



VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Jari Öljymäki
EU:n TIETOSUOJAUDISTUS

Liiketalous
2017

TIIVISTELMÄ

Tekijä	Jari Öljymäki
Opinnäytetyön nimi	EU:n Tietosuojauudistus
Vuosi	2017
Kieli	suomi
Sivumäärä	86
Ohjaaja	Marika Teirfolk-Naarmala

Tämän opinnäytetyön aiheena on Euroopan unionin tietosuojauudistus, jonka valmistelu aloitettiin jo vuonna 2010, tarkoituksena yhtenäistää ja päivittää henkilötietojen käsittelyä koskeva tietosuoja-lainsäädäntö EU:n alueella ja parantaa rekisteröityjen oikeuksia rekisterinpitäjien vastuuvollisuutta lisäämällä. Uusi yleinen tietosuoja-asetus ja direktiivi ovat olleet voimassa vuoden 2016 toukokuusta lähtien ja niitä on sovellettava EU:n jäsenvaltioiden kansallisiin lakeihin kahden vuoden siirtymäajan jälkeen toukokuussa vuodesta 2018.

Opinnäytetyössä keskitytään EU:n tietosuojauudistuksen sisältöön, yleiseen tietosuoja-asetukseen (EU) 2016/679 ja tietosuojadirektiiviin (EU) 2016/680, ja vertaillaan niiden säännöksiä tietosuoja-uudistusta edeltäneeseen EU-lainsäädäntöön ja Suomessa voimassa olevaan henkilötietolakiin. Opinnäytetyön tutkimusmenetelmä on lainopillinen ja tutkimusongelmana työssä käsitellään, miten Suomi on valmistautunut EU:n yleisen tietosuoja-asetuksen soveltamiseen kansallisessa lainsäädännössään. Pääasiallisina lähteinä ovat EU:n viralliset asiakirjat ja lainsäädäntö, kansallinen lainsäädäntö, sekä oikeusministeriön ja tietosuojavaltuutetun toimiston viralliset asiakirjat ja verkkosivut.

EU:n tietosuojauudistus tulee yhtenäistämään EU:n kaikkien jäsenvaltioiden tietosuojakäytännöt EU:n kansalaisia ja yrityksiä palvelevaksi ajanmukaiseksi, vahvaksi ja kattavaksi kokonaisuudeksi, ja näin myös edistämään EU:n digitaalista sisämarkkinoiden kehitystä. Suomen valmius soveltaa EU:n tietosuojauudistus omaan kansalliseen lainsäädäntöönsä vuoden 2018 keväällä on hyvällä tasolla. Valmistelutyö oikeusministeriössä ja tietosuojasta vastuussa olevissa sidosryhmissä on käynnissä kansallisen tietosuojalainsäädännön saattamiseksi EU:n lainsäädännön mukaiseksi.

Avainsanat: EU, tietosuoja, uudistus, lainsäädäntö, henkilötieto, oikeudet

ABSTRACT

Author	Jari Öljymäki
Title	The Data Protection Reform in the Europe Union
Year	2017
Language	Finnish
Pages	86
Name of Supervisor	Marika Teirfolk-Naarmala

The topic of this thesis is the reform of Europe Union data protection. The preparation work was started already in the year 2010 by the EU Commission to standardize and update the legislation of data protection in the EU and improve the status and the rights of registered persons by increasing the responsibility of the registration authorities. The new EU data protection regulation and directive came into effect in May 2016 and must be put into practice in national legislations in the EU countries after a two-year-transition period in May 2018.

In this thesis the focus is on the new statutes included into the reform of EU data protection; general data protection regulation (EU) 2016/679 and data protection directive (EU) 2016/680, and comparing them to former EU statutes, which were in force before the reform of EU data protection as well as to the Finnish data protection statute. The method of study is jurisprudence and the thesis problem is how Finland has prepared to put into practice the general data protection regulation in its national legislation. The main sources consist of official EU documents, legislation and websites, national legislation, and official documents and websites of the Finnish Department of Justice and the Office of Data Protection Authority in Finland.

The reform of EU data protection will integrate and standardize the data communication between the EU member states in the EU area and by doing so, it will also serve the EU citizens and companies in building a modern, strong and inclusive unity, which will at the same time improve the development of the digital internal market in the European Union. Finland's readiness to put into practice the reform of EU data protection in its national legislation by spring 2018 is already on a good level. Preparations are underway in the Department of Justice and with other data protection stakeholders for matching the national data protection legislation with the EU legislation.

Keywords: EU, data protection, reform, law, personal data, permission

LYHENTEET

EU	Euroopan unioni
euvl	Euroopan unionin virallinen lehti
Henkilötiedodirektiivi	Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24.10.1995 yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
Puitepäättös	Neuvoston puitepäättös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta
Tietosuojadirektiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27.4.2016, 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 puitepäättökseen 2008/977/YOS kumoamisesta
Yleinen tietosuojaja-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27.4.2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta sekä direktiivin 95/46/EY kumoamisesta

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

LYHENTEET

1. JOHDANTO.....	7
2. EU:n TIETOSUOJAUDISTUS.....	9
2.1 Taustaa.....	9
2.2 Syitä uudistukseen.....	10
3. YLEINEN TIETOSUOJA-ASETUS.....	12
3.1 Taustaa.....	12
3.2 Oikeusperusta.....	13
3.3 Rekisteröidyn oikeudet.....	14
3.3.1 Tiedonsaantioikeus ja ilmoittaminen.....	14
3.3.2 Läpinäkyvyys.....	16
3.3.3 Tietojen oikaiseminen, poistaminen ja oikeus tulla unohdetuksi.....	17
3.3.4 Käsittelyn rajoittamisoikeus.....	18
3.3.5 Tietojensiirto-oikeus järjestelmästä toiseen.....	20
3.3.6 Henkilötietojen käsittelyn vastustusoikeus.....	20
3.3.7 Profilointi.....	21
3.3.8 Rajoitukset.....	22
3.4 Rekisterinpitäjän velvollisuudet.....	23
3.4.1 Yleiset velvollisuudet.....	23
3.4.2 Tietoturvallisuus.....	27
3.4.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen.....	29
3.4.4 Tietosuojavastaava.....	31
3.5 Henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille.....	33
3.5.1 Yleistä.....	34
3.5.2 Siirron edellytykset komission taholta.....	34
3.5.3 Yritystä koskevat sitovat säännöt.....	36
3.5.4 Poikkeukset erityistilanteissa.....	36
3.5.5 Kansainvälinen yhteistyö henkilötietojen suojaamiseksi.....	38
3.6 Valvontaviranomaiset.....	39
3.6.1 Riippumattomuus.....	39
3.6.2 Toimivalta ja tehtävät.....	40
3.7 Yhdenmukaisuus ja yhteistyö.....	42
3.7.1 Yhteistyö ja avunanto.....	42
3.7.2 Yhdenmukaisuusperiaate.....	43
3.8 Oikeussuojakeinot, vastuu ja seuraamukset.....	43
3.9 Loppusäännökset.....	47
4. TIETOSUOJADIREKTIIVI (EU)2016/680.....	48
4.1 Taustaa.....	48
4.2 Oikeusperusta, toissijaisuus ja suhteellisuus.....	50
4.3 Yleiset säännöt ja periaatteet.....	51
4.4 Rekisteröidyn oikeudet.....	55
4.4.1 Ilmoittaminen, tiedonsaanti, tietojen oikaiseminen ja poistaminen.....	55
4.5 Rekisterinpitäjä ja henkilötietojen käsittelijä.....	57
4.5.1 Yleiset velvollisuudet.....	58
4.5.2 Henkilötietojen turvallisuus.....	61

4.5.3 Tietosuojavastaava.....	64
4.6 Henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille.....	65
4.7 Valvontaviranomaiset.....	69
4.7.1 Riippumattomuus.....	69
4.7.2 Toimivalta, tehtävät ja valtuudet.....	71
4.8 Yhteistyö.....	73
4.9 Oikeussuojakeinot, vastuu, seuraamukset ja loppusäännökset.....	74
5. SUOMI JA YLEINEN TIETOSUOJA-ASETUS.....	79
6. JOHTOPÄÄTÖKSET.....	82
LÄHTEET.....	84

1. JOHDANTO

Opinnäytetyöni käsittelee EU:n tietosuojauudistusta. EU on valmistellut uutta tietosuoja-asetusta vuodesta 2010, tarkoituksena yhtenäistää EU:n tietosuojakäytäntö ja parantaa digitaalista tiedonsiirtoa ja vahvistaa yksilön oikeuksia sekä EU:n sisämarkkinoita. EU:n yhtenäinen tietosuojareformi parantaa lisäksi kasvavan rikollisuuden ja terrorismin torjuntaa yli kansallisten rajojen. (Eurooppa-neuvosto 2015, tietosuojauudistus, viitattu 11.3.2015.)

Euroopassa ja myös sen rajojen ulkopuolella viime vuosikymmeninä tapahtunut valtavan nopea teknologian ja viestinnän kehitys on luonut haasteita tietosuoja-verkkotoiminnoille. Tietomäärät ja tiedonsiirtonopeudet kasvavat jatkuvasti, mikä edellyttää myös turvallista tietosuojaa. Lisäksi EU:n sisämarkkinat mahdollistavat kansalaisten vapaan liikkuvuuden sekä sosiaalisen ja taloudellisen integraation, mikä on myös lisännyt tiedonsiirtoa yli kansallisten rajojen EU:n sisällä ja myös maanosien välillä. Henkilötietojen käyttö sähköisissä viestimissä ja erilaisissa datapalveluissa kasvaa koko ajan. (Eurooppa-neuvosto 2015, tietosuojauudistus, viitattu 11.3.2015.)

Näitä taustoja vastaan on helppo ymmärtää miksi EU:n alueelle halutaan yhtenäinen ja ajantasainen tietosuojaverkosto palvelemaan sen kansalaisia ja sisämarkkinoita sekä takaamaan tietojen turvallinen ja vapaa liikkuvuus. EU:n tietosuojauudistuspaketti sisältää seuraavat kaikkia EU:n jäsenvaltioita velvoittavat säädökset, jotka opinnäytetyössäni keskeisesti käyn läpi:

Yleinen tietosuoja-asetus, viralliselta nimeltään Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27.4.2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, sekä tietosuojadirektiivi lainvalvontatarkoitukses-

sa käsiteltävien henkilötietojen suojasta, viralliselta nimeltään Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27.4.2016, 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 puitepäättöksen 2008/977/YOS kumoamisesta.

Lisäksi tarkastelen ja vertailen voimaan tulleen yleisen tietosuoja-asetuksen edeltäjää EU:n henkilötietodirektiiviä 95/46/EY (24.10.1995), viralliselta nimikkeeltään Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, sekä neuvoston puitepäättöstä 2008/977/YOS (27.11.2008) rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, jonka uusi voimaan tullut tietosuojadirektiivi korvaa, sekä Suomen henkilötietolakia (523/1999), joka vastaa tietosuojalainsäädännöstä Suomessa.

Yleinen tietosuoja-asetus (EU) 2016/679 tuli voimaan 24.5.2016 ja sillä on kahden vuoden siirtymäaika eli sitä sovelletaan sellaisenaan kaikissa EU:n jäsenvaltioissa 25 päivästä toukokuuta 2018 ja asetusta on kaikilta osiltaan velvoittava. (Yleinen tietosuoja-asetus, viitattu 5.6.2016.) Tietosuojadirektiivi (EU) 2016/680 puolestaan astui voimaan jo 5.5.2016 ja on osoitettu kaikille EU:n jäsenvaltioille. Direktiivillä on myös kahden vuoden siirtymäaika eli sitä tulee soveltaa jäsenvaltioiden kansalliseen lainsäädäntöön viimeistään 6.5.2018. (Tietosuojadirektiivi, viitattu 5.6.2016.)

2. EU:n TIETOSUOJAUUDISTUS

Tässä luvussa käydään läpi lyhyesti EU:n tietosuojauudistuksen taustaa sekä syitä, jotka ovat synnyttäneet tarpeen uudistaa EU:n tietosuojalainsäädäntöä.

2.1 Taustaa

Kaikkialla maailmassa ja Euroopassa teknologian kehitys on luonut uusia haasteita tietojen suojaamiseen. Tietoja kerätään ja välitetään valtavan paljon enemmän kuin aikaisemmin, mikä asettaa Euroopan unionin tietosuojaturvalle täten myös enemmän vaatimuksia ja tarvetta päivityksiin. Henkilötietoja välitetään sekä yritysten, viranomaisten että kansalaisten kesken yhä enemmän verkossa.

EU:n lainsäädännössä ennen voimassa ollut henkilötietodirektiivi 95/46/EY sisälsi kaksi tärkeää tavoitetta: sallia henkilötietojen vapaa liikkuvuus jäsenvaltioiden välillä ja yksilön tietosuojan perusoikeuksien suojaaminen. (henkilötietodirektiivi, viitattu 2.4.2015.) Nämä periaatteet ovat päteviä edelleenkin, mutta eivät riittäviä kehityksen mukana tuomaan tietosuojan hajanaisuuteen unionin alueella ja oikeudellisten seikkojen epävarmuuteen sekä erityisesti näkemykseen, joka vallitsee laajalti unionin alueen kansalaisten, yritysten ja viranomaisten kesken, että verkotoimintaan liittyy paljon epävarmuustekijöitä ja riskejä. (COM (2012) 11 final, viitattu 6.7.2015.)

Tämä käy ilmi mm. EU:n toimesta tehdyssä erityiseurobarometritutkimuksessa (EB) 359 *Data Protection and Electronic Identity in the EU* (2011), jonka mukaan mm. 63% eurooppalaisista kokee että henkilötietojen luovuttaminen on ongelmallista, ainoastaan 26% sosiaalisen median käyttäjistä ja 18% verkko-ostajista kokevat tietojensa luovuttamisen olevan täysin omassa hallinnassaan, 70% on huolissaan siitä, että yritykset käyttävät keräämiään tietoja muuhun kuin ne on tarkoitett-

tu, ja 90% eurooppalaisista on sitä mieltä että sääntöjen ja tietosuojatason pitäisi olla samanlainen kaikissa EU-maissa. (Eriytyisbarometritutkimus EB 359, viitattu 4.4.2015.)

2.2 Syitä uudistukseen

Euroopan unioni on tällä hetkellä monien haasteiden edessä. Maailma on muuttunut monin tavoin. Digitalisaatio ja yleinen tekninen kehitys ovat lisänneet tietojen vaihtoa niin EU:n sisällä kuin ulkopuolellakin merkittävässä määrin. Eurooppaa koettelee myös useita kriisejä, jotka horjuttavat EU:n yhtenäisyyttä ja vakautta; terrorismi, poliittiset levottomuudet, ääripopulismi, pakolaiskriisi ja talouden epävarmuus sekä kansalaisten eriarvoisuus ovat jo arkipäivää Euroopassa.

Tämän vuoksi onkin ensiarvoisen tärkeää, että EU:n tietosuojaverkosto on yhtenäinen, johdonmukainen ja selkeä, ja että jäsenvaltioiden eri viranomaiset voivat tarvittaessa tehdä laaja-alaista yhteistyötä keskenään; vaihtaa, kerätä, luovuttaa, pyytää tietoja ja tunnisteita jne. rikollisuuden ja terrorismin torjumiseksi. Tämän vuoksi EU:n tietosuojauudistuspakettiin sisältyykin yleisen tietosuoja-asetuksen lisäksi direktiivi, joka suojaa lainvalvontatarkoituksessa käsiteltäviä henkilötietoja. Lisäksi EU:lla on tarve vahvistaa digitaalitaloutta ja sisämarkkinoita, mikä omalta osaltaan on lisännyt tietojen siirtoa ja vaihtoa yli kansallisten rajojen ja siten lisännyt tarvetta yhtenäiseen, vahvaan tietosuojakehykseen.

Muun muassa näiden edellä mainittujen seikkojen vuoksi Euroopan Komissio pani vireille aloitteen uudesta EU:n tietosuojaa koskevasta säädöspaketista, johon kuului kaksi säädösehdotusta, COM (2012) 11 final ja COM (2012) 10 final, jotka eri käsittelyvaiheiden kautta ovat EU- asetuksena ja -direktiivinä tulleet voimaan ja joita on sovellettava EU:n jäsenvaltioiden kansallisiin lainsäädäntöihin vuonna 2018:

- Yleinen tietosuoja-asetus (EU) 2016/679
- Tietosuojadirektiivi (EU) 2016/680

3. YLEINEN TIETOSUOJA-ASETUS

EU:n yleinen tietosuoja-asetus tuli voimaan 24.5.2016 ja se tulee korvaamaan henkilötiedodirektiivin 95/46/EY, joka vastasi ennen EU:n tietosuojalainsäädännössä henkilötietojen käsittelyn suojasta luonnollisen henkilön osalta.

Tässä luvussa selvitetään yleisen tietosuoja-asetuksen taustoja ja oikeusperustaa sekä käydään läpi asetuksen artikloja rekisteröidyn oikeuksista loppusäännöksiin.

3.1 Taustaa

Lissabonin sopimuksessa vahvistettiin oikeusperusta, johon perustuen EU voi antaa henkilötietojen suojaa koskevia sääntöjä (Lissabonin sopimus, viitattu 4.7.2015) ja Euroopan ihmisoikeussopimuksesta, jota myös EU:n perusoikeuskirjaksi kutsutaan, tuli perussopimusten kanssa samanarvoinen ja oikeudellisesti sitova asiakirja. Euroopan ihmisoikeussopimuksen 8.artiklan mukaan ”jokaisella on oikeus henkilötietojensa suojaan”. (EU:n perusoikeuskirja, viitattu 6.7.2015.) Näin vahvistettiin, että henkilötietojen suoja kuuluu perusoikeuksiin.

Euroopan parlamentti antoi 25.11.2009 päätöslauselman ns. Tukholman ohjelmasta (Vapauden, turvallisuuden ja oikeuden alue kansalaisia varten, annettu 25.11.2009, (P7_TA(2009)0090)), jossa parlamentti totesi, että EU:n tulisi tehdä kattava ja yhtenäinen järjestelmä henkilötietojen suojausta varten ja kehotti komissiota tarkistamaan aiemmin tehtyä puitepäätöstä. (COM (2012) 11 final, viitattu 6.7.2015.)

Euroopan komission tiedonannossa ”Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa” todetaan, että EU tarvitsee nykyistä kattavamman ja johdonmukaisemman politiikan, jotta henkilötietojen suojaa koskeva perusoikeus toteutuisi. (COM (2012) 11 final, viitattu 6.7.2015.)

Ennen komission antamia lopullisia ehdotuksia EU:n tietosuojauudistuksesta käytiin laajamittainen kuuleminen eri sidosryhmien kesken nykyisen tietosuojalainsäädännön uudistamisen tarpeellisuudesta ja tämä prosessi kesti kaikkiaan yli kaksi vuotta, jona aikana järjestettiin lukuisia eritasoisia seminaareja, konferensseja ja mielipidetutkimuksia. (COM(2012) 11 final, viitattu 6.7.2015.)

25.01.2012 Komissio antoi lopulliset EU:n tietosuojauudistuspakettiin liittyvät lopulliset ehdotukset; yleinen tietosuoja-asetusehdotus (COM(2012)11 final) ja ehdotus tietosuojadirektiivistä lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta (COM(2012)10 final).

Lopullinen versio yleisestä tietosuoja-asetuksesta tehtiin Brysselissä 27.4.2016, viralliselta nimeltään 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, viitattu 8.7.2015.)

3.2 Oikeusperusta

Asetus on annettu Euroopan unionin toiminnasta tehdyn ns. SEUT-sopimuksen 16.artiklaan perustuen (euvl, viitattu 6.7.2015), joka Lissabonin sopimuksen mukaisesti on oikeusperusta tietosuojaa koskevien säädösten ja sääntöjen antamiseen. (COM(2012) 11 final, viitattu 6.7.2015.) Kyseinen artikla mahdollistaa sääntöjen ja säädösten antamisen yksilön suojelusta henkilötietojen käsittelyssä, kun kyseessä ovat jäsenvaltiot, jotka tällaisia tietoja käsitellessään ovat tekemisissä unionin toimivaltaan liittyviin tehtäviin, ja riippumatta, onko kysymyksessä yksityinen taho vai jäsenvaltio henkilötietokäsittelyssä, artikla mahdollistaa henkilötietojen vapaata liikkuvuutta koskevien sääntöjen antamisen (COM (2012) 11 final, euvl,

viitattu 6.7.2015). EU:n perusoikeuskirjan 2.luvun 7. ja 8.artikla vahvistavat henkilötietojen suojan olevan kansalaisten perusoikeus. (EU:n perusoikeuskirja, viitattu 6.7.2015)

3.3 Rekisteröidyn oikeudet

Asetuksessa vahvistetaan, täsmennetään ja lisätään tietyiltä osin rekisteröidyn, eli henkilön, jonka henkilötietoja käsitellään, oikeuksia henkilötietodirektiiviin 95/46/EY nähden, ja taataan vahvemmat tietosuojaoikeudet rekisteröidylle, kuten omiin tietoihin helpompi pääsy, henkilötietojen entistä läpinäkyvämpi ja avoimempi käsittely rekisterinpitäjien taholta, oikeus saada henkilötiedot poistetuiksi ja ”unohdetuksi”, eri järjestelmien välisien tiedonsiirtojen helpottuminen ja lisärajoitusten asettaminen ”profiloinneille”. Myös henkilötietojen käsittelyn vastustus-oikeus laajenee. Lisäksi asetus tulee vahvistamaan rekisteröidyn oikeussuojaturvaa muun muassa rekisteröidyn laajemmalla oikeudella valittaa henkilötietojen käsittelystä sitä suorittaville valvontaviranomaisille, tai käyttää oikeussuojakeinoja kuten asian vieminen tuomioistuinmenettelyyn.

3.3.1 Tiedonsaantioikeus ja ilmoittaminen

Rekisteröity on oikeutettu saamaan rekisterinpitäjältä milloin tahansa tieto siitä, käsitelläänkö häntä koskevia henkilötietoja vai ei ja jos tietoja käsitellään, on rekisterinpitäjän annettava rekisteröidylle tiedot muun muassa käsittelyn tarkoituksesta, käsiteltävistä henkilötietoryhmistä, vastaanottajista, tietojen säilytysajasta sekä tieto rekisteröidyn valitusoikeudesta valvontaa suorittaville eri viranomaisille ja että rekisteröidyllä on mahdollisuus ottamalla yhteys rekisterinpitäjään poistaa tai oikaista häntä koskevia tietoja tai vastustaa itse käsittelyä (yleinen tietosuojasetus, 15.artiklan 1 kohta).

13 artiklassa on säädetty rekisterinpitäjän velvollisuudesta ilmoittaa rekisteröidylle toimitettavat tiedot kun henkilötietoja saadaan ja kerätään rekisteröidyltä. 14 artikla taas säättää rekisterinpitäjän velvollisuudesta toimittaa rekisteröidylle henkilötietoja kun rekisteröidyltä ei ole saatu tietoja. 13 ja 14 artikla velvoittavat rekisterinpitäjää ilmoittamaan rekisteröidylle muun muassa käsittelyn tarkoitus ja oikeusperuste, henkilöllisyys- ja yhteystiedot rekisterinpitäjästä sekä tämän mahdollisesta edustajasta ja tietosuojavastaavasta, tieto rekisteröidyn tietojen siirrosta EU:n ulkopuolelle kolmansiin maihin taikka kansainvälisille järjestöille ja tietosuojan riittävyttä koskeva tieto (yleinen tietosuojasetus, 13. ja 14. artiklan 1 kohdat).

Lisäksi on ilmoitettava mm. henkilötietojen säilytysajasta tai määrittämiskriteerit kyseiselle ajalle, rekisteröidyn oikeudesta päästä omiin henkilötietoihin ja oikeudesta saada tiedot oikaistuiksi tai poistetuiksi taikka rajoittaa tai vastustaa käsitteilyä ja saada tiedot siirretyksi toiseen järjestelmään sekä oikeudesta valittaa valvontaviranomaiselle (yleinen tietosuojasetus, 13. ja 14. artiklan 2 kohdat). Jos kerättyjä henkilötietoja aiotaan rekisterinpitäjän toimesta käyttää edelleen muuhun tarkoitukseen, on siitä annettava rekisteröidylle ilmoitus sekä siihen liittyvät tiedot 2 kohtien mukaisesti (yleinen tietosuojasetus, 13. artiklan 3 kohta ja 14. artiklan 4 kohta).

