

UUSI TIETOSUOJA- LAINSÄÄDÄNTÖ

Päivi Korpisaari – Olli Pitkänen – Eija Warma-Lehtinen

Päivi Korpisaari on viestintäoikeuden professori Helsingin yliopistossa. Korpisaari on tutkinut viestintä- ja informaatio-oikeutta yli 25 vuoden ajan. Hän on johtanut useita tietosuojaan liittyviä tutkimusprojekteja ja osallistunut asiantuntijana moniin lainvalmisteluhankkeisiin.

Olli Pitkänen on tutkimusjohtaja IPR University Centerissä sekä dosentti Aalto-yliopistossa ja Helsingin ja Turun yliopistoissa. Koulutukseltaan hän on tekniikan tohtori ja lakimies. Hän on vetänyt lukuisia tutkimusprojekteja, joissa on tutkittu erityisesti tieto- ja viestintätekniikkaan liittyviä oikeudellisia kysymyksiä.

Eija Warma-Lehtinen Asianajaja, LL.M., CIPP/E on yksi johtavista tietosuojalainsäädännön asiantuntijoista Suomessa ja arvostettu osaja myös kansainvälisesti. Hän on jo vuosia vastannut Asianajotoimisto Castrén & Snellmanilla tämän oikeudenalan toimeksiantojen hoitamisesta.

Copyright © 2018 Alma Talent Oy ja tekijät
Yhteistyössä Lakimiesliiton Kustannus

Kansi: Outi Pallari
Taitto: NotePad Ay

ISBN 978-952-14-3169-2
ISBN (verkkokirja) 978-952-14-3170-8
BALTOprint Liettua 2018

Anna palautetta kirjasta: protoimitus@almamedia.fi

Esipuhe

EU:n tietosuojalainsäädännön uudistaminen käynnistyi vuonna 2012, kun tietosuojalainsäädäntö ei enää vastannut globaalin tietoympäristön ja digitaalitalouden tarpeisiin. Uudistuksen tarkoituksena oli turvata henkilötietojen suoja samalla, kun parannettaisiin EU:n sisämarkkinoiden toimintaedellytyksiä. Tämän prosessin tuloksena syntyivät tässä kirjassa käsiteltävä EU:n yleinen tietosuoja-asetus (GDPR) (EU) 2016/679, ja kirjan alan ulkopuolelle jäävä rikosasioita koskeva tietosujadirektiivi (EU) 2016/680.

Uusi tietosuoja-asetus on henkilötietojen käsittelyä koskeva yleis-säädös. Se tuli voimaan 25.5.2016, ja sitä on sovellettu 25.5.2018 lukien. Asetuksessa on kansallista liikkumavaraa, jonka käyttämisestä säädetään uudessa tietosuojalaissa. Hallituksen esitys EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi annettiin eduskunnalle maaliskuun alussa 2018, ja eduskunta hyväksyi sen 13.11.2018 hallintovaliokunnan mietinnön mukaisesti muutettuna. Halusimme sisällyttää kirjaamme myös uuden tietosuojalain, vaikka sen lopullinen sisältö vahvistui vasta juuri ennen kirjamme valmistumista, eikä aikaa sen huomioon ottamiseen siten ollut kovin paljon.

Yleislainsäädännössä olevan sääntelyn määrä lisääntyi merkittävästi tietosuojauudistuksen myötä. Henkilötietolaissa oli 51 pykälää, kun tietosuoja-asetuksessa on 99 artiklaa, joista monet ovat hyvinkin laajoja ja monimutkaisia, ja tietosuojalaissa on vielä tämän lisäksi 38 pykälää. Tietosuojalain ohella henkilötietojen käsittelystä säädetään edelleen myös sektorikohtaisessa lainsäädännössä.

Kirjan kirjoittaminen uuden lainsäädännön voimaantulo- ja syntyvaiheessa on omalla tavallaan haastavaa, koska tulkintaohjeita tai -kannanottoja ei kovin paljon ole – oikeuskäytännöstä puhumattakaan. Aikaisempaa kirjallisuutta ja ratkaisukäytäntöä on hyö-

dynnetty soveltuvien osien, ja jo kirjoitettujakin osia on päivitetty ja uudelleenkirjoitettu sitä mukaa, kun esimerkiksi Euroopan tietosuojaneuvoston ohjeistuksia on julkaistu.

