Sympa HR - täysin GDPR-valmis HR-ratkaisu

Miten takaamme täyden GDPR-valmiuden?

25.5.2018 astuu EU:n uusi tietosuoja-asetus, GDPR (General data protection regulation), voimaan. Toukokuu lähestyy nopeasti. Sympa HR on ollut valmis toukokuun muutoksiin jo kauan sitten, ja takaamme henkilötiedoillenne täyden tietoturvan jatkossa - myös GDPR:n jälkeen.

GDPR:n on yksinkertaistettuna tarkoitus pitää yritysten työntekijöiden henkilöstötiedot ajan tasalla, turvassa ja saataville vain niille, jotka sitä tarvitsevat. Me puolestamme tarjoamme HR-järjestelmän ja asiakkaidemme tietoturva on kaiken toimintamme lähtökohta. GDPR-yhteensopiva HR-järjestelmä helpottaa siirtymäaikaa ja varmistaa tietoturvan helpon ylläpidettävyyden myös jatkossa.

Meiltä saat GDPR-asioissa kokonaisvaltaisen tuen

Olemme aktiivisesti kehittäneet GDPR-prosessejamme ja luoneet käyttöönne erilaisia ohjeita ja materiaaleja tukeaksemme teitä kohti GDPR-valmiutta. Hyödyllistä GDPR-tietoutta on saatavilla esimerkiksi Sympan GDPR-sivustolla sekä asiakkaillemme suunnatussa Sympa HR -tukiportaalissa.

Sympalle tietoturva ja tietosuoja ovat ensiarvoisen tärkeitä, ja noudatamme GDPR:n taustalla vaikuttavia sisäänrakennetun tietosuojan (Privacy by Design) periaatteita. Sympa HR on GDPR-yhteensopiva, ja huolehdimme järjestelmämme tietoturvallisuudesta pitkäjänteisesti myös jatkossa. Jokainen asiakkaamme voi siis nauttia GDPR-yhteensopivasta HR-järjestelmästä. Varmistaaksenne GDPR-yhteensopivuuden organisaationne muiden järjestelmiesi kanssa, olemme koostaneet käyttöönne kätevän GDPR-muistilistan.

On myös paikallaan todeta, että GDPR on uusi asia meistä useimmille. Viranomaisten julkaisemat toimintaohjeet ja -oppaat muuttuvat ja päivittyvät vielä jatkuvasti. Otamme kiitollisena vastaan kaiken palautteen ja autamme mielellämme myös muissa järjestelmään liittyvissä GDPR-kysymyksissä. Olethan siis kysymyksissä rohkeasti meihin sympalaisiin yhteydessä!

Tekniset määritelmät, Sympa HR & GDPR-yhteensopivuus

Halusimme tehdä Sympa HR:n GDPR-yhteensopivuuden mahdollisimman läpinäkyväksi, ja valmistelimme oheisen dokumentin, joka sisältää kaikki tärkeät tekniset määritelmät GDPR:stä sekä asetuksen ja Sympa HR:n yhteensopivuudesta. Tutustu aiheeseen seuraavilla sivuilla, ja kysy rohkeasti, mikäli kysymyksiä herää. Nauti teknisistä yksityiskohdista!

Keijo Karjalainen
Toimitusjohtaja ja perustaja
+358 40 521 8517
keijo.karjalainen@sympa.com

Sympa HR - täysin GDPR-yhteensopiva HR-ratkaisu

Miten takaamme täyden GDPR-valmiuden?

SYMPA HR – AINOA HR-JÄRJESTELMÄ, JONKA TARVITSET
Technopolis Helsinki-Vantaa · Teknobulevardi 3–5, 01530 Vantaa
+358 290 001 200 · sympa.fi · Kotipaikka: Lahti, Finland · y-tunnus: FI19385975

Sympa HR & GDPR-roolit

Rekisterinpitäjä

Sympan asiakkaana olet rekisterinpitäjä. Rekisterinpitäjä tekee sisältöön, prosesseihin ja henkilötietojen (datan) käyttöoikeuksiin liittyvät päätökset.

Henkilötietojen käsittelijä

Sympa, palveluntarjoajana, on henkilötietojen käsittelijä. Käsittelemme asiakkaidemme henkilöstön tietoja ainoastaan tarjotaksemme Sympa HR-palveluratkaisun. Sympa on vastuussa asiakasorganisaatioillemme sekä tietysti suoraan viranomaisille.

Rekisteröity

Rekisteröity-termillä tarkoitetaan Sympan asiakasorganisaation työntekijöitä. Tyypillisesti tähän luetaan myös freelancerit, työnhakijat, alihankkijat, entiset työntekijät ja kaikki muut, joiden henkilötiedot varastoidaan ja käsitellään Sympa HR -järjestelmässä.

Tietosuojavastaava

Laajamittaista datan käsittelyä suorittavilla organisaatioilla on oltava nimetty tietosuojavastaava.

Sympa HR suojelee rekisteröityjen oikeuksia

Sisäänrakennettu tietosuoja

Henkilöstötietojen yksityisyys ja tietoturva ovat Sympa HR -ratkaisun perustuksissa. Liiketoimintamme koostuu henkilöstötietojen käsittelystä, ja sekä yksityisyys että tietosuojan noudattaminen ovat olennainen osa palveluamme.

