COR Groupin tietoturva- ja tietosuojapolitiikka

Sisällysluettelo

1. Politiikan tarkoitus, tavoite ja soveltamisala

Tämä Cor Group -konsernin tietoturva- ja tietosuojapolitiikka määrittää ne pääperiaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita Cor Group-konsernin yhtiöiden ja liiketoimintojen (myöhemmin Konserni) toiminnassa noudatetaan tietoturvan ja tietosuojan toteuttamisessa ja kehittämisessä. Politiikan määrittämissä periaatteissa, vastuissa ja toimintatavoissa huomioidaan soveltuvan lainsäädännön mukainen tietoturvan ja tietosuojan korkea taso. Tietojen käsittely tukee eri liiketoimintojen palveluiden tuottamista. Käsiteltävät tietoaineistot sisältävät liiketoiminnalle tärkeitä sekä potilaisiin, asiakkaisiin, työntekijöihin ja omaan toimintaan liittyvää tietoa, jotka ovat lainsäädännön perusteella suojattava.

Tietoturvan ja tietosuojan hallintamalli on rakennettu määrittämällä periaatteet, toimintatavat ja käytänteet Konsernille ja viestimällä ne henkilöstölle ja sidosryhmille. Hallintamallia päivitetään ja ylläpidetään lainsäädännön ja Konsernin toiminnan tarpeiden mukaisesti.

Tämä politiikka kattaa Konsernin liiketoiminnot ja tukitoiminnot sekä ulkoistukset, hankinnat ja toiminnan sopimuskumppaneiden kanssa. Politiikka asettaa perustan ja vähimmäistason siinä määritetyille tietoturvan ja tietosuojan periaatteille, vastuille ja toimintatavoille, joiden soveltamista ja toteuttamista tarkennetaan tietoturvan ja tietosuojan vaatimuksilla, ohjeistuksilla ja muulla dokumentaatiolla.

2. Noudatettavat periaatteet

Tietoturvan ja tietosuojan ensisijainen tarkoitus on varmistaa liiketoiminnan jatkuvuus, sekä käytössä olevan tiedon täsmällisyys, eheys ja luottamuksellisuus. Tietojenkäsittelyn tulee olla mahdollisimman virheetöntä, tehokasta, luotettavaa ja lainmukaista. Tietoturvan ja tietosuojan periaatteet ja niiden toteuttamiseksi määritetyt vaatimukset ja muu tarkentava dokumentaatio perustuvat liiketoiminnan vaatimuksiin, toimialan lainsäädäntöön ja henkilötietojen käsittelyn osalta yleisen tietosuoja-asetukseen ja muun kulloinkin soveltuvaan lainsäädäntöön sekä soveltuvin osin tietoturvan ja tietosuojan hyvien käytäntöjen standardeihin sekä jatkuvan parantamisen malleihin. Konsernissa sitoudutaan tietosuoja-asetuksen edellyttämän osoitusvelvollisuuden mukaisesti osoittamaan, että henkilötietojen käsittelyn periaatteita on noudatettu.

Kaikessa tietojen käsittelyssä noudatetaan riskiperusteista lähestymistapaa. Tietoturvariskit arvioidaan liiketoimintavaikutusten perusteella ja riskienarvioinnissa huomioidaan tiedon kriittisyys sekä tiedon luottamuksellisuudelle, eheydelle ja täsmällisyydelle asetetut tavoitteet. Henkilötietojen käsittelyssä riskejä arvioidaan lisäksi rekisteröidyn oikeuksille ja vapauksille aiheutuvan haitan perusteella. Kun käsittelyn arvioidaan aiheuttavan rekisteröidylle korkean

