VALTIOVARAINMINISTERIÖ

VAHTI

EU-tietosuojan kokonaisuudistus

VAHTI-raportti – 1/2016

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Valtioneuvoston hallintoyksikkö/Tietotuki- ja julkaisuyksikkö / Pirkko Ala-Marttila

ISSN 1798-0860 (pdf)
ISBN 978-952-251-778-4 (pdf)

Sisältö

1 Johdanto

Henkilötietojen käsittelyn merkitys on kasvanut jo pitkään tapahtuneen palveluiden ja tietojen sähköistämisen myötä. Digitalisaation johdosta henkilötietoja hyödynnetään entistä kattavammin, sillä data on uusien digitalisoitujen palveluiden polttoainetta. Tätä ruokkii jatkuva tarve tuottaa palveluita uudenlaisilla tuotantotavoilla (ns. virtualisoidut, jaetut kapasiteetti- ja pilvipalvelut), tarve ottaa käyttöön uudenlaisia päätelaitteita ja käyttötapoja (puhe- ja katseohjaus, virtuaali- ja lisätty todellisuus) sekä tarve tuottaa ja hyödyntää palveluita uudella tavalla (massadata, omadata sekä avoin data). Siirtyminen ICT-aikakaudesta palvelupohjaisempaan, asiakkaat paremmin huomioivaan digitaaliseen aikakauteen, jossa pääpaino on teknologian sijaan asiakaskokemus, asettaa suuria vaatimuksia myös henkilötietojen käsittelylle. Euroopan Unioni on myös tämän kehityksen tunnistanut. Sen johdosta tässä raportissa käsitellään lainsäädäntöuudistusta, joka päivittää henkilötietojen käsittelyyn liittyvät vaatimukset muuttuneen toimintaympäristön tasolle.

Tämän raportin on laatinut valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) asettama erillinen työryhmä. Raportin luonnosversion työryhmän käyttöön on laatinut Nixu Oyj:n tietosuojakonsultti Sanna Kuikka. Raportissa kuvataan tietosuoja-asetuksen keskeiset termit ja sisältö, rekisteröidyn oikeudet ja merkittävimmät rekisterinpitäjän vastuut. Lisäksi annetaan suosituksia toimenpiteistä, joiden avulla rekisterinpitäjät voivat ryhtyä toteuttamaan tietosuojavastuita toiminnassaan kahden vuoden siirtymäajan kuluessa.

Raportti antaa organisaatioille tietoa ja suosituksia asetuskokonaisuuden tuomista muutoksista siten, että organisaatio voi käynnistää niihin valmistautumisen mahdollisimman aikaisessa vaiheessa. Jokaisen henkilötietoja käsittelevän viranomaisen, yrityksen ja organisaation tulisi tarkastella miten tuleva lainsäädäntöuudistus on huomioitava jo nyt käynnissä olevissa henkilötietojen käsittelyä sisältävissä hankkeissa ja ennen kuin hankkeet päättyvät. Samassa yhteydessä on suunniteltava miten lainsäädännön edellyttämät vaatimukset toteutuvat siirtymäkauden jälkeen myös silloin toiminnassa olevissa palveluissa ja prosesseissa, joissa henkilötietoja käsitellään.

Raportti pohjautuu toukokuun 2016 tilanteeseen. Raporttia tullaan päivittämään vuosien 2016–2017 aikana, kun tarkempia yksityiskohtia ja esimerkiksi lainsäädäntöön liittyvää kansallista liikkumavaraa on saatu tarkennettua. Tässä versiossa ei vielä käsitellä kansallisen liikkumavaran käyttöä.

Tietosuoja-asetuksen soveltamisalan ulkopuolelle jääviä kokonaisuuksia, joita ovat esimerkiksi kansallinen turvallisuus, ei myöskään käsitellä tässä raportissa. Soveltamisalan ulkopuolista lainsäädäntöä ja niiden muutostarvetta selvitetään ja täsmennetään kansallisesti. Niihin liittyvät muutokset ja lisätiedot lisätään aikanaan tämän raportin päivitettyyn versioon.

Tämä raportti on hyväksytty VAHTI-johtoryhmän kokouksessa 3.5.2016. Tuorein versio sekä raportin tueksi laadittu Excel-työväline ovat ladattavissa www.vahtiohje.fi-sivustolta. Raportin tueksi järjestetään myös seminaareja eri kohderyhmille.

Toivomme palautetta tästä raportista ja tulevissa päivityksissä huomioitavista asioista sähköpostitse vahti@vm.fi tai kimmo.rousku@vm.fi.

2 Lainsäädännön taustaa

Euroopan Unionin (EU) tietosuojauudistuksella viitataan lainsäädäntöuudistukseen, johon kuuluvat yleinen tietosuoja-asetus[1] ja direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta[2]. Tietosuoja-asetus koskettaa sekä EU:ssa että sen ulkopuolella toimivia yrityksiä, jotka käsittelevät jäsenvaltioiden kansalaisten henkilötietoja. Direktiivi sen sijaan ohjaa EU:n viranomaisten henkilötietojen käsittelyä muun muassa rikosten tutkinnassa.

Tietosuoja-asetus korvaa direktiivin 95/46/EY sekä vuoden 2008 tietosuoja-alan puitepäätöksen 2008/977/YOS.

Euroopan komissio julkaisi ehdotuksen tietosuojan lainsäädäntöuudistuksesta tammikuussa 2012. Noin neljän vuoden jälkeen parlamentti, komissio ja neuvosto pääsivät sopuun asetuksen ja direktiivin sisällöstä joulukuussa 2015. Säädökset on julkaistu 4.5.2016, jolloin sekä asetus että direktiivi astuvat voimaan **25.5.2018** kahden vuoden siirtymäajan jälkeen.

2.1 Lainsäädäntöuudistuksen taustaa

Henkilötietojen käsittelyn laajuus on muuttunut paljon viime vuosien aikana. EU:n nykyinen, vielä voimassa oleva henkilötietodirektiivi on vuodelta 1995, jolloin henkilötietojen käsittely ja henkilötietojen hyödyntäminen liiketoiminnassa oli hyvin erilaista.

Teknologian kehittyminen esimerkiksi sosiaalista mediaa, pilvipalveluita ja sijaintitietoa hyödyntävissä palveluissa, entistä globaalimpi toimintaympäristö ja digitalisoituminen ovat lisänneet henkilötietojen käsittelyä sekä siten myös muuttaneet tietosuojatarpeen luonnetta. Myös osittainen tai täysimittainen ulkoistuskumppanien hyödyntäminen henkilötietojen käsittelyssä on huomattavasti lisääntynyt. Näin ollen myös eurooppalaisen tietosuojasääntelyn uudistaminen on ollut tarpeen. Tarve on ollut riskilähtöiseen ja teknologiariippumattomaan sääntelyyn, joka huomioi uudet teknologiat ja tiedonkeruumenetelmien riskit sekä velvoittaa mitoittamaan suojausmekanismit suhteutettuna käsittelyyn liittyvään riskiin. Toisaalta sääntelyn tulisi toimia myös digitaalisen liiketoiminnan mahdollistajana.

Direktiivi oikeudellisena välineenä asettaa tavoitteet, joihin kaikkien unionin jäsenvaltioiden on päästävä. Direktiivi on lainsäädäntöohje, jonka kukin jäsenvaltio toteuttaa omassa kansallisessa lainsäädännössään. Koska henkilötietojen käsittelyä ohjaa ennen tietosuoja-asetuksen voimaantuloa henkilötietodirektiivi, on kussakin jäsenvaltiossa kansallinen henkilötietojen käsittelyä koskeva lainsäädäntö. Näin ollen useassa EU:n jäsenvaltiossa toimiva rekisterinpitäjä on tähän asti joutunut selvittämään jokaisen maan tietosuojalainsäädännön sekä asioimaan erikseen jokaisen maan tietosuojaviranomaisen kanssa. Nyt julkaistu tietosuoja-asetus tulee harmonisoimaan tietosuojasääntelyn EU:ssa tasapuolisilla säännöksillä, jotka koskevat sekä EU:ssa että sen ulkopuolella toimivia rekisterinpitäjiä.

Asetus tuo rekisterinpitäjille uusia hallinnollisia tehtäviä, ja teknisten vaatimusten toteuttaminen voi myös aiheuttaa kustannuksia. Rekisterinpitäjän lisäksi asetus kohdistaa vaatimuksia myös suoraan henkilötietojen käsittelijälle.

Digitaalisten palvelujen yleistyessä myös palveluja hyödyntävien yksityishenkilöiden oikeudet tulee turvata, mikä on yksi kokonaisuuden keskeisimmistä ja laajavaikutteisimmista muutoksista.

Tietosuoja-asetusta tulee soveltaa yhdenmukaisesti kaikissa EU:n jäsenvaltioissa. Jotta tämä onnistuisi, on jäsenvaltioiden valvontaviranomaisten tehtävä yhteistyötä. Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) voi antaa asetuksen soveltamisesta sitovia päätöksiä, mikä tekee siitä keskeisen toimijan yhdenmukaisuuden varmistamisessa. Osaltaan asetuksen vaatimusten täytäntöönpanoa

[1] Euroopan parlamentin ja neuvoston asetus (eu) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
[2] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta

ohjaa myös tuntuva sakko, jonka valvontaviranomainen voi määrätä rekisterinpitäjälle ja/tai käsittelijälle asetuksen vaatimusten laiminlyönnistä. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.

Kuva 1. Keskeiset osa-alueet. Tässä yhteydessä tulee huomata, että osaa oikeuksista ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten.

2.2 Tietosuoja osana muuta turvallisuuden viitekehystä

Tieto- ja kyberturvallisuuden merkitys on kasvanut viimeisten vuosien aikana merkittävästi sekä toiminnan muuttumisen (palveluiden sähköistäminen, toiminnan digitalisoiminen), palveluiden tuotantotapojen (palveluiden ulkoistaminen, ns. ”pilvipalvelutuotantomalli”) että käyttäjien palveluiden käyttötapojen (uudenlaiset päätelaitteet, ajasta ja paikasta riippumaton työskentely) takia.

Tämä on myös synnyttänyt uudenlaisia tapoja kerätä (sensorit, aktiivisuusrannekkeet), käsitellä (Big Data, massatieto) ja hyödyntää tietoa (visualisointi, ohjelmistorobotiikka). Samanaikaisesti tietoverkkorikollisten, terroristien- ja muiden ääriryhmittymien sekä valtiollisten tiedusteluorganisaatioden muodostamat uhat ovat kasvaneet myös merkittävästi.

Tietoturvallisuutta on kehitetty valtionhallinnossa vuonna 2010 voimaan astuneen tietoturvallisuusasetuksen (681/2010) perusteella, mikä on parantanut mitatusti valtionhallinnon organisaatioiden tieto- ja kyberturvallisuutta sekä palveluiden turvallisuutta.

Euroopan unioni on vaikuttanut tieto- ja kyberturvallisuuden kehittämiseen muun muassa kyberturvallisuusstrategian (6/2013) sekä verkko- ja tietoturvadirektiivin (NIS) avulla. Nyt valmistunut tietosuojaa käsittelevä uudistus täydentää kokonaisuutta siten, että kaikki keskeiset tieto- ja kyberturvallisuuden velvoitteet on päivitetty vastaamaan sekä yhteiskunnan että ympäristön ja teknologiakehityksen edellyttämiä vaati-

muksia. Seuraavaksi EU:n tarkoituksena on uudistaa sähköisen viestinnän tietosuojadirektiivi (ePrivacy Directive).

Kuva 2. Tieto- tai laajemmassa mittakaavassa digitaalinen ja kyberturvallisuus ovat edellytyksiä myös tietosuojan toteutumiselle.

2.3 Valmistelu Suomessa

Oikeusministeriö on asettanut 17.2.2016 päivätyllä päätöksellä työryhmän selvittämään Euroopan unionin yleisen tietosuoja-asetuksen edellyttämien kansallisten lainsäädäntötoimenpiteiden tarvetta. Työryhmä valmistelee myös tietosuoja-asetuksen edellyttämiä muutoksia henkilötietojen käsittelystä annettuun yleiseen kansalliseen lainsäädäntöön sekä koordinoi asiasta annetun erityislainsäädännön tarkistamiseksi tarpeellista lainvalmistelutyötä. Työryhmän toimikausi päättyy 16.2.2018.

2.3.1 Kansallinen liikkumavara

Yleinen tietosuoja-asetus tulee sovellettavaksi sekä julkisella että yksityisellä sektorilla. Asetus korvaa vuoden 1995 henkilötietodirektiivin (95/46/EY) ja sen kansalliseksi täytäntöön panemiseksi annetun henkilötietolain (523/1999) säännökset niiltä osin kuin henkilötietojen käsittely kuuluu asetuksen soveltamisalaan.

Vaikka kyseessä on kansallisesti suoraan sovellettava asetus, se jättää jäsenvaltioille direktiivinomaista kansallista liikkumavaraa. Tätä liikkumavaraa on erityisesti julkisella sektorilla, mutta jossain määrin myös yksityisellä sektorilla. Asetuksen puitteissa on mahdollista antaa kansallista lainsäädäntöä, jolla tarkennetaan asetuksen säännöksiä. Lisäksi kansallisella lainsäädännöllä on jossain määrin mahdollista myös poiketa asetuksen velvoitteista.

2.3.2 Tietosuoja-asetuksen ja julkisuusperiaatteen yhteensovittaminen

Komission antamassa ehdotuksessa yleiseksi tietosuoja-asetukseksi jäi asetuksen suhde asiakirjojen julkisuuteen ratkaisematta. Toukokuussa 2016 voimaan tulleessa yleisessä tietosuoja-asetuksessa on kuitenkin kansallisen asiakirjajulkisuuden ja henkilötietojen suojan yhteensovittamisen mahdollistava 86 artikla.

