

KÄSIKIRJA

# Käsikirja Euroopan tietosuojaoikeudesta



COUNCIL OF EUROPE



© Tämän käsikirjan teksti saatiin valmiiksi huhtikuussa 2014  
Euroopan neuvosto, 2014

Tämän käsikirjan teksti saatiin valmiiksi huhtikuussa 2014.

Päivitettyjä versioita on myöhemmin saatavilla Euroopan unionin perusoikeusviraston verkkosivustolla osoitteessa [fra.europa.eu](http://fra.europa.eu), Euroopan neuvoston verkkosivuilla osoitteessa [coe.int/dataprotection](http://coe.int/dataprotection), ja Euroopan ihmisoikeustuomioistuimen verkkosivustolla oikeuskäytännön kohdalla osoitteessa [echr.coe.int](http://echr.coe.int).

Tekstin jäljentäminen on sallittu ei-kaupallisiin tarkoituksiin, kunhan lähde mainitaan.

***Europe Direct -palvelu auttaa sinua löytämään  
vastaukset EU:hun liittyviin kysymyksiisi.***

**Yhteinen maksuton palvelunumero (\*):**

**00 800 6 7 8 9 10 11**

(\* ) Saat pyytämäsi tiedot maksutta. Myös useimmat puhelut ovat maksuttomia, joskin jotkin operaattorit, puhelin kioskit tai hotellit voivat periä puhelusta maksun.

Foto (kansi & sisäpuolella): © iStockphoto

Euroopan unionia koskevia lisätietoja on saatavilla Internetissä (<http://europa.eu>).

Luettelointitiedot ovat teoksen lopussa.

Luxemburg: Euroopan unionin julkaisutoimisto, 2014

ISBN 978-92-871-9946-1 (Euroopan neuvosto)

ISBN 978-92-9239-496-7 (FRA)

doi:10.2811/73623

*Printed in Belgium*

PAINETTU KLOORIVALKAISEMATTOMALLE PAPERILLE (ECF)



Tämä käsikirja on laadittu englanniksi. Euroopan neuvosto (EN) ja Euroopan ihmisoikeustuomioistuin (EIT) ei vät vastaa kielitoisintojen laadusta. Tässä käsikirjassa esitetyt mielipiteet eivät sido Euroopan neuvostoa ja EIT:tä. Käsikirjassa viitataan erilaisiin lainselitysteoksiin ja käsikirjoihin. Euroopan neuvostoa ja EIT ei vät vastaa näiden julkaisujen sisällöstä, eivätkä ne välttämättä edusta Euroopan neuvosto ja EIT:n kantoja, vaikka ne on sisällytetty kirjallisuusluetteloon. EIT:n kirjaston verkkosivuilla osoitteessa [echr.coe.int](http://echr.coe.int) on lueteltu lisää julkaisuja.



# Käsikirja Euroopan tietosuojaoikeudesta



# Esipuhe

Euroopan unionin perusoikeusvirasto ja Euroopan neuvosto ovat laatineet tämän käsikirjan Euroopan tietosuoja-oikeudesta yhdessä Euroopan ihmisoikeustuomioistuinten kirjaamon kanssa. Käsikirja on kolmas oikeudellisten käsikirjojen sarjassa, joka on Euroopan unionin perusoikeusviraston ja Euroopan neuvoston yhteistyön tulosta. Ensimmäinen käsikirja Euroopan syrjinnänvastaisesta lainsäädännöstä julkaistiin maaliskuussa 2011 ja toinen käsikirja Euroopan turvapaikkaan, rajoihin ja maahanmuuttoon liittyvästä lainsäädännöstä huhtikuussa 2013.

Jatkamme yhteistyötä erittäin ajankohtaisen aiheen – henkilötietojen suojelun – parissa, joka vaikuttaa meihin kaikkiin joka päivä. Eurooppalainen järjestelmä tällä alalla on yksi parhaiten suojaavista maailmassa. Se perustuu Euroopan neuvoston yleissopimukseen 108, Euroopan unionin säädöksiin sekä Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytäntöön.

Tämän käsikirjan tavoitteena on lisätä tietoa Euroopan unionin ja Euroopan neuvoston jäsenvaltioissa voimassa olevista tietosuojasäännöistä sekä parantaa niiden tuntemusta toimimalla ensisijaisena tiedonlähteenä lukijoille. Se on suunnattu oikeusalan ammattilaisille, tuomareille, kansallisille tietosuojaviranomaisille ja muille tietosuoja-alalla työskenteleville henkilöille, jotka eivät ole erikoistuneet tietosuojaan.

Kun Lissabonin sopimus tuli voimaan syyskuussa 2009, Euroopan unionin perusoikeuskirjasta tuli oikeudellisesti sitova ja samalla oikeudesta henkilötietojen suojaan tuli itsenäinen perusoikeus. Perusoikeuksien turvaamisen kannalta on ratkaisevan tärkeää, että ihmiset oppivat tuntemaan nykyistä paremmin Euroopan neuvoston yleissopimuksen 108 ja Euroopan unionin (EU) säädökset, jotka viitoittivat tietä tietosuojaalle Euroopassa, sekä Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön.

Haluamme kiittää Ludwig Boltzmannin ihmisoikeus instituuttia heidän osallisuudestaan tämän käsikirjan laatimiseen. Haluamme osoittaa kiitollisuutemme Euroopan tietosuojavaltuutetun toimistolle heidän käsikirjan valmisteluvaiheessa antamansa palautteen johdosta. Haluamme erityisesti kiittää Euroopan komission tietosuojayksikköä avusta tämän käsikirjan laatimisessa Lopuksi, haluamme myös kiittää

Suomen tietosuojavaltuutetun toimistoa käsikirjan suomenkielisen käännöksen sisällön tarkastamisesta.

**Philippe Boillat**

Pääjohtaja Ihmisoikeuksia ja  
oikeusvaltiota käsittelevä osasto  
Euroopan neuvosto

**Morten Kjaerum**

Johtaja Euroopan unionin  
perusoikeusvirasto

# Sisältö

ESIPUHE .....	3
LYHENTEET .....	9
MITEN KÄYTÄT TÄTÄ KÄSIKIRJAA .....	11
1. EUROOPAN TIETOSUOJAOIKEUDEN TAUSTAA .....	13
1.1. Oikeus tietosuojaan .....	14
Keskeiset kohdat .....	14
1.1.1. Euroopan ihmisoikeussopimus .....	14
1.1.2. Euroopan neuvoston yleissopimus 108 .....	15
1.1.3. Euroopan unionin tietosuojalainsäädäntö .....	17
1.2. Tasapainottavat oikeudet .....	21
Keskeiset kohdat .....	21
1.2.1. Sananvapaus .....	22
1.2.2. Asiakirjojen saatavuus .....	26
1.2.3. Taiteen ja tutkimuksen vapaus .....	30
1.2.4. Omaisuudensuoja .....	31
2. TIETOSUOJAN TERMINOLOGIA .....	33
2.1. Henkilötiedot .....	34
Keskeiset kohdat .....	34
2.1.1. Henkilötietojen käsitteen tärkeimmät näkökohdat .....	35
2.1.2. Erityiset tietoryhmät .....	41
2.1.3. Anonyymit ja pseudonyymit tiedot .....	42
2.2. Tietojenkäsittely .....	44
Keskeiset kohdat .....	44
2.3. Henkilötietojen käyttäjät .....	47
Keskeiset kohdat .....	47
2.3.1. Rekisterinpitäjät ja henkilötietojen käsittelijät .....	47
2.3.2. Vastaanottajat ja sivulliset .....	52
2.4. Suostumus .....	54
Keskeiset kohdat .....	54
2.4.1. Pätevän suostumuksen edellytykset .....	54
2.4.2. Oikeus perua suostumus milloin tahansa .....	59

3. EUROOPAN TIETOSUOJAOIKEUDEN PÄÄPERIAATTEET .....	61
3.1. Laillisen käsittelyn periaate .....	62
Keskeiset kohdat .....	62
3.1.1. Edellytykset EIS:n mukaiselle oikeutetulle puuttumiselle oikeuden käyttämiseen .....	63
3.1.2. EU:n perusoikeuskirjassa määritellyt edellytykset oikeuden lailliselle rajoittamiselle .....	66
3.2. Tarkoituksen määrittämisen ja käyttötarkoitussidonnaisuuden periaatteet .....	68
Keskeiset kohdat .....	68
3.3. Tietojen laatua koskevat periaatteet .....	70
Keskeiset kohdat .....	70
3.3.1. Tietojen tarpeellisuusvaatimus .....	70
3.3.2. Tietojen virheettömyysvaatimus .....	71
3.3.3. Tietojen säilyttäminen .....	73
3.4. käsittelyn periaate .....	73
Keskeiset kohdat .....	73
3.4.1. Avoimuus .....	74
3.4.2. Luottamuksen rakentaminen .....	74
3.5. Vastuullisuuden periaate Keskeiset kohdat .....	76
Keskeiset kohdat .....	76
4. EUROOPAN TIETOSUOJAA KOSKEVAT SÄÄNNÖT .....	79
4.1. Laillista käsittelyä koskevat säännöt .....	81
Keskeiset kohdat .....	81
4.1.1. Muiden kuin arkaluonteisten tietojen laillinen käsittely .....	81
4.1.2. Arkaluonteisten tietojen laillinen käsittely .....	87
4.2. Käsittelyn turvallisuutta koskevat säännöt .....	91
Keskeiset kohdat .....	91
4.2.1. Tietoturvaan liittyvät näkökohdat .....	91
4.2.2. Luottamuksellisuus .....	94
4.3. Käsittelyn avoimuutta koskevat säännöt .....	96
Keskeiset kohdat .....	96
4.3.1. Informointi .....	97
4.3.2. Ilmoitusmenettely .....	99
4.4. Sääntöjenmukaisuuden edistämistä koskevat säännöt .....	100
Keskeiset kohdat .....	100
4.4.1. Ennakkotarkastus .....	100
4.4.2. Tietosuojavastaavat .....	101
4.4.3. Käytännösäännöt .....	102



5.	REKISTERÖITYJEN OIKEUDET JA NIIDEN VALVONTA .....	105
5.1.	Rekisteröityjen oikeudet .....	107
	Keskeiset kohdat .....	107
5.1.1.	Tarkastusoikeus .....	107
5.1.2.	Oikeus vastustaa henkilötietojen käsittelyä .....	114
5.2.	Riippumaton valvonta .....	116
	Keskeiset kohdat .....	116
5.3.	Oikeuskeinot ja sanktiot .....	120
	Keskeiset kohdat .....	120
5.3.1.	Pyynnöt rekisterinpitäjälle .....	121
5.3.2.	Valvontaviranomaiselle esitettävät vaateet .....	122
5.3.3.	Tuomioistuimelle esitettävät vaateet .....	123
5.3.4.	Sanktiot .....	128
6.	RAJAN YLI TAPAHTUVA HENKILÖTIETOJEN SIIRTO .....	131
6.1.	Rajan yli tapahtuvan tietojen siirron luonne .....	132
	Keskeiset kohdat .....	132
6.2.	Vapaa tietojen siirto jäsenvaltioiden tai sopimuspuolien välillä .....	134
	Keskeiset kohdat .....	134
6.3.	Vapaa tietojen siirto kolmansiin maihin .....	135
	Keskeiset kohdat .....	135
6.3.1.	Vapaa tietojen siirto riittävän suojan takia .....	135
6.3.2.	Vapaa tietojen siirto erityisissä tapauksissa .....	137
6.4.	Rajoitettu tietojen siirto kolmansiin maihin .....	138
	Keskeiset kohdat .....	138
6.4.1.	Sopimuslausekkeet .....	139
6.4.2.	Konsernin sisäiset sitovat tietosuojasäännöt .....	141
6.4.3.	Erytyiset kansainväliset sopimukset .....	141
7.	TIETOSUOJA POLIISI- JA RIKOSASIOISSA .....	147
7.1.	Tietosuojaaja poliisi- ja rikosasioissa käsittelevä EN-oikeus .....	148
	Keskeiset kohdat .....	148
7.1.1.	Poliisiasioita koskeva suositus .....	148
7.1.2.	Tietoverkkorikollisuutta koskeva Budapestin yleissopimus .....	152
7.2.	Tietosuojaaja poliisi- ja rikosasioissa käsittelevä EU-oikeus .....	153
	Keskeiset kohdat .....	153
7.2.1.	Tietosuojaaja koskeva puitepäätös .....	153
7.2.2.	Erytyiset oikeudelliset instrumentit , joilla säännellään tietosuojaaja poliisi- ja oikeusviranomaisten rajat ylittävän yhteistyön puitteissa .....	155
7.2.3.	Tietosuojaaja Europolissa ja Eurojustissa .....	157
7.2.4.	Tietosuojaaja EU-tason yhteisissä tietojärjestelmissä .....	160

8. MUUT ERITYISET EUROOPAN TIETOSUOJASÄÄDÖKSET .....	169
8.1. Sähköinen viestintä .....	170
Keskeiset kohdat .....	170
8.2. Työsuhdetta koskevat tiedot .....	174
Keskeiset kohdat .....	174
8.3. Terveystilaa koskevat tiedot .....	177
Keskeiset kohdat .....	177
8.4. Tietojen käsittely tilastollisiin tarkoituksiin .....	179
Keskeiset kohdat .....	179
8.5. Rahataloudelliset tiedot .....	182
Keskeiset kohdat .....	182
KIRJALLISUUTTA .....	185
OIKEUSKÄYTÄNTÖ .....	191
Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöä .....	191
Euroopan unionin oikeuskäytäntöä .....	195
LUETTELO OIKEUSTAPAUKSISTA .....	199

# Lyhenteet

BCR	Konsernin sisäiset sitovat tietosuojasäännöt (Binding corporate rules)
CCTV	Kameravalvonta (Closed circuit television)
CETS	Euroopan neuvoston sopimussarja (Council of Europe Treaty Series)
CRM	Asiakashallintajärjestelmä (Customer relations management)
C-SIS	Schengenin keskustietojärjestelmä
EAMV	Euroopan arvopaperimarkkinaviranomainen
EAW	Eurooppalainen pidätysmääräys (European arrest warrant)
EDPS	Euroopan tietosuojavaltuutettu
EFTA	Euroopan vapaakauppaliitto
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EN	Euroopan neuvosto
ENISA	Euroopan unionin verkko- ja tietoturvavirasto
ENU	Europolin kansallinen yksikkö
ETA	Euroopan talousalue
eTEN	Euroopan laajuiset televerkot
EU	Euroopan unioni
eu-LISA	Tietotekniikkavirasto
EuroPriSe	Eurooppalainen yksityisyyden suojaa koskeva tunnus (European Privacy Seal)
EUTI	Euroopan unionin tuomioistuin, ennen joulukuuta 2009: yhteisöjen tuomioistuin, EYTI
EY	Euroopan yhteisö
FRA	Euroopan unionin perusoikeusvirasto

GPS	Maailmanlaajuinen paikantamisjärjestelmä
IYJ	Ihmisoikeuksien yleismaailmallinen julistus
NGO	Kansalaisjärjestö (Non-governmental organisation)
N-SIS	Schengenin tietojärjestelmän kansallinen osa
OECD	Taloudellisen yhteistyön ja kehityksen järjestö
Perusoikeuskirja	Euroopan unionin perusoikeuskirja
PIN	Henkilökohtainen tunnusluku
PNR	Matkustajarekisteri
SEPA	Yhtenäinen euromaksualue
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta
SIS	Schengenin tietojärjestelmä
SWIFT	Kansainvälinen maksuliikennejärjestö
TTJ	Tullitietojärjestelmä
VIS	Viisumitietojärjestelmä
YK	Yhdistyneet kansakunnat
<b>Yleissopimus 108</b>	Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (Euroopan neuvosto)
YVV	Yhteinen valvontaviranomainen

# Miten käytät tätä käsikirjaa

Tässä käsikirjassa esitetään yleiskatsaus lainsäädäntöön, jota sovelletaan tietosuojan Euroopan unioniin (EU) ja Euroopan neuvostoon (EN) nähden.

Käsikirja on tarkoitettu avuksi oikeusalan ammattilaisia, jotka eivät ole erikoistuneet tietosuojaan; se on suunnattu asianajajille, tuomareille ja muille ammatinharjoittajille samoin kuin eri paikoissa, kuten kansalaisjärjestöissä, työskenteleville henkilöille, jotka joutuvat käsittelemään tietosuojaan liittyviä oikeudellisia kysymyksiä.

Se on ensisijainen tiedonlähde tietosuojaan liittyvän EU:n lainsäädännön että Euroopan ihmisoikeussopimuksen (EIS) alalla. Siinä selitetään, miten tietosuoja säännellään EU-oikeudessa ja EIS:ssa sekä EN:n yleissopimuksessa yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108) ja muissa EN:n oikeudellisissa välineissä. Kunkin luvun alussa on lueteltu sovellettavat säännökset ja määräykset sekä Euroopan kahteen oikeusjärjestelmään kuuluvia merkittäviä oikeustapauksia. Tämän jälkeen Euroopan kahden oikeusjärjestelmän kannalta merkittävät lait esitellään yksi kerrallaan siltä osin, kuin niitä saatetaan soveltaa käsiteltävänä olevaan aiheeseen. Näin lukija näkee, missä kohdissa oikeusjärjestelmät yhtenevät ja missä ne eroavat toisistaan.

Kunkin luvun alussa olevassa taulukossa numeroidaan luvussa käsiteltävät aiheet ja nimetään sovellettavat säännökset ja määräykset sekä muu merkittävä aineisto, kuten oikeustapaukset. Aiheiden käsittelyjärjestys voi hivenen vaihdella luvuittain, jos sen on katsottu helpottavan luvun sisällön ytimekästä esittämistä. Taulukot kattavat sekä EN:n että EU:n oikeuden. Tämän on tarkoitus auttaa lukijaa löytämään omaan tilanteeseensa liittyvä tärkein tieto erityisesti, jos tilanteeseen sovelletaan ainoastaan EN:n oikeutta.

EU:n ulkopuolisissa EN-maissa, jotka ovat allekirjoittaneet EIS:n ja yleissopimuksen 108, toimivat ammatinharjoittajat löytävät omaa maataan koskevat tiedot suoraan EN:a koskevista asioista. EU:n jäsenvaltioissa toimivat ammatinharjoittajat löytävät tietoa molemmista asioista, sillä kyseisiä maita sitovat molemmat oikeusjärjestykset. Niille, jotka tarvitsevat lisätietoja jostakin tietystä aiheesta, löytyy käsikirjan kohdasta "Kirjallisuutta" luettelo erikoistuneemmasta aineistosta.

EN-oikeutta esitellään lyhyinä otteina Euroopan ihmisoikeustuomioistuimen (EIT) käsittelemistä asioista. Asiat on valittu EIT:n lukuisista tietosuojaa käsittelevistä tuomioista ja päätöksistä.

EU-oikeudesta esitetään erilaisia lainsäädännöllisiä toimia, sopimusten määräyksiä sekä Euroopan unionin perusoikeuskirjan kohtia, sellaisina kuin niitä on tulkittu Euroopan unionin tuomioistuimen (EUTI, joka oli vuoteen 2009 asti Euroopan yhteisöjen tuomioistuin, EYTI) oikeuskäytännössä.

Tässä käsikirjassa kuvailtu tai lainattu oikeuskäytäntö tarjoaa kattavasti esimerkkejä sekä EIT:n että EUTI:n oikeuskäytännöstä. Käsikirjan lopussa olevat ohjeet auttavat lukijaa oikeuskäytännön hakemisessa verkosta.

Lisäksi tekstilaatikoissa esitetään käytännönläheisiä esimerkkejä kuvitteellisista tilanteista, jotka auttavat ymmärtämään Euroopan tietosuojasääntöjen soveltamista käytännössä erityisesti silloin, kun aihetta ei ole suoranaisesti käsitelty EIT:n tai EUTI:n oikeuskäytännössä.

Käsikirjan alussa kuvataan lyhyesti EIS:n ja EU:n oikeuden mukaiset kaksi oikeusjärjestelmää (luku 1). Luvuissa 2–8 käsitellään seuraavia asioita:

- tietosuojan terminologia;
- Euroopan tietosuojaoikeuden pääperiaatteet;
- Euroopan tietosuojaoikeuden säännöt;
- rekisteröityjen oikeudet ja niiden valvonta;
- rajan yli tapahtuva tietojen siirto;
- tietosuoja poliisi- ja rikosasioissa;
- muut erityiset Euroopan tietosuojasäädökset.

# 1

## Euroopan tietosuojaoikeuden taustaa

EU	Katetut aiheet	EN
<b>Oikeus tietosuojaan</b>		
Direktiivi 1995/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ( <i>tietosuojadirektiivi</i> ), EYVL 1995 L 281		EIS, 8 artikla (oikeus nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta) Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108)
<b>Tasapainottavat oikeudet</b>		
Yhdistetyt asiat C-92/09 ja C-93/09, <i>Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen</i> , EUTI 2010	Yleisesti	
Asia C-73/07, <i>Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy</i> , EYTI 2008	Sananvapaus	Asia <i>Axel Springer AG v. Saksa</i> , EIT 2012 Asia <i>Mosley v. Yhdistynyt kuningaskunta</i> , EIT 2011
	Taiteen ja tutkimuksen vapaus	Asia <i>Vereinigung bildender Künstler v. Itävalta</i> , EIT 2007
Asia C-275/06, <i>Productores de Música de España (Promusicae) v. Telefónica de España SAU</i> , EYTI 2008	Omaisuuksensaaja	
Asia C-28/08 P, <i>Euroopan komissio v. The Bavarian Lager Co. Ltd</i> , EUTI 2010	Asiakirjojen saatavuus	Asia <i>Társaság a Szabadságjogokért v. Unkari</i> , EIT 2009

# 1.1. Oikeus tietosuojaan

## Keskeiset kohdat

- EIS:n 8 artiklan mukaan oikeus suojaan henkilötietojen keruulta ja käytöltä kuuluu oikeuteen nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta.
- EN:n yleissopimus 108 on ensimmäinen oikeudellisesti sitova kansainvälinen sopimus, joka koskee erityisesti tietosuojaa.
- EU-oikeudessa tietosuojaa säänneltiin ensimmäisen kerran tietosuojadirektiivillä.
- EU-oikeudessa tietosuoja on tunnustettu perusoikeudeksi.

Oikeus yksityisyyden piirin suojaamiseen tunkeilijoilta, erityisesti valtiolta, vahvistettiin ensimmäisen kerran kansainvälisessä oikeudellisessa instrumentissa vuoden 1948 Yhdistyneiden kansakuntien (YK) ihmisoikeuksien yleismaailmallisen julistuksen 12 artiklassa, joka käsittelee yksityis- ja perhe-elämää.<sup>1</sup> Ihmisoikeuksien yleismaailmallinen julistus vaikutti muiden ihmisoikeuksia koskevien instrumenttien kehittämiseen Euroopassa.

## 1.1.1. Euroopan ihmisoikeussopimus

Euroopan neuvosto (EN) perustettiin toisen maailmansodan jälkimainingeissa saattamaan Euroopan maat yhteen oikeusvaltion, demokratian, ihmisoikeuksien ja sosiaalisen kehityksen edistämiseksi. Tätä tarkoitusta varten se hyväksyi vuonna 1950 [Euroopan ihmisoikeussopimuksen \(EIS\)](#), joka tuli voimaan vuonna 1953.

Valtioilla on kansainvälinen velvollisuus noudattaa EIS:ta. Kaikki EN:n jäsenvaltiot ovat nyt saattaneet EIS:n osaksi kansallista lainsäädäntöään, mikä edellyttää niiden noudattavan sopimuksen määräyksiä.

Ranskan Strasbourgiin perustettiin vuonna 1959 Euroopan ihmisoikeustuomioistuin (EIT), jonka tehtävänä on varmistaa, että sopimuspuolet täyttävät EIS:n mukaiset velvollisuutensa. Tämän EIT tekee tutkimalla yksityishenkilöiden, ryhmien, kansalaisjärjestöjen ja oikeushenkilöiden väitteitä sopimuksen rikkomisesta. Vuonna 2013 Euroopan neuvostoon kuului 47 jäsenvaltiota, joista 28 on myös EU:n jäsenvaltioita.

<sup>1</sup> Yhdistyneiden kansakuntien 10. joulukuuta 1948 antama ihmisoikeuksien yleismaailmallinen julistus.



EIT:ssa kantajan ei tarvitse olla EN:n jäsenvaltion kansalainen. EIT voi myös tarkastella valtioiden välisiä asioita, joissa yksi tai useampi EN:n jäsenvaltio on nostanut kanteen joltain jäsenvaltiota vastaan.

Oikeus henkilötietojen suojaan kuuluu EIS:n 8 artiklassa turvattuihin oikeuksiin. Kyseisessä artiklassa taataan oikeus nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta ja määrätään ehdot, joilla tätä oikeutta voidaan rajoittaa.<sup>2</sup>

EIT on oikeuskäytännössään tutkinut useita tilanteita, joissa on noussut esiin kysymys tietosuojasta. Ne ovat koskeneet erityisesti telekuuntelua,<sup>3</sup> tarkkailun eri muotoja<sup>4</sup> sekä viranomaisten suorittamaa henkilötietojen taltiointia.<sup>5</sup> EIT on tarkentanut, että EIS:n 8 artiklaan sisältyy paitsi valtioiden velvollisuus pitäytyä toimista, jotka saattavat rikkoa tätä sopimuksessa vahvistettua oikeutta, myös tietyissä olosuhteissa myönteinen velvollisuus turvata aktiivisesti yksityis- ja perhe-elämän kunnioitus.<sup>6</sup> Monia näistä asioista esitellään tarkemmin asianmukaisissa luvuissa.

## 1.1.2. Euroopan neuvoston yleissopimus 108

Tietotekniikan kehittyminen 1960-luvulla loi tarpeen kehittää yksityiskohtaisemmat säännöt henkilöiden suojelemiseksi suojaamalla heidän (henkilö)tietojaan. Euroopan neuvoston ministerikomitea antoi 1970-luvun puolivälissä erilaisia henkilötietojen suojelua koskevia julkilausumia, jotka perustuivat EIS:n 8 artiklaan.<sup>7</sup> Vuonna 1981 avattiin allekirjoitettavaksi yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (**yleissopimus 108**)<sup>8</sup>. Yleissopimus 108 oli tuolloin ja on edelleen ainoa oikeudellisesti sitova kansainvälinen sopimus tietosuojan alalla.

2 EN, Euroopan ihmisoikeussopimus, CETS nro 005, 1950.

3 Ks. esim. asia nro 8691/79, *Malone v. Yhdistynyt kuningaskunta*, EIT 2.8.1984; asia nro 62617/00, *Copland v. Yhdistynyt kuningaskunta*, EIT 3.4.2007.

4 Ks. esim. asia nro 5029/71, *Klass ym. v. Saksa*, EIT 6.9.1978; asia nro 35623/05, *Uzun v. Saksa*, EIT 2.9.2010.

5 Ks. esim. asia nro 9248/81, *Leander v. Ruotsi*, EIT 26.03.1987; asiat nro 30562/04 ja 30566/04, *S. ja Marper v. Yhdistynyt kuningaskunta*, EIT 4.12.2008.

6 Ks. esim. asia nro 20511/03, *I. v. Suomi*, EIT 17.7.2008; asia nro 2872/02, *K.U. v. Suomi*, EIT 2.12.2008.

7 EN, ministerikomitea (1973), julkilausuma (73) 22 henkilöiden yksityisyyden suojelusta yksityissektorin sähköisten tietopankkien yhteydessä, 26. syyskuuta 1973; EN, ministerikomitea (1974), julkilausuma (74) 29 henkilöiden yksityisyyden suojelusta julkisen sektorin sähköisten tietopankkien yhteydessä, 20. syyskuuta 1974.

8 EN, yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, Euroopan neuvosto, CETS nro 108, 1981.

Yleissopimusta 108 sovelletaan henkilötietojen käsittelyyn sekä yksityisellä että julkisella sektorilla, kuten esimerkiksi henkilötietojen käsittelyyn oikeuslaitoksessa ja lainvalvonta viranomaisissa. Se yksilöitä väärinkäytöltä, jota henkilötietojen keruun ja käsittelyn yhteydessä voi tapahtua, ja samalla pyrkii sääntelemään henkilötietojen siirtoa rajojen yli. Henkilötietojen keruun ja käsittelyn osalta yleissopimuksessa vahvistetut periaatteet koskevat erityisesti tietojen oikeudenmukaista ja laillista keruuta ja automaattista käsittelyä, kun tiedot on tallennettu määritellyä lainmukaista tarkoitusta varten eikä niitä käsitellä määritellyn tarkoituksen kanssa yhteensopimattomalla tavalla tai säilytetä pidempään kuin on tarpeellista määritellyn tarkoituksen kannalta. Periaatteet koskevat myös tietojen laatua, erityisesti tietojen asianmukaisuutta, tarpeellisuutta sekä virheettömyyttä.

Sen lisäksi, että yleissopimuksessa annetaan henkilötietojen keruuseen ja käsittelyyn liittyviä takeita, siinä kielletään ”arkaluonteisten” henkilötietojen, kuten rotua, politiikkaa, terveyttä, uskontoa, sukupuolielämää tai rikosrekisteriä koskevien tietojen, käsitteleminen ilman riittäviä oikeudellisia suojatoimia.

Yleissopimuksessa myös vahvistetaan yksilön oikeus saada tietää, että hänestä on tallennettu tietoja, ja tarvittaessa saada korjata tietoja. Yleissopimuksessa asetettuja oikeuksia voidaan rajoittaa vain, jos välttämätön etu, kuten valtion turvallisuus tai puolustus, edellyttää sitä.