Yksityisyys on tärkein lähtökohta kaikessa toiminnassamme, niin palvelunkehityksessä, palvelinten ylläpidossa, tukipalveluissa, käyttöönotoissa kuin myynnissä ja markkinoinnissakin. Yksityisyys on myös tärkeä osa sekä käynnissä olevia, että tulevia HR- järjestelmämme kehitysprojekteja. Olemme luoneet tietoturvanhallintajärjestelmämme (ISMS) alusta alkaen mahdollisimman turvalliseksi, ja meille onkin tärkeää saavuttaa ISO27001-standardin mukainen sertifiointi vuosi toisensa jälkeen. Sertifioinnin myötä haluamme osoittaa sitoutumisemme tietoturva-alan keskeisiin standardeihin niiden jatkuvaan kehitykseen. ISMS-käytänteemme ja sertifikaattimme kattavat toimintamme Sympan kaikissa toimintamaissa.

Asiakkaidemme tietoturva on meille kunnia-asia. Arvioimme ja kehitämme Sympan teknisiä sekä organisatorisia suojausmenetelmiä jatkuvasti. Panostamme jatkuvasti myös riskiarvioprosesseihin turvataksemme parhaan mahdollisen tietosuojan ja yksityisyydensuojan kaikille asiakkaillemme myös jatkossa.

Oikeus saada tietoa henkilötietojen keräämisestä ja käsittelystä

Rekisteröidyillä on oikeus saada tietää, milloin ja mitä heitä koskevia henkilötietoja käsitellään ja mitä tallennetaan.

Sympa HR:

- Tarjoaa selkeitä ja luettavia GDPR-yhteensopivia malleja ja asiakirjapohjia käytettäväksi henkilötietojen tietosuojan dokumentointiin
- Ajantasainen Sympa HR -palvelukuvaus ja tiedot henkilötietojen käytön yksityiskohdista ovat aina saatavilla
- Mikäli jokin GDPR-yhteensopivuuteen vaikuttava seikka palvelussamme muuttuu, tiedotamme asianomaisia

Oikeus päästä omiin tietoihin ja tietojen oikaisuun

Rekisteröidyillä on oikeus saada pääsy omiin tietoihinsa ja saada epätarkat ja virheelliset tiedot korjattua.

Sympa HR:

- Tarjoamme kokonaisvaltaisen HR-ratkaisun. Rekisterinpitäjän roolissa asiakkaamme voivat helposti valita, kenellä on pääsy henkilöstötietoihin esimerkiksi vain luku- tai luku ja kirjoitus -oikeuksilla.
- Asiakkaamme voivat myös muuttaa käyttöoikeuksia, jolloin on helppo varmistaa, että vain asiaankuuluvilla henkilöillä on pääsy tiettyihin tietoihin.
- Pääsy käyttäjien omiin tietoihin mukautetaan asiakkaidemme prosessien mukaisesti
- Itsepalvelu pätee myös IT-liittymiin (integraatiot): asiakkaamme valitsevat ja hallitsevat itse, mitä tietoa siirretään Sympa HR -järjestelmään ja sieltä muihin IT-järjestelmiin liittymien yhteydessä.
- Sympa HR -ratkaisu mahdollistaa rekisteröidyille pääsyn omiin tietoihinsa silloinkin, kun he eivät suoraan pääse Sympa HR -järjestelmään. Julkaisemme käyttäjäkokemuspäivityksiä vielä ennen toukokuuta 2018.

Oikeus tietojen poistamiseen eli oikeus tulla unohdetuksi

Rekisteröidyillä on oikeus saada tietonsa poistetuksi,
kun tiedon käsittely ei ole enää aiheellista.

Sympa HR:

- Tarpeettoman tiedon poistaminen on Sympa HR:n perusominaisuus ja tämä voidaan automatisoida tukemaan asiakkaidemme prosesseja. Julkaisemme päivitetyt automaatiotyökalut vielä ennen toukokuuta 2018.
- Tietojen poisto voidaan tehdä myös vaiheittain. Joitakin tietoja tulee säilyttää pidempään kuin toisia (esimerkiksi sopimukset vs. kehityskeskustelut).
- Sympa HR:llä datan poistaminen on aina tietoturvallista ja myös varmuuskopiojärjestelmämme tukevat GDPR:n vaatimuksia.

Oikeus siirtää tiedot järjestelmästä toiseen.

Yksilöillä on oikeus saada omat tietonsa helposti luettavassa muodossa
sekä siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

Sympa HR:

- Tallennettu tieto voidaan siirtää Sympa HR:n ulkopuolelle järjestelmästä tai avointa rajapintaa, APIa käyttäen.
- Sympa HR tukee helppoa ja nopeaa tapaa täyttää tietojen siirrettävyyden vaatimukset.

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle.

Tietoturvaloukkaukset tulee raportoida viranomaisille 72 tunnin kuluessa.