2.3.3 Viranomaisten roolien ja yhteistyön määrittely

Oikeusministeriön asettaman työryhmän yhtenä tehtävänä on selvittää, onko kansallista tietosuojaviranomaista koskevaa kansallista lainsäädäntöä tarpeen tarkistaa. Lisäksi työryhmän tehtäviin kuuluu valmistella ehdotus tarvittavaksi lainsäädännöksi kansallisesta tietosuojaviranomaisesta, sen organisaatiosta, tehtävistä ja toimivaltuuksista.

3 Keskeiset termit

Tässä luvussa esitellään kokonaisuuteen liittyvät keskeisimmät termit selitteineen. Termit selitteineen ovat pääosin peräisin tietosuoja-asetuksesta, ja niitä on täydennetty tarvittavin osin.

Termi	Kuvaus
Anonymisointi	Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista.
Hallinnollinen sakko	Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella. Sakon enimmäismäärä on 20 milj. € tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.
Hallinnolliset seuraamukset	Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
Henkilötietojen erityiset tietoryhmät, ”arkaluonteiset henkilötiedot”	Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.
Henkilötietojen käsittelijä	Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.
Henkilötietojen käsittely	Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.
Henkilötietojen tietoturvaloukkaus	Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.
Johtava valvontaviranomainen (’One-stop-shop’)	Rekisterinpitäjä, joka toimii useassa Euroopan Unionin jäsenvaltiossa, voi asetuksen myötä asioida päätoimipaikkansa valvontaviranomaisen, eli johtavan valvontaviranomaisen, kanssa henkilötietojen käsittelyä koskevissa asioissa. Näin ollen tarve asioida usean jäsenvaltion valvontaviranomaisen kanssa poistuu.

Kyberturvallisuus	Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan (yhteiskunnalle | organisaatiolle) merkittävien ICT-toimintojen häiriöihin. Se yhdistää laaja-alaisesti riskienhallinnan, tietoturvallisuuden, tietosuojan, jatkuvuuden hallinnan, sekä varautumis- ja toipumissuunnittelun kokonaisuuksia.
Lapsen henkilötietojen käsittely (tietoyhteiskunnan palvelujen tarjoamisesta suoraan lapselle)	Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta.
Osoitusvelvollisuus	Osoitusvelvollisuuden (”accountability”) avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista: • lainmukaisuus, kohtuullisuus ja läpinäkyvyys • käyttötarkoitussidonnaisuus • tietojen minimointi • täsmällisyys • säilytyksen rajoittaminen ja • eheys ja luottamuksellisuus. Eräs keino osoittaa tämä on toteuttaa edellisten tietojen perusteella laadittava tietotilinpäätös.
Profilointi	Mikä tahansa henkilötietojen automaattinen käsittely, jossa henkilötietojen avulla arvioidaan tiettyjä henkilön ominaisuuksia tai analysoidaan tai ennakoidaan näkökohtia, jotka liittyvät kyseiseen henkilöön. Henkilötietojen automaattista käsittelyä, jossa arvioidaan kyseisen henkilön henkilökohtaisia ominaisuuksia henkilön tietoja käyttäen. Erityisesti analysoidaan tai ennakoidaan työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin tai kiinnostuksen kohteisiin, luotettavuuteen tai käyttäytymiseen sekä sijaintiin tai liikkeisiin liittyviä asioita. Profilointia käytetään lukuisissa sosiaalisen median palveluissa ja osassa päätelaitteita käytössä olevissa sovelluksissa.
Pseudonymisointi **(’salanimellä julkaiseminen’)**	Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.
Päätoimipaikka	Keskushallinnon sijaintipaikka, jos rekisterinpitäjällä on toimipaikkoja useammassa kuin yhdessä EU:n jäsenvaltiossa. Jos päätökset ja keinot henkilötietojen käsittelystä tehdään toisessa toimipaikassa, ja tällä toimipaikalla on myös toimivalta panna ne täytäntöön, tällöin päätoimipaikka on se sijaintipaikka, jolla on kyseinen toimivalta.
Rekisterinpitäjä	Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteriseloste, tietosuojaseloste	Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.
Rekisteröity	Henkilö, jonka henkilötietoja käsitellään.
Sisäänrakennettu ja oletusarvoinen tietosuoja	Tietosuojaperiaatteiden sisällyttäminen aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Periaatteiden huomioiminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä, siten että varmistetaan käsittelyn vastaavuus tietosuoja-asetuksen vaatimusten kanssa. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta mm. • oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta • tietoja ei kerätä eikä säilyttää suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen • henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville • taataan rekisteröityjen oikeuksien toteutuminen Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta aina koko käsiteltävien henkilötietojen elinkaaren loppuun.
Tiedollinen itsemääräämisoikeus	Tiedollisten oikeuksien joukko, joka rekisteröidyillä on henkilötietojaan kohtaan. Näihin oikeuksiin kuuluvat asetuksen mukaisesti mm. pääsy tietoihin, tietojen oikaiseminen ja poistaminen, oikeus rajoittaa käsittelyä ja oikeus siirtää tiedot järjestelmästä toiseen. Tiedolliseen itsemääräämisoikeuteen kuuluu keskeisesti oikeus saada tietoa henkilötietojen käsittelystä.
Tietosuoja	Yksityisyyden suojaaminen henkilötietoja käsiteltäessä.
Tietosuojan sertifiointimekanismit	Tietosuojaa koskevia sertifiointimekanismeja, tietosuojasinettejä ja -merkkejä kannustetaan ottamaan käyttöön erityisesti Euroopan Unionin tasolla. Niiden tarkoitus on osoittaa, että rekisterinpitäjä ja / tai käsittelijä, jolle sertifikaatti, sinetti tai merkki on myönnetty, noudattaa hyvää tietojenkäsittelytapaa ja asetuksen vaatimuksia. Euroopan tietosuojaneuvosto tulee kokoamaan kaikki saataville tulevat sertifiointimekanismit julkisesti nähtäville.
Tietosuojavastaava	Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä määritellyissä tilanteissa: • jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin), • ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa laajassa mitassa, tai • ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin. Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan. Yritysryhmä voi nimittää yhden tietosuojavastaavan samoin kuin yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai

	julkishallinnon elintä varten.
Tietotilinpäätös	Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden (”accountability”) toteuttamisessa.
Tietoturvallisuus	Tiedon luottamuksellisuuden, eheyden ja saatavuuden takaaminen teknisten ja organisatoristen toimenpiteiden ja menettelyjen avulla.
Vaikutustenarviointi	Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.
Yhdenmukaisuusmekanismi	Tietosuoja-asetuksen määritelmän mukaan jäsenvaltioiden valvontaviranomaisten on tehtävä yhteistyötä, jotta varmistetaan asetuksen yhdenmukainen soveltaminen kaikkialla Euroopan Unionissa. Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) voi antaa asetuksen soveltamisesta sitovia päätöksiä ja on siten keskeinen toimija yhdenmukaisuuden varmistamisessa.

Taulukko 1. Keskeiset termit ja selitteet.

4 Rekisteröidyn oikeudet

Tietosuoja on ihmisten yksityiselämän suojaamista, ja siihen kuuluu kunkin oikeus henkilötietoihinsa. Rekisteröityjen oikeuksien perusperiaatteena on henkilötietojen suojan takaaminen valtuudettomalta tai henkilöä vahingoittavalta tietojen käytöltä. Tietosuoja-asetuksen määrittelemät rekisteröityjen oikeudet ovat osin vastaavia kuin henkilötietolaissakin määritellyt oikeudet. Asetus kuitenkin tuo myös uusia oikeuksia rekisteröidyille vastaamaan teknologian ja henkilötietoja käsittelevien palveluiden kehitystä. Näitä ovat esimerkiksi oikeus siirtää tiedot järjestelmästä toiseen, jonka merkitys on kasvanut toiminnan digitalisoituessa.

Rekisteröidyn oikeuksien toteuttaminen on yksi rekisterinpitäjän päävelvollisuuksista. Rekisteröidyn oikeuksien lisäksi asetus määrittelee uutena rekisterinpitäjän velvollisuutena ilmoitusvelvollisuuden. Ilmoitusvelvollisuus koskee henkilötietojen tietoturvaloukkaustilanteita, joissa henkilötietojen luottamuksellisuus on vaarantunut. Näin ollen asianomaisilla rekisteröidyillä on oikeus saada ilmoitus, jos hänen henkilötietonsa ovat vuotaneet ulkopuolisille luvattomasti. Oikeus saada ilmoitus tietovuodosta voidaan nähdä loogisena kokonaisuutena asetuksen määrittelemiin rekisteröidyn oikeuksiin, minkä vuoksi se käsitellään osana tätä kappaletta, vaikka se kuuluukin asetuksen eri artiklaan. Ilmoitus on tehtävä, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille.

Rekisterinpitäjällä on velvollisuus tunnistaa rekisteröidyn henkilöllisyys, kun hän käyttää oikeuksiaan saadakseen pääsyn tietoihinsa, oikeuksiaan häntä koskevien tietojen oikaisuun, poistamiseen tai siirtääkseen tietonsa järjestelmästä toiseen. Näin vältytään tilanteilta, joissa muiden oikeuksia tai vapauksia loukattaisiin. Rekisteröidyn pyyntöihin näitä oikeuksia koskien tulee vastata kuukauden kuluessa pyynnön vastaanottamisesta. Tarvittaessa rekisterinpitäjä voi soveltaa kahden kuukauden jatkoaikaa, mikäli rekisteröidyn

pyyntö on monimutkainen tai niitä on tullut määrällisesti useita. Tiedot tulee pääsääntöisesti toimittaa sähköisessä muodossa ja maksutta. Järjestelmien suunnittelussa tulee ottaa huomioon rekisteröidyn oikeuksien toteuttaminen. Erityisesti kannattaa arvioida henkilötietoihin kohdistuvien pyyntöjen lukumäärä, ja mikäli määrä arvioidaan suureksi, kiinnittää huomioita manuaalisten työvaiheiden minimointiin tietoja koostettaessa.

4.1 Rekisterinpitäjän tiedonantovelvoitteet

Nykysääntelyä vastaavasti rekisterinpitäjällä on velvollisuus tiedottaa avoimesti henkilötietojen käsittelystä ennen käsittelytoimien aloittamista. Uusia viestittäviä asioita ovat asetuksen mukaan henkilötietojen säilytysajan ja tietosuojavastaavan yhteystietojen ilmoittaminen.

Rekisterinpitäjän tulee ilmoittaa rekisteröidyille helposti ymmärrettävässä muodossa esimerkiksi seuraavat kohdat ennen kuin henkilötietoja kerätään:

- Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot (mikäli tietosuojavastaava on nimitetty)
- Mihin tarkoituksiin henkilötietoja käsitellään ja mikä on käsittelyn oikeusperusta (esim. palvelun tarjoamiseksi rekisteröidyn suostumuksella)
- Jos henkilötietoja luovutetaan kolmansille osapuolille, henkilötietojen vastaanottajat
- Jos henkilötietoja siirretään kolmanteen maahan, miten tietosuojan riittävyydestä on huolehdittu ja mistä rekisteröity voi saada siitä lisätietoja
- Henkilötietojen säilytysaika tai kriteerit sille, miten säilytysaika määräytyy
- Tämän raportin kappaleissa 4.2.–4.6. esitellyt rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää
- Oikeus tehdä valitus valvontaviranomaiselle
- Mihin henkilötietojen antamisen vaatimus perustuu, onko rekisteröidyn pakko toimittaa tiedot ja mitkä ovat seuraukset tietojen antamatta jättämisestä
- Liittyykö käsittelyyn automaattista päätöksentekoa tai profilointia, millainen käsittelylogiikka niihin liittyy, sekä niiden merkitys ja seuraukset rekisteröidyille.

Mikäli rekisterinpitäjä ei kerää henkilötietoja rekisteröidyiltä suoraan vaan muista lähteistä, yllä mainittujen kohtien lisäksi on ilmoitettava:

- Kerättävät tiedot
- Mistä henkilötiedot on saatu ja onko tiedot saatu yleisesti saatavilla olevista lähteistä.

Rekisterinpitäjän antama kuvaus henkilötietojen käsittelystä tulee pitää julkisesti saatavilla ja sen ajantasaisuus tulee tarkistaa säännöllisesti. Rekisterinpitäjien on erittäin suositeltavaa panostaa avoimeen ja läpinäkyvään viestintään käsittelytoimista ja rekisteröityjen oikeuksien toteutuksesta. Digitaalisten palvelujen luotettavuus tulee kasvamaan entistä suurempaan rooliin lähitulevaisuudessa.

4.2 Oikeus saada pääsy tietoihin

Nykysääntelyn tarkastusoikeutta vastaavasti rekisteröidyillä on asetuksen mukaan oikeus saada pääsy omiin henkilötietoihinsa. Tämä tarkoittaa, että rekisterinpitäjän on rekisteröidyn pyytäessä ilmoitettava käsitelläänkö häntä koskevia henkilötietoja vai ei sekä toimitettava jäljennös käsiteltävistä henkilötiedoista.

Lisäksi rekisterinpitäjän tulee ilmoittaa seuraavat kohdat:

- Henkilötietojen käsittelyn tarkoitukset
- Käsiteltävät henkilötietoryhmät
- Jos henkilötietoja luovutetaan kolmansille osapuolille, henkilötietojen vastaanottajat
- Henkilötietojen säilytysaika tai kriteerit, miten säilytysaika määräytyy
- Tämän raportin kappaleissa 4.2.–4.6. esitellyt rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää
- Oikeus tehdä valitus valvontaviranomaiselle
- Jos henkilötietoja ei kerätä suoraan rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot
- Liittyykö käsittelyyn automaattista päätöksentekoa tai profilointia, millainen käsittelylogiikka niihin liittyy, sekä käsittelyn merkitys ja seuraukset rekisteröidyille
- Jos henkilötietoja siirretään kolmanteen maahan se, miten tietosuojan riittävyydestä on huolehdittu.