Yleissopimuksessa mahdollistetaan henkilötietojen vapaa siirto sopimuspuolena olevien jäsenvaltioiden välillä, mutta siinä myös asetetaan tiettyjä rajoituksia siirtoille sellaisiin maihin, joissa ei ole vahvistettu säädöksillä riittävää suojaa.

Yleissopimuksessa vahvistettujen yleisten periaatteiden ja sääntöjen viemiseksi eteenpäin EN:n ministerikomitea on antanut useita suosituksia, jotka eivät ole oikeudellisesti sitovia (ks. luvut 7 ja 8).

Kaikki EU:n jäsenvaltiot ovat ratifioineet yleissopimuksen 108. Vuonna 1999 yleissopimusta muutettiin siten, että EU:sta saattoi tulla sen osapuoli.<sup>9</sup> Vuonna 2001 hyväksyttiin yleissopimuksen 108 lisäpöytäkirja, jossa määritettiin maan rajan yli

<sup>9</sup> EN, ministerikomitean Strasbourgissa 15. kesäkuuta 1999 hyväksymät muutokset yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä (ETS nro 108) Euroopan yhteisöjen liittymisen mahdollistamiseksi; yleissopimuksen, sellaisena kuin se on muutettuna, 23 artiklan 2 kohta.

tapahtuvasta tietojen siirrosta sopimuksen ulkopuolisiin niin kutsuttuihin kolmansiin maihin ja kansallisen tietosuojaviranomaisen pakollisesta perustamisesta.<sup>10</sup>

## Tulevaisuudennäkymiä

Yleissopimusta 108 on päätetty ajantasaistaa, ja vuonna 2011 toteutettu julkinen kuuleminen auttoi vahvistamaan työn kaksi tärkeintä tavoitetta: yksityisyyden suojaa digitaalisella on vahvistettava ja yleissopimuksen seurantamekanismeja on tehostettava.

Yleissopimukseen 108 voivat liittyä myös Euroopan neuvoston ulkopuoliset maat, mukaan lukien Euroopan ulkopuoliset maat. Yleissopimus voisi toimia yleismaailmallisena normina, ja avoimuutensa ansiosta se voisi auttaa edistämään tietosuojaa koko maailmassa.

Tällä hetkellä 45 maata yleissopimuksen 108 allekirjoittaneesta 46 maasta on EN:n jäseniä. Uruguay liittyi yleissopimukseen 108 elokuussa ensimmäisenä Euroopan ulkopuolisenä maana, ja Marokolla, jonka ministerikomitea on kutsunut liittymään, on vielä liittymisprosessi kesken.

### 1.1.3. Euroopan unionin tietosuojalainsäädäntö

EU-oikeus koostuu perussopimuksista ja johdetusta oikeudesta. Perussopimukset, eli [sopimus Euroopan unionista \(SEU\)](#) ja [sopimus Euroopan unionin toiminnasta \(SEUT\)](#), ovat kaikkien EU:n jäsenvaltioiden hyväksymiä. Niitä kutsutaan myös EU:n primaarioikeudeksi. EU:n toimielimet antavat asetuksia, direktiivejä ja päätöksiä perussopimusten mukaisten valtuuksiensa nojalla. Näitä säädöksiä kutsutaan usein EU:n johdetuksi oikeudeksi.

EU:n pääasiallinen oikeudellinen väline tietosuojan alalla on Euroopan parlamentin ja neuvoston 24 päivänä lokakuuta 1995 antama [direktiivi 95/46/EY](#) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ([tietosuojadirektiivi](#)).<sup>11</sup> Se annettiin vuonna 1995, jolloin useat jäsenvaltiot olivat jo säätäneet kansallisia tietosuojalakeja. Tavaroiden, palvelujen ja henkilöiden vapaa liikkuvuus sisämarkkinoilla edellytti tietojen vapaata siirtoa, jota ei olisi voitu toteut-

<sup>10</sup> EN, valvontaviranomaisia ja maan rajan yli tapahtuvaa tietojen siirtoa koskeva lisäpöytäkirja yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, CETS nro 181, 2001.

<sup>11</sup> Tietosuojadirektiivi, EYVL 1995 L 281, s. 31.

taa, elleivät jäsenvaltiot olisi voineet luottaa yhtenäiseen korkeaan tietosuojan tasoon.

Koska tietosuojadirektiivillä oli tarkoitus yhdenmukaistaa<sup>12</sup> tietosuojalainsäädäntöä jäsenvaltioiden tasolla, se vastaa yksityiskohtaisuudeltaan (silloisia) kansallisia tietosuojalakeja. EUTI ennakkoratkaisussaan toteaa, että: ”Direktiivi 95/46/EY on tarkoitettu [...] saattamaan henkilöiden oikeuksien ja vapauksien suoja henkilötietoja käsiteltäessä samalle tasolle kaikissa jäsenvaltioissa. [...] sovellettavien kansallisten lainsäädäntöjen lähentäminen ei saa johtaa lainsäädännöllä turvattavan tietosuojan heikentymiseen, vaan sillä on päinvastoin varmistettava tietosuojan korkea taso unionissa. Sen vuoksi [...] kansallisten lainsäädäntöjen harmonisointia ei ole rajoitettu vähimmäistasolle, vaan sillä pyritään yhdenmukaistamiseen, joka on yleisesti ottaen aukoton.”<sup>13</sup> Näin ollen, jäsenvaltioilla on vain vähän liikkumavaraa direktiivin täytäntöönpanossa.

Tietosuojadirektiivin on tarkoitus tukea yleissopimuksessa 108 vahvistettua oikeutta yksityisyyteen ja laajentaa sitä. Näissä kahdessa oikeudellisessa instrumentissa olisi ollut mahdotonta asettaa ristiriitaisia sääntöjä, sillä kaikki EU:hun vuonna 1995 kuuluneet 15 jäsenvaltiota olivat jo yleissopimuksen 108 sopimuspuolia. Tietosuojadirektiivissä kuitenkin hyödynnetään yleissopimuksen 108 11 artiklassa annettua mahdollisuutta myöntää laajempi suoja. Erityisesti riippumattoman valvonnan käyttöönotto tietosuojasääntöjen noudattamisen parantamiseksi, tehosti merkittävästi Euroopan tietosuojalainsäädännön toimivuutta. (Tämä sisällytettiin vuonna 2001 EN:n oikeuteen yleissopimuksen 108 lisäpöytäkirjalla.)

Tietosuojadirektiivin soveltamisalue ulottuu EU:n 28 jäsenvaltiota laajemmalle ja kattaa myös EU:n ulkopuoliset Euroopan talousalueen (ETA) maat<sup>14</sup> Islannin, Liechtensteinin ja Norjan.

Luxemburgissa sijaitsevilla EUTI:lla on toimivalta määritellä, onko jäsenvaltio täytäntöyteen pantu tietosuojadirektiivin mukaiset velvollisuutensa. EUTI antaa ennakkoratkaisuja direktiivin pätevytydestä ja tulkinnasta, jotta se voisi varmistaa direktiivin tehokkaan ja yhdenmukaisen soveltamisen jäsenvaltioissa. Merkittävä poikkeus tietosuojadirektiivin soveltamiseen on niin kutsuttu kotitaloutta koskeva poikkeus jolla

12 Ks. esim. tietosuojadirektiivin johdanto-osan 1, 4, 7 ja 8 kappale.

13 EUTI, yhdistetyt asiat C-486/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 23 Marraskuuta 2011, kappaleet 28-29.

14 Sopimus Euroopan talousalueesta, EYVL 1994 L 1, joka tuli voimaan 1. tammikuuta 1994.

tarkoitetaan henkilötietojen käsittelyä, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa.<sup>15</sup> Tällaisen käsittelyn katsotaan yleensä kuuluvan yksilön vapauksiin.

Tietosuojadirektiivin hyväksymisen aikaan voimassa olleen EU:n primaarioikeuden mukaisesti direktiivin aineellinen soveltamisala rajoittuu sisämarkkinoita koskeviin asioihin. Soveltamisalan ulkopuolelle jää erityisesti yhteistyö poliisiasioissa ja rikos-oikeudellisissa asioissa. Sillä alalla tietosuoja perustuu erilaisiin oikeudellisiin välineisiin, joita kuvaillaan tarkemmin luvussa 7.

Koska tietosuojadirektiivi oli suunnattu vain jäsenvaltioille, tarvittiin toinen oikeudellinen instrumentti säätelemään tietosuojaa EU:n toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä. Tämän tehtävän täyttää yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettu asetus (EY) N:o 45/2001 (*EU:n toimielinten tietosuoja-asetus*).<sup>16</sup>

Lisäksi tietosuojadirektiivin kattamillakin aloilla tarvitaan usein yksityiskohtaisempia tietosuojasäännöksiä selventämään direktiivin suhdetta muihin oikeutettuihin etuihin. Kaksi esimerkkiä tällaisista ovat henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettu *direktiivi 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi)*<sup>17</sup> ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja *direktiivin 2002/58/EY muuttamisesta* annettu *direktiivi 2006/24/EY (tietojen säilyttämistä koskeva direktiivi, kumottu 8.huhtikuuta 2014)*.<sup>18</sup> Muita esimerkkejä esitellään myöhemmin luvussa 8. Tällaisten säännösten on oltava yhdenmukaisia tietosuojadirektiivin kanssa.

15 Tietosuojadirektiivi, 3 artiklan 2 kohdan toinen luetelmakohta.

16 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001 L 8.

17 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (*sähköisen viestinnän tietosuojadirektiivi*), EYVL 2002 L 201.

18 Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta (*tietojen säilyttämistä koskeva direktiivi*), EUVL 2006 L 105, kumottu 8. Huhtikuuta 2014.

## Euroopan unionin perusoikeuskirja

Euroopan yhteisöjen alkuperäisissä perussopimuksissa ei viitattu ihmisoikeuksiin eikä niiden suojaamiseen. Silloisen Euroopan yhteisöjen tuomioistuimen (EYTI) oli kuitenkin kehitettävä uusi lähestymistapa, kun sen käsiteltäväksi tuli asioita, joissa epäiltiin ihmisoikeusrikkomuksia EU:n lainsäädännön soveltamisalaan kuuluvilla aloilla. Yksilöiden suojaamiseksi tuomioistuin saattoi perusoikeudet osaksi niin kutsuttuja Euroopan oikeuden yleisiä periaatteita. EYTI:n mukaan nämä yleiset periaatteet vastaavat sisällöltään kansallisiin perustuslakeihin ja ihmisoikeussopimuksiin, etenkin EIS:een, perustuvaa ihmisoikeuksien suojaamista. EYTI ilmoitti varmista- vansa, että nämä periaatteet ovat yhteisön oikeuden mukaiset.

EU tiedosti, että sen politiikka voi vaikuttaa ihmisoikeuksiin ja lisäksi se oli asetta- nut tavoitteekseen kansalaisläheisyyden. Tämän seurauksena EU vahvisti [Euroopan unionin perusoikeuskirjan](#) vuonna 2000. Perusoikeuskirja kattaa monipuolisesti Euroopan kansalaisten kansalaisoikeuksia sekä poliittisia, taloudellisia ja sosiaalisia oikeuksia, jotka perustuvat jäsenvaltioille yhteisiin valtiosääntöperinteisiin ja kansainvälisiin velvollisuuksiin. Perusoikeuskirjassa määritellyt oikeudet on jaettu kuu- teen lukuun: ihmisarvo, vapaudet, tasa-arvo, yhteisvastuu, kansalaisten oikeudet ja lainkäyttö.

Perusoikeuskirja oli alun perin vain poliittinen asiakirja, mutta siitä tuli oikeudellisesti sitova<sup>19</sup> osa EU:n primaarioikeutta (ks. SEU 6 artiklan 1 kohta), kun [Lissabonin sopi- mus](#) tuli voimaan 1. joulukuuta 2009.<sup>20</sup>

EU:n primaarioikeuteen kuuluu myös EU:n yleinen lainsäädäntövalta tietosuo- ja-asioissa (SEUT 16 artikla).

Sen lisäksi, että perustamissopimuksessa taataan oikeus yksityis- ja perhe-elä- män kunnioittamiseen (7 artikla), siinä vahvistetaan oikeus henkilötietojen suojaan ( artikla) niin, että tämä suoja yksiselitteisesti korotetaan EU-oikeuden mukaiseksi perusoikeudeksi. Velvollisuus kunnioittaa ja suojata tätä oikeutta koskee paitsi EU:n toimielimiä myös jäsenvaltioita, kun ne implementoivat unionin oikeutta (perus- oikeuskirjan 51 artikla). Vuosia tietosuojadirektiivin antamisen jälkeen kirjoitetun perusoikeuskirjan 8 artiklan on ymmärrettävä ilmentävän jo voimassa olevaa EU:n

19 EU (2012), [Euroopan unionin perusoikeuskirja](#), EUVL 2012 C 326.

20 Ks. Euroopan unionista tehdyn sopimuksen konsolidoitu versio (2012), EUVL 2012 C 326; ja [Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu versio \(2012\)](#), EUVL 2012 C 326.

tietosuojalainsäädäntöä. Siksi perusoikeuskirjassa ei pelkästään mainita 8 artiklan 1 kohdassa oikeutta tietosuojaan vaan myös viitataan 8 artiklan 2 kohdassa tietosuojan pääperiaatteisiin. Lopuksi perusoikeuskirjan 8 artiklan 3 kohdassa varmistetaan, että riippumaton viranomainen valvoo periaatteiden noudattamista.

## Tulevaisuudennäkymiä

Euroopan komissio ehdotti tammikuussa 2012 tietosuojan uudistuspakettia todeten, että voimassa olevia tietosuojasääntöjä oli ajantasaistettava tekniikan nopean kehityksen ja globalisaation huomioimiseksi. Uudistuspaketti koostuu ehdotuksesta yleiseksi tietosuoja-asetukseksi,<sup>21</sup> jolla on tarkoitus korvata tietosuojadirektiivi, ja uudesta tietosuojadirektiivistä,<sup>22</sup> jossa säädetään tietosuojasta poliisiyhteistyön ja rikosasioissa tehtävän oikeudellisen yhteistyön alalla. Uudistuspaketista käytiin vielä keskustelua, kun tämä käsikirja julkaistiin.

## 1.2. Tasapainottavat oikeudet

### Keskeiset kohdat

- Oikeus tietosuojaan ei ole ehdoton oikeus; sitä on punnittava muita oikeuksia vasten.

Perusoikeuskirjan 8 artiklan mukainen perusoikeus henkilötietojen suojaan ”ei kuitenkaan ole ehdoton oikeus, vaan se on suhteutettava siihen tehtävään, joka sillä on yhteiskunnassa”.<sup>23</sup> Täten perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen oikeuksien kaltaisten oikeuksien käyttämistä voidaan rajoittaa, jos näistä rajoituksista säädetään lailla, jos niissä kunnioitetaan kyseisten oikeuksien ja vapauksien olennaista sisältöä ja jos ne suhteellisuusperiaatteen mukaisesti ovat välttämättömiä ja vastaavat tosiasiallisesti

21 Euroopan komissio (2012), ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (*yleinen tietosuoja-asetus*), KOM(2012) 11 lopullinen, Bryssel, 25. tammikuuta 2012.

22 Euroopan komissio (2012), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (*yleinen tietosuojadirektiivi*), KOM(2012) 10 lopullinen, Bryssel, 25. tammikuuta 2012.

23 Ks. esim. yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen*, EUTI 9.11.2010, 48 kohta.

Euroopan unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.<sup>24</sup>

EIS:n järjestelmässä tietosuoja on taattu 8 artiklassa (oikeus nauttia yksityis- ja perhe-elämän kunnioitusta), ja – samalla tavoin kuin perusoikeuskirjan järjestelmässä – tämän oikeuden soveltamisessa on otettava huomioon kilpailevat oikeudet. EIS:n 8 artiklan 2 kohdassa määrätään seuraavaa: ”Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa – – muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.”

Sekä EIT että EUTI ovatkin toistuvasti todenneet, että EIS:n 8 artiklan ja perusoikeuskirjan 8 artiklan soveltamisen ja tulkinnan yhteydessä on punnittava muitakin oikeuksia.<sup>25</sup> Tasapainon saavuttamisesta on useita tärkeitä esimerkkejä.

## 1.2.1. Sananvapaus

Sananvapautta ja henkilötietojen suojaa turvaavat oikeudet voivat olla ristiriidassa keskenään.

Sananvapaus on turvattu perusoikeuskirjan 11 artiklassa (”Sananvapaus ja tiedonvälityksen vapaus”). Oikeus sisältää ”mielipiteenvapauden sekä vapauden vastaanottaa ja levittää tietoja tai ajatuksia viranomaisten siihen puuttumatta ja alueellisista rajoista riippumatta”. Perusoikeuskirjan 11 artikla vastaa EIS:n 10 artiklaa. Perusoikeuskirjan 52 artiklan 3 kohdan mukaan, siltä osin kuin perusoikeuskirjan oikeudet vastaavat EIS:ssa taattuja oikeuksia, ”niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa”. Perusoikeuskirjan 11 artiklassa taatulle oikeudelle ei siis voida laillisesti asettaa rajoituksia, jotka menevät EIS:n 10 artiklan 2 kohdassa säädettyjä oikeuksia pidemmälle, toisin sanoen rajoituksista on säädettävä laissa ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa ”muiden

24 *Ibid.*, 50 kohta.

25 Asiat nro 40660/08 ja nro 60641/08, *Von Hannover v. Saksa (nro 2)* [suuri jaosto], EIT 7.2.2012; yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, EUTI 24.11.2011, 48 kohta; asia C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, EYTI 29.1.2008, 68 kohta. Ks. myös Euroopan neuvosto (2013), Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö henkilötietojen suojelun alalla, DP (2013). Oikeuskäytäntö on saatavilla osoitteessa [www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP\\_2013\\_Case\\_Law\\_Eng\\_FINAL.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP_2013_Case_Law_Eng_FINAL.pdf).



henkilöiden maineen tai oikeuksien turvaamiseksi”. Tämä käsite kattaa oikeuden tietosuojaan

Henkilötietojen suojaamisen ja sananvapauden välistä suhdetta säädellään tietosuojadirektiivin 9 artiklalla, jonka otsikkona on ”Henkilötietojen käsittely ja ilmaisuvapaus”.<sup>26</sup> Artiklassa säädetään seuraavaa: Jäsenvaltioiden on säädettävä ainoastaan journalistisia tarkoituksia tai taiteellisen tai kirjallisen ilmaisun tarkoituksia varten toteutettua henkilötietojen käsittelyä varten poikkeuksista ja vapautuksista tästä luvusta, IV luvusta ja VI luvusta, ainoastaan jos ne osoittautuvat välttämättömiksi yksityisyyttä koskevan oikeuden ja ilmaisuvapautta koskevien sääntöjen yhteensovittamisessa.

Esimerkki: Asiassa *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy*,<sup>27</sup> EYTI:ta pyydettiin tulkitsemaan tietosuojadirektiivin 9 artiklaa ja määrittelemään tietosuojan suhdetta lehdistönvapauteen. Tuomioistuimen piti tarkastella, miten Markkinapörssi ja Satamedia olivat levittäneet noin 1,2 miljoonan luonnollisen henkilön verotietoja, jotka ne olivat saaneet laillisesti Suomen veroviranomaisilta. Tuomioistuimen piti erityisesti varmistaa, oliko veroviranomaisten saataville saattamien henkilötietojen käsittely siten, että matkapuhelinten käyttäjät voivat saada muiden luonnollisten henkilöiden verotietoja, katsottava yksinomaan journalistisiin tarkoituksiin toteutetuksi toiminnaksi. Todettuaan, että Satakunnan toteuttama toiminta oli tietosuojadirektiivin 3 artiklan 1 kohdassa tarkoitettua ”henkilötietojen käsittelyä”, tuomioistuin siirtyi tulkitsemaan direktiivin 9 artiklaa. Tuomioistuin toi ensin esiin sananvapauden tärkeyden kaikissa demokraattisissa yhteiskunnissa ja jatkoi, että siihen liittyviä käsitteitä, journalismin käsite mukaan lukien, on tulkittava laajasti. Seuraavaksi tuomioistuin huomautti, että näiden kahden perusoikeuden välisen tasapainon löytämiseksi tietosuojaa koskevaan oikeuteen säädettyjä poikkeuksia ja rajoituksia on toteutettava vain täysin välttämättömän rajoissa. Asian olosuhteissa tuomioistuin katsoi, että Markkinapörssin ja Satamedian toteuttamien toimintojen kaltaisia toimintoja, jotka koskevat kansallisen lainsäädännön nojalla julkisista asiakirjoista peräisin olevia tietoja, voidaan pitää ”journalistisina toimintoina”, jos niiden tarkoituksena on tietojen, mielipiteiden tai ajatusten ilmaiseminen yleisölle millä tahansa tiedonsiirron välineellä. Tuomioistuin myös totesi, että näitä toimintoja eivät harjoita ainoastaan joukkotiedotusyritykset, ja

26 Tietosuojadirektiivi, 9 artikla.

27 Asia C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy*, EYTI 16.12.2008, 56, 61 ja 62 kohta.

ne voivat liittyä voiton tavoitteluun. EYTI jätti kuitenkin kansallisen tuomioistuimen tehtäväksi arvioida, oliko tämä ollut tarkoituksena kyseisessä asiassa.

EIT on antanut useita tärkeitä ennakkopäätöksiä tietosuojaa koskevan oikeuden sovittamisesta yhteen sananvapauden kanssa.

Esimerkki: Asiassa *Axel Springer AG v. Saksa*<sup>28</sup> EIT katsoi, että kansallisen tuomioistuimen määräämä kielto sanomalehden omistajalle, joka halusi julkaista artikkelin tunnetun näyttelijän pidätyksestä ja tuomitsemisesta, rikkoi EIS:n 10 artiklaa. EIT toisti perusteet, jotka se oli antanut oikeuskäytännössään, kun se oli punninnut ilmaisunvapauden oikeutta suhteessa oikeuteen nauttia yksityiselämän kunnioitusta:

- ensinnäkin, koskiko julkaistu artikkeli yleistä etua: henkilön pidätys ja tuomio oli julkinen oikeudellinen tosiasia ja siten koski yleistä etua;
- toiseksi, oliko asianosainen julkisuuden henkilö: asianosainen oli riittävän tunnettu näyttelijä, jotta häntä saatettiin luonnehtia julkisuuden henkilöksi; ja
- kolmanneksi, miten tiedot oli saatu ja olivatko ne luotettavia: tiedot oli saatu syyttäjän virastosta eikä kumpikaan osapuoli kiistänyt julkaistujen tietojen todenmukaisuutta.

Näin ollen EIT totesi, etteivät yhtiölle määrätyt julkaisurajoitukset olleet kohutuullisia suhteessa oikeutettuun tavoitteeseen suojella kantajan yksityiselämää. Tuomioistuim katsoi, että EIS:n 10 artiklaa oli rikottu.

Esimerkki: Asiassa *Von Hannover v. Saksa (nro 2)*,<sup>29</sup> EIT katsoi, ettei EIS:n 8 artiklan mukaista oikeutta nauttia yksityiselämän suojaa ollut rikottu, kun Monacon prinsessa Carolinelta oli evätty kielto määräys sellaisen valokuvan julkaisemista vastaan, joka hänestä oli otettu hänen puolisonsa kanssa laskettelulomalla. Valokuva liittyi artikkeliin, jossa kerrottiin muun muassa ruhtinas Rainierin heikosta terveydestä. EIT totesi, että kansalliset tuomioistuimet olivat huolellisesti punninneet kustannusyhtiön oikeutta ilmaisunvapautteen suhteessa kantajan oikeuteen nauttia yksityiselämän kunnioitusta. Kansallisen tuomioistuimen

28 Asia nro 39954/08, *Axel Springer AG v. Saksa* [suuri jaosto], EIT 7.2.2012, 90 ja 91 kohta.

29 Asiat nro 40660/08 ja nro 60641/08, *Von Hannover v. Saksa (nro 2)* [suuri jaosto], EIT 7.2.2012, 118 ja 124 kohta.

luonnehdintaa ruhtinas Rainierin sairaudesta ajankohtaisena yhteiskunnallisena asiana ei voitu pitää kohtuuttomana, ja EIT pystyi hyväksymään sen, että valokuva yhdessä artikkelin kanssa liittyi ainakin jossain määrin yleistä etua koskevaan keskusteluun. Tuomioistuin totesi, ettei EIS:n 8 artiklaa ollut rikottu.

EIT:n oikeuskäytännössä yksi oikeuksien tasapainottamisen kannalta keskeinen peruste on se, liittykö käsiteltävä ilmaisu yleistä etua koskevaan keskusteluun.

Esimerkki: Asiassa *Mosley v. Yhdistynyt kuningaskunta*<sup>30</sup> kansallinen viikkolehti oli julkaissut intiimejä valokuvia kantajasta. Kantaja väitti, että EIS:n 8 artiklaa oli rikottu, kun hän ei ollut voinut hakea kieltomääräystä ennen kyseisten valokuvien julkaisemista, sillä lehdellä ei ollut mitään velvollisuutta ilmoittaa ennalta aikomuksestaan julkaista aineistoa, joka saattoi loukata henkilön oikeutta yksityisyyteen. Vaikka tällaista aineistoa levitetään yleensä enemmän viihdekuin opetustarkoituksiin, se nauttii epäilemättä EIS:n 10 artiklan mukaista suojaa, joka saattaisi hävitä EIS:n 8 artiklan vaatimuksille, jos tieto olisi luonteeltaan yksityistä ja intiimiä eikä sen levittäminen olisi mitenkään yleisen edun mukaista. Rajoituksiin, jotka voisivat toimia sensuurina ennen julkaisemista, on kuitenkin kiinnitettävä erityistä huomiota. Otettuaan huomioon ennakoilmoitusvaatimuksen mahdollisen oikeuksia rajoittavan vaikutuksen, epävarmuuden tällaisen vaatimuksen tehokkuudesta ja näissä asioissa sallitun laajan harkintavallan, EIT totesi, ettei 8 artikla edellyttänyt oikeudellisesti sitovaa ennakoilmoitusvaatimusta. Näin ollen tuomioistuin katsoi, ettei 8 artiklaa ollut rikottu.

Esimerkki: Asiassa *Biriuk v. Liettua*<sup>31</sup> kantaja vaatii sanomalehdeltä vahingonkorvausta, koska se oli julkaissut artikkelin, jossa kerrottiin kantajan olevan HIV-positiivinen. Paikallisen sairaalan lääkärien väitettiin vahvistaneen tiedon. EIT:n mielestä kyseinen artikkeli ei liittynyt mihinkään yleistä etua koskevaan keskusteluun, ja se totesi, että henkilötietojen – erityisesti potilastietojen – suoja on olennaisen tärkeä edellytys sille, että henkilö voi nauttia EIS:n 8 artiklan mukaisesta oikeudesta yksityis- ja perhe-elämään kohdistuvaan kunnioitukseen. Tuomioistuin piti erityisen tärkeänä sitä, että sanomalehdessä esitettyjen tietojen mukaan sairaalan hoitohenkilökunta oli antanut tietoa kantajan HIV-infektioista vaitiolovelvollisuutensa vastaisesti. Valtio oli täten epäonnistunut velvollisuudessaan turvata kantajalle oikeus nauttia yksityiselämään kohdistuvaa kunnioitusta. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

30 Asia nro 48009/08, *Mosley v. Yhdistynyt kuningaskunta*, EIT 10.5.2011, 129 ja 130 kohta.

31 Asia nro 23373/03, *Biriuk v. Liettua*, EIT 25.11.2008.

## 1.2.2. Asiakirjojen saatavuus

Perusoikeuskirjan 11 artiklan ja EIS:n 10 artiklan mukainen sananvapaus ja tiedonvälityksen vapaus kattaa paitsi oikeuden esittää tietoa myös oikeuden saada tietoa. Hallinnon avoimuuden merkitys demokraattisen yhteiskunnan toiminnalle ymmärretään yhä paremmin. Siksi oikeus saada viranomaisten hallussa olevia asiakirjoja on tunnustettu jokaisen EU:n kansalaisen sekä jokaisen luonnollisen henkilön ja oikeushenkilön, jonka asuinpaikka tai rekisteröity toimipaikka on EU:n jäsenvaltiossa, tärkeäksi oikeudeksi.

**EN-oikeudessa** on mahdollista vedota virallisten asiakirjojen saatavuutta koskevassa suosituksessa määriteltyihin periaatteisiin. Kyseisen suosituksen pohjalta laadittiin virallisten asiakirjojen saatavuutta koskeva yleissopimus (*yleissopimus 205*).<sup>32</sup> **EU-oikeudessa** oikeus saada asiakirjoja on vahvistettu Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi annetussa asetuksessa (EY) N:o 1049/2001 (*asiakirjojen saatavuutta koskeva asetus*).<sup>33</sup> Perusoikeuskirjan 42 artiklassa ja SEUT 15 artiklan 3 kohdassa tämä oikeus on laajennettu kattamaan ”unionin toimielinten, elinten ja laitosten asiakirjat niiden tallennemuodosta riippumatta”. Perusoikeuskirjan 52 artiklan 2 kohdan mukaan oikeutta saada asiakirjoja sovelletaan SEUT 15 artiklan 3 kohdassa määriteltyjen edellytysten ja rajoitusten mukaisesti. Oikeus saada asiakirjoja voi olla ristiriidassa henkilötietojen suojaa koskevien oikeuksien kanssa, jos asiakirja sisältää muiden henkilötietoja. Viranomaisten hallussa olevien asiakirjojen tai tietojen saantia koskevia pyyntöjä voidaan näin ollen joutua punnitsemaan niiden henkilöiden tietosuojaoikeutta vasten, joiden tietoja pyydytetyt asiakirjat sisältävät.

