TERVEYSKAUPAN TIETOSUOJAOPAS

Tämän oppaan avulla pääset käytännönläheisesti alkuun tietosuoja-asian toteuttamiseksi terveyskaupassa. Oppaassa on esimerkein käyty läpi EU:n tietosuoja-asetuksen velvoitteiden huomioiminen.

Terveyskaupan tietosuoja-oppaan avulla pystyt perehtymään tietosuoja-asioihin ja tarvittaessa osaltaan osoittamaan viranomaiselle, että yrityksessäsi tietosuoja-asiat ovat kunnossa.

Terveyskaupan tietosuoja-opas on vapaasti luontaistuote- ja terveys-kauppojen käyttöön. Opasta päivitetään säännöllisesti. Lisäksi Suomen Terveystuotekauppiaiden Liiton jäsenyrityksille on tehty terveyskaupalle räätälöityjä mallipohjia rekisteriselosteista.

ver. 14.5.2018

JOHDANTO

EU:n tietosuoja-asetus (GDPR) voi kuulostaa aluksi monimutkaiselta ja vaikealta ymmärtää. Kyse on yksinkertaistettuna siitä, että yrityksessä olevia henkilötietoja käsitellään ja säilytetään asianmukaisesti. Aikaisemmin henkilötietojen käsittely oli huomioitu henkilötietolaissa ja monet sen periaatteista säilyvät ennallaan. Nykyiseen henkilötietolakiin verrattuna tietosuoja- asetus sisältää yrityksille uusia velvoitteita.

Terveyskaupan tietosuojaopas on helppo työkalu täyttää tietosuoja-asetuksen velvoitteet yrityksessäsi.

> Vinkki: Jos tietosuoja-asetus ja sen velvoitteet tuntuvat aluksi vierailta, niin vertaa sitä ajattelussasi elintarvikehuoneiston omavalvontasuunnitelmaan. Elintarvikehuoneiston omavalvontasuunnitelmaan on kirjattu asiat, joilla varmistetaan myymiisi elintarvikkeisiin, kuten ravintolisiin liittyvää kuluttajaturvallisuutta. Omavalvontasuunnitelmaan on kirjattu terveyskauppasi toiminnan rutiinit, jotka ovat mukana arjen toiminnassa. Tietosuoja-asioiden vaatima omavalvonta on hyvin samankaltainen kuin elintarvikkeisiin liittyvä omavalvonta.

Tietosuoja-asiassa pääset hyvin alkuun, kun tämän oppaan myötä ryhdyt pohtimaan, millaisia tietoja yrityksessäsi kerätään.

Tietosuoja-asetuksen velvoitteet kirjataan tiedonhallintasuunnitelmaan, jolla varmistetaan henkilötietojen oikea hallinta- ja käsittely terveyskaupassa. Yrityksessä olevien henkilötietojen käsittely on jo nyt ollut säädetty muun muassa henkilötietolaissa, joten täysin uudesta asiasta ei ole kyse. Nyt tietosuoja-asetuksen avulla käytännöt harmonisoidaan Euroopan alueella.

Vertaa siis tätä tietosuoja-asiaa ja siitä muodostuvaa terveyskaupan tiedonhallintasuunnitelmaa elintarvikkeilta vaadittavaan omavalvontasuunnitelmaa, niin uskoisin, että henkilötietoihin liittyvien asioiden huomioiminen yrityksessäsi on helpompaa.

Mika Rönkkö

Suomen Terveystuotekauppiaiden Liitto

Käsitteitä

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity) liittyvät tiedot. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, kotiosoitteen tai sähköpostiosoitteen perusteella.

Henkilötietojen käsittely

Toimintaa, jotka kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Henkilötietorekisteri tai rekisteri

Mikä tahansa jäsennelty henkilötietoja sisältävää tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Esimerkiksi terveyskaupan kanta-asiakasrekisteri.

Rekisterinpitäjä

Rekisterinpitäjä on yritys, kuten terveyskauppa, joka säilyttää henkilötietoja ja jolla on oikeus määrätä henkilörekisterin käytöstä.

Henkilötietojen käsittelijä

Taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällaisesta on kysymys esimerkiksi silloin, kun terveyskauppa siirtää työntekijätietoja palkanmaksusta vastaavalle tilitoimistolle. Tällöin henkilötietojen katsotaan siirtyvän henkilötietojen käsittelijälle eli esimerkiksi tilitoimistolle, joka käsittelee henkilötietoja rekisterinpitäjän, kuten terveyskaupan puolesta.

Tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Lisää käsitteitä ja sanastoa:

http://www.tietosuoja.fi/fi/index/sanasto.html

Selvitä, mitä henkilötietoja terveyskaupassa käsitellään?

Tyypillisesti näitä ovat muun muassa: Terveyskaupan kanta-asiakasrekisteri, henkilökunnan palkanlaskennan tiedot, työpaikkahakemukset, työsopimukset ja tavarantoimittajien yhteystiedot, laskutustiedot, verkkokaupan tilaajatiedot. Henkilötietoja voi tulla myös esimerkiksi sähköpostilla, jos olet saanut esimerkiksi avoimia työpaikkahakemuksia sähköpostilla.

Asiakas- ja työntekijärekisteri

Useimmilla terveyskaupoilla on jonkinlainen asiakasrekisteri tai tuotteiden tilauksiin liittyvä tilausrekisteri. Terveyskaupassa kannattaa käydä läpi, mitä tietoa näihin rekistereihin on yksittäisistä henkilöistä tallennettu. Yleensä terveyskaupan asiakasrekisterit eivät sisällä kovinkaan arkaluontoisia henkilötietoja. Omien toimintatapojen kartoitus on kuitenkin paikallaan. Esimerkiksi terveyskaupan kanta-asiakastietojärjestelmän asianmukainen käyttäjähallinta on tärkeää myös liikesalaisuuksien, eikä vain henkilötietojen turvallisuuden näkökulmasta.

Terveyskaupan työntekijärekisteri sen sijaan sisältää arkaluontoista henkilötietoa. Palkanlaskennan tarpeisiin tarvitaan tietoa henkilön sairaspoissaoloista, ay-jäsenyyksistä sekä toisinaan myös ulosotosta. Myös työntekijöiden henkilötunnusta käytetään palkanlaskennassa säännönmukaisesti.

Listaa tähän, mitä henkilötietoja yrityksessäsi käsitellään:

-Henkilökunnan työsopimukset

-Palkanlaskentaan liittyvät henkilötiedot

-Sähköpostiosoitteita

-Puhelinnumeroita

-Tukkuyrityksien yhteystiedot

-Tukkuyrityksien edustajien ja muiden toimijoiden käyntikortteja

-Kanta-asiakastiedot

-_____

-_____

-_____

-_____

Selvitä, missä tiedot sijaitsevat ja millä järjestelmällä niitä käsitellään.

Näitä ovat esimerkiksi Excel-taulukot, sähköpostit, paperiarkistot, skannatut dokumentit ja valvontakameradata. Näitä kaikkia käsitellään mahdollisesti vain tietokoneella tai valvontakameradataa myös kameran muistikortilla.

Listaa tähän, missä yrityksesi käsittelemät henkilötiedot sijaitsevat ja millä järjestelmällä niitä käsitellään:

-Työsopimukset / toimistomapissa

-Henkilökunnan palkkatiedot / toimistomapissa ja arkistossa

-Sähköpostiosoitteet / sähköpostiohjelmassa

-Puhelinnumerot / puhelimessa

-Tukkuyrityksien yhteystiedot / tilauskirjassa ja tietokoneella

-Tukkuyrityksen edustajien ja sidosryhmien käyntikortit / toimistossa

-Kanta-asiakasrekisteri / kassajärjestelmä ja toimiston tietokone

-_____

-_____

-_____

-_____

-_____

-_____

-_____

-_____

-_____

-_____

-_____

Käy läpi seuraavat kysymykset?

Alla olevien kysymysten avulla pääset liikkeelle ja ehkä paremmin hahmottamaan tietosuojaan liittyviä asioita terveyskauppasi näkökulmasta. Sinulla ei tarvitse olla heti vastausta kaikkiin alla oleviin kysymyksiin. Tärkeä on päästä alkuun ja hahmottaa henkilötietojen käsittelyn periaatteita.

