

ALKUSANAT	11
1. JOHDANTO	13
1.1 Kirjan tavoite	13
1.2 Muutokseen varautuminen	15
2. TIETOSUOJA-ASETUksen KESKEISET KÄSITTEET	18
2.1 Käsiteistä ja niiden tarpeesta	18
2.2 Asetuksen yleiset soveltamisedellytykset	18
2.3 Henkilötieto	19
2.4 Rekisteröity	20
2.5 Käsittely	20
2.6 Profilointi	21
2.7 Anonymisointi	21
2.8 Pseudonymisointi	21
2.9 Rekisteri	22
2.10 Rekisterinpitäjä	22
2.11 Henkilötietojen käsittelijä	22
2.12 Vastaanottaja	23
2.13 Suostumus	23
2.14 Tietoturvaloukkaus	23
3. HENKILÖTIEtojen KÄSITTELIJÄN JA REKISTERINPITÄJÄN ROOLIT JA VASTUUT	24
3.1 Rekisterinpitäjän ja henkilötietojen käsittelijän roolit	24
3.2 Miten rekisterinpitäjän ja henkilötietojen käsittelijän roolit määräytyvät?	25
3.3 Rekisterinpitäjän erityiset velvoitteet	26
3.4 Henkilötietojen käsittelijän erityiset velvoitteet	27
3.5 Yhteisrekisterinpitäjät	28
4. KÄSITTELYN LAINMUKAISUUS	29
4.1 Tietosuoja-asetuksen mukaiset käsittelyperusteet	29
4.1.1 Suostumus	30
4.1.2 Sopimus	30
4.1.3 Lakisääteiset velvoitteet	31
4.1.4 Elintärkeä etu	31
4.1.5 Yleinen etu tai julkisen vallan käyttö	31
4.1.6 Oikeutettu etu	32
4.2 Henkilötietojen käsittely muuta kuin alkuperäistä tarkoitusta varten	32
4.3 Oikeutettu etu	33

4.3.1	Intressipunninta oikeutetun edun ja rekisteröidyn oikeuksien välillä	33
4.3.2	Asiakkaiden ja työntekijöiden henkilötietojen käsittely	33
4.3.3	Konsernin sisäinen henkilötietojen käsittely	34
4.3.4	Suoramarkkinointi	34
4.4	Suostumuksen edellytykset	35
4.4.1	Suostumus edellyttää rekisteröidyn aktiivista toimintaa	36
4.4.2	Edellytyksenä rekisteröidyn tietoisuus ja vapaaehtoisuus	36
4.4.3	Suostumus arkaluonteisten tietojen käsittelyyn	37
4.4.4	Suostumuksen kattavuus ja esitystapa	37
4.4.5	Suostumuksen olemassaolo on pystyttävä osoittamaan	38
4.4.6	Mahdollisuus peruuttaa suostumus ja suostumuksen tarpeellisuus	38
4.4.7	Suostumus lapsen henkilötietojen käsittelyyn	39
5.	TIEDOT, JOIDEN KÄSITTELY VAATII ERITYISIÄ PERUSTEITA	40
5.1	Erityiset henkilötietoryhmät eli arkaluonteiset tiedot	40
5.1.1	Arkaluonteisten tietojen käsittely suostumuksen perusteella	41
5.1.2	Asiakkaiden arkaluonteiset tiedot	42
5.1.3	Arkaluonteisten tietojen käsittely sallitaan työlainsäädännössä	42
5.1.4	Työntekijöiden terveydentilatietojen käsittely	43
5.2	Rikostuomiot ja rikkomukset	44
5.3	Henkilötunnus	44
6.	TIETOJEN KÄSITTELYN YLEISET PERIAATTEET	47
6.1	Tietosuojaperiaatteet	47
6.1.1	Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys	48
6.1.2	Käyttötarkoitussidonnaisuus	49
6.1.3	Tietojen minimointi	49
6.1.4	Tietojen täsmällisyys	50
6.1.5	Tietojen säilytyksen rajoittaminen	50
6.1.6	Tietojen eheys ja luottamuksellisuus	51
6.1.7	Rekisterinpitäjän osoitusvelvollisuus	51
6.2	Sisäänrakennettu ja oletusarvoinen tietosuoja	54
6.3	Vaadittavat tekniset ja organisatoriset toimenpiteet	55
7.	REKISTERÖITYJEN HENKILÖIDEN OIKEUDET	56
7.1	Yrityksen tulee mahdollistaa rekisteröidyn oikeuksien käyttö	56
7.2	Rekisteröidyn tunnistaminen	57
7.3	Yrityksen toimet rekisteröidyn pyynnön vastaanottamisen jälkeen	58
7.4	Oikeus saada pääsy tietoihin	59
7.5	Oikeus tietojen oikaisemiseen	61

