Elisa Haverinen

EU:n yleinen tietosuoja-asetus tilitoimistossa

Tradenomi
Liiketalous
Syksy 2019

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä: Elisa Haverinen

Työn nimi: EU:n yleinen tietosuoja-asetus tilitoimistossa

Tutkintonimike: Tradenomi, liiketalous ja hallinto

Asiasanat: tietosuoja-asetus, GDPR, tilitoimisto, tietosuoja

Tämä opinnäytetyö käsittelee EU:n yleisen tietosuoja-asetuksen vaikutuksia tilitoimistoon. EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation) on alettu soveltamaan 25.5.2018. Aiempaan verrattuna uusi asetus tuo muutoksia vahvistaen yksilön oikeuksia. Tilitoimiston velvollisuudet henkilötietojen käsittelijänä muuttuvat. Yhtenä isona muutoksena on toteen näyttäminen. Tilitoimiston tulee dokumentoida henkilötietojen käsittelytoimet.

Opinnäytetyön tavoitteena oli laatia toimeksiantajalle tarvittavat dokumentaatiot liittyen henkilötietojen käsittelyyn tilitoimistossa. Työ toteutettiin kehittämistyönä, jossa uuden lainsäädännön pohjalta laadittiin toimeksiantajatilitoimistolle toimintaohjeet sekä dokumentointipohjat. Laadittuja asiakirjoja olivat sopimus henkilötietojen käsittelystä, palkanlaskennan prosessikuvaus sekä seloste käsittelytoimista. Lisäksi laadittiin toimintaohjeita dokumenttien käyttöönottoon. Laaditut pohjat otettiin käyttöön sellaisenaan tai toimeksiantajaohjaajan kanssa yhdessä tehtyjen muutosten jälkeen.

Tilitoimistoala on muuttunut vuosi vuodelta enemmän digitaaliseksi. Perinteinen paperinen kirjanpito on jäämässä taakse, samoin palkanlaskennan tulosteita pyritään koko ajan vähentämään. Digitaalisuus ja sen tuomat muutokset ovat luoneet uusia haasteita niin taloushallinnon alalla kuin muillakin aloilla, mikä on osaltaan vaikuttanut tietosuoja-asetuksen syntyyn.

Teoria osuudessa käydään ensin lyhyesti läpi tilitoimistoa, digitaalisuutta taloushallinnossa sekä tietoturvaa tilitoimistossa. Toisessa teoria osuudessa on kerrottu EU:n yleisestä tietosuoja-asetuksesta ja sen näkymisestä tilitoimistossa. Lopuksi esitellään työn käytännön toteutus ja pohdinta osuudessa käydään läpi työn lopputulos.

Abstract

Author(s): Elisa Haverinen

Title of the Publication: GDPR in Accounting Company

Degree: Bachelor of Business Administration

Keywords: General Data Protection Regulation, GDPR, accounting company, protection regulation

This thesis was commissioned by an Accounting Company that has offices in five localities in Finland. The application of General Data Protection Regulation (GDPR) began on 25.5.2018. The commissioner needed someone to do the documentation.

Purpose of this thesis was to create documentation based on General Data Protection Regulation. The thesis was development work. By familiarizing with GDPR and participating in some training, it was possible to create the instructions and documentation.

The theory part consists of accounting company and General Data Protection Regulation. After the theory, the practical implementation is explained. The last part presents the conclusions and the appendices are an agreement to handle personal data, a payroll computation process description and a description of handling personal data.

Sisällys

1 Johdanto

EU:n yleinen tietosuoja-asetus (jäljempänä pelkkä asetus) on astunut voimaan 25.5.2018. Asetuksen myötä henkilötietojen käsittely on entistä säännellympää. Henkilötiedoista, joista muodostuu rekisteri, tulee olla asianmukaiset selosteet. Henkilötietojen käsittelijöiden tulee näyttää toteen käsittelytavat ja prosessit. Prosessit sekä ohjeet tulee päivittää vastaamaan asetuksen tasoa kaikissa yrityksissä. Tämä on iso prosessi, joka osin jatkuu edelleen.

Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojan sääntelyä. Tämä johtuu siitä, että teknologia on kehittynyt niin paljon. Tavoitteena asetuksella on, että kansalaiset voivat hallita tietojaan paremmin. Henkilötietojen keräämistä, käsittelyä sekä luovuttamista ja näihin liittyviä oikeuksia ja velvollisuuksia säätelee asetus. Asetusta täydentää tietosuojalaki, joka on säädetty 1.1.2019.

Työn tarkoituksena on perehtyä tietosuoja-asetukseen ja sen vaikutuksiin toimeksiantaja tilitoimiston prosesseissa. Tutkinnan kohteena on tietosuoja-asetuksen vaikutus tilitoimiston arkeen. Mitä tilitoimistossa tulee tehdä toisin asetuksen astuessa voimaan? Tavoitteena on tilitoimiston prosessin dokumentoinnin saaminen mahdollisimman pitkälle sekä osallistuminen muiden tarvittavien dokumentoitavien asiakirjojen, kuten ohjeiden tekoon.

Alussa on lyhyesti tilitoimistosta, sen palveluista ja digitalisaation vaikutuksesta taloushallintoon. Tämän jälkeen avataan asetuksen sisältöä ja sen vaikutuksia tilitoimistoon. Neljännessä luvussa käydään läpi käytännön toteutusta. Lopuksi on pohdinta ja tehdyt johtopäätökset.

Eniten tietosuoja-asetus vaikuttaa palkanlaskentaan, koska siinä käsitellään jatkuvasti henkilötietoja. Käytännön toteutuksessa tutkittiin tilitoimiston palkanlaskentaprosessia ja laadittiin siitä tietosuoja-asetuksen vaatima prosessikuvauskaavio. Henkilötietojen ja muiden tietosuoja-asetuksen mukaisten tietojen välittäminen asiakkaalta tilitoimistolle ja päinvastoin muuttuu, sillä ennen asetuksen voimaan tuloa paljon käytettyä sähköpostia ei enää suositella kyseisten tietojen välitykseen. Kuinka tilitoimistossa taataan henkilötietojen tietoturvallisuus? Tarkoituksena on auttaa luomaan käytänteitä valittujen välineiden käyttöön.

Tilitoimistolle on tärkeää, että dokumentointi on mahdollisimman pitkällä uuden tietoturva-asetuksen astuessa voimaan. Henkilötietolain aikana on riittänyt, että säännöksiä noudatetaan. Asetuksen mukainen osoitusvelvollisuus puolestaan edellyttää käsittelyyn liittyvien prosessien

sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia. (Oikeusministeriö 2017, 14.)

2 Tilitoimisto

Toimeksiantaja on tilitoimisto, jolla on toimistoja useammalla paikkakunnalla Suomessa. Tilitoimiston palveluihin kuuluu kaikki taloushallinnon palvelut, kuten esimerkiksi kirjanpito, osto- ja myyntireskontrien käsittely ja palkanlaskenta. Palkanlaskennan palvelut on keskitetty Kainuun toimistolle. Työtä tehdään etänä asiakkaille eri puolilla Suomea. Tässä opinnäytetyössä on paneuduttu lähinnä palkanlaskentaan siksi, että EU:n yleinen tietosuoja-asetus koskettaa tilitoimistossa eniten sitä. Taloushallinto on koko ajan enenevissä määrin digitaalista ja paperista kirjanpitoa sekä palkanlaskennan tulosteita pyritään koko ajan vähentämään. Digitaalisuus ja sen tuomat muutokset ovat luoneet uusia haasteita myös taloushallinnon alalla. Tämä on yhtenä isona tekijänä myös EU:n yleisen tietosuoja-asetuksen synnylle.

2.1 Digitaalisuus taloushallinnossa

Digitaalisuus tarkoittaa sähköisessä muodossa olevan tiedon käsittelyä, siirtämistä, varastointia sekä esittämistä. Pääsääntöisesti tieto sijaitsee tietokannoissa, joita on useita erilaisia. Tiedon rakenne määritellään kyseisellä tietokantaohjelmistolla. Tietojen siirtely ja käsittely tapahtuu erilaisilla sovelluksilla ja ohjelmistoilla, jotka myös ovat jollakin tunnetulla ohjelmistokielellä tuotettuina sähköisessä muodossa. Digitaalinen tieto kulkee tietoverkoissa ja sitä on tehokkaampi ja nopeampi käsitellä ja siirtää, varastoida ja esittää kuin perinteisessä, fyysisessä muodossa olevaa tietoa. (Lahti & Salminen 2014, 19.)

Digitaalisen taloushallinnon Lahti ja Salminen (2014, 23-24) määrittelevät taloushallinnon kaikkien tietovirtojen ja käsittelyvaiheiden automatisointina ja käsittelynä digitaalisessa muodossa. Kaikki kirjanpidon ja sen osaprosessien tapahtumat käsitellään ilman paperia ja ne myös syntyvät mahdollisimman automaattisesti. Parhaimmillaan digitaalinen taloushallinto on näin automaattista. Nykypäivänä ollaan kuitenkin vasta matkalla tähän automaattiseen kirjanpitoon. Asiakkaalla saattaa olla käytössään sähköinen kirjanpito-ohjelma, joka parhaimmillaan tekisi suurimman työn kirjanpitäjän ja yrittäjän puolesta. Monikaan ei kuitenkaan vielä näitä ominaisuuksia osaa käyttää hyödykseen, jolloin sähköinen ohjelma menee hukkaan ja vie enemmän aikaa kuin aikaisemmat kirjanpito-ohjelmat kirjanpitäjän joutuessa käsin syöttämään tositteet paperilta.

Nykypäivänä teknologisia esteitä ei enää ole ja monessa tilitoimistossa automaatioaste on jo varsin korkea nousten kiihtyvällä tahdilla. Kirjanpito voidaan parhaimmillaan jo nyt tehdä siten, ettei kirjanpitäjä itse kirjaa ainoatakaan tositetta. Kirjanpitäjä ainoastaan tarkastelee lopputulosta ja ihmettelee valmista tuotosta. Digitalisaatio tulee entistä enemmän muuttamaan perinteisiä palveluita liittyen muun muassa tiedon analysointiin ja johdon raportointiin. Kirjanpitäjän kannattaakin olla kiinnostunut alan muutoksista ja miettiä haluaako itse olla aktiivinen toimija ja kehittää omia tietoja ja taitoja, joita muutos edellyttää. Kirjanpitäjän on syytä olla kiinnostunut myös asiakkaidensa odotuksista. Mitä voit heille tarjota muuttuvassa taloushallinnon kentässä? (Aho 2019, 18-20.)

Kaarlejärvi ja Salminen (2018, 169-170) pitävät taloushallinnon kehittämisen edellytyksenä riittävää käsitystä nykytilanteesta. Kehittämistä on sitä helpompi lähteä tekemään, mitä paremmin nykytila on dokumentoitu. Dokumentoinnilla on oleellinen rooli lisäksi myös riskien hallinnassa, tiedon jakamisessa, toiminnan tehokkuudessa sekä laadun varmistamisessa. Riskien hallintaa dokumentaatio parantaa muun muassa siten, että kriittiset tehtävät pystytään hoitamaan myös äkillisessä poissaolotilanteessa dokumentoitujen ohjeiden pohjalta. Esimerkiksi automaatiorobotin ollessa esimerkiksi virhetilan vuoksi kykenemätön hoitamaan tehtäviään, pystyy ihminen hoitamaan tehtävät manuaalisesti ohjeiden avulla. Dokumenttien avulla voidaan jakaa tietoa taloushallinon prosesseista ja saadaan tämän avulla läpinäkyvyyttä tekemiseen. Perehdyttäminen onnistuu nopeammin ohjeiden ja työkuvausten avulla. Näin toiminta tehostuu uuden työntekijän aloittaessa. Dokumentoidut ohjeet ovat hyödyksi myös prosesseista vastaavalle henkilölle itselleenkin, jos kyseessä on työtehtävä, joka tulee tehtäväksi harvoin. Muistelemiseen ei mene aikaa, kun on käytettävissä ohje. Lisäksi dokumentointi varmistaa yhtenäisiä toimintatapoja ohjeen toimiessa sovitun toimintamallin vahvistajana. Näin voidaan varmistaa tasalaatuinen lopputulos.

Aho (2019, 23-25) näkee digitalisaation urakehityksen mahdollistajana. Digitalisaation poistaessa rutiinityöt mahdollistuu työnkuvan muutos. Hänen mukaansa kirjanpitäjä voi tulevaisuudessa joko kasvaa konsultiksi tai toimia prosessinhoitajana. Digitalisaation muuttaessa toimenkuvaa, tulee kirjanpitäjän työstä selkeästi asiantuntijatyötä.

Lahden ja Salmisen (2014, 17) mukaan palkkakirjanpito prosessina sisältää palkanlaskennan lisäksi niin työaika- kuin muidenkin palkkatapahtumatietojen keräämisen sekä tapahtumien tulkinnan. Itse lisäisin tähän vielä eri ilmoitusten lähettämisen viranomaistahoille, sekä kommunikoinnin niin työnantajan kuin työntekijöidenkin kanssa. Työnantajan ulkoistaessa palkanlaskennan tilitoimistolle, tulee tilitoimiston huolehtia työnantajan puolesta ilmoitukset

esimerkiksi verottajalle ja vakuutusyhtiöille. Nämä ovat olennainen osa palkkahallintoa. Lisäksi on tärkeää kommunikoida työnantajan kanssa, jotta palkat tulee hoidetuksi hänen haluamallaan tavalla, mutta kuitenkin lain ja työehtosopimusten asettamissa rajoissa. Yhtälailla tärkeää on kommunikoida työntekijöille esimerkiksi verotukseen liittyvissä asioissa tulorajan tulessa täyteen tai tarvittaessa on pyydettävä täsmennystä annetuihin tietoihin.

Palkanlaskentaprosessin tarve syntyy siitä, että yrityksessä työskenteleville työntekijöille pitää maksaa korvaus tehdystä työstä. Lainsäädäntö ja erilaiset sopimukset sääntelevät palkkausta Suomessa. Palkanlaskentaa liittyvät lisäksi erilaiset lakisääteiset vakuutus- ja sosiaaliturvamaksut, verotus sekä työ- ja loma-aikojen käsittelyt. Ennakonperintäasetus määrittelee, että yrityksen velvollisuus on pitää palkkakirjanpitoa aina, kun se maksaa palkkoja. Palkka muodostuu työsopimuslain, noudatettavien työehtosopimuksien, yrityskohtaisten käytäntöjen sekä palkansaajan kanssa solmitun työsopimuksen perusteella. Palkka pitää usein sisällään aikasidonnaisen palkan lisäksi erilaisia suorituslisiä, joita kutsutaan palkkalajeiksi. Kaikki erilaiset palkkalajit asettavat palkanlaskentaprosessille ja palkkahallintojärjestelmille erilaisia vaatimuksia. (Lahti ym. 2014, 137.)

Palkanlaskennasta toimitetaan paljon erilaisia raportteja eri sidosryhmille, kuten esimerkiksi palkansaajalle, viranomaisille sekä eri tahoille yrityksen sisällä. Raportointeja tehdään pääsääntöisesti kuukausitasolla, joitakin vuositasolla. Tämän lisäksi palkkahallintoon kuuluu erillisiä arkistointivaatimuksia. (Lahti ym. 2014,140.) Arkistointi voidaan asiakkaasta riippuen suorittaa joko tilitoimistolla tai asiakaan toimesta, sähköisesti tai paperisena.