Rekisterinpitäjän vastuulla ja velvoitteena on toimittaa edellä mainitut 1 ja 2 kohdan tiedot kohtuullisen ajan sisällä, kuitenkin niin että takaraja on 1kk siitä kun henkilötiedot on vastaanotettu tietojen käsittelyyn liittyvät erityisolosuhteet huomioon ottaen. Jos henkilötietoja on tarkoitus käyttää viestinnässä rekisteröidyn kanssa, tiedot on toimitettava viimeistään kun ollaan ensimmäisen kerran yhteydessä rekisteröityyn tai jos tarkoituksena on henkilötietojen luovutus toiselle vastaanottajalle, viimeistään ensimmäisellä luovutuskerralla (yleinen tietosuojasetus, 14. artiklan 3 kohta).

Entiseen EU:n ja nykyiseen Suomen tietosuojalainsäädäntöön verrattuna asetus lisää rekisterinpitäjän ilmoitusvelvollisuutta rekisteröidylle koskien henkilötietojen säilytysaikaa ja valitusoikeutta tietosuojavaltaviranomaisiin.

3.3.2 Läpinäkyvyys

Uutena erillisenä osiona asetukseen on sisällytetty ja rekisteröidyn oikeuksia vahvistamaan lisätty III luvun 1 jakso läpinäkyvyys, joka on jäänyt puuttumaan henkilötietodirektiivistä samoin kuin Suomen henkilötietolaista.

Asetuksen 12 artiklan mukaan rekisterinpitäjän toimintatapojen henkilötietojen käsittelyssä rekisteröidyn oikeuksien eduksi tulee olla helposti saatavilla olevia ja läpinäkyviä ja rekisteröidylle tulee toimittaa rekisteröidyn tarpeet huomioon ottaen, varsinkin lapsen ollessa tietojen kohteena, kaikki henkilötietokäsittelyn alaiset tiedot kirjallisesti tai muulla tavoin ja tapauskohtaisesti sähköisesti, selkeän yksinkertaisella kielellä ja helposti ymmärrettävällä tavalla. Suullinen tietojen luovutus on mahdollista rekisteröidyn pyynnöstä edellyttäen, että rekisteröidyn henkilöllisyyden tunnistaminen ei tapahdu suullisesti (yleinen tietosuoja-asetus, 12.artiklan 1 kohta). Rekisterinpitäjän velvollisuutena on toimittaa rekisteröidylle tiedot toimista, jotka rekisterinpitäjä on aloittanut rekisteröidyn 15-22 artiklan nojalla tekemän pyynnön vuoksi viipymättä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Tätä määräaika on mahdollista pidentää enintään kahdella kuukaudella ottamalla huomioon pyyntöjen monimutkaisuus ja määrä ja tällöin rekisterinpitäjän on ilmoitettava rekisteröidylle määräajan jatkamisesta ja viivästymisen syistä kuukauden sisällä pyynnön vastaanottamisesta. Tiedot tulee toimittaa mahdollisuuksien mukaan sähköisesti jos pyyntökin on esitetty sähköisesti, paitsi jos rekisteröity toisin pyytää (yleinen tietosuoja-asetus, 12.artiklan 3 kohta). Ellei rekisterinpitäjä toteuta rekisteröidyn pyytämiä toimenpiteitä on rekisterinpitäjän ilmoitettava syyt siihen ilman aiheetonta viivytystä tai viimeistään

kuukauden kuluessa pyynnön saamisesta sekä ilmoittaa valitusmahdollisuudesta valvontaviranomaisia kohtaan ja mahdollisuudesta turvautua muihin oikeussuojakeinoihin (yleinen tietosuoja-asetus, 12.artiklan 4 kohta). 13 ja 14 artiklan nojalla toimitetut sekä 15-22 ja 34 artiklaan perustuvat tiedot ja toimet ovat maksuttomia, paitsi jos rekisteröidyn esittämät pyynnöt ovat kohtuuttomia tai perusteettomia, jolloin rekisterinpitäjällä on oikeus periä kohtuullinen maksu ottamalla huomioon tietojen toimittamisesta tai pyynnön toteuttamisesta aiheutuneet hallinnolliset kustannukset, tai oikeus kieltäytyä toimeenpanemasta pyydettyä toimenpidettä. Molemmissa tapauksissa rekisterinpitäjän on voitava osoittaa että rekisteröidyn esittämä pyyntö on ilmeisen perusteeton tai kohtuuton (yleinen tietosuoja-asetus, 12.artiklan 5 kohta). Jos rekisterinpitäjällä on perustellusti syytä epäillä rekisteröidyn henkilöllisyyttä, on rekisterinpitäjällä oikeus pyytää lisätietoja rekisteröidyltä (yleinen tietosuoja-asetus, 12.artiklan 6 kohta).

3.3.3 Tietojen oikaiseminen, poistaminen ja oikeus tulla unohtetuksi

Asetuksen 16.artikla vahvistaa ja täsmentää henkilötietodirektiivin 95/46/EY 12.artiklan b kohtaa. Asetuksen mukaan rekisteröity on oikeutettu vaatimaan rekisterinpitäjää oikaisemaan viipymättä rekisteröityä koskevat virheelliset henkilötiedot sekä saamaan puutteelliset henkilötietonsa täydennetyiksi toimittamalla lisätietoja. (Yleinen tietosuoja-asetus, 16.artikla.)

Rekisteröidyllä on edelleen 17.artiklan nojalla oikeus ja rekisterinpitäjällä velvollisuus poistaa rekisteröityä koskevat henkilötiedot viipymättä jos tietoja ei enää siihen tarkoitukseen, johon niitä kerättiin, tarvita, tai rekisteröity peruuttaa antamansa suostumuksensa henkilötietokäsittelyyn, tai vastustaa sitä, tai käsittely on suoritettu lainvastaisesti, tai rekisterinpitäjää sitova lakisääteinen velvoite, joka perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön, vaatii henkilötietojen poistamista, tai henkilötietojen kerääminen on tapahtunut tämän asetuksen 8 artik-

lan 1 kohdan mukaisen tietoyhteiskunnan palvelujen tarjoamisen yhteydessä. (Yleinen tietosuoja-asetus, 17. artiklan 1 kohta.) Tällöin rekisterinpitäjä on velvollinen, jos hän on julkistanut rekisteröidyn henkilötiedot, saattamaan muille rekisterinpitäjille viipymättä tiedoksi rekisteröidyn pyyntö henkilötietoihin liittyvien linkkien, jäljennöksiä tai kopioiden poistamisesta (yleinen tietosuoja-asetus, 17. artiklan 2 kohta). 1 ja 2 kohtia ei kuitenkaan sovelleta silloin, kun henkilötietojen käsittely katsotaan tarpeelliseksi sanan- ja tiedonvälitysvapausoikeuksien vuoksi, lainsäädännöllisen velvoitteen, joka perustuu rekisterinpitäjään sovellettavaan unionioikeuteen tai jäsenvaltion lainsäädäntöön, noudattamisessa, tai yleisen edun takia taikka rekisterinpitäjälle kuuluvan julkisen vallan käytössä. 1 ja 2 kohtia ei myöskään sovelleta, jos käsittely on aiheellinen 9 artiklan 2 kohdan h ja i alakohdian ja saman artiklan 3 kohdan mukaisten kansanterveyteen liittyvän yleistä etua käsittelevien syiden vuoksi, yleistä etua vaativien arkistointi-, tutkimus-, tai tilastotarkoitusten vuoksi 89 artiklan 1 kohdan mukaisella tavalla, jos 1 kohdan mukainen oikeus todennäköisimmin estäisi kyseisenkaltaista käsittelyä taikka vaikeuttaisi sitä, tai oikeudellisen vaateen laatimisen, esittämisen tai puolustamisen takia. (Yleinen tietosuoja-asetus, 17. artiklan 3 kohta.)

Henkilötietodirektiivin 95/46/EY 12. artiklan b kohta sisälsi lausekkeen tietojen oikaisusta ja poistamisesta tapauskohtaisesti, silloin kun tällaisten tietojen käsittely ei täytä direktiivin vaatimuksia. Artiklan c kohdassa mainitaan rekisterinpitäjän ilmoitusvelvollisuudesta tietoja haltuunsa saaneille sivullisille tehdyistä poistoista tai oikaisuksista (henkilötietodirektiivi, 12. artikla, b ja c kohta). EU:n tietosuoja-asetuksen 17. artikla täsmentää ja vahvistaa 16. artiklan tavoin näitä direktiivin säädöskohtia kuin myös henkilötietolain (523/1999) puolella 6. luvun 29§ ja 30§ säädöskohtia, joissa säädetään rekisteröidyn oikeudesta tietojensa oikaisemiseen tai poistamiseen tai tulla unohdetuksi (henkilötietolaki, viitattu 8.8.2016.)

3.3.4 Käsittelyn rajoittamisoikeus

18.artiklan mukaan rekisteröidyllä on oikeus henkilötietojensa käsittelyn rajoittamiseen rekisterinpitäjän toimesta, jos rekisteröity ilmoittaa ettei hänen henkilötietonsa pidä paikkansa, jolloin rekisterinpitäjä voi rajoittaa käsittelyä, jona aikana rekisteröidyn tiedot tarkistetaan, tai jos henkilötietojen käsittely on laitonta ja rekisteröidyn vaatimuksena on tietojen poistamisen sijaan käsittelyn rajoittaminen, tai vaikei rekisterinpitäjän enää tarvitsisi kyseisiä henkilötietoja käsittelytarkoituksiinsa, mutta rekisteröidyllä on tarve niiden käyttöön oikeudellista vaadetta varten, tai jos asetuksen 21 artiklan 1 kohtaan perustuen rekisteröity vastustaa henkilötietokäsittelyä sinä aikana, kun odotetaan toteennäyttöä siitä, ovatko rekisterinpitäjän oikeudet perusteet vahvempia ja syrjäyttävätkö ne rekisteröidyn perusteet. (Yleinen tietosuoja-asetus, 18. artiklan 1 kohta.) Jos tietojen käsittelyyn kohdistetaan 1 kohdan mukaisia rajoituksia, saa kyseisiä henkilötietoja käsitellä, lukuun ottamatta säilyttämistä, vain jos siihen on olemassa rekisteröidyn lupa, tai käsittelyn tarkoituksena on oikeudellisen vaateen laatiminen, esittäminen tai puolustaminen, taikka toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaaminen, tai Euroopan unionin tai sen jäsenvaltion tärkeinä pidettävien yleisten etujen turvaaminen (yleinen tietosuoja-asetus, 18.artiklan 2 kohta). Tapauksessa, jossa käsittelyä on rajoitettu rekisteröidyn toimesta 1 kohdan nojalla, on rekisterinpitäjän velvollisuutena ilmoittaa rekisteröidylle, että rajoitus tullaan poistamaan (yleinen tietosuoja-asetus, 18.artiklan 3 kohta).

Rekisterinpitäjän vastuulla on ilmoittaa kaikille vastaanottajatahoille, joille henkilötietoja on luovutettu, niistä kaikista tämän asetuksen 16 artiklan, 17 artiklan 1 kohdan ja 18 artiklan mukaisesti suoritetuista henkilötietojen poistoista, oikaisuisista tai käsittelyn rajoituksista, paitsi jos se on mahdotonta tai kohtuutonta. Lisäksi rekisteröidyn on, pyytäessä, saatava näistä vastaanottajista ilmoitus rekisterinpitäjältä (yleinen tietosuoja-asetus, 19. artikla).

3.3.5 Tietojensiirto-oikeus järjestelmästä toiseen

Rekisteröidyllä on oikeus siirtää häntä koskevat henkilötiedot toiselle rekisterinpitäjälle siltä rekisterinpitäjältä, ja tämän sitä estämättä, jolle tiedot on alkujaan toimitettu, jos henkilötietojen käsittely perustuu annettuun suostumukseen 6 artiklan 1 kohdan a alakohdan tai 9 artiklan 2 kohdan a alakohdan mukaisesti, tai laadittuun sopimukseen 6 artiklan 1 kohdan b alakohdan nojalla, ja käsittely toimitetaan automaattisesti (yleinen tietosuoja-asetus, 20. artiklan 1 kohta). Jos tekniikka mahdollistaa, on rekisteröidyllä oikeus siirtää henkilötiedot suoraan rekisterinpitäjältä toiselle, rekisteröidyn käyttäessä 1 kohdan mukaista tietojensiirto-oikeuttaan järjestelmästä toiseen (yleinen tietosuoja-asetus, 20. artiklan 2 kohta), tämän kuitenkaan estämättä tai rajoittamatta 17 artiklan soveltamista, eikä kyseistä tietojensiirto-oikeutta myöskään sovelleta sellaiseen tietojen käsittelyyn, joka katsotaan tarpeelliseksi yleisen edun kannalta tai joka koskee rekisterinpitäjälle kuuluvaa julkisen vallan käyttöä (yleinen tietosuoja-asetus, 20. artiklan 3 kohta). 1 kohdan mukaisella tietojensiirto-oikeudella ei saa olla haitallisia vaikutuksia muihin vapauksiin ja oikeuksiin (yleinen tietosuoja-asetus, 20. artiklan 4 kohta).

Suomen henkilötietolaki (523/1999) ja EU:n henkilötietodirektiivi 95/46/EY eivät tunne tietosuoja-asetuksen 18. artiklan mukaista säädöstä, joka siis asetusta sovellettaessa otetaan EU:n jäsenvaltioiden kansallisissa laissa käyttöön.

3.3.6 Henkilötietojen käsittelyn vastustusoikeus

Henkilötietodirektiivin 95/46/EY 14. artiklan tekstiin perustuu asetuksen 21. artikla, joka antaa rekisteröidylle oikeuden vastustaa henkilötietojensa käsittelyä. Direktiivin tekstiin on asetuksessa tehty vähän muutoksia. Artiklan mukaan rekisteröity voi vastustaa koska tahansa henkilötietojensa sellaista käsittelyä, josta on perustelut asetuksen 6 artiklan 1 kohdan e), tai f) alakohdissa, kuitenkin niin, että jos

rekisterinpitäjä pystyy näyttämään toteen perustellun ja pakottavan syyn, joka menee rekisteröidyn etujen tai perusvapauksien ja -oikeuksien edelle, tai jos oikeudellisen vaateen laatimisessa, esittämisessä tai puolustamisessa rekisteröidyn henkilötietojen käsittely katsotaan välttämättömäksi, ei oikeutta henkilötietojen käsittelyn vastustamiseen ole. (Yleinen tietosuoja-asetus, 21 artiklan 1 kohta.)

Suoramarkkinoinnin ollessa kyseessä rekisteröity on oikeutettu koska tahansa vastustamaan henkilötietojensa käsittelyä, myös profilointia kun sen katsotaan liittyvän kyseiseen suoramarkkinointiin (yleinen tietosuoja-asetus, 21. artiklan 2 kohta) ja tällöin hänen tietojansa ei enää jatkossa ole lupa käsitellä kyseisiin tarkoituksiin (yleinen tietosuoja-asetus, 21. artiklan 3 kohta). Rekisteröityä on informoitava 1 ja 2 kohdan mukaisesta vastustusoikeudesta viimeistään ensimmäisellä yhteydenotokerralla selkeästi muista tiedoista erillään (yleinen tietosuoja-asetus, 21. artiklan 4 kohta) ja rekisteröity voi tietoyhteiskunnan palveluja käyttäessä ja direktiivin 2002/58/EY estämättä hyödyntää automaattisia teknisiä ominaisuuksia käyttäessään hänelle kuuluvaa vastustamisoikeuttaan (yleinen tietosuoja-asetus, 21. artiklan 5 kohta). Jos henkilötietojen käsittelyyn liittyy tieteellistä tai historiallista tutkimusta taikka tilastollisia tarkoituksia 89 artiklan 1 kohdan mukaisesti, on rekisteröidyllä oikeus vastustaa itseään käsittelevien henkilötietojen käsittelyä omaan henkilökohtaiseen tilanteeseensa vedoten, paitsi jos yleinen etu toisin vaatii (yleinen tietosuoja-asetus, 21. artiklan 6 kohta).

Henkilötietolain (523/1999) 6. luvun 30§ käsittelee asetuksen 21 artiklaa. Siinä säädetään rekisteröidyn henkilötietojen käsittelyn kielto-oikeudesta rekisterinpitäjää kohtaan, kun on kysymys suoramarkkinoinnista, etämyynnistä, markkina- ja mielipidetutkimuksista, henkilömatrikkelista tai sukututkimuksesta. (henkilötietolaki 523/1999, 6. luku, 30§.)

3.3.7 Profilointi

Rekisteröidyillä on asetuksen 22.artiklan mukaan oikeus olla tulematta profiloinnin ja automaattiseen käsittelyyn perustuvien päätösten kohteeksi silloin, kun niillä katsotaan olevan oikeusvaikutuksia rekisteröityyn (yleinen tietosuojasetus, 22. artikla, 1 kohta).

Jos kuitenkin tällainen päätös katsotaan välttämättömäksi rekisterinpitäjän ja rekisteröidyn välisen sopimuksen teossa tai sen täytäntöönpanossa, tai rekisterinpitäjään sovellettava unionin oikeus tai rekisteröidyn oikeudet ja vapaudet turvaava jäsenvaltion kansallinen lainsäädäntö sallii ja hyväksyy päätöksen, tai rekisteröity on antanut nimenomaisen suostumuksensa tällaiseen päätökseen, ei edellä mainittua 1 kohtaa sovelleta (yleinen tietosuojasetus, 22.artiklan 2 kohta). Päätösten perustuminen 9 artiklan 1 kohdan mukaisiin henkilötietoryhmiin on kiellettyä, paitsi jos 9 artiklan 2 kohdan a tai g alakohtia sovelletaan, ja rekisteröidyn oikeudet ja vapaudet asianmukaisin toimin turvataan (yleinen tietosuojasetus, 22. artiklan 4 kohta).

Profilointi on siis mahdollista ainoastaan rekisterinpitäjän ja rekisteröidyn välisen sopimisen tai sen täytäntöönpanon yhteydessä, rekisteröidyn esittämästä nimenomaisesta pyynnöstä, hänen suostumuksella tai toimimalla muutoin siten, että rekisteröidyn oikeutetut edut tulevat huomioon otetuiksi, taikka profiloinnin ollessa nimenomaisesti hyväksytty unionin tai jäsenvaltion lainsäädännössä. EU:n henkilötietodirektiivi 95/46/EY sisälsi profilointia koskevaa säädöstä sen 15.artiklassa otsikolla automatisoidut yksittäispäätökset.

3.3.8 Rajoitukset

Asetuksen 23 artiklassa on säädetty, että lainsäädäntötoimin voidaan päättää artiklojen 12-22, 34 ja 5 mukaisten oikeuksien ja velvollisuuksien soveltamisalaa kos-

kevistä rajoituksista, niiltä osin kuin rekisterinpitäjään tai henkilötietojen käsittelijään sovellettavan unionin oikeuden tai jäsenvaltion lainsäädännön säännökset ovat yhteneväiset 12-22 artiklan mukaisten velvollisuuksien ja oikeuksien kanssa ja kyseiset rajoitukset noudattavat pääosiltaan perusoikeuksia ja -vapauksia ja ne katsotaan välttämättömiksi toimenpiteiksi demokraattisessa yhteiskunnassa, jotta taataan muun muassa kansallinen ja yleinen turvallisuus, puolustus ja rikosten ennalta ehkäisy. (Yleinen tietosuoja-asetus, 23.artikla.)

3.4 Rekisterinpitäjän velvollisuudet

Yleinen tietosuoja-asetus määrittelee henkilötietodirektiiviä selvemmin ja tiukemmin rekisterinpitäjän ja henkilötietojen käsittelijän vastuista ja velvollisuuksista henkilötietojen käsittelyssä. Asetuksessa säädetään rekisterinpitäjän yleisistä velvoitteista ja vastuusta, kuten hyväksyttävät ja oikeat toimintamenetelmät ja toimenpiteet henkilötietojen käsittelyssä, velvollisuudesta huolehtia ja varmistaa tietojen käsittelyn asiallinen, kattava ja riittävä tietoturvaso, tietoturvaloukkauksista ilmoittamisesta rekisteröidylle sekä seuraamuksista ja sanktioista jos käsittelyssä tapahtuu rikkomuksia. Uutena velvollisuutena asetus sisältää vaikutustenarvioinnin tarvittaessa henkilötietojen suojaksi ja rekisteröidyn oikeuksien ja vapauksien takaamiseksi.

3.4.1 Yleiset velvollisuudet

Asetuksessa on kahdeksan rekisterinpitäjän ja henkilötietojen käsittelijän yleisiä velvollisuuksia käsittelevää artiklaa. Niistä ensimmäinen, 24.artikla käsittelee rekisterinpitäjän vastuuta.

Rekisterinpitäjän on kaikin teknisin ja organisatorisin toimenpitein varmistettava tämän asetuksen noudattaminen ottamalla huomioon riskit, jotka kohdistuvat

luonnollisten henkilöiden vapauksiin ja oikeuksiin, sekä itse henkilötietokäsittely, sen tarkoitus, laajuus ja asiayhteys. Tarvittaessa toimenpiteitä tulee päivittää ja tarkistaa (yleinen tietosuoja-asetus, 24.artiklan 1 kohta). Rekisterinpitäjän on lisäksi asiallisin tietosuojatoimenpitein varmistettava käsittelyn tietoturva (yleinen tietosuoja-asetus, 24.artiklan 2 kohta).

25.artikla kuvaa oletusarvoiseen ja sisäänrakennettuun tietosuojaan perustuvia rekisterinpitäjän velvollisuuksia. Rekisterinpitäjän on sekä käsittelykeinojen määrittelyssä että itse käsittelyssä uusinta tekniikkaa ja kustannuksia huomioimalla varmistettava, että käsittely täyttää asetuksen mukaiset vaatimukset ja taattava rekisteröidylle kuuluvat oikeudet asianmukaisilla, teknisillä ja organisatorisilla toimenpiteillä (yleinen tietosuoja-asetus, 25.artiklan 1 kohta). Rekisterinpitäjällä on oltava keinot, joilla varmistetaan käsittelyn koskevan oletusarvoisesti ainoastaan välttämättömiä henkilötietoja, joita ei tule säilyttää eikä kerätä enempää kuin on tarpeen, eikä oletusarvoisesti saa luovuttaa rajattomien henkilömäärien käyttöön (yleinen tietosuoja-asetus, 25.artiklan 2 kohta).

Tämä periaate oli henkilötietodirektiivissä ilmaistu sen 6.artiklan c ja e kohdissa; henkilötietojen tulee olla olennaisia, eikä liian laajoja tarkoituksiinsa nähden, ja tiedot tulee säilyttää vain niin kauan kuin se on niiden keräämisen ja käsittelyn kannalta tarpeen (henkilötietodirektiivi, 6.artikla, c ja e kohdat). Henkilötietolaissa (523/1999) on ns. tarpeellisuusvaatimus, jonka mukaan käsiteltävät henkilötiedot on oltava tarpeellisia niiden käsittelyn tarkoituksen kannalta. (henkilötietolaki 523/1999, 9§).

Asetuksen 26.artikla sisältää määrittelyn yhteisrekisterinpitäjistä. Kun henkilötietokäsittelystä ovat vastuussa vähintään kaksi rekisterinpitäjää, jotka vastaavat käsittelyn tarkoituksesta ja keinoista, ovat kyseiset rekisterinpitäjät tällöin yhteisrekisterinpitäjiä. Asetuksen mukaisten velvoitteiden noudattamista varten yhteisrekisterinpitäjien vastuualueet tulee määritellä keskinäisin järjestelyin läpinäkyvästi,

etenkin rekisteröityjen oikeuksien käyttöä sekä 13 ja 14 artiklan mukaisten tietojen toimittamista koskevissa asioissa, kuitenkin niin että rekisterinpitäjiin sovellettava unionin oikeus tai jäsenvaltion lainsäädäntö on ensisijainen rekisterinpitäjien vastuista määräävä taho (yleinen tietosuojasetus, 26.artiklan 1 kohta). Keskinäiset järjestelyt tulee toteuttaa siten, että niistä käy asiallisesti ilmi yhteisrekisterinpitäjien roolit ja suhteet rekisteröityjen suhteen ja järjestelyjä koskevat olennaimmat seikat tulee olla rekisteröityjen saatavilla (yleinen tietosuojasetus, 26.artiklan 2 kohta).

