Tampereen teknillisen yliopiston tietotilinpäätös

1 Johdanto

Yliopiston toiminta perustuu tietoon. Tietoa kerätään, tallennetaan, jaetaan, tuotetaan, jalostetaan ja arkistoidaan. Yliopistotoiminta ja yliopistoissa tapahtuva tietojenkäsittely perustuu lakeihin ja asetuksiin. Tietotilinpäätöksessä esitetään yliopiston tietojenkäsittelyn pääperiaatteet, tietovarannot ja suojausperiaatteet.

Tampereen teknillisen yliopiston lakisääteiset perustehtävät ovat:

- tutkimus,
- koulutus ja
- yhteiskunnallinen vaikuttaminen.

Yliopiston tehtävänä on edistää vapaata tutkimusta sekä tieteellistä ja taiteellista sivistystä, antaa tutkimukseen perustuvaa ylintä opetusta sekä kasvattaa opiskelijoita palvelemaan isänmaata ja ihmiskuntaa. Tehtäviään hoitaessaan yliopiston tulee edistää elinikäistä oppimista, toimia vuorovaikutuksessa muun yhteiskunnan kanssa sekä edistää tutkimustulosten ja taiteellisen toiminnan yhteiskunnallista vaikuttavuutta.

Yliopiston tulee järjestää toimintansa siten, että tutkimuksessa, taiteellisessa toiminnassa, koulutuksessa ja opetuksessa varmistetaan korkea kansainvälinen taso eettisiä periaatteita ja hyvää tieteellistä käytäntöä noudattaen.

Yliopiston tietojenkäsittely koskettaa laajaa yhteisöä. Tutkinto-opiskelijoita on noin 8 000 ja henkilöstöä noin 1600.

Tampereen teknillinen yliopisto (TTY), Tampereen yliopisto (TaY) ja Tampereen ammattikorkeakoulu (TAMK) ovat luomassa yhdessä uudenlaista korkeakouluyhteisöä, joka rakentuu nykyisten TTY:n ja TaY:n muodostamasta säätiöyliopistosta sekä autonomisesta ammattikorkeakoulusta. Muutosorganisaatiota kutsutaan nimellä Tampere3.

Uuden korkeakouluyhteisön toiminta käynnistyy vuoden 2019 alussa. Parhaillaan on menossa kartoitukset eri tietojärjestelmistä ja niiden yhteensovittamisesta sekä entisten järjestelmien tietojen siirtämisprosesseista uusiin yhteisiin järjestelmiin tietoturva ja tietosuoja huomioiden. Uudessa korkeakouluyhteisössä tulee olemaan opiskelijoita n. 35 000 ja henkilöstöä n. 5 000.

2 Lainsäädäntö

2.1 Lainsäädännön viitekehys

Yliopiston tietojärjestelmiin tallennetaan vuosittain merkittävä määrä uutta tietoa. Tästä tiedosta suuri osa on henkilötietoja, eli tietoja, joiden avulla yksittäinen henkilö on tunnistettavissa.

Yliopiston tavoitteena on kaikessa toiminnassa käsitellä henkilötietoja vastuullisesti ja turvallisesti. Yliopiston henkilötietojen käsittelyä ohjaavat useat kansalliset ja kansainväliset säädökset.

Tietotilinpäätöksen laatimishetkellä henkilötietojen käsittelyn lainsäädännöllinen viitekehys perustuu EU:n henkilötietodirektiiviin (Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta, henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta) sekä vuonna 1999 voimaan tulleeseen kansalliseen henkilötietolakiin (523/1999, ”HeTiL”), jolla Suomen lainsäädäntö on saatettu vastaamaan henkilötietodirektiiviä. Tämän vuoksi alla muun muassa rekisterinpitäjän vastuista ja rekisteröidyn oikeuksista esitetty perustuu vielä henkilötietolain sääntelyyn.

Yliopisto noudattaa lisäksi toimintaansa koskevan erityislainsäädännön määräyksiä. Yliopiston toimintaa ja tietojen käsittelyä yliopistossa ohjaavat muun muassa seuraavat kansalliset lait:

- Perustuslaki (731/1999)
- Yliopistolaki (558/2009)
- Hallintolaki (434/2003)
- Julkisuuslaki (621/1999)
- Henkilötietolaki (523/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Tietoyhteiskuntakaari (917/2014)

Lainsäädännön lisäksi yliopiston tiedonkäsittelyä ohjaavat useat alemman tasoiset säädökset, valtionhallinnon ohjeet sekä yliopistotason politiikat ja ohjeet. TTY on julkaissut Intranetissä henkilöstön ja opiskelijoiden tiedoksi seuraavat tietoturvaan liittyvät säännöt ja ohjeet:

Tietosuojapolitiikka

- Tietosuojan yleisohje
- Tietoturvapolitiikka
- Tietoturvapolitiikan määritelmät
- Tietoturvavastuut
- Tietotekniikkapalvelujen käyttösäännöt
- Tietotekniikkapalvelujen ylläpitosäännöt
- Tietotekniikkarikkomusten seuraamuskäytännöt
- Tietotekniikkarikkomusten seuraamusasteikko
- Sähköpostisäännöt
- Sähköpostin suodatus
- Sähköpostin hakeminen ja avaaminen
- Keskeinen lainsäädäntö

Lisäksi sisäisiä kohdennettuja ohjeita on järjestelmien ylläpitäjille, tietojen käsittelijöille ja muille erityisille kohdennetuille tarpeille. Yliopiston ohjeistusta tarkastellaan ja päivitetään säännöllisesti.

Yliopisto on lisäksi vuoden 2017 aikana toteuttanut koko yliopistoyhteisön henkilöstöä koskevan pakollisen tietosuoja- ja tietoturvakoulutuksen sekä järjestänyt henkilöstön ydinryhmille tietosuoja-asetuksen voimaantuloon ja soveltamiseen valmistavaa koulutusta.

EU:n yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, ”tietosuoja-asetus”) astui voimaan 27.4.2016. Tietosuoja-asetuksella kumotaan henkilötietodirektiivi. Tietosuoja-

asetusta ryhdytään soveltamaan 25.5.2018. Tietosuoja-asetus on kansallisesti suoraan sovellettavaa lainsäädäntöä. Tietosuoja-asetusta täydennetään kansallisella tietosuojalailla.

Tietotilinpäätöstä laadittaessa tietosuoja-asetuksen tulkinta on vielä vakiintumatonta ja asetuksen vaikutukset kansalliseen lainsäädäntöön avoimia. Yliopisto seuraa lainsäädännön kehittymistä ja valmistautuu uusien vaatimusten täytäntöönpanoon toiminnassaan. Yliopisto odottaa EU:n tietosuojatyöryhmän (WP 29) sekä kansallisen tietosuojaviranomaisen (www.tietosuoja.fi) antamia ohjeita ja tulkintoja tietosuoja-asetuksen soveltamisesta. Tietotilinpäätöksen laatiminen on osa yliopiston valmistautumista tietosuoja-asetuksen soveltamiseen.

2.2 Rekisterinpitäjän vastuut ja rekisteröidyn oikeudet

Asianmukainen tietojenkäsittely edellyttää, että yliopisto rekisterinpitäjänä huolehtii tärkeimpien tietosuojaperiaatteiden, kuten henkilötietolain 2 luvussa ilmaistujen suunnittelu-, tarpeellisuus- ja huolellisuusvelvoitteiden sekä henkilötietojen suojaamisvelvoitteiden asianmukaisesta toteutumisesta tietojen käsittelyssä, ja varmistaa rekisteröityjen oikeuksien asianmukaisen toteuttamisen.

Henkilötietolain nojalla rekisteröidyllä on seuraavat oikeudet:

- **Oikeus saada informaatiota** rekisteröidyn henkilötietojen käsittelystä, kuten rekisterinpitäjästä ja tämän edustajasta, käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan. Rekisteröidyllä on samoin oikeus saada ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi.

- **Oikeus tarkastaa tietonsa**. Kaikilla rekisteröidyillä on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu, tai ettei rekisterissä ole häntä koskevia tietoja. Yliopisto voi pyytää rekisteröityä täsmentämään, mitä tietoja pyyntö koskee, ja pyytää rekisteröityä ilmoittamaan muut tietojen etsimiseksi tarpeelliset seikat.

- **Oikeus vaatia virheellisten tietojen korjaamista.** Rekisterinpitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Rekisteröity voi ilmoittaa yliopistolle omissa tiedoissaan havaitsemistaan virheistä.

- **Oikeus kieltää tietojen käsittely.** Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten.

EU:n yleisen tietosuoja-asetuksen soveltaminen vahvistaa edelleen rekisteröidyn oikeutta hallita omien henkilötietojensa käsittelyä.