Sympa HR:

- Erillinen turvallisuusasiantuntijoiden tiimi tarkkailee ja vartioi Sympa HR:n tietoturvaa vuorokauden ympäri.
- Hypoteettisen tietoturvaloukkauksen sattuessa ilmoitamme välittömästi asianomaisia ja ohjeistamme asiakkaitamme tiedottamaan viranomaisia ja rekisteröityjä asianmukaisesti.

Sympa HR täyttää tekniset ja organisaatioon liittyvät GDPR-vaatimukset

Sympa HR turvaa tietosi - tallennettuina ja siirrettäessä

Sympan tietoturvapolitiikka on rakennettu turvaamaan henkilöstötietosi. Edistynyt tietoturvajärjestelmä sekä kolmannen osapuolen suorittamat turvallisuuden valvontatarkastukset, auditoinnit, ja sertifioinnit ovat tärkeimmät tietoturvan varmistamisen menetelmät. Tämän lisäksi turvaamme tietosi ja varmistamme GDPR-yhteensopivuuden seuraavilla ominaisuuksilla ja prosesseilla.

Riskiarviot ja riskinhallinta

Riskejä ennakoiva ajattelutapa muodostaa keskeisen osan Sympan laadunvalvonta- (ISO9001-sertifikaatti) sekä tietoturvajärjestelmiä (ISO27001-sertifikaatti). Riskien arviointiprosessissa tunnistetaan ja arvioidaan todennäköisyyksiä, eri skenaarioiden vaikutuksia ja niiden vähentämiskeinojen tunnistamista sekä kartoitetaan jo tunnistettuihin riskeihin liittyviä toimintamahdollisuuksia. Kaikkien asiakkaiden tietojen suojaaminen on Sympan tärkein tehtävä. Tämän vuoksi riskien arviointi- ja hallintaprosessit auditoidaan vuosittain kolmannen osapuolen toimesta.

Salaus

Kaikki tieto, joka tallennetaan Sympa HR:ään tai siirretään Sympan järjestelmästä, salataan vahvalla salauksella sekä tietoa siirrettäessä että tallennettuna.

Käyttäjähallinta, käyttöoikeudet ja tunnistautuminen

Käyttäjäorganisaation kaikki työntekijät lisätään oletusarvoisesti Sympa HR -järjestelmään. Tietyissä tapauksissa organisaatio voi itse rajoittaa pääsyä järjestelmään haluamiltaan osin. Sympa HR on henkilöstötiedon master-järjestelmä, ja tyypillisesti käyttäjät hyödyntävät Sympan HR-järjestelmän tietoja myös muissa IT-järjestelmissä sekä käyttäjähallinnassa.

Käyttäjien oikeuksia tietoihin voidaan tarpeen mukaan rajoittaa järjestelmässä, jotta vain tietyt henkilöt näkevät tiettyjä tietoja. Tyypillisesti pääsy suurimpaan osaan tiedoista määritellään organisaatiohierarkian mukaan, mutta Sympa HR sallii myös räätälöityjen käyttöoikeuksien luomisen, esimerkiksi IT-henkilöstölle.

Sympa suosittelee Single Sign-On (SSO) -menetelmän sekä vahvan tunnistautumisen käyttämistä järjestelmään kirjautumiseen, jotta sisäänkirjautuminen on mahdollisimman käyttäjäystävällistä ja turvallista. SSO-kirjautumista voidaan käyttää yhdessä vahvan, useaan tekijään perustuvan tunnistautumisen kanssa. Mikäli SSO:ta ei ole mahdollista käyttää, Sympa HR tukee myös käyttäjänimellä ja salasanalla tapahtuvaa kirjautumista. Tällöin salasanan monimutkaisuudelle voidaan määrittää organisaatiokohtaiset minimivaatimukset.

Lokitiedostot

Sisään- ja uloskirjautumiset, sekä tietojen hyväksynnät ja hylkäykset kirjataan lokitiedostoon. Kaikki muutokset dataan voidaan kirjata lokitiedostoon, myös esimerkiksi aikaleimat, ja tiedot siitä, kuka on muuttanut mitäkin tietoa järjestelmässä. Sympa HR:n järjestelmänhallintatiimillä on pääsy yksityiskohtaisempiin lokitiedostoihin tarpeen vaatiessa.

Ylläpitotoimenpiteet ja -tapahtumat palvelinympäristössä kirjataan ja lokitiedostot suojataan.

Varmuuskopiot ja tiedon palauttamisen järjestelmät (disaster recovery)

Sympa HR on suunniteltu ja rakennettu ns. aina saatavilla olevaksi (High availability eli HA) järjestelmäksi, jonka kaikissa osissa on redundanssia.

Asiakasdatasta (muutokset) otetaan päivittäiset varmuuskopiot, reaaliaikaisen lokitiedoston kera. Täydelliset varmuuskopiot otetaan kerran viikossa. RPO (recovery point objective), eli tiedon palauttamisen tavoite järjestelmässä on yksi päivä. Kun tietojen menetys on inhimillisen erehdyksen tai ohjelmistovirheen aiheuttama, RPO on kaksi minuuttia.