Rekisterinpitäjän velvollisuus toimittaa jäljennös sähköisesti kaikista käsiteltävistä rekisteröidyn henkilötiedoista on syytä ottaa huomioon henkilötietoja käsittelevien järjestelmien ja käsittelyä hoitavien kolmansien osapuolten näkökulmasta. On suositeltavaa ottaa huomioon, että rekisteröityä koskevien tietojen kerääminen voi olla hyvin aikaa vievää, erityisesti jos tiedot joudutaan keräämään manuaalisesti useasta eri järjestelmästä ja / tai välittämään pyyntöjä edelleen käsittelyä suorittaville kolmansille osapuolille. Siten on perusteltua luoda määrämuotoinen prosessi, johon rekisteröityjen pyynnöt ohjataan ja joka sisältää tarvittavat sidosryhmät tietojen keräämiseksi.

4.3 Oikeus tietojen oikaisemiseen

Myös rekisteröidyn oikeus tietojen oikaisemiseen vastaa nykysääntelyä. Rekisteröidyllä on asetuksen mukaisesti oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat virheelliset henkilötiedot tai täydentää puutteellisia henkilötietoja.

4.4 Oikeus poistaa tiedot (”oikeus tulla unohdetuksi”)

Oikeus tulla unohdetuksi tarkoittaa rekisteröidyn oikeutta pyytää rekisterinpitäjää poistamaan esimerkiksi häntä koskevat vanhentuneet henkilötiedot. Rekisteröidyllä on esimerkiksi oikeus peruuttaa suostumuksensa, johon käsittely on perustunut. Jos rekisteröity peruuttaa suostumuksen, hän voi esittää rekisterinpitäjälle pyynnön poistaa rekisteröityä koskevat tiedot järjestelmistään, minkä jälkeen rekisterinpitäjän on poistettava henkilötiedot, ellei käsittelylle ole muuta laillista perustetta. Suostumuksen peruuttamisen tulee olla yhtä helppoa kuin sen antamisen.

Poiston tekninen toteuttaminen asettaa vaatimuksia henkilötietoja käsittelevälle järjestelmälle, mutta asetusteksti itsessään ei aseta vaatimuksia poiston tekniselle toteutukselle. Poiston teknisen toteutukselle on olemassa ainakin seuraavat vaihtoehdot:

- Tietojen merkitseminen niin, ettei niitä enää käsitellä tuotantojärjestelmissä ja niihin pääsyä rajoitetaan merkittävästi, mutta tiedot kuitenkin ovat fyysisesti edelleen järjestelmän tietovarastoissa.
- Tietojen salaaminen vahvalla, nykyaikaisella salausalgoritmilla ja yksilöllisellä salausavaimella kullekin rekisteröidylle. Salausavaimet on voitava tuhota ylikirjoittamalla, jolloin salattu tieto ei käytännössä ole purettavissa luettavaan muotoon nykytietokoneiden laskentateholla. Tämä vaihtoehto asettaa vaatimuksia salausalgoritmin valinnalle sekä avainten hallinnalle.
- Tietojen ylikirjoittaminen.

Tiedontallennusvälineiden fyysinen tuhoaminen on vaihtoehtona ylimitoitettu ja epäkäytännöllinen erityisesti, kun pilvipalveluihin pohjautuvissa järjestelmissä tietojen fyysinen paikallistaminen on lähes mahdotonta. Levyjen fyysinen tuhoaminen lisäisi myös kustannuksia. Euroopan tietosuojaneuvoston tai valvontaviranomaisen soveltamisohjeistusta tarvitaan teknisen toteuttamisen asetuksen vaatimuksenmukaisuuden määrittelemiseksi.

Oikeutta tulla unohdetuksi ei sovelleta lakisääteisiin rekistereihin. Tietojen poistaminen niistä ei ole mahdollista lakisääteisen tehtävän suorittamiseen liittyvän käsittelyn yhteydessä.

4.5 Oikeus siirtää tiedot järjestelmästä toiseen

Asetuksen uusi rekisteröidyn oikeus on oikeus siirtää tiedot järjestelmästä toiseen. Käytännössä rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa siirtomuodossa ja toimittaa ne toiselle rekisterinpitäjälle. Siirto-oikeuteen kuuluu myös tietojen siirtäminen suoraan rekisterinpitäjältä toiselle jos se on teknisesti mahdollista. Oikeus edellyttää, että käsittely perustuu suostumukseen tai sopimukseen ja käsittely tehdään automatisoidusti.

Siirto-oikeus ei velvoita rekisterinpitäjiä suunnittelemaan tai toteuttamaan keskenään yhteensopivia järjestelmiä. Rekisterinpitäjien järjestelmien ollessa keskenään erilaisia, on yksi mahdollisuus tehdä siirto toimittamalla tiedot esimerkiksi siirrettävällä muistivälineellä, josta ne voidaan siirtää edelleen uuden rekisterinpitäjän järjestelmään. Siirto-oikeuden toteuttaminen aiheuttanee monissa tietojärjestelmissä muutoksia manuaalisten työvaiheiden välttämiseksi tietojen koostamisessa ja luovuttamisessa.

Siirto-oikeutta sovelletaan myös julkisella sektorilla niihin rekistereihin, jotka on kerätty vapaaehtoisten tehtävien hoitamiseen. Siirto-oikeutta ei sovelleta käsittelyyn, joka on tarpeen yleistä etua koskevan tehtävän suorittamisessa tai julkisen vallan käyttämisessä. Käytännössä esimerkiksi kuntien järjestelmiin tulee kuitenkin rakentaa mahdollisuus henkilötietojen siirtoon, sillä samoja järjestelmiä käytetään sekä lakisääteisten että vapaaehtoisten tehtävien hoitamiseen.

4.6 Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia

Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 artiklan 1 kohdan e tai f alakohtaan, kuten näihin säännöksiin perustuvaa profilointia. Rekisterinpitäjä ei saa enää käsitellä henkilötietoja, paitsi jos rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, tai jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Jos rekisteröity vastustaa henkilötietojen käsittelyä suoramarkkinointia varten, niitä ei saa enää käsitellä tähän tarkoitukseen.

Tämä oikeus ei koske julkisen sektorin rekistereitä, joita pidetään lain perusteella..

Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi vastaavalla tavalla.

Edellä olevaa kohtaa ei sovelleta, jos päätös esimerkiksi:

- on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten
- on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi
- perustuu rekisteröidyn nimenomaiseen suostumukseen.

4.7 Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta

Uutena velvollisuutena rekisterinpitäjille on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta henkilökohtaisesti niille rekisteröidyille, joiden tietoja loukkaus koskettaa. Oikeus astuu voimaan, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esimerkiksi identiteetinvarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa. Ilmoitusta ei tarvitse lähettää tietyissä tilanteissa, esimerkiksi jos vuotaneet henkilötiedot ovat salattu ja salausavaimet eivät ole vaarantuneet. Rekisterinpitäjä voi ilmoittaa vuodosta median välityksellä, jos henkilökohtaisten ilmoitusten lähettäminen vaatisi kohtuutonta vaivaa. Tällaisiksi tilanteiksi voidaan nähdä suuren kokoluokan tietovuodot, joiden piirissä on lukemattomia rekisteröityjä.

Rekisteröidylle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa listatut kohdat. Ilmoitus tulee antaa ilman aiheetonta viivytystä. Ilmoitukselle on suositeltavaa laatia pohja osaksi rekisterinpitäjän kriisiviestintää. Ilmoituksen tulisi sisältää

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

Henkilötietojen tietoturvaloukkauksesta ilmoittamiseen liittyy olennaisesti rekisterinpitäjän ja mahdollisten käsittelijöiden tietoturvallisuuden tekninen ja hallinnollinen toteutus mm. havainnointi- ja reagointikyvykkyyksien osalta. Näitä käsitellään tämän raportin seuraavissa kappaleissa.

5 Rekisterinpitäjän velvollisuudet

Edellä käsiteltyjen rekisteröidyn oikeuksien toteuttamisen ohella tietosuoja-asetus määrittelee joukon muitakin velvollisuuksia rekisterinpitäjälle. Tämä luku kuvaa asetuksen päävelvollisuudet. Seuraavassa kappaleessa 6 kuvataan suosituksia toimenpiteistä, joilla organisaation tietosuojakyvykkyyttä on suositeltavaa lähteä rakentamaan ja kehittämään määrämuotoisesti.

Nykysääntelystä poiketen asetus määrittelee velvollisuuksia myös suoraan henkilötietojen käsittelijälle. Tässä kappaleessa keskitytään kuitenkin rekisterinpitäjän velvollisuuksiin. Valvontaviranomaisen sanktiointioikeus koskettaa rekisterinpitäjän ohella kuitenkin myös käsittelijöitä.

Tietosuoja-asetuksen tullessa voimaan pelkkä vaatimuksenmukaisuus ei enää riitä, vaan rekisterinpitäjän on pystyttävä osoittamaan, miten se on varmistanut tietosuojavelvollisuuksien toteutumisen toiminnassaan tarvittavin teknisin, hallinnollisin ja organisatorisin toimenpitein. Tätä kutsutaan osoitusvelvollisuudeksi.

5.1 Käsittelyn oikeusperusta

Henkilötietojen käsittely on lainmukaista ainoastaan asetuksen määrittelemin edellytyksin. Rekisterinpitäjä on vastuussa siitä, ettei henkilötietoja käsitellä ilman asianmukaista oikeusperustaa. Asetuksen mukaan lainmukaisia käsittelyn edellytyksiä ovat muun muassa:

- rekisteröidyn vapaaehtoinen ja informoitu suostumus. Rekisterinpitäjän velvollisuuksiin kuuluu pystyä osoittamaan jälkikäteen, että suostumus on annettu
- sellaisen sopimuksen täytäntöön paneminen, jossa rekisteröity on osapuolena
- rekisterinpitäjän lakisääteinen velvoite. Asetus sallii kansallista liikkumavaraa lakisääteisten velvoitteiden toteuttamisessa
- rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen
- rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen, jonka soveltamiseen myös sallitaan kansallista liikkumavaraa.

Rekisterinpitäjän tulee huolehtia, että henkilötietoja käsitellään vain asianmukaisin edellytyksin ja että tämä huomioidaan myös uusia käsittelytapoja suunniteltaessa. Henkilötietojen käsittelyn tulee olla tarkoitussidonnaista; hänen tulee ennakkoon määritellä ne tarkoitukset, joihin henkilötietoja käsitellään ja varmistua, ettei tietoja käsitellä muihin tarkoituksiin.

5.2 Tietosuojan hallinnointi, roolit ja vastuut

Rekisterinpitäjän tietosuojavelvollisuudet koskettavat kaikkia organisaation käsittelemiä henkilötietoja, olipa kyseessä yksityishenkilöiden, yhteistyökumppaneiden, asiakkaiden tai organisaation henkilöstön tiedot. Jotta tietosuojasta voidaan huolehtia organisaation laajuisesti huomioiden kaikki käsiteltävät tiedot, tulee tietosuojan hallinnointi vastuuttaa organisaatiossa sekä varata riittävästi resursseja koko organisaation tietosuojatehtävien toteuttamiseen.

5.2.1 Tietosuojavastaava

Asetus velvoittaa määrätynlaisia rekisterinpitäjiä nimeämään tietosuojavastaavan. Tietosuojavastaavan nimeäminen on ollut vaatimuksena nykysääntelyssäkin esimerkiksi terveydenhuollon alalla. Nimeäminen täytyy tehdä, jos jokin seuraavista ehdoista täyttyy:

a) jtietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin),

b) ydintehtävät muodostuvat käsittelytoimista, jotka ovat luonteelta sellaisia, että ne edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa laajassa mitassa, tai

c) ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin.

Edellä mainituilla perusteilla tietosuojavastaavan nimittäminen kohdistuu erityisesti julkiselle sektorille. Yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten. Tällöin on huomioitava organisaatiorakenteet ja organisaatioiden koko, jotta tietosuojavastaavan toimenkuvan laajuus on hallittavissa. Myös yritysryhmä voi nimittää yhden tietosuojavastaavan, jonka toimenkuvaan kuuluu koko ryhmän henkilötietojen käsittely ja tietosuojan toteutumisesta huolehtiminen.

Seuraavassa on listattu tärkeimpiä asetuksen määrittämiä tietosuojavastaavan asemaan ja tehtävänkuvaan liittyviä seikkoja.

Tietosuojavastaavan asema

- Riippumaton asema organisaatiossa
- Raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle
- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojaan liittyviin kysymyksiin
- Pätevyysvaatimus tietosuojan alalta: tietosuojalainsäädäntötuntemus, lain vaatimusten soveltamisosaaminen ja alan käytäntöjen tuntemus
- Voi olla rekisterinpitäjän tai käsittelijän palkkalistoilla, tai ulkoistettu palveluntuottajalle
- Taattava tarvittavat resurssit sekä asianmukainen pääsy henkilötietoihin ja niiden käsittelytoimiin tietosuojavastaavan tehtävien hoitamiseksi
- Tehtävä yhteistyötä useiden organisaation yksiköiden kanssa
- Julkinen yhteyspiste valvontaviranomaisen ja rekisteröityjen suuntaan
- Salassapitovelvollisuus
- Ei saa erottaa tai rangaista tietosuojavastaavan tehtävien hoitamisen vuoksi
- Voi suorittaa muitakin tehtäviä tietosuojavastaavan tehtävien ohella kuitenkin niin, ettei niistä aiheudu eturistiriitoja.