27.artiklassa määritetään rekisterinpitäjien ja henkilötietojen käsittelijöiden edustajista, jotka ovat sijoittautuneet unionin ulkopuolelle. Kun sovelletaan asetuksen 3.artiklan 2 kohtaa, on rekisterinpitäjän tai henkilötietojen käsittelijän velvollisuutena nimittää kirjallisesti edustajansa unionin alueelle (yleinen tietosuojasetus, 27.artiklan 1 kohta), paitsi jos henkilötietojen käsittelyn katsotaan olevan satunnaista ja sen ei katsota kohdistuvan laaja-alaisesti asetuksen 10 artiklan mukaisiin henkilötietoihin tai 9.artiklan 1 kohdan mukaisiin tietoryhmiin ja käsittelyn ei katsota todennäköisesti vaarantavan luonnollisen henkilön oikeuksia ja vapauksia tai aiheuttavan riskiä viranomais- taikka julkishallinnollisille tahoille, kun huomioidaan käsittelyn laajuus, asiayhteys, tarkoitukset ja luonne (yleinen tietosuojasetus, 27.artiklan 2 kohta). Edustajan toimipaikan täytyy olla jossakin niissä jäsenmaissa, joihin ne rekisteröidyt, joiden henkilötietoja käsitellään, ovat sijoittautuneet (yleinen tietosuojasetus, 27.artiklan 3 kohta). Lisäksi edustajalle tulee antaa toimivaltuudet mahdollistaa rekisteröityjen ja valvontaviranomaisten yhteydenotot kaikissa käsittelyyn liittyvissä asioissa, jotta varmistetaan annetun asetuksen oikea noudattaminen (yleinen tietosuojasetus, 27.artiklan 4 kohta). Edustajan nimeäminen ei rajoita oikeustoimien käyttöä rekisterinpitäjää tai henkilötietojen käsittelijää kohtaan (yleinen tietosuojasetus, 27.artiklan 5 kohta).

28.artikla sisältää henkilötietojen käsittelijää koskevat säädökset. Siinä on yksityiskohtaisesti selvitetty henkilötietojen käsittelijän oikeudet ja velvollisuudet ar-

tiklan 10 kohdassa. Henkilötietojen käsittelijän tekemää käsittelytyötä sitoo sopimus tai muu unionin oikeuden tai jäsenvaltion lainsäädännön vahvistama oikeudellinen asiakirja, jossa vahvistetaan rekisterinpitäjän oikeudet ja velvollisuudet sekä käsittelyyn liittyvät seikat, henkilötietojen tyyppi ja rekisteröidyt ryhmät (yleinen tietosuoja-asetus, 28.artiklan 3 kohta). Henkilötietojen käsittelijän tai rekisterinpitäjän alaisuudessa työskentelevän henkilön tulee käsitellä henkilötietoja vain ja ainoastaan rekisterinpitäjän ohjeiden mukaan, ellei unionin oikeus tai jäsenvaltion lainsäädäntö toisin määrää (yleinen tietosuoja-asetus, 29.artikla).

30.artikla säättää käsittelytoimista ylläpidettävästä selosteesta, joka jokaisen rekisterinpitäjän tai rekisterinpitäjän edustajan tulee laatia. Selosteessa on oltava nimet ja yhteystiedot tietosuojavastaavasta, rekisterinpitäjistä ja mahdollisista yhteisrekisterinpitäjistä ja rekisterinpitäjän edustajasta, tiedot käsittelyn tarkoituksesta, henkilötietoryhmistä ja rekisteröityjen ryhmistä, henkilötietojen vastaanottajaryhmät, myös kolmansissa maissa ja kansainvälisissä järjestöissä olevat ryhmät, tarvittaessa henkilötietojen siirtoon kolmansiin maihin tai kansainvälisiin järjestöihin liittyvät tiedot, ja resurssien mukaan suunniteltu määräaikatieto eri tietoryhmien poistoista ja yleiskatsaus 32 artiklan 1 kohdan mukaisista organisatorisista ja teknisistä turvallisuustoimista. (Yleinen tietosuoja-asetus, 30.artiklan 1 kohta.) Vastaavasti jokaisen henkilötietojen käsittelijän ja tarvittaessa tämän edustajan tulee ylläpitää samanlaista selostetta rekisterinpitäjän lukuun tehtävistä käsittelytoimista ja sen on sisällettävä vastaavat tiedot kuin edellä mainitut rekisterinpitäjän tiedot (yleinen tietosuoja-asetus, 30.artiklan 2 kohta). Seloste on oltava kirjallisessa ja sähköisessä muodossa (30.artiklan 3 kohta) ja valvontaviranomaisten saatavilla pyydettyä (30.artiklan 4 kohta). 30.artiklan 1 ja 2 kohdissa mainitut velvollisuudet eivät koske alle 250 työntekijän yrityksiä tai järjestöjä, paitsi jos käsittelytoimet todennäköisesti ovat riski rekisteröidyn oikeuksille ja vapauksille tai käsittely ei ole satunnaista tai se suuntautuu 10 artiklan mukaisiin henkilötietoihin, jotka käsittelevät rikkomuksia tai rikostuomioita tai 9 artiklan 1 kohdan mukaisiin erityisiin tietoryhmiin (30.artiklan 5 kohta).

31.artikla velvoittaa rekisterinpitäjää ja henkilötietojen käsittelijää sekä tarvittaessa myös näiden edustajaa pyydettyä tekemään yhteistyötä valvontaviranomaisien kanssa. (Yleinen tietosuoja-asetus, 31.artikla.)

3.4.2 Tietoturvallisuus

Asetuksen 32.artikla säättää henkilötietojen käsittelyn turvallisuudesta. Rekisterinpitäjää ja henkilötietojen käsittelijää velvoitetaan asianmukaisin teknisin ja organisatorisin toimin varmistamaan käsittelyn riittävä turvallisuustaso huomioimalla luonnollisten henkilöiden oikeuksia ja vapauksia rajoittavat riskit ja tietojen käsittelyssä käytettävä uusin teknologia ja sen toteutuskustannukset sekä itse käsittelyn tarkoitukset, laajuus, luonne ja asiayhteys. Näitä toimenpiteitä ovat muun muassa henkilötietojen salaus ja pseudonymisointi, nopea tietojen saannin palauttaminen, tietoihin pääsy vikatapauksissa, käsittelyprosessin jatkuvan luotettavuuden, eheyden, käytettävyyden ja vikasietoisuuden takaaminen sekä menetelmät, joiden tarkoituksena on käsittelyn turvallisuuden varmistaminen tutkimalla, testaamalla ja arvioimalla säännöllisin ajoin käytössä olevia (yleinen tietosuoja-asetus, 32.artiklan 1 kohta). Rekisterinpitäjä ja henkilötietojen käsittelijä ovat velvoitettuja toteuttamaan nämä toimenpiteet jotta voidaan varmistua siitä, että rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa työskentelevä luonnollinen henkilö, joka pääsee käsiksi henkilötietoihin, noudattaa tietojenkäsittelyssään vain ja ainoastaan rekisterinpitäjän ohjeita, paitsi jos unionin oikeus tai jäsenvaltion lainsäädäntö toisin määrää. (Yleinen tietosuoja-asetus, 32.artiklan 4 kohta.)

33.artikla velvoittaa rekisterinpitäjää antamaan ilmoitus valvontaviranomaiselle henkilötietojen tietoturvaloukkaustapauksessa. Tietoturvaloukkauksesta on ilmoitettava toimivaltaiselle valvontaviranomaiselle 55 artiklan mukaisesti viipymättä ja jos mahdollista 72 tunnin sisällä tietoturvaloukkauksen ilmitulosta, paitsi jos

voidaan katsoa ettei tietoturvaloukkaus todennäköisyydellä tule aiheuttamaan luonnollisten henkilöiden oikeuksia ja vapauksia rajoittavaa riskiä. Ellei rekisterinpitäjä anna ilmoitusta 72 tunnin sisällä, tulee hänen siinä tapauksessa toimittaa valvontaviranomaiselle perustelut sisältävä selvitys tapahtuneesta tietoturvaloukkauksesta. (Yleinen tietosuoja-asetus, 33.artiklan 1 kohta.) Henkilötietojen käsitelijä on velvollinen ilmoittamaan rekisterinpitäjälle tapahtuneesta tietoturvaloukkauksesta viipymättä saatuaan tiedon siitä. (33.artiklan 2 kohta.) Valvontaviranomaiselle annettavassa ilmoituksessa tulee kuvata tapahtunut tietoturvaloukkaus, sisältäen, jos se on mahdollista, tiedot rekisteröityjen ja henkilötyyppien ryhmistä sekä näiden arvioidut lukumäärät. Lisäksi ilmoituksesta on käytävä ilmi tietosuojavastaavan nimi ja yhteystiedot tai joku muu lisätietoja antava taho, ja ilmoituksessa tulee kuvata, mitä seurauksia henkilötietojen tietoturvaloukkauksella todennäköisesti tulee olemaan ja millaisia toimia rekisterinpitäjä on loukkauksen johdosta toteuttanut tai ehdottanut toteutettavaksi sekä mahdollisia haittavaikutuksia lieventämään suunnitellut toimenpiteet tarvittaessa. (33.artiklan 3 kohta). Ilmoituksen tietoja ei tarvitse välttämättä toimittaa samanaikaisesti, jos ja kun se ei ole mahdollista, vaan ne voidaan toimittaa vaiheittain, kuitenkin ilman turhaa viivytelyä (33.artiklan 4 kohta), ja kaikki henkilötietojen tietoturvaloukkaukset sekä niihin liittyvät asiat on dokumentoitava, jotta valvontaviranomainen voi dokumentointia apuna käyttäen tarkistaa tämän artiklan noudattamista (33.artiklan 5 kohta). 34.artiklassa velvoitetaan rekisterinpitäjää ilmoittamaan rekisteröidylle tapahtuneesta henkilötietojen tietoturvaloukkauksesta viipymättä kun sen katsotaan todennäköisesti aiheuttavan korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. (Yleinen tietosuoja-asetus, 34.artiklan 1 kohta.). Ilmoitus tulee antaa yksinkertaisen selkeällä kielellä ja siitä on käytävä selville tietoturvaloukkauksen luonne ja ainakin tiedot ja toimet, jotka sisältyvät 33 artiklan 3 kohdan b, c ja d alakohtiin. (34.artiklan 2 kohta.) Rekisteröidylle annettavaa ilmoitusta ei tarvitse kuitenkaan antaa, jos rekisterinpitäjä on toteuttanut asianmukaiset, tekniset ja organisatoriset suojoimenpiteet, kuten tietojen salaamisen ulkopuolisilta, luvattomilta henkilöiltä (34.artiklan 3 kohdan a) alakohta) tai toteuttamallaan jatkotoi-

menpiteillä rekisterinpitäjä on varmistanut, että 1 kohdan mukainen suuri riski rekisteröidyn oikeuksia ja vapauksia kohtaan ei ilmeisesti tule toteutumaan (34.artiklan 3 kohdan b) alakohta) tai ilmoituksen antaminen vaatisi kohtuutonta vaivaa, jolloin rekisteröidylle annettava ilmoitus tietoturvaloukkauksesta tulisi antaa julkisella tiedonannolla tai vastaavalla toimenpiteellä (34.artiklan 3 kohdan c) alakohta). Tapauksessa, jossa rekisterinpitäjä ei ole vielä tehnyt ilmoitusta rekisteröidylle koskien henkilötietojen tietoturvaloukkausta, on valvontaviranomaisella oikeus vaatia sen tekemistä, tai arvioituaan ensin, millä todennäköisyydellä henkilötietojen tietoturvaloukkauksesta seuraa suuri riski, olla vaatimatta sitä sillä perusteella, että jokin 34 artiklan 3 kohdan alakohdista toteutuu. (Yleinen tietosuoja-asetus, 34.artiklan 4 kohta.)

Henkilötietodirektiivi velvoitti aikaisemmin käsittelemään henkilötietoja lain mukaan ja asiallisesti, sekä keräämään tietoja vain laillisiin tarkoituksiin (henkilötietodirektiivi, 6.artikla, a ja b kohta).

3.4.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

Rekisterinpitäjällä on velvollisuus laatia vaikutustenarviointi henkilötietojen suojalle jos rekisteröidyn oikeudet ja vapaudet ovat uhattuna tietojenkäsittelyyn liittyvien riskien takia (yleinen tietosuoja-asetus, 35.artiklan 1 kohta). Jos tietosuoja-vastaava on nimitetty, tulee rekisterinpitäjän pyytää tältä neuvoja tehdessään tietosuojaa koskevaa vaikutustenarviointia. (35.artiklan 2 kohta.) Erityisesti on 1 kohdan mukainen vaikutustenarviointi tehtävä, jos luonnollisia henkilöitä ja heidän henkilökohtaisia ominaisuuksia järjestelmällisesti ja kattavasti arvioidaan esimerkiksi profiloinnin perusteella ja tällä on luonnolliseen henkilöön oikeudellisia tai vastaavia vaikutuksia olennaisesti (35.artiklan 3 kohdan a) alakohta), tai kyseessä oleva laaja-alainen henkilötietojen käsittely koskee 9 artiklan 1 kohdan mukaisia erityisiä henkilötietoryhmiä tai 10 artiklan mukaisia rikkomuksia tai rikostuomioi-

ta käsitteleviä tietoja (35.artiklan 3 kohdan b) alakohta), tai yleisölle avointa aluetta valvotaan laajasti (35.artiklan 3 kohdan c) alakohta). Valvontaviranomainen on velvollinen laatimaan ja julkaisemaan erityinen luettelo sellaisista käsittelytoimista, jotka vaativat 35 artiklan 1 kohdan mukaisen tietosuojaa käsittelevän vaikutustenarvioinnin ja toimittamaan ne 68.artiklan mukaiselle Euroopan tietosuojaneuvostolle. (Yleinen tietosuoja-asetus, 35.artiklan 4 kohta.) Sellaisista käsittelytoimista, jotka eivät vaadi tietosuojaa käsittelevän vaikutustenarvioinnin tekemistä, voi valvontaviranomainen halutessaan laatia ja julkaista luetteloita, jotka tulee myöskin toimittaa tietosuojaneuvostolle. (Yleinen tietosuoja-asetus, 35.artiklan 5 kohta.) Arvioinnin tulee sisältää kuvaukset tietojenkäsittelyn tarkoituksista ja toimenpiteistä sekä tarvittaessa rekisterinpitäjän oikeudet edut, käsittelyn tarpeellisuus- ja oikeasuhteisuusarvio suhteessa sen tarkoituksiin, riskiarvio suhteessa rekisteröidyn oikeuksiin ja vapauksiin, sekä riskienhallintamenettelyt sekä tietosuojan varmistamiseksi tarvittavat suojatoimet, takeet ja menettelyt, joilla vahvistetaan asetuksen noudattaminen rekisteröityjen oikeuksien hyväksi. (Yleinen tietosuoja-asetus, 35.artiklan 7 kohta.)

35.artikla korvaa tietosuojadirektiivin 95/46/EY 18.artiklan, jossa säädetään rekisterinpitäjän tai hänen edustajan ilmoitusvelvollisuudesta ja -menettelyn yksinkertaistamisesta tai siitä poikkeamisesta valvontaviranomaisille (direktiivi 95/46/EY, 18.artikla). 35 artiklan 1-7 kohtia ei kuitenkaan sovelleta, jos 6.artiklan 1 kohdan c tai e alakohdassa tarkoitettun käsittelyn oikeusperusteeksi katsotaan rekisterinpitäjään sovellettava unionin oikeus tai käsittelytoimia säätelevä jäsenvaltion lainsäädäntö ja vaikutustenarviointi käsittelyn tietosuojan osalta on jo tehty kyseessä olevan käsittelyn oikeusperustehyväksynnän yhteydessä, paitsi jos jäsenvaltiot yhdessä päättävät, että tällainen arvio on tarpeellista toteuttaa ennen käsittelytoimia. (Yleinen tietosuoja-asetus, 35.artiklan 10 kohta.)

36.artiklan ennakkokuuleminen tarkoittaa rekisterinpitäjän velvollisuutta kuulla valvontaviranomaista ennen tietojenkäsittelyprosessia, jos 35 artiklan mukaisessa

vaikutustenarvioinnissa käsittelyn katsotaan aiheuttavan suuren riskin tapauksessa, jossa rekisterinpitäjä ei ole toteuttanut riittäviä toimia riskin. (Yleinen tietosuoja-asetus, 36.artiklan 1 kohta.) Henkilötietodirektiivissä 95/46/EY on sama asia säädetty direktiivin 20.artiklassa ennakkotarkastus -käsitteellä. Rekisterinpitäjän on valvontaviranomaista kuullessaan toimitettava tälle muun muassa tietosuoja-vastaavan yhteystiedot, 35 artiklan mukainen vaikutustenarviointi, rekisteröityjen oikeuksien ja vapauksien suojaamistoimenpiteet, tiedot käsittelyn tarkoituksista ja keinoista sekä muut tiedot, joita valvontaviranomainen rekisterinpitäjältä pyytää (36.artiklan 3 kohta).

3.4.4 Tietosuojavastaava

Velvollisuudesta nimittää tietosuojavastaava on säädetty asetuksen 37.artiklassa, joka nojaa henkilötietodirektiivin 95/46/EY 18.artiklan 2 kohtaan. Rekisterinpitäjän tai henkilötietojen käsittelijän tulee aina nimittää tietosuojavastaava kun käsittelyn hoitaa lainkäyttötehtävistä vastaavan tuomioistuimen sijaan jokin muu julkishallinnollinen elin tai viranomainen, tai käsittelytoimet ovat niin mittavia että ne vaativat rekisteröityjen säännöllisen ja järjestelmällisen seurannan, tai käsittely kohdistuu 9 artiklassa määriteltyihin henkilötietoryhmiin ja 10 artiklan mukaisiin tietoihin, jotka käsittelevät rikkomuksia tai rikostuomioita. (Yleinen tietosuoja-asetus, 37.artiklan 1 kohta). Konserni on oikeutettu nimittämään vain yhden tietosuojavastaavan, jos yhteydenotot jokaisesta toimipaikasta onnistuvat helposti. (37.artiklan 2 kohta.) Yhden tietosuojavastaavan nimittäminen on myös mahdollista, jos rekisterinpitäjänä tai henkilötietojen käsittelijänä toimii julkishallinnollinen elin tai viranomainen, näiden koko ja organisaatiorakenne huomioimalla. (37.artiklan 3 kohta.) Tietosuojavastaavan nimittäminen on mahdollista myös muissa kuin 37 artiklan 1 kohdan mukaisissa tapauksissa, ja myös rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä edustavien yhdistysten tai muiden elimien toimesta ja tietosuojavastaavan nimittäminen on pakollista jos unio-

nin oikeus tai jäsenvaltion lainsäädäntö niin vaatii (37.artiklan 4 kohta). Tietosuojavastaava nimitetään huomioimalla ammattipätevyys ja erikoisesti tietosuojalainsäädännön asiantuntemus sekä kyky hoitaa 39 artiklan mukaiset tehtävät. (Yleinen tietosuojasetus, 37.artiklan 5 kohta.) Tietosuojavastaavana voi toimia myös rekisterinpitäjän tai henkilötietojen käsittelijän henkilöstöön kuuluva tai tietosuojavastaavan tehtävien hoidon perusteena voi olla palvelusopimus. (37.artiklan 6 kohta.) Rekisterinpitäjä tai henkilötietojen käsittelijä velvoitetaan julkistamaan tietosuojavastaavaa koskevat yhteystiedot ja ilmoittamaan ne myös valvontaviranomaiselle. (37.artiklan 7 kohta.)

Tietosuojavastaavan asemasta on säädetty asetuksen 38 artiklassa. Rekisterinpitäjän ja henkilötietojen käsittelijän vastuulla on varmistaa tietosuojavastaavan ottaminen mukaan riittävän ajoissa kaikkiin henkilötietosuojakäsittelyä koskeviin asioihin. (Yleinen tietosuojasetus, 38.artiklan 1 kohta.) Rekisterinpitäjän ja henkilötietojen käsittelijän tulee antaa tietosuojavastaavalle riittävät resurssit tehtäviensä hoitamiseen sekä mahdollistaa pääsy henkilötietoihin ja käsittelytoimiin tietosuojavastaavan asiantuntemuksen säilyttämiseksi. (38.artiklan 2 kohta.) Rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa lisäksi tietosuojavastaavan toimiminen itsenäisesti niin ettei hän ota ohjeita työtehtäviä hoitaessaan ja tietosuojavastaavan erottaminen tai rankaiseminen tehtäviensä hoidon vuoksi on kiellettyä rekisterinpitäjän tai henkilötietojen käsittelijän taholta. Tietosuojavastaavan on raportoitava suoraan rekisterinpitäjän tai henkilötietojen käsittelijän korkeimmalle johdolle. (38.artiklan 3 kohta.) Rekisteröidyt ovat oikeutettuja ottaamaan yhteyttä tietosuojavastaavaan kaikissa heidän henkilötietokäsittelyä koskevissa kysymyksissä sekä tämän asetuksen mukaisten oikeuksien käytössä. (38.artiklan 4 kohta.) Tietosuojavastaava on työssä toimiessaan salassapitovelvollinen sen mukaan kuin unionin oikeus tai jäsenvaltion lainsäädäntö siitä määrää. (38.artiklan 5 kohta.) Tietosuojavastaava saa hoitaa myös muita tehtäviä ja tällöin on rekisterinpitäjän ja henkilötietojen vastuulla valvoa etteivät nämä aiheuta eturistiriitoja. (38.artiklan 6 kohta.)

Asetuksen 39 artikla säättää tietosuojavastaavalle määrätyistä välttämättömistä tehtävistä. Näitä ovat muun muassa tietojen ja neuvojen antaminen rekisterinpitäjille ja henkilötietojen käsittelijöille sekä henkilötietoja käsitteleville työntekijöille kysymyksissä, jotka käsittelevät heille tässä asetuksessa ja unionin oikeudessa tai jäsenvaltioiden tietosuojasäännöksissä asetettuja velvollisuuksia, tämän asetuksen, muiden unionin tai jäsenvaltioiden tietosuojaa koskevan lainsäädännön ja rekisterinpitäjän tai henkilötietojen käsittelijän henkilötietosuojaan liittyvien toimintamennettelyjen valvonta ja seuranta sekä henkilötietoja käsittelevän henkilöstön koulutus, siihen liittyvät tarkastukset ja yleinen tiedon lisääminen. Lisäksi tietosuojavastaavan on annettava pyydettyä tietosuojaa koskevan vaikutustenarvioinnin osalta neuvoja ja valvottava se toteutumista niin kuin 35 artiklassa on säädetty, yhteistyön toteuttaminen valvontaviranomaisten kanssa sekä yhteyskontaktina oleminen näille henkilötietokäsittelyyn, 36 artiklan mukaiseen ennakkuulemiseen ja tarvittaessa muunlaistenkin asioiden kuulemiseen liittyvissä seikoissa. (Yleinen tietosuojasetus, 39.artiklan 1 kohta.) Tehtäviään hoitaessaan tietosuojavastaavan on aina huomioitava niihin liittyvät riskit huomioimalla samalla myös käsittelytoimien tarkoitukset, laajuus, luonne ja asiayhteys. (39.artiklan 2 kohta.)

Asetus tuo voimaan tullessaan siis uusia velvoitteita ja kustannuksia suomalaisille yrityksille, niin yksityisille kuin julkiselle sektorille. Jo nyt voimassa oleva lainsäädäntö velvoittaa esimerkiksi terveydenhuoltoalan yrityksiä ja apteekkeja nimeämään tietosuojavastaavan (Oikeusministeriö, tiedote 18.12.2015, viitattu 23.12.2015).

3.5 Henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille

Asetuksessa säädettyt artiklat 44-50 sisältävät säädöksiä koskien henkilötietojen siirtoa EU-maiden ulkopuolelle ns. kolmansiin maihin tai kansainvälisille järjes-

töille. Siirroille on asetuksessa määritelty tarkat velvoitteet rekisterinpitäjille, henkilötietojen käsittelijöille ja valvontaviranomaisille EU-komission taholta.

3.5.1 Yleistä

44.artikla sisältää siirtoja koskevan yleisperiaatteellisen lausekkeen koskien rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuutta noudattaa asetuksen mukaisia määräyksiä henkilötietojen siirrossa kolmansiin maihin tai kansainvälisille järjestöille (yleinen tietosuojasetus, 44.artiklan 1 kohta). Mikäli EU-komissio katsoo, että siirron kohteena olevassa kolmannessa maassa tai kansainvälisessä järjestössä on varmistettu riittävä tietosuojataso, voidaan henkilötietojen siirto toteuttaa ilman erillistä lupaa (yleinen tietosuojasetus, 45.artiklan 1 kohta).