Työsuhteen elinkaaren aikaisten tietojen ylläpitäminen on haastavaa, esimerkiksi erilaisten työsuhteen aikana tapahtuvien muutosten hallinta ja seuranta vaatii jonkin järjestelmän. Tällaisia muutoksia ovat esimerkiksi verokorttimuutokset, lomat ja muut poissaolot ja palkanmuutokset. Tavoitteena digitaalisessa palkkahallinnossa on muutostietojen tallentaminen yhteen paikkaan, mistä tieto on kaikkien sitä tarvitsevien saatavilla. Näin vältettäisiin päällekkäisiä työvaiheita saman tiedon tallentamisessa useaan kertaan sekä nopeutettaisiin tietojen ylläpitoa. (Lahti ym. 2014, 143.)

2.2 Tietosuoja tilitoimistossa

Tietosuoja tilitoimistoissa on ollut tarkkaa jo ennen EU:n yleistä tietosuoja-asetusta. Henkilötietolaissa säännellään, milloin henkilötietoja voi käsitellä. Lisäksi laissa säännellään niistä

velvoitteista, joita henkilötietojen käsittelyssä tulee noudattaa. (Lahti ym. 2014, 143-144.) Aikaisemmin on riittänyt, että annettuja säännöksiä noudatetaan (Oikeusministeriö 2017, 14).

Henkilötietolaki on säädetty 22.4.1999. Henkilötietolain 1§:n mukaan lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Henkilötietolain 2§:n 2 momentin mukaan lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Lakia sovelletaan myös muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. (L 523/1999.)

Olennaisena osana toiminnallisia ratkaisuja sekä toimintojen että tietojärjestelmien suunnittelua, liittyy yksityisyydensuoja. Henkilötietolain yhtenä pyrkimyksenä on ollut löytää ratkaisu yksityisyyden suojan ja muiden henkilötietojen käsittelyyn liittyvien intressien välillä. Henkilötietolaki määrittelee, kuinka kauan joitain tietoja saa säilyttää. Arkaluonteisena pidetyt tiedot sekä aika, kuinka kauan niitä saadaan säilyttää, määrittyvät lain perusteella. Arkaluonteisia tietoja ovat esimerkiksi sairauslomatodistukset ja muut asiakirjat, joissa on henkilön terveydentilaan liittyviä tietoja. Tällaisia asiakirjoja saa säilyttää vain sen aikaa, mitä on välttämätöntä. Vähintään viiden vuoden välein tulisi arvioida tietojen säilyttämisen tarvetta. (Lahti ym. 2014, 144.)

Palkkahallinnossa tietoihin pääsy tulisi olla vain sellaisilla henkilöillä, jotka tarvitsevat tietoa työtehtäviään varten. Palkka- ja taloushallinnon välillä tehtävien palkkatietojen siirrossa tulisi ottaa huomioon, ettei tietoja esitetä liian tarkalla tasolla. Tiedoista ei saisi esimerkiksi ilmetä tietyn henkilön ansiotasoa sellaisille henkilöille, joilla ei ole niitä syytä saada tietoonsa. (Lahti ym. 2014, 144.)

3 EU:n yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, myöhemmin GDPR) on tullut voimaan 24.5.2016. Asetuksen soveltaminen on alkanut 25.5.2018 kaikissa EU:n jäsenmaissa. Kun otetaan huomioon koko Euroopan komission antama ehdotus tietosuojapaketiksi, on kyseessä suurin lainsäädännön muutos Euroopassa yli 20 vuoteen. Komission pyrkimys kyseisellä lainsäädäntöhankkeella on eurooppalaisten henkilösuojaa koskevan lainsäädännön yhdenmukaistaminen, vahvistaminen ja ajantasaistaminen. (HE 9/2018, 26 - 27.) GDPR:n pyrkimyksenä on vahvistaa yksilöiden oikeuksia tietosuojaan sekä alentaa hallinnollista taakkaa (Rodrigues, Barnard-Wills, Hert & Papakonstantinou 2016, 253). Pyrkimykset näkyvät muun muassa täytäntöön panon valvonnan tehostamisena sekä yksilön oikeuksien lujittamisena. Lisäksi tietosuoja-asetuksen tavoitteena on sisämarkkinoiden vahvistaminen. Asetus tulee voimaan sellaisenaan kaikissa jäsenvaltioissa. (HE 9/2018, 26-27.)

GDPR tuo käyttöön tietosuojan vaikutustenarvioinnin käsitteen. Artiklan 35 mukaan tietosuojan vaikutusten arviointi toteutuu silloin, kun käsittely todennäköisesti saa aikaan korkean riskin henkilön oikeuksille ja vapauksille. GDPR tarjoaa esimerkkejä, jolloin tietosuojan vaikutusten arviointi on pakollista. (Chirica 2017, 164-165.)

Tietosuoja-asetuksen 4 artiklan 1) kohdan mukaan henkilötiedoilla tarkoitetaan kaikenlaisia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraa tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Luonnollisella henkilöllä asetuksessa tarkoitetaan lähtökohtaisesti vain elävää henkilöä. Suomessa ei tehty poikkeusta ja säädetty erikseen vainajien henkilötietojen käsittelystä, vaikka se olisikin ollut kansallisesti mahdollista. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 49-51.)

Henkilötiedon käsite on laaja, sillä esimerkiksi kiinteistötunnus tai osoite on henkilötieto, koska se voidaan yhdistää luonnolliseen henkilöön lisätietoja käyttämällä. Yhdistämisen lisäksi keinot henkilön tunnistamiseen ovat kohtuullisesti käytettävissä. Tietosuojaryhmän mukaan on parempi tulkita henkilötietojen käsitettä laajasti ja pohtia tarkkaan, kuuluuko tilanne tietosuojadirektiivin soveltamisalaan vai ei. Ryhmän mukaan henkilötietojen käsitettä tulee

tulkita sen tarkoituksen mukaisesti pyrkien löytämään henkilötietojen käsittelylle lainmukainen peruste. (Korpisaari ym. 2018, 53.)

3.1 Oikeusperusta

EU:n perusoikeuskirjan 8. artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen käsittelyn on oltava asianmukaista ja käsittelyn on tapahduttava tiettyä tarkoitusta varten. Käsittelylle on oltava asianomaisen henkilön suostumus tai muu laissa säädetty oikeutettu peruste. Kaikilla on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi. Sääntöjen noudattamista valvoo riippumaton viranomainen. (HE 9/2018, 27.)

Tietosuoja-asetuksen 5 artiklan 1 kohdan mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (lainmukaisuus, kohtuullisuus ja läpinäkyvyys). Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla (käyttötarkoitussidonnaisuus). Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (tietojen minimointi). Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. On toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyys). Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (säilytyksen rajoittaminen). Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus (eheys ja luottamuksellisuus). Asetuksen 5 artiklan 2 kohdan mukaan rekisterinpitäjä vastaa siitä ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (osoitusvelvollisuus). (Korpisaari ym. 2018, 88-89.)

Tilitoimiston kohdalla tämä tarkoittaa sitä, että kaikkien asiakkaiden, joiden kanssa käsitellään henkilötietoja, tulee tehdä kirjallinen sopimus henkilötietojen käsittelystä. Tilitoimisto on asiakkaisiinsa nähden henkilötietojen käsittelijä. Käsittelijällä tarkoitetaan sellaista luonnollista tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta. Rekisterinpitäjä puolestaan on luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee

henkilötietojen käsittelyn tarkoitukset ja keinot. (Valtiovarainministeriö 2016, 10-11.) Rekisterinpitäjä on siis yritys, joka säilyttää henkilötietoja ja jolla on oikeus määrätä henkilörekisterin käytöstä. Esimerkiksi tilitoimiston asiakas, jonka palkkahallinto tilitoimistossa hoidetaan, on rekisterinpitäjä. Henkilötietojen käsittelijä on itsenäinen elinkeinon- tai toiminnanharjoittaja (tilitoimisto), joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi tilitoimisto käsitellessään työntekijöiden henkilötietoja palkanmaksua varten. (Holopainen, 5.)

3.2 Asetuksen soveltaminen

Asetuksen soveltamisala määritellään aineelliseen ja aineettomaan soveltamisalaan. Aineellinen soveltamisala määrittelee asetuksen 2 artiklassa asetuksen soveltamisen näin:

1. Asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

2. Asetusta puolestaan ei sovelleta henkilötietojen käsittelyyn

    a. jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan,

    b. jota suorittavat jäsenvaltiot toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa,

    c. jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa tai,

    d. jota toimivaltaiset viranomaiset suorittava rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. (Korpisaari ym. 2018, 38.)

Alueellinen soveltamisala puolestaan on asetuksen 3 artiklan mukaan seuraavanlainen: asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. Asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua tai näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa. Asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla. (Korpisaari ym. 2018, 45.)

Soveltamisala yleiselle tietosuoja-asetukselle on laaja. Ratkaisevaa asetuksen soveltamisen kannalta on se, muodostuuko tiedoista rekisteri, tai onko niistä tarkoitus muodostaa rekisteri tai sen osa. (HE 9/2018, 28.) Tilitoimiston kohdalla tämä tarkoittaa sitä, että tiedostetaan, muodostuuko henkilötietorekisteri ja muodostuuko se tilitoimistolle vai sen asiakkaalle. Tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovelleta erityisiä henkilötietoryhmiä koskevien tietojen käsittelyssä. Tietosuoja lain 6§:n mukaan tällaisia erityisiä henkilötietoryhmiä ovat esimerkiksi ammattiliittoon kuuluminen sekä vakuutuslaitoksen vakuutustoiminnassa saadut tiedot vakuutetun ja korvauksen hakijan terveydentilasta. (L 1050/2018.)

3.3 S Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyn keskeisiä periaatteita ovat käyttötarkoitussidonnaisuus, tietojen minimoinnin periaate, täsmällisyys, lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate, säilytyksen rajaus sekä eheys ja luottamuksellisuus. Käyttötarkoitussidonnaisuus tarkoittaa sitä, että henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Myöhemminkään ei henkilötietoja saa käsitellä näiden käyttötarkoitusten kanssa yhteensopimattomalla tavalla. Tietojen minimoinnin periaate tarkoittaa sitä, että kerättävien henkilötietojen tulee olla asianmukaisia, olennaisia ja tarpeellisia niiden käsittelytarkoituksen kannalta. Henkilötietoja ei siis voi kerätä vain varmuuden vuoksi siltä varalta, että niiden käyttö voisi myöhemmin olla hyödyllistä. Täsmällisyyden periaate puolestaan tarkoittaa sitä, että rekisterinpitäjän on huolehdittava henkilötietojen täsmällisyydestä. Virheelliset ja/tai epätarkat tiedot tulee oikaista tai poistaa viipymättä. (HE 9/2018, 28.)

Henkilötietojen käsittelyn tulee olla lainmukaista ja rekisteröidyn kannalta läpinäkyvää. Tämä tarkoittaa sitä, että rekisteröity saa tietoja itseään koskevasta henkilötietojen käsittelystä. Lisäksi tietojen on oltava helposti saatavilla, ymmärrettäviä sekä selkeästi muotoiltuja. (HE 9/2018, 28.) Läpinäkyvyydellä tarkoitetaan sitä, että tiedot olisi esitettävä tehokkaasti ja ytimekkäästi, jotta rekisteröityjä ei kuormiteta liialla tiedolla. Lisäksi tiedot olisi esitettävä selkeästi erillään muusta kuin tietosuojaan liittyvästä tiedosta, kuten yleisistä käyttöehdoista tai sopimusmääräyksistä. (Tietosuojaryhmä 2017, 7.)

Tilitoimistossa tämä tarkoittaa sitä, että kaikista asiakkaista, joiden henkilötietoja käsitellään, tulee tehdä seloste henkilötietojen käsittelystä. Selosteesta tulee käydä ilmi rekisterinpitäjän eli asiakkaan sekä käsittelijän eli tilitoimiston yhteyshenkilöiden yhteystiedot, mahdollisten alihankkijoiden tiedot, mikä rekisteri on kyseessä, henkilötietojen käsittelyn tarkoitus, mitä henkilötietoja kyseisen asiakkaan kohdalla käsitellään eli henkilötieto, säännönmukaiset tietolähteet sekä henkilötietojen vastaanottajien ryhmät (verohallinto, ay-järjestöt, ulosottoviranomainen ym.), tekniset ja organisatoriset turvatoimet, rekisteröidyn oikeudet sekä kuvaus toiminnasta tietoturvaloukkauksen sattuessa. (HE 9/2018, 30.)

Uutena henkilötietodirektiiviin ja henkilötietolakiin nähden on henkilötietojen käsittelyä koskeva periaate osoitusvelvollisuudesta. Tämä tarkoittaa sitä, että rekisterinpitäjän on kyettävä osoittamaan henkilötietojen käsittelynsä olevan tietosuoja-asetuksen mukaista. (HE 9/2018, 28.) Tilitoimistossa osoitusvelvollisuuden voi toteuttaa tekemällä tarvittavat dokumentoinnit, joista käy ilmi henkilötietojen käsittelyn oikeellisuus. Osoitusvelvollisuuden avulla tilitoimiston tulee kyetä osoittamaan, että se on huolehtinut henkilötietojen käsittelyn osa-alueista (Valtiovarainministeriö 2016, 11). Tärkeää olisi saada dokumentoitua ohjeistus asiakkaille muun muassa siitä, miten he jatkossa voivat turvallisesti toimittaa tietoja tilitoimistolle. Asetuksen mukaan henkilötietojen käsittelijöiden ja rekisterinpitäjien on pääsääntöisesti ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista. Näin voidaan osoittaa, että ne ovat asetuksen mukaisia. (Oikeusministeriö 2017, 14.) Tietosuojaselosteen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa (Valtiovarainministeriö 2016, 12).

3.4 Henkilötietojen käsittelyn lainmukaisuus

Tietosuoja-asetuksen 6 artiklassa säädetään henkilötietojen käsittelyn oikeusperusteesta. Henkilötietojen käsittelylle tulee olla oikeudellinen perusta. 6 artikla on suoraan sovellettavaa lainsäädäntöä lukuun ottamatta artiklan alakohtia c ja e. Asetuksessa säädetään entistä tarkemmin myös suostumuksen edellytyksistä. (HE 9/2018, 29.)

Tietosuojalain 4 §:n mukaisissa käsittelyn perusteissa on vaatimus oikeasuhtaisuudesta. Tämä tarkoittaa sitä, että lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhtainen sillä tavoiteltuun oikeutettuun päämäärään nähden. (Korpisaari ym. 2018, 100.) Asetuksen 6 artiklan mukaan käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy: rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten, käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi, käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. (Korpisaari ym. 2018, 98.)

Lyhyesti sanottuna henkilötietojen käsittelyn yleisiä edellytyksiä ovat suostumus, sopimus, elintärkeä tai yleinen etu, julkinen tehtävä, oikeutettu etu sekä lakisääteinen velvoite (Holopainen, 9). Näistä tilitoimistossa toteutuvat pääsääntöisesti sopimus, suostumus sekä lakisääteinen velvoite.