RTO (recovery time objective) on riskiarvioprosessiin perustuva palautukseen kuluvan ajan tavoite joka, ja se vaihtelee tilanteen mukaan. Primäärin ja redundantin laitteiston vikatilanteissa RTO on 60 minuuttia. RTO palvelinkeskuksen täydellisen menetyksen tapauksessa on 7 päivää.

Palveluntarjoajan pääsy dataan

Rajatulla joukolla Sympa HR:n palveluntoimitus-, ylläpito-, turvallisuus- ja palvelutiimien jäseniä on pääsy Sympa HR -palveluun tallennettuun dataan. Pääsyoikeuksia hallinnoidaan yksilötasolla ja tarvittaessa käyttäjien toimenpiteitä voidaan tarkkailla tapahtumatasolla. Tehtävien eriyttäminen toteutetaan henkilökohtaisten työkuvausten pohjalta. Erillinen turvallisuusselvitys tehdään ennen henkilön nimittämistä kriittiseen rooliin. Oikeudet tarkastetaan tai poistetaan säännöllisesti työntekijän työnkuvan ja vastuiden muuttuessa tai työsuhteen päättyessä.

Tietojen poistaminen

Asiakas voi poistaa henkilöstönsä tietoja järjestelmästä. Poistettu data säilyy tiedon palauttamiseen tarkoitetuissa järjestelmissä tietyn ajan ja poistetaan automaattisesti varmuuskopiointisyklin myötä. Tietojen poistoprosessi on tietoturvan mukainen, ja kun tiedot poistetaan varmuuskopioista, ei niitä voida palauttaa.

Asiakkaan pyynnöstä ja asiakassuhteen päättyessä kaikki asiakkaan tiedot poistetaan tietoturvan mukaisesti Sympa HR -järjestelmästä ja tietokannoista, myös varmuuskopiointijärjestelmistä. Täysi tietojen poisto sovitaan yhdessä asiakkaan kanssa siten, että kaikki tiedot voidaan toimittaa asiakkaalle tai siirtää toiseen asiakkaan käyttämään järjestelmään ennen tietojen lopullista pyyhkimistä.

Ylläpito ja tietojen sijainti

Kaikki EU-alueen asiakkaidemme tiedot varastoidaan EU-alueella sijaitsevissa datakeskuksissa. Ensisijainen hosting-ympäristö sijaitsee Lontoossa. Jotkin palvelun osat, kuten off-site -varmuuskopiot, järjestelmäpalautukset, integraatiot ja binääritiedostojen tallentaminen, toimitetaan toissijaisista EU-alueella sijaitsevista datakeskuksista. Tällä hetkellä keskukset sijaitsevat mm. Saksassa, Irlannissa ja Alankomaissa. Pidämme henkilöstötietosi EU-alueen sisällä myös Brexitin jälkeen.

Vuorokauden ympäri toimivat turvallisuuspalvelut toimitamme nk. follow-the-sun -mallia noudattaen, jonka ansiosta voimme tarjota huipputason turvallisuusasiantuntijat asiakkaidemme käyttöön ympäri vuorokauden. Tiimimme sijaitsevat ympäri maailmaa ja tulevat työvuoroon peräkkäin, jolloin kaikkiin turvallisuusuhkiin voidaan vastata ja ratkaista ne jo sekuntien, ei tuntien kuluessa. Euroopan öisen ajan turvallisuus- ja tarkkailupalvelut toimitetaan Yhdysvalloista US-EU Privacy Shield -sopimuksen mukaisesti.

Hosting-palveluntarjoajinamme on tällä hetkellä mm. Rackspace (pääasiallinen palveluntoimittaja), Microsoft (Azure infrastructure) sekä Amazon (tietojen palauttamisen järjestelmät sekä valinnaiset liittymäteknologiat).

Sympa HR -tukipalvelut tuotetaan Sympan EU/EEA-toimipisteissä.

Liittymät (integraatiot)

Käytämme tiedonsiirtoon aina turvallisia SFTP- tai HTTPS-protokollia. Liittymiä voidaan mukauttaa niin, että ne sisältävät ainoastaan tarpeellisen tiedon. Jos jokin toinen Sympa HR:ään liitettävä järjestelmä (esimerkiksi palkanlaskentajärjestelmäsi) tarvitsee vain yksilön postiosoitteen eikä esimerkiksi henkilötunnusta tai muita tietoja, Sympa HR voidaan asettaa jakamaan liittymässä ainoastaan osoitetieto.

Tietojen säilyttäminen

Rekisterinpitäjänä päätät etukäteen, kenellä on pääsy mihinkin tietoihin Sympa HR -järjestelmässä. Mukauttamalla käyttäjärooleja (esimerkiksi työnkuvan mukaan) voit varmistaa että vain tietyt henkilöt pääsevät arkaluontoiseen tietoon. Henkilötietojen käsittelijänä Sympa ylläpitää lokitiedostoa kaikista käsittelytoimenpiteistä.

Tietojen minimointi

Tietojen minimointi on mitä suurimmassa määrin GDPR:n hengen mukaista. Sympan HR-järjestelmä tukee tietokenttien mukauttamista sekä tarpeettoman tiedon poistamista (ja korjaamista), ja näin helpottaa asiakkaidemme työtä tietokannan siivoamisessa.