Esimerkki: Asiassa *komissio v. Bavarian Lager*<sup>34</sup> EUTI määritteli henkilötietojen suojan laajuuden EU:n toimielinten asiakirjojen saatavuuden yhteydessä sekä asetusten (EY) N:o 1049/2001 (*asiakirjojen saatavuutta koskeva asetus*) ja (EY) N:o 45/2001 (*tietosuojasetus*) välisen suhteen. Vuonna 1992 perustettu Bavarian Lager tuo pulloitettua saksalaista olutta Yhdistyneeseen kuningaskuntaan, pääasiallisesti pubeihin ja baareihin. Se kuitenkin kohtasi vaikeuksia siksi,

- 32 Euroopan neuvosto, ministerikomitea (2002), suositus Rec(2002)2 virallisten asiakirjojen saatavuudesta, 21. helmikuuta 2002; Euroopan neuvosto, virallisten asiakirjojen saatavuutta koskeva yleissopimus, CETS nro 205, 18. kesäkuuta 2009. Yleissopimus ei ole vielä tullut voimaan.
- 33 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi, EYVL 2001 L 145.
- 34 Asia C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd*, EUTI 29.6.2010, 60, 63, 76, 78 ja 79 kohta.

että Yhdistyneen kuningaskunnan lainsäädäntö tosiasiallisesti suosii kansallisia valmistajia. Bavarian Lagerin tekemän valituksen seurauksena Euroopan komissio päätti käynnistää Yhdistynyttä kuningaskuntaa vastaan menettelyn velvollisuuksien noudattamatta jättämisen johdosta. Yhdistynyt kuningaskunta muuttikin kiistanalaisia säännöksiä ja saattoi ne yhdenmukaisiksi EU-oikeuden kanssa. Tämän jälkeen Bavarian Lager pyysi komissiolta muiden asiakirjojen mukana kopiota komission edustajien, Yhdistyneen kuningaskunnan viranomaisten ja ammattiyhdistyksen *Confédération des Brasseurs du Marché Commun* (CBMC) edustajien välisen kokouksen pöytäkirjasta. Komissio suostui paljastamaan joitakin tapaamiseen liittyneitä asiakirjoja, mutta peitti viisi pöytäkirjassa esiintynyttä nimeä, sillä kaksi henkilöä oli vastustanut henkilöllisyytensä paljastamista eikä komissio ollut onnistunut tavoittamaan kolmea muuta. Komissio hylkäsi 18. maaliskuuta 2004 tekemällään päätöksellä Bavarian Lagerin uuden pyynnön saada kokouksen pöytäkirja kokonaisuudessaan ja vetosi erityisesti asianomaisten yksityiselämän suojeluun sellaisena kuin se taataan tietosuoja-asetuksessa. Bavarian Lager ei hyväksynyt komission kantaa vaan nosti kanteen unionin yleisessä tuomioistuimessa. Tuomioistuin kumosi komission päätöksen 8. Marraskuuta 2007 tekemällään päätöksellä (asia T-194/04, *Bavarian Lager v. komissio*) ja katsoi erityisesti, että pelkkä asianomaisten nimien esiintyminen kokouksen osanottajaluettelossa niiden elinten kohdalla, joita he edustivat, ei vahingoittanut eikä vaarantanut yksityiselämän suojaa.

Komission valitettua EUTI kumosi unionin yleisen tuomioistuimen antaman tuomion. EUTI katsoi, että asiakirjojen saatavuutta koskevalla asetuksella "otetaan käyttöön erillinen ja vaativampi järjestely sellaisen henkilön suojaamiseksi, jonka henkilötiedot saatetaan joissain tapauksissa luovuttaa yleisölle". EUTI:n mukaan silloin, kun asiakirjojen saatavuutta koskevaan asetukseen perustuvalla hakemuksella pyydetään oikeutta tutustua henkilötietoja sisältävään asiakirjaan, asiakirjojen saatavuutta koskevan asetuksen säännökset tulevat kaikilta osin sovellettaviksi. Tämän jälkeen EUTI totesi, että komissio saattoi perustellusti hylätä hakemuksen saada tutustua lokakuussa 1996 pidetyn kokouksen täydelliseen pöytäkirjaan. Koska viisi kokouksen osanottajaa ei ollut antanut suostumustaan, komissio oli noudattanut riittävällä tavalla avoimuusveloitetaan luovuttamalla riidanalaisesta asiakirjasta version, josta kyseisten henkilöiden nimet oli poistettu.

Lisäksi EUTI katsoi seuraavaa: "Koska Bavarian Lager ei ole esittänyt mitään nimenomaista ja laillista tarkoitusta eikä minkäänlaisia vakuuttavia argumentteja osoittaakseen tarpeen näiden henkilötietojen siirtoon, komissio ei ole

voinut vertailla asianosaisten eri intressejä. Se ei ole myöskään voinut selvittää, oliko syytä ajatella, että rekisteröityjen oikeutetut edut voisivat siirron vuoksi vaarantua,” kuten tietosuoja-asetuksessa edellytetään.

Tuomion mukaan asiakirjojen saatavuus voi mennä yksityiselämän suojan edelle vain erityisestä ja perustellusta syystä. Oikeus saada asiakirjoja ei voi automaattisesti kumota oikeutta yksityiselämän- ja henkilötietojen suojaan.<sup>35</sup>

Seuraavassa EIT:n tuomiossa käsiteltiin yhtä asiakirjapyyntöihin liittyvää erityistä näkökohtaa.

Esimerkki: Asiassa *Társaság a Szabadságjogokért v. Unkari*<sup>36</sup> kantajana ollut ihmisoikeusjärjestö oli pyytänyt perustuslakituomioistuimelta tietoja käsiteltävänä olleesta asiasta. Kuulematta parlamentin jäsentä, joka oli saattanut asian sen käsiteltäväksi, perustuslakituomioistuin eväsi asiakirjapyyntön sen perusteella, että se saattoi käsiteltäväänään olleita valituksia ulkopuolisten saataville ainoastaan valituksen tekijän suostumuksella. Kansalliset tuomioistuimet pitivät epäämispäätöksen voimassa sen perusteella, ettei tällaisten henkilötietojen suoja voinut rajoittaa muilla oikeutetuilla eduilla, kuten oikeudella saada julkista tietoa. Kantaja oli toiminut ”sosiaalisena valvojana”, jolla oli toiminnassaan samanlainen suoja kuin lehdistöllä. Lehdistönvapauden yhteydessä EIT on toistuvasti todennut, että yleisöllä on oikeus saada yleistä etua koskevaa tietoa. Kantajan pyytämät tiedot olivat helposti saatavilla eivätkä edellyttäneet mitään tiedonkeruuta. Näissä olosuhteissa valtiolla oli velvollisuus olla haittaamatta kantajan pyytämää tietojen siirtoa. Yhteenvetona EIT katsoi, että esteet, joilla on tarkoitus haitata yleistä etua koskevien tietojen saantia, voivat rajoittaa tiedotusvälineissä tai vastaavilla aloilla työskentelevien henkilöiden mahdollisuutta suorittaa tärkeää tehtäväänsä ”vallan vahtikoirina”. Tuomioistuin totesi, että EIS:n 10 artiklaa oli rikottu.

Julkisuusperiaate on vakiintunut kiinteäksi osaksi **EU-oikeutta**. Julkisuusperiaate on vahvistettu SEU 1 ja 10 artiklassa sekä SEUT 15 artiklan 1 kohdassa.<sup>37</sup> Asetuksen (EY) N:o 1049/2001 johdanto-osan 2 kappaleen mukaan julkisuusperiaate parantaa

35 Ks. kuitenkin Euroopan tietosuojavaltuutetun (EDPS) yksityiskohtainen pohdinta asiakirjassa *Public access to documents containing personal data after the Bavarian Lager ruling*, Bryssel, 24. maaliskuuta 2011, saatavana osoitteessa: [www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24\\_Bavarian\\_Lager\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf).

36 Asia nro 37374/05, *Társaság a Szabadságjogokért v. Unkari*, EIT 14.4.2009; ks. 27, 36–38 kohta.

37 EU (2012), SEU:n ja SEUT:n konsolidoidut versiot, EUVL 2012 C 326.

kansalaisten mahdollisuuksia osallistua päätöksentekomenettelyihin ja sen avulla varmistetaan, että hallinnolla on demokraattisessa järjestelmässä suhteessa kansalaisiin suurempi legitimitetti, ja että se on tehokkaampaa ja vastuullisempaa.<sup>38</sup>

Tämän mukaisesti yhteisen maatalouspolitiikan rahoituksesta annetussa neuvoston asetuksessa (EY) N:o 1290/2005 ja kyseisen asetuksen soveltamista koskevista yksityiskohtaisista säännöistä annetussa komission asetuksessa (EY) N:o 259/2008 vaaditaan julkaisemaan tiettyjen maatalousalan EU-rahastojen tuensaajat ja kunkin tuensaajan saamat määrät.<sup>39</sup> Tietojen julkaisemisen on tarkoitus edistää julkisten varojen asianmukaisen käytön julkista valvontaa. Monet tuensaajat kiistivät tietojen julkaisemisen suhteellisuuden.

Esimerkki: Yhdistetyissä asioissa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*<sup>40</sup> EUTI joutui ottamaan kantaa siihen, oliko EU:n lainsäädännössä vaadittu EU:n maataloustukien saajien nimien ja heidän saamiensa määrien julkaiseminen suhteellisuusperiaatteen mukaista.

Tuomioistuimien toi esiin, että oikeus henkilötietojen suojaan ei ole ehdoton oikeus, ja se katsoi, että tietojen, joissa mainitaan kahden EU:n maatalousrahaston tuensaajien nimet ja heidän saamansa tarkat määrät, julkaisemisessa internetsivustolla on kyse puuttumisesta tuensaajien oikeuteen nauttia yksityiselämäänsä kohdistuvaa kunnioitusta yleensä ja erityisesti heidän oikeutensa saada henkilötiedoilleen suoja.

Tuomioistuimen mukaan tällainen puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin oikeuksiin oli ollut lainmukaista ja vastannut EU:n tunnustamaa yleisen edun mukaista tavoitetta, joka oli yhteisön varojen käytön avoimuuden lisääminen. EUTI katsoi kuitenkin, että kyseisistä EU:n maatalousrahastoista tukea saavien luonnollisten henkilöiden nimien ja heidän saamiensa tarkkojen määrien julkaiseminen oli suhteeton toimenpide eikä sitä

38 Asia C-41/00 P, *Interporc Im- und Export GmbH v. Euroopan yhteisöjen komissio*, EYTI 6.3.2003, 39 kohta; ja asia C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd.*, EUTI 29.6.2010, 54 kohta.

39 Neuvoston asetus (EY) N:o 1290/2005, annettu 21 päivänä kesäkuuta 2005, yhteisen maatalouspolitiikan rahoituksesta, EUVL 2005 L 209; ja komission asetus (EY) N:o 259/2008, annettu 18 päivänä maaliskuuta 2008, neuvoston asetuksen (EY) N:o 1290/2005 soveltamista koskevista yksityiskohtaisista säännöistä Euroopan maatalouden tukirahaston (maataloustukirahaston) ja Euroopan maaseudun kehittämisen maatalousrahaston (maaseuturahaston) varoja saavia tuensaajia koskevien tietojen julkaisemisen osalta, EUVL 2008 L 76.

40 Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen*, EUTI 9.11.2010, 47-52, 58, 66-67, 75, 86 ja 92 kohta.

voitu perustella perusoikeuskirjan 52 artiklan 1 kohdalla. Näin ollen tuomioistuin totesi, että EU:n maatalousrahastojen tuensaajia koskevien tietojen julkaisemisesta annettu EU:n lainsäädäntö oli osittain pätemätöntä.

### 1.2.3. Taiteen ja tutkimuksen vapaus

Yksi oikeus, jota on punnittava suhteessa yksityiselämän- ja henkilötietojen suojaan koskeviin oikeuksiin, on taiteen ja tutkimuksen vapaus, joka on nimenomaisesti turvattu perusoikeuskirjan 13 artiklassa. Tämä oikeus on johdettu pääasiallisesti oikeudesta ajatuksen- ja ilmaisunvapauteen ja sen käytössä on otettava huomioon perusoikeuskirjan 1 artikla (ihmisarvo). EIT katsoo, että taiteen vapaus on turvattu EIS:n 10 artiklalla.<sup>41</sup> EIS:n 10 artiklassa sallittuja rajoituksia voidaan soveltaa myös perusoikeuskirjan 13 artiklassa taattuun oikeuteen.<sup>42</sup>

Esimerkki: Asiassa *Vereinigung bildender Künstler v. Itävalta*<sup>43</sup> itävaltalaiset tuomioistuimet kielsivät kantajana ollutta yhdistystä jatkamasta sellaisen taulun näyttämistä, jossa oli valokuvia julkisuuden henkilöistä seksiasennoissa. Itävallan parlamentin jäsen, jonka valokuvaa oli käytetty maalauksessa, nosti kantajana ollutta yhdistystä vastaan kanteen, jolla se haki kieltomääräystä taulun näyttämislle. Kansallinen tuomioistuin hyväksyi pyynnön ja antoi kieltomääräyksen. EIT totesi, että EIS:n 10 artiklaa sovelletaan sellaisten ajatusten esittämiseen, jotka loukkaavat, järkyttävät tai häiritsevät valtiota tai jotain väestön osaa. Taideteoksia luovat, esittävät tai näyttävät henkilöt osallistuvat ajatusten ja näkemysten vaihtoon, ja valtiolla on velvollisuus olla rajoittamatta perusteettomasti heidän ilmaisunvapauttaan. Kun otetaan huomioon, että kyseinen taulu oli kollaasi, jossa käytettiin valokuvia ainoastaan henkilöiden päistä ja heidän vartalonsa oli maalattu epärealistisesti ja liioitellusti tavalla, jonka ei selvästi ollut tarkoitus heijastaa todellisuutta tai edes viitata todellisuuteen, EIT katsoi, ettei taulun voitu ymmärtää käsittelevän esitetyn henkilön yksityiselämää, vaan sen oli pikemminkin ymmärrettävä liittyvän taiteilijan näkemykseen poliitikoista, ja että esitetyn henkilön oli asemansa puolesta suvaittava kritiikkiä tavallista laajemmin. Punnittuaan asiaan liittyviä erilaisia etuja EIT päätyi siihen, että taulun esittämisen rajoittamaton kieltö oli suhteeton. Tuomioistuin katsoi, että EIS:n 10 artiklaa oli rikottu.

41 Asia nro 10737/84, *Müller ym. v. Sveitsi*, EIT 24.5.1988.

42 Euroopan unionin perusoikeuskirjan selitykset, EUVL 2007 C 303.

43 Asia nro 68345/01, *Vereinigung bildender Künstler v. Itävalta*, EIT 25.1.2007; ks. erityisesti 26 ja 34 kohta.



Euroopan tietosuoja säännöksissä on otettu huomioon tieteen erityinen merkitys yhteiskunnalle. Siksi henkilötietojen käsittelyä koskevia yleisiä rajoituksia on vähennetty. Sekä tietosuojadirektiivissä että yleissopimuksessa 108 sallitaan tietojen säilyttäminen tieteellistä tutkimusta varten sen jälkeen, kun niitä ei enää tarvita siihen käyttöön, johon ne on alun perin kerätty. Lisäksi henkilötietojen myöhempää käsittelyä tieteelliseen tutkimukseen ei pidetä yhteensopimattomana sen tarkoituksen kanssa, johon henkilötiedot on alun perin kerätty. Yksityiskohtaisemmat säännökset, kuten tarvittavat suojoitoimet, joilla tieteellisen tutkimuksen etu ja henkilötietojen suoja sovitaan yhteen, määritellään kansallisessa lainsäädännössä (ks. myös 3.3.3 ja 8.4 kohta).

## 1.2.4. Omaisuudensuoja

Oikeus omaisuudensuojaan on vahvistettu EIS:n ensimmäisen lisäpöytäkirjan 1 artiklassa ja perusoikeuskirjan 17 artiklan 1 kohdassa. Yksi omaisuudensuojaa koskevan oikeuden tärkeä näkökohta on oikeus teollis- ja tekijänoikeuksien turvaan, joka mainitaan erikseen perusoikeuskirjan 17 artiklan 2 kohdassa. EU:n oikeusjärjestykseen kuuluu useita direktiivejä, joilla pyritään turvaamaan tehokkaasti henkinen omaisuus, erityisesti tekijänoikeudet. Henkinen omaisuus kattaa kirjallisen ja taiteellisen omaisuuden lisäksi patenti- ja tavaramerkkioikeudet sekä niihin liittyvät oikeudet.

EUTI:n oikeuskäytännöstä käy ilmi, että perusoikeutta omaisuudensuojaan on punnittava suhteessa muihin perusoikeuksiin, erityisesti suhteessa yksityiselämän suojaan.<sup>44</sup> Tekijänoikeusjärjestöt ovat joissakin tapauksissa vaatineet internetpalvelujen tarjoajia paljastamaan internetissä olevien tiedostojen jako-ohjelmien käyttäjien henkilöllisyyden. Tällaiset ohjelmat antavat internetin käyttäjille usein mahdollisuuden ladata musiikkikappaleita ilmaiseksi, vaikka kappaleet olisi suojattu tekijänoikeuksilla.

Esimerkki: Asiassa *Promusicae v. Telefónica de España*<sup>45</sup> espanjalainen internetyhteyspalvelujen tarjoaja, Telefónica, oli kieltäytynyt luovuttamasta musiikkitalenteiden ja audiovisuaalisten tallenteiden tuottajien ja julkaisijoiden voittoa tavoittelemattomalle yhdistykselle, Promusicaelle, tiettyjen sellaisten henkilöiden tietoja, joille se tarjosi internetyhteyspalveluja. Promusicae tarvitsi tietoja

44 Asia nro 36769/08, *Ashby Donald ym. v. Ranska*, EIT 10.1.2013.

45 Asia C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, EYTI 29.1.2008, 54 ja 60 kohta.

voidakseen panna vireille siviiliprosessit niitä henkilöitä vastaan, jotka olivat sen mukaan käyttäneet tiedostojen jako-ohjelmaa, jonka avulla oli mahdollista saada äänitteitä, joiden käyttöön liittyvät taloudelliset oikeudet kuuluivat Promusicaen jäsenille.

Espanjalainen tuomioistuin saattoi asian EYTI:n käsiteltäväksi ja kysyi, velvoittaako yhteisön oikeus luovuttamaan henkilötietoja siviiliprosessin yhteydessä tekijänoikeuden tehokkaan suojan varmistamiseksi. Espanjalainen tuomioistuin viittasi direktiiveihin 2000/31, 2001/29 ja 2004/48, kun niitä luetaan myös perusoikeuskirjan 17 ja 47 artiklan valossa. EYTI totesi, että kyseisissä kolmessa direktiivissä sen enempää kuin sähköisen viestinnän tietosuojadirektiivissäkään (direktiivi 2002/58) ei suljeta pois jäsenvaltioiden mahdollisuutta säätää velvollisuudesta paljastaa henkilötietoja siviiliprosessin yhteydessä tekijänoikeuden tehokkaan suojan varmistamiseksi.

EYTI esitti, että asiassa tuli esiin kysymys eri perusoikeuksien eli yhtäältä yksityisyyden kunnioittamista koskevan oikeuden ja toisaalta omaisuudensuojaa ja tehokkaita oikeussuojakeinoja koskevien oikeuksien suojaan liittyvien vaatimusten välttämättömästä yhteensovittamisesta.

Tuomioistuin totesi, että ”jäsenvaltioiden on pannessaan täytäntöön edellä mainittuja direktiivejä huolehdittava siitä, että ne nojautuvat sellaiseen kyseisten direktiivien tulkintaan, jolla voidaan varmistaa yhteisön oikeusjärjestyksessä suojattujen eri perusoikeuksien välinen asianmukainen tasapaino. Jäsenvaltioiden viranomaisten ja tuomioistuinten on pannessaan täytäntöön kyseisten direktiivien noudattamisen edellyttämiä toimenpiteitä tulkittava kansallista oikeuttaan mainittujen direktiivien mukaisesti, ja niiden on tämän lisäksi myös varottava nojautumasta sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan mainittujen perusoikeuksien kanssa tai muiden yhteisön oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa.”<sup>46</sup>

46 *Ibid.*, 65 ja 68 kohta; ks. myös asia C-360/10, *SABAM v. Netlog N.V.*, EUTI 16.2.2012.

# 2

## Tietosuojan terminologia

EU	Katetut aiheet	EN
<b>Henkilötiedot</b>		
Tietosuojadirektiivi, 2 artiklan a alakohta Yhdistetyt asiat C-92/09 ja C-93/09, <i>Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen</i> , EUTI 9.11.2010 <i>Asia, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU</i> , EYTI 29.1.2008	Oikeudellinen määritelmä	Yleissopimus 108, 2 artiklan a alakohta <i>Asia nro 24117/08, Bernh Larsen Holding AS ym. v. Norja</i> , EIT 14.3.2013
Tietosuojadirektiivi, 8 artiklan 1 kohta <i>Asia C-101/01, Bodil Lindqvist</i> , EYTI 6.11.2003	E erityiset tietoryhmät (arkaluonteiset tiedot)	Yleissopimus 108, 6 artikla
Tietosuojadirektiivi, 6 artiklan 1 kohdan e alakohta	Anonyymit ja pseudonyymit tiedot	Yleissopimus 108, 5 artiklan e alakohta Yleissopimus 108, selitysmuistio, 42 artikla
<b>Tietojen käsittely</b>		
Tietosuojadirektiivi, 2 artiklan b alakohta <i>Asia C-101/01, Bodil Lindqvist</i> , EYTI 6.11.2003	Määritelmät	Yleissopimus 108, 2 artiklan c alakohta
<b>Tietojen käyttäjät</b>		
Tietosuojadirektiivi, 2 artiklan d alakohta	Rekisterinpitäjä	Yleissopimus 108, 2 artiklan d alakohta Profilointia koskeva suositus, 1 artiklan g alakohta *

EU	Katetut aiheet	EN
Tietosuojadirektiivi, 2 artiklan e alakohta Asia C-101/01, <i>Bodil Lindqvist</i> , EYTI 6.11.2003	Henkilötietojen käsittelijä	Profilointia koskeva suositus, 1 artiklan h alakohta
Tietosuojadirektiivi, 2 artiklan g alakohta	Vastaanottaja	Yleissopimus 108, lisäpöytäkirja, 2 artiklan 1 kohta
Tietosuojadirektiivi, 2 artiklan f alakohta	Sivullinen	
<b>Suostumus</b>		
Tietosuojadirektiivi, 2 artiklan h alakohta Asia C-543/09, <i>Deutsche Telekom AG v. Bundesrepublik Deutschland</i> , EUTI 5.5.2011	Pätevän suostumuksen määritelmä ja edellytykset	Potilastietoja koskeva suositus, 6 artikla, ja erilaisia myöhempiä suosituksia

Huom.: \* Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä (profilointia koskeva suositus), 23. marraskuuta 2010.

## 2.1. Henkilötiedot

### Keskeiset kohdat

- Tiedot ovat henkilötietoja, jos ne koskevat tunnistettua tai tunnistettavissa olevaa henkilöä, eli rekisteröityä.
- Henkilöä pidetään tunnistettavissa olevana, jos hänestä on ilman kohtuutonta vaivaa mahdollista saada lisätietoa, jonka avulla hänet voi tunnistaa.
- Todentaminen tarkoittaa sen todistamista, että tietyllä henkilöllä on tietty henkilöllisyys ja/tai lupa toteuttaa tiettyjä toimintoja.
- Yleissopimuksessa 108 ja tietosuojadirektiivissä on lueteltu erityisiä tietoryhmiä, niin kutsuttuja arkaluonteisia tietoja, jotka vaativat vahvempaa suojaa ja joihin sitä varten sovelletaan erityistä oikeudellista järjestelmää.
- Tiedot on tehty anonyymeiksi, jos tiedot eivät sisällä mitään tunnistetta. Jos henkilötietojen tunnisteen salataan, tiedot ovat pseudonyymejä.
- Toisin kuin anonyymit tiedot, pseudonyymit tiedot ovat henkilötietoja.

## 2.1.1. Henkilötietojen käsitteen tärkeimmät näkökohdat

**EU-oikeudessa** samoin kuin **EN-oikeudessa** henkilötiedot määritellään tiedoiksi, jotka koskevat tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä,<sup>47</sup> eli sellaiseksi henkilöä koskevaksi tiedoksi, josta henkilö voidaan tunnistaa suoraan tai välillisesti.

Jos tällaista henkilöä koskevia tietoja käsitellään, henkilöstä käytetään nimitystä ”rekisteröity”.

### Henkilö

Oikeus tietosuojaan kehittyi oikeudesta nauttia yksityiselämään kohdistuvaa kunnioitusta. Yksityiselämän käsite liittyy ihmisiin. Näin ollen tietosuojaa sovelletaan ensisijaisesti luonnollisiin henkilöihin. Tietosuojadirektiivin 29 artiklan mukaisen työryhmän laatimassa lausunnossa todetaan vielä, että Euroopan tietosuojaoikeutta sovelletaan ainoastaan *eläviin olentoihin*.<sup>48</sup>

EIS:n 8 artiklaa koskevasta EIT:n oikeuskäytännöstä ilmenee, että yksityis- ja työelämä voi toisinaan olla vaikea erottaa selkeästi toisistaan.<sup>49</sup>

Esimerkki: Asiassa *Amann v. Sveitsi*<sup>50</sup> kantajan työnpuhelua oli kuunneltu viranomaisten toimesta. Puhelun perusteella viranomaiset tutkivat kantajan tiedot ja laativat hänestä kordin kansalliseen turvallisuuskorttihakemistoon. Vaikka telekuuntelu kohdistui työnpuheluun, EIT katsoi, että kyseistä puhelua koskevien tietojen säilyttäminen liittyi kantajan yksityiselämään. Se toi esiin, ettei termiä ”yksityiselämä” tullut tulkita rajoittavasti, erityisesti siksi, että yksityiselämän kunnioitus kattoi oikeuden luoda ja ylläpitää suhteita muihin ihmisiin. Lisäksi ei ollut mitään periaatteellista syytä sulkea työ- tai liikeasioita ”yksityiselämän” käsitteen ulkopuolelle. Tällainen laaja tulkinta oli yleissopimuksen 108 mukainen. EIT vielä katsoi, että kantajan tapauksessa telekuuntelu oli ollut laitonta,

47 Tietosuojadirektiivi, 2 artiklan a alakohta; yleissopimus 108, 2 artiklan a alakohta.

48 Tietosuojatyöryhmä (2007), *lausunto 4/2007 henkilötietojen käsitteestä*, WP 136, 20. kesäkuuta 2007, s. 22.

49 Ks. esim. asia nro 28341/95, *Rotaru v. Romania* [suuri jaosto], EIT 4.5.2000, 43 kohta; asia nro 13710/88, *Niemietz v. Saksa*, EIT 16.12.1992, 29 kohta.

50 Asia nro 27798/95, *Amann v. Sveitsi* [suuri jaosto], EIT 16.2.2000, 65 kohta.

sillä kansallisessa lainsäädännössä ei ollut erityisiä eikä yksityiskohtaisia säännöksiä tietojen keruusta, tallennuksesta ja säilytyksestä. Tuomioistuin totesi näin ollen, että EIS:n 8 artiklaa oli rikottu.

Jos työelämään liittyviin asioihin voidaan soveltaa tietosuojaa koskevia säännöksiä, vaikuttaa kyseenalaiselta, että suoja koskisi ainoastaan luonnollisia henkilöitä. EIS:n mukaiset oikeudet on taattu kaikille, ei vain luonnollisille henkilöille.

EIT on oikeuskäytännössään ratkaissut asioita, joissa oikeushenkilöt ovat kanteessaan väittäneet, että niiden EIS:n 8 artiklan mukaista oikeutta yksityiselämän suojaan on rikottu. Tuomioistuin on kuitenkin painottanut enemmän oikeutta nauttia kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta kuin oikeutta nauttia yksityiselämään kohdistuvaa kunnioitusta:

Esimerkki: *Asiassa Bernh Larsen Holding AS ym. v. Norja*<sup>51</sup> kolme norjalaista yritystä oli tehnyt valituksen veroviranomaisen päätöksestä, jolla ne määrättiin toimittamaan verotarkastajille jäljennös kaikista niiden yhteisessä käytössä olleella palvelimella olleista tiedoista.

EIT totesi, että tällainen kantajina olleille yrityksille määrätty velvollisuus rikkoi EIS:n 8 artiklassa tarkoitettua oikeutta nauttia ”kotiin” ja ”kirjeenvaihtoon” kohdistuvaa kunnioitusta. Tuomioistuin kuitenkin katsoi, että veroviranomaisilla oli tehokkaat ja riittävät suojaustoimet väärinkäytöksiä vastaan: kantajina olleille yrityksille oli ilmoitettu asiasta hyvissä ajoin; ne olivat läsnä ja saivat esittää huomioita, kun paikalla tehty tarkastus toteutettiin; ja aineisto oli määrää tuhota sen jälkeen, kun verotarkastus olisi saatettu päätökseen. Näissä olosuhteissa kantajina olleiden yritysten oikeus nauttia kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta oli saatettu asianmukaisesti tasapainoon yhtäältä sen intressin kanssa, joka yrityksillä on työntekijöiden yksityisyyden suojaamisessa, ja toisaalta sen yleisen intressin kanssa, joka on verojen arviointiin tarvittavan tehokkaan tarkastuksen varmistaminen. Tuomioistuin katsoi näin ollen, ettei EIS:n 8 artiklaa ollut rikottu.