3.5.2 Siirron edellytykset komission taholta

Komissio edellyttää että siirron kohteena olevassa maassa tai kansainvälisessä järjestössä toimii ainakin yksi valvontaviranomainen, jonka tehtävinä on valvoa tietosuojaa koskevien sääntöjen noudattamista, avun tarjonta ja neuvonta rekisteröidyille sekä yhteistyö jäsenvaltioiden ja EU:n valvontaviranomaisten kesken. Lisäksi komissio ottaa huomioon kohdemaan tai kansainvälisen järjestön solmimat kansainväliset sopimukset, oikeusvaltioperiaatteen, voimassa olevan lainsäädännön, sekä rekisteröityjä koskevat oikeudet (yleinen tietosuojasetus, 45.artiklan 2 kohta). Komissiolla on päätäntävalta sen suhteen, tarjoaako henkilötietojen siirron kohteena oleva kolmas maa tai kansainvälinen järjestö edellä mainittujen ehtojen mukaisesti riittävän tietosuojatason vai ei ja siirtoa koskeva täytäntöönpanosäädös määrää määräaikaistarkastuksesta, joka on tehtävä vähintään joka neljäs vuosi (45.artiklan 3 kohta). Kolmannet maat ja kansainväliset järjestöt ovat jatkuvasti komission kehitysseurannassa, jolla pyritään tarkastamaan tämän asetuksen 45 artiklan 3 kohdan ja direktiivin 95/46/EY 25 artiklan 6 kohdan mukaisten päätösten

toimivuutta. (45.artiklan 4 kohta.) Jos komissio katsoo ettei kolmas maa tai kansainvälinen järjestö täytä riittävän tietosuojatason kriteereitä, voi komissio kumota 3 kohdan mukaisen päätöksensä, muuttaa sitä tai lykätä sen voimaantuloa erillisellä täytäntöönpanosäädöksellä (45.artiklan 5 kohta). Tällöin komission on aloitettava tällaisen tilanteen korjaamiseksi neuvottelut kyseisen kolmannen maan tai kansainvälisen järjestön kanssa. (45.artiklan 6 kohta.) 5 artiklan mukaisen päätöksen ei kuitenkaan katsota rajoittavan 46-49 artiklassa tarkoitettuja henkilötietojen siirtoja kolmansiin maihin tai niiden alueille tai yhdelle tai useammalle sektorille, tai kansainvälisille järjestöille. (45.artiklan 7 kohta.) Komission on julkaistava Euroopan unionin virallisessa lehdessä (euvi) ja verkkosivullaan luettelo kaikista niistä kolmansista maista, niiden alueista ja sektoreista ja kansainvälisistä järjestöistä, joissa komissio katsoo tietosuojatason olevan riittävä tai riittämätön. (45.artiklan 8 kohta.) Komission henkilötietojen siirtoa koskevat päätökset, jotka perustuvat direktiivin 95/46/EY 6 artiklaan, ovat voimassa, ellei niitä muuteta, korvata tai kumota komission päätöksellä 45 artiklan 3 tai 5 kohdan mukaisesti. (45.artiklan 8 kohta.)

Ellei komissio ole tehnyt tietosuojatason riittävydestä päätöstä täytäntöönpanosäädöksen voimaansaattamiseksi 45 artiklan 3 kohdan mukaisesti, rekisterinpitäjällä tai henkilötietojen käsittelijällä on oikeus henkilötietojen siirtoon kolmansiin maihin tai kansainvälisiin järjestöihin vain, jos riittävät ja asianmukaiset suojatoimet on toteutettu rekisterinpitäjän tai henkilötietojen käsittelijän taholta ja rekisteröidyillä on tehokkaat oikeussuojakeinot ja täytäntöönpanokelpoiset oikeudet käytävissään. (Yleinen tietosuoja-asetus, 46.artiklan 1 kohta.) Ilman valvontaviranomaisilta vaadittavaa erityislupaa tällaisia 1 kohdan mukaisia suojatoimia voivat olla muun muassa täytäntöönpanokelpoinen ja oikeudellisesti sitova väline julkisten elinten ja viranomaisten välillä, yritystä käsittelevät sitovat säännöt 47 artiklan mukaisesti ja tietosuojaviranomaisen vahvistamat ja komission 93 artiklan 2 kohdan mukaisen tarkastelumenettelyn kautta hyväksymät tietosuoja käsittelevät vaatiolausekkeet (46.artiklan 2 kohta). Valvontaviranomaisen luvan vaativia 1 koh-

dan mukaisia suojatoimia ovat esimerkiksi tehokkaat ja täytäntöönpanokelpoiset rekisteröityjen oikeuksia sisältävät säännökset, jotka esiintyvät julkisten elinten tai viranomaisten välisissä hallinnollisissa järjestelyissä tai sopimuslausekkeet rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön vastaanottajan, henkilötietojen käsittelijän tai rekisterinpitäjän välillä (46 artiklan 3 kohta).

3.5.3 Yritystä koskevat sitovat säännöt

Asetuksen 47 artiklassa säädetään yrityksiä koskevista sitovista säännöistä, jotka velvoittavat yrityksiä tarkistamaan ja päivittämään tietosuojakäytäntöjään tämän asetuksen tullessa voimaan.

Toimivaltaisella viranomaisella on oikeus vahvistaa yrityksiä koskevat sitovat säännöt, jos ne täyttävät 47 artiklan 2 kohdan mukaiset vaatimukset ja ne sisältävät rekisteröidyille annettavia täytäntöönpanokelpoisia ja heidän henkilötietojensa käsittelyyn liittyviä oikeuksia ja ovat myös oikeudellisesti sitovia ja koskettavat kaikkia yhteistä taloudellista toimintaa harjoittavia yritysryhmän tai konsernin jäseniä, myös työntekijöitä (yleinen tietosuoja-asetus, 47.artiklan 1 kohta). Säännöissä on määriteltävä vähintään muun muassa yhteistä taloudellista toimintaa harjoittavan konsernin tai yritysryhmän ja näiden jäsenten yhteystiedot ja rakenne, sääntöjen oikeudellinen sitovuus unionin sisä- ja ulkopuolella, tiedonsiirrot henkilötietoryhmineen, henkilötietokäsittelyn tarkoitukset ja sen kohteena oleva rekisteröityjen ryhmä, käsittelytoimien tyyppi ja tieto siirron kohteena olevasta kolmannelta maasta tai kolmansista maista, valitusmenettelyt, yhteistyömenettely valvontaviranomaisten kanssa ja menettelytavat sääntömuutoksista tehtävistä ilmoituksista ja niiden kirjaamisesta (47.artiklan 2 kohta).

3.5.4 Poikkeukset erityistilanteissa

Jos tietosuojatason riittävyyttä käsittelevää päätöstä ei ole tehty kuten 45 artiklan 3 kohdassa on säädetty tai asialliset suojatoimet 46 artiklan mukaisesti puuttuvat, mukaan lukien yritystä koskevat sitovat säännöt, on henkilötietosiirrot tai siirtojen sarjat kolmanteen maahan tai kansainväliselle järjestölle mahdollista toteuttaa seuraavilla edellytyksillä:

-Rekisteröity on antanut siirtoon oman suostumuksensa saatuaan tiedon siirtoon liittyvistä mahdollisista riskeistä koska asialliset suojatoimet ja riittävä tietosuojatase puuttuvat.

-Siirto katsotaan tarpeelliseksi, jotta rekisterinpitäjän ja rekisteröidyn välinen sopimus voidaan panna täytäntöön tai koska rekisteröity on pyytänyt toteuttamaan sopimuksen tekoa edeltävät toimenpiteet.

-Siirto on tarpeellinen tärkeään yleiseen etuun liittyvien syiden takia.

-Siirto on tarpeellinen oikeusvaateen laatimisen, esittämisen tai puolustamisen vuoksi.

-Siirto on tarpeellinen, jotta rekisteröityä tai muita henkilöitä koskevat elintärkeät edut

tulevat suojelluiksi, jos rekisteröity on juridisesti tai fyysisesti esteellinen suostumuksensa antoon.

-Siirto suoritetaan sellaisesta rekisteristä, joka unionin oikeuden ja jäsenvaltion lainsäädännön mukaisesti luovuttaa tietoja yleisölle ja jota saa yleisesti käyttää kuka tahansa, jolla on esittää perusteltu syy tiedonsaannilleen, kuitenkin vain siltä osin kuin rekisterin käyttöä koskevat edellytykset, jotka on kirjattu unionin oikeuden tai jäsenvaltion lainsäädäntöön, toteutuvat kussakin yksittäisessä tapauksessa. (49.artikla, 1.kohta.)

Jos siirtoa ei voida suorittaa 45 tai 46 artiklan sääntöihin perustuen, eikä siirtoon voida soveltaa mitään edellä mainituista poikkeuksista erityistilanteissa, voidaan henkilötietojen siirto toteuttaa kolmanteen maahan tai kansainväliselle järjestölle

vain, jos siirto ei ole toistuvaa, kohdistuu vain rajalliseen rekisteröityjen määrään ja siirto katsotaan tarpeelliseksi, jotta rekisterinpitäjän sellaiset oikeutetut edut, joita rekisteröidyn perusoikeudet ja -vapaudet tai edut eivät kumoa, ja jos rekisterinpitäjä on suorittanut tiedonsiirtoon liittyvien asioiden perusteellisen arvioinnin ja tämän jälkeen toteuttanut arviointiin perustuvat asialliset suojoimet henkilötietojen suojan turvaamiseksi. Rekisterinpitäjän on tehtävä siirrosta valvontaviranomaisilmoitus ja annettava siirto sekä pakottavat ja oikeutetut edut tiedoksi rekisteröidylle 13 ja 14 artiklan tietojen lisäksi. (49.artiklan 1 kohta.)

Jos tietosuojan riittävyttä koskeva päätös on antamatta, tiettyjen henkilötietoryhmien siirrolle kolmanteen maahan tai kansainväliselle järjestölle voidaan asettaa rajoitteita unionin oikeudessa tai jäsenvaltion lainsäädännössä tärkeää yleistä etua koskevien syiden takia. Jäsenvaltioiden tulee ilmoittaa tällaisista tapauksista komissiolle. (49.artiklan 5 kohta.)

3.5.5 Kansainvälinen yhteistyö henkilötietojen suojaamiseksi

Valvontaviranomaiset ja komissio sitoutuvat kolmansien maiden ja kansainvälisten järjestöjen suhteen kehittämään kansainvälistä yhteistyötä ja tarjoamaan keskinäistä kansainvälistä apua henkilötietojen suojaukseen liittyvän lainsäädännön täytäntöönpanossa muun muassa tietojen vaihdolla, tutkinta-avun annolla, valitusmenettelyillä ja ilmoituksilla sillä edellytyksellä, että asialliset, henkilötietojen suoja ja perusoikeuksia ja -vapauksia koskevat suojoimet on toteutettu. Lisäksi komissio ja valvontaviranomaiset ovat sitoutuneet toteuttamaan asianmukaisia toimia, joilla keskeiset sidosryhmät saadaan kehitystoimintaan ja keskusteluun mukaan kansainvälisen yhteistyön edistämiseksi henkilötietosuojalainsäädännön toimeenpanossa, ja joilla edistetään henkilötietosuojalainsäädäntöön liittyvien käytänteiden ja dokumentoinnin vaihtoa esimerkiksi toimivaltaristiriitojen suhteen kolmansien maiden kanssa. (Yleinen tietosuojasetus, 50.artikla.)

3.6 Valvontaviranomaiset

51 artiklan 1 kohdan mukaan valvontaviranomainen on jäsenvaltiossa toimiva riippumaton yksi tai useampi viranomainen, jonka vastuulla on tämän asetuksen soveltamisen valvonta henkilötietosuojakäsittelyssä luonnollisten henkilöiden perusoikeuksien ja -vapauksien turvaamiseksi sekä helpottaa henkilötietojen vapaata liikkuvuutta unionin alueella. Kukin jäsenvaltio on velvollinen varmistamaan tämän. (Yleinen tietosuojasetus, 51.artiklan 1 kohta.) Jokainen valvontaviranomainen on velvollinen myötävaikuttamaan siihen, että tätä asetusta sovelletaan yhdenmukaisesti koko unionin alueella ja tämän vuoksi tulee valvontaviranomais-ten olla yhteistyössä keskenään ja komission kanssa 60-62 artiklan mukaisesti. (51.artiklan 2 kohta.) Jos valvontaviranomaisia toimii jäsenvaltiossa useampi kuin yksi, tulee kyseisen jäsenvaltion nimetä valvontaviranomainen edustamaan viranomaisia tietosuojaneuvostoon, ja perustaa järjestelmä varmistamaan 63 artiklan mukaisten sääntöjen noudattaminen muiden valvontaviranomaisten osalta. (51.artiklan 3 kohta.) Kukin jäsenvaltio on velvollinen toimittamaan tämän asetuksen 6 lukuun perustuvat säännökset komissiolle tietoon viimeistään 25.5.2018 mennessä ja niihin liittyvät mahdolliset muutokset niin pian kuin mahdollista. (51.artiklan 4 kohta.)

3.6.1 Riippumattomuus

Kunkin valvontaviranomaisen on oltava täysin riippumaton tehtävissään ja valtuuksiensa käytössä niin kuin tässä asetuksessa on säädetty. (Yleinen tietosuojasetus, 52.artiklan 1 kohta.) Valvontaviranomaisjäsenen tai -jäseniin vaikuttaminen suoraan tai välillisesti ulkoa on kiellettyä, samoin kuin ohjeiden pyytäminen tai ottaminen miltään taholta (52.artiklan 2 kohta) ja valvontaviranomaisen ja sen jäsenten tulee jättäytyä pois tehtävistä, jotka eivät heidän toimenkuvaansa kuulu ja

muu palkallinen tai palkaton ammatinharjoittaminen toimikauden aikana on kiellettyä. (52.artiklan 3 kohta.) Jäsenvaltioiden tulee varmistaa riittävät taloudelliset, tekniset ja henkilölliset resurssit sekä infrastruktuuri ja tilat, tehtävien suorittamiseen ja valtuuksien käyttöön, sisältäen keskinäistä avunantoa, yhteistyötä ja tietosuojaneuvoston toimintaan osallistumista käsittelevät tehtävät ja valtuudet. (52.artiklan 4 kohta.) Lisäksi jäsenvaltioiden tulee edelleen varmistaa, että jokaisella valvontaviranomaisella on heidän itsensä valitsema henkilöstö, joka työskentelee ainoastaan kyseisten valvontaviranomaisten jäsenten alaisuudessa (52.artiklan 5 kohta) ja että varainhoidon valvonta koskee jokaista valvontaviranomaista, ja varainhoito sisältää erillisen julkisen vuotuisen talousarvion, joka voidaan lukea osaksi kansallista tai valtion kokonaistalousarviota (52.artiklan 6 kohta). Säädös nojaa (EY) N:o 45/2001, 44.artiklaan. Henkilötietolaissa 9.luku 38§ säättää Suomen valvonta- eli tietosuojaviranomaisista, tietosuojavaltuutetusta ja tietosuojalautakunnasta (henkilötietolaki, 9.luku, 38§).

3.6.2 Toimivalta ja tehtävät

Valvontaviranomaisten toimivaltaa koskevat säädökset ovat asetuksen 55. ja 56.artiklassa. Henkilötiedodirektiivin mukainen pääsääntö, eli toimivallan rajoittaminen valvontaviranomaisen kotijäsenvaltion alueeseen (direktiivi 95/46/EY 28.artikla, 6.kohta) säilytetään, mutta sitä laajennetaan ns. yhden luukun järjestelmän periaatteella; henkilötietojen käsittelyn tapahtuessa useammassa kuin yhdessä jäsenvaltiossa, valvonnan suorittaisi ainoastaan yksi toimivaltainen viranomainen, ns. johtava valvontaviranomainen, joka on siitä jäsenvaltiosta, jota rekisterinpitäjä pitää päätoimipaikkanaan tai ainoana toimipaikkanaan (Eurooppa-neuvosto, viitattu 11.3.2015). Näin pyritään johdonmukaistamaan ja yhtenäistämään tietosuojalainsäädännön soveltamista koko EU:n alueella.

Jokaisella valvontaviranomaisella on tämän asetuksen mukainen toimivalta tehtä-

viensä hoitoon ja valtuuksiensa käyttöön omalla jäsenvaltioalueellaan. (Yleinen tietosuoja-asetus, 55.artiklan 1 kohta.) Jos henkilötietojen käsittelytoimien suorittamisvastuu on viranomaisilla taikka yksityisillä elimillä rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi tai rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, kuuluu toimivalta tällöin kyseiselle jäsenvaltion valvontaviranomaiselle, jolloin 56 artiklaa ei sovelleta. (55.artiklan 2 kohta.) Tuomioistuimien lainkäytön yhteydessä suorittamien käsittelytoimien suhteen valvontaviranomaisilla ei ole toimivaltuuksia valvoa kyseisiä käsittelytoimia. (55.artiklan 3 kohta.)

Johtavalla valvontaviranomaisella on toimivalta valvonnan toteuttamiseen rajat ylittävien käsittelyjen osalta, ts. kun henkilötietojen käsittely ulottuu useampaan kuin yhteen jäsenvaltioon, kun menettely noudattaa 60 artiklan säädöksiä, eikä sa-notulla rajoiteta 55 artiklan säädöksiä. (56.artiklan 1 kohta) ja johtava valvontaviranomainen toimii rekisterinpitäjän tai henkilötietojen käsittelijän ainoana yhteystahona rajat ylittävissä käsittelyissä. (56.artiklan 6 kohta.) Jokaisella valvontaviranomaisella on kuitenkin toimivalta sille osoitettujen valitusten tai asetusrikkomusten käsittelyyn, jos näiden kohteen voidaan katsoa liittyvän ainoastaan valvontaviranomaisen jäsenvaltioon kuuluvaan toimipaikkaan tai vaikuttavan olennaisesti ainoastaan sen jäsenvaltion rekisteröityihin. (56.artiklan 2 kohta.) Tällöin on valvontaviranomaisen annettava viipymättä ilmoitus kyseisestä tapauksesta johtavalle valvontaviranomaiselle, jonka on kolmen viikon sisällä ilmoituksen saamisesta tehtävä päätös ryhtyykö hän käsittelemään asiaa 60 artiklan mukaisesti sekä selvitettävä kuuluuko käsittelyn suorittama rekisterinpitäjä tai henkilötietojen käsittelijä ilmoituksen antaneen valvontaviranomaisen jäsenvaltioon vai ei. (56.artiklan 3 kohta.) Johtavan valvontaviranomaisen päättäessä ottaa asian käsittelyynsä, sovelletaan asetuksen 60 artiklaa ja tällöin on valvontaviranomaisella mahdollisuus vielä toimittaa johtavalle valvontaviranomaiselle kyseisestä asiasta oma päätösehdotuksensa, joka tämän tulee huomioida olennaisesti lopullista 60 artiklan 3 kohdan mukaista päätösehdotusta tehdessään. (56.artiklan 4 kohta.)

58 artikla käsittelee valvontaviranomaiselle kuuluvia eri valtuuksia. Näitä ovat tutkinta-, hyväksymis- ja neuvontavaltuudet sekä korjaavat toimivaltuudet (58.artikla, 1., 2., ja 3.kohta). Lisäksi jäsenvaltiot voivat säätää lakiinsa lisää valvontaviranomaisilleen kuuluvia valtuuksia (58.artikla, 6.kohta).

57 artiklan mukaisia jokaiselle valvontaviranomaiselle kuuluvia tehtäviä ovat muun muassa tämän asetuksen soveltamisen valvominen ja täytäntöönpano, käsittelyyn liittyvien riskien, sääntöjen, suoja toimien ja oikeuksien yleisen tietoisuuden ja ymmärryksen edistäminen sekä rekisteröidyille tietojen antaminen pyynnöstä liittyen rekisteröidyille kuuluvien oikeuksien käyttöön tämän asetuksen mukaisesti ja yhteistyön tekeminen tarvittaessa muiden jäsenvaltioiden viranomaisten kesken (57.artikla,1.kohta).

3.7 Yhdenmukaisuus ja yhteistyö

EU:n jäsenvaltioiden keskinäisestä yhteistyöstä, avunannosta ja yhdenmukaisuusperiaatteesta säädetään asetuksen artikloissa 60-66.

3.7.1 Yhteistyö ja avunanto

Direktiivin 95/46/EY 28.artiklan 6.kohtaan perustuu asetuksen 61.artikla, joka sisältää keskinäistä avunantoa koskevat säännöt.

Valvontaviranomaisten tulee keskenään luovuttaa tarvittavia tietoja ja noudattaa keskinäisen avunannon periaatetta tämän asetuksen mukaisesti ja kiinnitettävä erityistä huomiota ennakkohyväksyntää ja -kuulemista sekä tarkastusten tekoa koskeviin tietopyyntöihin. (61.artiklan 1 kohta.) Edelleen valvontaviranomaisten on vastattava keskinäisiin avunpyyntöihin viipymättä kaikin mahdollisin toimenpi-

tein, viimeistään kuitenkin kuukauden kuluessa siitä, kun pyyntö on vastaanotettu (61.artiklan 2 kohta.).

3.7.2 Yhdenmukaisuusperiaate

Yleisen tietosuojasetuksen 63.artikla säätelee yhdenmukaisuusmekanismista, jolla varmistetaan EU:n yhtenäinen tietosuojalainsäädäntö ja säännösten yhdenmukainen soveltaminen jäsenvaltioiden kansalaisiin henkilötietojen käsittelyssä (63.artikla).

Komissio, Euroopan tietosuojaneuvosto ja valvontaviranomainen voivat tarvittaessa pyytää minkä tahansa asian käsittelyn aloittamista yhdenmukaisuusmekanismien puitteissa ja komission sekä valvontaviranomaisen velvollisuutena on toimittaa kaikki asiaa koskevat tiedot kuten toimenpideluonnos perusteluineen.

Euroopan tietosuojaneuvosto ja komissio antavat lausuntoja esille tulevista asioista ja valvontaviranomaisen tulee ottaa ne huomioon sekä ilmoittaa komissiolle ja Euroopan tietosuojaneuvostolle hyväksyykö se toimenpideluonnoksen sellaisenaan vai aikooko muuttaa sitä (63. ja 64.artikla). Valvontaviranomaisella on oikeus kiireelliseen menettelyyn, jos tämä on tarpeen rekisteröityjen etujen turvaamiseksi ja tiedotettava siitä muille asianomaisille valvontaviranomaisille, komissiolle ja tietosuojaneuvostolle. (66.artikla, 1.kohta.)

3.8 Oikeussuojakeinot, vastuu ja seuraamukset

Tietosuojasetuksen 77.artikla säätelee lain- ja asetuksen vastaisen toiminnan myötä syntyneen vahingon vastuista ja oikeuksista korvauksiin.

Jokainen rekisteröity on oikeutettu tekemään valvontaviranomaiselle valitus jos

hän kokee hänen henkilötietoja koskevassa käsittelyssä rikottavan tämän asetuksen mukaisia säännöksiä, tämän kuitenkin rajoittamatta muita oikeussuojakeinoja tai hallinnollisia muutoksenhakukeinoja. (Yleinen tietosuoja-asetus, 77.artiklan 1 kohta.) Henkilötietodirektiivissä 95/46/EY tämä periaate on sen 23.artiklan 1.kohdassa. Valituksen vastaanottaneen valvontaviranomaisen tulee ilmoittaa valituksen tehneelle, miten valitus etenee sekä lopullisesta päätöksestä ja 78 artiklan mukaisista oikeussuojakeinoista. (77.artiklan 2 kohta.)

Jokainen luonnollinen tai oikeushenkilö on oikeutettu käyttämään tehokkaita oikeussuojakeinoja itseään koskeviin ja valvontaviranomaisen tekemiin oikeudellisesti sitoviin päätöksiin, tämän rajoittamatta kuitenkin muita hallinnollisia muutoksenhakukeinoja tai muita kuin oikeudellisia oikeussuojakeinoja. (Yleinen tietosuoja-asetus, 78.artiklan 1 kohta.) Jokainen rekisteröity on myös oikeutettu oikeussuojakeinoihin, jos 55 ja 56 artiklaan perustuen toimivaltaisen viranomaisen taholta ei ole käsitelty rekisteröidyn jättämää valitusta tai tämä on jättänyt ilmoittamatta rekisteröidylle kolmen kuukauden sisällä 77 artiklan mukaan toimitetun valituksen etenemisestä tai päätöksestä, tämän rajoittamatta muita hallinnollisia muutoksenhakukeinoja tai muita kuin oikeudellisia oikeussuojakeinoja. (78.artiklan 2 kohta.) Valvontaviranomaista vastaan nostettava kanne on toimitettava sen jäsenvaltion tuomioistuimissa, jossa kyseisen valvontaviranomaisen toimipaikka sijaitsee. (78.artiklan 3 kohta.) Tapauksessa, jossa kanne nostetaan sellaista valvontaviranomaispäätöstä vastaan, johon tietosuojaneuvosto on yhdenmukaisuusmekanismiin perustuen antanut lausuntonsa tai päätöksensä aikaisemmin, on valvontaviranomainen velvoitettu toimittamaan kyseinen päätös tai lausunto tuomioistuimen käsiteltäväksi. (78.artiklan 4 kohta.)

