TIETOTURVAKÄSIKIRJA – FYSSARIT

1. Johdanto

EU:n yleistä tietosuoja-asetusta (GDPR) on sovellettu 25.5.2018 alkaen kaikessa henkilötietojen käsittelyssä. Sen tavoitteena on suojella luonnollisen henkilön oikeuksia ja vapauksia henkilötietojen käsittelyssä. EU:n tietosuoja-asetuksen määräyksiä täydentää 1.1.2019 voimaan tullut kansallinen Tietosuojalaki. Näiden lisäksi henkilötietojen käsittelyä ohjaavat monet muut lait, kuten esim. Julkisuuslaki ja sosiaali- ja terveydenhuollon erityislainsäädäntö.

Tämä tietoturvaohje on tarkoitettu Fyssarit Oy osakkaille ja henkilöstölle sekä yrityksen toimeksiannosta työskenteleville.

1. Henkilötietojen käsittelyä koskevat periaatteet

Rekisterinpitäjän on toteutettava EU:n tietosuoja-asetuksessa määritetyt henkilötietoja koskevat periaatteet.

* Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Lainmukaiselle henkilötietojen käsittelylle on oltava käsittelyperuste, kuten rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoite tai elintärkeiden etujen suojaaminen. Rekisteröidylle on myös kerrottava, mitä tietoja hänestä kerätään, mihin tarkoitukseen, millä tavoin niitä käsitellään ja mitä oikeuksia hänellä on.

* Käyttötarkoitussidonnaisuus

Tietojen käsittelyn tarkoitus tulee suunnitella ja määritellä etukäteen. Tietoja ei saa myöhemmin käyttää muihin kuin ennalta määritettyihin tarkoituksiin.

* Tietojen minimointi

Käsiteltävien henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja. Tietoja saa käsitellä vain silloin ja sen verran, kuin on tarkoituksen mukaista.

* Tietojen täsmällisyys

Tietojen on oltava ajan tasalla ja täsmällisiä. Virheelliset ja puutteelliset henkilötiedot on oikaistava.

* Tietojen säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan, kuin on tarpeellista tietojen käyttötarkoitusta varten. Säilytysaika tulee suunnitella ja sille on oltava perusteet.

* Tietojen eheys ja luottamuksellisuus

Henkilötietojen käsittelyn on oltava turvallista ja luottamuksellista. Rekisterinpitäjän on suoritettava riskienhallintaa ja suojattava tiedot luvattomalta käsittelyltä sekä vahingossa tapahtuvalta hävittämiseltä ja vahingoittumiselta.

* Rekisterinpitäjän osoitusvelvollisuus

Rekisterinpitäjän on pystyttävä osoittamaan noudattavansa edellä mainittuja tietosuojasäädöksiä ja -periaatteita.

1. Käyttöoikeudet henkilötietojärjestelmään

Käyttäjä tunnistetaan käyttäjätunnuksella. Käyttäjätunnus ja salasana ovat henkilökohtaisia, eikä niitä saa luovuttaa kenellekään muulle. Käyttäjä sitoutuu tunnusten huolelliseen säilyttämiseen. Jokainen käyttäjä vastaa omalla käyttäjätunnuksellaan tehdyistä kirjautumisista ja järjestelmään tehdyistä merkinnöistä sekä tietojen katselusta.

1. Potilas- ja asiakastietojen käsittely, salassapito ja vaitiolovelvollisuus

Potilas- ja asiakastietojen käyttötarkoitus on potilas- ja asiakassuhteen hoitaminen ja sekä niihin liittyvien palvelujen toteuttaminen. Tiedot ovat salassa pidettäviä, eikä niitä saa luovuttaa ulkopuolisille. Salassapitovelvollisuus pitää sisällään asiakirjasalaisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon.

* Salassa pidettävää asiakirjaa ei saa näyttää eikä luovuttaa sivullisille ilman laissa säädettyä oikeutta tai asiakkaan suostumusta.
* Vaitiolovelvollisuus tarkoittaa myös suullisesti saatuja tai tallentamattomia tietoja. Vaitiolovelvollisuus jatkuu myös työsuhteen päättymisen jälkeen.
* Hyväksikäyttökielto tarkoittaa sitä, ettei vaitiolovelvollinen henkilö saa käyttää salassa pidettäviä tietoja omaksi tai toisen hyödyksi tai vahingoksi.