**Yleissopimuksen 108 mukaan** tietosuoja koskee ensisijaisesti luonnollisia henkilöitä; sopimuspuolet voivat kuitenkin kansallisessa lainsäädännössään ulottaa tietosuojan oikeushenkilöihin, kuten yrityksiin ja yhdistyksiin. **EU:n** tietosuojaa koskevaa

51 Asia nro 24117/08, *Bernh Larsen Holding AS ym. v. Norja*, EIT 14.3.2013. Ks. kuitenkin myös asia nro 58243/00, *Liberty ym. v. Yhdistynyt kuningaskunta*, EIT 1.7.2008.

säädöksiä ei pääsääntöisesti sovelleta oikeushenkilöitä koskevien tietojen käsitteilyyn. Tästä asiasta voidaan vapaasti säätää kansallisella tasolla.<sup>52</sup>

Esimerkki: Yhdistetyissä asioissa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*<sup>53</sup> EUTI totesi maatalousrahastojen tuensaajien henkilötietojen julkaisemisen osalta, että ”oikeushenkilöt voivat vedota tällaisen yksilöinnin kannalta perusoikeuskirjan 7 ja 8 artiklan mukaiseen suojaan vain siltä osin kuin oikeushenkilön virallisessa nimessä yksilöidään yksi tai usea luonnollinen henkilö. Perusoikeuskirjan 7 ja 8 artiklassa tunnustettu oikeus yksityiselämän kunnioittamiseen henkilötietojen käsittelyssä koskee kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja.”<sup>54</sup>

## Henkilön tunnistettavuus

Sekä **EU-oikeudessa** että **EN-oikeudessa** tieto sisältää henkilötietoja, jos

- henkilö on tunnistettu; tai
- henkilöä ei ole tunnistettu, mutta hänet on kuvattu tavalla, jolloin tunnistaminen on mahdollista tiettyjen lisätoimenpiteiden avulla.

Molemmat näistä tiedon muodoista on suojattu Euroopan tietosuojaa koskevissa säädöksissä. EIT on useasti todennut, että henkilötietojen käsite on yleissopimuksessa 108 sama kuin EIS:ssa, erityisesti siltä osin, kuin niiden edellytetään viittaavan tunnistettuihin tai tunnistettaviin henkilöihin.<sup>55</sup>

Henkilötietojen oikeudellisissa määritelmissä ei selvitetä tämän tarkemmin, milloin henkilön katsotaan olevan tunnistettu.<sup>56</sup> Tunnistaminen edellyttää tietenkin henkilön kuvaamista tavalla, joka erottaa hänet kaikista muista henkilöistä ja mahdollistaa hänen yksilöimisensä. Henkilön nimi on hyvä esimerkki tällä tavalla kuvaavasta tiedosta. Poikkeuksellisissa tapauksissa muilla tunnisteilla voi olla samankaltainen

52 Tietosuojadirektiivi, johdanto-osan 24 kappale.

53 Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR (C-92/09) ja Hartmut Eifert (C-93/09) v. Land Hessen*, EUTI 9.11.2010, 53 kohta.

54 *Ibid.*, 52 kohta.

55 Ks. asia nro 27798/95, *Amann v. Sveitsi* [suuri jaosto], EIT 16.2.2000, 65 kohta ja sitä seuraavat kohdat.

56 Ks. myös asia nro 42326/98, *Odièvre v. Ranska* [suuri jaosto], EIT 13.2.2003; ja asia nro 33783/09, *Godelli v. Italia*, EIT 25.9.2012.

vaikutus kuin nimellä. Julkisuuden henkilöiden osalta voi riittää, että viitataan henkilön asemaan, esimerkiksi Euroopan komission puheenjohtaja.

Esimerkki: Asiassa *Promusicae*<sup>57</sup> EYTI totesi, että ”on kiistatonta, että Promusicaen vaatima [tietyn tiedostojen jako-ohjelman] tiettyjen käyttäjien nimien ja osoitteiden luovuttaminen merkitsee henkilötietojen eli direktiivin 95/46 2 artiklan a alakohdassa olevan määritelmän mukaisesti tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevien tietojen käyttöön antamista – -. Niiden tietojen luovuttaminen, jotka Telefónica on Promusicaen mukaan tallentanut – mitä Telefónica ei ole kiistänyt – on direktiivin 2002/58 2 artiklan ensimmäisessä kohdassa, luettuna yhdessä direktiivin 95/46 2 artiklan b alakohdan kanssa, tarkoitettua henkilötietojen käsittelyä.”

Monet nimet eivät ole ainutlaatuisia ja siksi voidaan tarvita muita tunnisteita, jotta varmistettaisiin, ettei henkilöllisyyksissä tapahdu sekaannuksia. Syntymäaikaa ja -paikkaa käytetään usein. Lisäksi joissakin maissa on otettu käyttöön yksilölliset numerot helpottamaan kansalaisten yksilöimistä. Biometrisiä tietoja, kuten sormenjälkiä, digitaalisia valokuvia tai iiriksen kuvaa, käytetään tekniikan aikakaudella yhä useammin henkilöiden tunnistamiseen.

Euroopan tietosuojasäännösten soveltaminen ei kuitenkaan edellytä rekisteröidyn tarkkaa tunnistamista vaan riittää, että asianomainen henkilö on tunnistettavissa. Henkilöä pidetään tunnistettavissa olevana, jos tieto sisältää tunnisteita, joiden avulla henkilö voidaan tunnistaa suoraan tai välillisesti.<sup>58</sup> Tietosuojadirektiivin johdanto-osan 26 kappaleen mukaan olennaista on se, onko tiedon ennakoitavissa olevilla käyttäjillä, sivulliset vastaanottajat mukaan luettuina, todennäköisesti käytössään kohtuullisesti toteutettavissa olevia keinoja henkilön tunnistamiseksi (ks. 3.3.2 kohta).

Esimerkki: Paikallisviranomaisen päättää kerätä tietoa alueen teillä ylinopeutta ajavista autoista. Se valokuvaa autot tallentaen automaattisesti aika- ja paikkatiedot, jotta toimivaltainen viranomais voisi sakottaa niitä henkilöitä, jotka rikkovat nopeusrajoituksia. Rekisteröity tekee valituksen ja väittää, ettei paikallisviranomaisella ole lain mukaista oikeudellista perustetta tällaiselle

57 Asia, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, EYTI 29.1.2008, 45 kohta.

58 Tietosuojadirektiivi, 2 artiklan a alakohda.



tiedonkeruulle. Paikallisviranomaisen katsoo, että se ei kerää henkilötietoja. Sen mielestä rekisterikilvet ovat anonyymien henkilöiden tietoja. Paikallisviranomaisella ei ole laillista toimivaltaa käyttää yleistä ajoneuvorekisteriä auton omistajan tai kuljettajan henkilöllisyyden selvittämiseksi.

Tämä perustelu ei ole yhdenmukainen tietosuojadirektiivin johdanto-osan 26 kappaleen kanssa. Kun otetaan huomioon, että tiedonkeruun tarkoituksena selkeästi on ylinopeutta ajavien henkilöiden tunnistaminen ja sakottaminen, on ennakoitavissa, että henkilöitä pyritään tunnistamaan. Vaikka paikallisviranomaisella ei ole suoraan käytettävissään tunnistuskeinoja, se välittää tiedot toimivaltaiselle viranomaiselle, poliisille, jolla on tällaiset keinot. Johdanto-osan 26 kappaleessa on myös erikseen mainittu tilanne, jossa tulevat tiedon vastaanottajat, muut kuin välitön tiedon käyttäjä, voivat yrittää tunnistaa henkilön. Johdanto-osan 26 kappaleen valossa paikallisviranomaisen toiminta vastaa tiedon keräämistä tunnistettavissa olevista henkilöistä ja siksi sillä tulisi olla lain mukainen oikeudellinen peruste.

**EN-oikeudessa** tunnistettavuus ymmärretään samankaltaisesti. Maksutapahtumia koskevan suosituksen<sup>59</sup> 1 artiklan 2 kohdassa esimerkiksi todetaan, että henkilöä ei pidetä tunnistettavissa olevana, jos tunnistaminen vaatii kohtuuttoman paljon aikaa, kustannuksia tai työtä.

## Todentaminen

Todentaminen on menettely, jonka kautta henkilö voi todistaa, että hänellä on tietty henkilöllisyys ja/tai lupa tehdä tiettyjä asioita, kuten päästä suljetulle alueelle tai nostaa rahaa pankkitililtä. Todentaminen voidaan toteuttaa vertaamalla biometrisiä tietoja (kuten passissa olevaa valokuvaa tai sormenjälkeä) esimerkiksi maahanmuuttoa varten esittäytyvän henkilön tietoihin, tai kysymällä tietoja, jotka voi tietää vain henkilö, jolla on tietty henkilöllisyys tai lupa (kuten henkilökohtainen tunnusluku tai salasana), tai vaatimalla henkilöä esittämään tietty merkki, jonka pitäisi olla vain sellaisen henkilön hallussa, jolla on tietty henkilöllisyys tai lupa (kuten erityinen sirukortti tai tallelokeron avain). Paitsi salasanojen ja sirukorttien avulla, yhdistettyinä toisinaan henkilökohtaiseen tunnuslukuun, henkilö voidaan sähköisessä viestinnässä tunnistaa ja todentaa erityisesti sähköisellä allekirjoituksella.

59 EN, ministerineuvosto (1990), suositus R Rec(90) 19 henkilötietojen suojaamisesta maksutapahtumissa, 13. syyskuuta 1990.

## Tiedon luonne

Kaikenlaiset tiedot voivat olla henkilötietoja, jos ne liittyvät henkilöön.

Esimerkki: Työntekijän henkilökansioon tallennettu esimiehen arvio työntekijän työsuorituksesta on työntekijää koskeva henkilötieto, vaikka se vain kuvastaisi osittain tai kokonaisuudessaan esimiehen henkilökohtaista näkemystä, esimerkiksi näin: ”työntekijä ei ole omistautunut työlleen” eikä paljastaisi tosiseikkoja, esimerkiksi näin: ”työntekijä on ollut viimeisen puolen vuoden aikana viisi viikkoa poissa töistä”.

Henkilötietoihin kuuluvat tiedot, jotka liittyvät henkilön yksityiselämään, samoin kuin tiedot hänen työ- tai julkisesta elämästään.

Asiassa *Amann*<sup>60</sup> EIT tulkitsi henkilötietojen käsitettä siten, että se ei rajoittunut henkilön yksityisasioihin (ks. 2.1.1 kohta). Tämä termin ”henkilötiedot” merkitys on olennainen myös tietosuojadirektiivin näkökulmasta:

Esimerkki: Yhdistetyissä asioissa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*<sup>61</sup> EUTI totesi seuraavaa: ”Tässä on merkityksetöntä, että julkaistavat tiedot liittyvät ammattitoimintaan –. Euroopan ihmisoikeustuomioistuin on tältä osin todennut Euroopan ihmisoikeussopimuksen 8 artiklan tulkinnasta, ettei ilmaisua ’yksityiselämä’ pidä tulkita suppeasti ja ettei mikään periaatteellinen syy salli sitä, että ammattitoiminta jätettäisiin – ’yksityiselämän’ käsitteen ulkopuolelle.”

Tiedot liittyvät henkilöön myös silloin, kun tiedon sisältö paljastaa välillisesti tietoja henkilöstä. Joissakin tapauksissa, joissa esineen tai tapahtuman – esimerkiksi matkapuhelimen, auton tai onnettomuuden – ja tietyn henkilön – esimerkiksi omistajan, käyttäjän tai uhrin – välillä on läheinen kytkös, esinettä tai tapahtumaa koskevaa tietoa tulisi myös pitää henkilötietona.

60 Ks. asia nro 27798/95, *Amann v. Sveitsi*, EIT 16.2.2000, 65 kohta.

61 Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen*, EUTI 9.11.2010, 59 kohta.

Esimerkki: Asiassa *Uzun v. Saksa*<sup>62</sup> kantajaa ja toista miestä seurattiin toisen miehen autoon asennetulla GPS-laitteella, koska heidän epäiltiin osallistuneen pommi-iskuihin. Kyseisessä asiassa EIT katsoi, että kantajan tarkkaileminen GPS-laitteella rikkoi EIS:n 8 artiklan mukaista oikeutta nauttia yksityiselämän suojaa. GPS-valvonta oli kuitenkin ollut lainmukaista ja oikeassa suhteessa lailiseen tarkoitukseen, joka oli useiden murhayritysten tutkiminen, ja siksi sen katsottiin olevan tarpeellista demokraattisessa yhteiskunnassa. Tuomioistuimien totesi, ettei EIS:n 8 artiklaa ollut rikottu.

## Tiedon esitysmuoto

Muoto, jossa henkilötietoja säilytetään ja käytetään, ei vaikuta tietosuojaa koskevien säännösten sovellettavuuteen. Henkilötietoja voi sisältyä yhtä lailla kirjalliseen kuin puheviestintään samoin kuin kuvamateriaaliin,<sup>63</sup> kuten kameravalvontatallenteisiin,<sup>64</sup> tai äänimateriaaliin.<sup>65</sup> Sähköisesti tallennettu tieto voi olla henkilötietoa siinä missä paperillakin oleva tieto; jopa ihmiskudoksen solunäytteet voivat olla henkilötietoa, sillä niihin on tallentunut henkilön dna.

## 2.1.2. Erityiset tietoryhmät

**EU-oikeudessa** ja **EN-oikeudessa** on erityisiä henkilötietojen ryhmiä, jotka saattavat luonteensa takia aiheuttaa rekisteröidyille riskin, kun niitä käsitellään, ja jotka tarvitsevat siksi erityistä suojaa. Näiden erityisten tietoryhmien (”arkaluonteisten tietojen”) käsittely voidaan sallia vain, kun on käytössä tarkoin määritellyt suojatoimet.

Arkaluonteisten tietojen määrittelemiseksi luetellaan sekä [yleissopimuksessa 108](#) (6 artikla) että [tietosuojadirektiivissä](#) (8 artikla) seuraavat ryhmät:

- henkilötiedot, joista käy ilmi rotu tai etninen alkuperä;
- henkilötiedot, jotka paljastavat poliittiset mielipiteet, uskonnollisen tai muun vakaumuksen; sekä

<sup>62</sup> Asia nro 35623/05, *Uzun v. Saksa*, EIT 2.9.2010.

<sup>63</sup> Asia nro 59320/00, *Von Hannover v. Saksa*, EIT 24.6.2004; asia nro 50774/99, *Sciacca v. Italia*, EIT 11.1.2005.

<sup>64</sup> Asia nro 44647/98, *Peck v. Yhdistynyt kuningaskunta*, EIT 28.1.2003; asia nro 420/07, *Köpke v. Saksa*, EIT 5.10.2010.

<sup>65</sup> Tietosuojadirektiivi, johdanto-osan 16 ja 17 kappale, asia nro 44787/98, *P.G. and J.H. v. Yhdistynyt kuningaskunta*, EIT 25.9.2001, 59 ja 60 kohta; asia nro 71611/07, *Wisse v. Ranska*, EIT 20.12.2005.

- henkilötiedot, jotka koskevat terveyttä tai seksuaalista käyttäytymistä

Esimerkki: Asiassa *Bodil Lindqvist*<sup>66</sup> EYTI totesi, että ”mainintaa siitä, että henkilö on loukannut jalkansa ja on osa-aikaisella sairauslomalla, on pidettävä direktiivin 95/46/EY 8 artiklan 1 kohdassa tarkoitettuna terveyteen liittyvänä henkilötietona”.

Tietosuojadirektiivissä mainitaan lisäksi ”ammattiliittoon kuuluminen” arkaluonteisena tietona, sillä tämä tieto voi olla merkki poliittisesta näkemyksestä tai kytköksestä.

Yleissopimuksessa 108 taas pidetään rikosoikeudellisiin tuomioihin liittyviä henkilötietoja arkaluonteisina.

Tietosuojadirektiivin 8 artiklan 7 kohdassa annetaan EU:n jäsenvaltioille tehtäväksi ”määritellä olosuhteet, joiden vallitessa henkilönumeroa tai muuta yleistä tunnistetta voidaan käsitellä”.

### 2.1.3. Anonyymit ja pseudonyymit tiedot

Tietosuojadirektiivin ja yleissopimuksen 108 mukainen tietojen käyttötarkoitussidonnaisuuden periaate (jota käsitellään tarkemmin 3 luvussa) edellyttää, että tietoja säilytetään ”muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan, kuin on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään”.<sup>67</sup> Tämä tarkoittaa, että jos rekisterinpitäjä haluaisi säilyttää tietoja sen jälkeen, kun ne ovat vanhentuneet eivätkä enää palvele alkuperäistä tarkoitustaan, tiedot pitäisi tehdä anonyymeiksi.

#### Anonyymit tiedot

Henkilötiedot tehdään anonyymeiksi siten, että niistä poistetaan kaikki tunnistamisen mahdollistavat ainekset. Tietoihin ei saa jättää mitään sellaista, minkä avulla voisi kohtuullisella vaivalla selvittää asianomaisen henkilön henkilöllisyyden.<sup>68</sup> Kun tiedot on tehty anonyymeiksi, niitä ei enää pidetä henkilötietoina.

66 Asia C-101/01, *Bodil Lindqvist*, EYTI 6.11.2003, 51 kohta.

67 Tietosuojadirektiivi, 6 artiklan 1 kohdan e alakohta; ja yleissopimus 108, 5 artiklan e alakohta.

68 *Ibid.*, johdanto-osan 26 kappale.

Tietosuojadirektiivissä ja yleissopimuksessa 108 annetaan mahdollisuus säilyttää henkilötietoja tunnistellisessa muodossa historian tutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten sen jälkeen, kun henkilötiedot eivät enää palvele alkuperäistä tarkoitustaan, kunhan ne suojataan väärinkäytöltä asianmukaisilla suojaustoimilla.<sup>69</sup>

## Pseudonyymit tiedot

Henkilötiedot sisältävät tunnistetta, kuten nimen, syntymäajan, sukupuolen ja osoitteen. Henkilötiedot käsitellään pseudonyymeiksi siten, että tunnistet korvataan ns. salanimellä. Pseudonyymeissä henkilötiedoissa tunnistet on salattu. Tiedot voidaan käsitellä pseudonyymeiksi esimerkiksi ns. kryptaamalla henkilötietoja sisältävästä datasta tunnistetiedot.

Pseudonyymejä tietoja ei mainita erikseen sen enempää yleissopimuksen 108 kuin tietosuojadirektiivinkään oikeudellisissa määritelmissä. Yleissopimuksen 108 selitysmuistion 42 artiklassa kuitenkin todetaan, ettei nimeen yhdistettyjen tietojen säilyttämisen aikarajoja koskeva vaatimus tarkoita, että tiedot tulisi tietyn ajan kuluttua erottaa peruuttamattomasti sen henkilön nimestä, johon ne liittyvät, vaan ainoastaan, ettei tietoja pitäisi voida helposti yhdistää tunnisteesiin. Tämä voidaan saavuttaa tietojen pseudonyymisoinnilla. . Kukaan sellainen henkilö, jolla ei ole hallussaan salauksen avainta, ei voi ilman vaivaa tunnistaa pseudonyymeistä tiedoista tiettyjä henkilöitä Tiedot on kuitenkin kytketty tunnistettavissa olevaan henkilöön salanimen ja salauksen avaimen avulla, Niillejoilla on oikeus käyttää salauksen avainta, henkilöiden tunnistaminen on edelleen vaivatta mahdollista. . On huolehdittava erityisten suojaustoimien käyttöönotosta, joilla voidaan estää salauksen avaimien luvaton käyttö.

Silloin kun ei ole tarkoituksen mukaista pidättäytyä henkilötietojen käsittelystä, tiedon pseudonyymisointi on yksi tärkeimmistä keinoista, joilla voidaan saavuttaa kattavampi henkilötietojen suoja. Näin ollen pseudonyymisoinnin periaatteet ja vaikutukset on selitettävä yksityiskohtaisesti.

Esimerkki: Virke ”huhtikuun 3. päivänä 1967 syntynyt Charles Spencer on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tyttärtä” voidaan salanimetä esimerkiksi seuraavasti:

<sup>69</sup> *Ibid.*, 6 artiklan 1 kohdan e alakohta; ja yleissopimus 108, 5 artiklan e alakohta.

”C.S. 1967 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä”; tai

”324 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä”; tai

”YESz320l on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä”.

Näiden pseudonyymien tietojen käyttäjillä ei yleensä ole mahdollisuutta tunnistaa, että ”huhtikuun 3. päivänä 1967 syntynyt Charles Spencer” on ”324” tai ”YESz3201”. Pseudonyymit tiedot ovat näin ollen melko hyvin suojattu väärinkäytöltä.

Ensimmäinen esimerkkivirke on kuitenkin heikoiten suojattu. Jos virkettä ”C.S. 1967 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä” käytettäisiin pienessä kylässä, jossa Charles Spencer asuu, hänet voitaisiin helposti tunnistaa. Pseudonymisoinnissa käytetty menetelmä vaikuttaa tietosuojan kattavuuteen.

Henkilötietojen tunnisteiden salaamista käytetään monissa tilanteissa henkilöiden henkilöllisyyden salaamiseksi. Se on erityisen hyödyllistä silloin, kun rekisterinpitäjien on varmistettava, että ne käsittelevät samojen rekisteröityjen tietoja, mutta niiden ei tarvitse tietää rekisteröityjen todellista henkilöllisyyttä. Näin voi olla esimerkiksi silloin, kun tutkija tutkii taudin kehittymistä potilailla, joiden henkilöllisyys tiedetään vain sairaalassa, jossa heitä on hoidettu ja josta tutkija on saanut salanimetyt potilastiedot. Pseudonymisointi on näin ollen tärkeä työkalu yksityisyyttä suojaavan tekniikan varastossa. Se voi auttaa merkittävästi yksityisyyden suojan ennakoivassa toteuttamisessa. Tällä tarkoitetaan tietosuojan sisällyttämistä kehittyneisiin tiedonkäsittelyjärjestelmiin jo suunnitteluvaiheessa.

## 2.2. Tietojenkäsittely

### Keskeiset kohdat

- Termillä ”käsittely” viitataan pääasiallisesti automaattiseen käsittelyyn.
- EU-oikeudessa ”käsittelyllä” viitataan lisäksi jäsenmetyissä rekistereissä olevien tietojen manuaaliseen käsittelyyn.
- EN-oikeudessa ”käsittelyn” merkitystä voidaan laajentaa kansallisessa lainsäädännössä niin, että se kattaa manuaalisen käsittelyn.

Yleissopimuksessa 108 ja tietosuojadirektiivissä henkilötietojen suojaa käsitellään pääasiallisesti automaattisen tietojenkäsittelyn näkökulmasta.

**EN-oikeudessa** automaattisen käsittelyn määritelmässä on kuitenkin otettu huomioon, että automaattisten toimintojen välillä saattaa olla vaiheita, joissa henkilötietoja käsitellään manuaalisesti. Samaten **EU-oikeudessa** automaattinen tietojenkäsittely on määritelty henkilötietoihin kohdistetuiksi osittain tai kokonaan automatisoiduiksi toiminnoiksi.<sup>70</sup>

Esimerkki: Asiassa *Bodil Lindqvist*<sup>71</sup> EYTI totesi seuraavaa:

”sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumeronsa tai antamalla tietoja heidän työsuhteestaan ja harrastuksistaan, on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä.”

Henkilötietojen suojaa koskevat säännökset on ulotettava myös manuaaliseen henkilötietojen käsittelyyn.

**EU-oikeudessa** tietosuojaa ei ole mitenkään rajoitettu automaattiseen tietojenkäsittelyyn. Näin ollen EU-oikeudessa tietosuojaa sovelletaan manuaalisessa rekisterissä, eli jäsenneytyssä paperiarkistossa, olevien henkilötietojen käsittelyyn.<sup>72</sup> Tietosuoja on haluttu ulottaa näihin seuraavista syistä:

- paperiarkistot voidaan jäsentää niin, että tiedot löytyvät niistä helposti ja nopeasti; ja
- automaattista tietojenkäsittelyä varten lainsäädännössä asetettuja rajoituksia on helppo kiertää säilyttämällä henkilötiedot jäsenneytyissä paperiarkistoissa.<sup>73</sup>

**EN-oikeudessa** yleissopimuksella 108 säännellään pääasiallisesti automaattisissa tiedostoissa olevien henkilötietojen käsittelyä.<sup>74</sup> Yleissopimuksessa kuitenkin anne-

70 Yleissopimus 108, 2 artiklan c alakohta; ja tietosuojadirektiivi, 2 artiklan b alakohta ja 3 artiklan 1 kohta.

71 Asia C-101/01, *Bodil Lindqvist*, EYTI 6.11.2003, 27 kohta.

72 Tietosuojadirektiivi, 3 artiklan 1 kohta.

73 *Ibid.*, johdanto-osan 27 kappale.

74 Yleissopimus 108, 2 artiklan b alakohta.

taan lisäksi mahdollisuus ulottaa kansallisessa lainsäädännössä suoja manuaaliseen käsittelyyn. Monet yleissopimuksen 108 osapuolet ovat hyödyntäneet tätä mahdollisuutta ja antaneet tätä asiaa koskevan selityksen Euroopan neuvoston pääsihteerille.<sup>75</sup> Tällaisen selityksen mukaisesti tehtävän tietosuojan laajentamisen on katettava kaikki manuaalinen tietojenkäsittely, se ei voi rajoittua manuaalisten rekisterien käsittelyyn.<sup>76</sup>

Tietojenkäsittelyyn sisältyvien toimien luonteen osalta käsite on sekä **EU- että EN-oikeudessa** kattava: ”henkilötietojen käsittelyllä [tarkoitetaan] kaikenlaisia sellaisia toimintoja – –, joita kohdistetaan henkilötietoihin – – kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen sekä suojaaminen, poistaminen tai tuhoaminen”.<sup>77</sup> Käsittely kattaa myös toimet, joilla tieto siirretään yhden rekisterinpitäjän vastuulta toisen rekisterinpitäjän vastuulle.

Esimerkki: Työnantajat keräävät ja käsittelevät työntekijöitään koskevia tietoja, myös palkkaa koskevia tietoja. Tällaisen toiminnan oikeudellisena perusteena on työsopimus.

Työnantajien on toimitettava työntekijöidensä palkkatiedot veroviranomaisille. Tällainen tietojen luovuttaminen on yleissopimuksessa 108 ja direktiivissä tarkoitettua tietojenkäsittelyä. Tietojen luovuttamisen oikeudellinen peruste ei kuitenkaan ole työsopimus. Tarvitaan toinen oikeudellinen peruste niille käsittelytoimille, jotka johtavat palkkatietojen siirtoon työnantajalta veroviranomaisille. Tämä oikeudellinen peruste sisältyy yleensä kansalliseen velolainsäädäntöön. Ilman näitä säännöksiä, tietojen luovuttaminen olisi laitonta käsittelyä.

75 Ks. yleissopimuksen 108 3 artiklan 2 kohdan c alakohdan nojalla annetut selitykset.

76 Ks. yleissopimuksen 108 3 artiklan 2 kohdan sanamuoto.

77 Tietosuojadirektiivi, 2 artiklan b alakohta. Vastaavasti ks. myös yleissopimus 108, 2 artiklan c alakohta.



## 2.3. Henkilötietojen käyttäjät

### Keskeiset kohdat

- "Rekisterinpitäjä on taho, joka päättää käsitellä henkilötietoja omiin tarkoituksiinsa. Jos monta tahoja tekee yhdessä kyseisen päätöksen, voidaan heitä nimittää "yhteiseksi rekisterinpitäjäksi".
- "Henkilötietojen käsittelijä" on rekisterinpitäjistä oikeudellisesti erillinen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.
- Henkilötietojen käsittelijästä tulee rekisterinpitäjä, jos hän käyttää tietoja omiin tarkoituksiinsa rekisterinpitäjän ohjeiden vastaisesti.
- Jokainen, joka vastaanottaa tietoja rekisterinpitäjältä, on "vastaanottaja".
- "Sivullinen" on luonnollinen tai oikeushenkilö, joka ei toimi rekisterinpitäjän alaisuudessa (eikä ole itse rekisteröity).
- "Sivullinen vastaanottaja" on henkilö tai elin, joka on oikeudellisesti erillinen rekisterinpitäjistä, mutta vastaanottaa henkilötietoja rekisterinpitäjältä.

### 2.3.1. Rekisterinpitäjät ja henkilötietojen käsittelijät

Rekisterinpitäjänä tai henkilötietojen käsittelijänä olemisen tärkein seuraus on oikeudellinen vastuu tietosuojasäännöksissä asetettujen velvollisuuksien noudattamisesta. Siksi näitä tehtäviä voivat hoitaa vain tahot, jotka voidaan asettaa vastuuseen sovellettavan lain nojalla. Yksityissektorilla kyseisiä tehtäviä hoitaa yleensä luonnollinen tai oikeushenkilö; julkisella sektorilla se on yleensä viranomainen. Muut tahot, kuten laitokset tai toimielimet, joilla ei ole oikeushenkilöyttä, voivat toimia rekisterinpitäjinä tai henkilötietojen käsittelijöinä vain, jos asiasta on säädetty erikseen.