riskin tai laki tai tietosuojaviranomainen edellyttää arviointia, käsittelylle suoritetaan tietosuojan vaikutustenarviointi. Tietojen käsittelyyn tai sen toteutukseen osallistuviksi sopimuskumppaneiksi valitaan vain sellaisia toimijoita, jotka noudattavat Politiikan ja tarkentavan dokumentaation mukaisia vaatimuksia ja toimintatapoja. Konsernissa on määritetyt vastuut, prosessit ja ohjeistukset tietoturvan ja tietosuojan riskienarviointiin. Riskien arvioinnit tehdään tiedon käsittelyä suunniteltaessa ja päivitetään olennaisten muutosten yhteydessä.
Henkilötietojen käsittely toteutetaan Konsernissa koko tiedon elinkaaren ajan tietojen keräämisestä niiden tuhoamiseen huomioiden sisäänrakennetun ja oletusarvoisen tietosuojan ja muut tietosuojaperiaatteet ja rekisteröidyn oikeudet.

Henkilötietojen käsittely suunnitellaan etukäteen siten, että käsittely on lainmukaista, asianmukaista ja läpinäkyvää ja tehdään tiettyjä ja nimenomaisia tarkoituksia varten lainmukaisella oikeusperusteella. Henkilötietoja kerätään vain käsittelyn tarkoitukseen nähden tarpeellinen määrä. Tietojen oikeellisuus pyritään varmistamaan ja epätarkat tai virheelliset tiedot poistetaan tai oikaistaan viipymättä rekisteröidyltä itseltään tai luotettavasta lähteestä. Kun tiedot eivät ole enää tarpeellisia käsittelylle määritettyyn tarkoitukseen, ne tuhotaan asianmukaisesti. Henkilötietoja käsitellään luottamuksellisesti ja turvallisesti huomioiden olosuhteet ja tietoihin liittyvät riskit. Konsernissa toteutetaan asianmukaiset tekniset ja organisatoriset suojatoimet sen varmistamiseksi, että henkilötietojen käsittely tapahtuu soveltuvan lainsäädännön mukaisesti.

Konsernissa toteutetaan asianmukaiset toimenpiteet rekisteröityjen oikeuksien toteuttamiseksi ja oikeuksien käyttämisen helpottamiseksi. Rekisterinpitäjän on huolehdittava siitä, että henkilötietojen käsittely toteutetaan läpinäkyvästi ja rekisteröidylle annetaan rekisteröidyn pyytäessä tieto siitä, käsitelläänkö rekisteröidyn henkilötietoja vai ei. Silloin, kun rekisteröidyn tietoja käsitellään, rekisteröidylle annetaan mahdollisuus saada jäljennös käsiteltävistä henkilötiedoista, virheelliset tai puutteelliset henkilötiedot korjataan tai poistetaan ja tiedot voidaan rekisteröidyn pyytäessä poistaa ja tietojen käsittelyä voidaan rajoittaa tai käsittely voidaan lopettaa rekisteröidyn vastustaessa käsittelyä. Rekisterinpitäjä vastaa siitä, että rekisteröidyn tietosuoja-asetuksen mukaiset oikeudet toteutetaan siten, kun oikeudet soveltuvat kussakin yksittäistilanteessa huomioiden käsittelytilanteen ja oikeusperusteen.

Tietoja ei luovuteta ulkopuolisille tahoille, ellei luovutukselle ole lain asettamaa perustetta. Henkilötietoja ei siirretä tai tallenneta EU:n tai Euroopan talousalueen ulkopuolelle ilman asianmukaista siirtoperustetta.

3. Tietoturvan ja tietosuojan toteuttaminen

Organisoituminen ja vastuut

Cor Groupin hallituksella on tietoturva- ja tietosuoja-asioiden Konsernitasoinen vastuu. Tähän kuuluu vastuu Konsernin tietoturva- ja tietosuojapolitiikasta, Konsernitasoisten ohjeistusten vahvistamisesta sekä tietoturvan ja -suojan kehittämisen järjestämisestä ja resursoinnista.