2.3 Rekisteröidyn oikeuksien toteuttaminen

Yliopiston tavoite on tehdä henkilötietojen hallinnasta rekisteröidyilleen mahdollisimman helppoa. Yliopiston opiskelijoilla, henkilöstöllä ja vierailijoilla on mahdollisuus tarkastaa perustietonsa seuraavien itsepalvelujärjestelmien kautta (käyttö vaatii kirjautumisen):

Henkilöstö ja vierailijat:

- HR SUITE – henkilöstötietojärjestelmä
  http://www.tut.fi/hrsuite

Opiskelijat ja vierailijat:

- POP – Personoitu opiskelijaportaali
  http://www.tut.fi/pop

Yliopiston intranet-sivulla ylläpidetään lisäksi päivitettävää listaa muista yliopiston itsepalvelujärjestelmistä, joista yliopistoyhteisön jäsenet voivat omilla käyttäjätunnuksillaan tarkistaa henkilötietonsa.

Muut kuin itsepalvelujärjestelmien kautta toteutettavissa olevat tarkastuspyynnöt ja muut rekisteröidyn oikeuksien käyttämistä koskevat pyynnöt tehdään keskitetysti yliopiston IT-Helpdeskiin henkilökohtaisen käynnin yhteydessä. Pyynnön esittäjän henkilöllisyys tarkistetaan pyyntöä esitettäessä ja ennen tietojen antamista, jotta yliopisto voi varmistua siitä, että rekisteröidyn henkilötiedot luovutetaan ainoastaan rekisteröidylle itselleen tai muulle tietojen vastaanottamiseen oikeutetulle henkilölle (kuten rekisteröidyn valtuuttamalle vastaanottajalle). Henkilöllisyys voidaan todistaa valokuvalla varustetulla virallisella henkilöllisyystodistuksella, joksi hyväksytään EU-ajokortti, passi tai poliisiviranomaisen antama henkilökortti.

Mikäli yliopisto kieltäytyy ryhtymästä toimiin rekisteröidyn oikeuksien käyttämistä koskevan pyynnön perusteella, yliopisto antaa rekisteröidylle tästä kirjallisen ilmoituksen. Rekisteröidyllä on oikeus saattaa asia toimivaltaisen viranomaisen ratkaistavaksi (Tietosuojavaltuutetun toimisto, PL 315, 00181 Helsinki).

2.4 Rekisteröidyn informointi

Yliopisto informoi rekisteröityjä suorittamastaan tietojenkäsittelystä. Yleisölle ja yliopiston rekisteröidyille tarjotaan yleiskuva yliopiston harjoittamasta tietojenkäsittelystä ja tietojenkäsittelyn käytännöistä yliopiston julkisilla internetsivuilla (http://www.tut.fi/fi/tietoa-yliopistosta/yksityisyys/). Yliopiston tietotilinpäätös julkaistaan samalla sivulla.

Yliopiston rekistereitä koskevat rekisteriselosteet (ja tietojärjestelmäselosteet) on asetettu keskitetysti saataville yliopiston intranet-palveluun (https://tutfi.sharepoint.com/sites/intra-fi/organisaatio-ja-kehittaminen/toiminnan-saannot-ohjeet/rekisteriselosteet).
Tietoturvasyiden vuoksi rekisteriselosteiden ja tietojärjestelmäselosteiden tarkastelu edellyttää pääasiassa kirjatumista. Ulkoisille sidosryhmille (kuten uutiskirjeiden tilaajille tai asiakasrekisterin rekisteröidyille) kohdennetut tietosuojaselosteet tallennetaan kuitenkin pääsääntöisesti asiayhteyden mukaan yliopiston julkisille internet-sivuille. Yliopiston tietosuojaselosteista ilmenevät muun ohella kussakin rekisterissä käsiteltävät henkilötietoryhmät, käsittelyn tarkoitukset ja säännönmukaiset luovutukset.

Yliopiston tietosuojaselosteet tullaan korvaamaan EU:n yleisen tietosuoja-asetuksen soveltamisen myötä tietosuojailmoituksilla, joilla yliopisto kuvaa entistä laajemmin suorittamaansa henkilötietojen käsittelyä.

3 Tietovarannot ja tietoarkkitehtuuri

Yliopistolla on määriteltyjä tietojärjestelmiä päätehtävien suorittamiseen. Näitä ovat opintojen suorittamiseen, tutkimukseen sekä hallintoon käytettävät tietojärjestelmät. Li-säksi käytössä on erillisiä tietojärjestelmiä, joihin perustiedot yleensä saadaan edellä mainitusta järjestelmistä. Tietojen tallentamista useaan eri paikkaan vältetään, tavoitteena on käyttää aina päätietojärjestelmiä. Tällä vältetään tiedon turhaa kertymistä eri paikkoihin ja vähennetään tietovuotoriskien vaaraa.