Kirjan kirjoittajista Päivi Korpisaari oli EU:n yleisen tietosuojasetuksen täytäntöönpanotyöryhmän (ns. TATTI-työryhmän) jäsen koko sen toimikauden (17.2.2016–16.2.2018) ajan. Lisäksi Korpisaari toimi kirjan kirjoittamisen aikana henkilötunnuksen uudistamista valmistelleen työryhmän (ns. HETU-työryhmän) johtoryhmän jäsenenä. Olli Pitkänen puolestaan on vetänyt Valtioneuvoston kanslian rahoittaman EU:n yleisen tietosuojasetuksen (2016/679) kansallista toimeenpanoa selvittäneen erillishankkeen ja tutkinut uudistuksen vaikutuksia mm. Business Finlandin ja yritysten rahoittamassa Future Regulation of Industrial Internet (FRII)-tutkimushankkeessa. Eija Warma-Lehtinen on avustanut lukuisia suomalaisia ja kansainvälisiä organisaatioita erilaisissa tietosuojasetukseen ja sen voimaantumiseen liittyvissä projekteissa.

Haluamme kiittää läheisiamme tuesta ja jaksamisesta kirjoitusprosessin aikana sekä sisältöpäällikkö Arja Lappeteläistä ja kustannustoimittaja Inka Remonen-Niitepöldiä kaikesta avusta kirjan valmiiksi saattamisessa.

Helsingissä, marraskuun 30. päivänä 2018.

Kirjoittajat

Sisällys

Esipuhe	V
Lyhenteet	XV
Pikaopas	XVII
Lukijalle	XIX
Johdanto	1
Tutkimuksen kohde ja lähdeaineisto.....	1
Henkilötietojen suoja perus- ja ihmisoikeutena	5
Henkilötietojen ja yksityiselämän suojien suhde.....	13
Muuttuneen soveltamisympäristön luomat haasteet	16
Henkilötietojen erilaiset suojakeinot	17
Voiko omia tietojaan omistaa?	20
Periaatteet	23
Riskienhallinta	25
Osapuolet	28
Lähdeaineisto	29
I YLEISET SÄÄNNÖKSET	33
1 ARTIKLA Kohde ja tavoitteet	34
2 ARTIKLA Aineellinen soveltamisala	38
3 ARTIKLA Alueellinen soveltamisala	45
4 ARTIKLA Määritelmät	49

II PERIAATTEET	87
5 ARTIKLA Henkilötietojen käsittelyä koskevat periaatteet	88
6 ARTIKLA Käsittelyn lainmukaisuus	98
7 ARTIKLA Suostumuksen edellytykset	127
8 ARTIKLA Tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot	138
9 ARTIKLA Erityisiä henkilötietoryhmiä koskeva käsittely	146
10 ARTIKLA Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittely	164
11 ARTIKLA Käsittely, joka ei edellytä tunnistamista	168
III REKISTERÖIDYN OIKEUDET	171
12 ARTIKLA Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten	172
13 ARTIKLA Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä	183
14 ARTIKLA Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä	193
15 ARTIKLA Rekisteröidyn oikeus saada pääsy tietoihin	208
16 ARTIKLA Oikeus tietojen oikaisemiseen	216
17 ARTIKLA Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")	222
18 ARTIKLA Oikeus käsittelyn rajoittamiseen	235

19 ARTIKLA Henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus.....	239
20 ARTIKLA Oikeus siirtää tiedot järjestelmästä toiseen.	241
21 ARTIKLA Vastustamisoikeus.....	250
22 ARTIKLA Automatisoidut yksittäispäätökset, profilointi mukaan luettuna	257
23 ARTIKLA Rajoitukset.....	263
IV REKISTERINPITÄJÄ JA HENKILÖTIETOJEN KÄSITTELIJÄ.....	267
24 ARTIKLA Rekisterinpitäjän vastuu.....	268
25 ARTIKLA Sisäänrakennettu ja oletusarvoinen tietosuojaja	276
26 ARTIKLA Yhteisrekisterinpitäjät.....	282
27 ARTIKLA Unionin ulkopuolelle sijoittautuneiden rekisterinpitäjien tai henkilötietojen käsittelijöiden edustajat.....	286
28 ARTIKLA Henkilötietojen käsittelijä.....	290
29 ARTIKLA Tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa.....	297
30 ARTIKLA Seloste käsittelytoimista.....	298
31 ARTIKLA Yhteistyö valvontaviranomaisen kanssa	304
32 ARTIKLA Käsittelyn turvallisuus	305
33 ARTIKLA Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle.....	312