Tietosuojavastaavan tehtävänkuva

- Asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa
- Organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä
- Dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta
- Ilmoitusvelvollisuuden toteutumisen seuranta
- Vaikutustenarviointien tekemisen tukeminen ja valvonta
- Yhteistyö valvontaviranomaisen kanssa
- Tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle
- Rekisteröityjen oikeuksien toteuttamisen tukeminen
- Käsittelytoimiin liittyvän riskin asianmukainen huomiointi tehtävien suorittamisessa

5.2.2 Tietosuojaorganisaatio

Koska tietosuojatyö on laaja-alaista ja koskettaa lähes kaikkia organisaation yksiköitä, on tietosuojavastaavan, jos sellainen on nimetty, tai muun tietosuojavastuullisen roolin, ympärille on suositeltavaa muodostaa tietosuojaorganisaatio, joka koostuu useamman yksikön jäsenistä.

Yksiköitä, joista tietosuojaorganisaatio on suositeltavaa muodostaa, ovat

- henkilötietoja käsittelevät yksiköt, kuten esimerkiksi asiakaspalvelu, henkilöstöhallinto, palvelutuotanto, myynti ja markkinointi
- yksiköt, jotka vastaavat henkilötietoja käsittelevien järjestelmien, sovellusten tai palvelujen hankinnasta, kehityksestä, käyttöönotosta tai ylläpidosta, kuten esimerkiksi hankinta-, IT-, tietoturva- ja tuotekehitys-yksikkö.

Tietosuojaorganisaation tavoitteena on viedä tietosuojatyö osaksi organisaation operatiivista toimintaa ja raportoida esimerkiksi uusista henkilötietojen käsittelyä koskettavista hankkeista, muutoksista ja haasteista, jotta asetuksen määrittelemä osoitusvelvollisuus voidaan toteuttaa. Täten tietosuojaorganisaatio ja sen tehtävät kannattaa suunnitella siten, että organisaation olemassa olevaa organisaatiorakennetta, yhteistyörakenteita ja prosesseja hyödynnetään mahdollisimman paljon.

Koska organisaatiossa on jo todennäköisesti olemassa toimintamallit henkilötietojen käsittelyn osalta, kannattaa tämä uusi lainsäädäntökokonaisuus nähdä eräänlaisena facelift-päivityksenä, jonka avulla olemassa olevia toimintamalleja ja prosesseja päivitetään uusien vaatimusten mukaisiksi – niitä ei tarvitse tai pidä alusta saakka kokonaan miettiä, jos ne ovat kerta jo toiminnassa.

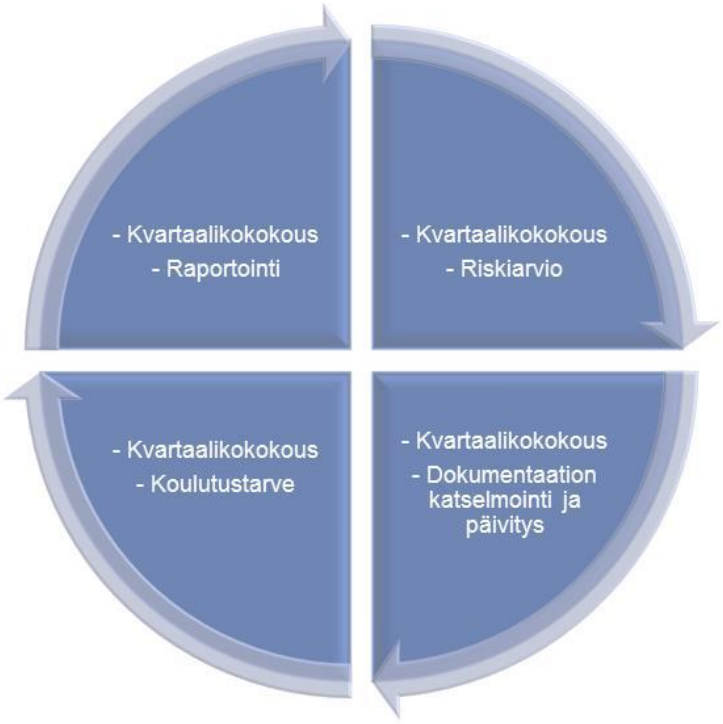
5.2.3 Vuosikello

Tietosuojaorganisaation säännölliset ja määrämuotoiset tehtävät on hyvä määritellä ja ryhmitellä vuosikelloon, jotta voidaan taata niiden hoitamiseen tarvittava aika ja seurata niiden toteutumista. Kuvassa 3 on esimerkki tietosuojaorganisaation vuosikellosta.

Säännöllisiin tehtäviin kuuluvat tietosuojaorganisaation tapaamiset, tietosuojadokumentaation katselmointi ja päivitys, koulutustarpeen arviointi, riskiarvio ja johdon raportointi. Tapaamiset voidaan järjestää esimerkiksi kerran kvartaalissa, ja niissä käsiteltäviin asioihin voi kuulua esimerkiksi

- tärkeimpien järjestelmähankkeiden ja muutosten tilanne,
- rekisteröidyiltä ja valvontaviranomaisilta tulleet yhteydenotot,
- tietosuojavaikutuksia sisältävien merkittävien tietoturvatapahtumien käsittely,
- vaikutustenarvioinnit ja niissä määriteltyjen hankintakeinojen tilanne sekä
- yleisesti tietosuojaan liittyen havaitut puutteet ja tarpeet.

Säännöllisten ja määrämuotoisten tehtävien lisäksi tietosuojaorganisaation vastuulle voivat kuulua operatiiviset tietosuojatehtävät, kuten rekisteröityjen pyyntöihin vastaaminen (joita käsitellään luvussa 4), tietosuojan vaikutustenarviointien laatiminen, vaatimusmäärittelyt tuotekehityksessä ja hankinnoissa, sopimusvaatimusten määrittelyt ja käsittelyn seurannan tehtävät. Näitä tehtäviä kuvataan tämän raportin seuraavissa kappaleissa.



Kuva 3. Yksinkertaistettu tietosuojatehtävien vuosikello.

5.3 Tietosuojariskienhallinta

Tietosuoja-asetuksen lähtökohtana on riskilähtöisyys. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvollisia arvioimaan henkilötietojen käsittelyyn liittyviä riskejä ja valitsemaan arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on syytä liittää osaksi organisaation riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Jos tietosuojavastaava on nimetty, hänen tulee tukea organisaation eri yksiköitä, jotta tietosuojariskejä tunnistettaisiin paremmin sekä olla mukana määrittelemässä tunnistetuille, hallintaan otettaville riskeille tarvittavia hallintakeinoja. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

5.3.1 Tietosuojan vaikutustenarvioinnit

Asetus määrittää tietosuojan vaikutustenarvioinnin pakolliseksi toimenpiteeksi sellaisille henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia tulee käyttää niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään riskitasoa, sekä samalla varmistumaan asetuksen vaatimusten toteutumisesta. Jos vaikutustenarvioinnin perusteella riskitaso on suuri, eikä rekisterinpitäjä pysty sitä pienentämään, on otettava yhteyttä valvontaviranomaiseen (ennakkokuuleminen).

Vaikutustenarviointi kohdistetaan suunnitteluvaiheessa olevalle järjestelmälle, sovellukselle, palvelulle tai hankkeelle, jossa tullaan käsittelemään henkilötietoja. Arviointi tulee suorittaa mahdollisimman aikaisessa vaiheessa, jotta tarvittavat hallintakeinot saadaan mukaan kehitystyöhön. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen. Vaikutustenarviointien tekeminen on kuitenkin suositeltavaa kaikille rekisterinpitäjille, jotta asetuksen vaatimustenmukaisuudesta voidaan varmistua. Arviointien tulokset on hyvä dokumentoida määrämuotoisesti, jotta niiden tulokset ovat vertailukelpoisia ja jotta määriteltyjen hallintakeinojen toteuttamista voidaan seurata. Dokumentaatio on tärkeä osa osoitusvelvollisuuden toteuttamista. Vaikutustenarviointi tehdään asetuksen (ja muun sovellettavan tietosuojasääntelyn) vaatimuksista johdettua kriteeristöä vasten. Vaikutustenarviointia tehtäessä tulee pystyä kuvaamaan henkilötietojen tietovuot ja käyttötarkoitukset, arvioimaan vaatimuksenmukaisuutta ja yksilöiden tietosuojaan liittyviä riskejä sekä muodostamaan hallintakeinoja havaittujen puutteiden ja riskien pienentämiseksi. Nykyisin valmiita vaikutustenarviointimalleja ei ole saatavilla, sillä sovellettavat

tietosuojasäännökset vaihtelevat arvioinnin kohteen mukaan. Tällöin organisaatiot joutuvat usein kehittämään mallin itse. Jos organisaatiolla ei ole omaa kyvykkyyttä suorittaa vaikutustenarviointia, voidaan sen tekemisessä hyödyntää riippumatonta kolmatta osapuolta.

Vaikutustenarviointi on syytä liittää osaksi kehitystyötä sekä teknistä tietoturvatestausta, jossa hallinnolliseen riskitarkasteluun perustuvan vaikutustenarvioinnin hallintakeinojen toteutus voidaan teknisesti todentaa. Esimerkiksi pääsynhallintaa ja teknisten suojausmekanismien toteutusta voidaan testata hyökkääjän näkökulmasta. Näitä asioita käsitellään tämän raportin kappaleissa 5.3. ja 5.4.

5.4 Sisäänrakennettu- ja oletusarvoinen tietosuoja

Asetus velvoittaa sisäänrakennetun ja oletusarvoisen tietosuojan käsitteillä rekisterinpitäjää sisällyttämään tietosuojaperiaatteet ja -vaatimukset aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta mm.

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin.

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojan velvollisuuksista voidaan huolehtia, pitää tietosuojavaatimukset analysoida ja toteuttaa aikaisessa vaiheessa. Käytännössä tämä tarkoittaa tietosuojan sisällyttämistä sekä järjestelmä- ja sovelluskehitykseen että hankintoihin ja projektinhallintaan.

5.4.1 Tietosuoja järjestelmä- ja sovelluskehityksessä

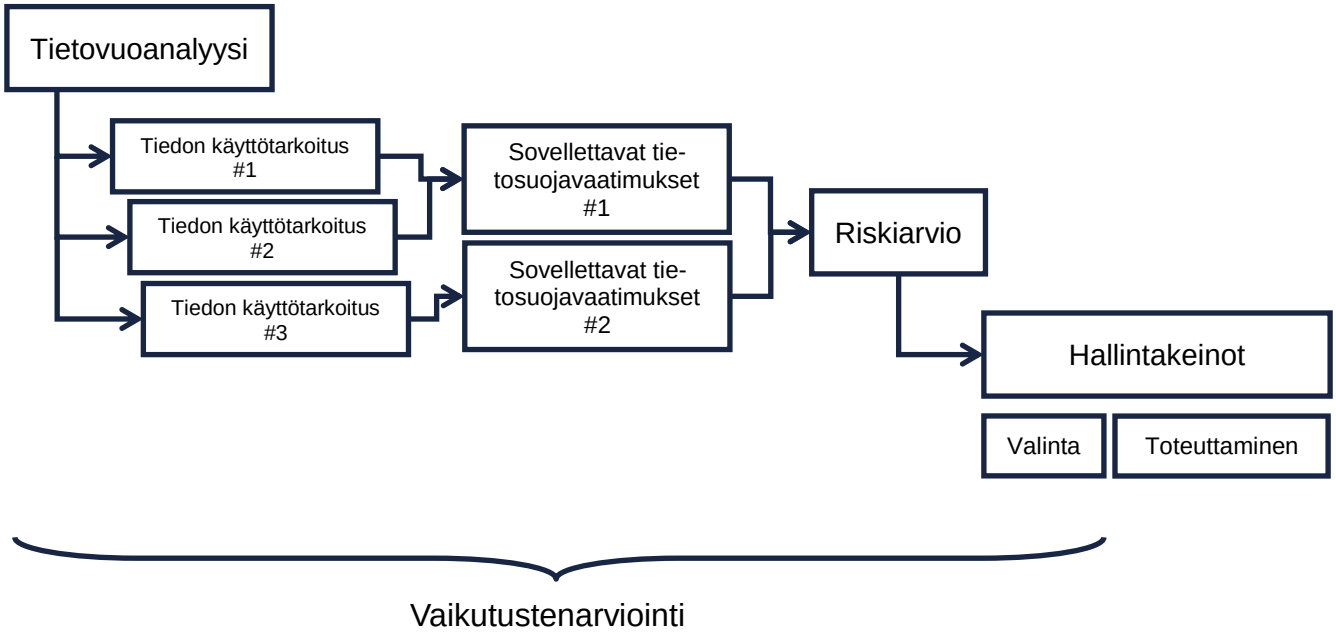
Rekisterinpitäjän järjestelmä- ja sovelluskehitysprosesseissa tulee olla mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tietosuoja-asetuksen ohella tietosuojavaatimuksia ovat toimialakohtaiset lait esimerkiksi terveydenhuollon ja teleoperaattoriliiketoiminnan alalla sekä käsiteltäessä työntekijöiden henkilötietoja työnantajan roolissa.

Tekninen toteutus tulee suunnitella siten, että se vastaa käsittelyn riskitasoa. Näin ollen on perusteltua liittää vaikutustenarviointi osaksi kehitystyötä, jossa riskilähtöisesti valitaan tarvittavat hallintakeinot riskitason hallitsemiseksi (esimerkiksi pienentämiseksi) ja vaatimustenmukaisuuden saavuttamiseksi (kuva 4). Muuten riskinä on, että suunnittelu ei ota huomioon järjestelmän tietosisällön erityispiirteitä. Väärin suunniteltu järjestelmä voi olla hankalaa tai jopa mahdotonta jälkikäteen muuttaa niin, että ongelma saadaan korjattua.