3.4.1 Sopimus henkilötietojen käsittelystä

GDPR:n 5 artiklan 1 kohdan b alakohdassa säädetään tarkoitusrajoittamisperiaatteesta, jonka mukaan henkilötietoja on kerättävä määriteltyihin, nimenomaisiin ja laillisiin tarkoituksiin, eikä niitä saa enää käsitellä tavalla, joka ei sovellu näihin tarkoituksiin. (European Data Protection Board 2019, 5.) Sopimuksessa tulee asetuksen mukaan määritellä henkilötietojen käsittelyn kohde, tarkoitus, kesto sekä sopia käsiteltävät henkilötiedot. Näiden lisäksi sopimuksella tulee varmistaa, että henkilötietojen käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän

dokumentoitujen ohjeiden mukaisesti sisältäen henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit. (Valtiovarainministeriö 2016, 28-29.)

Käsittelijän tulee noudattaa salassapitovelvollisuutta sekä toteuttaa tietoturvallisuutta henkilötietojen käsittelyssä tietosuoja-asetuksen vaatimilla toimenpiteillä. Käsittelijä ei saa ulkoistaa henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta. Käsittelijän tulee auttaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa sekä käsittelyn tietoturvallisuuden toteuttamisessa. Tietoturvaloukkauksien havaitseminen ja niistä ilmoittaminen sekä vahinkojen minimoiminen ovat niin ikään käsittelijän tehtäviä. (Valtiovarainministeriö 2016, 28-29.)

Käsittelysuhteen päättyessä käsittelijän tulee joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle. Käsittelijän on lisäksi sallittava rekisterinpitäjän suorittaa auditoinnit sekä osallistua niihin itse. Rekisterinpitäjän saataville on saatettava kaikki sellaiset tiedot, jotka ovat tarpeen asetuksen velvollisuuksien noudattamisen osoittamista varten. (Valtiovarainministeriö 2016, 28-29.) Tilitoimiston kohdalla tämä ei käytännössä ole niiltä osin mahdollista, että kirjanpitolaki 10§ edellyttää kirjanpitoaineiston säilyttämisen 6 tai 10 vuotta. Taloushallintoliiton mukaan tällä voidaan perustella myös palkanlaskentamateriaalien säilyttäminen, sillä se tehostaa Audit Trailia sekä auttaa mahdollisissa työntekijää palvelevissa selvityksissä.

Leppänen ja Partanen kertovat artikkelissaan (2017) tietojenkäsittelyn yksilöinnistä. Heidän mukaansa sopimuksessa on yksilöitävä, mitä tietojen käsittelyä ollaan ulkoistamassa, esimerkiksi palkanmaksu. Lisäksi yksilöidään, keitä yksilöitä, esimerkiksi työntekijät sekä mitä tietoluokkia, esimerkiksi työntekijöiden yhteystiedot, ulkoistaminen koskee. Tämä kuvaa hyvin tilitoimistossa huomioon otettavia asioita.

3.4.2 Suostumus

Mikäli kyseessä on yksittäinen henkilö, voidaan häneltä ottaa kirjallinen suostumus henkilötietojen käsittelyyn, eikä varsinaista sopimusta tarvitse tehdä. Tämä perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohtaan, minkä mukaan henkilötietojen käsittely on lainmukaista, jos rekisteröity on antanut siihen suostumuksensa. Rekisteröidyn tulee antaa suostumus vapaaehtoisesti, tiettyä erityistä tarkoitusta varten. Suostumuksen voi antaa yhdellä kertaa useampaankin tarkoitukseen. Rekisteröidyn tulee kuitenkin tietää, mihin suostumuksensa antaa. (Korpisaari ym. 2018, 101.)

Kun kyseessä on esimerkiksi yritys, jonka palkanlaskenta hoidetaan tilitoimistossa, tulee tehdä sopimus henkilötietojen käsittelystä. Tämä perustuu henkilötietolain 8 §:n 1 momentin 2 kohtaan, minkä mukaan henkilötietoja voi käsitellä rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena. Lisäksi kaikille palkansaajille, henkilöille, joiden henkilötietoja käsitellään, tulee tehdä tiettäväksi heidän oikeutensa tutustua heistä kerättyyn tietoon sekä saada ne oikaistuiksi (Valtiovarainministeriö 2016, 14-15).

Asetuksen 5 artiklassa mainittuja yleisiä henkilötietojen käsittelyn periaatteita ei voida suostumuksella syrjäyttää. Esimerkiksi käyttötarkoitussidonnaisuutta, käsiteltävien tietojen minimointia, oikeellisuutta ja eheyttä tulee suostumuksesta huolimatta toteuttaa. Yksittäinen henkilö ei voi siis antaa sellaista yleistä suostumusta, jonka perusteella häntä koskevia tietoja voitaisiin käyttää miten tahansa tai mihin tahansa tarkoituksiin. (Korpisaari ym. 2018, 102.)

3.4.3 Lakisääteinen velvoite

Edellä mainittujen lisäksi henkilötietojen käsittelyn perusteina tilitoimistossa on lakisääteinen velvoite. Henkilötietolain 8 §:n 1 momentin 4 kohdan mukaan henkilötietoja saa käsitellä, jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetyistä tai sen nojalla määrätystä tehtävästä tai velvoitteesta. (HE 9/2018, 36.) Tällainen velvoite on muun muassa palkanmaksu työntekijälle. Tämän perusteen toteutumisesta huolimatta, on tilitoimistolla oltava asiakkaan kanssa kirjallinen sopimus henkilötietojen käsittelystä.

Useiden käsittelytoimien perustana oleva yksi laki voi olla riittävä, kaikkia yksittäisiä tiedonkäsittelytilanteita varten olevia erityislakeja ei asetuksessa edellytetä. Suomessa on asetuksen valmistelun yhteydessä suoritetussa säädöstarkastelussa käyty läpi yli 800 henkilötietojen käsittelystä säätävää lakia henkilötietojen käsittelyn perusteen osalta. Perustuslakivaliokunta totesi antamassaan lausunnossa, että joiltakin osin voidaan henkilötietojen suojaan liittyvät sääntelyn kattavuuden, täsmällisyyden ja tarkkarajaisuuden vaatimukset täyttää tietosuoja-asetuksella ja kansalliseen oikeuteen sisältyvällä yleislailla. Erityislainsäädännön säätämiseen tulee valiokunnan mukaan jatkossa suhtautua pidättyvästi myös sääntelyn selkeyden vuoksi rajaten erityislainsäädännön säätäminen vain välttämättömään tietosuoja-asetuksen antaman kansallisen liikkumavaran puitteissa. (Korpisaari ym. 2018, 103-105.)

3.5 Rekisteröidyn oikeudet

Rekisteröidyn oikeuksien lujittaminen on yksi tietosuoja-asetuksen tavoitteista. Jo aiemmin rekisteröidyn oikeuksiin on kuulunut oikeus saada tieto henkilötietojen käsittelyn tarkoituksesta, rekisterinpitäjästä ja siitä, mihin tietoja säännönmukaisesti luovutetaan. Rekisteröidyllä on lisäksi oikeus tarkastaa, mitä tietoja hänestä on tallennettu tai saada vastaavasti tietää, ettei hänestä ole tallennettu tietoja. Yleisessä tietosuoja-asetuksessa säädetään rekisteröidyn oikeuksista kuitenkin nykyistä yksityiskohtaisemmin. Niiden on kehitetty myös vastaamaan paremmin digitalisoituneen yhteiskunnan rakenteita. Uutena tietosuoja-asetuksessa säädetään esimerkiksi rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen. Lisäksi uutena säännöksenä on esimerkiksi se, että tiedot on toimitettava rekisteröidylle lähtökohtaisesti sähköisesti. (HE 9/2018, 29.)

Tietosuoja-asetuksen tavoitteena on ollut rekisteröidyn tietosuojan parantaminen. Tähän on pyritty esimerkiksi ohjaamalla rekisterinpitäjiä tietojen vastuulliseen ja mahdollisimman läpinäkyvään käsittelyyn. Rekisterinpitäjän on annettava tiedot henkilötietojen käsittelystä tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Voidakseen suorittaa informoinnin oikein, on rekisterinpitäjällä itsellään oltava selkeä tieto siitä, kenen tietoja käsitellään, mihin tarkoituksiin ja millä perusteella, luovutetaanko tai siirretäänkö henkilötietoja organisaation ulkopuolelle ja kauanko niitä säilytetään. (Korpisaari ym. 2018, 172-176)

Tilitoimistossa tämä tarkoittaa käytännössä sitä, että asiakkaalle kerrotaan, mitä tietoja henkilöistä tallennetaan ja miksi. Yksittäiselle työntekijälle kerrotaan ja perustellaan tietojen tallennuksen syyt. Esimerkiksi osoitetieto on suositeltua tulorekisterin kannalta. Verkkopalkkalaskelman lähettämistä varten se on välttämätön. Toisin sanoen, jos työnantaja tulostaa ja jakaa tai tilitoimisto postittaa työntekijöiden palkkalaskelmat työnantajalle, ei työntekijöiden osoitetietoja ole välttämätöntä tilitoimistoon antaa. Mikäli käytössä on verkkopalkka, eli palkkalaskelmat menevät palkanlaskentaohjelmistosta jokaisen henkilökohtaiseen verkkopankkiin, tilitoimisto tarvitsee työntekijöiden osoitetiedot. Verkkopalkan lähettäminen ei muutoin onnistu.

3.6 Tietosuoja-vastaava

EU:n tietosuoja-asetuksen 37 artiklan 1 momentin mukaan organisaatioon pitää nimetä tietosuoja-vastaava aina, kun tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin, rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu 9 artiklan mukaisiin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioihin tai rikkomuksiin liittyviin henkilötietoihin.

Tietosuojavastaavan tai tietosuoja-asioista vastaavan henkilön voi nimittää organisaatioon vapaaehtoisestikin. Tämä on monessa tilanteessa suositeltavaa ja tietosuojatyöryhmä onkin todennut, että tietosuojavastaavan rooli on yksi osoitusvelvollisuuden kulmakivistä. Työryhmän mielestä organisaatioiden tulisi nähdä tietosuojavastaava niin, että hän auttaa sääntelyn noudattamisen käytännön tilanteissa, kouluttaa henkilöstöä, ylläpitää suhteita viranomaiseen ja näin toimii samalla kilpailuetua kasvattavana tekijänä. (Korpisaari ym. 2018, 347.)

Kokonaisvastuu henkilötietojen käsittelystä on rekisterinpitäjällä ja käsittelijällä, ei tietosuojavastaavalla. Tietosuojavastaavalta edellytetään asiantuntemusta ja huolellisuutta omassa työssään ihan niin kuin keneltä tahansa työntekijältä, hän ei kuitenkaan ole henkilökohtaisesti vastuussa asetuksen noudattamisesta rekisterinpitäjän tai käsittelijän sijaan. Tietosuojavastaavalle on rekisterinpitäjän ja käsittelijän toimesta varmistettava tehtävien hoitaminen asetuksen edellyttämällä tavalla. On siis tärkeää varmistaa tietosuojavastaavan riippumattomuuden toteutuminen ja riittävät resurssit työn tekemiselle. (Korpisaari ym. 2018, 3447-348.)

Tilitoimistossa tämä tulee vastaan siinä kohtaa, kun palkanlaskentaa on paljon. Tällöin on kyseessä laajamittainen rekisteröityjen seuranta. Tilitoimiston pitää miettiä, onko toiminta niin laajamittaista, että tietosuojavastaava pitää nimetä. Tietosuoja-vastaavalle pitää varata työaikaa suorittaa tarvittavat työtehtävät, jotka on määritelty 39 artiklassa. Toimeksiantaja tilitoimistolla osakeyhtiön hallitus harkitsi asiaa tarkoin ja tuli lopputulokseen, että tietosuojavastaavaa ei konserniin tarvitse nimetä. Tämän sijaan henkilöstön joukosta valittiin henkilö, joka sai vastattavakseen tietosuoja-asiat. Käytännössä tämä tarkoittaa tilitoimistossa sitä, että tietosuoja-asioista vastaavan henkilön yhteystiedot tulevat yrityksen verkkosivuille ja tarvittaessa hän tekee

ilmoitukset valvontaviranomaisille. Samoin häneen voivat olla yhteydessä yrityksen työntekijät, asiakkaat sekä rekisteröidyt henkilöt, mikäli heillä on kysyttävää tietosuoja-asioista.

4 Tietosuoja-asetuksen soveltaminen tilitoimistoon

Opinnäytetyössä on kyse kehittämistehtävästä, jossa uuden lainsäädännön pohjalta laadittiin toimeksiantajalle tarvittavat toimintaohjeet sekä dokumentoinnit. Työssä perehdyttiin lainsäädäntöön, saatavilla olevaan ajantasaiseen materiaaliin sekä tilitoimistoalan valtakunnallisen toimialaliiton, Taloushallintoliiton antamiin ohjeisiin. Katsottiin Taloushallintoliiton sekä Arjen tietosuoja -koulutukset. Taloushallintoliiton pohjien ja ohjeiden avulla muokattiin dokumentit toimeksiantajatilitoimistolle sopiviksi. Lisäksi haastateltiin Kainuun toimiston toimistonvetäjää koskien tulevaa uudistusta. Häneltä saatiin toiveet ja yrityksen tarpeet dokumentteja varten. Yhdessä toimistonvetäjän kanssa käytiin laaditut dokumentit läpi ja hänen kanssaan käytiin avointa vuoropuhelua koko prosessin ajan.

Työn käytännön toteutuksessa laadittiin kaikki tietosuoja-asetukseen liittyvä dokumentointi tilitoimistossa. Toimeksiantajan edustaja hyväksyi dokumentaatiot sellaisenaan tai niihin tehtiin tarpeen vaatiessa muutoksia. Henkilötietojen välittämiseen tarvittiin sähköpostia luotettavampi väylä. Tilitoimistolla on käytössään pilvipalvelu, jota se käyttää omien tiedostojensa tallentamiseen ja jakamiseen käyttäjältä toiselle. Tätä pilvipalvelua voitaisiin käyttää myös tietojen välittämiseen asiakkaan ja tilitoimiston välillä. Tähän luodaan yhdessä IT-tukihenkilön kanssa yhteneväinen kansiorakenne ja ohjeet, kuinka käyttö onnistuu tietoturvallisesti. Yhtenä vaihtoehtona on turvasähköpostin hankinta kaikille tilitoimiston yksiköille, joiden on tarpeen käyttää tietoturvallista väylää henkilötietojen välittämiseen. Toimeksiantajaa autettiin luomaan uudet käytännöt turvalliseen henkilötietojen välittämiseen.

4.1 Laaditut dokumentoinnit

Toimeksiantajalle laadittiin taloushallintoliiton mallien pohjalta useita dokumentteja. Aluksi dokumentteja työstettiin ilman toimeksiantajaa, minkä jälkeen ne käytiin yhdessä toimeksiantajan edustajan kanssa läpi. Tarvittaessa dokumentteja muokattiin. Aluksi oli tarkoitus, että laaditaan sopimus henkilötietojen käsittelystä, palkanlaskennan prosessikuvaus sekä seloste henkilötietojen käsittelystä. Asiakirjojen dokumentoinnin päästyä hyvin vauhtiin, saatiin lisäksi laatia ohjeet niin henkilökunnalle kuin asiakkaillekin. Lisäksi pyydettiin tekemään ohjeistukset tietoturvaloukkaustilanteessa sekä tietosuojaseloste toimeksiantajan verkkosivuille.

