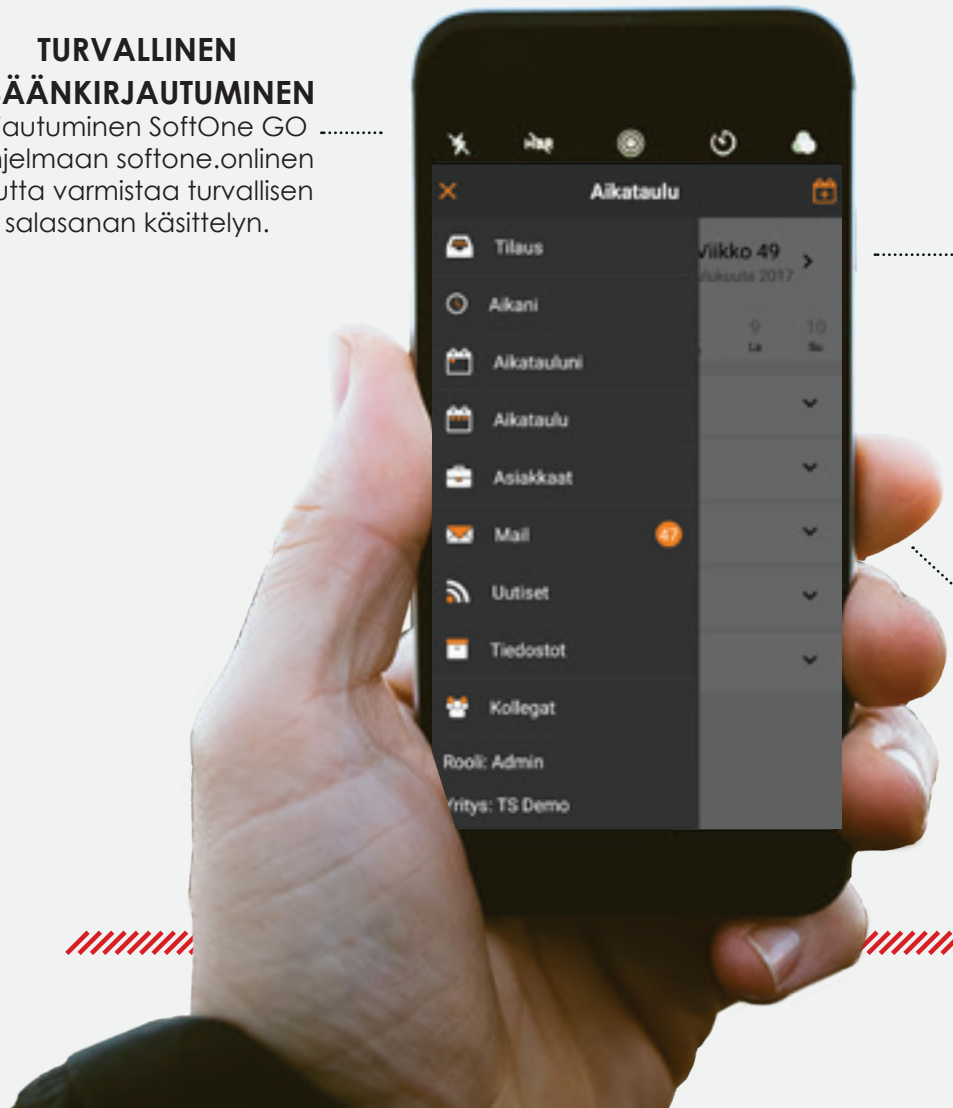
Mahdollisuus poistaa tai anonymisoida henkilötietoja, mikäli laissa ei toisin mainita.

HELPPO SIIRTÄÄ HENKILÖTIETOJA

Henkilötietoja on voitava siirtää järjestelmien välillä. SoftOne GO:n avulla tiedot voidaan muuttaa XML-muotoon ja siirtää sitten useimpiin järjestelmiin.

TURVALLINEN SISÄÄNKIRJAUTUMINEN

Kirjautuminen SoftOne GO -ohjelmaan softone.onlinen kautta varmistaa turvallisen salasanan käsittelyn.



PÄÄSY KERÄTTYIHIN HENKILÖTIETOIHIN

Rekisteröidyllä on oikeus nähdä, mitä henkilötietoja on kerätty. SoftOne GO:sta saa helposti yleiskatsauksen järjestelmään kerätyistä henkilötiedoista. Henkilötietoja on myös helppo päivittää järjestelmään.

TIETOTURVALOUKKAUSTEN HELPPO RAPORTOINTI

Kaikki henkilötietojen käsittelyt SoftOne GO:ssa kirjataan, jotta luvattomat toimet voidaan selvittää ja tapahtuneesta ilmoittaa asianosaiselle henkilölle. Tämä edellyttää, että henkilöiden yhteystiedot ovat ajan tasalla.

Jos jotain silti tapahtuu ...

HUOM!

Jos havaitsette henkilötietoihin kohdistuvan tietoturvaloukkauksen, siitä on ilmoitettava tietosuojaviranomaiselle ja asianosaiselle henkilölle 72 tunnin kuluessa.

Esimerkkejä tällaisesta tilanteesta voivat olla henkilötietoja sisältävän USB-muistin katoaminen, tietomurto tai tilanne, jossa sivullinen henkilö on vienyt osan henkilötiedoista.