Esimerkki: Kun Sunshine-yhtiön markkinointiosasto suunnittelee tietojen käsittelemistä markkinatutkimusta varten, rekisterinpitäjäksi katsotaan Sunshine-yhtiö, ei sen markkinointiosasto. Markkinointiosasto ei voi olla rekisterinpitäjä, koska sillä ei ole erillistä oikeushenkilöyttä.

Yritysryhmien kohdalla emoyhtiö ja jokainen tytäryhtiö lasketaan erillisinä oikeushenkilöinä erillisiksi rekisterinpitäjiksi tai henkilötietojen käsittelijöiksi. Koska yritysryhmän jäsenet ovat oikeudellisesti erillisiä, niiden välinen tietojensiirto tarvitsee

oman oikeudellisen perusteen. Henkilötietojen siirtämiseen yritysryhmän oikeudellisesti erillisten yksiköiden välillä ei ole mitään erioikeutta.

Yksityishenkilöiden roolia on syytä käsitellä tässä yhteydessä. **EU-oikeudessa** tietosuojadirektiivin sääntöjä ei sovelleta yksityishenkilöihin, kun he käsittelevät muita ihmisiä koskevia tietoja yksinomaan henkilökohtaisessa tai kotitalouteensa liittyvässä toiminnassa; heitä ei katsota rekisterinpitäjiksi.<sup>78</sup>

Oikeuskäytännössä on kuitenkin katsottu, että silloin kun yksityishenkilö julkaisee muiden henkilöiden tietoja avoimessa verkossa (internetissä), ei tämä täytä yksityisen käytön poikkeuksen edellytyksiä ja tietosuojasäännöksiä on sovellettava.

Esimerkki: EYTI totesi asiassa *Bodil Lindqvist*<sup>79</sup> seuraavaa:

”Sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin –, on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä.”<sup>80</sup>

Tällainen henkilötietojen käsittely ei ole yksinomaan henkilökohtaista tai kotitaloutta koskevaa toimintaa, joka on jätetty tietosuojadirektiivin soveltamisalan ulkopuolelle, sillä tätä poikkeusta on ”tulkittava niin, että se kohdistuu ainoastaan toimintaan, joka kuuluu yksityisen henkilön yksityis- tai perhe-elämään, mistä ei ilmeisestikään ole kysymys sellaisessa henkilötietojen käsittelyssä, jossa tiedot julkaistaan internet-sivulla siten, että ne saatetaan ennalta määrittelemättömän henkilöryhmän saataville”.<sup>81</sup>

## Rekisterinpitäjä

**EU-oikeudessa** rekisterinpitäjäksi määritellään taho, joka ”yksin tai yhdessä toisten kanssa, määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot”.<sup>82</sup> Rekisterinpitäjä päättää miksi ja miten tietoja käsitellään. **EN-oikeudessa** ”rekisterinpitäjän”

78 Tietosuojadirektiivi, johdanto-osan 12 kohta ja 3 artiklan 2 kohdan viimeinen luettelukohta.

79 Asia C-101/01, *Bodil Lindqvist*, EYTI 6.11.2003.

80 *Ibid.*, 27 kohta.

81 *Ibid.*, 47 kohta.

82 Tietosuojadirektiivi, 2 artiklan d alakohta.

määritelmässä mainitaan lisäksi, että rekisterinpitäjä päättää minkä tyyppisiä henkilötietoja säilytetään.<sup>83</sup>

Yleissopimuksessa 108 annetussa rekisterinpitäjän määritelmässä tuodaan esiin vielä yksi näkökohta, jota on syytä tarkastella. Määritelmässä viitataan kysymyksen siitä, kuka voi lainmukaisesti käsitellä tiettyjä henkilötietoja tiettyyn tarkoitukseen. Kuitenkin, kun laittomia käsittelytoimia väitetään tapahtuneen ja vastuussa oleva rekisterinpitäjä on löydettävä, rekisterinpitäjäksi katsotaan se henkilö tai yksikkö, kuten yritys tai viranomainen, joka on tehnyt päätöksen tietojen käsittelemisestä, riippumatta siitä, oliko sillä lainmukaista perustetta käsitellä tietoja vai ei.<sup>84</sup> Esimerkiksi tietojen poistamista koskeva pyyntö onkin aina esitettävä ”tosiasialliselle” rekisterinpitäjälle.

## Yhteinen rekisterinpitäjä

Tietosuojadirektiivissä esitetyn rekisterinpitäjän määritelmän mukaan useampi oikeudellisesti erillinen yksikkö voi toimia yhdessä tai yhteistyössä muiden kanssa rekisterinpitäjänä. Tällöin ne päättävät yhdessä käsitellä tietoja yhteiseen tarkoitukseen.<sup>85</sup> Tämä on kuitenkin oikeudellisesti mahdollista vain, kun tietojen yhteiselle käsittelylle yhteiseen tarkoitukseen on olemassa erityinen oikeudellinen peruste.

Esimerkki: Usean luottolaitoksen yhteisesti ylläpitämä tietokanta asiakkaista, joilla on maksuhäiriöitä, on tavallinen esimerkki yhteisestä rekisterinpidosta. Kun henkilö hakee luottoa pankista, joka on yksi yhteisistä rekisterinpitäjistä, pankki tarkistaa tietokannasta hakijan luottokelpoisuuden tietoon perustuvan päätöksen tekemiseksi.

Säännöksistä ei käy yksiselitteisesti ilmi, onko yhteistä rekisterinpitoa varten yhteisen tarkoituksen oltava kaikille sama vai riittääkö, että tarkoitukset ovat osittain päällekkäisiä. Euroopan tasolla ei ole vielä asiaa koskevaa oikeuskäytäntöä eikä selkeyttä seurauksista vastuun osalta. Tietosuojatyöryhmä kannattaa yhteisen rekisterinpidon laajaa tulkintaa, joka mahdollistaisi tietyn joustavuuden yhä

83 Yleissopimus 108, 2 artiklan d alakohta.

84 Ks. myös tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, 16. helmikuuta 2010, s. 15.

85 Tietosuojadirektiivi, 2 artiklan d alakohta.

monimuotoisemman tietojen käsittelyn kattamiseksi.<sup>86</sup> Tietosuojatyöryhmän kantaa kuvastaa tapaus, jossa Society for Worldwide Interbank Financial Telecommunication (SWIFT) oli osallisena.

Esimerkki: Niin kutsutussa SWIFT-asiassa eurooppalaiset pankit käyttivät SWIFTiä, alun perin tietojen käsittelijänä, tietojen siirtämiseen pankkitapahtumien yhteydessä. SWIFT paljasti nämä pankkitapahtumia koskevat tiedot, joita säilytettiin Yhdysvalloissa sijaitsevassa tietojenkäsittelykeskuksessa, Yhdysvaltojen valtiovarainministeriölle ilman, että sen asiakkaina olleet eurooppalaiset pankit olisivat nimenomaisesti määränneet sen tekemään niin. Tietosuojatyöryhmä arvioi tilanteen lainmukaisuutta ja tuli siihen johtopäätökseen, että SWIFTin kanssa sopimuksen tehneet eurooppalaiset pankit ja SWIFT olivat yhteisiä rekisterinpitäjiä, jotka olivat vastuussa eurooppalaisille asiakkaille näiden tietojen paljastamisesta Yhdysvaltojen viranomaisille.<sup>87</sup> Päättämällä paljastaa tiedot SWIFT oli – lainvastaisesti – asettunut rekisterinpitäjän asemaan; pankit olivat selkeästi laiminlyöneet velvollisuuttaan valvoa tietojensa käsittelijää, eikä niitä siksi voitu täydellisesti vapauttaa vastuustaan rekisterinpitäjänä. Tilanteesta oli siis kyse yhteisestä rekisterinpidosta.

## Henkilötietojen käsittelijä

**EU-oikeudessa** henkilötietojen käsittelijä määritellään tahoksi, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.<sup>88</sup> Henkilötietojen käsittelijän toiminta saattaa rajoittua tarkoin määriteltyyn tehtävään tai tilanteeseen tai se voi olla melko yleistä ja kattavaa.

**EN-oikeudessa** henkilötietojen käsittelijällä tarkoitetaan samaa asiaa kuin EU-oikeudessa.

Sen lisäksi, että henkilötietojen käsittelijät käsittelevät tietoja muiden lukuun, ne ovat itse rekisterinpitäjiä, kun ne käsittelevät tietoja omiin tarkoituksiinsa, esimerkiksi omien työntekijöidensä, myyntinsä ja tiliensä hallinnoinnissa.

86 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16. helmikuuta 2010, s. 19.

87 Tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22. marraskuuta 2006.

88 Tietosuojadirektiivi, 2 artiklan e alakohta.

Esimerkki: Everready-yhtiö on erikoistunut tietojenkäsittelyyn muiden yritysten henkilöstöhallinnon hoitamisen yhteydessä. Tässä tehtävässä Everready on henkilötietojen käsittelijä.

Kun Everready käsittelee omien työntekijöidensä henkilötietoja, se on kuitenkin rekisterinpitäjä niissä tietojenkäsittelytoimissa, jotka se toteuttaa täyttääkseen velvollisuutensa työnantajana.

## Rekisterinpitäjän ja henkilötietojen käsittelijän välinen suhde

Kuten olemme todenneet, rekisterinpitäjä on se, joka määrittelee käsittelyn tarkoitukset ja keinot.

Esimerkki: Sunshine-yhtiön johtaja päättää, että markkina-analyysihin erikoistuneen Moonlight-yhtiön pitäisi tehdä markkina-analyysi Sunshinen asiakastiedosta. Vaikka Moonlight saa näin tehtäväksi määritellä käsittelyn keinot, Sunshine säilyy rekisterinpitäjänä ja Moonlight on vain henkilötietojen käsittelijä, sillä sopimuksen mukaan Moonlight saa käyttää Sunshinen asiakastietoja yksinomaan Sunshinen määrittelemiin tarkoituksiin.

Vaikka henkilötietojen käsittelijälle annettaisiinkin valtuudet määritellä käsittelyn keinot, rekisterinpitäjän on voitava vaikuttaa henkilötietojen käsittelijän päätöksiin käsittelyn keinoista. Kokonaisvastuu henkilötietojen käsittelyn lainmukaisuudesta säilyy rekisterinpitäjällä, jonka on valvottava henkilötietojen käsittelijöitä ja varmistettava, että niiden päätökset noudattavat tietosuojalainsäädäntöä. Sopimuksen, joka estäisi rekisterinpitäjää puuttumasta henkilötietojen käsittelijän päätöksiin, katsottaisiin näin ollen todennäköisesti johtavan yhteiseen rekisterinpitoon, jossa molemmilla osapuolilla olisi rekisterinpitäjän oikeudellinen vastuu.

Lisäksi, jos henkilötietojen käsittelijä ei noudattaisi rajoituksia, jotka rekisterinpitäjä on asettanut tietojen käsittelylle, henkilötietojen käsittelijästä tulisi rekisterinpitäjä ainakin siinä määrin, kuin se olisi rikkonut rekisterinpitäjän ohjeita. Henkilötietojen käsittelijää pidettäisiin todennäköisesti laittomasti toimivana rekisterinpitäjänä. Alkuperäisen rekisterinpitäjän pitäisi vuorostaan selittää, miten henkilötietojen käsittelijä onnistui ylittämään valtuutensa. Tietosuojatyöryhmä vaikuttaa tosiaan lähtevän siitä, että tällaisissa tapauksissa on kyse yhteisestä rekisterinpidosta, koska

näin turvataan parhaiten rekisteröityjen edut.<sup>89</sup> Yhteisen rekisterinpidon tärkeänä seurauksena tulisi olla yhteisvastuu vahingoista siten, että rekisteröidyillä olisi käytössään mahdollisimman laajat oikeussuojakeinot.

Vastuun jakautuminen saattaa olla epäselvää myös silloin, kun rekisterinpitäjä on pieni yritys ja henkilötietojen käsittelijä on suuri yhtymä, jolla on valta sanella palvelujensa ehdot. Työsuojelutyöryhmä kuitenkin katsoo, ettei tällaisessa tilanteessa tulisi madaltaa vastuun kynnyistä taloudellisen eriarvoisuuden perusteella, vaan rekisterinpitäjän käsite tulisi ymmärtää edelleen samalla tavalla.<sup>90</sup>

Selkeyden ja avoimuuden vuoksi rekisterinpitäjän ja henkilötietojen käsittelijän välisen suhteen yksityiskohdista tulisi sopia kirjallisesti.<sup>91</sup> Tällaisen sopimuksen puuttuminen rikkoo rekisterinpitäjän velvollisuutta pystyä osoittamaan asiakirjojen avulla osapuolten vastuut, ja se voi johtaa seuraamuksiin.<sup>92</sup>

Henkilötietojen käsittelijät saattavat haluta delegoida joitakin tietojenkäsittelytehtäviä edelleen muille käsittelijöille. Se on lainsäädännön näkökulmasta mahdollista ja riippuu täysin siitä, mitä rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa määrätään muun muassa siitä, onko rekisterinpitäjältä pyydettävä joka kerta erikseen lupa vai riittääkö, että sille tiedotetaan asiasta.

**EN-oikeudessa** rekisterinpitäjän ja henkilötietojen käsittelijän käsitteitä tulkitaan, kuten edellä selitettiin, täydessä laajuudessaan, kuten yleissopimuksen 108 mukaisesti annetut suositukset osoittavat.<sup>93</sup>

## 2.3.2. Vastaanottajat ja sivulliset

Merkittävin ero näiden kahden tietosuojadirektiivissä määritellyn henkilö- tai yksiköryhmän välillä liittyy niiden suhteeseen rekisterinpitäjään ja siten niiden mahdollisuuden saada rekisterinpitäjän hallussa olevia henkilötietoja.

89 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16. Helmikuuta 2010, s. 25; ja tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22. marraskuuta 2006.

90 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16. helmikuuta 2010, s. 26.

91 Tietosuojadirektiivi, 17 artiklan 3 ja 4 kohta.

92 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16. helmikuuta 2010, s. 27.

93 Ks. esim. profiilontia koskeva suositus, 1 artikla.

”Sivullinen” on rekisterinpitäjistä oikeudellisesti erillinen taho. Näin ollen tietojen luovuttaminen sivulliselle vaatii aina erityisen oikeudellisen perusteen. Tietosuojadirektiivin 2 artiklan f alakohdan mukaan sivullisella tarkoitetaan ”luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää”. Toisin sanoen henkilö, joka työskentelee rekisterinpitäjistä oikeudellisesti erillisessä organisaatiossa – vaikka se kuuluisi samaan yhtiöön tai samalle omistajayhtiölle – on sivullinen (tai työskentelee sivullisella). Sen sijaan asiakkaan pankin sivukonttorit, jotka käsittelevät asiakkaan tilejä pääkonttorinsa suorassa alaisuudessa, eivät ole sivullisia.<sup>94</sup>

”Vastaanottaja” on laajempi käsite kuin ”sivullinen”. Tietosuojadirektiivin 2 artiklan g alakohdan mukaan vastaanottajalla tarkoitetaan ”luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, jolle tietoja luovutetaan, oli kyseessä sivullinen tai ei”. Vastaanottaja voi olla taho, joka ei kuulu rekisterinpitäjän eikä henkilötietojen käsittelijän organisaatioon – silloin kyseessä on sivullinen –, tai taho, joka kuuluu rekisterinpitäjän tai henkilötietojen käsittelijän organisaatioon, kuten työntekijä tai toinen saman yrityksen tai viranomaisen alainen osasto.

Vastaanottajien ja sivullisten erottaminen toisistaan on tärkeää vain arvioitaessa henkilötietojen luovutuksen laillisuuden edellytyksiä. Rekisterinpitäjän tai henkilötietojen käsittelijän työntekijän ei tarvitse täyttää muita oikeudellisia vaatimuksia voidakseen olla henkilötietojen vastaanottaja, jos hän osallistuu rekisterinpitäjän tai henkilötietojen käsittelijän suorittamiin käsittelytoimiin. Sen sijaan sivullinen, joka on oikeudellisesti erillinen rekisterinpitäjistä tai henkilötietojen käsittelijästä, ei saa käyttää henkilötietojen käsittelijän käsittelemiä henkilötietoja ilman, että tapausta varten on erityinen oikeudellinen peruste. Sivulliset vastaanottajat tarvitsevat näin ollen aina oikeudellisen perusteen voidakseen laillisesti vastaanottaa henkilötietoja.

Esimerkki: Henkilötietojen käsittelijän työntekijä, joka käyttää henkilötietoja niiden tehtävien suorittamiseen, jotka työnantaja on hänelle osoittanut, on henkilötietojen vastaanottaja muttei sivullinen, sillä hän käyttää henkilötietoja henkilötietojen käsittelijän nimissä ja alaisuudessa.

Jos sama työntekijä kuitenkin päättäisi käyttää henkilötietoja, jotka hänen on mahdollista saada henkilötietojen käsittelijän työntekijänä, omiin tarkoituksiinsa

94 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16. helmikuuta 2010, s. 31.

ja myydä niitä toiselle yritykselle, työntekijä toimisi sivullisena. Hän ei enää noudattaisi henkilötietojen käsittelijän (työnantajan) määräyksiä. Sivullisena työntekijällä pitäisi olla oikeudellinen peruste henkilötietojen keräämiselle ja myymiselle. Tässä esimerkkitapauksessa työntekijällä ei ole tarvittavaa oikeudellista perustetta, joten hänen toimintansa on lainvastaista.

## 2.4. Suostumus

### Keskeiset kohdat

- Henkilötietojen käsittelyn oikeudellisena perusteena suostumuksen on oltava vapaaehtoinen, tietoinen ja yksilöity.
- Suostumuksen on oltava yksiselitteinen. Suostumus voidaan antaa nimenomaisesti tai implisiittisesti toimimalla tavalla, joka ei jätä mitään epäilystä siitä, että rekisteröity suostuu henkilötietojensa käsittelyyn.
- Arkaluonteisten tietojen käsitteleminen suostumuksen nojalla edellyttää nimenomaista suostumusta.
- Suostumuksen voi perua milloin tahansa.

Suostumuksella tarkoitetaan ”kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua”.<sup>95</sup> Se on usein laillisen tietojenkäsittelyn oikeudellinen peruste (ks. 4.1 kohta).

### 2.4.1. Pätevän suostumuksen edellytykset

**EU-oikeudessa** asetetaan kolme edellytystä sille, että suostumusta voidaan pitää pätevänä. Niillä pyritään takaamaan, että rekisteröidyt ovat todella tarkoittaneet suostua henkilötietojensa käsittelyyn:

- rekisteröityyn ei ole saanut kohdistua mitään painostusta, kun hän on antanut suostumuksensa;
- rekisteröityä on pitänyt asianmukaisesti informoida siitä, mihin hän suostuu ja minkälaiset seuraamukset suostumuksella on; ja
- suostumuksen kohteen on oltava riittävän konkreettinen

<sup>95</sup> Tietosuojadirektiivi, 2 artiklan h alakohta.



Vain jos kaikki nämä vaatimukset täyttyvät, suostumusta voidaan pitää pätevänä tietosuojasäännöksissä tarkoitetulla tavalla.

Yleissopimuksessa 108 ei ole määritelty suostumusta, vaan asia on jätetty kansallisen lainsäädännön piiriin. **EN-oikeudessa** pätevän suostumuksen edellytykset kuitenkin vastaavat edellä esitettyjä, sikäli kuin niitä on käsitelty yleissopimuksen 108 nojalla annetuissa suosituksissa.<sup>96</sup> Suostumusta koskevat Euroopan siviilioikeudessa samat vaatimukset kuin pätevää tahdonilmaisua.

Muita siviilioikeuden mukaisia pätevän suostumuksen edellytyksiä, kuten oikeuskelpoisuutta, sovelletaan perustavanlaatuisina oikeudellisina ennakkotedellytyksinä luonnollisesti myös tietosuojan alalla. Oikeustoimikelvottoman henkilön antama suostumus on mitätön, eikä tällaisen henkilön henkilötietojen käsittelylle ole oikeudellista perustetta.

Suostumus voi olla nimenomainen<sup>97</sup> tai implisiittinen. Näistä ensimmäinen ei jätä mitään epäselvyyttä rekisteröidyn aikeista ja se voidaan antaa suullisesti tai kirjallisesti; jälkimmäinen päätellään olosuhteista. Suostumus on aina annettava yksiselitteisesti.<sup>98</sup> Tämä tarkoittaa, ettei saa jäädä epäselvyyttä siitä, onko rekisteröity suostunut tietojensa käsittelyyn. Esimerkiksi suostumuksen päättelemisen toiminnan puutteesta ei ole yksiselitteisellä tavalla annettu suostumus. Kun käsiteltävät henkilötiedot ovat arkaluonteisia, suostumuksen on ehdottomasti oltava nimenomainen ja yksiselitteinen.

## Vapaaehtoinen suostumus

Vapaaehtoinen suostumus on pätevä, vain jos ”rekisteröity pystyy tekemään aidon valinnan ilman pelottelun, harhaanjohtamisen tai pakottamisen riskiä ja ilman, että hänelle aiheutuu merkittävää haittaa suostumuksen epämisestä”.<sup>99</sup>

Esimerkki: Monilla lentoasemilla matkustajien on kuljettava henkilöskannerin läpi päästäkseen lähtöporttialueella.<sup>100</sup> Koska matkustajien henkilötietoja

96 Ks. esim. yleissopimus 108, tilastotietoja koskeva suositus, 6 kohta.

97 Tietosuojadirektiivi, 8 artiklan 2 kohta.

98 *Ibid.*, 7 artiklan a alakohta ja 26 artiklan 1 kohta.

99 Ks. myös tietosuojatyöryhmä (2011), *lausunto 15/2011 suostumuksen määritelmästä*, WP 187, Bryssel, 13. heinäkuuta 2011, s. 12.

100 Tämä esimerkki on otettu edellä mainitusta asiakirjasta, s. 15.

käsitellään skannauksen aikana, käsittelyllä on oltava jokin tietosuojadirektiivin 7 artiklassa esitetty oikeudellinen peruste (ks. 4.1.1 kohta). Henkilöskannerien läpi kulkeminen esitetään toisinaan matkustajille vaihtoehtona, mikä tarkoittaa, että heidän suostumuksena oikeuttaisi käsittelyn. Matkustajat saattavat kuitenkin pelätä, että skannauksesta kieltäytyminen herättäisi epäluuloa tai johtaisi ylimääräisiin tarkastuksiin kuten ruumiintarkastukseen. Monet matkustajat suostuvat skannaukseen, koska siten he välttyvät mahdollisilta hankaluuksilta tai viivytyksiltä. Tällainen suostumus ei oleltavasti ole riittävän vapaaehtoinen.

Näin ollen kunnollisena oikeudellisena perusteena voi toimia vain tietosuojadirektiivin 7 artiklan e kohtaan perustuva lainsäätäjän säädös, joka velvoittaa matkustajat tekemään yhteistyötä pakottavan yleisen edun nimissä. Lainsäädännössä voidaan antaa mahdollisuus valita skannauksen ja manuaalisen tarkastuksen välillä, mutta ainoastaan rajavalvonnan ylimääräisenä toimenpiteenä, jota voidaan tarvita erityisissä olosuhteissa. Näin Euroopan komissio säätöi kahdessa turvaskannereista vuonna 2011 antamassaan asetuksessa.<sup>101</sup>

Suostumuksen vapaaehtoisuus voi olla uhattuna myös suhteessa, jossa rekisterinpitäjän ja suostumuksen antavan rekisteröidyn välillä vallitsee merkittävä taloudellinen tai muu epätasapaino.<sup>102</sup>

Esimerkki: Suuri yritys haluaa luoda yksinomaan yrityksen sisäisen viestinnän parantamiseksi hakemiston, jossa on jokaisen työntekijän nimi, asema yrityksessä ja työosoite. Henkilöstöpäällikkö ehdottaa, että hakemistoon lisättäisiin esimerkiksi jokaisen työntekijän valokuva helpottamaan työtovereiden tunnistamista kokouksissa. Työntekijöiden edustajat vaativat, että tämä voitaisiin tehdä vain, jos työntekijä suostuu siihen.

101 Komission asetus (EU) N:o 1141/2011, annettu 10 päivänä marraskuuta 2011, siviili-ilmailun turvaamista koskevien yhteisten perusvaatimusten täydentämisestä annetun asetuksen (EY) N:o 272/2009 muuttamisesta turvaskannereiden käytön osalta EU:n lentoasemilla, EUVL 2011 L 293, ja komission täytäntöönpanoasetus (EU) N:o 1147/2011, annettu 11 päivänä marraskuuta 2011, yksityiskohtaisista toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi annetun asetuksen (EU) N:o 185/2010 muuttamisesta turvaskannereiden käytön osalta EU:n lentoasemilla, EUVL 2011 L 294.

102 Ks. myös tietosuojatyöryhmä (2001), *lausunto 8/2001 henkilötietojen käsittelystä työelämässä*, WP 48, Bryssel, 13. syyskuuta 2001; ja tietosuojatyöryhmä (2005), *valmisteluasiakirja 24 päivänä lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25. marraskuuta 2005.

Tässä tilanteessa työntekijän suostumusta tulisi pitää hakemistossa olevan valokuvan käsittelyn oikeudellisena perusteena, koska on selvää, ettei valokuvan julkaisemisella hakemistolla ole itsessään kielteisiä vaikutuksia, ja lisäksi voidaan olettaa, ettei työntekijälle aiheutuisi työnantajan taholta kielteisiä seurauksia, jos hän ei suostuisi valokuvansa julkaisemiseen hakemistossa.

Suostumus voi olla lainmukainen henkilötietojen käsittelyn peruste myös tilanteissa, jossa suostumuksen antamatta jättämisestä aiheutuisi kielteisiä seurauksia. Esimerkiksi vaikka valintamyymälän kanta-asiakaskortista kieltäytyminen johtaisi siihen, ettei henkilö saa alennusta tietyistä tuotteista, suostumus on pätevä oikeudellinen peruste niiden asiakkaiden henkilötietojen käsittelylle, jotka ovat suostuneet hankkimaan kortin. Yrityksen ja asiakkaan välillä ei ole alistussuhdetta ja suostumuksen epäämisen seuraukset eivät ole niin vakavia, ettei rekisteröidyllä olisi vapautta valita.

Toisaalta, jos esimerkiksi välttämättömyyshyödykkeitä voi saada vain ja ainoastaan paljastamalla tietyt henkilötiedot sivullisille, rekisteröidyn suostumusta henkilötietojen käsittelyyn ei yleensä voida pitää vapaana päätöksenä, eikä se siten ole pätevä tietosuojasäännösten näkökulmasta.

Esimerkki: Matkustajien lentoyhtiölle antamaa suostumusta matkustajarekisterin tietojen, eli matkustajien henkilöllisyyttä, ruokailutottumuksia tai terveysongelmia koskevien tietojen, luovuttamiseen tietyn vieraan maan maahanmuuttoviranomaisille ei voida pitää tietosuojaoikeuden mukaan pätevänä suostumuksena, sillä matkustajilla ei ole vapautta valita, jos he haluavat vierailulla kyseisessä maassa. Jos nämä tiedot halutaan siirtää laillisesti, tarvitaan muu oikeudellinen peruste kuin suostumus – todennäköisesti erityinen laki.

## Tietoinen suostumus

Rekisteröidyllä on oltava riittävästi tietoa ennen päätöksen tekemistä. Se, onko tietoa annettu riittävästi, on ratkaistava tapauskohtaisesti. Yleensä tietoinen suostumus edellyttää tarkkaa ja helposti ymmärrettävää kuvausta asiasta, johon suostumus tarvitaan, ja selitystä suostumuksen tai sen epäämisen seurauksista. Tiedon antamisessa on käytettävä kieltä, jota ennakoitu vastaanottaja ymmärtää.

Lisäksi tiedon on oltava helposti rekisteröidyn saatavilla. Tiedon saatavuus ja näkyvyys ovat tärkeitä seikkoja. Sähköisessä ympäristössä tiedot voidaan esittää

kerrostetusti siten, että rekisteröity pääsee lyhyestä tiedotteesta tutustumaan yksityiskohtaisempiin tietoihin.

## Yksilöity suostumus

Jotta suostumus olisi pätevä, sen on oltava myös yksilöity. Tämä liittyy tiiviisti suostumuksen kohteesta annetun tiedon laatuun. Tässä on myös otettava huomioon tyypillisen rekisteröidyn kohtuulliset odotukset. Rekisteröidyltä on pyydettävä suostumus uudelleen, jos käsittelytoimia lisätään tai muutetaan tavalla, jota alkuperäisen suostumuksen antamisen yhteydessä ei voinut kohtuullisesti ennakoita.

Esimerkki: Asiassa *Deutsche Telekom AG*<sup>103</sup> EUTI tarkasteli kysymystä siitä, tarvitsiko televerkko-operaattori, jonka oli luovutettava tilaajien henkilötietoja *sähköisen viestinnän tietosuojadirektiivin*<sup>104</sup> 12 artiklan nojalla, rekisteröidyiltä uuden suostumuksen, sillä vastaanottajia ei ollut nimetty, kun alkuperäinen suostumus oli annettu.

EUTI katsoi, että kyseisen artiklan nojalla tietojen luovuttamista varten ei tarvinnut uutta suostumusta, koska rekisteröidyillä oli säännöksen mukaan mahdollisuus suostua ainoastaan käsittelyn tarkoitukseen, joka oli heidän tietojensa julkaiseminen, eivätkä he voineet valita, missä hakemistoissa tiedot julkaistaisiin.