- Käy läpi yrityksessä tapahtuva henkilötietojen kerääminen, rekisteröinti ja käsittely sekä niihin liittyvät perusteet ja käytännöt. Mitä tietoja yrityksessä kerätään, ja sisältyykö niihin henkilötietoja? Millä perusteella henkilötietoja kerätään tai käsitellään? Mahdollisesti listasit näitä edellisille sivuille.
- Arvioi henkilötietojen käsittelyn tarpeellisuutta ja siihen liittyviä riskejä sekä sitä, miten riskejä voitaisiin vähentää? Tarvitaanko kaikkia nyt kerättäviä tietoja? Kuinka pitkään tietoa on liiketoiminnan kannalta tarpeen säilyttää?
- Millä tavalla yrityksessä huolehditaan eri tietomassojen, erityisesti henkilötietojen suojauksesta? Onko suojauskäytännöissä parantamisen varaa?
- Pohdi, millä tavalla varautua erilaisiin tietoturvaloukkauksiin? Miten näiden riskiä voitaisiin vähentää? Miten yrityksessä toimitaan tietoturvaloukkauksen sattuessa?
- Selvitä, millä tavalla yrityksessä reagoidaan rekisteröityjen pyyntöön tarkistaa tai poistaa itseään koskevat tiedot yrityksen rekistereistä?
- Vastuuta selkeästi taho huolehtimaan siitä, että tietoturva on riittävällä tasolla ja yrityksessä noudatetaan nykyistä henkilötietolainsäädäntöä.
- Selvitä, siirretäänkö yrityksen keräämiä tai käsittelemiä henkilötietoja muille tahoille, esimerkiksi kumppaniyrityksille, toimeksiantajille, alihankkijoille jne.? Onko henkilötietojen siirtämiseen saatu rekisteröityjen suostumus, ja onko henkilötietojen siirrosta tehty kirjallista sopimusta? Siirretäänkö henkilötietoja muihin EU-maihin tai EU:n ulkopuolelle?
- Jos yrityksessä suunnitellaan uusien asiakasrekisterien tai vastaavien ohjelmistojen hankintaa, selvitä myyjältä ennen hankintapäätöksen tekoa, onko ohjelmiston suunnittelussa varauduttu tietosuoja-asetuksen säännöksiin tai onko ohjelmisto mukautettavissa niihin?

Osa näistä kysymyksistä saattaa tuntua terveyskaupan näkökulmasta hieman vierailta tai epäolennaisilta. EU:n tietosuoja-asetus kuitenkin velvoittaa, että kaikissa yrityksissä nämä asioita huomioidaan ja tiedostetaan, joten niitä on hyvä pohtia terveyskauppasi kannalta.

Terveyskauppa, jolla ei ole esimerkiksi omaa verkkokauppaa käsittelee henkilötietoja pääasiassa henkilökuntaan liittyen (mm. työsopimukset ja palkanlaskennan asiat) ja mahdollisti kanta-asiakkaisiin liittyviä henkilötietoja.

Terveyskauppa, jolla on verkkokauppa, käsittelee jo enemmän erilaisia henkilötietoja. Terveyskauppa saattaa kerätä myös verkkokaupan kautta postituslistaa, joka sisältää henkilötietoja. Verkkokaupan pitäminen ei kuitenkaan välttämättä nosta riskitasoa oleellisesti, kunhan verkkokauppaan liittyvät tietosuoja-asiat ovat kunnossa.

ALKUKARTOITUS JO LÄHES VALMIS

Jos sait nämä ensimmäiset kohdat selvitettyä ja käytyä läpi edellä mainitut kysymykset, niin onneksi olkoon! Olet päässyt hyvän alkuun terveyskaupan tietosuoja-asetukseen valmistautumisessa.

Luo tämän alkukartoituksen pohjalta kokonaiskuva siitä, miten terveyskaupassasi käsitellään henkilötietoja.

Käy uudelleen läpi alkukartoituksessa keräämäsi tiedot ja vastaa muutamaan jatkokysymykseen, niin osalta.

Ketkä käsittelevät henkilötietoja yrityksessäsi? Jossain yrityksissä yrittäjä itse käsittelee kaikkia tietoja. Mutta, jos myös muut henkilöt niitä käsittelevät niitä, niin asia on hyvä tiedostaa.

Yrityksessämme henkilötietoja käsittelevät seuraavat henkilöt:

- _____
- _____
- _____
- _____
- _____
- _____
- _____

Tee riskien arviointi pohtimalla seuraavia asioita:

Voiko ulkopuolinen päästä käsiksi terveyskaupan henkilötietoihin? Vastaus on lähes kaikissa tapauksissa kyllä. Tärkeää onkin tiedostaa tietoturvaan liittyviä asioita.

Esimerkiksi, että henkilötietoja säilytetään yrityksessä asianmukaisesti esimerkiksi mapeissa ja paikassa, joihin ei ulkopuolisilla ole pääsyä. Tietokoneella olevia henkilötietoja suojaa esimerkiksi tietoturvaohjelmat. Jos valvontakameran data on muistikorteilla, niin näitä muistikortteja tulee säilyttää huolella. Terveyskauppaan kohdistuvat tietomurrot ovat erittäin harvinaisia, mutta toki mahdollisia.