Yliopistolla on käytössä yli 100 tietojärjestelmää, joista 73 muodostaa henkilörekisterin tai osarekisterin. Keskeisimmät tietojärjestelmien tukemat palvelut ja toiminnot ovat:

- Opiskelijapalvelut
- Henkilöstöpalvelut
- Sidosryhmäsuhteet
- Viestintä
- Kirjasto- ja tietopalvelut
- Tutkimus
- IT-palvelut, mm. tunnushallinta, identiteetin- ja pääsynhallinta (käyttövaltuushallinta)
- Talouspalvelut (tietovarasto)

Opintotietojärjestelmät ovat yliopistolle välttämätön toiminnan suunnittelun, toteutuksen, arvioinnin ja seurannan väline. Järjestelmään rekisteröidään vain opetushallinnon tehtävän hoitamisen, toiminnan suunnittelun, toteutuksen, seurannan ja arvioinnin kannalta tarpeelliset tiedot. Opintotietojärjestelmiin saadaan tiedot mm. valtakunnallisesta opintopolku.fi järjestelmästä ja niitä siirretään tietyiltä osin valtakunnallisiin järjestelmiin, kuten VIRTA ja KELA.

Henkilöstötietojärjestelmän käyttötarkoitus on henkilökunnan työsuhdetietojen hallinta. Järjestelmällä on kytkös mm. palkan maksuun ja muihin työsuhteeseen liittyviin järjes-telmiin.

Tutkimuksen tietojärjestelmät mahdollistavat laadukkaan tutkimuksen ja tutkimustoiminnan kehittämisen.

Muut listatut järjestelmät tukevat yliopistolle yhteisten palvelujen toimintaa. Tällaisia ovat esimerkiksi IT-palveluiden ja talouden järjestelmät.

4 Tietojen käsittelyn pääperiaatteet

4.1 Henkilötietojen käsittelyn yleiset periaatteet ja käytännöt

Yliopisto on sitoutunut noudattamaan henkilötietojen käsittelyssään kulloinkin voimassa olevan tietosuojalainsäädännön vaatimuksia. Henkilötietolain voimassa ollessa yliopisto on ollut velvollinen noudattamaan henkilötietolain mukaisia henkilötietojen käsittelyn edellytyksiä ja periaatteita. Tietosuoja-asetuksen soveltamisen alkaessa astuessa yliopisto on rekisterinpitäjänä velvollinen noudattamaan tietosuoja-asetuksen velvoitteita ja huomioimaan kaikessa henkilötietojen käsittelyssään seuraavat periaatteet:

- **Lainmukaisuus, kohtuullisuus ja läpinäkyvyys:** Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

- **Käyttötarkoitussidonnaisuus:** Henkilötietoja on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.

- **Tietojen minimointi:** Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

- **Täsmällisyys:** Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä.

- **Säilytyksen rajoittaminen:** Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

- **Eheys ja luottamuksellisuus:** Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Henkilötietojen käsittelyn **sisäänrakennettu ja oletusarvoinen tietosuoja** edellyttää, että käsittelyn periaatteiden sisältö ja ulottuvuus arvioidaan tapauskohtaisesti ja jo siinä vaiheessa, kun henkilötietojen käsittelyä tai käsittelytavan muutosta ryhdytään suunnittelemaan. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittelylle on aina lakiin perustuva peruste. Tietojenkäsittelyn tarkoitus on määriteltävä jo ennen kuin tietoja ryhdytään käsittelemään.

Yliopiston suorittaman henkilötietojen käsittelyn periaatteet ja käytännöt on vahvistettu yliopiston Tietosuojapolitiikassa ja Tietosuojan yleisohjeessa. Yliopiston tietojenkäsittelykäytäntöä kuvataan tarkemmin myös yliopiston julkisilla internetsivuilla julkaistavassa päivitettävässä selosteessa.

4.2 Tietojen suojauksen periaatteet

Tietojen suojauksen osalta yliopisto noudattaa kaikessa käsittelytoiminnassaan vähintään seuraavia periaatteita:

- **Tietojen minimointi:** Yliopisto kerää ja käsittelee ainoastaan niitä tietoja, jotka ovat tarpeen asianomaisen käsittelytarpeen toteuttamiseksi.

- **Riskienhallinta, DPIA:** Yliopistossa tehdään riskienhallintaa ja riskien arviointia osana normaalia linjatyötä.

- **Käyttövaltuudet:** Yliopiston henkilöstön käyttöoikeudet muun muassa verkkolevykansioihin on rajattu niin, että pääsy henkilötietoihin on ainoastaan niillä henkilöillä, joilla on työhön perustuva tarve henkilötietojen käsittelyyn.