Jokainen rekisteröity on oikeutettu käyttämään tehokkaita oikeussuojakeinoja, jos hänen tämän asetuksen mukaisia oikeuksiaan loukataan sen vuoksi, että hänen henkilötietoihinsa kohdistuvaa käsittelyä ei ole toimitettu tämän asetuksen mukaisesti (yleinen tietosuoja-asetus, 79.artiklan 1 kohta). Rekisterinpitäjää tai henkilö-

tietojen käsittelijää vastaan nostettava kanne on toimitettava sen jäsenvaltion tuomioistuimiin, jossa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka sijaitsee tai joka on rekisteröidyn vakituinen asuinpaikka, paitsi jos jäsenvaltion viranomaisen, joka on henkilötietojen käsittelijä tai rekisterinpitäjä, toiminnan katsotaan liittyvän sen julkisvallan käyttöön. (79.artiklan 2 kohta.)

Asetuksen 82.artikla säättää rekisterinpitäjän tai henkilötietojen käsittelijän vastuusta jos asetusta rikotaan ja rekisteröidyn oikeudesta vahingonkorvaukseen jos rekisteröidylle on aiheutettu vahinkoa. Henkilöllä on oikeus vahingonkorvaukseen rekisterinpitäjältä tai henkilötietojen käsittelijältä, jos hänelle tämän asetuksen rikkomisen vuoksi aiheutuu aineellista tai aineetonta vahinkoa. (Yleinen tietosuojasetus, 82.artiklan 1 kohta.) Rekisterinpitäjän katsotaan olevan vastuussa asetuksen vastaisen henkilötietojen käsittelyn aiheuttamasta vahingosta ja henkilötietojen käsittelijän katsotaan olevan vastuussa käsittelyn aiheuttamasta vahingosta ainostaan, jos kyseinen käsittelijä on rikkonut tälle kuuluvia velvoitteita tai toiminnut rekisterinpitäjän lakisääteisten ohjeiden vastaisesti tai niiden ulkopuolella. (82.artiklan 2 kohta.) Jos rekisterinpitäjä tai henkilötietojen käsittelijä voi osoittaa ettei ole aiheuttanut tapahtunutta vahinkoa, voidaan hänelle myöntää vastuuvapaus 2 kohdan mukaisesti. (82.artiklan 3 kohta.) Jos samassa henkilötietojen käsittelyssä osallisena on enemmän kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä, tai käsittelyyn osallistuu sekä rekisterinpitäjä että henkilötietojen käsittelijä, ja nämä ovat 2 ja 3 kohdassa tarkoitettulla tavalla vastuussa käsittelyn aiheuttamasta vahingosta, on jokainen rekisterinpitäjä tai henkilötietojen käsittelijä tällöin erikseen vastuussa syntyneestä kokonaisvahingosta, jotta varmistetaan rekisteröidylle todellisen korvauksen saaminen. (82.artiklan 4 kohta.) Rekisterinpitäjä tai henkilötietojen käsittelijä on oikeutettu perimään samassa tietojenkäsittelyssä toimineilta rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä se korvausosuus, joka vastaa 2 kohdassa edellytetyn mukaista vastuuosuutta kyseisestä vahingosta, jos henkilötietojen käsittelijä tai rekisterinpitäjä on suorittanut täyden korvauksen käsittelyn aiheuttamasta vahingosta 4 kohdan mukaan. (82.artiklan 5 kohta.) 79 ar-

tiklan 2 kohdan mukaiseen jäsenvaltion kansalliseen lainsäädäntöön perustuen toimivaltaiset tuomioistuimet vastaavat korvaussaamista koskevan oikeudenkäynnin tuomioistuinmenettelyistä. (82.artiklan 6 kohta.)

Asetuksen 83.artikla säätelee hallinnollisista seuraamuksista jos asetusta rikotaan. Jokainen valvontaviranomainen on velvollinen varmistamaan, että tämän artiklan 4, 5 ja 6 kohdan mukaisten, asetuksen rikkomisesta aiheutuvien hallinnollisten sakkojen määräämisessä kaikissa tapauksissa noudatetaan asetuksen 83.artiklaa tehokkaasti, oikeasuhteisesti ja varoittavasti. (Yleinen tietosuojasetus, 83.artiklan 1 kohta.) Hallinnollista sakkoa määrättäessä on otettava huomioon muun muassa sääntörikkomuksen vakavuus, kesto ja luonne, tuottamuksellisuus ja tahallisuus, rikkomuksen kohteeksi joutuneiden rekisteröityjen määrä ja heille aiheutettu kokonaisvahingon suuruus, rekisterinpitäjän tai henkilötietojen käsittelijän vastuuste ja mahdolliset aiemmat rikkomukset sekä heidän toteuttamat organisatoriset sekä tekniset toimet perustuen 25 ja 32 artiklaan, vahingon lieventämistoimet sekä valvontaviranomaisen välinen yhteistyö (83.artiklan 2 kohta). Rekisterinpitäjän tai henkilötietojen käsittelijän rikkoessa tahallisesti tai tuottamuksellisesti asetuksen useita säännöksiä samoissa tai toisiinsa kytköksissä olevissa käsittelyissä, ei määrättävä hallinnollinen kokonaissakko saa ylittyä siitä, mitä vakavimmasta rikkomuksesta on määrätty maksettavaksi. (83.artiklan 3 kohta.) 83 artiklan 4, 5 ja 6 kohtien säännökset sisältävät perusteet määrätä euromääräisiä hallinnollisia sakkoja 2 kohdassa tarkoitetulla tavalla kun asetuksen säännöksiä rikotaan. Euromäärät ovat enintään 10 000 000 tai 20 000 000 €. Yrityksen ollessa kyseessä sanktioperusteina ovat prosentuaaliset osuudet yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta. Euromääriä vastaavat yrityksen prosenttiluvut liikevaihdosta ovat 2 tai 4 prosenttia (83.artiklan 4 ja 5 kohta). Nämä yksityiskohtaisen tarkasti määritetyt hallinnolliset seuraamukset puuttuvat henkilötietodirektiivistä 95/46/EY.

Näin ollen EU:n uusi tietosuojasetus voimaan tullessaan lisää erityisesti yritysten tietosuojavastuuta ja velvoittaa yrityksiä tarkistamaan ja päivittämään tieto-

suojakäytäntöjään tämän asetuksen mukaisiksi, koska seuraamukset ovat niin merkittäviä ettei yrityksillä ole yksinkertaisesti varaa olla huomioimatta asetuksen mukaisia velvoitteita tietojen käsittelyssä.

3.9 Loppusäännökset

EU:n tietosuojasetuksen 94.artiklassa kumotaan direktiivi 95/46/EY 25.5.2018 alkaen (94.artiklan 1 kohta) ja viittaukset kumottuun direktiiviin katsotaan viittauksiksi EU:n uuteen yleiseen tietosuojasetukseen (EU) 2016/679, ja viittauksia, jotka ovat kohdistuneet direktiivin 95/46/EY 29.artiklassa perustettuun tietosuojatyöryhmään katsotaan viittauksiksi tässä asetuksessa muodostettuun Euroopan tietosuojaneuvostoon (94.artiklan 2 kohta).

Komissio veloitetaan julkaisemaan ja toimittamaan säännöllisin ajoin asetuksen arviointia ja uudelleentarkastelua koskevat kertomukset Euroopan parlamentille ja neuvostolle siten, että ensimmäinen on annettava viimeistään kun asetuksen voimaantulosta on kulunut neljä vuotta (25.5.2020) ja sitä seuraavat neljän vuoden välein (97.artiklan 1 kohta). Tarvittaessa voi komissio, ottamalla huomioon tietoteknisen ja yhteiskunnallisen kehityksen, esittää muutosehdotuksia asetukseen (97.artiklan 5 kohta).

99.artiklassa vahvistetaan asetuksen voimaantulo kahdentenakymmenentenä päivänä siitä, kun Euroopan unionin virallinen lehti (euvi) on sen julkaissut (99.artiklan 1 kohta) ja asetuksen soveltaminen EU:n jäsenvaltioissa aloitetaan kahden vuoden kuluttua tästä eli 25.5.2018 alkaen (99.artiklan 2 kohta).

4. TIETOSUOJADIREKTIIVI (EU)2016/680

EU:n uusi tietosuojadirektiivi tuli voimaan 5.5.2016 puitepäättöksen 2008/977/YOS tilalle ja sitä on sovellettava EU:n jäsenvaltioissa 6.5.2018 alkaen. Direktiivi luotiin yhdessä yleisen tietosuoja-asetuksen kanssa tarkoituksena uudistaa EU:n tietosuojalainsäädäntö ajanmukaiseksi ja yhtenäiseksi kokonaisuudeksi. Tämän luvun alussa käydään läpi direktiivin taustaa ja oikeusperustaa, ja seuraavissa alaotsikoissa ja kappaleissa syvennyttään tarkemmin itse direktiivin sisältöön artiklojen myötä.

4.1 Taustaa

24.lokakuuta 1995 voimaan tulleen henkilötietodirektiivin 95/46/EY tavoitteena oli tietosuoja koskevan perusoikeuden turvaaminen ja henkilötietojen siirron vapaan liikkuvuuden takaaminen jäsenvaltioiden kesken. Direktiiviä täydentämään luotiin säädöksiä, joilla haluttiin vahvistaa tietosuoja koskevat säännöt erityisesti aloilla, jotka käsittelevät jäsenvaltioiden välisiä poliisi- ja rikosasioissa tehtävää oikeudellista yhteistyötä, kuten 27. marraskuuta 2008 annettu EU:n neuvoston puitepäättös 2008/977/YOS. (COM (2012) 10 final, viitattu 2.5.2016.)

Puitepäättös on kuitenkin myöhemmin katsottu riittämättömäksi ja vaillinaiseksi turvaamaan riittävästi poliisi- ja rikosasioita käsittelevää oikeudellista yhteistyötä, koska sitä sovelletaan ainoastaan valtioiden välillä tapahtuvaan, rajat ylittävään tietojenkäsittelyyn eikä kansallisella tasolla, maan sisällä tapahtuvaan, mikä on koettu ongelmalliseksi toimivaltaisten viranomaisten välisissä yhteyksissä poliisi- ja rikosoikeudellisia asioita käsittelevillä aloilla. Puitepäättös antaa lisäksi liian suuret toimivaltuudet jäsenvaltioille toteuttaa kansallisia täytäntöönpanotoimia, jotka saattavat poiketa hyvinkin merkittävästi eri jäsenvaltioiden kesken, mikä enemmän hajottaa kuin yhtenäistää EU-alueen poliisi- ja rikosoikeudellista yhteis-

työtä. (COM (2012) 10 final, viitattu 2.5.2016.)

Tietosuojadirektiivialoitetta on edeltänyt kattava kuuleminen eri sidosryhmien kesken henkilötietosuojakäsittelyä koskevan lainsäädännön tarkistamisesta ja uudistamisesta. Kuulemiset ovat pääosin keskittyneet direktiivin 95/46/EY tarkistamiseen ja lainvalvontaa suorittaville tahoille, ja sidosryhmille on järjestetty erityiskohdennettuja kuulemistilaisuuksia. Näistä esimerkkeinä v.2010 kesällä (29.6.2010) EU:n jäsenvaltioiden viranomaisten kesken järjestetty konferenssi, joka käsitteli muun muassa poliisi- ja rikosoikeudellista yhteistyötä sekä 2.2.2011 komission jäsenvaltioiden viranomaisten kanssa järjestämä tilaisuus, jossa käsiteltiin puitepääöstä 2008/977/YOS sekä poliisi- ja rikosasioihin liittyvää oikeudellista yhteistyötä tietosuojaa koskevissa asioissa laaja-alaisesti. (COM(2012) 10 final, viitattu 2.5.2016.)

v.2010 lopulla marras-joulukuussa suoritettiin EU:n kansalaisille kohdennettu eurobarometrikysely (erityisbarometritutkimus EB 359, viitattu 4.4.2015). 6.7.2011 Euroopan parlamentti hyväksyi päätöslauselmassaan (2011/2025 INI, viitattu 2.4.2016) tukemaan komission ehdotusta tietosuojauudistuksesta ja tukirintamaan yhtyvät niin Euroopan unionin neuvosto kuin Euroopan talous- ja sosiaalikomiteakin. (COM(2012) 10 final, viitattu 2.5.2016.)

Näin syntyi ehdotus Euroopan parlamentin ja neuvoston direktiivistä lainvalvontatarkoituksessa käsiteltävien henkilötietojen käytöstä, viralliselta nimeltään Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (COM(2012)10 final). Tämä direktiiviehdotus, yhdessä tietosuojauudistuspakettiin kuuluvan yleisen tietosuojasetusehdotuksen (COM(2012) 11 final) kanssa allekirjoitettiin Euroopan parlamentin ja neuvoston puolesta Brysselissä 25.1.2012 tavoitteena jäsen-

valtioiden välisen yhteistyön ja tietojen vapaan liikkuvuuden lisääminen ja helpottaminen erityisesti poliisi- ja oikeuslaitoksen aloilla sekä samalla yksilön oikeuksien turvaaminen henkilötietojen suojassa ja korkean yleisen turvallisuustason varmistaminen. (COM (2012) 10 final, viitattu 2.5.2016.)

12. maaliskuuta 2014 Euroopan parlamentti vahvisti ensimmäisen käsittelyn kantansa direktiiviehdotuksesta ja 8. huhtikuuta 2016 Euroopan neuvosto vahvisti ensimmäisen käsittelyn kantansa (5418/1/16 REV 1) tietosuojadirektiivistä, joka on muokattu kompromissitekstiksi alkuperäisestä direktiiviehdotuksesta ns. kolmi-kantaneuvottelujen tuloksena parlamentin, komission ja neuvoston välillä. 11. huhtikuuta 2016 Brysselissä komissio antoi tiedonannon Euroopan parlamentille, jossa se hyväksyi neuvoston ensimmäisen käsittelyn kannan ja esitti tietosuojadirektiivin hyväksymistä neuvoston kannan mukaisesti (COM (2016) 213 final, viitattu 6.7.2016). Lopullinen, 65 artiklaa sisältävä, virallinen direktiivi ((EU) 2016/680) allekirjoitettiin Brysselissä 27.4.2016 ja julkaistiin Euroopan unionin virallisessa lehdessä (euvi/L 119) 4.5.2016, jota seuraavana päivänä 5.5.2016 direktiivi tuli voimaan osoitettuna kaikille EU:n jäsenvaltioille.

4.2 Oikeusperusta, toissijaisuus ja suhteellisuus

Lissabonin sopimus (13.12.2007) määritteli erityisen oikeusperustan, joka mahdollisti henkilötietojen suojaa koskevien säädösten antamisen ja sitä sovelletaan yleisen tietosuojasetuksen lisäksi myös tietosuojadirektiiviin, jonka erityisalueina on rikosoikeudellinen- ja poliisiyhteistyö EU:n jäsenvaltioiden välillä. (COM (2012) 10 final, viitattu 2.5.2016.)

Euroopan unionista tehdyn sopimuksen (SEUT- sopimuksen) 16. artiklassa on säädetty yksilöiden oikeussuojasta henkilötietokäsittelyissä, jotka koskevat rikostapauksissa tehtävää poliisi- ja oikeudellista yhteistyötä, ja tämä koskee sekä val-

tioiden välistä että kansallista yhteistyötä. (COM (2012) 10 final, viitattu 2.5.2016.)

Direktiivillä on tarkoitus luoda yhtenäinen ja korkeatasoinen tietosuojaa rikosoikeudellisen- ja poliisiyhteistyön alalla EU:n jäsenvaltioiden oikeus- ja poliisiviranomaisten keskinäisen luottamuksen lujittamiseksi sekä helpottaa tietojen siirtoa ja keskinäistä kanssakäymistä poliisi- ja oikeuslaitosten viranomaisten kesken jäsenvaltioiden välillä. (COM (2012) 10 final, viitattu 2.5.2016.)

Toissijaisuusperiaate on vahvistettu SEUT-sopimuksen 5.artiklan 3.kohdassa, jonka mukaan unionin tasolla tulisi toteuttaa toimia vain, mikäli jäsenvaltiot eivät yksin omalla toiminnallaan kykene riittävän hyvin saavuttamaan suunnitellulle toiminnalle asetettuja tavoitteita ja EU:n tasoinen toiminta etenkin poliisitoiminnassa ja rikosoikeudellisissa käsittelyissä on tämän periaatteen mukaisesti hyvin perusteltua ja tarpeen. (COM (2012) 10 final, viitattu 2.5.2016.)

Suhteellisuusperiaatteella tarkoitetaan, että kaikki käytetyt toimet suunnitellun tavoitteen saavuttamiseksi ovat hyvin kohdennettuja ja niitä toteutetaan vain siinä määrin kuin on tarpeen. Tämä periaate on seurannut koko prosessin eri vaiheita aina säädösehdotukseen asti. (COM (2012) 10 final, viitattu 2.5.2016.)

4.3 Yleiset säännöt ja periaatteet

Direktiivin 1., 2. ja 3. artikla määrittelevät direktiiviä koskevat yleiset säännökset ja artiklat 4-11 periaatteet, jotka perustuvat puitepäätökseen 2008/977/YOS ja direktiiviin 95/46/EY tarkennettuina, täydennettyinä tai lisättyinä (COM (2012) 10 final, viitattu 2.5.2016).

1.artiklan mukaan direktiivi vahvistaa toimivaltaisten viranomaisten toimesta suo-

rittamaa luonnollisten henkilöiden henkilötietojen käsittelyä koskevat säännöt, jotka liittyvät rikoksen torjuntaan, niihin liittyviin syytetoimiin, rikosoikeudellisten seuraamusten toimeenpanoon tai yleiseen turvallisuuteen kohdistuvien uhkien suojeluun ja niiden ennaltaehkäisyyn. Lisäksi artiklassa säädetään direktiivin tavoitteista eli jäsenvaltioiden velvollisuudesta suojella luonnollisten henkilöiden perusoikeuksia, -vapauksia, erityisesti heidän henkilötietosuojaoikeuttaan sekä varmistaa tietojen vapaa liikkuvuus EU:n alueella toimivaltaisten viranomaisten kesken jos unionin oikeus tai jäsenvaltion lainsäädäntö sitä edellyttää luonnollisten henkilöiden suojelua koskevissa henkilötietokäsittelyissä. Jäsenmaat voivat lisäksi säätää direktiivin ylittävistä suojoitoista, jotka kohdistuvat rekisteröidyn oikeuksien ja vapauksien suojeluun toimivaltaisten viranomaisten toimesta suoritettussa henkilötietokäsittelyssä direktiivin sitä estämättä. (Tietosuojadirektiivi, 1.artikla.)

Jokaisen ihmisen oikeus henkilötietojen suojaan on kirjattu myös Nizzassa 7. joulukuuta v.2000 allekirjoitetun EU:n perusoikeuskirjan 8.artiklaan. (EU:n perusoikeuskirja, 8.artikla.)

2.artiklassa on säädetty direktiiviä koskeva soveltamisala, joka koskee toimivaltaisten viranomaisten rikoksen torjuntaa ja siihen liittyvää rikosoikeudellista toimintaa varten suorittamaa osittain tai kokonaan automatisoitua henkilötietojen käsittelyä, tai sellaista ei automatisoitua henkilötietojen käsittelyä, joka muodostaa tai on tarkoitus muodostaa rekisterin osa, mutta direktiiviä ei sovelleta unionin oikeuteen kuulumattoman toiminnan yhteydessä tapahtuvaan käsittelyyn eikä myöskään unionin toimielimien, laitosten ja elimien suorittamaan tietojenkäsittelyyn. (2.artikla, 1-3 kohdat.)

3.artiklassa on määritelty direktiivissä esiintyvät käsitteet. Direktiivistä 95/46/EY ja puitepäätöksestä 2008/977/YOS on siirretty osa määritelmistä sellaisenaan ja joitakin määritelmiä on täydennetty ja muokattu alkuperäisistä. Täysin uusia mää-

ritelmiä ovat ”toimivaltaiset viranomaiset”, ”henkilötietojen tietoturvaloukkaus”, ”biometriset tiedot” ja ”geneettiset tiedot” (COM (2012) 10 final, viitattu 2.5.2016) . Komission Euroopan parlamentille 11.4.2016 annetussa tiedonannossa todetaan, että ”toimivaltaiset viranomaiset” voivat olla myös yksityisiä tahoja, sillä edellytyksellä, että niillä on kansallisen lainsäädännön mukainen julkinen toimivalta tehtävien hoitoon direktiivissä säädettyjä tarkoituksia varten, esimerkiksi yksityiset vankilat. (COM(2016) 213 final, viitattu 6.7.2016.)

4.artikla säätelee henkilötietojen käsittelyn periaatteista, joka perustuu puitepäätöksen 2008/977/EY 3.artiklaan täydennettynä ja tarkennettuna, kuten että käsiteltävien henkilötietojen tulee olla täsmälliset ja päivitettyt, tietoja säilytetään vain välttämätöntä tarvetta ja rekisteröidyn etua varten suorittamalla tietojen käsittely siten, ettei vaaranneta henkilötietojen tietoturvaa (tietosuojadirektiivi, 4.artiklan 1. kohta). Rekisterinpitäjän vastuu ja valvonta henkilötietojen käsittelyn periaatteista vahvistetaan 4.artiklan 4.kohdassa; rekisterinpitäjän on vastattava ja kyettävä osoittamaan todeksi se, että 4 artiklan 1, 2 ja 3 kohtaa noudatetaan (4.artiklan 4.kohta).

Direktiiviin on lisätty täysin uusina artiklat 5, 6 ja 7; säilyttämisen ja tarkistamisen määräajat (5.artikla), eri ryhmiin kuuluvien rekisteröityjen erottaminen (6.artikla) sekä henkilötietojen erottelu ja laadun varmentaminen (7.artikla).

Jäsenmaat veloitetaan säätämään tarkat määräajat henkilötietojen säilyttämistä ja poistamista varten ja niiden noudattamista valvotaan erikseen säädetyin menettelysäännöin (5.artikla). Rekisterinpitäjän on myös jatkossa tarvittaessa eroteltava henkilötiedot sen mukaan mihin ryhmään rekisteröity kuuluu, kuten rikoksesta tuomion saaneet, rikokseen todennäköisin syin ja vakavin perustein syyllistymässä olevat henkilöt ja näiden kumppanit tai/ja kontaktit, rikosuhreiksi joutuneet tai joiden oletetaan joutuvan uhreiksi ja rikosasioihin liittyvät todistajat (6.artikla). Jäsenvaltioiden on eroteltava toisistaan henkilökohtaisiin arvioihin ja tosiseikkoi-

hin perustuvat henkilötiedot mahdollisuuksien mukaan (7.artiklan 1.kohta) ja varmistettava henkilötietojen siirto toimivaltaisten viranomaisten taholta siten, että siirrettävät tiedot ovat virheettömiä, täydellisiä ja ajan tasalla, ja että siirron vastaanottava viranomainen voi luotettavasti tarkastaa ja arvioida tietojen oikeellisuuden (7.artiklan 2.kohta). Jos on siirretty virheellisiä tietoja tai muutoin rikottu lakia on vastaanottajan saatava tästä heti tieto ja 16.artiklan mukaisesti tiedot tulee oikaista, poistaa tai rajoittaa niiden käsittelyä (7.artiklan 3.kohta).

Puitepäättöksen 3.artiklaa on tarkennettu direktiivin 8.artiklalla, jossa määritellään käsittelyn lainmukaisuus, joka toteutuu ainoastaan jos ja vain siltä osin kuin se on tarpeen toimivaltaisen viranomaisen tehtävän suorittamiseksi tämän direktiivin 1 artiklan 1 kohdan tarkoitusta varten ja se perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön. (Tietosuojadirektiivi, 8.artikla, 1.kohta.)

Direktiivin 11.artiklan säädös, joka perustuu puitepäättöksen 2008/977/YOS 7.artiklaan, kieltää sellaiset päätökset, jotka perustuvat yksinomaan rekisteröidyn tiettyjen henkilökohtaisten ominaisuuksien arviointia eli profilointia varten tehtävään automatisoituun käsittelyyn, ja joiden oikeusvaikutukset rekisteröityyn ovat kielteiset tai jotka vaikuttavat rekisteröityyn merkittäväällä tavalla, ellei niitä ole hyväksytty rekisterinpitäjään sovellettavassa jäsenmaan lainsäädännössä tai unionin oikeudessa, jossa rekisteröidyn oikeuksiin ja vapauksiin kohdistuvat suojaamistoimet on otettu huomioon (tietosuojadirektiivi, 11.artikla, 1.kohta). Aiheettomasti ja ilman asianmukaisia rekisteröidyn oikeutettuja etuja, vapauksia ja oikeuksia varten tehtyjä suojatoimia, rotuun tai etniseen alkuperään, poliittiseen mielipiteeseen, uskontoon tai filosofiseen vakaumukseen, ammattiliittojäsenyyteen, terveyteen, geneettiseen tai biometriseen tietoon tai seksuaaliseen suuntautumiseen kohdistuvat edellä mainitut 1 kohdan kaltaiset päätökset ovat kielletty. (11. artikla, 2.kohta.) Artiklan 3.kohta kieltää unionin oikeuteen nojaten 2.kohdan mukaisten erityisryhmien syrjintään johtavan profiloinnin (11.artikla 3.kohta).