Hallintakeinot -työvaiheessa määritellään ne tekniset keinot, joilla riskitasoa pienentävät hallintakeinot voidaan toteuttaa. Hallintakeinojen valinnassa tulee huomioida kulloinkin voimassa olevat parhaat käytännöt tietoturvan suhteen. Osa-alueet, kuten salaus, kehittyvät jatkuvasti, mistä johtuen kulloinkin voimassa olevat suositukset vaihtuvat ajoittain. Järjestelmien suunnittelusta vastaavien henkilöiden on tärkeä pysyä ajan tasalla kulloinkin voimassa olevista parhaista tietoturvakäytännöistä sekä miettiä, kuinka mahdolliset tulevat muutokset voidaan huomioida toteutuksessa. Lisätietoa salauksesta on julkaisussa VAHTI 2/2015 Ohje salauskäytännöistä.

Teknisiä keinoja voivat olla esimerkiksi pääsynhallinnan toteuttaminen, tiedon salaaminen oikein valituilla salausalgoritmeilla sekä tietojen anonymisointitavan suunnittelu ja tekninen toteuttaminen. Hallintakeinot tulee toteuttaa osaksi järjestelmän tai sovelluksen arkkitehtuuria mahdollisimman aikaisessa vaiheessa,

koska niillä voi olla vaikutusta järjestelmän muihin toimintoihin. On mahdollista, että esimerkiksi tietojen anonymisointi vaikuttaa siihen, millaisia toimintoja järjestelmään voi toteuttaa, koska kaikki järjestelmään tuleva tieto ei ole sellaisenaan käytettävissä.



Kuva 4. Tietosuoja osana kehitystyötä.

Järjestelmäkehityksen aikana ja sen päättyessä on tärkeää varmistaa, että toteutus vastaa suunniteltua ja että vaaditut kontrollit on toteutettu järjestelmään oikein. Monet kontrolleista ovat sellaisia, ettei niiden puutetta tai virheellistä toimintaa havaitse normaalissa käytössä. Tyypillisesti järjestelmäkokonaisuus toimii ongelmitta, vaikka osa kontrolleista olisikin tehty väärin tai jätetty kokonaan pois toteutuksesta. Testaus edellyttää sellaisten testitapausten tunnistamista ja toteutusta, joissa käydään läpi erilaiset väärinkäyttötapaukset. Näiden ottaminen mukaan perinteiseen sovellustestaukseen varmistaa, että myös tietosuojaan liittyvät tarpeet on huomioitu.

5.4.2 Tietosuoja hankinnoissa ja projektinhallinnassa

Mikäli rekisterinpitäjä ulkoistaa sovelluskehityksen kolmannelle osapuolelle, tulee ulkoistussopimuksessa vaatia sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen kehitysprosessissa. Vaatimukset tulisi pystyä yksilöimään mahdollisimman tarkasti eikä viittaamaan yleisesti ”riittävän tietosuojan toteuttamiseen”. Rekisterinpitäjän tulee hallita sovelluskehityksen ulkoistussopimuksissa olevia vaatimuksia.

Rekisterinpitäjän hankkiessa järjestelmiä, sovelluksia ja palveluja, jotka tulevat käsittelemään henkilötietoja, tietosuoja tulee huomioida jo hankintaprosessissa. Näin valitaan sellaisia toimittajia, joiden toimittamien tuotteiden tietosuojataso vastaa asetuksen vaatimuksia. Tietosuojavaatimukset tulee asettaa jo tarjouspyynnössä ja liittää ne osaksi tarjouspyynnön perusteella tehtäviä sopimuksia. Suositeltavaa on vaatia salassapitoa sopimuksissa ja tarvittaessa lisäksi myös erillisillä vaitiolositoumuksilla. Sopimuksia, joissa toimeksisaaja toimii myös henkilötietojen käsittelijänä, käsitellään kappaleessa 5.7.

Tietosuojasta huolehtiminen on hyvä liittää osaksi rekisterinpitäjän projektinhallintamallia. Kun uusia järjestelmiä, sovelluksia tai palveluja otetaan käyttöön, tulee ennen käyttöönottoa arvioida tarvittavat toimenpiteet tietosuojan säilymisen kannalta. Tällaisia toimenpiteitä voivat olla esimerkiksi rekisteriselosteen laadinta tai päivittäminen, ja aloitettavan käsittelyn liittäminen osaksi rekisteröidylle tarjottavia kanavia heidän oikeuksiensa toteuttamiseen.

5.4.3 Tiedon elinkaaren hallinta

Henkilötietojen elinkaaren määrittäminen kuuluu myös olennaisena osana sisäänrakennetun- ja oletusarvoisen tietosuojan käsitteisiin. Elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon, kuva 5.

Kuva 5. Henkilötietojen elinkaari.

Rekisterinpitäjän on ennen käsittelyn aloittamista määriteltävä sovellettavien tietosuojasääntelyjen ja liiketoiminnan vaatimusten perusteella henkilötietojen tarpeellinen säilytysaika, eli kuinka kauan henkilötietoja tarvitaan niiden käsittelytarkoitukseen. Vähintäänkin on määriteltävä ne kriteerit, joiden pohjalta säilytysaika määräytyy. Säilytysaikamääritykset tulee tehdä lisäksi henkilötietoja käsitteleviin sovelluksiin ja järjestelmiin hallintakeinojen toteutusvaiheessa. Säilytysaika on huomioitava myös varmistuksissa, ettei vanhentunutta ja käsittelystä poistunutta tietoa pääse palautumaan esimerkiksi epäsuotuisista tilanteista järjestelmän toipumisen yhteydessä. Mikäli henkilötietoja ei enää tarvita niiden käsittelytarkoituksen toteuttamiseen, mutta niitä ei voida poistaa muun sääntelyn takia, tulee tiedot arkistoida ja niiden käsittelyä rajoittaa. Tällaisia tietoja voivat olla esimerkiksi kirjanpitoa varten säilytettävät tiedot. Kun määritelty säilytysaika tuotantojärjestelmissä ja arkistossa on umpeutunut, tiedot tulee joko poistaa tietoturvallisesti tai anonymisoida siten, että rekisteröidyt eivät enää ole tunnistettavissa. Säilytysaika tulee ilmoittaa myös rekisteröidyille suunnattavassa viestinnässä tämän raportin kappaleessa 4.1. kuvatulla tavalla.

5.5 Tietoturvallisuuden toteuttaminen

Tietosuoja-asetus velvoittaa rekisterinpitäjää toteuttamaan asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta henkilötietojen käsittely on turvattua. Henkilötiedot tulee suojata siirron, tallennuksen ja käsittelyn aikana oikeudetta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai pääsyltä. Valtionhallinnossa tietoturvan toteuttamista ohjaa tietoturvallisuusasetus (681/2010), jossa on myös määritetty tietoturvatasot ja tietoturvatasoihin liittyvät hallinnolliset ja tekniset vaatimukset. Organisaation pitää tunnistaa sen toimintaan kohdistuvat tietoturvallisuuteen liittyvät vaatimukset, jotka koskevat myös sen tietojenkäsittelyä sekä toteuttaa organisaation toiminta vaatimusten edellyttämällä tavalla. Tietoturvallisuuden hallintaan voi hyödyntää saatavilla olevia hallintamalleja, kuten kansainvälisesti tunnettua standardia ISO/IEC 27001. Tietoturvallisuuden toteuttaminen riippuu merkittävästi myös organisaation koosta ja muusta toiminnasta; se tulee suhteuttaa toimintaan ja suojattaviin tietoihin.

Asetus velvoittaa rekisterinpitäjää huolehtimaan tietoturvallisuudesta koko henkilötietojen elinkaaren ajan. Seuraavassa on listattu muutamia tyypillisimpiä tietoturvallisuuden osa-alueita, jotka rekisterinpitäjän tulee ottaa huomioon henkilötietoja käsiteltäessä silloin, kun se on perusteltua suhteessa käsittelyyn liittyviin riskeihin.

- **Riskianalyysi**

  Riskianalyysi tietoturvan mitoittamisen apuvälineenä. Asetus velvoittaa rekisterinpitäjää ottamaan huomioon uusimman tekniikan ja toteuttamiskustannukset sekä toisaalta arvioimaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin.

- **Turva-arkkitehtuuri**

  Turvallinen verkko- ja järjestelmäarkkitehtuuri sisältäen esimerkiksi asianmukaiset palomuurit, verkkojen eriyttämisen, palvelinten kovennukset sekä henkilötietojen ja tietojen siirtoväylien salaamisen.

- **Tietojärjestelmien hankinta, kehitys ja ylläpito**

  Tietoturvavaatimusten määrittäminen hankintaa ja kehitystä varten. Henkilötietojen käytön rajoittaminen tietojärjestelmien testauksessa. Tietoturvatestauksen suorittaminen järjestelmien hyväksyntätestauksen yhteydessä. Henkilötietoja käsittelevien järjestelmien ylläpitohenkilöstön sijainnin huomioiminen.

- **Pääsynhallinta**

  Pääsyn rajaaminen ja pääsyoikeuksien hallinta. Pääsynhallinnassa tulee ottaa huomioon myös etäyhteydet EU:n tai Euroopan talousalueen ulkopuolelta, sillä etäyhteyden ottaminen rinnastetaan henkilötietojen siirtoon, mikäli toimenpiteessä käsitellään henkilötietoja.

- **Omaisuuden ja tiedon hallinta**

  Tietovälineiden käsittely sekä tiedon luokittelu ja luokitellun tiedon käsittelyohjeistukset. Henkilöstölle tulee olla selvää, miten henkilötietoja on sallittua käsitellä esimerkiksi pilvipalveluun tallentamisessa, sähköpostilla siirtämisessä ja siirrettäville tietovälineille tallentamisessa. Valtionhallinnossa suojaustasot (IV – III – II – I) määräävät tiedon luokittelua ja käsittelyä.

- **Päivitysten ja muutosten hallinta**

  Ohjelmistokomponenttien haavoittuvuuksien saatavilla olevien päivitysten seuranta ja hallinta (CERT-ryhmät). Järjestelmien tietoturvallisuudesta huolehtiminen päivitysten ja muutosten yhteydessä. Muutosten hallinnasta ja jäljitettävyydestä huolehtiminen.

- **Fyysinen turvallisuus**

  Tilaturvallisuudesta huolehtiminen tarvittavin pääsykontrollein ja -rajauksin. Tietovälineiden, joilla henkilötietoja käsitellään, turvallinen huolto ja hävittäminen, jotta henkilötietoja ei päädy luvattomasti kolmansille osapuolille.

- **Henkilöstöturvallisuus**

  Henkilöstön tietoturvatietoisuuden ja osaamisen varmistaminen koulutuksilla ja ohjeilla. Vaitiolo- ja salassapitosopimukset henkilöstön sekä alihankkijoiden kanssa. Tarvittaessa ja lain mahdollistaessa tehtävät henkilöiden turvallisuusselvitykset.

- **Toimittajien ja sopimusten hallinta**

  Tietoturva- ja tietosuojavaatimusten määrittely sopimuksen/hankinnan kohteelle ja alihankkijoille. Sovittava tietoturvan ja tietosuojan hallinnan menettelyt, mukaan lukien henkilötietojen käsittelyn seuranta ja valvonta sekä tietoturvaraportointi ja tietoturvapoikkeamien hallinta.

- **Toiminnan jatkuvuuden hallinta**

  Henkilötietojen varmuuskopioinnista huolehtiminen ja niitä käsittelevien järjestelmien kapasiteetin hallinta. Tarvittavat suunnitelmat epäsuotuisiin tilanteisiin ja niistä toipumiseen, jotta voidaan taata henkilötietojen saatavuus esimerkiksi teknisen vian sattuessa.

- **Käsittelyn valvonta ja seuranta**

  Rekisterinpitäjän tulee voida jälkikäteen todentaa lokitiedostoista, kuka on suorittanut henkilötietojen haun järjestelmästä, mitä henkilötietoja on katsottu, muutettu, lisätty tai poistettu sekä milloin toimenpide on suoritettu (aikaleima). Menettelyt, joilla lokitiedostoja seurataan ja miten epäillyt väärinkäytökset käsitellään, tulee suunnitella etukäteen. Tärkeää on myös varmistaa, että tietojen käsittelyn seuranta- ja valvontatehtävät ovat selkeästi vastuutettu ja riittävästi resursoidut. Myös mahdolliset seuraamukset henkilötietojen väärinkäytöksistä olisi hyvä kartoittaa ja määritellä etukäteen. Rekisteröityjen viestinnän osana olisi syytä viestiä myös tietojen käsittelyn seurannasta ja mahdollisten väärinkäytösten seuraamuksista. Seurantaa on mah-

dollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon. Poikkeamien hallintaa käsitellään tarkemmin kappaleessa 5.6.

- **Tietoturvallisuuden hallinta**

  Tietoturva-organisaation määrittäminen, roolit ja vastuut sisältäen henkilöstölle määriteltävät tietoturvavastuut. Tietoturvan hallintatehtävien määrittäminen vuosikelloon. Tietoturvan säännöllinen mittaaminen, todentaminen ja kehittäminen. Tietoturvaa voidaan todentaa esimerkiksi teknisellä testauksella ja hallinnollisten prosessien auditoimisella.

5.6 Poikkeamien hallinta ja ilmoitusvelvollisuus

Yksi asetuksen uusista rekisterinpitäjän velvollisuuksista on ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista. Ilmoitusvelvollisuus kohdistuu sekä rekisteröityihin, mikä käsitellään tämän raportin kappaleessa 4.7, että valvontaviranomaiseen. Rekisterinpitäjän tulee tehdä ilmoitus valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa siitä, kun loukkaus on havaittu.

Valvontaviranomaiselle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa listatut kohdat. Ilmoitukselle on suositeltavaa laatia pohja osaksi rekisterinpitäjän kriisiviestintää sekä muutenkin ilmoitusvelvollisuus on huomioitava organisaation kriisi- ja häiriötilanneviestinnässä niin prosessin kuin ohjeistuksen osalta.