Konsernin liiketoimintojen johdolla ja yhtiöiden hallituksilla ja toimivalla johdolla on vastuu tietoturvan ja tietosuojan tavoitteiden, periaatteiden ja toimintatapojen mukaisen toiminnan toteuttamisesta ja niiden seurannasta sekä valvonnasta omassa organisaatiossaan. Jokaisessa Konsernin yhtiössä ja liiketoiminnossa tulee täsmentää tietoturvan ja tietosuojan toteuttamisen vastuut ja roolit organisaatiossaan ja huolehtia tarvittavasta ohjeistuksesta ja koulutuksesta.

Jokaisen Konsernin yhtiön ja liiketoiminnon on huolehdittava asianmukaisten tietoturva- ja tietosuojavaatimusten ja ohjeiden toteuttamisesta omien sopimuskumppaniensa ja toimittajiensa kanssa, sekä tunnistettava käsittelemien henkilötietojen käsittelyroolit. Henkilötietojen rekisterinpitäjä on se Konsernin yhtiö, liiketoiminto tai itsenäinen ammatinharjoittaja, joka kulloinkin määrittelee yksin tai yhdessä toisen rekisterinpitäjän kanssa henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä tai yhteisrekisterinpitäjät vastaavat henkilötietojen käsittelyn lainmukaisuudesta, tietosuojaperiaatteiden noudattamisesta ja sen lukuun toimivien henkilötietojen käsittelijöiden suorittamasta käsittelystä, käsittelijöiden ohjeistamisesta, valvonnasta ja sopimuksista.

Konsernin tietoturvan ja tietosuojan ohjausryhmä kehittää toimintaa ja seuraa tietoturva ja -suojatyön toteutumista.

Konsernin tietosuojavastaava vastaa tietosuoja-asioiden neuvonnasta ja opastuksesta vastuualueellaan, seuraa tietosuoja-asetuksen ja muun soveltuvan tietosuojalainsäädännön noudattamista ja raportoi Konsernin johdolle. Tietosuojavastaava toimii rekisteröidyille ja valvontaviranomaiselle tietosuojan yhteyshenkilönä.

Konsernin tietoturvajohtaja vastaa konsernin yhteisten palveluiden tietojärjestelmien tietoturvallisuudesta sekä tietoturvaan liittyvästä neuvonnasta ja opastuksesta. Tietoturvan tilannekuvasta raportoidaan Konsernin hallitukselle sekä liiketoimintayksiköiden tietoturvan yhteyshenkilöille.

Yrityskohtaisista sovelluksista ja palveluista vastaa pääsääntöisesti yritys itse mutta näiden hankintojen yhteydessä tehdään näille esitys konsernin arkkitehtuuriryhmälle, joka tukee yrityksiä tietoturvan ja tietosuojan osalta ja toimii samalla myös kontrollipisteenä.

Konserni pyrkii vahvistamaan ja ylläpitämään työntekijöidensä ammatillista tietoturva- ja tietosuojaosaamista. Konsernin uudet työntekijät suorittavat työsuhteen alkaessa tietoturva- ja tietosuojaperehdytyskoulutuksen, jonka lisäksi henkilöstölle järjestetään vuosittain pakollinen tietoturva- ja tietosuojakoulutus. Koulutusten suorituksia valvotaan Konsernin henkilöstöhallinnon ja Rekisterinpitäjän toimesta. Pakollisten koulutusten lisäksi henkilöstölle viestitään aktiivisesti alueen uutisista ja muutoksista, sekä tuotetaan erilaisia harjoituksia ja koulutuksia. Jokaisen työntekijän on toiminnassaan noudatettava tietoturva- ja tietosuojapolitiikkaa, sitä täydentävää tarkentavaa dokumentaatiota sekä lainsäädäntöä.