4.4 Rekisteröidyn oikeudet

Tietosuojavaltuutettujen kansainvälisen konferenssin antaman, henkilötieto- ja yksityisyysuojaa käsittelevien kansainvälisten standardien, ns.Madridin päätöslauselman (annettu 5.11.2009) periaatteeseen nro 10 perustuen direktiivin 12.artiklassa veloitetaan rekisterinpitäjää kohtuullisin toimin toimittamaan rekisteröidylle kaikki artiklojen 11, 13-18 ja 31 tiedot ja ilmoitukset asianmukaisesti, ymmärrettävästi, helposti saatavassa muodossa ja kieliasultaan selkeän yksinkertaisella tavalla, kuten sähköisesti ja pääsääntöisesti samaa muotoa noudattaen kuin pyyntö, ja näin toimien helpottamaan rekisteröidyn oikeuksien käyttöä.

Rekisterinpitäjän tulee rekisteröidyn pyynnöstä antaa tälle viipymättä kirjallinen ilmoitus henkilötietojen käsittelystä ja toimitetuista tiedoista, tehdyistä ilmoituksista tai toteutetuista toimista ei saa periä maksua, paitsi jos rekisteröidyn esittämät pyynnöt toistuvuudeltaan katsotaan perusteettomiksi tai kohtuuttomiksi. Tällöin rekisterinpitäjä on oikeutettu perimään hallinnolliset kulut kattavan kohtuullisen maksun tai kieltäytymään pyydetyn tehtävän toteuttamisesta. Rekisterinpitäjän tulee tällöin kuitenkin todistaa että pyyntö on perusteeton tai kohtuuton. (Tietosuojadirektiivi, 12.artikla.)

4.4.1 Ilmoittaminen, tiedonsaanti, tietojen oikaiseminen ja poistaminen

13.artiklassa on säädetty tiedoista, jotka rekisterinpitäjän toimesta on rekisteröidylle annettava tai asetettava saataville. Saataville asetettavia ovat rekisterinpitäjän henkilöllisyys- ja yhteystiedot, henkilötietokäsittelyn tarkoitukset, tietosuojavastaavan yhteystiedot tarvittaessa, rekisteröidyn valitusoikeusmahdollisuus valvontaviranomaiselle yhteystietoineen, oikeus estää rekisterinpitäjän pääsy rekisteröityä koskeviin henkilötietoihin esittämällä tällainen pyyntö ja oikeus pyytää tietojen oikaisemista, poistamista tai käsittelyn rajoittamista. Lisäksi lakiin on kirjat-

tava, että rekisteröidyllä on erikoistapauksissa oikeuksiensa käyttöön saatava rekisterinpitäjältä tiedot käsittelyn oikeusperusteesta, henkilötietojen säilytysajoista tai jos tämä on mahdotonta, ainakin tiedot näiden aikojen määrittämiskriteereistä, mahdollisista henkilötietojen vastaanottajista tai vastaanottajaryhmistä mukaan lukien kansainväliset järjestöt ja kolmannet maat sekä tarvittaessa lisätietoja etenkin jos henkilötietojen kerääminen tapahtuu ilman että rekisteröity on siitä tietoinen. (Tietosuojadirektiivi, 13.artikla, 1-2 kohdat.)

13.artiklan 3.kohdan ja 15.artiklan 1.kohdan mukaan EU:n jäsenvaltioilla on lainsäädännöllinen valta rajoittaa tai viivyttää tietojen ilmoittamista rekisteröidylle taikka kokonaan poistaa säännös, joka koskee rekisteröidylle ilmoittamista, silloin kun tämä on välttämätöntä ja oikeutettua rekisteröidyn edun kannalta, jotta lailliset ja viralliset tutkimukset ja menettelyt voidaan toteuttaa minkään tai kenenkään niitä estämättä, jotta ei tuotettaisi haittaa rikostorjuntamenettelyille, rikosoikeudellisten seuraamusten toimeenpanolle ja syytteenostamiselle sekä yleisen ja kansallisen turvallisuuden takaamiseksi, ja muiden henkilöiden vapauksien ja oikeuksien turvaamiseksi (13.artikla,3.kohta, 15.artikla,1.kohta).

Säädöskohdat perustuvat puitepäätöksen 2008/977/YOS 17.artiklan 2.kohtaan ja henkilötietodirektiivin 95/4/EY 13.artiklaan (COM (2012) 10 final, viitattu 2.5.2016). Jäsenmailla on myös oikeus määritellä ne tietoja käsittelevät tahot, jotka voivat soveltaa osittain tai kokonaan tätä säädöskohtaa toimintaansa (13.artiklan 4.kohta ja 15.artiklan 2.kohta). 15 artiklan 1 ja 2 kohdan mukaisissa tapauksissa on rekisterinpitäjän annettava rekisteröidylle viipymättä kirjallinen ilmoitus jos pääsy henkilötietoihin estetään tai sitä rajoitetaan sekä näiden perustelut ja tiedot on mahdollista jättää kokonaan pois, jos tietojen ilmoittamisen katsottaisiin vaarantavan mitä 1 kohdassa on säädetty. Lisäksi jäsenvaltioiden tulee säätää rekisterinpitäjän velvollisuudesta ilmoittaa rekisteröidylle tämän valitusmahdollisuudesta valvontaviranomaista kohtaan tai oikeudesta muihin oikeussuojakeinoihin. (15.ar-

tikla, 3.kohta.).

Rekisteröidyllä on 16.artiklan mukaisesti oikeus pyytää rekisterinpitäjää oikaisemaan tai poistamaan häntä koskevia tietoja tai rajoittamaan niiden käsittelyä. Lisäksi rekisterinpitäjä velvoitetaan antamaan rekisteröidylle kirjallinen ilmoitus jos hän kieltäytyy näistä velvoitteista sekä kieltäytymisen syistä ja rekisteröidyn valitusoikeudesta valvontaviranomaisia kohtaan tai muista oikeussuojakeinoista (16.artikla, 4.kohta). Sama asia on ilmaistu puitepäätöksen 2008/977/YOS 17.artiklan 3.kohdassa ja 18.artiklan 1.kohdassa. Virheellisten henkilötietojen oikaisemisesta on rekisterinpitäjä ilmoitusvelvollinen toimivaltaista viranomaista kohtaan (16. artikla, 5. kohta).

18.artiklassa on säädetty rekisteröidyn oikeuksista rikostutkinta- ja oikeudenkäyntitapauksissa ja perustuu puitepäätöksen 2008/977/YOS 4.artiklaan (COM (2012) 10 final, viitattu 2.5.2016). Jos henkilötiedot sisältyvät rikostutkinnan ja -oikeudenkäynnin yhteydessä annettuun tuomioistuinpäätökseen, asiakirjaan tai tapausaineistoon, on jäsenmailla mahdollisuus säätää, että 13, 14 ja 16 artiklan mukaiset rekisteröidyn oikeudet toimeenpannaan kansallisten oikeussääntöjen mukaisesti (Tietosuojadirektiivi, 18.artikla).

4.5 Rekisterinpitäjä ja henkilötietojen käsittelijä

Direktiivi sisältää kaiken kaikkiaan 15 artiklaa, joissa käsitellään rekisterinpitäjän tai henkilötietojen käsittelijän velvollisuuksista. Tämä on merkittävä muutos puitepäätökseen 2008/977/YOS nähden, sillä siinä ei ole yhtään artiklaa, joka käsittelee yhtä yksityiskohtaisesti rekisterinpitäjälle tai henkilötietojen käsittelijälle lankeavia velvollisuuksia. Puitepäätös ja direktiivi sisältävät kyllä samoja artikloja, kuten käsittelyn turvallisuus ja valvontaviranomaisten ennakkokuuleminen, joissa säädetään rekisterinpitäjän tai henkilötietojen käsittelijän vastuusta ja velvollisuu-

desta toimia säädösten mukaisesti, mutta puitepääatöksessä rekisterinpitäjä tai henkilötietojen käsittelijä -termi on korvattu ”toimivaltaisella viranomaisella” tai säädöksessä vedotaan yleiseen velvollisuuteen. Direktiivissä on siis tarkennettu ja lisätty nimenomaan rekisterinpitäjää tai henkilötietojen käsittelijää koskevia velvollisuuksia merkittävällä tavalla.

4.5.1 Yleiset velvollisuudet

Direktiivi sisältää yhteensä 9 artiklaa koskien rekisterinpitäjän tai henkilötietojen käsittelijän yleisiä velvollisuuksia. Direktiivin artikkelit 19-28 sisältävät säännöksiä rekisterinpitäjän ja henkilötietokäsittelijän yleisistä velvollisuuksista ja vastuista, kuten lainmukaisuuden noudattamisesta ja rekisteröidyn oikeuksien suojelusta henkilötietokäsittelyissä, asiakirjamenettelyistä ja valvontaviranomaistoiminnasta.

19 ja 20 artikla säätävät rekisterinpitäjän yleisestä velvollisuudesta huolehtia rekisteröityjen oikeuksien suojaustoimista ja henkilötietojen käsittelyn lainmukaisuudesta sekä sisäänrakennetusta ja oletusarvoisesta tietosuojasta huomioimalla käsittelyssä uusin teknologia, kustannukset, luonne, laajuus, tarkoitukset, ja että käsitellään oletusarvoisesti ainoastaan sellaisia henkilötietoja, jotka ovat käsittelyn kannalta välttämättömiä lainmukaisuuden varmistamiseksi, ja tällaisille toimenpiteille on tehtävä tarkistuksia ja päivityksiä jos siihen on tarvetta (tietosuojadirektiivi, 19 ja 20 artikla).

21 artiklan mukaan kahden tai useamman rekisterinpitäjän määrittäessä käsittelyssä käytettävät keinot ja sen tarkoitukset, katsotaan ne tällöin yhteisiksi rekisterinpitäjiksi, joista jäsenvaltioilla on oikeus nimetä yksi hoitamaan yhteyspisteenä rekisteröityjen oikeuksien käyttöön liittyviä asioita (tietosuojadirektiivi, 21. artikla, 1 kohta).

22 artiklan nojalla rekisterinpitäjä saa käyttää käsittelyssä tilallaan sellaisia henkilötietojen käsittelijöitä, jotka sitoutuvat toteuttamaan käsittelytoimet direktiivin vaatimusten mukaisesti varmistaen samalla rekisteröidyn oikeuksien suojelun (tietosuojadirektiivi, 22.artikla, 1.kohta). Henkilötietojen käsittelijä saa rekisterinpitäjän erityisellä tai yleisellä kirjallisella luvalla käyttää toisen henkilötietojen käsittelijän palveluksia siten, että yleisen luvan ollessa kyseessä on henkilötietojen käsittelijällä aina ilmoitusvelvollisuus rekisterinpitäjää kohtaan muiden käsittelijöiden vaihtamista tai lisäämistä käsittelevistä muutoksista, jotta rekisterinpitäjällä olisi tällaisten muutosten vastustusmahdollisuus (22.artikla, 2.kohta). Käsittelyä, joka tapahtuu henkilötietojen käsittelijän toimesta, on säänneltävä joko sopimukseen tai muuhun jäsenmaan lain tai EU-oikeuden mukaiseen oikeustoimeen perustuen (22.artikla, 3.kohta) ja tällaisen kirjallisen käsittelyasiakirjan tulee viitata myös sähköiseen versioon (22.artikla, 4.kohta).

23 artikla velvoittaa henkilötietojen käsittelijää, hänen alaisuudessaan toimivaa henkilöä tai rekisterinpitäjää, joilla on mahdollisuus päästä henkilötietoihin käsiksi, suorittamaan tietojenkäsittelyn rekisterinpitäjän antaman ohjeistuksen mukaan ellei EU-oikeus tai jäsenmaan lainsäädäntö muutoin ole säättänyt. (Tietosuojadirektiivi, 23.artikla.)

Rekisterinpitäjän tulee ylläpitää erityistä selostetta sen vastuulle kuuluvista käsittelytoimiryhmistä, joita ovat muun muassa käsittelyn tarkoitukset, henkilötietojen vastaanottajat kolmannet maat ja kansainväliset järjestöt mukaan lukien, nimet ja yhteystiedot tietosuojavastaavasta, rekisterinpitäjistä ja mahdollisesta yhteisestä rekisterinpitäjistä (24. artikla, 1.kohta), ja selostetiedoista on käytävä ilmi muun muassa eri rekisterinpitäjien toimesta tehtyjen käsittelyiden ryhmät, henkilötietojen siirtämistiedot kolmansiin maihin tai kansainvälisille järjestöille niin, että siirron kohteina olevat maat ja järjestöt tunnistetaan (24.artikla, 2.kohta), ja valvontaviranomaisen on pyynnöstä saatava tällaiset selosteet rekisterinpitäjältä ja henkilötietojen käsittelijältä (24.artikla, 3.kohta).

Ainakin tietojen keräämisestä, muuttamisesta, kyselystä, siirrot sisältävästä luovuttamisesta, yhdistämisestä ja poistamisesta tulee säilyttää lokitiedot (25.artikla, 1.kohta), joita saa käyttää vain tarkistettaessa käsittelyn lainmukaisuutta, omaehtoisessa valvonnassa, rikosoikeudellisissa menettelyissä sekä varmistettaessa henkilötietojen luotettavuutta ja turvallisuutta (25.artikla, 2.kohta). Myös lokitietojen on valvontaviranomaisen pyynnöstä oltava tämän saatavilla (25.artikla, 3.kohta).

26 artikla säätelee henkilötietojen käsittelijän ja rekisterinpitäjän yhteistyövelvoitteesta valvontaviranomaisia kohtaan jos tällainen pyyntö valvontaviranomaisten taholta esitetään. (Tietosuojadirektiivi, 26. artikla.)

27 artikla sisältää säädökset tietosuojaa koskevasta vaikutustenarvioinnista. Jos on todennäköistä että käsittely, sen tarkoitukset, asiayhteys, laajuus ja luonne huomioiden, vaarantaa luonnolliselle henkilölle kuuluvia vapauksia ja oikeuksia, on rekisterinpitäjän suoritettava henkilötietosuojaa koskeva vaikutustenarviointi ennen käsittelyn aloittamista. (Tietosuojadirektiivi, 27. artikla, 1.kohta.) Siinä tulee esittää ainakin yleiskuvaus suunnitelluista käsittelytoimista, rekisteröityä koskevien oikeuksien ja vapauksien riskiarvio ja toimintasuunnitelma riskien käsittelyyn, sekä suoja- ja turvatoimet ja suojamekanismit henkilötietojen suojaksi ja tämän direktiivin lainmukaisen noudattamisen varmistamiseksi, kun rekisteröityjen ja muiden asianosaisten oikeudet ja oikeutetut edut otetaan huomioon. (27.artikla, 2.kohta.)

Valvontaviranomaisen ennakkokuulemista käsittelevän 28 artiklan mukaisesti on rekisterinpitäjän tai henkilötietojen käsittelijän kuultava valvontaviranomaista ennen, uuden tekeillä olevan rekisterin osana olevaa, henkilötietokäsittelyä, jos 27.artiklan mukaisessa tietosuojaa koskevassa vaikutustenarvioinnissa käsittelyn todetaan, ilman rekisterinpitäjän toimia, aiheuttavan korkean riskin tai käsittelyn luonteen vuoksi se vaarantaa rekisteröityjen oikeuksien ja vapauksien käytön (28.

artikla, 1.kohta). Lisäksi valvontaviranomaisia on kuultava lain valmisteluvaiheessa kun lakia valmistellaan kansallisen parlamentin hyväksyttäväksi tai lakivalmistelu sisältää käsittelyyn liittyvää sääntelyä (28.artikla, 2.kohta). Rekisterinpitäjän on toimitettava valvontaviranomaiselle 27 artiklan mukainen vaikutustenarviointi ja pyydettyä myös mahdolliset muut käsittelyä koskevat tiedot valvontaviranomaisen tekemää arviointia varten käsittelyn vaatimustenmukaisuudesta, henkilötietosuojaan liittyvistä riskeistä ja turvatoimista (28.artikla, 4.kohta). Valvontaviranomaisen on annettava enintään kuuden viikon sisällä siitä kun kuulemispyyntö on otettu vastaan kirjalliset ohjeistukset rekisterinpitäjää ja mahdollista henkilötietojen käsittelijää varten, ja voi ottaa käyttöön 47 artiklan mukaiset valtuudet, jos valvontaviranomainen katsoo, että tämän direktiivin 28 artiklan 1 kohdan mukainen ennakkokuuleminen rikkoo tässä direktiivissä annettuja säännöksiä, etenkin jos riskiä ei rekisterinpitäjän taholta ole riittävästi lievennetty tai yksilöity. Tätä määräaikaa voidaan kuukaudella pidentää suunnitellun käsittelyn monimutkaisuuden vedoten, jolloin valvontaviranomaisen on annettava ilmoitus rekisterinpitäjälle ja mahdolliselle henkilötietojen käsittelijälle pidennetystä määräajasta ja viivästyymiseen johtaneista syistä kuukauden sisällä siitä kun kuulemispyyntö on vastaanotettu. (28 artikla, 5.kohta.)

4.5.2 Henkilötietojen turvallisuus

Artiklat 29-31 käsittelevät tietoturvallisuutta ja perustuvat henkilötietodirektiiviin 95/46/EY, puitepäätökseen 2008/977/YOS ja sähköisen viestinnän tietosuojadirektiiviin 2002/58/EY. (COM(2012) 10 final, viitattu 2.5.2016.)

29 artikla käsittelee käsittelyn turvallisuutta ja perustuu puitepäätöksen 2008/977/YOS 22 artiklaan (COM (2012) 10 final, viitattu 2.5.2016). Riittävän turvallisuustason varmistamiseksi, etenkin 10 artiklan mukaisten henkilötietoryhmien osalta, rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riittä-

vän laajat ja asialliset organisatoriset ja teknilliset toimet siten, että käsittelyn luonne, tarkoitukset, asiayhteys sekä luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuva riski tulevat huomioon otetuiksi (Tietosuojadirektiivi, 29.artikla, 1.kohta.) Lisäksi turvallisuuden takaamiseksi on riskianalyysiin pohjautuen suoritettava toimenpiteitä, joiden tarkoituksena on 29 artiklan 2 kohdan mukaisesti kohdennetusti valvoa automaattiseen tietojenkäsittelyyn perustuvaa henkilötietojen käsittelyä (29 artikla, 2 kohta).

Direktiivin artikkelat 30 ja 31 käsittelevät henkilötietojen tietoturvaloukkauksia ja niistä annettavia ilmoituksia.

Säännökset perustuvat tarkennettuina yleisen tietosuoja-asetuksen 33 ja 34 artiklaan. Puitepäättös 2008/977/YOS on tältä osin puutteellinen sillä se ei sisällä lainkaan artiklaa, jossa mainittaisiin tietoturvaloukkauksista.

30 artikla säättää rekisterinpitäjän ja henkilötietojen käsittelijän velvoitteesta ilmoittaa valvontaviranomaiselle henkilötietoihin kohdistuneesta tietoturvaloukkauksesta, ja perustuu tarkennettuna (kohta 6 lisätty) yleisen tietosuoja-asetuksen 33 artiklaan. Tietoturvaloukkaustapauksen tultua ilmi on rekisterinpitäjän tehtävä valvontaviranomaisilmoitus viipymättä ja resurssien mukaan 72 tunnin sisällä jos on todennäköistä ja oletettavaa, että tietoturvaloukkaus voi riskeerata ja vaarantaa luonnollisen henkilön vapauksia ja oikeuksia, ja tämän määräajan ylittyessä on ilmoituksen liitteessä eriteltävä syyt myöhästymiseen. (Tietosuojadirektiivi, 30.artikla, 1.kohta.) Henkilötietojen käsittelijän puolestaan on annettava rekisterinpitäjälle tietoturvaloukkausilmoitus viipymättä tällaisen tiedon saatuaan (30.artikla, 2. kohta). Rekisterinpitäjän valvontaviranomaiselle annettavasta ilmoituksesta on käytävä ilmi kuvaus tapahtuneesta tietoturvaloukkauksesta, ottamalla mahdollisuuksien mukaan huomioon siinä asianosaisryhminä mukana olleet rekisteröidyt ja henkilötietotyypit lukumäärällisesti arvioituna, kuvaus tietoturvaloukkauksen seurauksista, ja toteutetuista tai ehdotetuista toimista liittyen tietoturvaloukkauk-

seen ja sen hättävää vaikutuksien lieventämiseksi sekä tietosuojavastaavan yhteystiedot tai -piste, joka mahdollistaa lisätietojen saannin. (30.artikla, 3.kohta.) Tiedot saa, jos samanaikainen toimitus ei ole mahdollista, toimittaa myös vaiheittain ilman että sitä aiheuttomasti viivytetään (30.artikla, 4.kohta) ja kaikki 1 kohdan mukaiset tietoturvaloukkaukset tulee rekisterinpitäjän dokumentoida jotta valvontaviranomainen voi valvoa artiklan noudattamista (30.artikla, 5.kohta). Jos tietoturvaloukkaus sisältää henkilötietoja, jotka ovat toisen EU:n jäsenvaltion rekisterinpitäjälle lähetettyjä tai tämän lähettämiä, tulee 3 kohdassa mainitut tiedot toimittaa aikailematta kyseisen maan rekisterinpitäjälle. (30.artikla, 6.kohta.)

31.artikla velvoittaa rekisterinpitäjää antamaan viipymättä rekisteröidylle selkeän ja ymmärrettävän ilmoituksen tietoturvaloukkauksesta ja sen luonteesta jos sen katsotaan aiheuttavan korkean todennäköisyysriskin luonnollisille henkilöille kuuluville oikeuksille ja vapauksille, ja ilmoituksessa on oltava vähintään tiedot tietosuojavastaavasta, tietoturvaloukkauksen seurauksista sekä sen johdosta toteutetuista toimista ja toimenpide-ehdotuksista tietoturvaloukkauksesta aiheutuvien haittojen minimoimiseksi siten kuin 30 artiklan 3 kohdassa säädetään. (Tietosuojadirektiivi, 31.artiklan 1 ja 2 kohta.) Rekisterinpitäjältä ei kuitenkaan vaadita tällaisen ilmoituksen antamista rekisteröidylle jos rekisterinpitäjä on asianmukaisilla teknisillä ja organisatorisilla suojaustoimilla, kuten salauksella, estänyt luvattomien henkilöiden pääsyn tietoturvaloukkauksen kohteena oleviin henkilötietoihin ja muutoinkin soveltanut kyseisiä suojaustoimia tällaisiin tietoihin, tai jos rekisterinpitäjä on toteuttamallaan jatkotoimenpiteillä varmistanut ettei 30 artiklan 1 kohdan mukainen rekisteröidyn oikeuksiin ja vapauksiin kohdistuva riski todennäköisesti tule toteutumaan, tai jos rekisteröidylle ilmoittaminen vaatisi rekisterinpitäjältä kohtuutonta vaivaa. Tällaisessa tapauksessa on rekisteröidylle tiedottaminen kuitenkin hoidettava julkista ilmoitus- tai vastaavaa menettelyä käyttäen jotta tietoturvaloukkaustieto saadaan yhtä tehokkaasti välitettyä rekisteröidylle. (31. artikla. 3.kohta.) Jos rekisterinpitäjä ei ole vielä antanut rekisteröidylle henkilötietojen tietoturvaloukkausilmoitusta, valvontaviranomaisella on oikeus, sen jälkeen kun

hän on tehnyt tietoturvaloukkauksen rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan todennäköisyysriskiarvion, vaatia rekisterinpitäjää tekemään henkilötietojen tietoturvaloukkausta koskeva ilmoitus rekisteröidylle tai päättää siitä, että jokin 3 kohdan ehdoista toteutuu jolloin rekisterinpitäjän ilmoitusvelvollisuus poistuu. (31.artikla, 4.kohta.) Rekisterinpitäjän ilmoittamista rekisteröidylle 31 artiklan 1 kohdan mukaisesti on mahdollista pitkittää tai rajoittaa tai se on mahdollista jättää kokonaan tekemättä jos 13 artiklan 3 kohdan edellytykset ja perusteet täyttyvät. (31.artikla, 5.kohta.)