34 ARTIKLA Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle.....	323
35 ARTIKLA Tietosuoja koskeva vaikutustenarviointi	327
36 ARTIKLA Ennakkokuuleminen.....	342
37 ARTIKLA Tietosuojavastaavan nimittäminen	346
38 ARTIKLA Tietosuojavastaavan asema	359
39 ARTIKLA Tietosuojavastaavan tehtävät.....	366
40 ARTIKLA Käytännesäännöt	370
41 ARTIKLA Hyväksytyjen käytännesääntöjen seuranta.....	378
42 ARTIKLA Sertifiointi	381
43 ARTIKLA Sertifiointielimet	387
V HENKILÖTIETOJEN SIIRROT KOLMANSIIN MAIHIN TAI KANSAINVÄLISILLE JÄRJESTÖILLE	391
44 ARTIKLA Siirtoja koskeva yleinen periaate	392
45 ARTIKLA Siirto tietosuojan riittävyttä koskevan päätöksen perusteella	397
46 ARTIKLA Siirto asianmukaisia suojatoimia soveltaen ..	403
47 ARTIKLA Yritystä koskevat sitovat säännöt.....	408
48 ARTIKLA Siirrot ja luovutukset, joita ei sallita unionin lainsäädännössä.....	414
49 ARTIKLA Erityistilanteita koskevat poikkeukset	416
50 ARTIKLA Kansainvälinen yhteistyö henkilötietojen suojaamiseksi.....	422

VI RIIPPUMATTOMAT VALVONTAVIRANOMAISET....	425
51 ARTIKLA Valvontaviranomainen	426
52 ARTIKLA Riippumattomuus.....	430
53 ARTIKLA Valvontaviranomaisen jäseniä koskevat yleiset edellytykset.....	435
54 ARTIKLA Valvontaviranomaisen perustamista koskevat säännöt	437
55 ARTIKLA Toimivalta	440
56 ARTIKLA Johtavan valvontaviranomaisen toimivalta.....	443
57 ARTIKLA Tehtävät	448
58 ARTIKLA Valtuudet.....	453
59 ARTIKLA Toimintakertomukset.....	460
VII YHTEISTYÖ JA YHDENMUKAISUUS.....	461
60 ARTIKLA Johtavan valvontaviranomaisen ja muiden osallistuvien valvontaviranomaisten välinen yhteistyö.....	462
61 ARTIKLA Keskinäinen avunanto.....	468
62 ARTIKLA Valvontaviranomaisten yhteiset operaatiot	472
63 ARTIKLA Yhdenmukaisuusmekanismi	476
64 ARTIKLA Tietosuojaneuvoston lausunto	478
65 ARTIKLA Euroopan tietosuojaneuvoston kiistan- ratkaisumenettely	483
66 ARTIKLA Kiireellinen menettely	487

67 ARTIKLA Tietojenvaihto	489
68 ARTIKLA Euroopan tietosuojaneuvosto	490
69 ARTIKLA Riippumattomuus	492
70 ARTIKLA Tietosuojaneuvoston tehtävät	493
71 ARTIKLA Kertomukset	500
72 ARTIKLA Menettely	501
73 ARTIKLA Puheenjohtaja	502
74 ARTIKLA Puheenjohtajan tehtävät	503
75 ARTIKLA Sihteeristö	504
76 ARTIKLA Tietojen salassapito	506
VIII OIKEUSSUOJAKEINOT, VASTUU JA SEURAAMUKSET	507
77 ARTIKLA Oikeus tehdä valitus valvontaviranomaiselle	508
78 ARTIKLA Oikeus tehokkaiiin oikeussuojakeinoihin valvontaviranomaista vastaan	510
79 ARTIKLA Oikeus tehokkaiiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan	514
80 ARTIKLA Rekisteröityjen edustaminen	517
81 ARTIKLA Menettelyn keskeyttäminen	519
82 ARTIKLA Vastuu ja oikeus korvauksen saamiseen	522
83 ARTIKLA Hallinnollisten sakkojen määräämisen yleiset edellytykset	532
84 ARTIKLA Seuraamukset	547