Ensimmäisenä laadittiin Taloushallintoliiton sopimuksen pohjalta tilitoimistolle räätälöity versio sopimus henkilötietojen käsittelystä (Liite 1). Sopimuksessa on kerrottu, kuinka henkilötietojen suoja toteutuu tilitoimistossa. Tämän sopimuksen oleellisena osana on liite, jossa käydään läpi tilitoimiston tietoturvalliset tietojen välityskanavat. Nämä ovat oleellisia siksi, että asiakkaan tulee osata valita omalle yritykselleen sopiva tietojen välityskanava.

Osana sopimusta on myös asiakkaan ohjeet tilitoimistolle, jossa asiakas ohjeistaa, miten haluaa tilitoimiston juuri heidän henkilötietojensa kanssa toimivan. Tämä osa on esitäytetty tilitoimiston puolesta, mutta siihen on aina mahdollista tehdä muutoksia, mikäli asiakas niin haluaa. Taloushallintoliitto neuvoo, että tilitoimisto voi halutessaan esitäyttää myös tämän asiakkaalle kuuluvan osan, sillä monikaan asiakas ei ymmärrä tai tiedä, mitä heidän tulisi siihen laittaa. (Fredman 2018).

Varsinainen sopimus on noin kolmen sivun mittainen ja siinä on kerrottu, mitä sopimus pitää sisällään. Siinä käydään lyhyesti läpi niin asiakkaan kuin tilitoimiston vastuut ja velvollisuudet. Kokonaisuudessaan sopimus on liitteineen noin yhdeksän sivun mittainen.

Tietosuoja-asetuksen myötä tilitoimistojen tulee kuvata asiakkailleen heidän ostamansa palvelun prosessi henkilötietojen käsittelyn osalta. Myös tähän on olemassa Taloushallintoliitolla malli, jota apuna käyttäen luotiin tilitoimistolle oma prosessikuvauskaavio palkanlaskennasta (Liite 2). Palkanlaskenta on iso osa tilitoimiston osaamisaluetta sekä suurin osa henkilötietojen käsittelystä tapahtuu nimenomaan palkanlaskennan puolella.

Prosessikuvauskaaviossa on vaiheittain kuvattu palkanlaskennan eri vaiheet. Jokaisen vaiheen kohdalle on eritelty, miten materiaali toimitetaan tilitoimistolle, kuinka sitä käsitellään, miten sitä säilytetään ja kuinka pitkä on säilytysaika sekä miten tiedot hävitetään. Tämä prosessikuvauskaavio tulee täyttää jokaisen asiakkaan kohdalla erikseen sen jälkeen, kun asiakas on palauttanut hyväksytyn, allekirjoitetun sopimuksen henkilötietojen käsittelystä.

Toinen dokumentti, joka tilitoimiston täytyy tehdä asiakkaittain, on seloste henkilötietojen käsittelystä (Liite 3). Tämäkin täytetään, kun asiakkaalta on saatu allekirjoitettu sopimus henkilötietojen käsittelystä. Seloste on kahden sivun mittainen. Siinä on kerrottu niin asiakkaan kuin tilitoimistonkin yhteyshenkilöt ja yhteystiedot. Lisäksi selosteessa kerrotaan, mistä henkilötietorekisteristä tämän asiakkaan kohdalla on kysymys sekä tiedot, joita asiakkaan kanssa käsitellään. Toisella sivulla kerrotaan tilitoimiston toimintatavat mahdollisessa tietoturvaloukkaustilanteessa.

Asiakkaille laadittiin taloushallintoliiton mallin pohjalta toimintaohje tietosuoja-asetuksen hallintaan (Liite 4). Ohjeessa on kerrottu mahdollisimman lyhyesti, mistä EU:n tietosuoja-asetuksessa on kysymys, miten se vaikuttaa asiakkaaseen sekä kuinka asiakkaan tulisi toimia. Lopussa on lyhyesti avattu asetuksen keskeisimmät käsitteet.

Myös tilitoimiston työntekijöille asetuksen tuomat muutokset olivat suuria. Asiakkaiden prosessien kuvaamiseen ja muiden tarvittavien dokumenttien täyttämiseen laadittiin yksinkertainen ohje (Liite 5) helpottamaan tilitoimiston työntekijöiden työtä. Ohjeen lisäksi dokumentointipohjissa on punaisella huomiovärillä kirjoitetut ohjetekstit kohdissa, jotka työntekijöiden on täydennettävä saatuaan asiakkaalta tarvittavat asiakirjat.

Aina on mahdollista, että tapahtuu jonkin asteinen tietoturvaloukkaus. Se voi olla pienimmillään sitä, että palkanlaskija lähettää tiedot väärälle vastaanottajalle ja pahimmillaan sitä, että joku ulkopuolinen murtautuu tilitoimiston tietoverkkoon ja sitä kautta asiakastiedostoihin.

Tilitoimiston henkilökunnalle laadittiin ohjeet (Liite 6), miten tietoturvaloukkaustilanteessa tulee toimia. Ilmoittamista helpottamaan laadittiin lomakepohja, jolla tietoturvaloukkauksesta voi ilmoittaa konsernin sisällä tietosuoja-asioista vastaavalle henkilölle (Liite 7) ja toinen lomakepohja, jolla tietoturvaloukkauksesta voi tehdä ilmoituksen tietosuojavaltuutetulle (Liite 8). Molemmissa lomakepohjissa on selkeät ohjeet, mitä tietoja niihin tulee laittaa. Ohjeissa neuvotaan työntekijälle, keneen hänen tulee olla yhteydessä tietoturvaloukkauksen sattuessa, ja mikä on yhteydenottojärjestys. Lisäksi ohjeesta löytyy listaus asioista, jotka tulee ilmetä esimerkiksi tietosuojavaltuutetulle tehtävässä ilmoituksessa.

4.2 Vaikutus tilitoimistoon

Suurin vaikutus tietosuoja-asetuksella tilitoimistoon on nähdäkseni sen työvaiheiden määrää lisäävä vaikutus. Aiemmin toimistossa on kyllä ollut selvillä palkanlaskentaprosessi ja asiakkaiden kanssa on tehty toimeksiantosopimukset. Nyt palkanlaskijan pitää jokaisen asiakkaan kohdalla täyttää erikseen palkanlaskennan prosessikuvaus sekä seloste käsittelytoimista. Nämä hän tekee saatuaan asiakkaalta allekirjoitettuina niin toimeksiantosopimuksen kuin siihen liittyvän sopimuksen henkilötietojen käsittelystä. Tämä on rutinoiduttuaan lyhyt ja helppo tehtävä. Näin alkuun, ennen kuin kaikkien jo olemassa olevien asiakkaiden kanssa sopimukset ja dokumentit ovat kunnossa, menee niiden työstämiseen huomattavasti enemmän aikaa.

Dokumentointien lisäksi asetus vaikuttaa olennaisesti tietojen välittämiseen ja siirtoon asiakkaiden sekä toimistojen välillä. Ennen voitiin palkanlaskentaan liittyvät tiedot ja valmiit palkkalaskelmat välittää niin asiakkaalle kuin hänen työntekijöilleen sähköpostin välityksellä. Nyt sitä ei suositella palkkalaskelmalla olevien arkaluonteisten henkilötietojen vuoksi. Suurimmasta osasta palkkaohjelmistoja onnistuu palkkalaskelmien lähettäminen suoraan työntekijöiden verkkopankkeihin, mikä on tietoturvallista. Toisena vaihtoehtona on turvasähköposti ja pilvipalveluihin tallennetut jaetut kansiot. Tämä on muuttanut jonkin verran toimistojen työskentelyä myös siinä, että enää eivät toimistot voi keskenään tietoja välittää sähköpostin välityksellä. Toimeksiantajalla on käytössään pilvitallennus, minkä avulla samat tiedot ovat kaikkien saatavilla toimistosta riippumatta. Tätä ei vain ole aiemmin osattu aktiivisesti käyttää, sillä jokaisella toimistolla on oma pilvikansio, jonne muut pääsevät vain synkronoimalla sen itselleen. Teknisiä haasteita on ollut, mutta ne on saatu ratkottua.

5 Pohdinta

Aihe opinnäytteeseen tuli toimeksiantajaltani. Yrityksellä oli akuutti tarve saattaa tietosuoja-asiat ja asiakirjat ajan tasalle tietosuoja-asetuksen astuessa voimaan muutaman kuukauden sisällä. Aloitin opinnäytteeni keräämällä tietoa, osallistumalla verkkokoulutuksiin sekä tekemällä toimeksiantajalleni kaikki tarvittavat dokumentoinnit. Samalla ohjeistin toimeksiantajan Kainuun toimiston työntekijöille, kuinka kaikkien asiakirjapohjien kanssa tulee toimia. Koin olevani isossa roolissa toimeksiantajan tietosuojatyössä ja välillä se tuntui jopa pelottavalta.

Tärkeimpänä tavoitteena opinnäytteelleni pidän henkilötietojen tietoturvallisuuden takaamisen toimeksiantaja tilitoimistossa. Tähän tavoitteeseen mielestäni on päästy. Tilitoimiston prosesseja sekä henkilötietojen välittämisen väyliä tarkasteltiin kriittisesti. Prosesseista luotiin dokumentaatiot, samoin muut tarvittavat asiakirjat laadittiin. Henkilötietojen välittämiseen asiakkaan ja tilitoimiston välillä löydettiin tietoturvalliset väylät ja ne otettiin käyttöön. Tilitoimiston tietosuojakäytänteet ovat tarkentuneet asetuksen mukaisiksi.

Laaditut asiakirjat ovat käytössä toimeksiantajan kaikissa toimistoissa. Ohjeet ovat olleet toimivia ja onneksi tietoturvaloukkaustilanteita ei ole ollut, joten niihin liittyviä dokumentteja ei ole tarvinnut käyttää. Taloushallintoliitto suosittelee, että tietoturvaan liittyvät asiakirjat ja sopimukset käytäisiin läpi vuosittain. Toimeksiantajalla on todettu, että läpikäynnin ajankohdaksi sopii syksy tai tilanne, jossa asiakkaan toimeksiantosipimusta päivitetään. Tarkoitus onkin vielä tämän vuoden puolella, ennen tilinpäätöskauden alkua läpikäydä sopimukset ja niiden pohjalta laaditut dokumentoinnit, mikäli sitä ei ole vielä tänä vuonna tehty.

Palkanlaskennan prosessikuvauskaaviosta on muokattavissa prosessikuvaus käytettäväksi myös kirjanpitoasiakkaille. Esimerkiksi osakeyhtiössä tulee lain mukaan ylläpitää osakasluetteloa. Tällöin puhutaan myös henkilötietojen keräämisestä rekisteriin ja tarvitaan vastaavat dokumentoinnit käsittelytoimista, mitä palkanlaskennan puolella. Seloste käsittelytoimista toimii niin ikään myös osakasluettelon dokumenttina. Se pitää vain laajemmalti täydentää uudelleen. Tekemäni dokumentoinnit ovat hyvinkin käytettävissä laajemmin ja tarkoitus onkin asiakaskohtaisesti nämä läpikäydä mahdollisimman pian.

Koen olleeni etuoikeutettu saadessani tämän toimeksiannon. Tietosuoja on asia, jota ei mielestäni milloinkaan tällä alalla voi tuntea liian hyvin. Mikäli toimii asetuksen vastaisesti, on vaarana saada muhkea uhkasakko.

Koulutukset, joihin sain osallistua, olivat osa taloushallintoliiton jäsenille tarkoitettuja koulutuksia, osa kaikille avoimia. Tällaisiin koulutuksiin on harvoilla mahdollisuus työajalla kaikkiin tai edes murto-osaan osallistua. Suurin osa koulutuksista oli tehty siten, että niitä ymmärsi maallikkokin. Koulutusten lisäksi tutkin erilaisia verkkosivuja Euroopan Unionin sivuista Suomen lain sivuihin unohtamatta useita artikkeleita, joita aiheesta on kirjoitettu.

Lähteitä työssäni voisi varmasti olla enemmänkin. Tuntuu itsestä kuitenkin hölmöltä kirjoittaa yksi lause toisesta lähteestä ja toinen lause toisesta lähteestä. Tieto aiheesta on kuitenkin pitkälti sama lähteestä riippumatta. Jokainen on vain kirjoittanut saman asian hieman eri sanoin. Pyrin kuitenkin käyttämään lähteitä mahdollisimman paljon ja löytämään mukaan sellaisia, joissa on pureuduttu asetukseen nimenomaan tilitoimiston kannalta.

Työni on toimeksiantaja kannalta hyvin hyödynnettävissä, sillä loin yritykselle pohjan kaikelle dokumentaatiolle. Lisäksi osallistuin henkilökunnan kouluttamiseen ja neuvomiseen tietoturvaan liittyvissä asioissa. Olen luetuttanut tämän kirjallisen työni merkonomiksi aikuisiällä opiskelevalla harjoittelijallamme ja sain hyviä kommentteja sekä rohkaisua siitä, että tekstini on hyvää asiatekstiä ja työ auttaa ymmärtämään tietoturva-asiakokonaisuutta. Tästä sain voimia saattaa työni loppuun.

Olen kokenut opinnäytteen tekemisen palkitsevana. Tietämykseni tietoturvaan on kasvanut kuvainnollisesti nollasta sataan. Voin sanoa olleeni aluksi tietämätön tietoturva-asioista, jotka liittyivät tilitoimistotyöskentelyyn. Opinnäytetyön tekeminen on tehnyt minusta lähes tietosuoja-asiantuntijan.

LÄHTEET

Aho, A. (2019). *Kirjanpitäjästä konsultiksi – pääkirja.* Helsinki: Alma Talent.

Chirica, S. (2017). The main novelties and implications of the new general data protection regulation. *Perspectives of Business Law Journal, 6*(1), pp. 159-176. Saatavilla 2.3.2019.

European Data Protection Board. (2019). *Guidelines2/2019onthe processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.* Adopted-version for public consultation. Saatavilla 13.10.2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

Fredman, J. (2018). TAL2018 Sopimusuudistus. *Tietosuoja-asetus ja tilitoimistojen muuttuneet toimintamallit sopimisessa.* Taloushallintoliitto.

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Saatavilla http://finlex.fi/fi/esitykset/he/ Suomen Laki.

Holopainen, P. (2018). *Yrittäjän tietosuojaopas.* Suomen yrittäjät. Saatavilla 25.8.2019. https://www.yrittajat.fi/yrittajan-abc/yritystoiminnan-abc/yrittajan-tietosuojaopas-570864

Kaarlejärvi, S. & Salminen, T. (2018). *Älykäs taloushallinto – Automaation aika.* Alma Talent Oy.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2018). *Uusi tietosuojalainsäädäntö.* Helsinki: Alma Talent.