- **Henkilötiedon anonymisointi tai pseudonymisointi:** Henkilötiedot tehdään tunnisteettomiksi, kun rekisteröidyn tunnistaminen ei ole enää tarpeen käsittelytarkoituksen. Tällainen tarve voi olla esim. tilastointi.

- **Tietosuojatyön sisältyminen yliopiston toimintaan:** Tietosuojatyö on sisällytetty yliopiston toimintaan kiinteänä osana tietoturvatyötä ja yleishallintoa. Yliopisto on varautunut jatkuvuuden turvaamiseen ja poikkeustilanteisiin reagoimiseen suunnittelemalla ja vahvistamalla prosessit ja toimenpiteet. Jatkuvuudenhallinnan ja poikkeustilanteiden prosessit sekä toimenpiteet ovat kartoitetut ja käytössä.

5 Tietojenkäsittelyn tietosuojan ja -turvan toteutuminen sekä seuranta

5.1 Tietosuojatyön tarkoitus

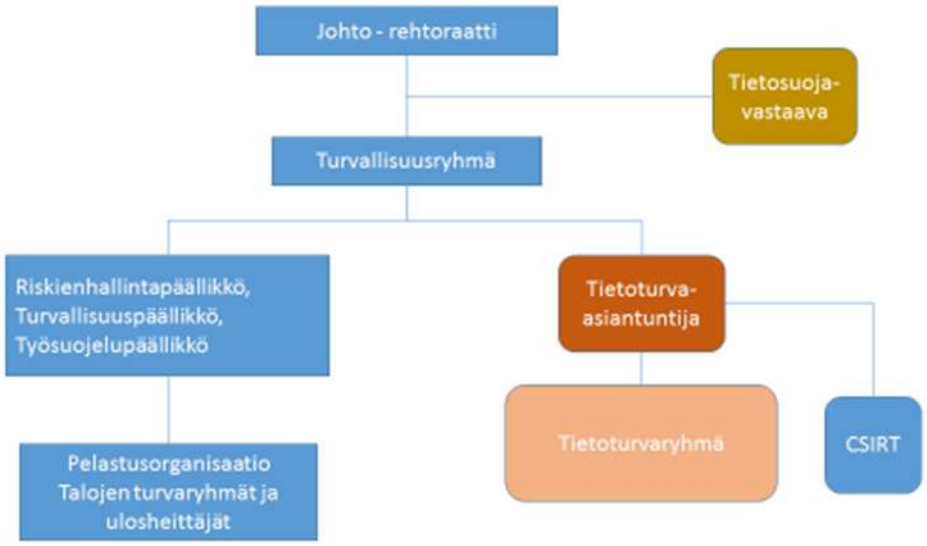
Tietosuojatyön ja tietoturvallisuuden päämääränä on turvata yliopiston toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaalin toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin tai sitä haittaaviin uhkatilanteisiin ja niistä toipumiseen. Lähtökohtana on, että yliopiston tietovarannot, tietojärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisin, teknisin ja muiden toimenpiteiden avulla. Yliopiston tietoverkossa toimivien tietoturva- ja tietosuojatietämyksen lisäämisen päämääränä on mahdollisimman turvallinen ja luotettava toimintaympäristö.

5.2 Tietosuoja- ja tietoturvatyön organisointi/organisaatio

Tietosuojatyö on osa kaikkea yliopiston toimintaa. Rekisterien omistajat vastaavat omien rekistereidensä osalta tietosuojasta ja tietosuojatyötä koordinoimaan on perustettu tietosuojaryhmä. Ryhmä koostuu tietosuojaan liittyvistä keskeisistä toimijoista sekä teknisistä asiantuntijoista. Ryhmän päävastuulla on valmistaa organisaatio tietosuo-ja-asetuksen vaatimuksiin 25.5.2018 mennessä. Tietosuojatyö on olennainen osa tieto-turvallisuutta ja tietoturva-asiantuntija osallistuu tietosuojaryhmän toimintaan.

Tampereen teknillisen yliopiston tietoturvaorganisaatio muodostuu tietoturvaryhmästä sekä poikkeamahallintaryhmästä (Computer Security Incident Response Team, CSIRT).
Ryhmien toimintaa ja tietoturvan kehittämistä koordinoi tietoturva-asiantuntija. Tietoturva-asiantuntijan rooli on osa strategista johtamista ja hän raportoi suoraan hallintojohtajalle ja tietohallintojohtajalle.