IX TIETOJENKÄSITTELYYN LIITTYVIÄ ERITYISTILANTEITA KOSKEVAT SÄÄNNÖKSET	571
85 ARTIKLA Käsittely ja sananvapaus ja tiedonvälityksen vapaus	572
86 ARTIKLA Henkilötietojen käsittely ja virallisten asiakirjojen julkisuus	584
87 ARTIKLA Kansallisen henkilötunnuksen käsitleminen	592
88 ARTIKLA Käsittely työsuhteen yhteydessä	602
89 ARTIKLA Yleisen edun mukaisia arkistointi- tarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten tapahtuvaa käsittelyä koskevat suojatoimet ja poikkeukset	608
90 ARTIKLA Salassapitovelvollisuus	622
91 ARTIKLA Kirkkojen ja uskonnollisten yhdistysten voimassa olevat tietosuojasäännöt	625
92 ARTIKLA Siirretyn säädösvallan käyttäminen	627
93 ARTIKLA Komiteamenettely	629
XI LOPPUSÄÄNNÖKSET	633
94 ARTIKLA Direktiivin 95/46/EY kumoaminen	634
95 ARTIKLA Suhde direktiiviin 2002/58/EY	637
96 ARTIKLA Suhde aiemmin tehtyihin sopimukseen	639
97 ARTIKLA Komission kertomukset	641
98 ARTIKLA Unionin muiden tietosuojasäädösten uudelleentarkastelu	643

Sisällys

99 ARTIKLA Voimaantulo ja soveltaminen.....	645
Lopuksi	647
Lähteet	651
Asiahakemisto.....	667

Lukijalle

Henkilötietojen suoja on nykyaikaisessa yhteiskunnassa yhä tärkeämpi osa oikeusjärjestelmää. Tietosuojalla on huomattavaa merkitystä sekä yksityiselämässä, elinkeinotoiminnassa että julkishallinnossa. Henkilötietolainsäädännön tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Viime aikoina henkilötietojen suoja on saanut suorastaan ylenpalttista huomiota. Siihen on toisaalta vaikuttanut EU:n uusi yleinen tietosuojasetus (General Data Protection Regulation, *GDPR*) ja sen ympärillä liikkuneet perättömätkin käsitykset lainsäädännön uusista vaatimuksista. Toisaalta Facebookin, Cambridge Analytican ja joidenkin muiden yritysten tekemät pahat virheet henkilötietojen käsittelyssä ja niistä aiheutuneet skandaalit ovat saaneet ihmiset kiinnostumaan tietoihinsa liittyvistä oikeuksista ja yritykset puolestaan ottamaan vakavammin henkilötietojen käsittelyyn liittyvät riskit.

Innoitus tämän kirjan kirjoittamiseen syntyi sekä käytännön lakimiestyössä että tutkimuksessa havaitusta tiedon tarpeesta. Tietosuojasetus on varsin monimutkainen ja vaikeaselkoinen säädös, jota joudutaan tulkitsemaan ja soveltamaan hyvin monenlaisissa tilanteissa ja myös muiden kuin juristien toimesta. Näin ollen pidimme tarpeellisenä kattavan yleisesityksen laatimista asetuksesta ja siihen liittyvästä kansallisesta lainsäädännöstä.

Olemme tehneet kirjan yhdessä. Pohjatekstiä kirjoittaessamme työnjako oli seuraava:

- Korpisaari: artikkelat 4–19, 21, 24, 26, 51–61, 85–86 ja 99
- Pitkänen: johdanto, artikkelat 1–3, 20, 22–23, 25, 28, 32–36, 77–84 ja 87–98
- Warma-Lehtinen: artikkelat 27, 29–31, 37–50, 62–76 ja loppusanat.

Olemme kuitenkin kaikki muokanneet myös toistemme alun perin kirjoittamia tekstejä, joten voimme sanoa kirjan olevan aidosti yhteistyömme tulos.

Osittain olemme myös hyödyntäneet aikaisemmassa yhteisessä kirjassamme Pitkänen – Tiilikka – Warma, Henkilötietojen suoja (Talentum 2013) kirjoittamiemme tekstejä. Monet aikaisemman lainsäädännön mukaiset periaatteet ovat pysyneet samoina, mutta yksityiskohdat ovat kuitenkin muuttuneet niin paljon, että vähintäänkin tekstien uudelleenmuotoilu on yleensä ollut tarpeen.