L 523/1999. Henkilötietolaki. https://www.finlex.fi/fi/laki/alkup/1999/19990523?search%5Btype%5D=pika&search%5Bpika%5D=henkil%C3%B6tietolaki#highlight0

L 1050/2018. Tietosuojalaki. http://finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuojalaki

Lahti, S. & Salminen, T. (2014). *Digitaalinen taloushallinto.* Helsinki: Talentum Media.

Leppänen, L. & Partanen, M-P. (2017). *Muista tietosuoja-asetus, kun ulkoistat palveluita.* Yrittäjäinfo, 4/2017.

Rodrigues, R., Barnard-Wills, D., De Hert, P., & Papakonstantinou, V. (2016). The future of privacy certification in europe: An exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology, 30*(3), 248-270. doi:10.1080/13600869.2016.1189737

Taloushallintoliitto. (2018). *Asiakastiedotemalli: Toimintaohje EU:n tietosuoja-asetuksen hallintaan.* Saatavilla https://taloushallintoliitto.fi/jasenet/ohjeet-ja-tyokalut

Taloushallintoliitto. (2018). *Henkilötietojen käsittelyn turvallisuuden varmistaminen – sähköinen prosessi.* Saatavilla https://taloushallintoliitto.fi/jasenet/ohjeet-ja-tyokalut

Taloushallintoliitto. (2018). *Seloste henkilötietojen käsittelytoimista -pohja.* Saatavilla https://taloushallintoliitto.fi/jasenet/ohjeet-ja-tyokalut

Taloushallintoliitto. (2018). *Sopimus henkilötietojen käsittelystä TAL2018.* Saatavilla https://taloushallintoliitto.fi/jasenet/ohjeet-ja-tyokalut

Tietosuojaryhmä. (2017.) *Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat.* Saatavilla 12.10.2019. https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet

Tietosuojavaltuutetun toimisto. (n.d.) *Tietoturvaloukkaukset.* Saatavilla 25.11.2019 https://tietosuoja.fi/tietoturvaloukkaukset

Valtiovarainministeriö. (2016). VAHTI-raportti – 1/2016. *EU-tietosuojan kokonaisuudistus.* Saatavilla 3.2.2018. https://vm.fi/vahti-materiaalit-ja-tilaisuudet

Muokattu Taloushallintoliiton mallista

Sopimus henkilötietojen käsittelystä TAL2018

SOPIMUS HENKILÖTIETOJEN KÄSITTELYSTÄ

ALUKSI

Asiakas ja tilitoimisto ovat tehneet toimeksiantosopimuksen, jolla asiakas hankkii siinä kuvatut palvelut tilitoimistolta. Palvelujen yhteydessä tilitoimisto käsittelee henkilötietoja, joiden käsittelyn ehdoista sovitaan tässä sopimuksessa. Käsittelytoimet kuvataan yksityiskohtaisemmin liitteessä 1-A, jota voidaan tarvittaessa yhteistyössä päivittää sopimuksen voimassaoloaikana.

Henkilötieto tarkoittaa kaikenlaisia luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Henkilötietojen käsittely tarkoittaa henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä

Henkilötietoja käsiteltäessä asiakas on rekisterinpitäjä, joka määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot. Tilitoimisto on käsittelijä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Alla tarkemmin sekä asiakkaan että tilitoimiston oikeuksista ja velvollisuuksista.

ASIAKKAAN OIKEUDET JA VELVOLLISUUDET REKISTERINPITÄJÄNÄ:

- vastaa tietojen keräämisestä
- käsittelee henkilötietoja laillisesti, huolellisesti ja hyvää tietojenkäsittelytapaa noudattaen
- määrittelee tietojen käsittelyn tarkoitukset ja keinot, **antaa tilitoimistolle kirjalliset ohjeet henkilötietojen käsittelystä**
- vastaa siitä, että rekisteröidylle toimitetaan kaikki lainsäädännön edellyttämä henkilötietojen käsittelyä koskevat ilmoitukset ja tiedot
- vastaa rekisteröityjen oikeuksien toteutumisesta
- vakuuttaa, että on oikeutettu sitoutumaan tähän sopimukseen ja antamaan tilitoimistolle oikeus käsitellä henkilötietoja edustaessaan konserniyhtiötään tai kolmansia osapuolia
- varmistaa, että henkilötietojen siirtäminen tilitoimistolle sekä henkilötietojen käsittely on lainmukaista
- vahvistaa ja vastaa siitä, että henkilötietojen käsittely on lain sekä tietoturvavaatimusten mukaista
- vahvistaa, että on antanut tilitoimistolle kaikki tarvittavat tiedot, jotta tilitoimisto voi täyttää sille asetetut velvoitteet
- asiakas tai sen valtuuttama ulkopuolinen tarkastaja voi auditoida tilitoimiston tai tämän alihankkijoiden sopimuksen alaista toimintaa
- vastaa siitä, että korjaukset, poistot ja muutokset henkilötietoihin toimitetaan viivytyksettä tilitoimistolle
- pidättää itsellään kaikki omistusoikeudet, immateriaalioikeudet ja muut oikeudet henkilötietoihin.

Muokattu Taloushallintoliiton mallista

Sopimus henkilötietojen käsittelystä TAL2018

TILITOIMISTON OIKEUDET JA VELVOLLISUUDET KÄSITTELIJÄNÄ

- käsittelee henkilötietoja ainoastaan toimeksiantosopimuksessa ja tässä sopimuksessa määriteltyihin tarkoituksiin, ellei pakottavasta lainsäädännöstä muuta johdu
- käsittelee henkilötietoja suojaten rekisteröityjen yksityiselämää

- varmistaa alaisuudessaan toimivan henkilön, jolla on pääsy henkilötietoihin
- varmistaa, että henkilötietoja käsittelevät henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä sitoo asianmukainen lakisääteinen salassapitovelvollisuus

- toteuttaa kaikki lainsäädännön henkilötietojen käsittelijöiltä edellyttämät turvallisuustoimenpiteet
- avustaa mahdollisuuksien mukaan asiakasta täyttämään asiakkaan velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröityjen oikeuksien käyttämistä
- avustaa käsittelyn luonteen ja tilitoimiston saatavilla olevat tiedot huomioon ottaen asiakasta varmistamaan, että asiakkaalle laissa asetettuja velvollisuuksia noudatetaan
- huomioi asiakkaan toimittamat tietojen korjaukset, poistot ja muutokset ilman aiheetonta viivytystä henkilötietojen käsittelyssä
- tämän sopimuksen aikana tai sen päätyttyä tuhoaa tai palauttaa asiakkaalle tämän valinnan ja ohjeiden mukaisesti kaikki henkilötiedot ja poistaa olemassa olevat jäljennökset, ellei pakottavasta lainsäädännöstä muuta johdu
- ylläpitää tarvittavia selosteita/kirjanpitoa käsittelytoimista ja saattaa asiakkaan saataville kaikki sellaiset tiedot, jotka osoittavat, että tilitoimisto noudattaa sille säädettyjä velvollisuuksia
- sallii asiakkaan tai asiakkaan valtuuttaman auditoijan suorittamat auditoinnit ja osallistuu niihin
- ilmoittaa asiakkaalle, jos tilitoimisto katsoo, että asiakkaan antama ohjeistus rikkoo sovellettavaa lainsäädäntöä
- ilmoittaa asiakkaalle, jos tilitoimisto katsoo, että asiakkaan toimintatavoissa on puutteita, ja avustaa tarvittaessa asiakasta toimintatapojen korjaamisessa.

Tilitoimistolla on oikeus laskuttaa yllä kuvatuista avustamis-, korjaamis- ja pyyntöihin vastaamisista, auditoinnin tuesta sekä asiakkaan ohjeistuksen muutoksista johtuvista toimista ja kustannuksista erikseen.

TIETOTURVA

Tilitoimisto toteuttaa ja ylläpitää asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan henkilötietojen käsittelyn riittävä turvallisuustaso.

Tilitoimiston tämän sopimuksen johdosta toteuttamat käsittelyn tietoturvaperiaatteet on kuvattu tarkemmin tämän sopimuksen liitteessä 1-B.

Asiakas on velvollinen varmistamaan, että tilitoimistoa informoidaan kaikista niistä asiakkaan toimittamiin henkilötietoihin liittyvistä seikoista, jotka vaikuttavat tämän sopimuksen mukaisiin teknisiin ja organisatorisiin toimenpiteisiin.

Tietoturvajärjestelyjä arvioidaan, tarkistetaan ja päivitetään säännöllisesti.

ALIHANKKIJAT

Tilitoimisto saa käyttää alihankkijoita henkilötietojen käsittelyssä tämän sopimuksen perusteella. Asiakkaan halutessa tilitoimisto ilmoittaa alihankkijoista sopimusten alkaessa. Tilitoimisto tiedottaa asiakkaalle ennalta suunnitelluista muutoksista, joilla alihankkijoita lisätään tai vaihdetaan.

Tilitoimisto solmii alihankkijan kanssa kirjallisen käsittelysopimuksen ja edellyttää kaikkien alihankkijoiden noudattavan tilitoimistolle tässä sopimuksessa asetettuja tietosuojavelvoitteita tai vastaava tietosuojan tason takaavia velvoitteita. Alihankkija

käsittelee henkilötietoja vain kirjallisen sopimuksen mukaisesti.

Tilitoimisto vastaa käyttämiensä alihankkijoiden toimista kuin omistaan.

HENKILÖTIETOJEN SIIRTO

Tilitoimisto voi siirtää henkilötietoja Euroopan unionin, Euroopan talousalueen tai muiden maiden, joiden Euroopan komissio on todennut takaavan riittävän tietosuojan tason, ulkopuolelle vain asiakkaan etukäteisellä kirjallisella suostumuksella.

HENKILÖTIETOJEN TIETOTURVALOUKKAUKSISTA ILMOITTAMINEN

Tilitoimiston on ilmoitettava henkilötietojen tietoturvaloukkauksesta asiakkaalle ilman aiheetonta viivytystä siitä, kun tilitoimisto tai sen käyttämä alihankkija on saanut loukkauksen tietoonsa.

Tilitoimiston on ilman aiheetonta viivytystä toimitettava asiakkaalle tieto henkilötietojen tietoturvaloukkaukseen johtaneista olosuhteista sekä muista siihen liittyvistä tilitoimiston saatavilla olevista seikoista asiakkaan kohtuullisten pyyntöjen mukaisesti.

AUDITOINTI

Asiakkaalla on oikeus auditoida käsittelijän tämän sopimuksen alainen tietojenkäsittelytoiminta.

Asiakas vastaa kaikista auditoinnista aiheutuvista kustannuksista. Lisäksi tilitoimistolla on oikeus laskuttaa avustamisesta auditoinnissa ja muusta auditoinnista johtuvasta lisätyöstä.

SALASSAPITO

Tilitoimisto sitoutuu

- pitämään luottamuksellisena kaikki asiakkaalta vastaanottamansa henkilötiedot,
- varmistamaan, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta sekä
- varmistamaan, että henkilötietoja ei siirretä/luovuteta kolmansille osapuolille ilman asiakkaan etukäteistä kirjallista suostumusta, ellei käsittelijä ole velvollinen ilmaisemaan tietoja pakottavan lainsäädännön tai viranomaisen määräyksen perusteella.

VASTUUNRAJOITUS

Toimeksiantosopimuksen mukaisia vastuunrajoituksia sovelletaan myös tähän sopimukseen.

VOIMASSAOLO

Tämän sopimuksen voimassaolo on sidottu toimeksiantosopimuksen voimassaoloon ja päättyy automaattisesti toimeksiantosopimuksen päättyessä mistä tahansa syystä.

Liitteenä on lisäksi luonnosteltu ohjeistus asiakkaalta tilitoimistolle. Siinä on nähtävillä muun muassa toimistomme turvalliset henkilötietojen välityskanavat. Tarkoitus on, että muokkaatte ohjeistuksesta oman näköisenne, teidän yrityksellenne sopivan. Lomake on tehty täytettäväksi Word-tiedostona. Sopimuksen liitteenä on tarkemmat kuvauksen yllä mainituista asioista.

Tästä sopimuksesta on tehty kaksi (2) samanlaista kappaletta, yksi kullekin allekirjoittajalle.

ALLEKIRJOITUKSET

Päiväys: 21.05.2018	Päiväys: _____
Tilitoimiston nimi: Tilitoimisto Oy	Asiakkaan nimi:
Allekirjoitus:	
_____	Allekirjoitus: _____
Nimenselvennys: Toimitusjohtaja	Nimenselvennys:

SELOSTE KÄSITTELYTOIMISTA LIITE 1-A

Tilitoimiston seloste henkilötietojen käsittelytoimista

Henkilötietojen käsittely

Asiakas on antanut yleisen suostumuksen tilitoimiston koko varmistetun henkilökunnan käsitellä palkanlaskennan materiaaleja tarvittaessa. Tilitoimisto toimittaa pyydettäessä luettelon tietoja käsittelevistä työntekijöistä.

Alihankkijat

Asiakas on antanut yleisen suostumuksen alihankkijoiden käyttöön. Tilitoimisto toimittaa pyydettäessä luettelon alihankkijoista

Rekisteröityjen ryhmät sekä henkilötietojen käsittelyn tarkoitus ja luonne

Tilitoimisto käsittelee seuraavien rekisteröityjen tietoja seuraaviin tarkoituksiin:

☐ Asiakkaan palkan- ja palkkionsaajat – palkka- ja henkilöstöhallinnon toteuttamiseksi
☐ Asiakkaan henkilöasiakkaat - saatavien seuraamista varten
☐ Yhdistyksen jäsenet – yhdistyksen jäsenhallintaa ja laskutusta varten
☐ Asunto-osakeyhtiön osakkaat - asunto-osakeyhtiön hallintoa varten
☐ Osakasrekisteri - osakeyhtiölain edellyttämällä tavalla
☐

Käsittelyn kohde ja ryhmät sekä henkilötietojen tyyppi

Tilitoimisto käsittelee seuraavia henkilötietoryhmiä:

☐ Nimi ja yhteystiedot
☐ Henkilötunnus
☐ Henkilön perustiedot, kuten syntymäaika, sukupuoli ja koulutustiedot
☐ Palkanlaskennassa tarvittavat tiedot, kuten ennakonpidätystiedot, sairauspoissaoloja koskevat tiedot
☐ Palkanlaskennassa tarvittavat tietosuoja-asetuksen tarkoittamat erityiset henkilötietoryhmät, kuten sairauspoissaolot/terveystiedot ja ammattiyhdistysjäsenyystiedot
☐ Palkanlaskennan perusteella syntyneet palkka-, eläke- ja verotustiedot sekä muut vastaavat tiedot
☐ Laskutusta ja perintää varten tarvittavat laskutus- ja perintätiedot
☐ Osakeyhtiön tai asunto-osakeyhtiön hallinnointia varten tarvittavat osakas- ja osakkuustiedot
☐

Tilitoimisto käsittelee lisäksi seuraavia erityisiä henkilötietoryhmiä:

☐

Henkilötietojen käsittelyn kesto

Elleivät osapuolet ole toisin sopineet, henkilötietoja käsitellään niin pitkään kuin palveluita toimitetaan toimeksiantosopimuksen mukaisesti tai lainsäädäntö tietojen säilyttämistä edellyttää.