Turvallisuus ja tietoturva- ja tietosuoja organisaatio:



5.3 Tietoturvallisuus

Tietoturvallisuuden toteuttamisen perustana on yliopiston tietoturvapolitiikka sekä politiikkaan liittyvä tietoturvavastuut-dokumentti. Kokonaisvastuu tietoturvan toteutumisesta on yliopiston johdolla. Tietoturvavastuut-dokumentissa on kuvattu organisaation eri toimintojen vastuut tietoturvan toteuttamisessa.

Tiedonkäsittelyn teknisestä tietoturvan toteuttamisesta vastaa IT-palvelut. Poikkeamahallintaryhmällä on kirjallisesti myönnetty oikeus merkittävää riskiä aiheuttavissa tieto-turvaa ja tietosuojaa uhkaavissa tilanteessa päättää yksittäisistä turvaamistoimenpiteistä. Muilta osin turvaamistoimenpiteistä vastaa tietohallintojohtaja. Toimista informoidaan viivytyksettä asianosaisia.

5.4 Tiedottaminen

Tietoturva-asiantuntija sekä IT-palvelut tiedottavat tietoturva-asioista yliopiston tietoverkossa toimiville. Tietoturva-asiantuntija kehittää ja ylläpitää tietoturvaan liittyviä ohjeita ja tiedottaa sisäisesti akuuteista tietoturvauhista tarkoituksenmukaisin keinoin. Ulkoisesta tietoturvatiedotuksesta vastaa tietohallintojohtaja.

5.5. Seuranta

Tietoturvan toteutumista seurataan mm. säännöllisten seurantaraporttien avulla sekä automatisoitujen teknisten menetelmien avulla. Johdolle raportoidaan säännöllisesti. Henkilökunnalle ja johdolle valmistellaan vuosittain turvallisuusraportti, jossa esitetään oleellisimmat tietoturvahuomiot sekä poikkeamatilastot. Tietosuoja on osa tietoturvaraportointia.

5.6 Henkilökunnan koulutus

Henkilökunnalle ja opiskelijoille on pakollinen tietoturvakurssi, joka on suoritettava tai käyttäjätunnus sulkeutuu. Henkilökunnalle järjestetään tietoturva- ja tietosuojakoulutusta. Tarvittaessa järjestetään tietoiskuja ja tiedotteita ajankohtaisista aiheista. Myös kohdennettua koulutusta järjestetään toiminnoittain tarpeen mukaan.

5.7 Tietoturvan tekninen toteutuminen

Yliopiston verkko ja palvelut on suojattu teknisin ja hallinnollisin järjestelyin ja keinoin. Palvelimissa ja työasemissa käytetään riskiarvion mukaan kovennuksia, laitekohtaisia palomuureja, pääsyrajoitteita sekä muita teknisiä suojauksia, kuten haittaohjelmien tunnistusta sekä haittaohjelmien toiminnan estämistä. Laite- ja palvelintilat ovat suojattuja ja päästy tiloihin on vain määrätyillä henkilöillä. Tiedon saatavuus on varmistettu teknisin varautumismenettelyin. Kriittisiä palveluja valvotaan automatisoidusti.

Verkko on jaettu erillisiin osiin riippuen käyttötarkoituksesta. Verkkoalueet on suojattu palomuureilla. Verkon aktiivilaitteisiin ja kriittisimpiin palvelimiin on rajoitettu pääsy ylläpidolle vain tietyistä verkkoalueista. Tietosuojan ja –turvan kannalta riskialttiiseen tutkimukseen on olemassa erillinen tutkimusverkko, jossa riskit ja tarve ovat mielekkäästi hallittavissa.

Tiedon luottamuksellisuus on suojattu liikenteen, laitteiden ja tiedostojen salausmenetelmillä sekä käyttäjätunnuksi. Kirjautuminen palvelimille ja työasemille tapahtuu henkilökohtaisella tunnuksella roolipohjaisesti. Yleisiä yhteiskäyttötunnuksia ei ole käytössä muualla kuin poikkeuksellisissa erikoistapauksissa riskiarvioin kautta. Ylläpitotoimet tehdään normaalista käyttäjätunnuksesta poikkeavalla henkilökohtaisella erillisellä pääkäyttäjätunnuksella. Oletussalasanoja ei käytetä missään laitteessa tai palvelussa.

Järjestelmät, palvelimet ja aktiivilaitteet keräävät lokitietoa ja palveluita monitoroidaan käyttövarmuuden, tietoturvan ja tietosuojan varmistamiseksi.