Tuomioistuimien korosti, että ”sähköisen viestinnän tietosuojadirektiivin 12 artiklan kontekstuaalisesta ja systemaattisesta tulkinnasta seuraa, että kyseisen artiklan 2 kohdassa tarkoitettu suostumus koskee tarkoitusta, jota varten henkilötiedot julkaistaan julkisessa luettelossa, eikä tiettyä luettelon tarjoajaa”.<sup>105</sup> Lisäksi ”juuri henkilötietojen julkaiseminen luettelossa, jolla on erityinen tarkoitus, voi osoittautua tilaajalle haitalliseksi”,<sup>106</sup> eikä olennaista ole, se, kuka tiedot julkaisee.

103 Asia C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, EUTI 5.5.2011, 53 ja 54 kohta.

104 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (*sähköisen viestinnän tietosuojadirektiivi*), EYVL 2002 L 201.

105 Asia C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, EUTI 5.5.2011, ks. erityisesti 61 kohta.

106 *Ibid.*, ks. erityisesti 62 kohta.

## 2.4.2. Oikeus perua suostumus milloin tahansa

Tietosuojadirektiivissä ei mainita yleistä oikeutta perua suostumus milloin tahansa. Yleisesti kuitenkin oletetaan, että tällainen oikeus on olemassa ja että rekisteröidyn on voitava käyttää sitä oman harkintansa mukaan. Perumiselle ei saisi vaatia perusteluja eikä sillä saisi olla muita kielteisiä seurauksia kuin niiden etujen päättymisen, joihin aiempi tietojen käytön hyväksyminen on oikeuttanut.

Esimerkki: Asiakas suostuu vastaanottamaan mainospostia osoitteeseen, jonka hän antaa rekisterinpitäjälle. Jos asiakas peruu suostumuksensa, rekisterinpitäjän on välittömästi lopetettava mainospostin lähettäminen. Asiakkaalle ei saa määrätä mitään rangaistusta kuten sakkoa.

Jos asiakas sai viiden prosentin alennuksen hotellihuoneen hinnasta vastineeksi siitä, että hän suostui tietojensa käyttämiseen mainospostia varten, suostumuksen peruminen myöhemmässä vaiheessa ei saa johtaa siihen, että häneltä peritään takaisin kyseiset alennukset.



# 3

## Euroopan tietosuojaoikeuden pääperiaatteet



EU	Katetut aiheet	EN
Tietosuojadirektiivi, 6 artiklan 1 kohdan a ja b alakohta Asia C-524/01, <i>Huber v. Saksa</i> , EYTI 16.12.2008 Yhdistetyt asiat C-92/09 ja C-93/09, <i>Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen</i> , EUTI 9.11.2010	Laillisen käsittelyn periaate	Yleissopimus 108, 5 artiklan a ja b alakohta Asia nro 28341/95, <i>Rotaru v. Romania</i> [suuri jaosto], EIT 4.5.2000 Asia nro 47114/99, <i>Taylor-Sabori v. Yhdistynyt kuningaskunta</i> , EIT 22.10.2002 Asia nro 44647/98, <i>Peck v. Yhdistynyt kuningaskunta</i> , EIT 28.1.2003 Asia nro 16188/07, <i>Khelili v. Sveitsi</i> , EIT 18.10.2011 Asia nro 9248/81, <i>Leander v. Ruotsi</i> , EIT 26.3.1987
Tietosuojadirektiivi, 6 artiklan 1 kohdan b alakohta	Käsittelyn tarkoituksen määrittämisen ja käyttötarkoituksidonnaisuuden periaate	Yleissopimus 108, 5 artiklan b alakohta
	Tietojen laatu koskevat periaatteet:	
Tietosuojadirektiivi, 6 artiklan 1 kohdan c alakohta	Tietojen olennaisuus	Yleissopimus 108, 5 artiklan c alakohta
Tietosuojadirektiivi, 6 artiklan 1 kohdan d alakohta	Tietojen täsmällisyys	Yleissopimus 108, 5 artiklan d alakohta
Tietosuojadirektiivi, 6 artiklan 1 kohdan e alakohta	Tietojen rajoitettu säilyttäminen	Yleissopimus 108, 5 artiklan e alakohta

EU	Katetut aiheet	EN
Tietosuojadirektiivi, 6 artiklan 1 kohdan a alakohta	Tieteellistä tutkimusta ja tilastointia koskeva poikkeus	Yleissopimus 108, 9 artiklan 3 kohta
Tietosuojadirektiivi, 6 artiklan 1 kohdan a alakohta	Asianmukaisen käsittelyn periaate	Yleissopimus 108, 5 artiklan a alakohta Asia nro 21737/03, <i>Haralambie v. Romania</i> , EIT 27.10.2009 Asia nro 32881/04, <i>K.H. ym. v. Slovakia</i> , EIT 6.11.2009
Tietosuojadirektiivi, 6 artiklan 2 kohta	Vastuullisuuden periaate	

Yleissopimuksen 108 5 artiklassa esitettyihin periaatteisiin kiteytyy Euroopan tietosuoja-oikeuden ydinolemus. Samat periaatteet esitetään tietosuojadirektiivin 6 artiklassa lähtökohtana direktiivin seuraavissa artikloissa säädetyille yksityiskohteisemmille säännöksille. EN:n ja EU:n tietosuojalainsäädäntöä laadittaessa ja tulkittaessa on aina noudatettava näitä periaatteita. Näihin pääperiaatteisiin voidaan säätää poikkeuksia ja rajoituksia kansallisella tasolla.<sup>107</sup> Poikkeuksista ja rajoituksista on säädettävä laissa, niillä on oltava laillinen tarkoitus ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa. Kaikkien kolmen ehdon on täytyttävä.

## 3.1. Laillisen käsittelyn periaate

### Keskeiset kohdat

- Laillisen käsittelyn periaatteen selittämiseksi on viitattava perusoikeuskirjan 52 artiklassa tietosuoja koskevan oikeuden lailliselle rajoittamiselle määriteltyihin edellytyksiin ja EIS:n 8 artiklan 2 kohdassa oikeuteen puuttumiselle asetettuihin vaatimuksiin.
- Niiden nojalla henkilötietojen käsittely on laillista vain, jos
  - siitä on säädetty lailla; ja
  - sillä on laillinen tarkoitus; ja
  - se on välttämätöntä demokraattisessa yhteiskunnassa laillisen tarkoituksen saavuttamiseksi.

<sup>107</sup> Yleissopimus 108, 9 artiklan 2 kohta; tietosuojadirektiivi, 13 artikla.



**EU:n ja EN:n tietosuojaoikeudessa** laillisen käsittelyn periaate on ensimmäisenä mainittu periaate; se on esitetty lähes samoilla käsitteillä yleissopimuksen 5 artiklassa ja tietosuojadirektiivin 6 artiklassa.

Kummassakaan näistä kohdista ei määritellä, mitä ”laillisella käsittelyllä” tarkoitetaan. Tämän oikeudellisen käsitteen ymmärtämiseksi on viitattava EIS:ssa mainittuun oikeutettuun puuttumiseen sellaisena kuin EIT on sitä tulkinut, ja perusoikeuskirjan 52 artiklassa tietosuojaa koskevan oikeuden lailliselle rajoittamiselle määriteltyihin edellytyksiin.

### 3.1.1. Edellytykset EIS:n mukaiselle oikeutetulle puuttumiselle oikeuden käyttämiseen

Henkilötietojen käsittely voi johtaa puuttumiseen rekisteröidyn oikeuteen nauttia yksityiselämäänsä kohdistuvaa kunnioitusta. Oikeus nauttia yksityiselämäänsä kohdistuvaa kunnioitusta ei kuitenkaan ole ehdoton oikeus, vaan se on saatettava tasapainoon muiden oikeutettujen etujen kanssa, niin muiden henkilöiden etujen (yksityisten etujen) kuin koko yhteiskunnan etujen (julkisten etujen) kanssa.

Valtion puuttuminen oikeuteen on perusteltua jäljempänä esitetyin edellytyksin.

#### Siitä säädetään lailla

EIT:n oikeuskäytännön nojalla oikeuteen puuttuminen on lainmukaista, jos se perustuu kansalliseen lakiin, joka täyttää tietyt vaatimukset. Lain on oltava asianomaisten henkilöiden saatavilla ja sen seurausten on oltava ennakoitavia.<sup>108</sup> Sääntöä pidetään ennakoitavana, jos se on muotoiltu niin selkeästi, että jokainen voi – tarvittaessa asianmukaisella opastuksella – noudattaa sitä toiminnassaan.<sup>109</sup> Lailta tässä yhteydessä vaadittu täsmällisyys riippuu aihealueesta.<sup>110</sup>

108 Asia nro 27798/95, *Amann v. Sveitsi* [suuri jaosto], EIT 16.2.2000, 50 kohta; ks. myös asia nro 23224/94, *Kopp v. Sveitsi*, EIT 25.3.1998, 55 kohta, ja asia nro 25198/02, *lordachi ym. v. Moldova*, EIT 10.2.2009, 50 kohta.

109 Asia nro 27798/95, *Amann v. Sveitsi* [suuri jaosto], EIT 16.2.2000, 56 kohta; ks. myös asia nro 8691/79, *Malone v. Yhdistynyt kuningaskunta*, EIT 26.4.1985, 66 kohta; yhdistetyt asiat nro 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, *Silver ym. v. Yhdistynyt kuningaskunta*, EIT 25.3.1983, 88 kohta.

110 Asia nro 6538/74, *The Sunday Times v. Yhdistynyt kuningaskunta*, EIT 26.4.1979, 49 kohta; ks. myös yhdistetyt asiat nro 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, *Silver ym. v. Yhdistynyt kuningaskunta*, EIT 25.3.1983, 88 kohta.

Esimerkki: Asiassa *Rotaru v. Romania*<sup>111</sup> EIT totesi EIS:n 8 artiklan vastaiseksi sen, että Romanian laki salli kansalliseen turvallisuuteen vaikuttavien salaisten tiedostojen keräämisen, tallentamisen ja arkistoinen ilman, että näille viranomaisten harkintavaltaan jätetyille valtuuksille asetettiin mitään rajoituksia. Kansallisessa lainsäädännössä ei esimerkiksi määritelty minkä tyyppisiä tietoja voitiin käsitellä, mihin ihmisryhmiin valvontatoimia saatettiin kohdistaa, missä olosuhteissa toimenpiteitä voitiin toteuttaa tai mitä menettelyjä oli noudatettava. Näiden puutteiden takia tuomioistuimien totesi, että kansallinen laki ei täyttänyt EIS:n 8 artiklassa määrättyä ennakoitavuuden vaatimusta ja että kyseistä artiklaa oli rikottu.

Esimerkki: Asiassa *Taylor-Sabori v. Yhdistynyt kuningaskunta*<sup>112</sup> kantaja oli ollut poliisivalvonnan kohteena. Poliisi oli kohdistanut kantajaan telepakkokeinoja käyttämällä tämän hakulaitteen ”kloonina”. Kantaja oli myöhemmin pidätetty ja asetettu syytteeseen osallisuudesta huumekauppaan. Osa syyttäjän aineistosta koostui poliisin puhtaaksikirjoittamista hakulaitteen viesteistä. Kantajan oikeudenkäynnin aikaan Yhdistyneessä kuningaskunnassa ei kuitenkaan ollut lainsäädäntöä, jolla olisi säännelty yksityisten televiestintäjärjestelmien kautta lähetettyihin viesteihin kohdistuneista pakkokeinoista. Näin ollen kantajan oikeuksiin puuttuminen ei ollut tapahtunut ”lainmukaisesti”. EIT totesi, että EIS:n 8 artiklaa oli rikottu.

## Sillä on laillinen tarkoitus

Laillinen tarkoitus voi olla jompikumpi mainituista julkisista eduista tai muiden henkilöiden oikeudet ja vapaudet.

Esimerkki: Asiassa *Peck v. Yhdistynyt kuningaskunta*<sup>113</sup> kantaja oli yrittänyt tehdä itsemurhan kadulla viiltämällä ranteensa, mutta hän ei ollut huomannut, että valvontakamera oli tallentanut tämän yrityksen. Kun poliisit, jotka olivat seuranneet valvontakameraa, olivat pelastaneet hänet, poliisiviranomainen luovutti valvontakameran kuvaaman aineiston tiedostusvälineille, jotka julkaisivat sen peittämättä kantajan kasvoja. EIT katsoi, ettei viranomaisilla ollut

111 Asia nro 28341/95, *Rotaru v. Romania* [suuri jaosto], EIT 4.4.2000, 57 kohta; ks. myös asia nro 62540/00, *Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria*, EIT 28.6.2007; asia nro 30194/09, *Shimovolos v. Venäjä*, EIT 21.6.2011; ja asia nro 59842/00, *Vetter v. Ranska*, EIT 31.5.2005.

112 Asia nro 47114/99, *Taylor-Sabori v. Yhdistynyt kuningaskunta*, EIT 22.10.2002.

113 Asia nro 44647/98, *Peck v. Yhdistynyt kuningaskunta*, EIT 28.1.2003, erityisesti 85 kohta.

merkittävää tai riittävää syytä luovuttaa aineistoa yleisölle pyytämättä kantajalta lupaa tai peittämättä hänen henkilöllisyyttään. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

## Se on välttämätöntä demokraattisessa yhteiskunnassa

EIT on todennut, että välttämättömyyden käsite edellyttää, että oikeuteen puuttuminen on vastaus pakottavaan yhteiskunnalliseen tarpeeseen ja erityisesti että se on oikeassa suhteessa lailliseen tarkoitukseen.<sup>114</sup>

Esimerkki: Asiassa *Khelili v. Sveitsi*<sup>115</sup> poliisi huomasi tarkastuksen yhteydessä, että kantajalla oli käyntikortteja joissa luki: ”Kaunis kolmekymppinen nainen haluaisi tavata miehen, jonka kanssa voisi joskus käydä lasillisella tai ulkona. Puhelinnumero --”. Kantaja väitti, että poliisi oli löytönsä jälkeen kirjannut naisen poliisirekisteriin prostituoituna, vaikka hän kielsi harjoittavansa kyseistä ammattia. Kantaja vaati, että sana ”prostituoitu” poistetaan poliisirekisteristä. EIT myönsi, että periaatteessa henkilötietojen säilyttäminen sillä perusteella, että henkilö voisi syyllistyä toiseen rikokseen, saattoi olla joissakin olosuhteissa oikeasuhteista. Kantajan tapauksessa väite laittomasta prostituutiosta vaikutti kuitenkin liian epämääräiseltä ja yleisluonteiselta, sen tueksi ei ollut konkreettista näyttöä, sillä kantajaa ei ollut koskaan tuomittu laittomasta prostituutiosta, eikä väitettä näin ollen voitu perustella pakottavalla yhteiskunnallisella tarpeella EIS:n 8 artiklassa tarkoitetulla tavalla. Tuomioistuin otti huomioon kantajan oikeuksiin puuttumisen vakavuuden ja katsoi, että oli viranomaisten tehtävä todistaa kantajasta säilytettyjen tietojen todenmukaisuus. Näin ollen tuomioistuin totesi, ettei sanan ”prostituoitu” säilyttäminen poliisirekisterissä vuosien ajan ollut välttämätöntä demokraattisessa yhteiskunnassa. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Leander v. Ruotsi*<sup>116</sup> EIT katsoi, että kansallisen turvallisuuden kannalta tärkeisiin tehtäviin hakevien henkilöiden salainen tutkiminen ei itsessään ollut vastoin vaatimusta, joka koski välttämättömyyttä demokraattisessa yhteiskunnassa. Kansallisessa lainsäädännössä rekisteröityjen etujen suojelemiseksi säädetyt erityiset suojatoimet – kuten parlamentin ja oikeuskanslerin harjoittama valvonta – saivat EIT:n päättämään siihen johtopäätökseen, että Ruot-

114 Asia nro 9248/81, *Leander v. Ruotsi*, EIT 11.7.1985, 58 kohta.

115 Asia nro 16188/07, *Khelili v. Sveitsi*, EIT 18.10.2011.

116 Asia nro 9248/81, *Leander v. Ruotsi*, EIT 11.7.1985, 59 ja 67 kohta.

sisä käytössä ollut työntekijöiden tarkastusjärjestelmä täytti EIS:n 8 artiklan 2 kohdan vaatimukset. Laajan harkintavaltansa ansiosta vastaajana ollut valtio saattoi oikeutetusti katsoa, että kantajan tapauksessa kansallisen turvallisuuden edut menivät yksilön etujen edelle. Tuomioistuin totesi, ettei EIS:n 8 artiklaa ollut rikottu.

### 3.1.2. EU:n perusoikeuskirjassa määritellyt edellytykset oikeuden lailliselle rajoittamiselle

Perusoikeuskirjan rakenne ja sanamuoto ovat erilaiset kuin EIS:n. Perusoikeuskirjassa ei mainita puuttumista turvattuihin oikeuksiin, mutta siinä on määräys, jonka nojalla voidaan rajoittaa perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttöä.

Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien – kuten henkilötietojen suoja (esimerkiksi henkilötietojen käsittelyn yhteydessä) koskevan oikeuden – käyttämistä voidaan rajoittaa ainoastaan, jos rajoitukset

- on säädetty lailla; ja
- ne noudattavat tietosuojan oikeuden olennaista sisältöä; ja
- ne ovat välttämättömiä suhteellisuusperiaatteen mukaisesti; ja
- ne vastaavat unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Esimerkkejä: Asiassa *Volker und Markus Schecke*<sup>117</sup> EUTI totesi, että neuvosto ja komissio ovat säätäessään kaikkien luonnollisten henkilöiden, jotka ovat [tiettyjen maatalousrahastojen] tuensaajia, nimien ja näiden saamien tarkkojen määrien julkaisemisesta tekemättä eroa sellaisten merkityksellisten kriteerien mukaan kuin ajanjaksot, joihin kyseiset luonnolliset henkilöt ovat saaneet tällaisia tukia, niiden toistuvuus tai niiden laji ja suuruus, ylittäneet suhteellisuusperiaatteen noudattamisen rajat.

117 Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen*, EUTI 9.11.2010, 89 ja 86 kohta.

Tästä syystä EUTI piti tarpeellisena todeta pätemättömiksi tietyt neuvoston asetuksen (EY) N:o 1290/2005 säännökset ja asetuksen (EY) N:o 259/2008 kokonaisuudessaan.<sup>118</sup>

Erilaisesta sanamuodosta huolimatta perusoikeuskirjan 52 artiklan 1 kohta, jossa esitetään laillisen käsittelyn edellytykset, muistuttaa EIS:n 8 artiklan 2 kohtaa. Perusoikeuskirjan 52 artiklan 1 kohdassa lueteltujen edellytysten on katsottava vastaavan EIS:n 8 artiklan 2 kohdassa esitettyjä edellytyksiä, sillä perusoikeuskirjan 52 artiklan 3 kohdan ensimmäisessä virkkeessä todetaan, että ”siltä osin kuin tämän perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamista koskevassa eurooppalaisessa yleissopimuksessa taattuja oikeuksia, niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa”.

Samoin 52 artiklan 3 kohdan viimeisessä virkkeessä kuitenkin tarkennetaan, että ”mitä tässä määrätään, ei estä unionia määräämästä tätä laajemmasta suojasta”. Kun EIS:n 8 artiklan 2 kohtaa luetaan yhdessä 52 artiklan 3 kohdan kanssa tämä voi tarkoittaa vain, että EIS:n 8 artiklan 2 kohdassa määritellyt oikeutetun puuttumisen edellytykset ovat vähimmäisvaatimus perusoikeuskirjan mukaiselle tietosuojaa koskevan oikeuden lailliselle rajoittamiselle. Tämän seurauksena EU-oikeudessa henkilötietojen laillinen käsittely edellyttää, että vähintään EIS:n 8 artiklan 2 kohdan edellytykset täyttyvät; EU-oikeudessa voidaan kuitenkin asettaa myös lisävaatimuksia tiettyjä tilanteita varten.

EU-oikeuden mukaisen laillisen käsittelyn periaatteen vastaavuutta EIS:n asiaa koskevien määräysten kanssa tukee SEU 6 artiklan 3 kohta, jonka mukaan ”ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä eurooppalaisessa yleissopimuksessa taatut – perusoikeudet ovat yleisinä periaatteina osa unionin oikeutta”.

<sup>118</sup> Neuvoston asetus (EY) N:o 1290/2005, annettu 21 päivänä kesäkuuta 2005, yhteisen maatalouspolitiikan rahoituksesta, EUVL 2005 L 209; komission asetus (EY) N:o 259/2008, annettu 18 päivänä maaliskuuta 2008, neuvoston asetuksen (EY) N:o 1290/2005 soveltamista koskevista yksityiskohtaisista säännöistä Euroopan maatalouden tukirahaston (maataloustukirahaston) ja Euroopan maaseudun kehittämisen maatalousrahaston (maaseuturahaston) varoja saavia tuensaajia koskevien tietojen julkaisemisen osalta, EUVL 2008 L 76.

## 3.2. Tarkoituksen määrittelemisen ja käyttötarkoitussidonnaisuuden periaatteet

### Keskeiset kohdat

- Henkilötietojen käsittelyn tarkoitus on määriteltävä selkeästi ennen käsittelyn aloittamista.
- EU-oikeuden mukaan käsittelyn tarkoitus on määriteltävä nimenomaisesti; EN-oikeudessa tämä näkökohta on jätetty kansallisen lainsäädännön piiriin.
- Käsittely määrittelemättömiin tarkoituksiin on tietosuojasäännösten vastaista
- Henkilötietojen myöhempään käsittelyyn muuhun kuin alun perin määriteltyyn tarkoitukseen on oltava erillinen oikeudellinen peruste, jos uusi käsittelytarkoitus on yhteensopimaton alkuperäisen tarkoituksen kanssa.
- Henkilötietojen luovuttaminen sivullisille on uusi käsittelyn tarkoitus ja sille on oltava oma oikeudellinen peruste.

Pohjimmiltaan henkilötietojen käsittelyn määrittelemisen ja käyttötarkoitussidonnaisuuden periaatteet tarkoittavat, että henkilötietojen käsittelyn lainmukaisuus riippuu käsittelyn tarkoituksesta.<sup>119</sup> Rekisterinpitäjän on täytynyt määritellä ja ilmoittaa tarkoitus ennen henkilötietojen käsittelyn aloittamista.<sup>120</sup> **EU-oikeudessa** tämä tapahtuu ilmoituksen tekemisellä asianomaiselle valvontaviranomaiselle tai vähintään laatimalla sisäisesti asiakirjat, jotka rekisterinpitäjä saattaa valvontaviranomaisen saataville tarkastusta varten ja rekisteröidyn saataville.

Henkilötietojen käsittely määrittelemättömiin ja/tai rajoittamattomaan tarkoituksiin on laitonta.

Jokaisella uudella henkilötietojen käsittelytarkoituksella on oltava oma oikeudellinen peruste eikä käsittelyssä voida lähteä siitä, että tiedot on alun perin kerätty tai käsitelty toiseen lailliseen tarkoitukseen. Laillinen käsittely puolestaan rajoittuu alun perin määriteltyyn tarkoitukseen ja jokaiselle uudelle käsittelytarkoitukselle on

<sup>119</sup> Yleissopimus 108, 5 artiklan b alakohta; tietosuojadirektiivi, 6 artiklan 1 kohdan b alakohta.

<sup>120</sup> Ks. myös tietosuojatryöryhmä (2013), *Opinion 03/2013 on purpose limitation*, WP 203, Bryssel, 2. huhtikuuta 2013.

oltava uusi erillinen oikeudellinen peruste. Henkilötietojen luovuttamista sivullisille on harkittava erityisen tarkasti, sillä luovutus katsotaan yleensä uudeksi tarkoitukseksi ja se vaatii näin ollen toisen oikeudellisen perusteen kuin tietojen kerääminen.

Esimerkki: Lentoyhtiö kerää asiakkaistaan tietoja varauksia varten, jotta lento voitaisiin suorittaa asianmukaisesti. Lentoyhtiö tarvitsee seuraavat tiedot: matkustajien paikanumerot; erityiset liikuntarajoitukset, kuten pyörätuolin tarve; ja erityiset ruokavaatimukset, kuten kosher- tai halal-sääntöjen mukainen ruoka. Jos lentoyhtiötä pyydetään luovuttamaan nämä matkustajarekisterin tiedot kohdemaan maahanmuuttoviranomaiselle, tietoja käytetään myöhemmin maahanmuuton valvontaan, joka on eri tarkoitus kuin se, johon tiedot on kerätty. Näin ollen tietojen luovuttamiselle maahanmuuttoviranomaiselle tarvitaan uusi erillinen oikeudellinen peruste.

Tarkoituksen laajuuden ja rajojen määrittelyä varten yleissopimuksessa 108 ja tietosuojadirektiivissä viitataan yhteensopivuuden käsitteeseen: Tietoja voidaan käyttää alkuperäisen tarkoituksen kanssa yhteensopiviin tarkoituksiin alkuperäisen oikeudellisen perusteen nojalla. Sitä, mitä ”yhteensopivalla” tarkoitetaan, ei kuitenkaan ole määritelty, vaan käsitettä tulkitaan tapauskohtaisesti.

Esimerkki: Jos Sunshine-yhtiö myy asiakashallintajärjestelmänsä sisältämiä henkilötietoja suoramarkkinointia harjoittavalle Moonlight-yhtiölle, joka haluaa käyttää näitä tietoja kolmansien osapuolien markkinointikampanjoissa, kyseessä on uusi tarkoitus, joka on yhteensopimaton asiakkuudenhallinnan, eli Sunshine-yhtiön alkuperäisen asiakastietojen keräämisen tarkoituksen, kanssa. Tietojen myynti Moonlight-yhtiölle tarvitsee näin ollen oman oikeudellisen perusteen.

Sen sijaan sitä, että Sunshine-yhtiö käyttää asiakashallintajärjestelmänsä tietoja omiin markkinointitarkoituksiinsa eli omia tuotteitaan koskevien markkinointiviestien lähettämiseen asiakkailleen, pidetään yleensä yhteensopivana tarkoituksena.

Tietosuojadirektiivissä nimenomaisesti säädetään, että ”myöhempiä käsittelyä historiantutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten ei pidetä

yhteensopimattomana, sillä edellytyksellä, että jäsenvaltiot toteuttavat tarpeelliset suojatoimet”<sup>121</sup>

Esimerkkejä: Sunshine-yhtiö on kerännyt ja säilyttänyt asiakkuudenhallintatietoja asiakkaistaan. Se, että Sunshine-yhtiö käyttää samoja tietoja asiakkaidensa ostokäyttäytymisen tilastoanalyysiin, on sallittua, koska tilastointi on yhteensopiva tarkoitus. Tällöin ei tarvita muuta oikeudellista perustetta, kuten rekisteröityjen suostumusta.

Jos kyseiset tiedot luovutettaisiin sivulliselle, Starlight-yhtiölle, yksinomaan tilastollisiin tarkoituksiin, luovuttaminen olisi mahdollista ilman uutta oikeudellista perustetta, mutta ainoastaan sillä ehdolla, että yhtiöt olisivat toteuttaneet tarpeelliset suojatoimet, kuten peittäneet rekisteröityjen henkilöllisyyden, sillä henkilöllisyyttä ei yleensä tarvita tilastollisiin tarkoituksiin.

## 3.3. Tietojen laatua koskevat periaatteet

### Keskeiset kohdat

- Rekisterinpitäjän on noudatettava tietojen laatua koskevia periaatteita kaikissa käsittelytoimissa.
- Kun henkilötietoja ei ole enää tarpeellista käsitellä siihen tarkoitukseen mihin ne on alun perin kerätty, tiedot on poistettava.
- Edellä mainitusta periaatteesta voidaan poiketa vain, jos poikkeuksista säädetään laissa ja rekisteröityjen suojaksi toteutetaan erityisiä suojatoimia.

### 3.3.1. Tietojen tarpeellisuusvaatimus

Vain sellaisia henkilötietoja voidaan käsitellä, jotka ovat ”asianmukaisia, olennaisia eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään”<sup>122</sup> Käsiteltäväksi valittujen tietoryhmien on oltava välttämättömiä käsittelytoimille ilmoitetun tarkoituksen saavuttamiseksi, ja rekisterinpitäjän

<sup>121</sup> Esimerkki vastaavasta kansallisesta säännöksestä löytyy Itävallan tietosuojalaista (*Datenschutzgesetz*), Fed. Law Gazette I No. 165/1999, 46 kohta, saatavana englanniksi osoitteessa: [www.dsk.gv.at/DocView.axd?CobId=41936](http://www.dsk.gv.at/DocView.axd?CobId=41936).

<sup>122</sup> Yleissopimus 108, 5 artiklan c alakohta; ja tietosuojadirektiivi, 6 artiklan 1 kohdan c alakohta.



tulisi tiukasti rajata kerättävät henkilötiedot niihin tietoihin, jotka liittyvät suoraan käsittelyn nimenomaiseen tarkoitukseen.

Nyky-yhteiskunnassa tietojen olennaisuuteen liittyy vielä yksi näkökohta: erityisen yksityisyyttä suojaavan tekniikan avulla voidaan toisinaan välttyä kokonaan henkilötietojen käytöltä tai käyttää pseudonyymeja henkilötietoja yksityisyyttä suojaavalla tavalla. Tämä on erityisen merkityksellistä laajoissa käsittelyjärjestelmissä.

Esimerkki: Kaupunginvaltuusto tarjoaa kaupungin julkisen liikenteen säännöllisille käyttäjille sirukortin tiettyä maksua vastaan. Käyttäjän nimi on kirjoitettu kortin pinnalle ja se löytyy myös sirulta sähköisessä muodossa. Aina kun henkilö matkustaa bussilla tai raitiovaunulla, hänen on käytettävä sirukorttia lukulaitteen edessä. Laite tarkistaa tiedot sähköisesti tietokannasta, joka sisältää matkakortin ostaneiden henkilöiden nimet.

