VAT:n tietosuoja, tietoturva ja uuteen henkilötietolakiin liittyvät tarkennukset.

Asiakkaiden tietojen turvallista käsittelyä säätelevät monet asetukset, lait ja määräykset, kuten EU:n henkilötietolaki (Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelystä sekä näiden tietojen vapaasta liikkuvuudesta).

EU:n henkilötietolaki

EU:n henkilötietolaissa on selkeästi määritelty asioita, jotka koskevat myös työpaja- ja avokuntoutustoimintaa. Seuraavaan on koottu keskeisiä em. toimintaan liittyviä määritelmiä ja periaatteita. Täydelliset kuvaukset löytyvät em. asetuksen eri kohdista.

- **Henkilötiedoilla**, kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ´**rekisteröity´,** liittyviä tietoja.
- **Rekisterillä,** mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot on saatavissa tietyin perustein.
- **Rekisterin pitäjällä,** luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
- **Kolmannella osapuolella**, luonnollista henkilöä, tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterin pitäjää, henkilötietojen käsittelijää ja henkilöä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.
- **Rekisteröidyn suostumuksella,** mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen**.**
- Jos tietojen **käsittely perustuu suostumukseen**, rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn.
- **Henkilötietojen** on oltava asianmukaisia ja olennaisia ja rajoittua siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Luonnolliselle henkilölle (rekisteröidylle) olisi tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista ja siitä, miten he voivat käyttää tallaista käsittelyä koskevia oikeuksiaan.
- Henkilötietojen käsittely on lainmukaista jos ja vain siltä osin kun vähintään yksi edellytyksistä täyttyy.
    - rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
    - käsittely on tarpeen rekisterin pitäjän lakisääteisen velvoitteen noudattamiseksi
    - käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi

- Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisten henkilöiden seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä. Ellei:
    - rekisteröity on antanut nimenomaisen suostumuksen kyseisten tietojen käsittelyyn
    - käsittely on tarpeen rekisterin pitäjän tai rekisteröidyn velvoitteiden tai erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla.

Rekisteröidylle toimitettavat / informoitavat tiedot kun tietoja kerätään rekisteröidyltä sekä rekisteröidyn oikeudet saada pääsy tietoihin.

Kerättäessä tietoja rekisteröidyltä häntä koskevia rekisteritietoja on silloin, kun rekisteritietoja saadaan, toimitettava rekisteröidylle seuraavat tiedot.

- rekisterin pitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot
- tapauksen mukaan tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- henkilötietojen vastaanottajat tai vastaanottajaryhmät
- tieto siitä siirretäänkö henkilötietoja kolmanteen maahan
- jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot

Lisäksi on toimitettava seuraavat lisätiedot jotka takaavat tietojen käsittelyn läpinäkyvyyden

- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- rekisteröidyn oikeus pyytää rekisterin pitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen
- oikeus peruuttaa suostumus milloin tahansa
- oikeus tehdä valitus valvontaviranomaiselle
- onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterin pitäjän on ilmoitettava rekisteröidylle

ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava asiaankuuluvat lisätiedot.

Tietojen oikaiseminen ja oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)

Rekisteröidyllä on oikeus vaatia, että rekisterin pitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.

Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, ja rekisterin pitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä.

- henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin
- rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytössä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterin pitäjälle jos:

- käsittely perustuu suostumukseen
- käsittely suoritetaan automaattisesti

Rekisteröidyllä on oikeus saada henkilötiedot siirrettyä suoraan rekisterin pitäjältä toiselle jos se on teknisesti mahdollista.

Rekisterin pitäjän vastuu

Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettavat tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.

Seloste käsittelytoimista

Jokaisen rekisterin pitäjän ja tarvittaessa rekisterinpitäjän edustajan on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Selosteen on käsitettävä seuraavat tiedot

- rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä

- henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan
- tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
- mahdollisuuksien mukaan eri tietoryhmien poistamiseen suunnitellut määräajat
- mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetusta teknisistä ja organisatorisista turvatoimista

Muut toimintaan vaikuttavat lait

Yllä on kuvattu niitä uuden lain mukanaan tuomia keskeisiä asioita jotka toteuttamalla henkilötietojen käsittely on pääosin kunnossa. Osa asioista on sellaisia jotka kerrottava asiakkaalle perehdyttämisen yhteydessä ja osa (rekisteriselosteen sisältö) on oltava myös vapaasti nähtävillä niissä tiloissa joissa asiakkaat ovat (esim. ilmoitustaululla).

Toimintaan vaikuttavia lakeja on toki muitakin. Alla on ainakin osa niistä, toki kaikki eivät koske jokaista työpajaa ja riippuen toimintaympäristöstä / asiakaskunnasta, lakeja voi olla myös lisää.