7.6 Oikeus tietojen poistamiseen eli oikeus tulla unohdetuksi	61
7.7 Oikeus käsittelyn rajoittamiseen	63
7.8 Oikeus siirtää tiedot järjestelmästä toiseen	64
7.8.1 Siirto-oikeuden kohteena olevat tiedot	66
7.8.2 Siirto-oikeuden toteuttaminen	67
7.9 Vastustamisoikeus	67
7.10 Automatisoituihin päätöksiin ja profilointiin liittyvät oikeudet	69
7.10.1 Oikeus olla joutumatta automatisoidun päätöksen kohteeksi	69
7.10.2 Tilanteet, joissa automatisoitu päätöksenteko on sallittua	70
7.10.3 Arkaluonteisten tietojen käsittely automatisoidussa päätöksenteossa	71

8. REKISTERÖITYJEN HENKILÖIDEN INFORMOINTI **73**

8.1 Läpinäkyvä informointi	73
8.2 Informointitavat	74
8.2.1 Tietosuojaselosteet	75
8.2.2 Suullinen informointi	76
8.2.3 Vakiomuotoiset kuvakkeet	76
8.3 Milloin tiedot tulee antaa?	76
8.4 Mitä tietoja rekisteröidyille on annettava?	78
8.4.1 Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä itseltään	78
8.4.2 Toimitettavat tiedot, kun henkilötietoja kerätään muualta kuin rekisteröidyltä	80

9. TIETOJENKÄSITTELYSOPIMUKSET **82**

9.1 Velvollisuus laatia tietojenkäsittelysopimus	82
9.1.1 Vakiosopimuslausekkeet	82
9.1.2 Sopimuksen sisältö	83
9.1.3 Varautuminen tietosuojasetuksen tulkintojen edellyttämiin muokkaamistarpeisiin	84
9.2 Tietosuojasetuksen erityisesti edellyttämät sopimusehdot	84
9.2.1 Henkilötietojen käsittely rekisterinpitäjän ohjeiden mukaisesti	84
9.2.2 Salassapitovelvollisuudet	85
9.2.3 Käsittelyn turvallisuudesta huolehtiminen asianmukaisilla toimenpiteillä	86
9.2.4 Alihankkijat	87
9.2.5 Rekisteröityjen pyyntöihin vastaaminen	87
9.2.6 Henkilötietojen käsittelijän avustusvelvollisuus	88
9.2.7 Tietojen poistaminen tai palauttaminen käsittelyn päättyessä	89
9.2.8 Auditointioikeus ja tarkastukset	89
9.3 Vastuut ja vahingonkorvaukset tietojenkäsittelysopimuksissa	90

9.3.1 Miten vastuuta voidaan rajoittaa?	90
9.3.2 Välittömät ja välilliset vahingot	90
9.3.3 Vastuunjakoehdo eli indemnity-ehto	91
9.4 Kustannusten jako ja maksut	91

10. LUOVUTUSSOPIMUKSET 93

10.1 Henkilötietojen luovuttaminen	93
10.2 Henkilötietojen luovuttamisen edellytykset	95
10.3 Luovutussopimuksen sisältö	95

11. HENKILÖTIETOJEN SIIRTO EU:N ULKOPUOLELLE 97

11.1 Siirtoja koskeva yleinen periaate	97
11.2 Siirto tietosuojan riittävyttä koskevan päätöksen perusteella	98
11.2.1 Yhdysvallat ja Privacy Shield -järjestelmä	99
11.3 Siirto asianmukaisia suojatoimia soveltaen	100
11.4 Vakiolausekkeet	101
11.4.1 Komission hyväksymiä	101
11.4.2 Vastaanottajan kyky huolehtia velvoitteista	101
11.4.3 Ei saa tehdä muutoksia	102
11.5 Yritystä koskevat sitovat säännöt	102
11.6 Muut asianmukaiset suojatoimet	103
11.7 Erityistilanteita koskevat poikkeukset	103