Saattaaksemme GDPR:n mukaisen tietojenkäsittelyn asiakkaillemme yhä helpommaksi, teemme järjestelmäämme jatkuvia käytettävyysparannuksia.

Nimimerkit ja nimettömyys järjestelmässä

Sympa HR -ratkaisun palveluntarkkailu, kehitys ja ylläpito vaativat käyttäjien toimien, järjestelmän käytettävyyden ja HR-prosessien tarkkailemista. Sympan HR-järjestelmä hyödyntää laajasti nimimerkkien käyttöä (pseudonymisointia) ja tietojen nimettömäksi saattamista (anonymisointia.) Molemmat käytänteet mahdollistavat parhaan mahdollisen HR-järjestelmän tuottamisen ilman tunnistettavissa olevia henkilöstö- tai henkilökohtaisia tietoja asiakasorganisaatiolta (Personally Identifiable Information, PII).

Tietomurrot

Sympa HR:n tietoturva- ja asiakastietoja tarkkaillaan ja suojellaan kaikkina vuorokaudenaikoina. Sympalla on selkeästi määritellyt toimintaohjeet tietomurtojen tunnistamiseen, niiden vaikutusten minimoimiseen ja niistä tiedottamiseen asiakkaille.

Henkilötietojen käsittely

Henkilötietojen käsittelijänä Sympa tarjoaa Asiakkaalle (Rekisterinpitäjä) sekä ylläpitää elektronista HR-järjestelmää, joka sallii Asiakkaan hallinnoida henkilöstön tietoja kuten työsuhdetietoja, palkkatietoja, kompetensseja ja muita työntekijöitä, entisiä työntekijöitä, työnhakijoita, freelancereita, alihankkijoita sekä vastaavia ryhmiä koskevia tietoja, Asiakkaan niin halutessa.

Asiakas kerää, tallentaa, analysoi ja muutoin käyttää asiakastiliinsä tallennettua tietoa. Sympa ei osallistu näihin toimenpiteisiin vaan toimittaa työkalun, jolla Asiakas voi tehdä kyseiset toimet, ellei Asiakas erikseen pyydä toisin.

Sympa tarkastelee HR-järjestelmään tallennettua tietoa vain siinä määrin kuin on välttämätöntä järjestelmän ylläpitämiseksi Asiakkaan tarkoituksiin (tämä voi sisältää esimerkiksi virheiden korjaamista sekä muiden teknisten ongelmien ratkaisua järjestelmässä). Sympa ei tarkastele HR-järjestelmään tallennettua tietoa enempää kuin on tarpeen itse järjestelmän ja siihen liittyvien palvelujen ylläpitämiseksi.

Tietojenkäsittelyn toimenpiteiden luonne riippuu Asiakkaan asetuksista. Toimenpiteet sisältävät mm. tietojen keräämistä loppukäyttäjiltä sekä API:en kautta, tiedon tallentamista palveluun ja sen varmuuskopiojärjestelmiin, tietojen jakelua loppukäyttäjille (raportointi) ja API:en kautta . Lisäksi myös tietojen muuttamista ja järjestelemistä Asiakkaan ohjeiden mukaisesti.

Sympa noudattaa jatkuvan kehityksen mallia

Muita Sympan GDPR-toimenpiteitä

Koulutus ja valmennus

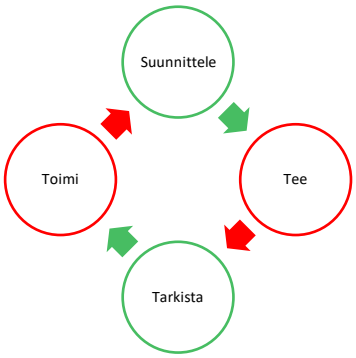
Kaikki Sympan työntekijät käyvät läpi GDPR-valmennuksen, joten yhteyshenkilösi auttaa sinua mielellään GDPR:ään liittyvissä asioissa. Voit myös käyttää tukipalveluamme, jossa on aina neuvoja saatavilla niin puhelimitse kuin sähköpostitsekin. Lisäksi tukiportaalissamme on asiakkaillemme tarjolla aina ajantasaisia materiaaleja.

Sopimusten päivittäminen

GDPR:n vaatimukset on huomioitu Sympa HR -sopimuksissa, mutta pienet päivitykset saattavat tulla ajoittain tarpeellisiksi. Otamme sinuun yhteyttä, mikäli organisaatiosi sopimus vaatii päivittämistä.

Tietoturvan hallinnointi (ISM)

Sympan tietoturvapäällikkö ja Data Protection Officer (DPO) Tommi Surakka johtaa Sympan tietoturvaorganisaatiota, joka ylläpitää Sympan tietoturvahallinnointijärjestelmää (ISMS). Organisaation toimintaan kuuluu jatkuva kehittäminen, riskien arviointi, turvallisuusauditointi, koulutus, jatkuva valvonta ja poikkeustilanteiden hallinta. Sympan tärkein tehtävä on asiakkaiden tietojen suojeleminen, ja otamme tämän tehtävän erittäin vakavasti.