- Henkilötietolaki 1999/523 (korvautuu tuolla edellä mainitulla EU asetuksella v. 2018)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 2007/159
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain muuttamisesta 2014/250
- Laki yksityisistä sosiaalipalveluista 2011/922
- Sähköisen viestinnän tietosuojalaki 2004/516
- Laki potilaan asemasta ja oikeuksista 1992/785
- Laki Kansaneläkelaitoksen kuntoutusetuuksista ja kuntoutusrahaetuuksista 2005/566
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 2009/298
- Laki yksityisyyden suojasta työelämässä 759/2004
- EU parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelystä (tulee voimaan 2018)

Kuten tuossa direktiivissäkin on mainittu, järjestelmän tietoturva koostuu monesta eri asiasta, joiden kaikkien on syytä olla kunnossa, kun asiakkaiden tietoja käsitellään.

Tietoturvan eri osa-alueet VAT-käyttäjillä

Palvelimen tietoturva

VAT ohjelmisto on asennettu HermanIT:n palvelin saliin joka fyysisesti sijaitsee Kajaanissa Renforsin rannassa olevassa rakennuksessa. Seuraavassa tiivistetysti ominaisuudet:

- Konesali on suunniteltu DC Design IBM Level 3+ mukaan eli on **TIER 3+**
- Sali vastaa vaatimuksiltaan **VAHTI 2 – 3** eli asettuu tuohon väliin; tiukempi vaatimus ei täyty, koska sali on maanpinnalla olevassa hallissa
- ISO/IEC 27001:2013 sertifioidut käytänteet
- Palvelimen valvonta on 24/7 ja tietokannoista otetaan säännöllisesti varmistukset.
- Lisää tietoa on löydettävissä osoitteesta http://www.hermanit.fi/?lang=fi kohdasta Data Center Palvelut.

Tietoliikenteen tietoturva

VAT käyttäjät käyttävät suojattua virallista ssl –suojausta tietoliikenteessä joten työaseman ja palvelimen välinen liikenne on suojattu.

Ohjelmiston tietoturva

Järjestelmään kirjautuminen on kaksivaiheinen. Ensimmäisessä vaiheessa kirjaudutaan organisaation tietokantaan. Tämä kirjautuminen on suojattu sekä salasanalla, että reCaptha- toiminnolla. Organisaatioon kirjautumisen jälkeen käyttäjä kirjautuu omalla henkilökohtaisella tunnuksellaan ja salasanallaan järjestelmään. Virhekirjautuminen missä tahansa vaiheessa palauttaa kirjautumisen ensimmäisen vaiheen alkuun.

VAT on toteutettu, siten että järjestelmään ei voida kirjoittaa tai tuoda ohjelmakoodia ulkopuolelta. Kaikki ulkopuolelta tuotava aineisto on oltava pdf –muodossa.

Ohjelmisto pitää yllä lokitiedostoa kaikista asiakkaan henkilötietoihin, kuntoutussuunnitelman tietoihin ja arviointituloksiin kohdistuneista katseluista, päivityksistä ja tulostuksista. Loki voidaan tulostaa pääkäyttäjän (admin) käyttöoikeuksilla. Tulostus voidaan ottaa siten, että tarkastellaan asiakkaan tietojen katselu, tai siten, että tarkastellaan sitä kenen tietoja yksittäinen valmentaja on tarkastellut.

Asiakas voidaan poistaa järjestelmästä joko yksittäin, tai siten, että valitaan päivämäärä jota vanhemmat asiakkaat poistetaan. Asiakkaan poistamisen yhteydessä poistuvat kaikki asiakastiedot lukuun ottamatta niitä tietoja (pdf) jotka on siirretty erilliseen arkistoon. Nämä tiedot voidaan poistaa arkistosta yksittäin pääkäyttäjän (admin) käyttöoikeuksilla. Asiakkaan arviointitulokset eivät poistu poiston yhteydessä, mutta järjestelmän antaman asiakastunnuksen tilalle kirjoitetaan poiston yhteydessä xxxxxx, joten mahdollisuus yksittäisen asiakkaan arviointitietojen kohdentaminen henkilöön ei poiston jälkeen ole mahdollista.

Käyttäjä

Jokaisen organisaation tiedot ovat omassa tietokannassaan ja käyttäjä ei pääse muuhun kuin oman organisaationsa tietoihin. Käyttäjien käyttöoikeudet on rajattu siten, että työvalmentajan käyttöoikeuksilla päästään vain niiden asiakkaiden tietoihin jossa voimassa olevan tai viimeisen päättyneen valmennusjakson tietoihin ao. työvalmentaja on merkitty valmentajaksi. Yksilövalmentajilla on pääsy oman organisaationsa kaikkien asiakkaiden tietoihin.

Kun valmentajan työsuhde organisaatioon on päättynyt, voidaan valmentajan käyttöoikeus pääkäyttäjän toimesta merkitä Ei aktiiviseksi, jolloin järjestelmä estää ao. käyttöoikeuden käytön. Valmentaja voidaan poistaa järjestelmästä kokonaan sen jälkeen kun kaikki ne asiakkaat, joille hän on ollut valmentajana, on poistettu.

Organisaation tulee huolehtia käytettävien työasemien asianmukaisesta suojauksesta. Asiattoman käytön estämiseksi selaimen tietoturva asetukset tulee asettaa siten että VAT:sta poistuttaessa historiatiedot poistetaan. Samoin käytettäviä salasanoja ei tule tallettaa selaimen muistiin.