12. YRITYKSEN TIETOTURVA, KÄYTÄNNESÄÄNNÖT JA SERTIFIINTI 106

12.1 Tietoturva	106
12.1.1 Henkilötietojen käsittelyn turvallisuus	106
12.1.2 Tietoturvallisuuden varmistaminen	107
12.1.3 Luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus	107
12.2 Ilmoitusvelvollisuus tietoturvaloukkauksesta	108
12.2.1 Tietoturvaloukkaus	108
12.2.2 Ilmoitusvelvollisuus valvontaviranomaiselle	109
12.2.3 Aikaraja	109
12.2.4 Ilmoituksen sisältö	110
12.2.5 Tietoturvaloukkauksen dokumentointi	111
12.2.6 Tietoturvaloukkauksesta ilmoittaminen rekisteröidylle	111
12.2.7 Valmistautuminen ja prosessit	112
12.3 Käytännestä	113
12.4 Sertifiointi	114

13. VAIKUTUSTEN-ARVIOINTI	115
13.1 Mikä on vaikutustenarviointi ja milloin se tulee tehdä?	115
13.2 Vaikutustenarvioinnin tekeminen	117
14. TIETOSUOJAVASTAAVA	120
14.1 Tietosuojavastaavan nimittämisvelvollisuus	120
14.2 Tietosuojavastaavan asema ja tehtävät	122
15. VALVONTA JA SANKTIOT	124
15.1 Valvonta	124
15.1.1 Tietosuojavirasto ja seuraamuslautakunta	124
15.1.2 Rekisteröidyn valitusoikeus	125
15.1.3 One-stop-shop -mekanismi eli yhden luukun periaate	125
15.2 Selosteet käsittelytoimista	125
15.3 Ilmoitukset valvontaviranomaiselle ja muu yhteistyö valvontaviranomaisen kanssa	127
15.3.1 Tietoturvaloukkauksista ilmoittaminen	128
15.3.2 Ennakkokuuleminen korkean riskin tapauksissa	128
15.3.3 Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille	128
15.3.4 Muu yhteistyö viranomaisten kanssa	128
15.4 Sanktiot	129
15.4.1 Hallinnolliset sakot	129
15.4.2 Vahingonkorvausvastuu	130
15.4.3 Rikosoikeudellinen vastuu	131

ALKUSANAT

Tämä kirja on tarkoitettu käytännön oppaaksi etenkin pienille ja keskisuurille yrityksille niiden valmistautuessa EU:n uuteen tietosuoja-asetukseen. Siitä käytetään suomeksikin yhä useammin lyhennystä GDPR, joka tulee sen englanninkielisestä nimestä General Data Protection Regulation. Asetus on suoraan sovellettavaa lainsäädäntöä 25.5.2018 alkaen koko EU:n alueella.

Asetus koskee nimensä mukaisesti tietosuojaa eli henkilötietojen käsittelyä. Tällaista käsittelyä tapahtuu käytännössä kaikissa, tai ainakin lähes kaikissa yrityksissä, yhdistyksissä ja muissa yhteisöissä. Tämä käytännön opas pyrkii antamaan ohjeistusta, jonka perusteella yritykset osaisivat ottaa huomioon asetuksen mukanaan tuomat velvollisuudet tai ainakin havaitsisivat, mitä muutoksia mahdollisesti tarvitaan.

Olemme pyrkineet tarjoamaan parhaan mahdollisen tulkinta-avun ja opastuksen siihen, miten EU:n tietosuoja-asetusta tulisi soveltaa pienen tai keskisuuren yrityksen toiminnassa. Tämän kirjan kirjoittamisen aikaan emme ole vielä saaneet kaikkea tarpeellista viranomaisohjeistusta, joten tietosuoja-asetuksen aukoton tai takuuvarma tulkinta ei ole vielä mahdollista. Monet asiat tulevat todennäköisesti tarkentumaan tai varmistumaan vasta kirjan ilmestymisen ja tietosuoja-asetuksen soveltamiskäytännön myötä.

Kirjan ovat kirjoittaneet Eversheds Asianajotoimisto Oy:n tietosuoja-asiantuntijat asianajaja, osakas Markku Varhela, asianajaja Minna Hanninen, lakimies Elli Laine, asianajaja Kati Rantala ja asianajaja Mari Rusi. Kiitämme työnantajaamme mahdollisuudesta tehdä tämä kirja ja kannustuksesta kirjoitustyön varrella.

Helsingissä 23.11.2017

Tekijät