Kuvaus turvallisuusorganisaatiosta ja turvaryhmistä löytyy kaaviosta alta (ISMS A6). Sympa HR:n tietoturvallisuushallinnon toimintamalliin kuuluu jatkuva kehittäminen, joka toimii suunnittele-tee-tarkista-toimi-sykleissä. Sympalle myönnettiin erinomaisen tietoturvan johdosta ISO27001-sertifikaatti ensimmäisen kerran jo 2014, ja siitä lähtien on Sympa saanut joka vuosi sertifikaatin myös uusittua. ISO-sertifikaatin on myöntänyt Bureau Veritas ja se kattaa kaiken Sympan toiminnan ja kaikki toimipaikat. Sertifikaatti ja todistus ovat nähtävillä pyynnöstänne.

Sympa HR:n tietoturvallisuusroolitukset ja tiimit punaisissa laatikoissa. Tietoturva-auditoinnit vaaleanvihreissä laatikoissa.

Tietoturvapäällikkö

- Vastuussa Sympan ISMS:stä

Data Protection Officer

- tiedon suojaamisen ja yksityisyydensuojan valvonta

Tietoturvahallinnointiryhmä

- Jatkuva ISMS-kehittäminen
- Muutoksien hallinta
- Säännölliset kokoukset
- Poikkeustilanteiden hallinnointi

Technical Information Security Group

- Teknisten tietojen turvallisuus
- Teknisen turvallisuuden arkkitehtuuri
- Teknisen turvallisuuden arviointi
- Tietoturvallisuuskoodien arviointi (Information security code reviews)

24/7 tietoturvallisuustiimi

- Tietoturvallisuuden monitorointi ja datan suojelu 24/7
- Nopea reagointi uhkiin 24/7
- Saatavuuden seuranta ja korjaukset 24/7
- Haavoittuvuusskannaukset
- Turvapäivitykset, alustojen ja infrastruktuurin hallinnointi

Järjestelmäoperaattori

- Proaktiivinen turvallisuus- ja saatavuushallinnointi
- Julkaisujen hallinta
- Tekninen tietoturvallisuuden suunnittelu ja hallinnointi tuotantoympäristössä

Sisäiset ISMS-auditoinnit

- Vuosittaiset, yksityiskohtaiset tietoturva-auditoinnit
- Seuraa jatkuvan kehityksen suunnitelmia, jotka kattavat useita vuosia
- Vuosittaiset 5–10 päivän mittaiset auditoinnit

Ulkoiset tietoturva-auditit

- ISMS auditoidaan vastaamaan ISO27001- ja ISO9001-standardeja
- Sertifioitu 2014 lähtien
- Vuosittaiset 3–7 päivän ulkoiset auditoinnit

Tekniset tietoturva-auditit

- Kolmannen osapuolen auditit tekniselle tietoturvalle
- Auditoinnit tehdään ennen suuria muutoksia Sympa HR -palvelussa
- Auditoinnit järjestetään vähintään kerran vuodessa
- Auditoinnit kestävät yli viisi päivää vuosittain

Tietoturvavalvonta

Sympan ISMS kattaa kaikki Sympan toiminnot ja sijainnit. Sympan tietoturvakäytännöt (ISMS A5.1) arvioidaan säännöllisesti ja ovat pyynnöstänne nähtävillä. Yleiskuva Sympan tietoturvan valvontajärjestelmästä ja tärkeimmistä valvontatoimenpiteistä löytyy alta. Toimitamme pyynnöstänne myös kattavamman listan toimenpiteistä (statement of applicability). Valvontatoimenpiteet ovat ISO27001-standardien mukaisia.

Henkilöstöhallinto (HR) (ISMS A7)

Ennen rekrytointia Sympan työntekijät käyvät läpi haastattelu- ja seulontaprosessin. Roolista riippuen (tai roolien vaihtuessa) yksityiskohtaisempi seulontaprosessi voi olla tarpeen. Poliisin turvallisuusselvitykset toteutetaan tarpeen vaatiessa. Kaikki Sympan työntekijät allekirjoittavat salassapitosopimuksen ennen töiden aloittamista. Työsuhteen aikana valmennus- ja koulutusohjelmamme vahvistavat henkilöstömme tietoturva- ja yksityisyysosaamista. Kun työntekijä lopettaa työsuhteensa Sympalla, prosessiimme kuuluu lupien päättäminen, tarvittavien tietojen muutokset ja poistot sekä jatkuvaa kehitystä tukevat lähtöhaastattelut.

Tietojen hallinta (ISMS A8)

Tietojen hallinta käsittää tietojen inventaarioon, omistukseen ja lajitteluun liittyvät prosessit ja työkalut. Lisäksi siihen kuuluvat toimintaohjeet tietojen hyväksyttävään käyttöön sekä fyysisten medioiden käyttöön ja hävittämiseen. Työmme luonteen vuoksi matkustaminen ja etätyöskentely ovat osa normaaleja toimintatapojamme. Tietojen suojelu toteutetaan tietojen salauksen ja fyysisestä sijainnista riippumattomien suojausmetodien avulla.