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

Jos ilmoitusta valvontaviranomaiselle ei ole mahdollista antaa tehdä 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta, on rekisterinpitäjän kuitenkin toimitettava tässä ajassa liitettävä ilmoitukseensa perusteltu selvitys viivästyksen syistä valvontaviranomaiselle. Tarvittaessa tietoja voidaan antaa vaiheittain.

Täyttääkseen ilmoitusvelvollisuuden sekä rekisteröidyille että valvontaviranomaiselle, rekisterinpitäjällä tulee olla kyvykkyys

- Havaita poikkeamat ympäristössään. Poikkeama voi eskaloitua henkilötietojen tietoturvaloukkaukseksi. Havainnointikyvykkyyden rakentaminen tulee aloittaa työasema- ja järjestelmäympäristön dokumentoinnilla ja valvonnan suunnittelulla. Valvontaa voi suorittaa esimerkiksi tietoturvatapahtumien havainnointiohjelmistolla, ns. SIEM-järjestelmällä (Security Information and Event Management, jolla voidaan keskitetysti kerätä ja analysoida mm. palomuurien, hakemistopalvelun ja tietoturvaohjelmistojen tapahtumia sekä työasema- ja palvelinlokeja). Rekisterinpitäjä voi hoitaa valvonnan itse, mutta tämä vaatii resursseja ja osaamista. Myös henkilöstön tulee olla tietoinen siitä, millaisia poikkeamatilanteita heidän tulee pystyä havainnoimaan työtehtävissään ja miten niistä raportoidaan eteenpäin.
- Selvittää havaitun poikkeaman syyt ja seuraukset sekä vaikutukset yksityisyydensuojaan ja eristää poikkeaman leviäminen asianmukaisilla hallintatoimenpiteillä, jotta tilanteesta voidaan toipua. Rekisterinpitäjän kannattaa varmistaa tarvittaessa ulkopuolista avuna saaminen, erityisesti laajavaikutteisissa poikkeamissa. Rekisterinpitäjän tulee myös dokumentoida tutkintaan ja

toipumiseen tehdyt toimenpiteet sekä huolehtia tarvittavien todistusaineistojen säilyttämisestä. Valvontaviranomainen voi pyytää dokumentaatiota auditoitavaksi.

- Analysoida, onko tarvetta asetuksen mukaisille ilmoituksille. Mikäli on, ilmoittaa sekä valvontaviranomaiselle että niille rekisteröidyille, joiden yksityisyyden suoja on vaarantunut. Rekisterinpitäjän on suositeltavaa laatia viestintäpohjat ja sisällyttää ne osaksi kriisiviestintää.
- Tilanteen ratkeamisen jälkeen tunnistaa tarvittavat muutokset ja kehitystoimenpiteet sekä huolehtia dokumentaation ja todisteiden säilyttämisestä.
- Tehdä tietoturvapoikkeamasta ilmoitus Viestintävirastossa toimivalle Kyberturvallisuuskeskukselle sekä tehdä tutkintapyyntö poliisille.

Edellä mainittujen tehtävien suorittamiseksi tarvitaan prosessimäärittely, johon kuuluvat selkeät roolit ja vastuut. Tyypillisesti prosessi integroidaan osaksi tapahtumien hallintaa. Mikäli rekisterinpitäjä ei hallinnoi työasema- ja järjestelmäympäristöä itse, tulee poikkeamien hallinta ja ilmoitusvelvollisuus sisällyttää toimittajasopimuksiin. Myös tällöin tarvitaan prosessimäärittely jossa kuvataan millaisista tilanteista ilmoitetaan rekisterinpitäjälle, mitä kanavia käyttäen ja miten tilanteen selvittämiseen ja ilmoitusvelvollisuuden täyttämiseen liittyvät vastuut jakautuvat.

5.7 Dokumentaatio, politiikat ja ohjeistukset

On suositeltavaa laatia johdon määrittelemä tietosuojapolitiikka tai muu vastaava asiakirja, joka kuvaa organisaation henkilötietojen käsittelyn perusperiaatteet ja tietosuojan merkityksen organisaatiolle. Tietosuojapolitiikka on ylin tietosuojaa ohjaava dokumentti organisaatiossa. Kaiken henkilötietojen käsittelyn tulee olla sekä lainsäädännön että tietosuojapolitiikan mukaista.

Rekisterinpitäjän tulee huolehtia myös siitä, että henkilötietoja käsitteleviä rooleja hoitavat henkilöt ovat asianmukaisesti koulutettuja. Tähän liittyy sellaisen tarvittavan ohjeistuksen laatiminen, jossa kuvataan, millainen henkilötietojen käsittely kuuluu roolin tehtävänkuvaan. Ohjeistuksen tulee olla henkilöstölle vapaasti saatavilla. Henkilöstön tietoisuutta voidaan parantaa ja ylläpitää tietosuojakoulutuksilla, joita käsitellään myöhemmin tässä raportissa. Rekisterinpitäjän on huolehdittava, että myös tietojen käsittelijällä ja rekisteripitäjän henkilötietojen käsittelyyn osallistuvilla henkilöillä on riittävä tietosuojaosaaminen. Lisäksi rekisterinpitäjän on tarpeen mukaan ohjeistettava myös henkilötietojen käsittelijän henkilöitä, jotka voivat olla esimerkiksi palveluita tuottavan organisaation asiantuntijoita.

Mikäli rekisterinpitäjällä on velvollisuus nimittää tietosuojavastaava, kuuluu asianmukaisen dokumentaation olemassaolon ja saatavuuden varmistaminen tietosuojavastaavan tehtäväkuvaan. Mikäli velvoitetta ei ole, tulee dokumentaatiosta huolehtiminen velvoittaa muille sopiville rooleille organisaatiossa.

Rekisterinpitäjän tulee huolehtia asianmukaisesta tietosuojadokumentaatiosta osana rekisterinpitäjän osoitusvelvollisuuden toteutumista. Ajantasaisen dokumentaation toimittaminen esimerkiksi valvontaviranomaisen pyynnöstä auditointitarkoituksiin on hyvä keino osoittaa, että tietosuojasta on huolehdittu asianmukaisella tavalla.

Käytännössä dokumentaatio (”tietosuojan hallintajärjestelmän”) voi sisältää esimerkiksi seuraavia asioita:

- tietosuojapolitiikka
- tietosuojaorganisaatio, -roolit ja -vastuut
- tietosuojaselosteet
- rekisterien tietovirta/vuokuvaukset
- kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyistä prosesseista
- tehdyt tietosuojan riski- ja vaikutustenarvioinnit hallintakeinoineen
- tietosuojaa ja tietoturvaa käsittelevien foorumeiden ja ohjausryhmien pöytäkirjat
- riskirekisterit ja kirjanpito riskien hyväksymisestä ja omistajuudesta
- tietoturvatestauksen tulokset
- kuvaukset prosesseista, joilla taataan sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen
- henkilötietoja käsittelevälle henkilöstölle suunnattavat ohjeet
- dokumentaatio mahdollisista henkilötietojen käsittelyssä tapahtuneista loukkauksista
- tietotilinpäätös (keinona toteuttaa osoitusvelvollisuus).

Tässä tulee korostaa sitä, että kaikki toimintamallit ja prosessit tulee suhteuttaa esimerkiksi organisaation kokoon sekä henkilötietojen käsittelytarpeen määrään. Erot korostuvat etenkin siirryttäessä julkishallinnon organisaatioista yrityksiin, joissa pienimmillään yhden hengen yrityksessä henkilötietoja käsitellään sisäisesti organisaation oman henkilöstön (omistaja) lisäksi esimerkiksi yhdessä asiakasrekisterissä.

5.8 Rekisterinpitäjän ja käsittelijän väliset sopimukset

5.8.1 Sopimusten ja alihankkijoiden hallinta

Rekisterinpitäjä on oikeutettu ulkoistamaan valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Tietosuoja-asetus selkiyttää rekisterinpitäjän ja käsittelijän välistä sääntelyä sekä osoittaa velvollisuuksia myös suoraan käsittelijälle. Rekisterinpitäjän velvollisuuksiin kuuluu valita vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on oltava sopimus, jonka olisi syytä olla kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Lisäksi tulee varmistaa, että henkilötietojen käsittelijä:

- Käsittelee henkilötietoja ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Tähän sisältyy myös henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit
- Noudattaa salassapitovelvollisuutta

- Toteuttaa tietoturvallisuuden henkilötietojen käsittelyssä tietosuoja-asetuksen vaatimilla toimenpiteillä
- Ei ulkoista henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta
- Auttaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa
- Auttaa rekisterinpitäjää käsittelyn tietoturvallisuuden toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa sekä vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa tietosuoja-asetuksen mukaisesti.
- Joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle käsittelypalvelujen päättyessä. Käsittelijän tulee myös poistaa niistä hallussaan olevat kopiot.
- Sallii rekisterinpitäjän suorittaa auditoinnit ja osallistuu niihin itse. Käsittelijän tulee myös saattaa rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen asetuksen velvollisuuksien noudattamisen osoittamista varten. Lisäksi on syytä erikseen miettiä ja sopia eli ilmoittaa rekisterinpitäjälle, mikäli sen ohjeistus rikkoo asetuksen säännöksiä.

Lisäksi organisaation tulee osana turvallisuussopimusta harkita seuraavaa:

- Sitoutumista siihen, että henkilötietojen käsittelyä suorittavat vain sellaiset henkilöt, jotka ovat saaneet hyväksyttävän tuloksen turvallisuusselvityksessä, jos rekisterinpitäjällä on lainmukainen oikeus teettää turvallisuusselvityksiä ja jos rekisterinpitäjä selvitysten teettämistä käsittelijältä vaatii.

Edellä esitettyjen sopimusvaatimusten ohella on suositeltavaa määritellä, miten henkilötietojen käsittelijän palvelun laatua seurataan. Voidaan esimerkiksi määritellä tietosuojan ja tietoturvan säännöllisen raportoinnin käytännöt ja järjestää säännöllinen rekisterinpitäjän ja käsittelijän välinen palaveri, jossa seurataan tietosuojan ja tietoturvan toteutumista henkilötietojen käsittelyssä.

Rekisterinpitäjän tulee pitää kirjaa kaikista henkilötietojen käsittelytoimista. Tähän velvollisuuteen kuuluu olennaisena osana tieto kaikista henkilötietojen käsittelijöistä, joille käsittelytoimia on ulkoistettu sekä inventaario kyseisten käsittelijöiden kanssa tehdyistä sopimuksista. Sopimusvaatimuksia tulee hallita ja tarvittaessa tehdä niihin tarkennuksia tai muutoksia esimerkiksi henkilötietojen käsittelyn riskiarvion muuttuessa.

5.8.2 Tiedonsiirto Euroopan talousalueen ulkopuolelle

Henkilötietojen siirron rajoittaminen Euroopan talousalueen (ETA) ulkopuolelle on tuttua jo tietosuoja-asetusta edeltävästä sääntelystä. Tietosuoja-asetus kuitenkin tiukentaa näitä rajoitteita. Asetuksen mukaan henkilötietojen siirto kolmanteen maahan ETA:n ulkopuolelle voidaan toteuttaa, pääsääntöisesti vain jos

- Euroopan komissio on päättänyt kohdemaan tietosuojan riittävyydestä. Tällöin siirrolle ei tarvita erityistä lupaa. Komissio julkaisee verkkosivuillaan, minkä maiden tietosuojan se on katsonut riittäväksi. Esimerkiksi Yhdysvaltojen tietosuojan tämänhetkistä tasoa ei ole katsottu riittäväksi, uutta päätöstä odotetaan kesäkuussa 2016 (tilanne toukokuu 2016).
- sovelletaan asianmukaisia suojatoimia, joita voivat olla esimerkiksi a) yrityksen sisäisiä siirtoja koskevat sitovat säännöt, b) rekisterinpitäjän ja käsittelijän, jonka välillä siirto tehdään, sopimukseen liitetyt komission vakiolausekkeet tai c) valvontaviranomaisen luvalla määritellyt sopimuslausekkeet, d) hyväksytyt käytännesäännöt tai e) sertifiointimekanismit.

Aikaisemmin henkilötietojen siirtoon ETA:sta Yhdysvaltoihin sovellettiin laajalti Safe Harbour -järjestelyä. Lokakuussa 2015 EU:n tuomioistuin kuitenkin katsoi järjestelyn pätemättömäksi Facebook -palvelun henkilötietojen siirtoon ja siitä nostettuun selvityspyyntöön liittyen. EU:n tuomioistuin katsoi, ettei järjestely ota riittävästi huomioon yksityisyyden suojaa.

Tuomioistuimen päätöksen jälkeen Euroopan komissio ja Yhdysvallat ovat työstäneet uutta henkilötietojen siirron järjestelyä tiedonsiirtoihin EU:sta Yhdysvaltioihin. Helmikuussa 2016 Euroopan komissio ja Yhdysvallat pääsivät yhteisymmärrykseen Privacy Shield -sopimuksesta. Parhaillaan työstetään tarvittavia toimenpiteitä, jotta uusi järjestely voidaan ottaa käyttöön.