Jos terveyskauppaan murtaudutaan niin on todennäköistä, että varkaus kohdistuu muuhun kuin henkilötietoihin. On kuitenkin hyvä tiedostaa myös murtoriski tietosuojan näkökulmasta. Säilytä siis henkilötietoja (esim. muistikortteja ja muita tiedon tallennusvälineitä huolellisesti).

TERVEYSKAUPAN TIETOSUOJAOHJELMA JA OMAVALVONTASUUNNITELMA

Nyt olet päässyt jo niin pitkällä, että alkukartoituksen perusteella päästään laatimaan sinun yrityksellesi ja terveyskaupallesi tietosuojaohjelma. Tämä tapahtuu tekemäsi kartoituksen pohjalta. Kun kartoitit terveyskaupassasi käsiteltäviä henkilötietoja, niiden käsittelyä ja säilytystä, niin olet jo osin täyttänyt tietosuoja-asetuksen velvoitteita.

Terveyskaupan tietosuojaoppaan avulla keräät itsellesi tietoa terveyskaupan tietosuoja-asioiden vaatimustenmukaisuuden täyttämiseksi sekä määrittelet käytännön ohjeistukset ja koulutukset yrityksesi sisällä. Näin tiedostat ja huolehdit tietosuojaan liittyvän riskienhallinnan, raportoinnin sekä seurannan toteuttamisen.

Tietosuojavastaava / tietosuoja-asioiden yhteyshenkilö

Tietosuoja-asetuksen mukaan velvollisuus nimittää yritykseen erityinen tietosuojavastaava koskee lähtökohtaisesti sellaisia yrityksiä, joissa henkilötietojen käsittely edellyttää laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai laajamittaista asetuksessa mainittua arkaluonteisten tietojen käsittelyä. Terveyskaupassa yrittäjä yleensä toimii tietosuoja-asioiden vastuuhenkilönä. Jos yrityksessä ei ole tarvis nimetä erillistä tietosuojavastaavaa, niin yrittäjä itse hoitaa tietosuojaan liittyvät asiat.

Yritykseni tietosuojavastaava/tietosuoja-asioiden yhteyshenkilö:

Nimi: _____

Puhelin:_____

Sähköposti:_____

Henkilökunnan perehdyttäminen

Kerro henkilökunnalle, että terveyskaupassa on tietosuoja-asetuksen mukainen tietosuojaohjelma. Korosta jokaisen omaa vastuuta ja huolellisuutta henkilötietojen asianmukaisesta käytöstä.

Muistathan, että tietosuoja-asioita voidaan terveyskaupassa verrata elintarvikkeiden omavalvonta-asioiden perehdyttämiseen.

Käytännön toimia terveyskaupassa tietosuoja-asiassa:

- Arkistoi terveyskaupassa käsiteltävät arkaluotoiset tiedot erityisen hyvin. Esimerkiksi työntekijöiden lääkärintodistukset, ulosottodokumentaatio, AY-jäsenyystiedot ja vastaavat omaan mappiinsa lukkojen taakse tai sähköisessä muodossa hakemistoon, jonka käyttöoikeudet on rajattu.
- Harkitse, voiko terveyskaupassa käsiteltävät arkaluontoiset tiedot lähettää suojaamattomassa sähköpostissa. Hyvin monet sähköpostipalvelut käyttävät jo salattua yhteyttä ja tarvittaessa löytyy ilmaisia sovelluksia sähköpostin sisällön suojaamisen.

Terveyskaupan henkilökunnan palkanlaskennan tiedot:

- Jos olet ulkoistanut palkanlaskennan tilitoimistolle, niin työntekijät eivät yleensä saa kysellä palkka-asioita suoraan palkanlaskennasta. Palkanlaskennassa ei yleensä ole mahdollisuutta tunnistaa kyselijää luotettavasti.
- Työntekijällä on kuitenkin oikeus tarkastaa omat tiedot ja korjauttaa virheet. Mieti ja sovi palkanlaskennan kanssa menettely, jolla työntekijä voidaan tällaisissa tapauksissa tunnistaa ja miten tiedot annetaan.
- Hävitä aineistot, kun ne eivät enää ole tarpeen. Palkanlaskennan aineistojen lakisääteinen säilytysaika on 6 tai 10 vuotta. Jos esimerkiksi lääkärintodistusten perusteella on haettu ja saatu KELA-korvauksia, ovat lääkärintodistukset tositteita, jotka tulee säilyttää 6 vuotta. Ne tulee hävittää säilytysvelvollisuuden umpeuduttua, koska säilytyksellä ei ole enää lakisääteistä tai muuta perustetta.