Työntekijällä on oikeus käsitellä potilas- ja asiakastietoja silloin, kun hän on osallinen potilaan hoitoon tai siihen liittyviin tehtäviin. Tietoja saa käsitellä vain siinä laajuudessa, kuin sen hetkiset työtehtävät edellyttävät.

1. Toimitilaturvallisuus

* Asiakaspalveluspisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle tai sivullisille.
* Säilytä tiedot ja laitteet turvallisessa paikassa, esimerkiksi lukitussa kaapissa ja huoneessa. Huolehdi myös, ettei pöydille, roskakoreihin tai muualle jää salassa pidettäviä asiakirjoja tai muistiinpanoja. Kun hävität salassa pidettäviä asiakirjoja, käytä aina tietosuojajätesäiliötä.
* Älä jätä kannettavaa päätelaitetta ilman valvontaa.
* Lukitse työhuoneen ovi työpäivän päättyessä ja aina kun poistut työpisteeltä pidemmäksi aikaa. Ulko-oven lukitseminen on varmistettava aina kun työpaikalta poistutaan päivän päätteeksi ja myös aukioloaikojen ulkopuolella, vaikka työntekijä olisikin vielä paikalla.

1. Internetin ja sähköpostin käyttö

Työhön liittyvässä internetin käytössä tulee olla erityisen huolellinen, sillä useimmat haittaohjelmien levitykset ja tietojenkalastelut tehdään juuri internetin kautta. Henkilökohtaiseen viestintään käytetään omaa yksityistä sähköpostia, ei työpaikan sähköpostia.

* Käytä vain tunnettuja, luotettuja ja asiallisia palveluja.
* Poistu aina palvelusta sen omalla uloskirjautumistoiminnolla.
* Ohjelmien lataaminen ja asentaminen internetin kautta on kielletty.
* Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työpaikan päätelaitteisiin tai palvelimelle.
* Internetin kautta ei saa välittää salassa pidettäviä tai luottamuksellisia tietoja ilman asianmukaista salausta/suojausta.
* Kaikkeen asiakastietoja tai muita salassa pidettäviä tietoja sisältävään sähköpostiviestintään on käytettävä suojattua sähköpostia.
* Sähköpostin lähettäjätieto on helppo väärentää, joten varmista aitous aina, jos on vähänkin syytä epäilyyn.
* Sähköpostin liitetiedostot voivat sisältää viruksia ja haittaohjelmia. Älä koskaan avaa liitteitä tai linkkejä sähköpostiviesteistä, jotka ovat tulleet tuntemattomalta lähettäjältä, ovat epätavallisesti otsikoituja tai muuten outoja.
* Varo kalasteluviestejä, joissa pyydetään syöttämään tunnuksia ja salasanoja aidon näköisille sivustoille.
* Roskapostiviestien ”spammit” tulee poistaa avaamatta.
* Olet vaitiolovelvollinen myös vahingossa saamistasi viesteistä tai kuulemistasi asioista. Ilmoita väärään osoitteeseen tulleesta sähköpostista lähettäjälle.

1. Tietoturvaloukkauksesta ilmoittaminen

Tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan luvattomasti sivulliselle tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkaus voi olla vahinko tai tahallinen tapahtuma.

Tietoturvaloukkauksia ovat esimerkiksi asiakas- tai potilastietojen postittaminen väärälle henkilölle, asiakas- tai potilastietojen katselu ilman asiallista syytä, tietojen kirjaaminen väärälle henkilölle, haittaohjelmatartunta, varastettu tietokone tai murtautuminen henkilötietorekisteriin.

EU-asetuksen mukaan rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset ja tehtävä niistä ilmoitus viranomaiselle sekä rekisteröidylle, jonka tietoja loukkaus koskee. Ilmoitus on tehtävä 72 tunnin kuluessa siitä, kun rekisterinpitäjä on saanut tietoturvaloukkauksen tietoonsa.