Tämä järjestelmä ei vastaa olennaisuuden periaatetta parhaalla mahdollisella tavalla: henkilön oikeus käyttää kulkuneuvoja olisi mahdollista tarkistaa vertaamalla kortin sirulla olevia henkilötietoja tietokantaan. Siihen riittäisi esimerkiksi, että kortin sirulla olisi erityinen sähköinen kuva, kuten viivakoodi, joka kertoisi lukulaitteen kohdalla, onko kortti voimassa. Tällainen järjestelmä ei tallentaisi tietoa siitä, kuka on käyttänyt kulkuneuvoa ja milloin. Henkilötietoja ei kerätäisi, mikä on olennaisuuden periaatteen kannalta paras vaihtoehto, sillä periaate velvoittaa välttämään tietojen keräämistä.

### 3.3.2. Tietojen virheettömyysvaatimus

Rekisterinpitäjä, jolla on hallussaan henkilötietoja, ei saa käyttää kyseisiä tietoja, ellei hän ole saanut kohtuullista varmuutta tietojen täsmällisyydestä ja ajantasaisuudesta.

Velvollisuutta varmistaa henkilötietojen virheettömyys ja ajantasaisuus, on tarkastettava tietojen käsittelyn tarkoitusta vasten.

Esimerkki: Huonekalumyymälä on tallentanut asiakkaan nimi- ja osoitetiedot laskun lähettämistä varten. Puoli vuotta myöhemmin sama yritys haluaisi käynnistää markkinointikampanjan ja ottaa yhteyttä vanhoihin asiakkaisiin. Heidän tavoittamiseksi yritys haluaisi saada kansallisesta väestörekisteristä ajantasaiset osoitetiedot, sillä maan kansalaisten on lain mukaan ilmoitettava

rekisteriin osoitteenmuutoksesta. Väestörekisteristä annetaan tietoja vain sellaisille henkilöille ja yhteisöille, jotka voivat esittää oikeutetun perusteen.

Tässä tilanteessa yritys ei voi vedota siihen, että tiedot on pidettävä täsmällisinä ja ajantasaisina, voidakseen saada väestörekisteristä kaikkien vanhojen asiakkaidensa uudet osoitetiedot. Tiedot on kerätty laskutusta varten; siihen tarkoitukseen riittää kyseisellä hetkellä käytössä ollut osoite. Uusien osoitetietojen keräämiselle ei ole oikeudellista perustetta, sillä markkinointi ei ole tärkeämpi etu kuin oikeus tietosuojaan eikä sillä siten voida oikeuttaa rekisterin tietojen saantia.

Joissakin tapauksissa säilytettyjen tietojen päivittäminen voi olla lailla kiellettyä siksi, että tietojen säilyttämisen syynä on pääasiallisesti tapahtumien dokumentointi.

Esimerkki: Hoitotoimenpiteen tietoja ei saa muuttaa, eli ”päivittää”, vaikka tiedoista paljastuisi myöhemmin virheitä. Tällaisessa tilanteessa tietoihin voidaan vain lisätä huomautuksia, kunhan ne merkitään selvästi jälkepäin tehdyiksi lisäyksiksi.

Toisaalta joissakin tilanteissa tietoja on ehdottomasti tarkistettava ja tarvittaessa päivitettävä säännöllisesti, koska tietojen säilyminen virheellisinä voisi aiheuttaa rekisteröidylle haittaa.

Esimerkki: Kun joku haluaa tehdä sopimuksen pankin kanssa, pankki yleensä tarkistaa mahdollisen asiakkaansa luottokelpoisuuden. Tätä tarkoitusta varten on erityisiä tietokantoja, jotka sisältävät tietoja henkilöiden luottohistoriasta. Jos tällainen tietokanta antaisi virheellistä tai vanhentunutta tietoa jostakin henkilöstä, tälle henkilölle voisi aiheutua merkittäviä ongelmia. Näiden tietokantojen rekisterinpitäjien onkin noudatettava virheettömyydenperiaatetta erityisen huolellisesti.

Lisäksi tietoja, jotka eivät liity tosiasioihin vaan epäilyihin, kuten rikostutkimuksiin, voidaan kerätä ja säilyttää niin kauan, kun rekisterinpitäjällä on oikeudellinen peruste tietojen keräämiselle ja riittävän vahvat perusteet epäilylle.

### 3.3.3. Tietojen säilyttäminen

Tietosuojadirektiivin 6 artiklan 1 kohdan e alakohdassa ja samaten yleissopimuksen 108 5 artiklan e alakohdassa vaaditaan jäsenvaltioita varmistamaan, että henkilötiedot ”säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan, kuin on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään”. Tiedot on näin ollen poistettava, kun tarkoitus on toteutettu.

Yhdistetyissä asioissa *S. ja Marper* EIT totesi, että Euroopan neuvoston asiaa koskevien asiakirjojen pääperiaatteet sekä sopimuspuolien lainsäädäntö ja oikeuskäytäntö edellyttivät, että tietoja säilytetään oikeassa suhteessa niiden keräämisen tarkoitukseen ja vain rajoitetun ajan, erityisesti poliisialalla.<sup>123</sup>

Henkilötietojen säilyttämisen aikarajoitus koskee kuitenkin vain tietoja, joita säilytetään sellaisessa muodossa, että rekisteröidyt voidaan tunnistaa. Tarpeettomia tietoja voitaisiin siis säilyttää laillisesti tekemällä ne anonyymeiksi tai pseudonyymeiksi ne.

Tietojen säilyttäminen historiantutkimusta taikka tilastollisia tai tieteellisiä tarkoituksia varten on tietosuojadirektiivissä jätetty nimenomaisesti tietojen käyttötarkoituksidonnaisuuden periaatteen soveltamisalan ulkopuolelle.<sup>124</sup> Tällainen henkilötietojen jatkuva säilyttäminen ja käyttö edellyttävät kuitenkin, että kansallisessa lainsäädännössä on säädetty asianmukaiset suojauskeinot.

## 3.4. käsittelyn periaate

### Keskeiset kohdat

- Asianmukaisellakäsittelyllä tarkoitetaan käsittelyn avoimuutta ja läpinäkyvyyttä erityisesti suhteessa rekisteröityihin.
- Ennen henkilötietojen käsittelyyn ryhtymistä, rekisterinpitäjän on informoitavarekisteröityjä ainakin tietojen käsittelyn tarkoituksesta sekä huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tämän toimipaikan sijainnista. .

123 Yhdistetyt asiat nro 30562/04 ja 30566/04, *S. ja Marper v. Yhdistynyt kuningaskunta*, EIT 4.12.2008; ks. myös esim. asia nro 24029/07, *M.M. v. Yhdistynyt kuningaskunta*, EIT 13.11.2012.

124 Tietosuojadirektiivi, 6 artiklan 1 kohdan e alakohta.

- Henkilötietoja ei saa käsitellä salaisesti tai peitellysti, ellei siitä nimenomaisesti säädetä laissa.
- Rekisteröidyillä on pääsääntöisesti aina oikeus tarkastaa henkilörekisteriin tallennetut tiedot.

Asianmukaisen käsittelyn periaate ohjaa ensisijaisesti rekisterinpitäjän ja rekisteröidyn välistä suhdetta.

### 3.4.1. Avoimuus

Tämä periaate asettaa rekisterinpitäjälle velvollisuuden kertoa rekisteröidyille, miten heitä koskevia tietoja käsitellään.

Esimerkki: Asiassa *Haralambie v. Romania*<sup>125</sup> kantaja oli pyytänyt nähdä tiedot, joita salainen palvelu säilytti hänestä, mutta hänen pyyntönsä hyväksyttiin vasta viisi vuotta myöhemmin. EIT totesi, että henkilöiden, joiden tietoja viranomaiset säilyttivät, oli erittäin tärkeää voida tutustua tietoihinsa. Viranomaisilla oli velvollisuus tarjota tehokas menettely tällaisten tietojen saantiin. EIT katsoi, ettei viiden vuoden viivettä kantajan tietopyynnön täyttämiseksi voitu perustella sen enempää tiedostojen määrällä kuin arkistointijärjestelmän heikkouksillakaan. Viranomaiset eivät olleet tarjonneet kantajalle tehokasta ja toimivaa menettelyä henkilötietojen saamiseksi kohtuullisessa ajassa. Tuomioistuimien totesi, että EIS:n 8 artiklaa oli rikottu.

Käsittelytoimet on selitettävä rekisteröidyille niin, että he varmasti ymmärtävät, mitä heidän tiedoilleen tapahtuu. Rekisteröidyillä on myös oikeus saada rekisterinpitäjältä vastaus siihen, käsittelee se rekisteröidyn henkilötietoja ja, jos käsittelee niin, mitä tietoja se käsittelee.

### 3.4.2. Luottamuksen rakentaminen

Rekisterinpitäjien tulisi osoittaa rekisteröidyille ja suurelle yleisölle, että ne aikovat käsitellä tietoja laillisesti ja avoimesti. Käsittelytoimia ei saa toteuttaa salaa, eikä niillä saisi olla ennakoimattomia kielteisiä vaikutuksia. Rekisterinpitäjien tulisi varmistaa, että asiakkaat tai kansalaiset ovat tietoisia henkilötietojensa käytöstä. Lisäksi rekisterinpitäjien tulisi mahdollisuuksien mukaan noudattaa rekisteröityjen

<sup>125</sup> Asia nro 21737/03, *Haralambie v. Romania*, EIT 27.10.2009

toiveita, erityisesti silloin, kun rekisteröidyn suostumus on tietojenkäsittelyn oikeudellinen peruste.

Esimerkki: *Asiassa K.H. ym. v. Slovakia*<sup>126</sup> kantajina oli kahdeksan romanisyn-typerää olevaa naista, joita oli hoidettu kahdessa itäisen Slovakian sairaalassa heidän raskautensa ja synnytyksensä aikana. Yksikään heistä ei pystynyt enää sen jälkeen saamaan lasta lukuisista yrityksistä huolimatta. Kansalliset tuomioistuimet määräsivät sairaalat sallimaan kantajien ja heidän edustajiensa tutustua potilaskertomuksiin ja kirjata niistä otteita käsin, mutta hylkäsivät pyynnön ottaa asiakirjoista valokopioita vedoten väärinkäytösten ehkäisemiseen. Valtion EIS:n 8 artiklan mukaisesti myönteisiin velvollisuuksiin kuului selvästi velvollisuus saattaa rekisteröityjen saataville kopiot heitä koskevista tiedoista. Valtion tehtävänä oli määrittellä, miten henkilötiedot kopioitaisiin, tai tarvittaessa esittää pakottavat syyt tästä kieltäytymiselle. Kantajien tapauksessa kansalliset tuomioistuimet perustelivat potilaskertomusten kopioinnin kieltämisen pääasiallisesti tarpeella suojata tietoja väärinkäytöiltä. EIT ei kuitenkaan voinut ymmärtää, miten kantajat, joille oli annettu mahdollisuus tutustua omiin potilaskertomuksiinsa, olisivat voineet käyttää väärin itseään koskevia tietoja. Lisäksi tällainen riski olisi voitu ehkäistä muilla keinoin kuin kieltämällä kertomusten kopiointi kantajilta, esimerkiksi rajoittamalla niiden henkilöiden määrää, joille annettiin oikeus tutustua asiakirjoihin. Valtio ei ollut osoittanut riittävän pakottavia syitä sille, miksi se ei ollut antanut kantajille asianmukaista mahdollisuutta tutustua omaa terveyttään koskeviin tietoihin. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

Internetpalvelujen yhteydessä tietojenkäsittelyjärjestelmien on oltava ominaisuuk-siltaan sellaisia, että rekisteröidyt voivat ymmärtää kunnolla, mitä heidän tiedoilleen tapahtuu.

Asianmukainen henkilötietojen käsittely tarkoittaa myös sitä, .rekisterinpitäjien on tarjottava lakisääteisiä vähimmäisvaatimuksia kattavampia palveluita, jos rekisteröidyn oikeudet edut sitä vaativat.

<sup>126</sup> Asia nro 32881/04, *K.H. ym. v. Slovakia*, EIT 6.11.2009.

## 3.5. Vastuullisuuden periaate Keskeiset kohdat

### Keskeiset kohdat

- Vastuullisuus edellyttää rekisterinpitäjiltä aktiivisia toimenpiteitä tietosuojan edistämiseksi ja turvaamiseksi henkilötietoja käsiteltäessä.
- Rekisterinpitäjät vastaavat siitä, että henkilötietojen käsittely on lainmukaista.
- Rekisterinpitäjien pitäisi pystyä milloin tahansa todistamaan tietosuojamääräysten noudattaminen rekisteröidyille, yhteiskunnalle ja valvontaviranomaisille.

Taloudellisen yhteistyön ja kehityksen järjestö (OECD) hyväksyi vuonna 2013 yksityisyyden suojaa koskevat suuntaviivat, joissa korostettiin rekisterinpitäjien tärkeää roolia tietosuojan toteuttamisessa käytännössä. Suuntaviivoissa käsitellään vastuullisuuden periaatetta toteamalla, että rekisterinpitäjän tulisi olla vastuussa sellaisten toimenpiteiden noudattamisesta, joilla toteutetaan aiemmin mainittuja olennaisia periaatteita.<sup>127</sup>

Siinä missä yleissopimuksessa 108 ei mainita lainkaan rekisterinpitäjien vastuullisuutta, vaan jätetään asia kansallisen lainsäädännön piiriin, tietosuojadirektiivin 6 artiklan 2 kohdassa todetaan, että rekisterinpitäjän on huolehdittava 1 kohdassa tietojen laadun osalta esitettyjen periaatteiden noudattamisesta.

Esimerkki: Lainsäädäntöön liittyvä esimerkki vastuullisuuden periaatteen merkityksestä on sähköisen viestinnän tietosuojadirektiiviin 2002/58/EY vuonna 2009 tehty muutos<sup>128</sup>. Muutetun direktiivin 4 artiklassa säädetään velvollisuudesta toteuttaa toimenpiteitä, joilla on "varmistettava henkilötietojen käsittelyä koskevan turvapolitiikan toteuttaminen". Lainsäätäjät siis katsoi, että direktiivin

127 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, 14 artikla.

128 Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta, EUVL 2009 L 337, s. 11.

turvasäännösten osalta oli tarpeen lisätä nimenomainen vaatimus turvapolitiikan laatimisesta ja toteuttamisesta.

Tietosuojatyöryhmän lausunnon<sup>129</sup> mukaan vastuullisuuden ytimessä on rekisterinpitäjän velvollisuus

- toteuttaa toimenpiteitä, joilla – tavallisissa olosuhteissa – varmistetaan, että käsittelytoimissa noudatetaan tietosuojasääntöjä; ja
- ylläpitää asiakirjoja, joilla se voi todistaa rekisteröidyille ja valvontaviranomaisille, mitä toimenpiteitä se on toteuttanut tietosuojasääntöjen noudattamiseksi.

Näin ollen vastuullisuusperiaate velvoittaa rekisterinpitäjät osoittamaan aktiivisesti sääntöjen noudattamisen sen sijaan, että ne vain odottaisivat, että rekisteröidyt tai valvontaviranomaiset tuovat esiin puutteita.

129 Tietosuojatyöryhmä, *lausunto 3/2010 tilivelvollisuuden periaatteesta*, WP 173, Bryssel, 13. heinäkuuta 2010.





# 4

## Euroopan tietosuojaa koskevat säännöt



EU	Katetut aiheet	EN
<b>Muiden kuin arkaluonteisten tietojen laillista käsittelyä koskevat säännöt</b>		
Tietosuojadirektiivi, 7 artiklan a alakohta	Suostumus	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta ja 3 artiklan 6 kohta
Tietosuojadirektiivi, 7 artiklan b alakohta	Sopimusta edeltävä suhde	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
Tietosuojadirektiivi, 7 artiklan c alakohta	Rekisterinpitäjän lailliset velvoitteet	Profilointia koskeva suositus, 3 artiklan 4 kohdan a alakohta
Tietosuojadirektiivi, 7 artiklan d alakohta	Rekisteröidyn elintärkeät edut	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
Tietosuojadirektiivi, 7 artiklan e alakohta ja 8 artiklan 4 kohta Asia C-524/06, <i>Huber v. Saksa</i> , EYTI 16.12.2008	Yleinen etu ja julkisen vallan käyttäminen	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
Tietosuojadirektiivi, 7 artiklan f alakohta, 8 artiklan 2 ja 3 kohta Yhdistetyt asiat C-468/10 ja C-469/10, <i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado</i> , EUTI 24.11.2011	Muiden oikeutetut edut	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
<b>Arkaluonteisten tietojen laillista käsittelyä koskevat säännöt</b>		
Tietosuojadirektiivi, 8 artiklan 1 kohta	Yleinen käsittelykielto	Yleissopimus 108, 6 artikla

EU	Katetut aiheet	EN
Tietosuojadirektiivi, 8 artiklan 2–4 kohta	Poikkeukset yleisestä säännöstä	Yleissopimus 108, 6 artikla
Tietosuojadirektiivi, 8 artiklan 5 kohta	(Rikosoikeudellisiin) tuomioihin liittyvien tietojen käsittely	Yleissopimus 108, 6 artikla
Tietosuojadirektiivi, 8 artiklan 7 kohta	Henkilönumeroiden käsittely	
<b>Turvallista käsittelyä koskevat säännöt</b>		
Tietosuojadirektiivi, 17 artikla	Velvollisuus turvata käsittely	Yleissopimus 108, 7 artikla Asia nro 20511/03, I. v. Suomi, EIT 17.7.2008
Sähköisen viestinnän tietosuojadirektiivi, 4 artiklan 2 kohta	Tietoturvaloukkauksesta ilmoittaminen	
Tietosuojadirektiivi, 16 artikla	Velvollisuus säilyttää luottamuksellisuus	
<b>Käsittelyn avoimuutta koskevat säännöt</b>		
	Avoimuus yleisesti	Yleissopimus 108, 8 artiklan alakohta
Tietosuojadirektiivi, 10 ja 11 artikla	Informointi	Yleissopimus 108, 8 artiklan alakohta
Tietosuojadirektiivi, 10 ja 11 artikla	Poikkeukset informointivelvollisuudesta	Yleissopimus 108, 9 artikla
Tietosuojadirektiivi, 18 ja 19 artikla	Ilmoitusmenettely	Profilointia koskeva suositus, 9 artiklan 2 kohdan alakohta
<b>Sääntöjen noudattamista edistävät säännöt</b>		
Tietosuojadirektiivi, 20 artikla	Ennakotarkastus	
Tietosuojadirektiivi, 18 artiklan 2 kohta	Henkilötietojen suojaamisesta vastaavat henkilöt	Profilointia koskeva suositus, 8 artiklan 3 kohta
Tietosuojadirektiivi, 27 artikla	Käytännösäännöt	

Periaatteet ovat väistämättä yleisluonteisia. Niiden soveltamisessa konkreettisiin tapauksiin on tiettyä tulkinnan varaa ja vapautta keinojen valinnassa. **EN-oikeudessa** on jätetty yleissopimuksen 108 osapuolille tehtäväksi rajata kansallisessa lainsäädännössä tätä tulkinnan varaa. **EU-oikeudessa** tilanne on toinen: tietosuojan turvaamiseksi sisämarkkinoilla on katsottu, että EU:n tasolla tarvitaan

yksityiskohtaisia sääntöjä, joilla yhdenmukaistetaan tietosuojan tasoa jäsenvaltioiden kansallisissa lainsäädännöissä. Tietosuojadirektiivissä säädetään 6 artiklassa esitettyjen periaatteiden yhteydessä yksityiskohtaisia sääntöjä, jotka on pantava tarkasti täytäntöön kansallisessa lainsäädännössä. Seuraavat huomiot Euroopassa sovellettavista yksityiskohtaisista tietosuojasäännöistä liittyvät näin ollen lähinnä EU:n lainsäädäntöön.

## 4.1. Laillista käsittelyä koskevat säännöt

### Keskeiset kohdat

- Henkilötietoja voidaan käsitellä laillisesti, jos
  - käsittely perustuu rekisteröidyn suostumukseen; tai
  - rekisteröityjen elintärkeät edut edellyttävät heidän henkilötietojensa käsittelyä; tai
  - käsittelyn syynä ovat muiden henkilöiden oikeutetut edut, mutta vain siinä tapauksessa, että ne eivät ole ristiriidassa rekisteröityjen perusoikeuksien suojaan liittyvien etujen kanssa.
- Arkaluonteisten henkilötietojen laillisessa käsittelyssä on noudatettava erikseen määriteltä, tiukempaa menettelyä.

Tietosuojadirektiivi sisältää kahdenlaisia sääntöjä henkilötietojen laillista käsittelyä varten: 7 artiklassa esitetään ne säännöt, jotka koskevat muita kuin arkaluonteisia tietoja, ja 8 artiklassa ne, jotka koskevat arkaluonteisia tietoja.

### 4.1.1. Muiden kuin arkaluonteisten tietojen laillinen käsittely

Direktiivin 95/46 II luvussa, jonka otsikko on ”yleiset säännöt henkilötietojen käsittelyn laillisuudesta”, säädetään, että jollei sen 13 artiklassa säädetystä poikkeuksesta muuta johdu, henkilötietojen käsittelyssä on noudatettava toisaalta tietojen laatua koskevia periaatteita, jotka mainitaan direktiivin 6 artiklassa, ja toisaalta

tietojenkäsittelyn laillisuutta koskevia periaatteita, jotka luetellaan sen 7 artiklassa.<sup>130</sup> Muiden kuin arkaluonteisten henkilötietojen käsittely on näissä puitteissa laillista.

## Suostumus

**EN-oikeudessa** suostumusta ei mainita EIS:n 8 artiklassa tai yleissopimuksessa 108. Se mainitaan kuitenkin EIT:n oikeuskäytännössä ja useissa Euroopan neuvoston suosituksissa. **EU-oikeudessa** suostumus on selkeästi vahvistettu henkilötietojen laillisen käsittelyn perusteeksi tietosuojadirektiivin 7 artiklan a alakohdassa, ja lisäksi se mainitaan perusoikeuskirjan 8 artiklassa.

## Sopimussuhde

**EU-oikeudessa** toinen peruste henkilötietojen lailliselle käsittelylle on tietosuojadirektiivin 7 artiklan b alakohdan mukaan se, ”jos käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena”. Tämä säännös kattaa myös sopimusta edeltävän suhteen. Otetaan esimerkiksi tilanne, jossa osapuoli aikoo tehdä sopimuksen, muttei ole vielä tehnyt sitä, mahdollisesti siksi, että hän haluaa vielä tarkistaa joitakin asioita. Jos yhden osapuolen on käsiteltävä henkilötietoja tätä tarkoitusta varten, käsittely on laillista, kunhan se tapahtuu ”sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä”.

**EN-oikeudessa** EIS:n 8 artiklan 2 kohdassa mainitaan ”muiden henkilöiden oikeuksien ja vapauksien turvaaminen” perusteena lailliselle puuttumiselle tietosuojaajaa koskevaan oikeuteen.

## Rekisterinpitäjän lailliset velvoitteet

**EU-oikeuden** mukaan toinen peruste, jolla henkilötietojen käsittely voi olla laillista, on se, ”jos käsittely on tarpeen rekisterinpitäjän laillisen velvoitteen noudattamiseksi” (tietosuojadirektiivin 7 artiklan c alakohta). Tällä säännöksellä viitataan yksityisellä sektorilla toimiviin rekisterinpitäjiin; julkisella sektorilla toimivien rekisterinpitäjien laillisista velvoitteista säädetään tietosuojadirektiivin 7 artiklan e alakohdassa.

<sup>130</sup> Yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, *Rechnungshof v. Österreichischer Rundfunk ym. sekä Neukomm ja Lauer mann v. Österreichischer Rundfunk*, EYTI 20.5.2003, 65 kohta; asia C-524/06, *Huber v. Saksa*, EYTI 16.12.2008, 48 kohta; yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, EUTI 24.11.2011, 26 kohta.

Yksityisellä sektorilla toimivilla rekisterinpitäjillä on monissa tilanteissa lakisääteinen velvollisuus käsitellä henkilötietoja; esimerkiksi lääkäreillä ja sairaaloilla on laillinen velvoite säilyttää potilaiden hoitotietoja monta vuotta, työnantajien on käsiteltävä työntekijöidensä henkilötietoja sosiaaliturvaan ja verotukseen liittyvistä syistä, ja yritysten on käsiteltävä asiakkaidensa henkilötietoja verotusta varten.

Lentoyhtiöiden velvollisuus luovuttaa matkustajatietoja vieraan maan maahanmuuttoviranomaisille nosti esiin kysymyksen siitä, voivatko *vieraan maan* lainsäädännössä asetetut lailliset velvoitteet muodostaa EU-oikeuden mukaisen oikeudellisen perusteen henkilötietojen käsittelylle (tätä kysymystä käsitellään tarkemmin [6.2 kohdassa](#)).

Rekisterinpitäjän lailliset velvoitteet toimivat myös **EN-oikeudessa** perusteena henkilötietojen lailliselle käsittelylle. Kuten edellä on todettu, yksityisellä sektorilla toimivan rekisterinpitäjän lailliset velvoitteet ovat vain yksi EIS:n 8 artiklan 2 kohdassa tarkoitetuista muiden henkilöiden oikeutetuista eduista. Edellä esitetty esimerkki pätee näin ollen myös EN-oikeudessa.

## Rekisteröidyn elintärkeät edut

**EU-oikeudessa tietosuojadirektiivin** 7 artiklan d alakohdassa säädetään, että henkilötietojen käsittely on laillista, ”jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi”. Tällaiset edut, jotka liittyvät tiiviisti rekisteröidyn eloonjääntiin, voivat toimia esimerkiksi terveystietojen tai kadonneiden henkilöiden henkilötietojen laillisen käytön perusteena.

**EN-oikeudessa** EIS:n 8 artiklassa ei mainita rekisteröidyn elintärkeää etua perusteena lailliselle puuttumiselle tietosuojaa koskevaan oikeuteen. Joissakin EN:n suosituksissa, joilla yleissopimusta 108 on täydennetty tarkoin määritellyillä aloilla, rekisteröityjen elintärkeät edut mainitaan laillisen tietojenkäsittelyn perusteena.<sup>131</sup> Rekisteröityjen elintärkeiden etujen katsotaan selvästi sisältyvän henkilötietojen käsittelyn oikeuttaviin syihin: perusoikeuksien suojele ei saa koskaan vaarantaa suojelun kohteena olevien henkilöiden elintärkeitä etuja.

<sup>131</sup> Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta.

## Yleinen etu ja julkisen vallan käyttäminen

Kun otetaan huomioon, että julkiset asiat voidaan organisoida monella eri tavalla, tietosuojadirektiivin 7 artiklan e alakohdassa säädetään, että henkilötietoja voidaan käsitellä laillisesti ”jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan”.<sup>132</sup>

Esimerkki: Asiassa *Huber v. Saksa*<sup>133</sup> Saksassa asuva Itävallan kansalainen Heinz Huber pyysi liittotasavallan siirtolais- ja pakolaisvirastoa poistamaan häntä koskevat tiedot ulkomaalaisista pidettävästä keskusrekisteristä (AZR:stä). Tätä rekisteriä, jossa ovat niiden ulkomaalaisten henkilötiedot, jotka oleskelevat Saksassa yli kolmen kuukauden ajan, käytetään tilastollisiin tarkoituksiin ja silloin, kun lainvalvontaviranomaiset ja oikeusviranomaiset tutkivat rikollista tai yleisen turvallisuuden vaarantavaa toimintaa syytteen nostamista varten. Ennakkoratkaisua pyytänyt tuomioistuin kysyi, oliko EU:n lainsäädännön mukaista käsitellä henkilötietoja, jotka oli kerätty sellaiseen ulkomaalaisista pidettävän keskusrekisterin kaltaiseen rekisteriin, johon muillakin viranomaisilla oli pääsy, kun tällaista rekisteriä ei pidetty Saksan kansalaisista.

EYTI katsoi ensinnäkin, että direktiivin 7 artiklan e alakohdan nojalla henkilötietoja voidaan käsitellä laillisesti vain, jos se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi.

Tuomioistuin totesi seuraavaa: ”Kun otetaan huomioon tavoite taata vastaavatasoinen suoja kaikissa jäsenvaltioissa, direktiivin 95/46 7 artiklan e alakohdan mukainen tarpeellisuuden käsite – ei näin ollen voi olla sisällöltään erilainen eri jäsenvaltioissa. Tämän vuoksi kyse on yhteisön oikeuden itsenäisestä käsitteestä, jota on tulkittava siten, että se vastaa täysimääräisesti tämän direktiivin tavoitetta, joka on määritetty sen 1 artiklan 1 kohdassa.”<sup>134</sup>

Tuomioistuin toi esiin, että unionin kansalaisen oikeus oleskella vapaasti sellaisen jäsenvaltion alueella, jonka kansalainen hän ei ole, ei ole ehdoton vaan siihen voi liittyä perustamissopimuksessa määrättyjä ja sen soveltamisesta annetuissa säännöksissä säädettyjä rajoituksia ja ehtoja. Näin ollen vaikka

<sup>132</sup> Ks. myös tietosuojadirektiivi, johdanto-osan 32 kappale.

<sup>133</sup> Asia C-524/06, *Huber v. Saksa*, EYTI 16.12.2008.