Henkilötietojen maantieteellinen sijainti

Henkilötietoja käsitellään seuraavissa maissa / seuraavilla alueilla:

☒ Suomi ja muut ETA-maat
☐

HENKILÖTIETOJEN TIETOTURVA TILITOIMISTOSSA LIITE 1-B 1/3)

Tietoturvaa ja henkilötietojen lainmukaista käsittelyä varmentavat toimet.
Tilitoimisto Oy
Laatija / päivittäjä Päiväys / muutospäiväys
21.5.2018

Hallinto

☒ Tietoturva sekä henkilötietojen lainmukainen käsittely ovat keskeinen osa tilitoimiston toimintaperiaatteita.
☒ Tietoturvaan ja henkilötietojen käsittelyyn liittyvät roolit ja vastuut on nimetty henkilötasolla.
☒ Tietoturvapolitiikka ja siihen liittyvät käytännöt on määritelty.
☐ Tietoturvapolitiikka ja tietoturvakäytännöt on auditoitu ulkopuolisen asiantuntijan toimesta ja ne katselmoidaan säännöllisesti.
☒ Tietoturvapolitiikka ja tietoturvakäytännöt katselmoidaan säännöllisesti.

Henkilöstö

☒ Henkilöstön roolit, työtehtävät ja vastuut on määritelty selkeästi.
☒ Työntekijöiden kanssa on laadittu sopimus liike- ja ammattisalaisuuden salassapidosta.
☐ Työsuhteiden päättymisen varalle on luotu toimintamalli, jossa on huomioitu käyttöoikeuksien poistaminen ja työntekijän hallussa mahdollisesti olevien aineistojen palauttaminen.
☒ Henkilöstö on perehdytetty tietoturvapolitiikkaan ja -käytäntöihin ja perehdytys kuuluu osana uusien työntekijöiden koulutusohjelmaa.
☐ Olennaisten tietoturvaan liittyvien vaaratilanteiden raportointiin ja käsittelyyn on toimintamalli.
☐

Toimintamallit

☒ Suojattavan tiedon käsittely erilaisissa viestintäjärjestelmissä, kuten sähköpostissa tai pikaviestimissä on määritelty ja internetin ja sosiaalisen median käytölle tilitoimiston tietoverkossa luotu hyväksyttävän käytön pelisäännöt.
☒ Ulkopuolisten pilvitallennuspalveluiden käyttö tapahtuu ainoastaan yrityksen johdon määrittämissä tilanteissa ja johdon määrittämillä palveluntarjoajilla.
☐ Etätyöskentelylle on luotu tietoturvaan liittyvät ohjeet.
☐

Toimitilaturvallisuus

☐ Tilitoimiston tiloissa on turvalukitus.
☐ Tilitoimiston tiloissa on sähköinen kulunvalvonta.
☒ Tilitoimistolla on ajantasainen rekisteri toimitilojen ja muiden suojattavien kohteiden avaimista sekä kulkutunnisteista.
☒ Asiakkaiden ja kolmansien osapuolien pääsy työpisteisiin sekä suojattaviin kohteisiin ja tietoihin on estetty.
☐

Asiakkaan tunnistaminen ja aineistojen luovutukset

☐ Asiakkaiden edustajat tunnistetaan ennen asiakassuhteen alkamista ja tunnistetiedot tallennetaan rahanpesulain edellyttämällä tavalla.
☒ Asiakkaan aineistojen luovutustilanteessa noudatetaan hyvän tilitoimistotavan edellyttämiä sekä asiakkaan kanssa sovittuja tunnistus- ja luovutuskuittauskäytäntöjä.
☒ Jos tilitoimisto hallinnoi sopimuksen mukaan asiakkaan puolesta asiakkaan käyttäjien pääsyä tietojärjestelmiin, käyttäjähallinnointi tapahtuu asiakkaan nimettyjen henkilöiden kanssa, sovittuja tunnistamistapoja hyödyntäen sekä huolehtien tunnusten ja salasanojen tietoturvallisista toimitustavoista.
☐

Käyttövaltuushallinta ja salasanapolitiikka **LIITE1-B (2/3)**

☒ Tietojärjestelmissä käytetään vain yksilöityjä, nimetyille henkilöille osoitettuja käyttäjätunnus/salasanapareja. Poikkeuksena ovat tilanteet, joissa tilitoimiston johto on arvioinut riskin epäolennaiseksi.

☒ Henkilöstön käyttäjätunnuksista ja käyttöoikeuksista tilitoimiston ulkopuolisiin tietojärjestelmiin pidetään kirjaa.

☒ Työntekijöiden käyttöoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa.

☒ Salasanat, PIN-koodit ja käyttäjähallintaan tarkoitetut koodit säilytetään tarkoitukseen soveltuvassa turvallisessa tietojärjestelmässä/tiedostossa.

☒ Kaikissa luottamuksellista tietoa sisältävissä tietojärjestelmissä on käytössä salasanaan tai vastaavaan menettelyyn perustuva pääsynhallinta.

☒ Tietojärjestelmien pääkäyttäjätunnusten oletussalasanat on vaihdettu ja tietojärjestelmien salasanat vaihdetaan säännöllisesti.

☐

Ulkopuoliset toimijat

Ulkopuolisia toimijoita ovat esimerkiksi siivousliikkeet, vartiointiliikkeet, kiinteistönhoitoyritykset, isännöintiliikkeet ja muut yhteistyökumppanit, joilla on pääsy organisaation toimitiloihin tai suojattaviin tietoihin.

☒ Tilitoimiston yhteistyökumppaneiden kanssa on laadittu kirjallinen sopimus luottamuksellisen tiedon salassapidosta.

☒ Toimitiloissa säännöllisesti työskentelevät ulkopuolisten toimijoiden työntekijät perehdytetään tarvittavissa määrin tilitoimiston tietoturvakäytäntöihin.

☐

Ulkoistetut ICT-palvelut

Ulkoistetuilla ICT-palveluilla tarkoitetaan tässä kohdassa tilitoimiston ulkopuolisia yrityksiä, jotka tuottavat tilitoimistolle esimerkiksi palvelimien ja työasemien ylläpitopalvelua, tallennus- sekä varmistuspalvelua, tietoturvan ylläpitopalvelua tai tietoliikenneyhteyksien ylläpitopalvelua.

☐ Ulkopuolisista ICT-palveluista on laadittu kirjalliset palvelusopimukset sekä kirjallinen sopimus luottamuksellisen tiedon salassapidosta.

☐ Tilitoimiston ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti ja palveluntarjoaja on tietoinen tilitoimiston tietoturvakäytännöistä ja suojattavista kohteista.

☒ Tilitoimiston ja ulkoistettujen ICT-palveluiden toiminnan ylläpidosta ja kehittämisestä keskustellaan määräajoin palveluntarjoajan kanssa.

☐

Suojattavien kohteiden ja tiedon hallinta

Suojattavia kohteita ovat esimerkiksi työasemat, kannettavat tietokoneet, palvelimet ja mobiililaitteet.

☒ Suojattaville kohteille on määritelty hyväksyttävän käytön pelisäännöt.

☒ Asiakkaan kirjanpitoaineistolle, henkilötiedoille ja muille tiedoille on laadittu käsittelyohjeet.

☒ Sekä digitaalisen tiedon että tulosteiden tuhoamiselle on laadittu tietoturvallisen tuhoamisen menettelyohjeet.

☒ Käytössä on asianmukaiset tietosuojaroskasäiliöt tai asiakirjasilppuri luokitellun tiedon tuhoamista varten.

☐

Tietokoneiden ja mobiililaitteiden tietoturva **LIITE 1-B (3/3)**

☒ Tilitoimiston käytössä olevat työasemat, kannettavat tietokoneet, mobiililaitteet ja muut päätelaitteet on rekisteröity ja dokumentoitu asianmukaisesti.

☒ Koneiden säännöllisistä tietoturvapäivityksistä on huolehdittu asianmukaisesti ja päivityksiä valvotaan.

☐ Työntekijöiden oikeutta asentaa ohjelmistoja työasemille on rajattu ja asennuksia valvotaan.

☒ Asianmukainen virus- ja haittaohjelmien torjuntaohjelmisto on käytössä.

☒ Tietoverkko ja tietokoneet on suojattu palomuurilla.

☐ Työntekijöiden henkilökohtaisten tietokoneiden ja mobiililaitteiden käyttö henkilötietojen käsittelyyn on kielletty.

☐

Siirrettävät tietovälineet

Siirrettäviä tietovälineitä ovat esimerkiksi USB-massamuistit, CD/DVD-levyt ja muut vastaavat muistilla tai tallennustilalla varustetut laitteet, jotka voidaan kytkeä tietokoneeseen.

☒ Tilitoimistossa ei käytetä siirrettäviä tietovälineitä työtehtävien hoitamiseen tai suojattavat tiedon käsittelyyn lukuun ottamatta erikseen sovittuja tilanteita, kuten aineiston luovutus tilintarkastajalle tai aineiston luovutus tai vastaanotto asiakkaan nimetyn yhdyshenkilön kanssa.

☐ Käytettäessä siirrettäviä tietovälineitä edellä mainittuihin tarkoituksiin on niiden sisältö suojattu salasanalla.

☐

Palvelin – ja tietoliikenneturvallisuus

☒ Toimitilojen palvelintilat ja tietoliikenneyhteyksien edellyttämät tilat pidetään lukittuina.

☒ Langattomien verkkojen tietoliikenne on salattu.

☒ Vierasverkot on eriytetty tilitoimiston sisäisestä tietoverkosta luotettavalla menetelmällä.

☒ Palvelinjärjestelmä on rakennettu vikasietoiseksi tai kahdennetuksi siten, että tietojärjestelmien toiminta ei keskeydy yksittäisestä laiterikosta.

☐

Taloushallinnon pilvipalvelut

Taloushallinnon pilvipalveluilla tarkoitetaan tässä kohdassa SaaS- tai ASP-palveluna toimitettavia taloushallinnon tietojärjestelmiä, joita organisaatio käyttää taloushallinnon palveluidensa tuottamiseen omille asiakkailleen.

☒ Sopimuksiimme taloushallinnon pilvipalveluiden käytöstä sisältyy kirjallinen palvelutasosopimus.

☐ Tilitoimiston ja palvelutarjoajan välinen vastuunjako on dokumentoitu kirjallisesti.

☐ Tilitoimisto on saanut palveluntarjoajalta selvitykset, jotka todentavat, että palvelua tuotetaan tietosuoja-asetuksen sekä kirjapitolain asettamat aineiston säilytysvaatimukset huomioiden.

☐

ASIAKKAAN ANTAMA OHJEISTUS HENKILÖTIETOJEN KÄSITTELYSTÄ LIITE 1-C

Tilitoimisto toimii henkilötietojen käsittelijänä, sisältäen arkaluontoisten tietojen käsittelyn. Perusteena tälle ovat (voi valita useita)

- ☐ Sopimus
- ☐ Suostumus
- ☐ Oikeutettu etu – merkityksellinen asiakassuhde
- ☐ Lakisääteinen velvoite – esimerkiksi työnantajavelvoitteet

Henkilötietojen välitys tapahtuu tilitoimistolle

- ☐ Sähköpostilla
- ☐ Turvasähköpostilla
- ☐ SharePoint pilvipalvelulla (käytettävissä myöhemmin ilmoitettavana ajankohtana)
- ☐ Postitse ja/tai faksilla
- ☐ Taloushallinto-ohjelmalla / työajanseurantaohjelmalla
- ☐ Muu (mikä?)

Tietoja tulee käsitellä asiantuntemuksella ja luottamuksellisesti, siten ettei niihin ole pääsyä muilla kuin tilitoimiston palkanlaskentaan osallistuvalla henkilökunnalla.

Tilitoimisto saa säilyttää henkilötietoja sisältävää materiaalia vain tarvittavan ajan**.** haluaa, että

- ☐ Tilitoimisto arkistoi tarvittavan palkkamateriaalimme
  - ☐ Paperisena
  - ☐ Sähköisenä
- ☐ Tilitoimisto toimittaa palkkamateriaalin meidän arkistoitavaksemme
  - ☐ Postitse
  - ☐ Sähköisesti

Henkilötietojen käsittelyn päättyessä tilitoimiston tulee

- ☐ Palauttaa aineisto.
  - ☐ Postitse
  - ☐ Sähköisesti
- ☐ Tuhota aineisto.

Tilitoimiston palkanlaskennanprosessin kuvaus tulee olla saatavillamme, samoin tietoturvaselosteen koskien yritystämme. Näin voimme varmistaa tilitoimiston tietosuojan olevan asetuksen vaatimalla tasolla.
Tilitoimiston tulee niin halutessamme olla valmis auditointiin.

Rekisterinpitäjänä huolehdimme, että rekisteröidyillä on oikeus

- saada tarkastaa itseään koskevat tiedot sekä oikeus vaatia virheellisen tiedon oikaisua
- oikeus kieltää henkilötietojen käsittely
- tiedon poistamiseen lakisääteisen säilyttämisvelvollisuuden päätyttyä tai
- ainakin tietojen anonymisointiin eli tietojen käsittelyyn siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn

Tilitoimiston henkilökunnalla ei ole oikeutta luovuttaa rekisteröityjen tietoja eteenpäin millekään taholle.

Paikka ja aika

_____

Allekirjoitus

Nimenselvennys

TURVALLISET TIEDONSIIRTOKANAVAT LIITE 1-D

Tilitoimisto ja asiakkaan välisenä tietoturvallisena tietojen siirron kanavana toimii SharePoint pilvipalvelu, joka on osa Microsoft Office 365: a. SharePoint on kaksisuuntainen kanava, jonne asiakas voi tallentaa palkkamateriaalia tilitoimiston käyttöön sekä hakea sieltä tilitoimiston tallentamaa palkanlaskentamateriaalia. Palvelua käytetään myös aineistojen arkistointiin tilitoimiston katsomassa laajuudessa. Palvelun käyttö vaatii Microsoft Live -tilin, jonka luominen on ilmaista ja sen voi luoda millä tahansa jo olemassa olevalla sähköpostiosoitteella. SharePoint on SSL -salattu.

SharePointin lisäksi tilitoimisto voi lähettää palkanlaskentamateriaalia, esimerkiksi palkansaajien henkilökohtaiset palkkalaskelmat, DSL -salausta käyttävän sähköpostin kautta. Microsoft Officen sähköpostiin on saatavissa maksullinen lisäosa, joka takaa tietoturvallisen sähköpostin lähetyksen. Tämä toimii kuitenkin vain yhteen suuntaan, joten palkka-aineiston lähettäminen tilitoimistolle ei onnistu, ellei asiakkaalla itsellään ole käytössä vastaavaa lisäosaa.

Asiakas voi halutessaan ottaa käyttöön myös verkkopalkan. Verkkopalkka -toiminnolla palkkalaskelma toimitetaan suoraan palkansaajan verkkopankkiin, josta hän voi sen omilla henkilökohtaisilla pankkitunnuksillaan noutaa. Verkkopalkka toimitetaan kanavan kautta, jonka välittäjänä toimii Maventa, ja palvelu on maksullinen.

Asiakkaalle voidaan antaa käyttäjätunnukset tiedon noutamiseen suoraan käytettävästä taloushallinto-ohjelmistosta. Käyttäjätunnuksilla voidaan mahdollistaa myös tiedon toimittaminen suoraan taloushallinto-ohjelmistoon. Ohjelmiston toimittaja voi edellyttää käyttäjätunnuksista maksua, jonka tilitoimisto on oikeutettu laskuttamaan asiakkaalta.