Varautuminen tietoturvaloukkauksiin ja odottamattomiin tilanteisiin

Terveyskaupassa on hyvä varautua tietoturvaloukkauksiin ja odottamattomiin tilanteisiin, vaikka riskit tuntuisivakin pieniltä. Hyvää riskienhallintaan kuuluu toimintasuunnitelma erilaisia odottamattomia tilanteita varten. Näitä voivat olla esimerkiksi murrot, tulipalot, vesivahingot, laiterikot tai vaikkapa vain sähkökatkos.

Tunnista nämä odottamattomat tilanteet terveyskauppasi osalta ja pohdi, miten terveyskaupassasi on näihin varauduttu. Esimerkiksi niin, että olet huomioinut varmuuskopioinnin merkityksen tai toteutat tätä käytännössä.

Varmista, että henkilökuntasi on myös tietoinen ja osaltaan varautunut odottamattomiin tilanteisiin. Terveyskaupassa voi olla käytäntönä se, että odottamattoman tilanteen sattuessa henkilökunta toimii tilanteen mukaan ehkäistäkseen tai minimoidakseen vahingot ja olemalla välittömästi yhteydessä yrittäjään.

Vaikka tämä voi tuntua itsestään selvyydeltä, niin asia on hyvä kerrata.

Jatkuva tietosuojan ylläpitäminen

Pysy ajan tasalla tietosuojan pitämiseksi kunnossa. Tämä voi tarkoittaa esimerkiksi siitä, että hoidat ohjelmien vaatimat päivitykset ja perehdytät uutta henkilökuntaa tietosuojaohjelmasta. Myös seuraamalla Suomen Terveystuotekauppiaiden Liiton tiedotusta varmistat osaltasi, että yrityksesi toiminta myös tietosuoja-asioissa on ajan tasalla. Esimerkiksi tätä Terveyskaupan tietosuoja-opasta päivitetään tarvittaessa.

Mistä saan lisätietoa tietosuoja-asioissa?

Tässä pari hyvää linkkiä, joista saat lisätietoa:

Suomen Yrittäjien opas:
https://www.yrittajat.fi/sites/default/files/yrittajat_tietosuojaopas_2018_130418.pdf

Tietosuojavaltuutetun toimisto:

http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tämän Terveyskaupan tietosuojaoppaan avulla pystyt osaltaan osoittamaan tietosuojaviranomaiselle, että yrityksessäsi toimitaan EU-tietosuoja-asetuksen vaatimuksien mukaisesti.

MITEN HOIDAN TIETOSUOJA-ASIAT KUNTOON TERVEYSKAUPASSANI?

1. Lue läpi tämä Suomen Terveystuotekauppiaiden Liiton Terveyskaupan tietosuojaopas. Pohdi siinä olevia kysymyksiä oman terveyskauppasi näkökulmasta. Kartoita henkilötietojen keruun nykytilanne ja kirjaa ne tähän oppaaseen tai dokumentoi ne muulla tavalla.

2. Tee yrityksellesi jokaisesta keräämästänne ja ylläpitämästänne henkilörekisteristä tietosuojaseloste. Tällaisia ovat esimerkiksi henkilöstörekisteri ja kanta-asiakasrekisteri. Selosteesta tulee käydä ilmi muun muassa, kuka on henkilötietojen käsittelystä vastaava rekisterinpitäjä, mitä henkilötietoja siellä on, mitä tarkoitusta varten ne on kerätty, miten niiden luvanvaraisuus on varmistettu, kenelle tietoja mahdollisesti luovutetaan ja miten tiedot on suojattu. Seloste käsittelytoimista on organisaation sisäinen asiakirja, jonka tarkoituksena on hahmottaa yrittäjälle henkilötietojen käsittelyä. Sen tarkoituksena on myös osoittaa, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti. Valvontaviranomainen voi tarvittaessa arvioida tietojenkäsittelytoimien lainmukaisuutta selosteen pohjalta. Seloste käsittelytoimista on pyydettäessä toimitettava valvontaviranomaiselle.

   Tietosuojaselosteesta löytyy malleja mm. www.tietosuoja.fi-sivustolta.

   Suomen Terveystuotekauppiaiden Liiton jäsenyrityksille on tehty terveyskaupalle räätälöityjä mallipohjia rekisteriselosteista. Terveystuotekauppiaiden Liiton jäsenyritykset voivat pyytää nämä liiton toimistolta (terveys@terveystuotekauppa.fi tai 0500 430 818)

- Terveyskaupan tietosuoja-asiat yhdessä kuntoon! -