5.8 Tietosuoja

Tietosuoja on sisällytetty tietoturvan toteutukseen. Esimerkiksi pakollinen tietoturvakoulutus sisältää tietosuojaan liittyvää materiaalia. Tietoturva toteuttaa myös tietosuojan tekniset suojausmenettelyt. Tietosuojan toteutumista seurataan sekä tietoturvan tarjoamin teknisin menetelmin että tietosuojaan kohdistetuin hallinnollisin menetelmin. Tiedoille on määrätty elinkaari elinkaarimallin ja arkistonmuodostussuunnitelman mukaisesti. Tiedoilla on omistaja, joka vastaa vaatimusten täyttämisestä.

6 Riskiperusteinen lähestymistapa ja kehittämistoimenpiteet

6.1 Riskiperusteinen lähestymistapa

Tulevan tietosuoja-asetuksen mukaan suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Asetuksen riskiperustaisuus on otettu TTY:llä kaiken tietojenkäsittelyn pohjaksi vuonna 2017. Tietosuoja-asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja. Erityisesti on kiinnitettävä huomiota,

mikäli henkilötietojen käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen.

Rekisterinpitäjän eli yliopiston on tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä, jotta voidaan osoittaa, että yliopisto toteuttaa asetukseen sisäänrakennettua ja oletusarvoista tietosuojaa ja asetuksessa säädettyjä velvollisuuksia. Tämän jälkeen tarpeelliset toimenpiteet suhteutetaan kulloinkin henkilötietojen käsittelyyn liittyvän riskin mukaisesti ja vältetään matalariskisen toiminnan ylisääntelyä.

Yliopistossa tunnistettiin tietosuojaprojektin aikana 73 järjestelmää ja tietovarantoa, joissa käsitellään henkilötietoa. Tiedot voidaan jakaa hallinnon toteuttamisen edellyttämiin tietoihin ja tutkimuksessa syntyvään tietoon.

Haastetta tietosuojatyölle yliopistossa aiheuttaa Tampere3 prosessi, jonka seurauksena suuri osa tietojärjestelmistä tulee vaihtumaan lähiaikoina. Tiettyjen järjestelmien osalta tullaankin keskittymään siihen, että riittävän nopealla aikataululla suljettavia järjestelmiä ei enää kehitetä, vaan keskitytään varmistamaan uusien Tampere3:n myötä käyttöön otettavien järjestelmien asetuksenmukaisuus.

Henkilötietojen käsittely muuttuu korkean riskin tietojenkäsittelyksi, mikäli kaksi seuraavista täyttyy:

- Sensitiivinen / arkaluontoinen henkilötieto
- Ihmismassojen henkilötietojen käsittely
- Henkilötietovaraintojen yhdistäminen tai täsmäyttäminen
- Heikon tai haavoittuvan ihmisen henkilötietojen käsittely
- Teknologisten ja organisatoristen ratkaisujen soveltaminen tai luova käyttö
- Tiedon siirtäminen EU:n ulkopuolelle
- Henkilötietojenkäsittely, jossa tarkoituksena on päättää tai estää palveluiden, sopimuksen tai oikeuksien käyttäminen (pääsykontrolli, hyväksyntätilanne)
- Henkilön arviointi, profilointi tai pisteytys
- Automatisoitu päätöksen teko tai vaikutus henkilön suhteen
- Järjestelmällinen valvonta ja kontrolli kohdistuvat henkilöön

6.2 Riskiarviot ja niiden tulokset

Korkean riskin tietovarannot

Tehdyn riskianalyysin perusteella korkean riskin järjestelmiksi tunnistettiin Henkilöstötietojärjestelmä ja Opiskelijatietojärjestelmä. Näissä järjestelmissä säilytetään ja käsitellään paljon henkilötietoja, joista osa on myös luonteeltaan sensitiivisiä. Järjestelmät ovat suuren riskin järjestelmiä sekä tietomäärien että tiedon laadun suhteen.

Muita korkean riskin hallinnollisia järjestelmiä on Identiteetin ja pääsynhallinta -järjestelmä, jossa tietojenkäsittely on osittain automaattista, sekä yliopiston tuotannon-ohjauksen tukena toimiva Tietovarasto.

Korkean riskin tietojärjestelmien hallinta toteutetaan pääsy vain määrätyillä tunnuksilla ja rajoitetuista verkkoalueista. Tapahtumista ja kirjautumisista kerätään näissä järjestelmissä

yksityiskohtaisempaa lokia. Pääkäyttäjien toimenpiteiden lokitukseen on kiinnitetty erityistä huomiota ja havaitut kehittämistarpeet ovat jo muutosprosessissa.