4.5.3 Tietosuojavastaava

Tietosuojavastaavan nimittämisestä, asemasta ja tehtävistä on säädetty artikloissa 32-34. Puitepäättös 2008/977/YOS ei käsittele lainkaan tietosuojavastaavan tehtäviä tai asemaa, joten tältäkin osin uusi tietosuojadirektiivi tulee merkittävästi uudistamaan, tarkentamaan ja yhtenäistämään EU:n tietosuojalainsäädäntöä.

32 artiklassa on säädetty tietosuojavastaavan nimittämisestä. Tietosuojavastaavan nimittämisestä vastaa rekisterinpitäjä. Silloin kun tuomioistuimet ja muut riippumattomat oikeusviranomaiset ovat suorittamassa lainkäyttötehtäviään, ne voidaan vapauttaa nimittämisvelvollisuudesta. Tietosuojavastaavan nimittämiskriteereinä ovat ammattipätevyys, tietosuojaoikeuden ja alan käytännön asiantuntemus sekä valmiudet 34 artiklan mukaisten tietosuojavastaavan tehtävien suorittamiseen. Useampaa toimivaltaista viranomaista kohden on mahdollista nimittää ainoastaan yksi tietosuojavastaava kun huomioidaan niiden koko ja organisaatorakenne. Tietosuojavastaavan yhteystietojen julkistaminen sekä niiden ilmoittaminen valvontaviranomaiselle kuuluu rekisterinpitäjälle. (Tietosuojadirektiivi, 32.artikla.)

Tietosuojavastaavan asemasta säädetyn 33 artiklan mukaan rekisterinpitäjän on huolehdittava siitä että kaikissa henkilötietokäsittelyyn liittyvissä asioissa tieto-

suojavastaava otetaan ajoissa ja asiallisesti mukaan (33.artikla, 1.kohta) ja että tietosuojavastaavaa tuetaan 34 artiklassa tarkoitetuissa tehtävissä antamalla riittävät resurssit ja pääsy henkilötietoihin ja niiden käsittelyyn (33.artikla, 2.kohta).

Rekisterinpitäjän tietosuojavastaavalle antamia tehtäviä ovat muun muassa yhteistyö valvontaviranomaisen kanssa, tietosuojadirektiivin noudattamisen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten ja rekisterinpitäjän toimintamennettelyjen valvonta, sekä pyydettyä neuvojen anto vaikutustentarvioinnissa, joka koskee tietosuojaa ja valvoa sitä kuten 27 artiklassa on säädetty (34. artikla).

4.6 Henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille

Puitepääöksessä 2008/977/YOS henkilötietojen siirtoa kolmansiin maihin ja kansainvälisiin järjestöihin on käsitelty sen 13.artiklassa ja tämän direktiivin artikloissa 35-40 tietojen siirtoa käsitellään paljon laajemmin ja täsmällisemmin. Lisäksi artiklat sisältävät täysin uutta säännöstöä puitepääökseen nähden.

35.artiklan mukaisten henkilötietojen siirtoja koskevien yleisten periaatteiden mukaan toimivaltaisten viranomaisten suorittamat henkilötietojen siirrot sekä edelleensirrot voi toteuttaa vain ja ainoastaan silloin kun tässä direktiivissä muiden säännösten nojalla annettuja säännöksiä noudatetaan ja seuraavat siirtoja koskevat vahvistetut edellytykset täyttyvät: 1) siirto katsotaan tarpeelliseksi 1 artiklan 1 kohdan mukaisesti, 2) henkilötietojen siirto tapahtuu kolmannen maan tai kansainvälisen järjestön 1 artiklan 1 kohdan mukaiselle toimivaltaviranomaisena toimivalle rekisterinpitäjälle, 3) jos henkilötietoja siirretään tai ovat saatavilla toisesta jäsenmaasta, kyseessä oleva jäsenvaltio kansalliseen lakiin nojautuen on antanut tälle siirrolle ennakkolupansa, 4) EU:n komissio on antanut hyväksyntänsä 36.artiklan mukaiseen tietosuojan riittävyttä käsittelevään päätökseen tai, ellei tällaista päätöstä ole, asianmukaiset suojatoimet on säädetty tai 37.artiklassa tarkoitettulla

tavalla ovat olemassa, tai, jos 36.artiklan mukainen päätös tai 37.artiklan mukaiset suojoimet puuttuvat, on sovellettava 38.artiklassa säädettyjä erikoistilanteita koskevia poikkeuksia, ja 5) henkilötietojen edelleensierrossa muuhun kolmanteen maahan tai kansainväliseen järjestöön on alkuperäisen siirron toimivaltaisen viranomaisen tai kyseisen jäsenmaan muun toimivaltaisen viranomaisen lupa tämän huomioidessa muun muassa rikoksen vakavuus, henkilötietojen alkuperäissiirron tarkoitus ja henkilötietojen suojan taso edelleensierroin kohteena olevassa kolmannessa maassa tai kansainvälisessä järjestössä. (Tietosuojadirektiivi, 35.artikla, 1. kohta.) Jos siirtoa aikovalla jäsenvaltiolla ei ole toisen jäsenvaltion myöntämää ennakkolupaa (1 kohdan c.alakohta) on siirto mahdollista vain jos se katsotaan välttämättömäksi sellaisen uhan torjumiseksi, joka saattaisi vaarantaa jäsenvaltion tai kolmannen maan yleistä turvallisuutta tai kohdistua jäsenvaltion olennaisiin etuihin ja ennakkoluvan saaminen myöhästyisi. Tällöin asiasta tulisi ilman aiheutonta viivytystä ilmoittaa viranomaiselle, joka vastaa ennakkoluvan myöntämisestä (35.artikla, 2. kohta).

36.artikla säättää riittävän tietosuojatason perusteella tehtävästä henkilötietojen siirrosta, joka on mahdollista toteuttaa ilman lupamenettelyä jos komissio katsoo että siirron kohteena oleva kolmas maa tai kansainvälinen järjestö kykenee tarjoamaan tällaisen riittävän tietosuojatason (36.artikla, 1.kohta). Komissiolla on erityiset arviointikriteerit, joiden avulla se tekee päätöksen tietosuojatason riittävydestä (36.artikla, 2.kohta) erityisellä täytäntöönpanosäädöksellä, joka säättää neljän vuoden välein tehtävästä määräaikaistarkastuksesta, jossa huomioidaan kyseisen kolmannen maan tai kansainvälisen järjestön asiaan liittyvä kehitys (36.artikla, 3.kohta). Lisäksi 4.kohta velvoittaa komissiota jatkuvasti seuraamaan kolmansien maiden ja kansainvälisten järjestöjen kehitystä, jolla saattaa olla vaikutusta siihen, miten 3 kohdan perusteella hyväksytyt päätökset käytännössä toimivat (36.artikla, 4.kohta). Komissio voi täytäntöönpanosäädöstä käyttäen tarvittaessa kumota tai muuttaa 3 kohdassa tarkoitettua tietosuojatason riittävyttä koskevan päätöksen tai keskeyttää sen soveltamisen jos käytettävissä olevien tietojen ja komission suorit-

taman 3 kohdassa tarkoitetun arvioinnin mukaan kolmas maa tai kansainvälinen järjestö ei kykene tarjoamaan tämän artiklan 2 kohdan mukaista riittävää tietosuojatason (36.artikla, 5.kohta). Tällöin komission on aloitettava neuvottelut kansainvälisen järjestön tai kolmannen maan kanssa tällaisen tilanteen korjaamiseksi (36.artikla, 6 kohta). Komission on julkaistava Euroopan unionin virallisessa lehdessä (euvi) sekä verkkosivuillaan luettelo niiden kansainvälisten järjestöjen ja kolmansien maiden sekä kolmansien maiden alueiden ja tiettyjen sektoreiden osalta, joissa komissio katsoo tietosuojatason olevan riittävä tai puutteellinen (36.artikla, 8.kohta).

Ellei päätöstä tietosuojatason riittävydestä komission taholta ole tehty on henkilötietojen siirto mahdollista toteuttaa kolmanteen maahan tai kansainväliseen järjestöön jos rekisterinpitäjä on kaikki tietojen siirtoon liittyvät asiat huomioituaan katsonut, että henkilötietojen suojaamistoimet ovat asianmukaisesti toteutetut tai henkilötietojen suojaaminen on varmistettu muun oikeudellisesti sitovan välineen asianmukaisilla suojatoimilla (37.artikla, 1.kohdan a ja b alakohdat).

Jos sekä 36.artiklan mukainen tietosuojatason riittävyttä koskeva komission päätös ja 37.artiklan 1.kohdan a ja b alakohtien mukaiset henkilötietojen suojaamiseksi tarkoitetut asianmukaiset suojatoimet puuttuvat voidaan henkilötietojen siirto tai siirtojen sarja kansainväliseen järjestöön tai kolmanteen maahan toteuttaa vain jos se katsotaan tarpeelliseksi jäsenvaltion tai kolmannen maan yleistä turvallisuutta vaarantavan vakavan ja välittömän uhan ehkäisemiseksi, rekisteröityä tai muuta henkilöä koskevien elintärkeiden etujen suojaamiseksi, rekisteröidylle kuuluvien oikeutettujen etujen turvaamiseksi, yksittäistapauksessa 1 artiklan 1 kohdan tarkoituksiin liittyvien oikeusvaateiden puolustamiseksi, laatimiseksi ja esittämiseksi tai yksittäistapauksissa 1 artiklan 1 kohdassa vahvistettuja tarkoituksia varten. (38.artikla, 1.kohta.) Henkilötietoja ei kuitenkaan saa siirtää edellä mainituissa yksittäistapauksissa koskevissa siirroissa, jos siirron suorittavan toimivaltaisen viranomaisen mielestä asianosaisena olevan rekisteröidyn perusvapaudet ja -oi-

keudet syrjäyttävät yleisen edun (38.artikla, 2. kohta). 1.kohdan mukaiset siirrot on dokumentoitava ja asiakirjat tulee olla valvontaviranomaisen saatavilla pyynnöstä (38.artikla, 3.kohta).

35.artiklan 1 kohdan b alakohdasta poiketen ja jäsenmaiden sekä kolmansien maiden kesken voimassa olevien kahden- tai monenvälisen poliisi- ja rikosasioissa tehtävää oikeudellista yhteistyöalaa käsittelevien kansainvälisten sopimusten soveltamista rajoittamatta voidaan kunkin jäsenvaltion lainsäädännössä tai unionin oikeudessa säätää toimivaltaisten viranomaisten toimesta yksittäis- ja erityistapauksissa tapahtuvasta henkilötietojen siirrosta kolmansiin maihin sijoittautuneille vastaanottajille vain, jos tässä direktiivissä säädettyjä muita säännöksiä noudatetaan ja seuraavat ehdot täyttyvät: Siirto on ehdottoman välttämätön, jotta siirron tekevä toimivaltainen viranomais voi toteuttaa hänelle määrätyt tehtävät niitä tarkoituksia varten, jotka on 1.artiklan 1.kohdassa vahvistettu, siirron tekevä toimivaltainen viranomais katsoo, että kolmannen maan 1.artiklan 1.kohdan mukaisesti toimivaltaiselle viranomaiselle siirto on tehoton tai muutoin epäsopiva erityisesti siksi, että tapahtuvaa siirtoa ei voida suorittaa ajoissa, tai että asianomaisena olevan rekisteröidyn perusoikeudet ja -vapaudet eivät syrjäytä yleistä etua, jonka vuoksi siirto katsotaan tarpeelliseksi, kolmannen maan toimivaltaiselle viranomaiselle annetaan siirtoilmoitus viipymättä, ellei se ole epätarkoituksenmukaista tai tehotonta, siirron toteutettava toimivaltainen viranomais ilmoittaa vastaanottajalle, mitä tiettyä tarkoitusta tai tiettyjä tarkoituksia varten tämä saa ainoastaan käsitellä henkilötietoja jos tällainen tietojenkäsittely on tarpeellista. (Tietosuojadirektiivi, 39.artikla, 1.kohta.)

40.artiklassa on säädetty kansainvälisestä yhteistyöstä henkilötietojen suojaamiseksi. Komissiota ja jäsenvaltioita velvoitetaan toimimaan kolmansiin maihin ja kansainvälisiin järjestöihin nähden siten, että kansainvälisiä yhteistyökeinoja kehitetään henkilötietosuojalainsäädännön täytäntöönpanon edistämiseksi ja tarjotaan keskinäistä kansainvälistä apua kuten tutkinta-avun anto ja tietojen vaihto, henki-

lötietosuojalainsäädännön ja käytännön vaihdon sekä dokumentoinnin edistämisen esimerkiksi toimivaltariidoissa kolmansien maiden kesken (40.artikla).

4.7 Valvontaviranomaiset

Puitepäättöksen 2008/977/YOS 25.artikla käsittelee kansallisia valvontaviranomaisia. Siinä veloitetaan jäsenvaltioita säätämään yhden tai useamman viranomaisen neuvonta- ja valvontatehtävästä puitepäättöksen soveltamisesta täysin itsenäisesti ja kullakin viranomaisella on oltava artiklassa tarkemmin määritetyt tutkinta- ja toimintavaltuudet sekä asianosaisvaltuus tehtäviensä hoitamiseen. Lisäksi puitepäättöksessä on säädetty jokaisen henkilön oikeudesta esittää valvontaviranomaiselle oikeuksiensa ja vapauksiensa suojelua koskeva vaade henkilötietojen käsittelyn osalta ja valvontaviranomaisina toimivia jäseniä ja sen henkilöstöä sitovat kulloiseenkin toimivaltaiseen viranomaiseen sovellettavat tietosuojasäännökset ja salassapitovelvollisuus luottamuksellisten tietojen osalta, myös työssäolon jälkeenkin (puitepäättös, 25.artikla).

Uusi direktiivi säätää valvontaviranomaisista paljon laajemmin ja yksityiskohtaisemmin. Artiklat 41-44 on omistettu valvontaviranomaisen riippumattoman aseman käsittelyyn ja artiklat 45-49 sen toimivallalle, tehtäville ja valtuuksille.

4.7.1 Riippumattomuus

Kuten puitepäättöksessä, myös uusi direktiivi velvoittaa EU:n jäsenvaltioita säätämään yhden tai useamman viranomaisen valvontatehtävästä tämän direktiivin soveltamisen osalta, mutta sanamuotoa on tarkennettu siten, että vähintään yhden riippumattoman viranomaisen, josta jäljempänä käytetään nimitystä ”valvontaviranomainen”, on vastattava kyseisestä tehtävästä, jotta luonnollisen henkilön perusoikeudet ja -vapaudet tulevat suojatuiksi henkilötietokäsittelyssä ja tietojen va-

paata liikkuvuutta unionin alueella edistettäisiin. Direktiivin yhdenmukaiseen soveltamiseen unionin alueen sisällä tulee jokaisen valvontaviranomaisen pyrkiä myötävaikuttamaan ja tekemään tämän tavoitteen saavuttamiseksi keskinäistä ja komission välistä yhteistyötä (Tietosuojadirektiivi, 41.artikla, 1-2 kohdat). Jos valvontaviranomaisia on enemmän kuin yksi, tulee jäsenvaltion nimetä näistä viranomaisista yksi tietosuojaneuvostoon edustamaan muita (41.artikla, 4.kohta).

Jokaisen valvontaviranomaisen jäsenen tai jäsenien on tehtäviensä hoidossa ja direktiivin mukaisten valtuuksiensa käytössä toimittava täysin riippumattomasti ilman suoria tai välillisiä vaikuttamispyrkimyksiä ja ohjeiden ottaminen tai pyytäminen kaikilta tahoilta on kielletty. Lisäksi tulee jättäytyä pois kaikesta sellaisesta toimesta, joka on ristiriidassa valvontaviranomaistehtävien kanssa ja palkallisen tai palkattoman yhteensopimattoman ammattitoiminnan harjoittaminen toimikauden aikana on myös kielletty. Valvontaviranomaistehtävien hoitoon ja valtuuksien käyttöön, myös keskinäiseen yhteistyöhön ja avunantoon sekä tietosuojaneuvostossa toimimiseen liittyvät, on osoitettava riittävät ja tarvittavat resurssit, tilat ja infrastruktuuri, ja jokaisen valvontaviranomaisen henkilöstö on kyseisen viranomaisen itsensä valitsema ja tämän alaisuudessa toimiva. Varainhoidon valvonassa huomioidaan riippumattomuuden säilyminen ja jokainen valvontaviranomainen julkistaa vuosittaisen talousarvionsa, joka voi olla osa kansallista kokonaistalousarviota. (Tietosuojadirektiivi, 42.artikla.)

Jäsenvaltioissa toimivien valvontaviranomaisten jäsenten nimittämisoiikeus on kyseisen jäsenvaltion hallituksella, valtionpäämiehellä, parlamentilla tai jäsenvaltion lainsäädännön perusteella tällaisen oikeuden omaavalla riippumattomalla elimellä ja jokaiselta jäseneltä vaaditaan tehtäviensä hoitamiseen ja valtuuksiensa käyttämiseen tarvittava pätevyys, koulutus ja ammattitaito erityisesti henkilötietojen suojausta koskevilta aloilta. Valvontaviranomaisen jäsenen tehtävät katsotaan päättyneiksi kun toimikausi päättyy tai jäsen eroaa tai hänet erotetaan tehtävästään jäsenvaltion lakia noudattaen ja erottaminen on mahdollista vain vakavissa väärin-

käytöksissä tai jos vaaditut kriteerit velvollisuuksien hoidossa eivät enää täyty. (Tietosuojadirektiivi, 43.artikla.)

Valvontaviranomaisen perustamista koskevien sääntöjen mukaan tulee EU:n jäsenvaltioiden lakien sisältää jokaisen valvontaviranomaisen perustamisesta koskeva säädös sekä jokaista valvontaviranomaisen jäsentä tai jäseniä koskevat säädökset tarvittavista pätevyys- ja kelpoisuusvaatimuksista sekä säännöistä ja menettelytavoista, joita sovelletaan valvontaviranomaisen jäsenen tai jäsenten nimittämisessä, toimikauden pituudesta, joksi on säädetty vähintään neljä vuotta, paitsi 6.5.2016 jälkeen tapahtuvaa ensimmäistä nimitystä, jona aikana jäsenistä osa on mahdollista nimittää alle neljäksi vuodeksi, jos tämä katsotaan tarpeelliseksi valvontaviranomaisen riippumattomuuden turvaamiseksi, uudelleennimittämisestä ja uusien toimikausien määrästä sekä, mukaan lukien henkilöstö, säännöistä koskien työtehtävien päättymistä, toimikauden aikaisista ja sen jälkeisistä kielloista koskien ammatteja, etuja ja toimintaa, jotka ovat ristiriidassa omiin työtehtäviin nähden sekä velvollisuuskriteereistä. Lisäksi, kullakin valvontaviranomaisen jäsenellä tai jäsenillä ja henkilöstöllä on luottamuksellisten tietojen osalta salassapitovelvollisuus toimikautenaan, jolloin sitä sovelletaan erityisesti luonnollisten henkilöiden direktiivinrikkomusilmoituksiin, ja sen jälkeen. (Tietosuojadirektiivi, 44.artikla.)

4.7.2 Toimivalta, tehtävät ja valtuudet

Kullakin jäsenvaltion valvontaviranomaisella on omalla jäsenvaltionsa alueellaan tämän direktiivin mukainen toimivalta tehtäviensä hoitoon ja valtuuksiensa käyttöön, mutta toimivaltaa ei ole tuomioistuimien lainkäyttötehtävien yhteydessä suorittamien käsittelytehtävien valvontaan, ja jäsenvaltiot voivat säätää ettei valvontaviranomaisella ole toimivaltuuksia muiden riippumattomien oikeusviranomaisten lainkäyttötehtäviensä yhteydessä suorittamien käsittelytoimien valvontaan (tietosuojadirektiivi, 45.artikla).

Direktiivin 46.artiklan 1.kohdassa säädetään riippumattomille valvontaviranomaisille kuuluvista tehtävistä, joita ovat muun muassa direktiivin mukaisten säädösten soveltamisen valvonta ja niiden täytäntöönpano, käsittelyyn liittyvien riskien, sääntöjen, suojatoimien ja oikeuksien yleisen tietoisuuden ja ymmärryksen edistäminen sekä antaa tarvittaessa rekisteröidylle hänen direktiivin mukaisten oikeuksien käyttöä koskevia tietoja ja yhteistyön tekeminen muiden jäsenvaltioiden viranomaisten kesken kyseistä tarkoitusta varten (tietosuojadirektiivi, 46.artikla, 1.kohta).

Jäsenvaltioiden valvontaviranomaisilla on direktiivin 47.artiklan nojalla tutkintavaltuudet saada kaikki tarpeelliseksi katsomansa tiedot henkilötietokäsittelyyn liittyen rekisterinpitäjältä ja henkilötietojen käsittelijältä (tietosuojadirektiivi, 47.artikla, 1.kohta), toimintavaltuudet kuten varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää ennalta käsittelytoimien direktiivin vastaisuudesta, määrätä rekisterinpitäjä tai henkilötietojen käsittelijä suorittamaan käsittelytoimet direktiivin mukaisesti tarvittaessa tietyllä tavalla ja määrätyn ajan sisällä sekä määrätä käsittelykielto tai pysyvä/väliaikainen käsittelyrajoitus (47.artikla, 2.kohta). Lisäksi valvontaviranomaisilla on direktiivin mukaan oltava tehokkaat neuvontavaltuudet neuvojen antoon rekisterinpitäjälle 28.artiklan ennakkokuulemismenettelyn mukaisesti ja lausuntojen myöntämiseen joko erityisestä pyynnöstä tai omasta aloitteesta kaikissa henkilötietosuojaan liittyvissä asioissa kyseisen jäsenmaan hallitukselle, parlamentille tai kansallisen lainsäädännön mukaisille muille toimielimille sekä kansalaisille (47.artikla, 3.kohta). Artiklan mukaisen toimivallan käytössä sovelletaan unionin oikeuden ja jäsenvaltioiden lainsäädännön perusoikeuskirjan mukaisia oikeussuojakeinoja sekä muutoinkin asian- ja oikeudenmukaisia suojatoimimenettelyjä (47.artikla, 4.kohta) ja jos direktiivin mukaisia sääntöjä rikotaan, on valvontaviranomaisilla täydet valtuudet ilmoittaa rikkomuksista oikeusviranomaisille ja tarvittaessa aloittaa tai laittaa vireille oikeustoimet (47.artikla, 5.kohta).

4.8 Yhteistyö

Direktiivin 50.artikla säätelee keskinäisestä avunannosta. Valvontaviranomaisten on luovutettava toisilleen tarvittavia tietoja ja keskinäistä apua sekä toteutettava toimenpiteet tehokkaan keskinäisen yhteistyön varmistamiseksi (tietosuojadirektiivi, 50.artikla, 1.kohta) ja toisen valvontaviranomaisen esittämään pyyntöön on vastattava viipymättä ja viimeistään kuukauden sisällä pyynnön vastaanottamisesta (50.artikla, 2.kohta). Avunantopyynnön tulee sisältää kaikki tarvittavat tiedot, kuten sen tarkoitus, ja pyyntö tulee aina perustella, ja keskenään vaihdettuja tietoja ei saa käyttää muuhun kuin pyydettyyn tarkoitukseen (50.artikla, 3.kohta). Vastaanottavalla valvontaviranomaisella on oikeus kieltäytyä toteuttamasta pyyntöä ainoastaan, jos pyynnössä esitetty asia kuuluu toimivallan ulkopuolelle tai hänellä ei ole valtuuksia toteuttaa pyyntöä, tai jos pyynnön toteuttamisella valvontaviranomainen rikkoisi tämän direktiivin säännöksiä tai unionin oikeutta/jäsenmaan lainsäädäntöä, jota sovelletaan pyynnön vastaanottavaan valvontaviranomaiseen (50.artikla, 4.kohta). Tällaisessa tapauksessa tulee esittää syyt kieltäytymiseen ja vastaanottavan valvontaviranomaisen on annettava selvitys pyynnön lähettäneelle valvontaviranomaiselle miten asia etenee ja mitä ratkaisuja ja toimenpiteitä jatkossa tapahtuu. Kaikki toimitettavat tiedot on lähtökohtaisesti lähetettävä sähköisessä vakiomuodossa, eikä pyynnön vastaanottanut valvontaviranomainen ole oikeutettu perimään maksuja niistä toteutetuista toimista, jotka perustuvat keskinäistä avunantoa koskeviin pyyntöihin, mutta valvontaviranomaisten kesken voidaan sopia keskinäisestä avunannosta maksettavista korvauksista, jotka perustuvat poikkeuksellisissa olosuhteissa syntyneisiin erityisiin kustannuksiin (50.artikla, 5., 6. ja 7.kohta). Puitepäättös 2008/977/YOS ei sisällä valvontaviranomaisten keskinäisestä avunannosta ja yhteistyöstä säädettyä artiklaa.