Privacy Shield -sopimus velvoittaa henkilötietoja Euroopasta siirtäviä yhdysvaltalaisia toimijoita, noudattamaan tietosuojavelvoitteita, joilla taataan yksilön oikeudet ja henkilötietojen eurooppalaista tietosuojaa noudattava käsittely. Yhdysvaltojen kauppaministeriö ja liittovaltion kilpailuviranomainen tulevat tehostamaan velvoitteiden täytäntöönpanoa ja valvontaa. Yhdysvaltalaisten toimijoiden tulee myös noudattaa Euroopan tietosuojaviranomaisten päätöksiä eurooppalaisten henkilötietojen käsittelyssä. Massavalvontaan liittyvien huolien vuoksi Yhdysvallat on sitoutunut varmistamaan, että viranomaisten pääsyyn siirrettyihin eurooppalaisten henkilötietoihin sovelletaan selkeitä ehtoja ja rajoituksia sekä pääsyn valvontaa. Yhdysvallat nimittävät uuden oikeusasiamiehen, jolle eurooppalaisilla on mahdollisuus esittää kysymyksiä tai valituksia viranomaisten henkilötietojen käsittelystä. Myös yksityishenkilöillä on mahdollisuus valittaa Privacy Shield -sopimuksen puitteissa, mikäli he katsovat, että heidän henkilötietojaan on väärinkäytetty. Valitukset voidaan tarvittaessa saattaa Yhdysvaltojen kauppaministeriön ja liittovaltion kilpailuviranomaisen käsiteltäväksi.

Kun Privacy Shield -järjestely otetaan käyttöön, yhdysvaltalaisilla toimijoilla tulee olemaan mahdollisuus rekisteröityä Privacy Shield -listalle. Rekisteröitymiseen vaaditaan toimijan itse suorittama arvio siitä, että se noudattaa Privacy Shield -järjestelyyn liittyviä tietosuojavelvoitteita asianmukaisesti. Yhdysvaltojen kauppaministeriö tulee valvomaan velvoitteiden täytäntöönpanoa. Lista rekisteröityneistä toimijoista tulee julkisesti saataville, ja järjestelyä voidaan käyttää tiedonsiirron perustana.

Koska Privacy Shield sopimuksen viimeistely ja toteutus on vielä kesken, organisaation tulee selvittää sopimuksen tilanne, mikäli se aikoo käyttää tätä perustana henkilötietojen siirron mahdollistamisessa Yhdysvaltoihin. Samoin tulee huomata, että on olemassa erikseen muita sopimuksia, jotka koskevat lentoyhtiöiden matkustajatietojen sekä pankkitapahtumatietojen luovuttamista

5.9 Rekisterinpitäjän yhteistyövelvoite

Rekisterinpitäjällä on velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa valvontaviranomaisen niin pyytäessä. Mikäli rekisterinpitäjällä on nimitetty tietosuojavastaava, kuuluu yhteistyö valvontaviranomaisen kanssa hänen vastuulleen. Mikäli rekisterinpitäjällä on toimintaa useassa EU:n jäsenvaltiossa, voi se asioida päätoimipaikkansa valvontaviranomaisen kanssa.

Valvontaviranomaisen pyynnön ohella rekisterinpitäjän on tehtävä yhteistyötä valvontaviranomaisen kanssa ennakkokuulemisen muodossa, jos tietosuojan vaikutustenarvioinnin perusteella suunniteltuun henkilötietojen käsittelyyn liittyy suuria riskejä, ja rekisterinpitäjällä ei ole keinoja riskitason pienentämiseksi.

Rekisterinpitäjällä on myös ilmoitusvelvollisuus valvontaviranomaiselle henkilötietojen tietoturvaloukkaustilanteissa luvussa 5.6 kuvatulla tavalla. Valvontaviranomainen voi vaatia yhteistyötä tilanteen selvityksen yhteydessä, jotta se voi arvioida rekisterinpitäjän asetuksen velvollisuuksien noudattamista. Henkilötietojen tietomurtotapauksissa rekisterinpitäjän on hyvä tehdä yhteistyötä myös Viestintäviraston kanssa tekemällä ilmoitus tietoturvaloukkauksesta Kyberturvallisuuskeskukselle sekä tehdä tutkintapyyntö poliisille.

5.10 Hallinnolliset sakot ja seuraamukset

Tietosuoja-asetus tuo valvontaviranomaisille uutena oikeuden määrätä rekisterinpitäjälle ja / tai henkilötietojen käsittelijälle sakkoja tai hallinnollisia seuraamuksia tietosuoja-asetuksen velvoitteiden laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella kolmeen luokkaan. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. Niiden tietosuoja-asetuksen vaatimusten laiminlyöntien osalta, joihin ei sovelleta hallinnollisia sakkoja, voi valvontaviranomainen määrä muita varoittavia seuraamuksia. Näitä voivat olla esimerkiksi käsittelyn kieltäminen, kunnes tarvittavat velvollisuudet on täytetty. Valvontaviranomaisella on oikeus auditoida rekisterinpitäjän tietosuojan toteutusta. Suomessa julkishallinnon osalta käytettävä menettely tarkentuu osana lainsäädäntötyön etenemistä.

6 Suosituksia toimenpiteistä

Rekisterinpitäjän kannattaa aloittaa asetuksen voimaantuloon valmistautuminen saman tien. Asetuksen voimaantuloa edeltävä kahden vuoden siirtymäaika on lyhyt mahdollisten puutteiden tunnistamiseksi ja korjaamiseksi jokapäiväisten operatiivisten toimien ohella. Siksi suunnitelmallinen ja ennakoiva lähestymistapa tietosuojan kehittämisessä kannattaa.

Kuva 6. Tarvittavan kokonaisuuden kehittämistä voi jakaa esimerkiksi neljään osa-alueeseen

6.1 Johdon osallistuminen ja tarvittavien resurssien varaaminen

Organisaation johdon osallistuminen ja tuki organisaation tietosuojatyölle on suositeltavista toimenpiteistä ensimmäinen ja yksi tärkeimmistä. Johdon tulisi omistaa organisaation tietosuojatoiminta ja vastata viimekädessä siitä, että tietosuoja toteutuu osana jokapäiväistä toimintaa tietosuojasääntelyn vaatimalla tavalla.

Johdon vastuulla on ohjata tarvittavat resurssit tietosuojan nykytilan arvioimiseksi, valtuuttaa ja mahdollistaa sen pohjalta tunnistettujen kehitystoimenpiteiden toteuttaminen. Tietosuoja on suositeltavaa sisällyttää johdon strategiseen ohjaukseen sisältäen etenkin alkuvaiheessa sen kehittämisen edistymisen raportoinnin ja mahdollisen projektin / hankkeen edistymisen seurannan.

6.2 Tietosuojan nykytila-analyysi ja kehitystoimenpiteet

Tietosuojan nykytila-analyysi tarkoittaa organisaation henkilötietojen käsittelyn ja tietosuojakyvykkyyksien nykytilan arviointia suhteessa tietosuoja-asetuksen vaatimuksiin. Arviointi on hyvä suorittaa osissa esimerkiksi toiminnoittain. Arvioon tulee sisällyttää erityisesti rekisteröityjen oikeuksien ja riskilähtöisyyden toteutuminen. Arvioinnin perusteella voidaan tunnistaa puutteet ja kehityskohteet sekä suunnitella toimenpiteet, joilla nykytilaa voidaan parantaa ja huolehtia tietosuojan toteutumisesta osana jokapäiväistä operatiivista toimintaa.

Kehitystoimenpiteet on suositeltavaa priorisoida niiden kriittisyyden mukaisesti sekä asettaa aikajanalle niin, että organisaation resurssit riittävät niiden toteuttamiseen. Kehitystehtävien edistymistä tulee myös seurata ja tarvittaessa puuttua havaittuihin ongelmiin. Tarvittaessa nykytilan arviointiin sekä kehitystoimenpiteiden määrittelyyn ja toteutukseen voi hakea ulkopuolista apua. Organisaation omien resurssien riittävyys kannattaa arvioida nykytila-analyysin suunnittelun yhteydessä.

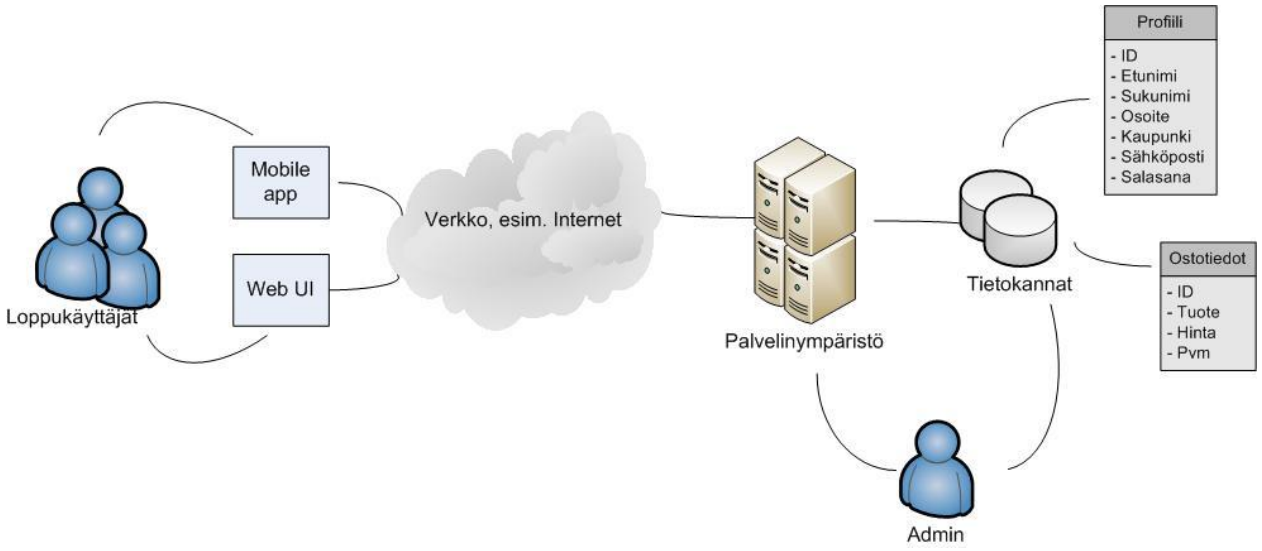
6.2.1 Henkilötieto- ja sopimusinventaario

Tärkeänä osana nykytila-analyysia tulee selvittää organisaation keräämien ja käsittelemien henkilötietojen kokonaiskuva. On syytä tehdä käsiteltävien henkilötietojen inventaario sekä tunnistaa missä ja kenen toimesta henkilötietoja käsitellään. Henkilötietoja käsittelevät kolmannet osapuolet tulee tunnistaa, arvioida sopimusten tietosuojavaatimukset ja huolehtia, että henkilötietojen siirtoihin Euroopan talousalueen ulkopuolelle on riittävät lailliset perusteet.

Myös sopimusten tietoturvavaatimukset henkilötietojen suojaamisen näkökulmasta tulee arvioida. Voimassaoleviin henkilötietojen käsittelysopimuksiin tulee viedä asetuksen vaatimukset erillisenä liitteenä tai uutena sopimuksena. Rekisterinpitäjän kannattaa myös tarkastella, miten sen hankintaprosessi ja projektinhallintamalli huomioivat tietosuojan. Myös sopimuspohjat kannattaa uusia asetuksen vaatimuksia vastaaviksi.

Henkilötieto- ja sopimusinventaario on helpointa selvittää mallintamalla henkilötietojen tietovirrat/vuot rekistereittäin. Tietovirran (kuva 7.) tulee kuvata käsiteltävät henkilötietotyypit, mistä henkilötiedot tulevat, henkilötietoja käsittelevät sovellukset, järjestelmät ja roolit sekä miten henkilötiedot liikkuvat niiden välillä, käsittelyyn liittyvät fyysiset sijainnit sekä luovutetaanko tai siirretäänkö henkilötietoja edelleen kolmansille osapuolille sekä kuinka kauan henkilötietoja käsitellään ja kuinka ne tullaan hävittämään.

Kun käsittelyyn osallistuvat kolmannet osapuolet on selvitetty, voidaan edetä sopimusvaatimusten kartoittamiseen ja arviointiin. Tietovirtojen dokumentoinnin jälkeen organisaatiolla on kattava yleiskuva henkilötietojen käsittelystä. Samalla voidaan tarkistaa, ovatko rekisteriselosteet ja muu rekisteröidyille suunnattava viestintä käsittelytoimista ajan tasalla. Dokumentaatio on tarpeen myös osoitusvelvollisuuden näkökulmasta.



Kuva 7. Yksinkertaistettu esimerkki tietovirrasta (tietovuo).

6.2.2 Riskiarvio

Kun henkilötietojen käyttötarkoitukset, henkilötietoja käsittelevät sovellukset ja järjestelmät sekä henkilötietojen siirtotilanteet ovat selvillä, on suositeltavaa suorittaa riskianalyysi, jotta tarvittavat hallintatoimenpiteet voidaan tunnistaa ja mitoittaa. Selvitä onko tietoturvan toteutus riittävällä tasolla henkilötietojen koko elin-

kaaren ajan. Riskiarvioon tulee sisällyttää myös meneillään olevien tietojärjestelmähankkeiden uudelleen arviointi.

6.2.3 Tietosuojavastuut

Selvitä onko organisaatiollasi velvollisuutta nimittää tietosuojavastaava. Nimitä tietosuojavastaava tarvittaessa ja huolehdi siitä, että hänellä on riittävä osaaminen ja toimivalta tehtävänsä hoitamiseen mahdollisimman riippumattomasti. Arvioi mihin tietosuojavastaavan on hyvä sijoittua organisaatiossa riippumattomuuden takaamiseksi.

Tietosuojavastaavan toimenkuvan hallitsemiseksi ja tehtävien hoidon helpottamiseksi on suositeltavaa laatia tietosuojavastaavan tehtäväluettelo (tehtäväkuvaus). Tehtäväluettelon avulla tietosuojavastaava voi määritellä, aikatauluttaa ja seurata toimenkuvaan kuuluvia rutiinitehtäviä sekä varata riittävästi aikaa myös jokapäiväiselle vaihtelevalle tietosuojatoiminnalle, johon voi kuulua esimerkiksi erilaisten tietosuojahaasteiden ratkaisua ja organisaation neuvontaa tietosuojakysymyksissä.