Kohtalaisen riskin tietovarannot

Kohtalaisen riskin järjestelmiä yliopistolta löytyy useita. Näihin tietojärjestelmiin on rajatut käyttöoikeudet, eikä niissä ole sensitiivisiä tietoja. Useimmat näistä järjestelmistä ovat elinkaarensa päässä ja poistumassa Tampere3:n myötä.

Matalan riskin järjestelmät ja henkilölistaukset

Pääsääntöisesti tietoja tulee käsitellä järjestelmässä, joka on tietojen pääasiallinen sijaintipaikka. Yliopistolla käytetään perustyöskentelyyn listauksia, joissa on listattu työntekijöitä tai opiskelijoita johonkin tiettyyn ryhmään tai tarpeeseen perustuen. Tiedot on tallennettu yleensä taulukkolaskentaohjelmaan tietyn henkilön päivittäiseen työskentelytarpeeseen. Tiedostoja säilytetään sisäverkon suojatulla levyllä tai lyhyitä yksittäisiä tarpeita varten henkilökohtaisella työasemalla, tai muualla yliopiston ohjeistamassa tallennuspaikassa asianmukaisesti suojattuina. Tällaiset erilliset työversiot katsotaan normaaliin työhön ja työtarpeeseen välttämättömäksi ja niistä ei tehdä erikseen rekisteriselosteita. Suuri osa tiedoista luetaan kuuluvaksi päärekistereihin. Näin vältetään ylisääntelyä. Työversioihin ei saa tallentaa erityisiä (ent. ”arkaluontoisia”) henkilötietoja.

Listausten ei koeta synnyttävän suurta riskiä, sillä niissä olevat tiedot ovat yleensä osajoukko henkilöstöstä julkisen henkilöhaun kautta saatavista tiedoista ja pakollisen koulutuksen kautta on korostettu käsiteltävän henkilötiedon minimointia. Henkilökohtaiset mobiilityöasemat pääsääntöisesti salataan, jolla on pyritty minimoimaan varkauden ja katoamisen aiheuttama tietovuotoriski.

Tutkimusdata

Tutkimusaineistoista lähetettiin tutkijoille kysely syksyllä 2017. Vastauksia saatiin 87. Saatu aineisto käytiin läpi ja tunnistettiin henkilötietoja sisältäviä aineistoja, poistettiin tunnistettuja tietosuojariskejä ja todettiin tarve jatko-ohjeistukselle. TTY:n Kirjasto neuvoo jatkossa tutkimusdatan käsittelystä ja hallinnasta.

6.3 Kehittämistoimenpiteet

Syksyn 2017 ja kevään 2018 aikana ylipisto on kyennyt madaltamaan yliopiston henkilötietojenkäsittelyyn liittyvää riskitasoa toimenpiteiden ja tietosuojaprojektiryhmälle kohdennettujen koulutusten avulla. Yliopiston tietojärjestelmistä on tehty tai päivitetty nykytila-analyysit ja tietovirtakuvaukset. Tämän lisäksi tehtiin tutkimusaineistokartoitus ja kohdennetulle henkilöstölle annettiin koulutusta sekä luotiin ohjeistusta. Nykytilakartoitusten perusteella suurimmat sensitiivistä tietoa sisältävät järjestelmät ja tietovarannot on tunnistettu.

Erilaisten ulkoisten pilvipalveluiden ja sovellusten käytön lisääntyessä käsittelijöille, tiedon omistajille sekä rekisteröidyille laaditaan ohjeistus siitä, miten ja missä tietoa voi käsitellä, jotta tietosuoja ja tietoturva toteutuu mahdollisimman hyvin.

Kevään 2018 aikana kehitetään tietosuojaprosesseja. Tietopyynnöille järjestetään yhden kontaktin yhteydenottopiste, ja näin helpotetaan rekisteröidyn oikeuksia saada tietopyyntö

hoidettua yhdenmukaisesti riippumatta organisaatiosta tai kysyjästä. Tietosuojapoikkemien käsittelyyn luodaan tekniset ja hallinnolliset menettelyt.

Kevään 2018 aikana toteutetaan laaja tietosuojakoulutus sekä päätetään miten tietosuoja tulee jatkossa integroitumaan henkilöstökoulutuksiin.

Syksyllä 2018 tehdään ulkopuolinen auditointi, jolla halutaan varmistaa, että henkilötietojenkäsittely on kattavaa. Auditoinnin tuotoksena saatava auditointiraportti toimii osana osoittamisvelvoitteen täyttämistä.

Tietotilinpäätös tai tiivistelmä tietotilinpäätöksestä julkaistaan jatkossa vuosittain.