Turvallisuus-vinkkejä!

Muista, että suurimmat turvallisuusriskit ovat inhimillinen toiminta ja yrityksen omat työntekijät, joilla on laillinen pääsy tietoihin.

- Käytä monimutkaisia salasanoja ja vaihda ne säännöllisesti.
- Noudata puhtaan pöydän periaatetta. Kirjautumistiedot, USB-muistit ja tulosteet on pantava lukkojen taakse silloin, kun et tarvitse niitä. Tietokone tulee aina lukita, kun et ole paikalla. Käytä tunnistautumista tulostaessa.
- Mieti, mitä kirjoitat sähköpostiin ja mihin vastaat. Kiinnitä huomiota kalasteluviesteihin.

SOFTONE-KONSERNI on ISO 27001-sertifioitu

- turvallisuutesi vuoksi

SoftOne on ISO 27001-sertifioitu. Se tarkoittaa, että meillä on tietoturvallisuuden hallintajärjestelmä.

Sertifiointi on erityisen tärkeä uuden tietosuoja-asetuksen kannalta ja tarjoaa asiakkaillemme turvaa.

Sertifiointi takaa korkean tietoturvatason ja tarkoittaa sitä, että koko organisaation tietoturvatyö on valvottua ja järjestelmällistä.

SAAT PALVELUNTARJOAJAN:

- Jonka kaikki työntekijät ovat erittäin päteviä tietoturva-alan osaajia
- jonka tietoturvallisuutta ja menettelytapoja koskevat riippumattomat ja jatkuvat tarkastukset suoritetaan sertifioidun tietoturvatarkastajan toimesta
- joka edellyttää tärkeimpien toimintojen riskianalyysien päivittämistä

CERTIFIED ISO 27001 CERTIFIED

Tarkistuslista GDPR

SELVITÄ NYT:

- [ ] Käy läpi ja dokumentoi, miten tällä hetkellä käsittelette henkilötietoja.
- [ ] Perehdy tietojenne turvallisuutta koskeviin näkökohtiin riippumatta siitä, säilytetäänkö tietoja tietojärjestelmässä tai varastossa/arkistossa.
- [ ] Perehdy nykyisiin tietojärjestelmiin ja niiden turvallisuuteen. Paikallisesti asennetut järjestelmät voivat aiheuttaa tietoturvariskin.
- [ ] Tarkista, onko IT-palveluntarjoajallasi turvallinen tiedonhallintajärjestelmä ja että palveluntarjoaja on ISO 27001 -sertifioitu.
- [ ] Tiedota säännöllisesti organisaation kaikille yksiköille suunnitteilla olevista muutoksista.
- [ ] Selvitä, tarvitseeko organisaatiosi tietosuojavastaavan. Tietosuojavastaava tulee olemaan keskeinen henkilö GDPR-hankkeessa.
- [ ] Johdon on osoitettava resurssit (aikaa ja rahaa) hankkeen loppuunsaattamiseksi.

SELVITÄ ENNEN 25.5.2018:

- [ ] Varmista, että menettelytavat, asiakirjat ja toimintaperiaatteet ovat valmiina sääntöjen noudattamista varten.
- [ ] Varmista, että henkilötietojen käsittelyä koskevat asiakirjat on päivitetty ja työntekijöitä on tiedotettu päivityksistä.
- [ ] Kouluta organisaatiota voimaan astuvista muutoksista.
- [ ] Päivitä IT-infrastruktuuri, tietojärjestelmä ja tietoturva. Sekä varmista, että ne täyttävät privacy by design -periaatteen mukaiset vaatimukset.
- [ ] Kehitä toimintatapoja tilanteisiin, joissa työskentelette muiden kanssa, sillä ketjun jokainen linkki on henkilökohtaisesti vastuussa henkilötietojen käsittelystä.
- [ ] Luo prosessi, jonka mukaan tietosuojaviranomaiselle ja asianosaiselle henkilölle ilmoitetaan tietoturvaloukkauksesta 72 tunnin kuluessa.

SELVITÄ NIIN PIAN KUIN MAHDOLLISTA:

- [ ] Selvitä, miten henkilötiedot liikkuvat organisaatiossa (elinkaari).
- [ ] Tee sopimus henkilötietojen käsittelijöiden ja / tai henkilötietovastaavien kanssa.
- [ ] Käy läpi ja muokkaa kaikki henkilötietojen käsittelyä koskevat sopimukset.
- [ ] Luo turvallista salasanan käsittelyä koskevat periaatteet ja säännöt.

Selvitä lisää

Olemme koonneet tähän esitteeseen uuden tietosuoja-asetuksen (GDPR) pääkohdat. Lisätietoja saat vierailemalla Suomen tietosuojavaltuutetun sivuilla osoitteessa **www.tietosuoja.fi**

SoftOne®
www.softone.fi

Vantaa
Perintötie 2 b
01510 Vantaa
+358 9 3507 750
myynti@softone.fi

Stockholm
Klarabergsgatan 23
Box 596
101 31 Stockholm
0771-55 69 00

Göteborg
Gårdatorget 1, 4trt
412 50 Göteborg
0771-55 69 00
marknad@softone.se