Oikeuksien valvonta (ISMS A9)

Sympan käyttäjien hallinnointi ja käyttöoikeuden myöntäminen perustuu ajankohtaiseen henkilöstöhallinto- ja alihankkijadataan, jota hallinnoidaan Sympa HR -järjestelmässä. Kaikkiin oikeuksiin ja käyttäjähallintaprosesseihin kuuluu nimetyt vastuut ja säännöllinen seuranta. Pääsy tärkeimpiin järjestelmiin on erittäin rajattua, tarkkaan harkittua ja suojattu tarvittavin toimenpitein. Suojauksessa käytetään parhaita saatavilla olevia suojautumiskeinoja, kuten moneen tekijään pohjautuvaa tunnistautumista, rajoituksia ja sisäänkirjautumista.

Tiedonsalaustekniikat (ISMS A10)

Salaustekniikat ovat tärkein tapa suojata tietoa. Niin siirrettävä kuin tallennettava tieto suojataan aina. Erityisen paljon kiinnitämme huomiota turvallisuuteen tehtäviä suorittaessamme, ja Sympa HR:n asiakasorganisaatioiden kanssa kommunikoidessamme. Vältämme heikon tietoturvan työkaluja, kuten sähköpostia.

Fyysinen turvallisuus (ISMS A11)

Sympa HR:n palvelu- ja muuta tärkeää dataa säilytetään erittäin turvallisissa fyysisissä ympäristöissä. Taatakseen fyysisen turvallisuuden Sympa on valinnut alan parhaat palveluntarjoajat. Tämänhetkiset palveluntarjoajamme ovat saaneet muun muassa seuraavat sertifikaatit: ISO27001, PCI-DSS sekä SSAE16 Type II SOC1, SOC2 ja SOC3. Toimipisteisiin ja tietoihin pääsy on rajoitettu biometrisellä tunnistautumisella, avainkorteilla sekä jatkuvalla valvonnalla. Palveluntarjoajien toimipisteissä on ympärivuorokautinen vartiointi.

Toimenpideturvallisuus (ISMS A12)

Toimenpideturvallisuus perustuu dokumentoituihin menettelytapoihin, vastuisiin sekä muutos- ja kapasiteettihallintaan. Kehitys-, testaus- ja tuotantoympäristöt ovat toisistaan eristettyjä. Asiakastietoja ei käytetä kehitys- tai testausympäristöissä.

Toimintaympäristöt on suojattu haittaohjelmistoja vastaan, tiedosta otetaan varmuuskopioita, toimet kirjataan lokeihin ja lokitiedostot suojataan luvattomalta käytöltä. Ohjelmistojen asentamista toimintaympäristöissä rajoitetaan ja kontrolloidaan turvallisuuden takaamiseksi.

Sympan toimintatapoja ja tietojärjestelmiä auditoidaan säännöllisesti. Haavoittuvuuksia etsitään ja auditoidaan muutosten yhteydessä sekä vähintään vuosittain, jotta kehittyneitä ja edistyneitä haavoittuvuuksien hyväksikäyttökeinoja vastaan voidaan suojautua tehokkaasti.

Viestintäturva (ISMS A13)

Kaikki luottamukselliset elektroniset tiedonsiirrot suojataan vahvan salauksen menetelmin, mikäli tiedonsiirto ei tapahdu tarkkaan turvatussa, eristetyssä verkossa. Kaikki luottamukselliset tiedonsiirrot julkisessa internetissä tehdään vahvan salauksen alla. Verkot eristetään aina, kun se on tarkoituksenmukaista. Henkilöiden välistä viestintää suojataan luottamuksellisuuslausekkeiden ja salassapitosopimusten avulla.

Kehitys ja ylläpito (ISMS A14)

Turvallisuustiimi seuraa tarkasti kehitys- ja ylläpitoprosesseja. Tuotearkkitehtuuria sekä suunnittelu- ja kehitystoimia arvioi erillinen tekninen turvallisuustiimi. Kaikki ohjelmistomuutokset arvioidaan erikseen ennen julkaistavaksi hyväksymistä. Kaikki ohjelmistomuutokset, kolmannen osapuolen komponenttimuutokset mukaan lukien, kirjataan lokitiedostoon ja niitä voidaan seurata yksityiskohtaisesti. Laaduntarkkailu- sekä testausprosesseihin kuuluvat myös turvallisuustestaus sekä haavoittuvuuksien etsiminen ja hallinta.

Alihankkijasuhteet (ISMS A15)

Sympa kantaa täyden vastuun alihankkijoistaan ja palveluntoimittajistaan. Palveluntoimittajasuhteisiin liittyvät riskit minimoidaan turvallisuuskäytäntöjen, ohjeistuksen ja opastuksen sekä luottamuksellisuuslausekkeiden ja salassapitosopimusten avulla. Muita riskejä minimoidaan tietoturvavakuutusten avulla.