Muokattu Taloushallintoliiton mallista

Henkilötietojen käsittelyn turvallisuuden varmistaminen - sähköinen prosessi

PALKANLASKENTAPROSESSI

Tässä dokumentissa näkyy listattuna, mitä eri aineistoja toimistomme palkanlaskennassa käsitellään. Kunkin aineiston kohdalla kuvataan prosessi palkanlaskennan lähdeaineistojen vastaanotosta tietojen tallentamiseen järjestelmiin sekä lähdeaineistojen arkistointiin tai hävitykseen.
Aineistot on luokiteltu kolmeen ryhmään:

- Arkaluontoinen – aineistossa on tai voi olla tietoa henkilön AY-jäsenyydestä tai terveydestä
- Normaali – aineisto sisältää henkilötietoja, kuten osoitteet tai pankkitiedot.
- Ei henkilötietoa – esimerkiksi kirjanpitoa varten tuotettu tosite ei yleensä sisällä lainkaan henkilötason tietoa.

Asiakkaille on suositeltu arkaluontoisten henkilötietojen toimittamista käyttäen suojattuja tietojen välityskanavia tai vaihtoehtoisesti faksia tai kirjepostia. Asiakas voi käyttää omia suojattuja tiedonsiirto kanavia, joita ovat esimerkiksi turvasähköposti. Tiedot voidaan toimittaa myös hyödyntäen asiakkaan käytössä olevia työajanseurantajärjestelmiä tai tieto voidaan liittää asiakkaan toimesta suoraan taloushallinto-ohjelmaan. Lisäksi käytössä on salasanasuojattu kahdensuuntainen tietojen siirto ja arkistointijärjestelmä Sharepoint, jonka käytöstä sovitaan asiakkaittain.
Myös muita ratkaisuja voi asiakkaan kanssa olla sovittuna. Tähän on kirjattava asiakaskohtaiset ratkaisut.

AINEISTO	LUOKITUS	VASTAANOTTOTAPA	JATKOKÄSITTELY	SÄILYTYSTAPA	SÄILYTYSAIKA	HÄVITYSTAPA
Työntekijän perustiedot – työsopimuksen kopio	Normaali (Huom AY, entä henkilötunnus)	Paperiposti, sähköposti (ei ay-tieto eikä henkilötunnus), (MUOKATTAVA ASIAKKAITTAIN!)	Syötetään palkkajärjestelmään, arkistoidaan palkanlaskenta-aineistoon henkilöiden perustietoihin	Asiakaskohtainen palkkamappi (henkilöiden perustiedot) Pilvipalvelussa asiakaskohtaisissa tiedostoissa (MUOKATTAVA ASIAKKAITTAIN)	10 vuotta työsuhteen päättymisestä. (Tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Ei hävitetä, jos työsuhde voimassa. (Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä päättyneiden työsuhteiden osalta).
AY-jäsenmaksun perintäsopimus	Arkaluontoinen	Paperiposti, sähköposti: sovittava säilyttääkö asiakas vai tilitoimisto alkuperäisen	Syötetään palkkajärjestelmään, arkistoidaan palkanlaskenta-aineistoon henkilöiden perustietoihin	Asiakaskohtainen palkkamappi (henkilöiden perustiedot)	10 vuotta (Liiketapahtumia koskevaa kirjeenvaihtoa)	Ei hävitetä, jos työsuhde voimassa. (Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä päättyneiden työsuhteiden osalta)
Ulosotto	Arkaluontoinen	Paperiposti, sähköposti	Syötetään palkkajärjestelmään, arkistoidaan palkanlaskenta-aineistoon henkilöiden perustietoihin	Asiakaskohtainen palkkamappi (henkilöiden perustiedot)	10 vuotta (Liiketapahtumia koskevaa kirjeenvaihtoa, tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Maksukielto hävitetään kerran vuodessa ulosoton päätyttyä (ei arkistoida). Tiedot ulosotosta hävitetään 10 vuoden

						säilytysajan täytyttyä.

AINEISTO	LUOKITUS	VASTAANOTTOTAPA	JATKOKÄSITTELY	SÄILYTYSTAPA	SÄILYTYSAIKA	HÄVITYSTAPA
Työaikalista	Normaali	Paperiposti, sähköposti	Syötetään palkkajärjestelmään, arkistoidaan palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot) Pilvipalvelussa asiakaskohtaisessa tiedostossa	10 vuotta Tosite (tuntipalkat, ylityöt, työajan joustot yms., tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Lääkärintodistus	Arkaluontoinen	Paperiposti, sähköposti: sovittava säilyttääkö asiakas vai tilitoimisto/palkanlaskenta alkuperäisen	Syötetään poissaolo palkkajärjestelmään. Tarvittaessa tehdään Kela- tai tapaturmavakuutushakemus, johon liitetään lääkärintodistuksen kopio, arkistoidaan arkaluontoisena tietona erilleen normaalista palkka-aineistosta	Erillinen asiakaskohtainen säilytys sairaustiedoille	10 vuotta Tosite ja hakemukset (Tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä), 1 vuosi Todistus	Hävitetään todistukset kerran vuodessa (ei viedä arkistoon). Hakemukset ja tositteet hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä.

AINEISTO	LUOKITUS	VASTAANOTTOTAPA	JATKOKÄSITTELY	SÄILYTYSTAPA	SÄILYTYSAIKA	HÄVITYSTAPA
KELAn/Tapaturmavakuutusyhtiön maksupäätös liittyen sairaslomaan	Arkaluontoinen	Paperiposti, sähköposti tai Kelan tulostus asiointipalvelusta	Tehdään sairausvakuutusmaksuvähennys, arkistoidaan arkaluontoisena tietona erilleen normaalista palkka-aineistosta	Erillinen asiakaskohtainen säilytys sairaustiedoille Pilvipalvelussa asiakaskohtaisessa tiedostossa erillään	10 vuotta Tosite (Tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Maksutiedot	Normaali; Arkaluontoinen, jos AY- ja ulosottotiedot sisältävät henkilötiedot	Palkanlaskennasta maksutiedot	Toimitetaan tieto asiakkaalle maksamista varten tai summatieto hyväksyttäväksi ennen tilitoimistossa maksua, maksukuittaukset	Asiakaskohtainen palkkamappi (palkka-ajot)	10 vuotta Tosite (Tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Palkkalista/ tapahtumalista	Normaali, jos AY tai ulosotto eriteltynä, arkaluontoinen	Palkanlaskennasta tiedot	Arkistoidaan tuloste palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot)	10 vuotta, päiväkirja	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Palkkalaskelma	Normaali	Palkanlaskennasta tiedot	Arkistoidaan tuloste palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi ja/	2 vuotta tulosteena ja/tai	Hävitetään kerran vuodessa 2

				kansio pilvipalvelussa. Palkanlaskentaohjelmassa	pilvipalvelussa. (Tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	vuoden säilytysajan täytyttyä, ei siirretä arkistoon.

AINEISTO	LUOKITUS	VASTAANOTTOTAPA	JATKOKÄSITTELY	SÄILYTYSTAPA	SAILYTYSAIKA	HÄVITYSTAPA
Palkanlaskennan yhteenveto kirjanpitoon ”Kirjanpidon tosite”	Ei henkilötietoja	Palkanlaskennasta tiedot	Tallennetaan kirjanpitoon	Taloushallinto-ohjelmassa, ei paperisäilytystä	10 vuotta, kirjanpitoviennit (tiliöinnit, tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Lomapalkkavelka erittely henkilöittäin	Normaali	Palkanlaskennasta tiedot	Arkistoidaan tuloste sovittavissa ajanjaksoissa (kk tai vuosi) palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot)	10 vuotta, päiväkirja	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Lomapalkkavelka yhteenveto kirjanpitoon ”Kirjanpidon tosite”	Ei henkilötietoja	Palkanlaskennasta tiedot	Tallennetaan kirjanpitoon, arkistoidaan tuloste palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot)	10 v vuotta, kirjanpitovienti (tiliöinnit, tehostaa Audit Trailia, auttaa mahdollisissa työntekijää palvelevissa selvityksissä)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä

AINEISTO	**LUOKITUS**	**VASTAANOTTOTAPA**	**JATKOKÄSITTELY**	**SÄILYTYSTAPA**	**SÄILYTYSAIKA**	**HÄVITYSTAPA**
Kuukausi-Ilmoitustiedot	Normaali, AY-jäsenmaksun henkilötason tieto arkaluontoinen	Palkanlaskennasta tiedot	Toimitetaan tieto ja tehdään tilitys verottajalle, AY-liitolle, TyEl-vakuutusyhtiölle (kuukausi-ilmoittaja), arkistoidaan tuloste palkanlaskenta-aineistoon. Jatkossa ilmoitus tulorekisteriin. (2019 alkaen)	Asiakaskohtainen palkkamappi (palkka-ajot)	10 vuotta (Liiketapahtumia koskevaa kirjeenvaihtoa, tehostaa Audit Trailia)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä
Vuosi-Ilmoitustiedot, viimeisen kerran vuodelta 2018	Normaali	Palkanlaskennasta tiedot	Toimitetaan tieto verottajalle, TyEl-vakuutusyhtiölle (vuosi-ilmoittaja), tapaturma- ja työttömyysvakuutusyhtiölle, arkistoidaan tuloste palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot) Pilvipalvelussa asiakaskohtaisessa tiedostossa	10 vuotta (Liiketapahtumia koskevaa tiedonsiirtoa, tehostaa Audit Trailia)	Hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä

AINEISTO	LUOKITUS	VASTAANOTTOTAPA	JATKOKÄSITTELY	SÄILYTYSTAPA	SÄILYTYSAIKA	HÄVITYSTAPA
Palkkakortti	Normaali	Palkanlaskennasta tiedot	Kerran vuodessa tulostetaan palkanlaskennasta, arkistoidaan tuloste palkanlaskenta-aineistoon	Asiakaskohtainen palkkamappi (palkka-ajot)	6 vuotta (Liiketapahtumia koskevaa kirjeenvaihtoa, tehostaa Audit Trailia)	Hävitetään kerran vuodessa 6 vuoden säilytysajan täytyttyä
Tukipäätökset esim. TEKES, EU	Normaali	Palkanlaskennasta ja kirjanpidosta tiedot	Toimitetaan tiedot tukipäätöksen myöntäjälle, arkistoidaan erillään palkanlaskenta-aineistosta se osuus, joka säilytettävä	Asiakaskohtainen säilytys pidempiaikaisille säilytettäville tiedoille	Säilytysaika löytyy avustussopimuksesta	Tiedot löytyvät avustussopimuksesta

Mikäli laadimme palkka- ja/tai työtodistuksia, säilytämme niistä kopiot pilvipalvelussamme ja palkkamapissa, säilytysaika 10 vuotta, hävitetään kerran vuodessa 10 vuoden säilytysajan täytyttyä.

Seloste henkilötietojen käsittelytoimista -pohja

SELOSTE HENKILÖTIETOJEN KÄSITTELYTOIMISTA

Rekisterinpitäjä [ ]
Käsittelijä [x]

Laatimispäivä
PVM

Rekisterinpitäjä; sekä tämän edustaja (tarvittaessa)	Nimi ASIAKKAAN TIEDOT
	Osoite ASIAKKAAN TIEDOT
	Muut yhteystiedot (puhelin, sähköpostiosoite) ASIAKKAAN TIEDOT
Käsittelijä	Nimi Tilitoimisto
	Osoite
	Muut yhteystiedot (puhelin, sähköpostiosoite) TÄHÄN OMAT TIETOSI
Alihankkijan yhteystiedot (tarvittaessa)	Alihankkijoita ei käytetä, päivitetään tieto tarvittaessa
Tietosuojavastaavan yhteystiedot (tarvittaessa)	
Rekisterin nimi	TÄHÄN YRITYKSENNIMI palkka ja henkilöstöhallinto
Henkilötietojen käsittelyn tarkoitus	Työnantajavelvoitteiden hoitaminen. Palkanlaskennan lisäksi rekisterissä käsitellään henkilöstöhallinnon tietoja mm. yhteistoimintalain velvoitteiden noudattamiseksi, kuten koulutussuunnitelmat.
Rekisteröityjen ryhmät ja henkilötietoryhmät	Kuukausipalkat Tuntipalkat Palkkiot Matkalaskut

Seloste henkilötietojen käsittelytoimista -pohja

Säännönmukaiset tietolähteet	Työntekijä, työnantaja, verohallinto, Kela, tapaturmavakuutusyhtiö, ay-jäsenmaksuliitot, ulosottoviranomainen Muut tahot, joiden antama tieto on käsiteltävä palkanlaskennassa
Henkilötietojen vastaanottajien ryhmät - myös kolmansissa maissa olevat sekä kansainväliset järjestöt (nimi)	Säännönmukaiset vastaanottajat: verohallinto, eläke- ja tapaturmavakuutusyhtiöt sekä työttömyysvakuutusrahasto, Kela, työnantajaliitto, tilastokeskus, ay-jäsenmaksuliitot, ulosottoviranomainen, tulorekisteri jatkossa vuoden 2019 alusta alkaen Muut tahot, joilla on oikeus saada tietoja yrityksen palkanlaskennasta. Tietoja ei luovuteta kolmansiin maihin tai kansainvälisille järjestöille.
Tekniset ja organisatoriset turvatoimet	Tilitoimisto on kuvannut asiakaskohtaisesti palkka- ja henkilöstöhallinnon prosessin, jossa on huomioitu rekisteröidyn oikeuksien turvaamiseksi tehdyt suojatoimenpiteet. Tilitoimisto on kouluttanut henkilöstönsä tietosuoja-asetuksen sisällöstä. Henkilöstö on tehnyt salassapitosopimuksen.
Tietoryhmien suunnitellut poistamisajat (mahdollisuuksien mukaan)	Poistamisajat on käsitelty prosessikuvauksessa.
Rekisteröidyn oikeudet	Rekisterinpitäjä on tehnyt erillisen kuvauksen tietosuoja-asetuksen mukaisesti rekisteröidylle tiedotettavista asioista
Rekisterinpitäjän ohjeistus tietojen käsittelijälle	Rekisterinpitäjä on antanut käsittelijälle erillisen ohjeistuksen palkka- ja henkilöstörekisterin tietojen käsittelystä
Tietoturvaloukkauksista ilmoittaminen	**Rekisterinpitäjälle** Ilmoitus tehdään rekisterinpitäjälle ilman aiheetonta viivästystä tietoturvaloukkauksen ilmitulosta.
	Rekisteröidylle Ilmoitus tehdään rekisteröidylle, jos tietoturvaloukkauksesta aiheutuu todennäköisesti korkea riski tämän oikeuksille ja vapauksille.
	Valvontaviranomaiselle Ilmoitus tehdään tietoturvaviranomaiselle 72 tunnin kuluessa ilmitulosta, mikäli tietoturvaloukkauksesta todennäköisesti aiheutuu luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Muokattu Taloushallintoliiton mallista
Asiakastiedotemalli: Toimintaohje EU:n tietosuoja-asetuksen hallintaan

TOIMINTAOHJE EU:N TIETOSUOJA-ASETUKSEN HALLINTAAN

EU:n tietosuoja-asetus tulee voimaan 25.5.2018. Asetus velvoittaa myös pieniä yrityksiä henkilötietojen tarkempaan suojaamiseen. Nykyiseen henkilötietolakiin verrattuna tietosuoja-asetus sisältää yrityksille uusia velvoitteita. EU:n tietosuoja-asetuksen kanssa samalla on tarkoitettu tulevaksi voimaan Suomen lainsäädäntöön hallituksen esittämät täydennykset ja täsmennykset. Voit halutessasi lukea tästä lisää osoitteesta www.finlex.fi → hallituksen esitykset → HE 9/2018.