Henkilötietojen omistajuus ja käsittely on tyypillisesti hajautunut useaan organisaation yksikköön. Tunnista henkilötietojen käsittelyä suorittavat yksiköt ja muut yksiköt, jotka ovat olennaisia tietosuojan toteutumisen kannalta. Valitse näistä yksiköistä sopivat roolit, jotka muodostavat tietosuojaorganisaation. Määrittele millaisia tehtäviä tietosuojaorganisaatio toteuttaa ja mitä heidän vastuulleen kuuluu. Määrämuotoiset tehtävät on hyvä ryhmitellä tietosuojan vuosikelloon.

Tietosuojaorganisaation nimeämisestä ja toiminnan aloittamisesta on hyvä tiedottaa koko organisaatiota ja tarvittavia sidosryhmiä.

6.2.4 Johdon raportointi

Johdon tietoisuus organisaation tietosuojan nykytilasta on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Nimettävän tietosuojavastaavan tai muun tietosuojaorganisaation jäsenen vastuulle on hyvä osoittaa sekä johdon säännöllinen raportointi että vuosiraportin laatiminen.

Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät asiat.

Niitä voivat olla esimerkiksi

- tietosuojamittarit sisältäen niiden käytön raportointikauden aikana,
- tietosuojan kehityshankkeet ja niiden tilanne,
- havaitut puutteet ja tarpeet,
- merkittävimmät tietoturvaloukkaukset, joilla on ollut tietosuojavaikutuksia,
- tehdyt riski- ja vaikutustenarvioinnit sekä niiden merkittävimmät löydökset hallintakeinoineen sekä
- rekisteröityjen oikeuksiin ja yhteistyöhön valvontaviranomaisen kanssa liittyvät tarpeelliset tiedot.

Johdon vuosiraportti voi olla esimerkiksi tietotilinpäätös. Tietotilinpäätös antaa kokonaiskuvan organisaation henkilötietojen käsittelyn ja tietosuojan nykytilasta. Sen avulla johto voi valvoa ja arvioida nykytilaa sekä ohjata resursseja sen kehittämiseen. Tietotilinpäätöksestä ja sen laatimisesta löytyy lisätietoja tietosuojavaltuutetun sivuilla:

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf

6.2.5 Henkilöstön koulutukset ja ohjeet

Huolehdi henkilöstösi riittävästä tietosuoja- ja tietoturvaosaamisesta sekä ohjeistuksesta, erityisesti niissä rooleissa, jotka käsittelevät henkilötietoja ja osallistuvat rekisteröidyn oikeuksien toteuttamiseen luotuihin prosesseihin esimerkiksi tarkastusoikeuden osalta. Selvitä vastaavatko organisaatiosi tietosuojakoulutukset tietosuoja-asetuksen myötä muuttuvaa sääntelyä.

Arvioi myös organisaatiosi tarpeet syventävään, rooliperusteiseen tietosuojakoulutukseen. Tällaisia rooleja voi olla esimerkiksi asiakaspalvelussa, kehitystyössä ja palveluntuotannossa. Organisoi päivitetty tietosuojan tietoisuuskoulutus koko organisaatiolle.

6.2.6 Viestintä ja dokumentaatio

Huolehdi, että henkilötietojen käsittelystä on ajantasaiset ja asianmukaiset kuvaukset tietosuojaselosteissa ja muissa käytössä olevissa viestintäkanavissa, esimerkiksi internet-sivuilla. Varmista organisaatiosi kriisiviestintäsuunnitelmasta, huomioidaanko tietosuojaloukkaukset asetuksen vaatimalla tavalla. Laadi kriisiviestintäpohjat rekisteröidyille ja valvontaviranomaiselle tietosuojaloukkaustilanteisiin. Huolehdi, että kappaleessa 5.7.1. esitellyt dokumentit ovat olemassa, ajantasaisia ja asianmukaisesti tarvittavien henkilöiden saatavilla.

Huolehdi myös, että rekisteröidyille lähtevät ilmoitukset ovat riittävän selkeitä ja yksinkertaisia tietoturvaloukkauksen tapahtuessa. Ilmoituksissa valvontaviranomaiselle ja rekisteröidyille on vähintään

- kuvattava henkilötietojen tietoturvaloukkausten luonne ja todennäköiset seuraukset,
- kuvattava toimenpiteet, joihin rekisterinpitäjä on ryhtynyt / tulee ryhtymään tietoturvaloukkauksen takia, ja tarvittaessa myös toimenpiteet haittavaikutusten lieventämiseksi
- ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoja

Valvontaviranomaiselle on kerrottava lisäksi loukkauksen kohteena olleiden rekisteröityjen ryhmät ja henkilötietotyypit sekä arvioidut lukumäärät.

6.2.7 Asetuksen huomioiminen meneillään olevissa järjestelmähankkeissa sekä sovelluskehityksessä

Asetus edellyttää, että organisaatiolla on velvollisuus järjestää tietojenkäsittely tavalla, jonka avulla asetus, tietosuojaperiaatteet ja rekisteröidyn oikeudet tulevat tehokkaasti huomioiduiksi kaikessa tietojenkäsittelyssä. Tämä tulee huomioida myös sovelluskehityksessä.

Organisaation tulisi kiinnittää huomiota erityisesti meneillään olevissa järjestelmähankkeissa siihen, että niissä otetaan kahden vuoden siirtymäkauden aikana huomioon kaikki tarvittavat muutokset. Tämä saattaa edellyttää asioiden erillistä sopimista ja tarvittavien muutoshallintaan liittyvien asioiden sopimista toimittajan kanssa. Muutoin vaarana on, että kehitettävä uusi palvelu ei täytä lainsäädännön vaatimuksia. Kokonaisuuteen vaikuttaa olennaisesti se, missä roolissa eri osapuolet hankkeessa toimivat ja miten vastuut eri toimijoiden osalta jakautuvat.

Käytännössä organisaation tulisi miettiä, mitä muutos edellyttää yleensä sovelluskehityksessä. Alla muutamia esimerkkejä järjestelmä- ja sovelluskehityksessä huomioitavista asioista:

- lasten tietosuojaan liittyvä kohta, kuinka kysytään vanhempien suostumus lasten osalta
- kuinka ylipäänsä pyydetään käyttäjän suostumusta
- kuinka varaudutaan siihen, että palvelusta pitää pystyä siirtämään tiedot toiseen järjestelmään silloin, kun se on sallittua (rekisteröidyn suostumukseen tai sopimukseen perustuva käsittely ja rekisteröidyn itsensä antama tai tuottama tieto)
- kuinka varaudutaan siihen, kun käyttäjä haluaa tietonsa poistettavan
- miten varaudutaan tietosuojaloukkausten raportointiin?

6.2.8 Uusien järjestelmähankkeiden osalta hankinnoissa edellytettävät vaatimusmääritykset

Organisaation tulisi varmistaa se, miten se huolehtii tarvittavien vaatimusten sisällyttämisestä vaatimusmäärittelyihin siirtymäkauden aikana uusien järjestelmähankkeiden tai muiden kilpailutusten yhteydessä käytettävissä tarjouspyynnöissä. Tämä on erityisen tärkeää kahden vuoden siirtymäkauden aikana, koska sen jälkeen käytännössä jokaisen organisaation, käytettävien palveluiden ja muun henkilötietojen käsittelyn tulisi olla vaatimusten mukaisia.

Mikäli nämä jatkossa edellyttävät muutokset koskevat ja edellyttävät palvelutuotannossa olevaa laajaa käyttöympäristöä, tulee muutosten toteuttamiseen varata riittävästi aikaa sekä resursseja.

6.2.9 Riskienhallinnan kehittäminen

Jos organisaatiolla ei ole ollut aikaisemmin käytössä riskienhallintamallia, sellaisen käyttöönottoon tulee varautua:

35 artiklassa todetaan:

”Jos tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle. Yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin.”

Edellä tarkoitettu tietosuojaa koskeva vaikutustenarviointi vaaditaan erityisesti tapauksissa joissa:

”a) luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin, joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi;

b) laajamittainen käsittely, joka kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin; tai

c) yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti.”

VAHTI tulee päivittämään olemassa olevan VAHTIn riskienhallintaohjeen ja mallin vuoden 2016 aikana siten, että sitä voidaan hyödyntää myös tietosuojaan liittyvien riskien arvioinnissa.

6.2.10 Tarkista ja päivitä rekisteriselosteet sekä varmista tietojenluovutusten oikeellisuus

Osana tietojärjestelmien ja sopimusten läpikäyntiä (kohta 6.2.1) on syytä tarkistaa ja päivittää rekisteriselosteet ajan tasalle sekä varmistaa, mitä henkilötietojen luovuttamisesta etenkin ETA-alueen ulkopuolelle on sovittu. Lisäksi tulee varmistaa, että tämä on huomioitu myös toimittajan kanssa tehdyssä sopimuksessa.

6.2.11 Huolehdi tietoturvallisuudesta ja toiminnan jatkuvuudesta

Asetuksen 32 artikla nostaa esille seuraavat asiat tietoturvallisuudesta ja toiminnan jatkuvuudesta:

”Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.”

Tässä tulee huomata erityisesti kohdassa b esille nostettu käytettävyys ja erikseen vikasietoisuus. Kahden vuoden siirtymäkauden aikana saataneen tarkempia määrityksiä siitä, mitä tietoturvallisuudelta edellytetään. Valtionhallinnossa vuonna 2010 voimaan astunut tietoturvallisuusasetus sisältää todennäköisesti riittävät periaatteet tarvittavan tietoturvallisuuden toteuttamisesta.

6.3 Kehittämisprojektin asettaminen

Kuten tästä raportista käy ilmi, edellyttää tietosuojaan liittyvien uusien vaatimusten toteuttaminen ja toiminnan kehittäminen jokaiselta organisaatiolta toimenpiteitä. Toteutettavan kokonaisuuden tarvittavan muutoksen laajuuteen, haastavuuteen ja kestoon vaikuttavat muun muassa seuraavat tekijät:

- johdon tuki ja ymmärrys
    - mitä paremmin organisaation johto on tietoinen kokonaisuudesta ja sitoutunut sen johtamiseen, tukemiseen ja toteuttamiseen, sitä helpompi projekti on viedä läpi
- organisaation koko
    - esimerkiksi koulutus, tiedottaminen ja päätöksenteon nopeus ja joustavuus
- organisaation toimiala sekä käsiteltävien henkilötietojen sekä tietojärjestelmien määrä
    - onko henkilötietojen käsittely vain organisaation oman henkilöstön tarpeista lähtevää vai onko se organisaation ydin- tai liiketoimintaa; onko tietojärjestelmiä muutama vai kymmeniä, kenties satoja - kuinka paljon näissä tietojärjestelmissä on henkilötietoja
    - palveluiden tuottamistapa; jos organisaatio vastaa itse kaikesta, on kokonaisuuden hallinta helpompaa kuin tilanteessa, jossa organisaatio on ulkoistanut toimintaa useille eri tahoille, jotka mahdollisesti käyttävät lukuisia muita alihankkijoita osana omaa toimintaansa
- olemassa oleva tietosuojaosaaminen ja -resurssit
    - mitä enemmän ja pitempään organisaatiossa on tehty tietosuojatyötä, sitä helpompaa on toteuttaa uuden lainsäädännön edellyttämät muutokset toimintaan.
- toiminnan prosessimuotoisuus
    - mitä enemmän henkilötietojen käsittely tapahtuu prosessimaisesti tai osana muita prosesseja, sitä helpompi näitä toiminnassa olevia prosesseja on päivittää verrattuna siihen, että sellaiset joudutaan nyt kuvaamaan, kouluttamaan ja ottamaan käyttöön kokonaan uusina asioina

Koska aikaa tarvittavien muutosten tekemiseen on toukokuuhun 2018 saakka, suosittelemme organisaatiota asettamaan tätä varten kehittämisprojektin. Julkaisemme tätä tukevan erillisen Excel-työkalutaulukon, johon olemme koonneet tästä raportista keskeisiä toimenpiteitä, jotka organisaation tulisi projektin aikana selvittää ja toteuttaa.

6.4 Asetuksen soveltamisohjeiden seuraaminen

Tietosuoja-asetus tulee olemaan suoraan sovellettavaa lainsäädäntöä kaikissa EU:n jäsenvaltioissa. Asetus antaa kuitenkin kansallista liikkumavaraa joissakin asioissa, erityisesti julkisella sektorilla, mikä tullaan huomioimaan Suomen lainsäädännössä. Oikeusministeriö valmistelee näitä lainsäädäntötoimia Suomessa. EU:n tasolla Euroopan tietosuojaneuvostolla tulee olemaan mahdollisuus antaa jäsenvaltioita sitovia asetuksen soveltamisohjeita. Kansallinen valvontaviranomainen voi julkistaa ohjeistusta esimerkiksi siitä, missä tilanteissa tietosuojan vaikutustenarviointi tulee tehdä. Näin ollen oikeusministeriön, valvontaviranomaisten (tällä hetkellä Tietosuojavaltuutetun toimisto, Viestintävirasto) ja Euroopan tietosuojaneuvoston viestintää on suositeltavaa seurata samoin kuin aikanaan tulevaa EU-tason ja kansallisen tason oikeuskäytäntöä, esimerkiksi ennakkopäätöksiä.

7 Lähteet

Tietosuoja-asetus:
http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN

http://www.consilium.europa.eu/fi/policies/data-protection-reform/data-protection-regulation/

Safe Harbour –päätös:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

EU:n ja Yhdysvaltojen välinen Privacy Shield –järjestely:
http://europa.eu/rapid/press-release_IP-16-433_fi.htm

http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

Lisätietoa, muun muassa sanastoa ja muuta täydentävää materiaalia löytyy Tietosuojavaltuutetun toimiston sivulta osoitteesta http://www.tietosuoja.fi/text/fi/index/euntietosuojauudistus.html