Tietoturvarikkomusten hallinta (ISMS A16)

Tietoturvarikkomukset, parannukset sekä tietoturvaan liittyvä palaute kirjataan ja käsitellään erikseen dokumentoitujen käytäntöjen mukaisesti. Prosessit vaihtelevat kriittisyyden mukaan; kriittiset tapahtumat käsitellään välittömästi ja alhaisen prioriteetin tapahtumat käsitellään säännöllisissä turvallisuusryhmän kokouksissa. Kaikki palveluntoimittamisen kanssa työskentelevät henkilöt ovat tietoisia tietoturvarikkomusten hallintaan liittyvistä käytännöistä.

Toiminnan jatkuvuus (ISMS A17)

Sympa HR -järjestelmän tietoturva ja palvelun jatkuvuus ovat elintärkeitä Sympan liiketoiminnan kannalta. Jatkuvuusriskien ja -mahdollisuuksien tunnistaminen on Sympan ISMS-suunnitelman keskeisin osa. Jatkuvuus varmistetaan tarkalla suunnittelulla, arvioinneilla sekä säännöllisillä kolmannen osapuolen suorittamilla auditoinneilla. Sympan järjestelmän jatkuvuussuunnittelu perustuu jatkuvan saatavuuden malliin sekä täysin redundanttiin infrastruktuuriin.

Sisäinen valvonta / ohjeidenmukaisuus (ISMS A18) (Compliance)

Sisäinen valvonta (compliance) tarkoittaa voimassa oleviin lakeihin, säännöksiin, viranomaisten opastuksiin sekä sopimusvaatimuksiin mukautumista. Erikoishuomiota kiinnitetään immateriaalioikeuksiin sekä henkilötietojen (PII) käsittelemiseen liittyviin säädöksiin.

Tietoturvan ohjeidenmukaisuutta arvioi säännöllisin väliajoin kolmannen osapuolen edustaja.

TIIVISTELMÄ

GDPR yhteistyömme: Takaamme henkilötietojen käsittelijän vastuut

Henkilötietojen käsittelijän vastuut:

- Sympa, henkilötietojen käsittelijänä, informoi rekisterinpitäjää välittömästi, mikäli uskomme rekisterinpitäjän ohjeistusten olevan ristiriidassa GDPR-vaatimusten tai EU:n tai sen jäsenvaltioiden lakien kanssa
- Sympa, henkilötietojen käsittelijänä, sitoutuu tekemään ja on tehnyt toimenpiteitä, jotka auttavat rekisterinpitäjää kunnioittamaan rekisteröityjen oikeuksia
- Sympa, henkilötietojen käsittelijänä, sitoutuu avustamaan ja avustaa rekisterinpitäjää hankkimaan Data Protection Act (DPA) -hyväksynnät silloin, kun se on tarpeen
- Sympa, henkilötietojen käsittelijänä, sitoutuu palauttamaan tai tuhoamaan ja tuhoaa tai palauttaa henkilökohtaisen datan yhteistyön päättyessä rekisterinpitäjän kanssa.
- Sympa, henkilötietojen käsittelijänä, sitoutuu toimittamaan ja toimittaa rekisterinpitäjälle kaiken tarpeellisen tiedon, jotta rekisterinpitäjä voi osoittaa GDPR-yhteensopivuutensa
- Sympa, henkilötietojen käsittelijänä, sitoutuu informoimaan ja informoi rekisterinpitäjää tietomurroista ilman tarpeetonta viivettä
- Rekisteröidyt voivat esittää vaateita suoraan henkilötietojen käsittelijälle (Sympa)

Sympa HR on täysin GDPR-yhteensopiva myös jatkossa

Kehitämme palveluamme sitä mukaa kun GDPR tai mikä hyvänsä muu EU-säädös kehittyy. Asiakkaanamme voit olla varma, että käytössäsi on aina turvallinen ja tietoturvasäädösten mukainen palvelu, jossa työntekijädatasi on aina ajan tasalla ja turvassa.

Esimerkkejä jatkuvista GDPR-yhteensopivuuden varmistavista toimistamme:

- Jatkuvat tietoturvatoimenpiteiden arvioinnit
- Redundanssin ja varmuuskopioiden varmistaminen
- Säännöllisten tietoturvaturvatestien suorittaminen

GDPR edellyttää, että henkilöstötiedot ovat aina ajan tasalla ja saatavilla ainoastaan niitä tarvitseville.

OTA YHTEYTTÄ

Onko sinulla kysymyksiä tai kerrottavaa?
- Älä epäröi ottaa yhteyttä!

Kuulemme mielellämme aina asiakkaistamme ja haluamme kuulla teiltä kehitysehdotuksia ja kysymyksiä. Kaikki muutkin yhteydenotot otamme ilolla vastaan!

Henrikki Kainulainen
Asiakkuusjohtaja
+358 50 537 4727
henrikki.kainulainen@sympa.com

Tommi Surakka
Data Protection Officer (DPO)
+358 50 4308360
tommi.surakka@sympa.com

Mikko Kojo
Tuotejohtaja
+358 50 371 7975
mikko.kojo@sympa.com

Keijo Karjalainen
Toimitusjohtaja ja perustaja
+358 40 521 8517
keijo.karjalainen@sympa.com