Asiakas- ja työntekijärekisteri

Useimmilla yrityksillä on jonkinlainen **asiakasrekisteri**. Vaikka asiakaskunta koostuisi pelkästään yrityksistä, on rekisterissä yleensä tietoa myös asiakasyritysten yhteyshenkilöistä. Teidän kannattaa käydä läpi, mitä tietoa sinne on henkilöistä tallennettu.

Yleensä asiakasrekisterit eivät sisällä kovinkaan arkaluontoisia henkilötietoja, joten niiden suhteen ei kannata tehdä kärpäsestä härkästä. Maanläheinen toimintatapojen kartoitus ja sopiminen ovat kuitenkin paikallaan. Esimerkiksi asiakastietojärjestelmän asianmukainen käyttäjähallinta on tärkeää myös liikesalaisuuksien, eikä yksinomaan henkilötietojen turvallisuuden näkökulmasta.

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

MUOKKAA TÄMÄ YRITYSKOHTAISESTI SOPIVAKSI
Olemme sopineet kanssanne palkanlaskentaa varten seuraavat yhteyskäytännöt:

- Yrityksessänne hoitaa palkanlaskentaan liittyviä asioita nimetty yhteyshenkilö
- Toimitatte meille palkanlaskentaa varten tarvittavat tiedot sovitulla tavalla
- Toimitamme teille palkanlaskennassa tuotetut tiedot sovitulla tavalla
- Palautamme tai hävitämme sovittavalla tavalla palkanlaskennan aineistot, kun niitä ei enää tarvita kirjanpitolain tai muun lainsäädännön perusteella

Tärkeintä on se, että teillä on selkeä toimintatapa, miten säilytätte työntekijöiltä keräämänne ja meiltä vastaanottamanne henkilötietoja sisältävän aineiston. **Aineisto tulee säilyttää paperilla lukkojen takana tai tiedostomuodossa sellaisissa hakemistoissa, jotka on rajattu käyttöoikeuksin henkilöille, jotka tietoja työssään tarvitsevat.**

Käytännön toimia pk-yrityksissä

- Arkistoi työntekijöiden lääkärintodistukset, ulosottodokumentaatio, AY-jäsenyystiedot ja vastaavat omaan mappiinsa lukkojen taakse tai sähköisessä muodossa hakemistoon, jonka käyttöoikeudet on rajattu.

- Harkitse, voiko arkaluontoiset tiedot lähettää suojaamattomassa sähköpostissa. Hyvin monet sähköpostipalvelut käyttävät jo salattua yhteyttä ja tarvittaessa löytyy ilmaisia sovelluksia sähköpostin sisällön suojaamisen.

- Laadi ohjeet henkilötietojen käsittelyyn ja kouluta henkilöstö. Muista arkijärki siinä, mikä on oikeasti arkaluontoista. Voit kysyä meiltä ohjausta tai apua.

- Muista, että jos et ole sopinut kanssamme toisin, työntekijäsi eivät saa kysellä palkka-asioitaan suoraan meiltä. Meillä ei yleensä ole mahdollisuutta tunnistaa kyselijää luotettavasti.

- Asiakasrekisteriinne rekisteröidyillä henkilöillä, samoin kuin työntekijöillänne, on oikeus tarkastaa omat tietonsa ja korjauttaa virheet. Mieti menettely, jolla kysyjä (esimerkiksi asiakkaan henkilö) tunnistetaan ja miten tiedot annetaan. Voit kysyä meiltä ohjausta tai apua.

- 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 asiakirjat tositteita, jotka tulee säilyttää vähintään 6 vuotta, lääkärintodistukset, joista on päätös tehty, ovat KELA:lla, joten niiden säilytykselle 1 vuotta pidempään emme näe tarvetta. Ne tulee hävittää säilytysvelvollisuuden umpeuduttua, koska säilytyksellä ei ole enää lakisääteistä tai muuta perustetta.

Tietosuoja-asetukseen liittyviä käsitteitä

Rekisteröity tarkoittaa henkilötietojen pohjalta tunnistettavissa olevaa ihmistä, jonka henkilötiedot ovat käsittelyn kohteena. Tietosuoja-asetus ei siis säätele esimerkiksi yrityksen asiakasrekisterin pitoa muuten kuin asiakkaiden yhteyshenkilöiden osalta.

Henkilötiedot tarkoittavat kaikkia rekisteröityä koskevia tietoja, joiden perusteella tämä on suoraan tai epäsuorasti tunnistettavissa. Osa tiedoista on asetuksessa säädetty erityisen arkaluontoiseksi. Esimerkkinä voidaan mainita ihmisen terveystiedot ja ay-jäsenyystiedot.

Rekisteri tarkoittaa mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa. Tietokantojen lisäksi esimerkiksi Excel-taulukko voi siis muodostaa rekisterin. Tyypillisiä rekistereitä pk-yrityksissä ovat asiakasrekisteri sekä työntekijärekisteri henkilöstöhallinnon ja palkanlaskennan tarpeisiin.

Rekisterinpitäjä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Pk-yritys on työntekijärekisterinsä pitäjä, vaikka palkanlaskenta olisikin ulkoistettu tilitoimistolle ja vaikka tilitoimisto hoitaisi rekisterin tietojen ylläpidon ja käyttäisi rekisteriä palkanlaskennan hoitoon.

Henkilötietojen käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi tilitoimisto, joka käsittelee asiakkaiden työntekijöiden tietoja laskeakseen palkat, on henkilötietojen käsittelijä.

Riskiperusteisuus tarkoittaa sitä, että yrityksen toimet on suunniteltava sen mukaan, mikä riski tietojen vuotamisella tai häviämisellä on. Esimerkiksi asiakasrekisterissä oleva tieto siitä, että Ville Virtanen (insinööri) toimii tuotantopäällikkönä yrityksessä X ja käyttää tiettyä puhelinnumeroa ja sähköpostiosoitetta ei aiheuta samanlaista riskiä kuin terveydenhuoltoalan yrityksen tieto asiakkaan terveydentilan kehityksestä tai palkanlaskentaa varten rekisteröity tieto Pekka Pekkalan sairauspoissaolojen suuresta määrästä.

OHJEET LAPPUSTEN TÄYTTÖÖN

PALKANLASKENNAN PROSESSIKAAVIO

1. Tallenna tiedosto asiakkaan kansioon nimellä esim. Prosessikuvaus *asiakkaan nimi*
2. Kirjoita ensimmäiselle sivulle palkanlaskentaprosessi *asiakkaan nimi :lla*
3. Kirjoita kolmanteen kohtaan (viimeinen lause punainen) kyseisen asiakkaan kanssa käytössä olevat tiedonvälityskanavat.
4. Käy taulukoista läpi kohdat **aineisto** ja **vastaanottotapa** tarkista, että
    a. kaikki kyseisen asiakkaan kanssa käytössä olevat palkanlaskennan prosessit ovat taulukoissa kuvattuina,
    b. vastaanottotapojen kohdalle lisää kyseisen asiakkaan kanssa käytössä olevat tavat *aineistokohtaisesti*.

SELOSTE HENKILÖTIETOJEN KÄSITTELYSTÄ

1. Kirjoita punaisella tehtyihin kohtiin pyydetyt tiedot → vaihda teksti mustaksi =)
2. Tarkista, että muut kohdat ovat kyseisen asiakkaan kohdalla paikkansapitävät

Tietosuojavastaavaa ei Tilitoimistolla tarvitse nimetä

ASIAKKAALLE TEHTÄVÄT LIPPUSET JA LAPPUSET

- Sopimus henkilötietojen käsittelystä - pohjalta
  - ✓ Prosessikuvaus
  - ✓ Seloste henkilötietojen käsittelystä
- Toimeksiantosopimus
  - ✓ Tee tämä olemassa olevan palvelusopimuksen/palvelukuvauksen perusteella
  - ✓ Mikäli asiakkaan kanssa on sovittu hinnastosta poikkeava hinta, pitää se merkitä sopimuksen ”muuta” riville.
  - ✓ Laita saate kirjeeseen, että sopimus on esitäytetty olemassa olevien tietojen pohjalta. Pyydä asiakasta käymään sopimus läpi ja tarvittaessa lisäämään/poistamaan kohtia.
- Lähetä asiakkaalle
  - ✓ Toimeksiantosopimus
  - ✓ Yleiset sopimusehdot TAL2018 LIITE 1
  - ✓ Apteekkien hinnasto 2018
  - ✓ Prosessikuvaus
  - ✓ Seloste henkilötietojen käsittelystä

MUUTA

Sopimus henkilötietojen käsittelystä -liitetiedostot ovat sellaisia, joita voidaan matkan varrella tarvittaessa päivittää. Tarkoitus olisi, että päivitys tapahtuu kerran vuodessa esimerkiksi syksyisin. Liite 1-B:ssä osassa kohtia ei ole vielä rastia, mutta niihin tulee rastit siinä vaiheessa, kun saamme asiat niiltä osin kuntoon. Pääasia on, että riskikohdat tunnistetaan ja niihin puututaan.

Toimintamalli työsuhteen päättyessä tilitoimistossa on lyhykäisesti seuraava;

> ”Materiaalia ei tulisi toimintatapojen mukaan olla työntekijän hallussa, vaan kaikki materiaali on joko toimistolla tai sähköisissä järjestelmissä. Sähköposti poistuu työntekijän käytöstä, mutta jää toimiston arkistoon. Käyttäjätunnukset poistetaan käytöstä.”

Tästä on siis tulossa dokumentoitu malli =) ja muitakin parannuksia.

Meillä on lakisääteinen velvollisuus säilyttää työmme jälki 10 vuotta eli asiakkaan dokumentteja ei tuhota ennen sen täyttymistä, vaikka hän valitsisi rastin kohtaan aineiston tuhoaminen.

- INNOX:ssa on jokaisen asiakkaan alla ”täppä” kohdat
  - ✓ Toimeksiantosopimus
  - ✓ Sopimus henkilötietojen käsittelystä

➔ Käy ruksimassa kohdat sitä mukaa, kun kyseisen asiakkaan kohdalta kyseiset asiakirjat ovat kunnossa!

KOULUTUSTA TULOSSA:

- Arkistointi
- TEAMS ja SharePoint
- Tietoturva

OHJEISTUS TIETOTURVALOUKKAUKSISSA

Mikäli huomaat tietoturvaloukkauksen tai epäilet sellaisen sattuneen

- ➔ Ota yhteys lähiesimieheesi
- ➔ Selvittäkää tilanne, onko tietoturvaa loukattu

Tietoturvaloukkauksen ollessa todella tapahtunut

- ➔ Tulee **Rekisterinpitäjälle** tehdä ilmoitus ilman aiheetonta viivästystä tietoturvaloukkauksen ilmitulosta

- ➔ Ottakaa yhteys myös tilitoimiston tietosuoja asioista vastaavaan työntekijäämme

  Milla Mallikas
  010 123 4567
  etunimi.sukunimi@tilitoimisto.go

- ➔ Mikäli tietoturvaloukkauksesta *aiheutuu todennäköisesti korkea riski* rekisteröityjen oikeuksille ja vapauksille, tehdään ilmoitus myös henkilökohtaisesti **rekisteröidyille**, joita loukkaus koskettaa.

Ilmoituksen tulisi sisältää:

- ➔ Selkeä ja yksinkertainen kuvaus tapahtuneesta
- ➔ Tietosuoja-asioista vastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta rekisteröidyt voivat halutessaan kysyä lisätietoja
- ➔ Tiedot siitä, millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidylle
- ➔ Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla

➔ Mikäli tietoturvaloukkauksesta *todennäköisesti aiheutuu luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä*, tulee ilmoitus tehdä myös **tietoturvaviranomaiselle** 72 tunnin kuluessa ilmitulosta.

Valvontaviranomaiselle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavat kohdat:

- ➔ Kuvaus, mitä on tapahtunut
- ➔ Mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa
- ➔ Tietosuoja-asioista vastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta valvontaviranomainen voi kysyä lisätietoja
- ➔ Millaisia vaikutuksia tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille
- ➔ Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi

Mikäli ilmoitusta valvontaviranomaiselle ei ole mahdollista tehdä 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta, on rekisterinpitäjän kuitenkin toimitettava tässä ajassa ilmoitukseensa perusteltu selvitys viivästyksen syistä valvontaviranomaiselle. Tarvittaessa tietoja voidaan antaa vaiheittain.
Ilmoituksista löytyy valmiiksi laadittu pohja Pilvestä → kansiosta GDPR

ILMOITUS TIETOTURVALOUKKAUKSESTA

Kirjoita tähän SELKEÄ ja YKSINKERTAINEN kuvaus tapahtuneesta tietoturvaloukkauksesta

Kuvaus tapahtuneesta
Tilitoimistolla tietosuoja asioista vastaa

Milla Mallikas
010 123 4567
milla.mallikas@tilitoimisto.go

Kerro tässä tietoturvaloukkauksen mahdollisista seurauksista rekisteröidylle

Yllä mainitulla henkilötietojen tietoturvaloukkauksella voi olla seuraavanlaisia vaikutuksia rekisteröidylle

Kirjoita tähän RIITTÄVÄN YLEISELLÄ TASOLLA toimenpiteet, joita aiotaan toteuttaa tai jotka on jo toteutettu haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi

Toimenpiteet haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi

Ilmoittajan tiedot

Toimisto, jossa loukkaus tapahtunut
Oma nimesi
010 123 XXXX
etunimi.sukunimi@tilitoimisto.go

ILMOITUS TIETOTURVALOUKKAUKSESTA

Kirjoita tähän SELKEÄ ja YKSINKERTAINEN kuvaus tapahtuneesta tietoturvaloukkauksesta

Kuvaus tapahtuneesta

Kirjoita tähän (mikäli mahdollista) niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa

Loukkauksen kohteeksi joutuneet ryhmät ja lukumäärät

Tilitoimiston tietosuoja asioista vastaa

Milla Mallikas
010 123 4567
milla.mallikas@tilitoimisto.go

Yllä mainitulla henkilötietojen tietoturvaloukkauksella voi olla seuraavanlaisia vaikutuksia rekisteröidylle

Kerro tässä tietoturvaloukkauksen mahdollisista seurauksista rekisteröidylle

Toimenpiteet haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi

Kirjoita tähän toimenpiteet, joita aiotaan toteuttaa tai jotka on jo toteutettu haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi

Ilmoittajan tiedot

Toimisto, jossa loukkaus tapahtunut
Oma nimesi
010 123 XXXX
etunimi.sukunimi@tilitoimisto.go