Politiikkaa tarkentava muu dokumentaatio

Politiikan soveltamista ja toteuttamista ohjataan tarkemmin erilaisilla Cor Group-konserni- tai liiketoimintokohtaisilla tietoturvan ja tietosuojan dokumenteilla, joilla voidaan määrittää toteutustavat tai vaatimukset tietoturvan ja tietosuojan johtamisjärjestelmän ja hallintamallin eri osa-alueille. Näihin lukeutuu suojatoimien vähimmäistasot, ylläpidettävät tietoturvan ja tietosuojan dokumentaatiot, tietoturvan ja tietosuojan toteutuksen roolit, vastuut ja tehtävät sekä noudatettavat prosessit sekä tietoturvan ja tietosuojan periaatteiden, vaatimusten ja ohjeistusten noudattamisen seuranta.

Konsernitasoisilla tietoturva- ja tietosuojavaatimuksilla säädetään kaikille konsernin yhtiöille ja liiketoiminnoille yhteiset vaatimukset, jotka tulee toiminnassa toteuttaa. Lisäksi tietoturva- ja tietosuojavaatimuksia voidaan laatia yhtiö- tai liiketoimintokohtaisesti huomioiden liiketoiminnan vaatimukset ja toimialan lainsäädäntö. Tietoturvan ja tietosuojan vaatimukset tukevat laadukasta toimittajanohjausta, sekä tietoturva- ja tietosuojaprosessien kehittämistä. Cor Group-konsernin tietoturva- ja tietosuojavaatimukset katselmoidaan ja päivitetään vuosittain konsernin tietoturvan- ja tietosuojan operatiivisen työryhmän toimesta ja hyväksytetään konsernin ICT-johtoryhmän toimesta.

Tietoturva- ja tietosuojaohjeistukset ovat tietoturvan ja tietosuojan toimintatapoja, prosesseja ja käytänteitä kuvaavia ohjeita. Ohjeistukset voivat olla yrityskohtaisia, palvelukohtaisia tai esimerkiksi järjestelmäkohtaisia. Jokaisen ohjeistuksen ylläpidosta vastaa nimetty henkilö, jonka tukena on organisaation tietoturvasta ja tietosuojasta vastaavat henkilöt.

Toimintatapa tietoturvan ja tietosuojan vaarantuessa

Käsitellyt tiedot pyritään turvaamaan tietoturvaloukkauksilta ja henkilötietojen tietoturvaloukkauksilta toteuttamalla käsittelyyn liittyvää riskiä vastaavat tekniset ja organisatoriset suojatoimet sekä valvomalla tietojen käsittelyä määritettyjen vaatimusten mukaisesti erilaisilla valvontaratkaisuilla.

Konsernissa on määritetty toimintatavat, ohjeet ja vastuut tietoturvaloukkausten ilmoittamiseen ja käsittelyyn sisäisesti yhtiöissä ja liiketoiminnoissa. Havaitut tietoturva- ja tietosuojaloukkaukset tai epäilyt tutkitaan viipymättä ja ryhdytään tapahtuman luonteen vaatimiin toimenpiteisiin.

Konsernissa dokumentoidaan kaikki tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa. Tapahtuneesta ilmoitetaan tietosuoja-asetuksen edellyttämällä tavalla lainmukaisten määräaikojen mukaisesti.

4. Politiikan hyväksyntä

Tietoturva- ja tietosuojapolitiikan hyväksyy Cor Group-konsernin hallitus. Politiikka katselmoidaan konsernin tietoturvan ja tietosuojan operatiivisen ryhmän toimesta vuosittain määritetyn tarkastelukäytännön mukaisesti tai merkittävien tietoturvaan ja tietosuojaan vaikuttavien muutosten yhteydessä.

Tämä politiikka on hyväksytty Cor Groupin hallituksessa. Viimeisin versio on päivitetty konsernin tietoturvan ja tietosuojan operatiivisen ryhmän toimesta ja hyväksytty konsernin ICT-ohjausryhmässä 15.12.2023.