Direktiivin 51.artiklassa on säädetty asetuksella (EU) 2016/679 perustetun tieto-

suojaneuvoston tehtävistä, jotka liittyvät direktiivin soveltamisalaan kuuluvaan käsittelyyn. Näitä ovat muun muassa erilaisten neuvojen, lausuntojen, suositusten ja suuntaviivojen antaminen esimerkiksi komissiolle ja valvontaviranomaisille kaikissa asioissa, jotka jollain tavoin liittyvät unionin henkilötietosuojaan ja tämän direktiivin soveltamisalaan sekä yhteistyön ja tietojen vaihdon edistäminen valvontaviranomaisten välillä EU rajojen sisä- ja ulkopuolella, ja tietosuojaoikeusperiaatteiden sekä niitä käsittelevien asiakirjojen vaihdon edistäminen tietosuojaviranomaisten kesken maailmanlaajuisesti (51.artikla, 1.kohta).

4.9 Oikeussuojakeinot, vastuu, seuraamukset ja loppusäännökset

Direktiivin artikkelat 52-57 käsittelevät oikeussuojakeinoja, vastuuta ja seuraamuksia. Puitepääöksessä 2008/977/YOS vastaavia asioita on käsitelty artikloissa 18-20 ja 24.

Rekisteröity on oikeutettu valittamaan yhdelle valvontaviranomaiselle jos rekisteröidyn mielestä häntä koskevassa henkilötietokäsittelyssä on menetelty virheellisesti ja direktiivin säännöksiä on rikottu (tietosuojadirektiivi, 52.artikla, 1.kohta). Ellei valitusta ole tehty 45.artiklan 1.kohdan mukaiselle toimivaltaiselle valvontaviranomaiselle, on valituksen vastaanottanut valvontaviranomainen velvollinen toimittamaan sen viipymättä toimivaltaiselle valvontaviranomaiselle ja ilmoittamaan tästä siirrosta rekisteröidylle, joka saa lisäapua niin halutessaan pyynnöstä valituksen vastaanottaneelta valvontaviranomaiselta ja toimivaltainen valvontaviranomainen on velvollinen ilmoittamaan rekisteröidylle miten valitus etenee ja mikä on sen lopullinen ratkaisupäätös sekä mahdollisuudesta käyttää 53.artiklan mukaisia oikeussuojakeinoja (52.artikla, 2., 3. ja 4.kohta).

Oikeus- tai luonnollisilla henkilöillä on oikeus tehokkaiden oikeussuojakeinojen käyttöön valvontaviranomaisen antamiin oikeudellisesti sitoviin ja heitä koskeviin

päätöksiin ja jos rekisteröidyn tekemä valitus on jätetty käsittelemättä tai rekisteröidylle ei ole ilmoitettu 52.artiklan mukaisen valituksen etenemisestä tai ratkaisusta toimivaltaisen valvontaviranomaisen taholta, tämän estämättä muitakaan hallinnollisia muutoksenhakukeinoja tai muita kuin pelkästään oikeudellisia oikeussuojakeinoja. Kanne valvontaviranomaista vastaan on nostettava sen jäsenvaltion tuomioistuimissa, jossa kyseisen valvontaviranomaisen toimipaikka sijaitsee (tietosuojadirektiivi, 53.artikla).

Edelleen, rekisteröidyllä on oikeus käyttää tehokkaita oikeussuojakeinoja rekisterinpitäjää tai henkilötietojen käsittelijää kohtaan, jos hänen näkemyksensä mukaan hänelle kuuluvia ja tähän direktiiviin perustuvia oikeuksiaan on rikottu virheellisen henkilötietokäsittelyn seurauksena, tämän kuitenkin edelleen estämättä muunlaisia hallinnollisia muutoksenhakukeinoja tai muita kuin oikeudellisia oikeussuojakeinoja, kuten 52.artiklassa säädetty valituksenteko-oikeus valvontaviranomaista kohtaan. (Tietosuojadirektiivi, 54.artikla.)

Rekisteröity voi halutessaan valtuuttaa jonkin järjestön, yhdistyksen tai elimen, joka edustaa rekisteröityjen oikeuksia ja vapauksia henkilötietosuojan osalta, laatimaan valitus ja käyttämään 52., 53. ja 54.artiklan mukaisia oikeuksia hänen puolestaan (tietosuojadirektiivi, 55.artikla).

Lisäksi direktiivissä on säädetty rekisterinpitäjän tai muun jäsenmaan lainsäädäntöön perustuvan toimivaltaisen viranomaisen vahingonkorvausvelvollisuudesta henkilöä kohtaan, jos lainvastaisen käsittelyn tai muun sellaisen menettelyn, jonka katsotaan rikkovan direktiivin mukaisia säännöksiä, seurauksena henkilölle katsotaan aiheutuneen joko aineellista tai aineetonta vahinkoa (tietosuojadirektiivi, 56.artikla).

Seuraamusten osalta, joiden tulee olla oikeasuhteisia, tehokkaita ja varoittavia, kaikkien jäsenvaltioiden tulee vahvistaa säännöt direktiivirikkomusten johdosta ja

varmistaa niiden täytäntöönpano kaikin tarvittavin toimenpitein. (Tietosuojadirektiivi, 57.artikla.)

Tietosuojadirektiivin (EU) 2016/680 loppusäännökset on säädetty 59-65 artikloissa. Puitepäättös 2008/977/YOS kumotaan 6.5.2018, jolloin uusi direktiivi (EU) 2016/680 astuu voimaan ja viittauksia kumottuun puitepäättökseen 2008/977/YOS katsotaan tällöin viittauksina uuteen direktiiviin (EU) 2016/680. (Tietosuojadirektiivi, 59.artikla.)

Jo voimassa oleviin, ennen 6.5.2016 lainvoiman saaneisiin, sellaisiin unionin säädöksiin, jotka koskevat henkilötietojen suojaa poliisiyhteistyön ja rikosasioissa tehtävän oikeudellisen yhteistyön aloilla, uudella direktiivillä ei ole vaikutusmerkitystä (tietosuojadirektiivi, 60.artikla).

Ennen 6.5.2016 jäsenvaltioiden kesken tehdyt kansainväliset sopimukset, jotka käsittelevät sekä poliisiyhteistyötä että rikosasioissa tehtävää oikeudellista yhteistyötä ja edellyttävät henkilötietojen siirtoa kansainvälisille järjestöille tai kolmansiin maihin, ovat voimassa kunnes ne muutetaan, korvataan tai poistetaan (tietosuojadirektiivi, 61.artikla).

62.artiklassa käsitellään komission kertomuksia liittyen tähän direktiiviin. Komission tulee arvioida ja uudelleen tarkastella voimaan tullutta direktiiviä sekä julkistaa ja toimittaa tehdystä arvioinnista erikseen laadittu kertomus Euroopan parlamentille ja neuvostolle ensimmäisen kerran 6.5.2022 mennessä ja tämän jälkeen säännöllisesti joka neljäs vuosi (tietosuojadirektiivi, 62.artikla, 1.kohta). Direktiiviä koskevassa tarkastelussa komission tulee kiinnittää erityistä huomiota kansainvälisiin järjestöihin ja kolmansiiin maihin suuntautuvaa henkilötietojen siirtoa koskevien säännösten soveltamiseen ja niiden toimivuuteen etenkin niiden päätösten osalta, jotka 36 artiklan 3 kohdan ja 39 artiklan nojalla hyväksytään (62.artikla, 2.kohta). Komissiolla on mahdollisuus tarvittaessa pyytää ja saada tietoja valvon-

taviranomaisilta sekä jäsenvaltioilta 1 ja 2 kohdissa määriteltyihin tarkoituksiin (62.artikla, 3.kohta) ja komission on otettava uudelleentarkasteluja tehdessään huomioon Euroopan parlamentin, neuvoston ja kaikkien muiden asianosaisten kannanotot ja näkemykset (62.artikla, 4.kohta). Lisäksi komissio voi ehdottaa direktiiviä muutettavaksi ottamalla erityisesti huomioon tietoyhteiskunnallinen ja -tekninen kehitys (62.artikla, 5.kohta). 6.5.2019 mennessä komission on käytävä läpi muita sellaisia unionin hyväksymiä säädöksiä, jotka koskevat 1.artiklan 1. kohdan mukaisia tarkoituksia varten toimivaltaisten viranomaisten toimesta tekemää käsittelyä, mukaan lukien 60.artiklan mukaiset unionin säädökset, jotta komissio kykenisi arvioimaan, tulisiko kyseiset säädökset yhdenmukaistaa tämän direktiivin kanssa ja tämän pohjalta antaa tarvittaessa muutosehdotuksia kyseisiin säädöksiin, jotta henkilötietojen suoja tulisi varmistetuksi direktiivin soveltamisalan puitteissa (62.artikla, 6.kohta).

63.artiklassa on säädökset siitä, miten direktiivi tulee saattaa osaksi kansallista lainsäädäntöä. Unionin jäsenvaltioiden on annettava ja julkaistava tämän direktiivin sisältämät lait, asetukset ja hallinnolliset määräykset viimeistään 6.5.2018, josta alkaen niitä tulee soveltaa ja jäsenvaltioiden on viipymättä annettava säännöksistä kirjallinen ilmoitus komissiolle. Jäsenvaltioiden antamissa säädöksissä on viitattava tähän direktiiviin tai niihin tulee liittää tällainen viittaus, kun ne virallisesti julkaistaan ja jäsenvaltioiden päätettävissä on, miten nämä viittaukset tehdään (tietosuojadirektiivi, 63.artikla, 1.kohta). Jäsenvaltiolla on 1.kohdasta poiketen oikeus säätää, että jos siitä aiheutuu suhteetonta vaivaa, ennen 6.5.2016 luodut automatisoidut käsittelyjärjestelmät tulee saattaa 25.artiklan 1.kohdan mukaisiksi viimeistään 6.5.2023 (63.artikla, 2.kohta). Tämän lisäksi jäsenvaltiolla on oikeus 1. ja 2.kohdasta poiketen saattaa 2.kohdan mukaiset automatisoidut käsittelyjärjestelmät 25.artiklan 1.kohdan mukaiseksi tietyn määräajan puitteissa myöhemmin kuin 6.5.2023, viimeistään kuitenkin 6.5.2026, jos se muutoin aiheuttaisi vakavia ongelmia käsittelyjärjestelmän toiminnalle. Tällöin asianomaisen jäsenvaltion velvollisuutena on ilmoittaa komissiolle ongelmista ja niiden määräajasta,

jonka sisällä kyseinen jäsenvaltio aikoo saattaa automatisoidut käsittelyjärjestelmät 25.artiklan 1.kohdan mukaisiksi (63.artikla, 3.kohta). Jäsenvaltioiden tulee toimittaa kirjallisina tämän direktiivin mukaisista kysymyksistä laaditut keskeiset kansalliset säännökset komissiolle (63.artikla, 4.kohta).

Tämä direktiivi astuu voimaan seuraavana päivänä siitä, kun se julkaistaan Euroopan unionin virallisessa lehdessä (euvi). (Tietosuojadirektiivi, 64.artikla.)

Direktiivi on osoitettu kaikille unionin jäsenvaltioille. (Tietosuojadirektiivi, 65.artikla.)

5. SUOMI JA YLEINEN TIETOSUOJA-ASETUS

Suomi on valmistautunut EU:n tietosuojauudistukseen jo monin eri tavoin. Tietosuojavaltuutetun toimisto on julkaissut 24.1.2017 rekisterinpitäjille tarkoitetun oppaan ”miten valmistautua EU:n tietosuoja-asetukseen”, joka sisältää muun muassa tietoja henkilötietojen käsittelyä koskevista oikeusperusteista ja arvioinnista, tietosuojakäytäntöjen toteutuksesta sekä varautumisesta tietoturvaloukkauksiin. Lisäksi oppaassa on selvitetty rekisteröityjen oikeuksia koskevia muutoksia ja riskiperusteisen lähestymistavan merkitystä rekisterinpitäjille. Opas on tehty yhteistyössä oikeusministeriön kanssa ja sen tarkoituksena on helpottaa henkilötietoja käsitteleviä eri organisaatioita valmistautumaan EU:n yleisen tietosuoja-asetuksen kansalliseen soveltamiseen antamalla ohjeita ja neuvoja millaisia toimenpiteitä näiden tulisi olla valmis toteuttamaan kahden vuoden siirtymäajan umpeutuessa 25.5.2018. Oppaassa ohjeistetaan ja neuvotaan EU:n yleisen tietosuoja-asetuksen mukaisesta henkilötietojen käsittelystä ja kohdistettu pääasiassa rekisterinpitäjille, mutta sopii soveltuvin osin myös henkilötietojen käsittelijälle. (Tietosuojavaltuutetun toimisto, ”miten valmistautua EU:n tietosuoja-asetukseen”, viitattu 16.4.2017.)

Oikeusministeriössä on myös perustettu 17.2.2017 työryhmä, jonka tarkoituksena on kartoittaa ja tarkistaa voimassa oleva henkilötietosuojaa koskeva kansallinen lainsäädäntö EU:n tietosuojauudistuksen mukaisesti. Hanke liittyy siis EU:n tietosuojauudistukseen ja sen tavoitteena on voimassa olevan henkilötietolain (523/1999) toimivuuden ja erityissäännösten tarpeellisuuden ja merkityksellisyyden arviointi sekä lainsäädännön toimivuuden ja johdonmukaisuuden varmistaminen sekä selkeyttäminen oikeuksien ja velvollisuuksien paremman toteuttamisen puolesta. Työryhmän tehtävänä on selvittää kansalliset lainsäädäntötoimenpiteet vastaamaan Euroopan unionin yleistä tietosuoja-asetusta ja onko henkilötietolain mukainen yleinen kansallinen tietosuojalainsäädäntö tarpeen sekä valmistelutyönä antaa ehdotus mahdollisesti tarvittavasta yleisestä tietosuojalainsäädännöstä. Li-

säksi työryhmän on selvitettävä kansallisen tietosuojaviranomaislainsäädännön tilanne, tulisiko sitä tarkistaa, ja valmistella ehdotus uudesta mahdollisesta laista, joka koskee kansallisia tietosuojaviranomaisia, sen organisaatiota, toimivaltuuksia ja tehtäviä. Edelleen, työryhmän tulee selvittää millaisen liikkumavaran EU:n yleinen tietosuoja-asetus antaa kansalliselle lainsäädännölle ja antaa esitys miten tätä liikkumavaraa tulisi järkevästi ja tarkoituksenmukaisesti käyttää jotta se palvelisi parhaiten kansalaisten oikeusturvaa, sekä avustaa lainvalmistelutyössä ja koordinoinnissa koskien henkilötietokäsittelystä annetun erityislainsäädännön tarkistamista. Työryhmän on otettava työtehtävissään huomioon Suomen hallituksen laatiman hallitusohjelman mukaiset tavoitteet, kuten kansallisesta lisäsääntelystä pidättäytyminen EU-lainsäädäntöä toimeenpantaessa, kansalaisten itsemääräämisen ja valvomisoikeuden vahvistaminen heitä itseään koskevissa henkilötietokäsittelyissä sekä viranomaisten välisen sujuvan tiedonsiirron varmistaminen ja tarpeettoman erityissääntelyn poistaminen. Lainsäädännön muutosehdotukset työryhmän on laadittava hallituksen esityksen muotoon ja mietintö saatava valmiiksi 31.5.2017 mennessä. (Tietosuojavaltuutetun toimisto, viitattu 16.4.2017.)

EU:n tietosuoja-asetuksen kansallinen sovellettavuusvelvoite koskee sekä yksityistä että julkista sektoria ja huolimatta siitä, että asetus on suoraan kansallista lainsäädäntöä velvoittava säädös, jättää se myös liikkumavaraa erityisesti julkisella mutta myös yksityisellä sektorilla. Uusi EU:n tietosuoja-asetus määrittelee siinä rajat, joiden puitteissa Suomikin voi säätää ja tarkentaa omaa kansallista tietosuojalainsäädäntöään, jonka sallitaan tiettyssä määrin poikkeavan asetuksessa vahvistetuista velvoitteista. (Tietosuojavaltuutetun toimisto, viitattu 16.4.2017.)

Suomen intressinä on ollut nykyisen kaltaisen biopankkitoiminnan, sukututkimuksen ja palkkatilastoinnin jatkaminen tietosuoja-asetuksen antamissa raameissa sekä erityisesti asiakirjajulkisuuden ja läpinäkyvyyden huomioiminen. Asetus sisältääkin artiklan, jonka perusteella kansallista julkisuuslakia voidaan soveltaa tietosuoja-asetuksen mukaisesti ilman ristiriitoja ja säilyttää hallinnollinen läpinäky-

vyys, avoimuus ja asiakirjajulkisuus. Lisäksi Suomen tavoitteena ja pyrkimyksenä kaikissa neuvotteluissa on ollut se, että tietosuoja-asetukseen sisällytetyt vaatimukset ja velvoitteet koskien rekisterinpitäjiä, kuten yrityksiä ja yhteisöjä, olisivat kustannuksiltaan kohtuullisia. Tällaisia tietosuojauudistuksen myötä suomalaisia yrityksiä koskettavia uusia kustannuksia ovat muun muassa tietosuojavastaavan nimittämisvelvollisuus ja tietoturvaloukkauksien ilmoitusvelvollisuus. Terveystieteiden huoltoalalla toimivat yritykset, kuten apteekit, ovat jo nykyäänkin velvollisia nimittämään tietosuojavastaavan. (Tietosuojavaltuutetun toimisto, viitattu 16.4.2017)

EU:n yleinen tietosuoja-asetus syrjäyttää voimassa olevan vuoden 1995 EU:n henkilötietodirektiivin (95/46/EY) ja korvaa täten myös Suomen kansallisen tietosuojalainsäädännön, henkilötietolain (523/1999), siltä osin kuin henkilötietojen käsittelyyn liittyvät säännökset lukeutuvat asetuksen soveltamisalaan. Alustavien arvioiden mukaan Suomessa tällaisia kansallisia säädöksiä, jotka sisältävät henkilötietojen käsittelyyn liittyviä säännöksiä, on useita satoja, jotka ovat lisäksi jakaantuneet useille eri ministeriöiden hallinnonaloille. Kaikki tällaiset säännökset tulee saattaa Suomen kansallisessa lainsäädännössä vastaamaan EU:n yleistä tietosuoja-asetusta, sen mahdollistaman kansallisen liikkumavaran puitteissa. EU:n tietosuojauudistus tulee vahvistamaan ja selkeyttämään Suomessa henkilötietojen suojaa sekä tätä koskevaa sääntelyä (Tietosuojavaltuutetun toimisto, viitattu 16.4.2017.)

6. JOHTOPÄÄTÖKSET

Henkilötietodirektiivin 95/46/EY tavoitteena oli suojata henkilötietosuojaoikeudet ja sallia henkilötietojen vapaa liikkuvuus Euroopan unionin alueella ja puitepäättös 2008/977/YOS luotiin myöhemmin täydentämään henkilötietodirektiiviä erityisesti poliisiyhteistyössä ja rikosasioihin liittyvässä oikeudellisessa yhteistyössä.

Yleinen tietosuojasetus (EU) 2016/679 ja tietosuojadirektiivi (EU) 2016/680 pitävät yllä näitä tärkeitä periaatteita ja tavoitteita sekä jatkavat voimassa olevien tietosuojasäännösten edelleen kehittämistä henkilötietomäärän jatkuvasti kasvavassa maailmalla tapahtuvan yleisen tietoteknillisen ja digitaalisen kehityksen sekä globalisaation seurauksena.

EU:n tietosuojauudistus tulee yhtenäistämään henkilötietojen käsittelyyn liittyviä tietosuojakäytäntöjä koko EU:n alueella, mikä vahvistaa ihmisten henkilötietosuojaan liittyviä oikeuksia ja vapauksia, helpottaa tietojen vapaata liikkuvuutta sekä vähentää hallinnollista byrokratiaa. Rekisterinpitäjien ja henkilötietojen käsittelijöiden lisääntyneeseen vastuuvollisuuteen on tietosuojauudistuksessa kiinnitetty erityistä huomiota. Tämän johdosta esimerkiksi julkiset sekä yksityiset yritykset ja laitokset joutuvat uudelleenarvioimaan tietosuojakäytäntöjään sanktio- ja seuraamusuhalla, ja rekisteröityjen tietosuojaoikeudet tulevat paremmin otetuiksi huomioon ja vahvistumaan entisestään.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 vahvistaa Euroopan ja sen ulkopuolisten alueiden turvallisuutta luomalla yhtenäisen EU-säädöksen henkilötietojen käsittelyissä, jotka liittyvät rikosten ennalta estämiseen, tutkimiseen, paljastamiseen tai rikoksiin liittyviin syytetoimiin taikka rikosoikeudellisten seuraamusten täytäntöönpanoon sekä tällaisten tietojen vapaaseen liikkuvuuteen.

Kaikkialla ja etenkin Euroopassa voimakkaasti lisääntynyt levottomuus, väkivalta ja terrorismi edellyttävät entistä parempia turvatoimia sekä nopeaa ja välitöntä tietojen vaihtoa eri poliisi- ja tiedusteluinstituutioiden välillä, minkä yhtenäinen EU-direktiivi tulee nyt mahdollistamaan entistä paremmin ja tehokkaammin.

Yleinen tietosuojalainsäädäntö (EU) 2016/679 vastaa kasvaneeseen teknologian kehitykseen ja globalisaation haasteisiin luomalla yhtenäisen tietosuojakehyksen henkilötietojen käsittelyssä EU-alueella ja sallimalla tietojen entistä vapaamman liikkuvuuden Euroopassa ja sen ulkopuolella turvallisesti. Lisäksi asetusta lisäluottamusta henkilötietojen globaalissa siirroissa maailmanlaajuisesti ja vahvistaa täten digitaalitaloutta EU:n sisämarkkinoilla. Yhtenäinen henkilötietolainsäädäntö EU-alueella tukee ja helpottaa kaupankäyntiä yli EU-rajojen ja yksittäisten kansalaisten luottamus esimerkiksi verkkokauppaan kasvaa kun on tiedossa että henkilötietoja käsitellään asianmukaisesti ja asetuksen mukaan.

LÄHTEET

Erityisbarometritutkimus (EB) 359, Data Protection and Electronic Identity in the EU (2011), viitattu 4.4.2015.
http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Eurooppa-neuvosto 2015. Tietosuojauudistus. Viitattu 11.3.2015.
<http://www.consilium.europa.eu/fi/policies/data-protection-reform/>

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus). Viitattu 5.6.2016. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&rid=1>

Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuojasetus (ehdotus)) COM (2012) 11 final. Viitattu 6.7.2015. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0011&rid=1>

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, 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. Viitattu 5.6.2016. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L0680&rid=3>

Euroopan parlamentin ja neuvoston direktiivi (ehdotus) yksilöiden suojelusta toi-

mivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta COM (2012) 10 final. Viitattu 2.5.2016. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52012PC0010&rid=1>

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Viitattu 2.4.2015. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:31995L0046&rid=1>

Euroopan parlamentin päätöslauselma 6. heinäkuuta 2011 kattavasta lähestymistavasta henkilötietojen suojaan Euroopan unionissa (2011/2025(INI)). Viitattu 2.4.2016. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52011IP0323&rid=2>

Euroopan unionin perusoikeuskirja. Viitattu 6.7.2015. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=FI>

Euroopan unionin virallinen lehti (euvi), s.47. Viitattu 6.7.2015. <http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ:C:2016:202:TOC>

Henkilötietolaki 22.4.1999/523. Viitattu 8.8.2016.

Komission tiedonanto Euroopan parlamentille (COM(2016) 213 final) Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 6 kohdan mukaisesti neuvoston kannasta yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen

2008/977/YOS kumoamisesta annettavan Euroopan parlamentin ja neuvoston direktiivin hyväksymiseen. Viitattu 6.7.2016. <http://eur-lex.europa.eu/legal-content/FI7txt7PDF/?uri=CELEX:52016PC0213&rid=3>

Lissabonin sopimus. Viitattu 4.7.2015. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=FI>

Neuvoston ensimmäisessä käsittelyssä vahvistama kanta (5418/1/16 REV 1) Euroopan parlamentin ja neuvoston direktiivin antamiseksi luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytöksiä tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. Neuvosto hyväksynyt 8 päivänä huhtikuuta 2016. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CONSIL:ST_5418_2016_REV_1&rid=1

Neuvoston puitepätös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta. <http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32008F0977&rid=8>

Tietosuojavaltuutetun toimisto, tietosuojauudistus. Viitattu 16.4.2017. <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html>