<sup>134</sup> *Ibid.*, 52 kohta.

jäsenvaltiolla on periaatteessa tarjota AZR:n kaltainen rekisteri oleskeluoikeutta koskevan lainsäädännön soveltamisesta vastaavien viranomaisten tueksi, tällainen rekisteri ei voi sisältää muita tietoja kuin ne, jotka ovat tarpeen tähän tarkoitukseen. Tuomioistuin totesi, että tällainen henkilötietojen käsittelyjärjestelmä on EU:n lainsäädännön mukainen, jos se sisältää yksinomaan tiedot, jotka ovat tarpeen tämän lainsäädännön soveltamiseksi, ja jos sen keskitetyn luonteen avulla tätä lainsäädäntöä voidaan soveltaa tehokkaammin. Kansallisen tuomioistuimen oli kyseisessä tapauksessa varmistettava, täytyivätkö mainitut ehdot. Jos ehdot eivät täytyneet, henkilötietojen säilyttämistä ja käsittelyä AZR:n kaltaisen rekisterin puitteissa tilastollisiin tarkoituksiin ei voitu mitenkään pitää direktiivin 95/46/EY 7 artiklan e alakohdassa tarkoitettulla tavalla tarpeellisenä.<sup>135</sup>

Lopuksi kysymykseen rekisterin sisältämien tietojen käytöstä rikollisuuden torjunnassa tuomioistuin vastasi, että tähän tavoitteeseen ”kuuluu väistämättä syytteiden nostaminen tehdyistä rikoksista ja rikkomuksista tekijöiden kansalaisuudesta riippumatta”. Kiistanalainen rekisteri ei sisältänyt asianomaisen jäsenvaltion kansalaisten henkilötietoja, ja tällainen eriarvoinen kohtelu oli SEUT 18 artiklassa kiellettyä syrjintää. Näin ollen kyseistä määräystä oli tuomioistuimen mukaan tulkittava siten, että sen ”vastaista on se, että jäsenvaltio ottaa rikollisuuden torjumiseksi käyttöön henkilötietojen käsittelyjärjestelmän, joka koskee ainoastaan unionin kansalaisia, jotka eivät ole tämän jäsenvaltion kansalaisia”.<sup>136</sup>

Henkilötietojen käyttöön viranomaisten julkisissa tehtävissä sovelletaan myös EIS:n 8 artiklaa.

## Rekisterinpitäjän tai sivullisen oikeutetut edut

Rekisteröity ei ole ainoa, jolla on oikeutettuja etuja. Tietosuojadirektiivin 7 artiklan f alakohdassa säädetään, että henkilötietoja voidaan käsitellä laillisesti, jos ”käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn – suoja tarvitsevat intressit ja perusoikeudet ja -vapaudet”.

<sup>135</sup> *Ibid*, 54, 58, 59, 66–68 kohta.

<sup>136</sup> *Ibid*, 78 ja 81 kohta.

Seuraavassa tuomiossa EUTI otti yksiselitteisesti kantaa direktiivin 7 artiklan f alakohtaan:

Esimerkki: Asiassa *ASNEF ja FECEMD*<sup>137</sup> EUTI selvensi, että kansallisessa lainsäädännössä ei saa asettaa henkilötietojen lailliselle käsittelylle muita edellytyksiä kuin ne, jotka mainitaan direktiivin 7 artiklan f alakohdassa. Käsiteltävänä olleessa tilanteessa Espanjan tietosuojalainsäädäntö sisälsi säännöksen, jonka mukaan sivulliset saattoivat vedota oikeutettuun etuunsa henkilötietojen käsittelyssä vain, jos tiedot olivat jo yleisön saatavilla olevissa lähteissä.

Tuomioistuin toi ensin esiin, että direktiivillä 95/46 pyritään saattamaan henkilöiden oikeuksien ja vapauksien suoja henkilötietojen käsittelyssä samalle tasolle kaikissa jäsenvaltioissa. Alalla sovellettavien kansallisten lainsäädäntöjen lähentäminen ei saa johtaa lainsäädännöllä turvattavan tietosuojan heikentymiseen. Sillä on päinvastoin varmistettava tietosuojan korkea taso unionissa.<sup>138</sup> Näin ollen EUTI totesi, että ”tavoitteesta taata kaikissa jäsenvaltioissa suojan saattaminen samalle tasolle johtuu siten, että direktiivin 95/46 7 artiklaan on otettu tyhjentävä luettelo, johon on rajattu tilanteet, joissa henkilötietojen käsittelyyn voidaan katsoa olevan laillista”. Lisäksi ”jäsenvaltiot eivät voi lisätä direktiivin 95/46 7 artiklaan uusia henkilötietojen käsittelyn laillistamista koskevia periaatteita eivätkä säättää lisävaatimuksista, joilla muutettaisiin jonkin niiden kuuden periaatteen ulottuvuutta, joista tässä artiklassa on säädetty”.<sup>139</sup> Tuomioistuin myönsi, että ”direktiivin 95/46 7 artiklan f alakohdan edellyttämää punnitsemista varten voidaan ottaa huomioon se, että rekisteröidyn perusoikeuksiin häntä koskevien tietojen käsittelyn vuoksi kohdistuvan loukkauksen vakavuus voi vaihdella sen mukaan, ovatko kyseessä olevat tiedot mahdollisesti jo yleisön saatavilla olevassa lähteessä”.

Se kuitenkin jatkoi toteamalla, että ”direktiivin 95/46 7 artiklan f alakohda on esteenä sille, että jäsenvaltio sulkee ehdottomasti ja yleisesti pois mahdollisuuden käsitellä tiettyihin tietoryhmiin kuuluvia henkilötietoja sallimatta niiden

137 Yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado*, EUTI 24.11.2011.

138 *Ibid.*, 28 kohta. Ks. tietosuojadirektiivi, johdanto-osan 8 ja 10 kappale.

139 Yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, EUTI 24.11.2011, 30 ja 32 kohta.



oikeuksien ja intressien punnitsemista, joista on kyse tietyssä yksittäisessä tapauksessa”.

Näiden näkökohtien perusteella tuomioistuin päätyi siihen johtopäätökseen, että ”direktiivin 95/46 7 artiklan f alakohtaa on tulkittava siten, että se on esteenä kansalliselle lainsäädännölle, jonka mukaan silloin, kun rekisteröidyn suostumusta ei ole saatu, henkilötietojen käsittely, joka on tarpeen rekisterinpitäjän tai sivullisen, jolle tiedot on luovutettu, oikeutettujen intressien toteuttamiseksi, edellyttää rekisteröidyn perusoikeuksien ja vapauksien kunnioittamisen lisäksi sitä, että henkilötiedot ovat yleisön saatavilla olevissa lähteissä, ja jolla suljetaan näin ehdottomasti ja yleisesti pois mahdollisuus käsitellä tietoja, jotka eivät ole tällaisissa yleisön saatavilla olevissa lähteissä”<sup>140</sup>

EN:n suosituksissa esitetään samansuuntaisia päätelmiä. Profilointia koskevassa suosituksessa katsotaan, että henkilötietojen käsittely profilointia varten on laillista, jos se on välttämätöntä muiden henkilöiden oikeutettujen etujen suojaamiseksi paitsi silloin, kun rekisteröityjen perusoikeudet ja vapaudet on asetettava näiden etujen edelle.<sup>141</sup>

## 4.1.2. Arkaluonteisten tietojen laillinen käsittely

**EN-oikeudessa** asianmukaisen suojan vahvistaminen arkaluonteisten henkilötietojen käytölle on jätetty kansallisen lainsäädännön asiaksi, kun taas **EU-oikeudessa** tietosuojadirektiivin 8 artikla sisältää yksityiskohtaiset säännöt sellaisten tietojen käsittelyyn, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta tai ammattiliittoon kuulumista, sekä terveyteen ja seksuaaliseen käyttäytymiseen liittyvien tietojen käsittelyyn. Arkaluonteisten henkilötietojen käsittely on periaatteessa kiellettyä.<sup>142</sup> Kieltoon on kuitenkin lueteltu tyhjentävästi poikkeuksia direktiivin 8 artiklan 2 ja 3 kohdassa. Poikkeuksiin kuuluvat rekisteröidyn nimenomainen suostumus, rekisteröidyn elintärkeät edut, muiden henkilöiden oikeutetut edut sekä yleinen etu.

Toisin kuin niiden henkilötietojen kohdalla, jotka eivät ole arkaluonteisia, sopimusuhdetta rekisteröidyn kanssa ei pidetä yleisenä perusteena arkaluonteisten tietojen lailliselle käsittelylle. Jos henkilötietoja käsitellään rekisteröidyn kanssa tehdyn

<sup>140</sup> *Ibid.*, 40, 44, 48 ja 49 kohta.

<sup>141</sup> Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta.

<sup>142</sup> Tietosuojadirektiivi, 8 artiklan 1 kohta.

sopimuksen perusteella, arkaluonteisten tietojen käsittelyyn on saatava rekisteröidyn erillinen nimenomainen suostumus. Rekisteröidyn nimenomainen pyyntö sellaisten tavaroiden tai palveluiden tilaamista tai ostamista, jotka väistämättä paljastavat arkaluonteista tietoa, on katsottava vastaavan nimenomaista suostumusta.

Esimerkki: Jos lentoyhtiön matkustaja pyytää lennon varauksen yhteydessä pyörätuolia tai kosher-ateriaa, lentoyhtiö saa käyttää tätä tietoa, vaikka matkustaja ei olisi allekirjoittanut erillistä suostumuslauseketta, jolla hän hyväksyy hänen terveyttään tai uskonnollista vakaumustaan koskevan tiedon käytön.

## Rekisteröidyn nimenomainen suostumus

Rekisteröidyn suostumus mainitaan ensimmäiseksi henkilötietojen laillisen käsittelyn edellytyksenä, riippumatta siitä ovatko tiedot arkaluonteisia vai eivät. Arkaluonteisten tietojen kohdalla tämän suostumuksen on oltava nimenomainen. Kansallisessa lainsäädännössä voidaan kuitenkin säätää, että suostuminen arkaluonteisten henkilötietojen käsittelyyn ei riitä näiden tietojen käsittelyn oikeudelliseksi perusteeksi<sup>143</sup> esimerkiksi silloin, kun käsittelystä aiheutuu rekisteröidylle erityisiä riskejä.

Yhdessä erityistilanteessa voidaan arkaluonteisten henkilötietojen käsittelyn oikeudelliseksi perusteeksi hyväksyä jopa implisiittinen suostumus: direktiivin 8 artiklan 2 kohdan e alakohdassa säädetään, että käsittely ei ole kiellettyä, jos se koskee tietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi. Tässä säännöksessä selkeästi oletetaan, että sen, että rekisteröity saattaa tietonsa julkisiksi, voidaan tulkitä tarkoittavan, että hän suostuu näiden tietojen käyttöön.

## Rekisteröidyn elintärkeät edut

Muiden tietojen tavoin myös arkaluonteisia tietoja voidaan käsitellä, kun rekisteröidyn elintärkeät edut sitä edellyttävät.<sup>144</sup>

Jotta arkaluonteisia henkilötietoja voitaisiin käsitellä laillisesti tällä perusteella, on rekisteröidyn täytynyt olla mahdotonta itse päättää asiasta esimerkiksi siksi, että hän on ollut tajuton tai poissa paikalta ja tavoittamattomissa.

143 *Ibid.*, 8 artiklan 2 kohdan a alakohta.

144 *Ibid.*, 8 artiklan 2 kohdan c alakohta.

## Muiden oikeutetut edut

Kuten muiden tietojen myös arkaluonteisten tietojen laillisen käsittelyn perusteena voivat olla muiden henkilöiden oikeutetut edut. Tietosuojadirektiivin 8 artiklan 2 kohdan mukaan tämä on arkaluonteisten tietojen kohdalla kuitenkin mahdollista vain seuraavissa tapauksissa:

- käsittely on tarpeen jonkun toisen henkilön elintärkeiden etujen suojaamiseksi,<sup>145</sup> jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan;
- arkaluonteisia henkilötietoja on käytettävä työoikeuden alalla, esimerkiksi terveystietoja voidaan tarvita vaarallisella työpaikalla tai uskonnollista vakaumusta koskevia tietoja lomien järjestämisessä;<sup>146</sup>
- poliittinen, filosofinen, uskonnollinen tai ammattiliittotoimintaan liittyvä säätiö, yhdistys tai muu voittoa tavoittelematon yhteisö käsittelee jäseniään, rahoittajiaan tai muita sidosryhmiä koskevia tietoja (tällaiset tiedot ovat arkaluonteisia siksi, että ne saattavat paljastaa asianomaisten henkilöiden uskonnollisen tai poliittisen vakaumuksen);<sup>147</sup>
- arkaluonteisia henkilötietoja käsitellään tuomioistuimen tai hallintoviranomaisen toimesta oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.<sup>148</sup>
- Lisäksi tietosuojadirektiivin 8 artiklan 3 kohdan nojalla myös terveydenhuolto- ja hoitoa varten kuuluu poikkeuksen piiriin. Erityisenä suojatoimena on säädetty, että terveydenhuolto- ja hoito- palvelujen tarjoajiksi tunnustetaan vain henkilöt, joita koskee salassapitovelvollisuus.

145 *Ibid.*

146 *Ibid.*, 8 artiklan 2 kohdan b alakohta.

147 *Ibid.*, 8 artiklan 2 kohdan d alakohta.

148 *Ibid.*, 8 artiklan 2 kohdan e alakohta.

## Yleinen etu

Tietosuojadirektiivin 8 artiklan 4 kohdan mukaan jäsenvaltiot voivat lisäksi määrittellä muita tarkoituksia, joihin arkaluonteisia henkilötietoja on mahdollista käsitellä, kunhan

- tietoja käsitellään tärkeää yleistä etua koskevasta syystä; ja
- siitä säädetään kansallisella lailla tai valvontaviranomaisen päätöksellä; ja
- kansallinen laki tai valvontaviranomaisen päätös sisältää tarvittavat suojatoimet rekisteröityjen etujen tehokasta turvaamista varten.<sup>149</sup>

Tärkeä esimerkki tällaisesta ovat sähköiset potilastietojärjestelmät, joita monissa jäsenvaltioissa ollaan ottamassa käyttöön. Näiden järjestelmien avulla terveydenhuoltopalvelujen tarjoaja voi saattaa potilaan hoidon yhteydessä keräämänsä terveystiedot muiden samalle potilaalle terveydenhuoltopalveluja tarjoavien toimijoiden saataville laajassa mittakaavassa, yleensä valtakunnallisesti.

Tietosuojatyöryhmä totesi, ettei sähköisiä potilastietojärjestelmiä voinut ottaa käyttöön potilastietojen käsittelyä säännelleen tietosuojadirektiivin 8 artiklan 3 kohtaan perustuneiden oikeussääntöjen nojalla. Jos kuitenkin oletetaan, että tällaisten sähköisten järjestelmien olemassaolo muodostaa tärkeän yleisen edun, niiden käyttöönoton perustana voitaisiin käyttää direktiivin 8 artiklan 4 kohtaa, jossa edellytetään nimenomaista oikeudellista perustetta sekä tarvittavia suojatoimia järjestelmän turvallisen toiminnan varmistamiseksi.<sup>150</sup>

---

<sup>149</sup> *Ibid.*, 8 artiklan 4 kohta.

<sup>150</sup> Tietosuojatyöryhmä (2007), *valmisteluasiakirja potilastietojen käsittelystä sähköisissä potilastietokannoissa*, WP 131, Bryssel, 15. helmikuuta 2007.

## 4.2. Käsittelyn turvallisuutta koskevat säännöt

### Keskeiset kohdat

- Käsittelyn turvallisuutta koskevat säännöt asettavat rekisterinpitäjälle ja henkilötietojen käsittelijälle velvollisuuden toteuttaa asianmukaista tekniset ja organisatoriset toimenpiteet, joilla ehkäistään luvaton puuttuminen henkilötietojen käsittelytoimiin.
- Tietoturvan riittävä taso määräytyy seuraavien perusteella:
  - markkinoilla tietynlaista käsittelyä varten saatavilla olevat turvatoiminnot; ja
  - kustannukset; ja
  - käsiteltävien tietojen arkaluonteisuus.
- Tietojen turvallista käsittelyä edistää vielä kaikkien henkilöiden, niin rekisterinpitäjien kuin henkilötietojen käsittelijöidenkin, yleinen velvollisuus varmistaa tietojen säilyminen luottamuksellisina.

Rekisterinpitäjien ja henkilötietojen käsittelijöiden velvollisuus toteuttaa asianmukaiset toimenpiteet tietoturvan varmistamiseksi onkin vahvistettu sekä **EN:n tietosuoja-säännöksissä** että **EU:n tietosuoja-säännöksissä**.

### 4.2.1. Tietoturvaan liittyvät näkökohdat

**EU:n lainsäädännössä** asiasta säädetään seuraavaa:

*”Jäsenvaltioiden on säädettävä siitä, että rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta, erityisesti jos käsittely muodostuu tietojen siirtämisestä verkossa, sekä kaikelta muulta laittomalta käsittelyltä.”<sup>151</sup>*

<sup>151</sup> Tietosuojadirektiivi, 17 artiklan 1 kohta.

**EN:n lainsäädännössä** on olemassa vastaavanlainen määräys:

*”Automaattisesti käsiteltäviin rekistereihin talletettujen henkilötietojen suojelemiseksi vahingossa tapahtuvalta tai luvattomalta tuhoamiselta tai vahingossa tapahtuvalta katoamiselta samoin kuin luvattoman tiedostoon pääsyn, tiedoston muuttamisen tai levittämisen varalta on ryhdyttävä asianmukaisiin turvatoimiin.”<sup>152</sup>*

Tietojen turvallista käsittelyä varten on myös laadittu useita toimialakohtaisia, kansallisia tai kansainvälisiä standardeja. Esimerkiksi eurooppalainen yksityisyyden suojaa koskeva tunnus (EuroPriSe) on Euroopan laajuisia televerkkoja koskeva (eTEN) hanke, jossa on tutkittu mahdollisuuksia sertifioida tuotteita, erityisesti ohjelmistoja, jotka täyttävät Euroopan tietosuojaoikeuden vaatimukset. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) perustettiin parantamaan EU:n, sen jäsenvaltioiden ja sen yritysmaailman mahdollisuuksia ehkäistä, käsitellä ja ratkaista verkko- ja tietoturvaongelmia.<sup>153</sup> ENISA julkaisee säännöllisesti analyyskejä uusista turvauhista ja ohjeita niiden käsittelemiseen.

Tietoturvaa ei saavuteta pelkästään oikeilla välineillä – laitteistoilla ja ohjelmistoilla. Siihen tarvitaan myös asianmukaiset organisaation sisäiset säännöt. Tällaisten sääntöjen olisi hyvä kattaa seuraavat asiat:

- säännöllinen tiedottaminen kaikille työntekijöille tietoturvasäännöistä ja heille tietosuoja-säännösten nojalla kuuluvista velvollisuuksista, erityisesti velvollisuudesta säilyttää tietojen luottamuksellisuus;
- selkeä vastuunjako ja selkeästi määritellyt valtuudet käsitellä henkilötietoja, erityisesti koskien päätöksiä henkilötietojen käsittelystä ja luovuttamisesta sivullisille;
- henkilötietojen käyttäminen käsittelemisen ainoastaan toimivaltaisen henkilön ohjeiden tai yleisesti sovittujen sääntöjen mukaisesti;

<sup>152</sup> Yleissopimus 108, 7 artikla.

<sup>153</sup> Euroopan parlamentin ja neuvoston asetukset (EY) N:o 460/2004, annettu 10 päivänä maaliskuuta 2004, Euroopan verkko- ja tietoturvaviraston perustamisesta, EUVL 2004 L 77.

- rekisterinpitäjän tai henkilötietojen käsittelijän tiloihin sekä laitteistoihin ja ohjelmistoihin pääsyn rajaaminen ja suojaaminen, mukaan lukien pääsyn luvallisuuden tarkistaminen;
- sen varmistaminen, että toimivaltainen henkilö on antanut luvan käsitellä henkilötietoja ja, että luvat dokumentoidaan asianmukaisesti;
- henkilötietojen sähköisen käytön automaattiset yhteyskäytännöt ja niiden säännölliset tarkistukset sisäisen valvontapalvelun toimesta;
- muiden tietojen luovuttamisen muotojen kuin automaattisen tietoihin pääsyn huolellinen dokumentointi sen todistamiseksi, ettei tietoja ole siirretty laittomasti.

Myös riittävän tietoturvakoulutuksen tarjoaminen henkilöstölle on tärkeä osa tehokkaita turvatoimia. Tarkistusmenettelyillä (kuten sisäisillä tai ulkoisilla tarkastuksilla) on varmistettava, että asianmukaiset toimenpiteet toteutuvat ja niitä noudatetaan.

Toimenpiteisiin, joilla rekisterinpitäjät tai henkilötietojen käsittelijät voivat parantaa turvallisuutta, kuuluvat muun muassa tietosuojavastaavan nimeäminen, työntekijöiden turvakoulutus, säännölliset tarkastukset, läpäisytestaus sekä laatua koskevat tunnukset.

Esimerkki: Asiassa *I. v. Suomi*<sup>154</sup> kantaja ei ollut pystynyt todistamaan, että muut työntekijät siinä sairaalassa, jossa hän työskenteli, olivat käyneet katsomassa hänen potilastietojaan. Näin ollen kansalliset tuomioistuimet hylkäsivät hänen väitteensä yksityiselämän suojaa koskevan oikeuden rikkomisesta. EIT kuitenkin katsoi, että EIS:n 8 artiklaa oli rikottu, sillä sairaalan potilastietojen rekisterijärjestelmästä ei voinut takautuvasti selvittää potilasasiakirjojen käyttöä, vaan järjestelmä näytti ainoastaan viisi viimeisintä käyttäjää ja tämäkin tieto poistui, kun asiakirja palautettiin arkistoon. Tuomioistuimen näkemyksen mukaan ratkaisevaa oli se, että sairaalassa käytössä ollut rekisterijärjestelmä ei selvästikään ollut vastannut kansallisen lain vaatimuksia, mitä kansalliset tuomioistuimet eivät olleet riittävästi painottaneet.

154 Asia nro 20511/03, *I. v. Suomi*, EIT 17.7.2008.

## Tietoturvaloukkauksesta ilmoittaminen

Useiden Euroopan maiden tietosuojalainsäädäntöön on lisätty uusi säännös, jolla puututaan tietoturvaloukkauksiin ja joka velvoittaa sähköisten viestintäpalvelujen tarjoajat ilmoittamaan tietoturvaloukkauksista niiden todennäköisille uhreille ja valvontaviranomaisille. Televiestintäpalvelujen tarjoajille tämä on pakollista EU:n lainsäädännön nojalla.<sup>155</sup> Tietoturvaloukkauksista ja niiden mahdollisista seurauksista ilmoittamisella on tarkoitus minimoida rekisteröidyille aiheutuvien vahinkojen riskiä. Vakavista laiminlyönneistä voidaan myös määrätä sakkoja palveluntarjoajille.

Tietoturvaloukkausten tehokkaaseen hallinnointiin ja raportointiin on luotava hyvissä ajoin sisäiset menettelyt, sillä aikaraja ilmoitusten tekemiselle rekisteröidyille ja/tai valvontaviranomaisille on kansallisessa lainsäädännössä yleensä melko lyhyt.

### 4.2.2. Luottamuksellisuus

**EU-oikeudessa** tietojen turvallista käsittelyä edistää vielä kaikkien henkilöiden, niin rekisterinpitäjien kuin henkilötietojen käsittelijöidenkin, yleinen velvollisuus varmistaa tietojen säilyminen luottamuksellisina.

Esimerkki: Vakuutusyhtiön työntekijä saa työpaikallaan puhelun henkilöltä, joka väittää olevansa asiakas ja joka haluaa saada tietoa vakuutus sopimuksestaan.

Velvollisuus säilyttää asiakkaiden tiedot luottamuksellisina edellyttää, että työntekijä toteuttaa ainakin vähimmäisturvatoimet ennen henkilötietojen paljastamista. Sen voi tehdä esimerkiksi ehdottamalla soittamista takaisin asiakastiedoissa olevaan puhelinnumeroon.

Tietosuodirektiivin 16 artikla käsittelee luottamuksellisuutta ainoastaan rekisterinpitäjän ja henkilötietojen käsittelijän välisessä suhteessa. Rekisterinpitäjien

<sup>155</sup> Ks. [Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY](#), annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (*sähköisen viestinnän tietosuojadirektiivi*), EYVL 2002 L 201, 4 artiklan 3 kohta, siten kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EYC, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja palvelujen alalla, EUVL 2009 L 337; ks. myös [direktiivi 2002/58/EY](#) henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän sekä alalla asetus (EY) N:o 2006/2004 kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä.



velvollisuutta säilyttää tietojen luottamuksellisuus siinä mielessä, että ne eivät saa luovuttaa tietoja sivullisille, käsitellään direktiivin 7 ja 8 artiklassa.

Salassapitovelvollisuus ei kata tilanteita, joissa henkilö saa tiedon yksityishenkilönä eikä rekisterinpitäjän tai henkilötietojen käsittelijän työntekijänä. Tällaisessa tilanteessa tietosuojadirektiivin 16 artiklaa ei sovelleta, koska yksityishenkilöiden suorittama henkilötietojen käsittely jää kokonaan direktiivin soveltamisalan ulkopuolelle silloin, kun sen katsotaan kuuluvan kotitaloutta koskevan poikkeuksen piiriin.<sup>156</sup> Kotitaloutta koskevalla poikkeuksella tarkoitetaan henkilötietojen käsittelyä, jonka ”luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa”.<sup>157</sup> EYTI:n asiassa *Bodil Lindqvist*<sup>158</sup> antaman ratkaisun jälkeen tätä poikkeusta on kuitenkin pitänyt tulkita suppeasti, erityisesti tietojen luovuttamisen yhteydessä. Kotitaloutta koskeva poikkeus ei etenäkään kata henkilötietojen julkaisemista internetissä rajoittamattomalle määrälle vastaanottajia (asiaa käsitellään tarkemmin 2.1.2, 2.2, 2.3.1 ja 6.1 kohdassa).

**EN-oikeudessa** luottamuksellisuuden säilyttämistä koskeva velvollisuus sisältyy implisiittisesti tietoturvan käsitteeseen yleissopimuksen 108 7 artiklassa, joka koskee tietoturvaa.

Henkilötietojen käsittelijöiden osalta luottamuksellisuudella tarkoitetaan, että ne voivat käsitellä rekisterinpitäjän niille luovuttamia henkilötietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti. Rekisterinpitäjän tai henkilötietojen käsittelijän työntekijöiden kohdalla luottamuksellisuus edellyttää, että he noudattavat henkilötietojen käytössä toimivaltaisten esimiestensä ohjeita.

Salassapitovelvollisuus on sisällytettävä kaikkiin rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä tehtäviin sopimuksiin. Lisäksi rekisterinpitäjien ja henkilötietojen käsittelijöiden on toteutettava erityisiä toimenpiteitä, joilla ne määräävät työntekijänsä salassapitovelvollisiksi. Yleensä tämä tehdään sisällyttämällä työntekijän työsopimukseen salassapitolauseke.

Ammattitoimintaan liittyvän salassapitovelvollisuuden rikkominen on monissa EU:n jäsenvaltioissa ja yleissopimuksen 108 sopimusvaltioissa rikoslain nojalla rangaistava teko.

<sup>156</sup> Tietosuojadirektiivi, 3 artiklan 2 kohdan toinen luetelmakohta.

<sup>157</sup> *Ibid.*

<sup>158</sup> Asia C-101/01, *Bodil Lindqvist*, EUTI 6.11.2003.

## 4.3. Käsittelyn avoimuutta koskevat säännöt

### Keskeiset kohdat

- Ennen henkilötietojen käsittelyn aloittamista rekisterinpitäjän on vähintäänkin ilmoitettava rekisteröidyille rekisterinpitäjän henkilöllisyys ja tietojenkäsittelyn tarkoitus, ellei rekisteröity ole jo saanut näitä tietoja.
- Jos tiedot on kerätty sivullisilta, ilmoitusvelvollisuutta ei sovelleta, mikäli
  - tietojenkäsittelystä on säädetty lailla; tai
  - tietojen antaminen osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa.
- Ennen henkilötietojen käsittelyn aloittamista rekisterinpitäjän on lisäksi
  - ilmoitettava suunnitellut käsittelytoimet valvontaviranomaiselle; tai
  - pyydyttävä riippumatonta tietosuojavastaavaa dokumentoimaan käsittely sisäisesti, jos kansallisessa lainsäädännössä säädetään tällaisesta menettelystä.

Asianmukaisen käsittelyn periaate edellyttää käsittelyn avoimuutta. **EN-oikeudessa** määrätään tältä osin, että kenen tahansa henkilön on voitava selvittää automaattisesti käsiteltävän henkilörekisterin olemassaolo, sen päätarkoitukset samoin kuin rekisterinpitäjän henkilöllisyys.<sup>159</sup> Se, miten tämä saavutetaan, on määriteltävä kansallisessa lainsäädännössä. **EU-oikeudessa** asiaa käsitellään yksityiskohtaisemmin. Tietojen käsittelyn avoimuuden turvaamiseksi, rekisterinpitäjälle on asetettu yleinen informointivelvollisuus henkilötietojen käsittelystä.

Sekä EN -oikeudessa että EU -oikeudessa rekisterinpitäjän toiminnan avoimuutta koskeviin velvollisuuksiin voidaan säätää kansallisessa lainsäädännössä poikkeuksia ja rajoituksia, jos rajoittaminen on tarpeellista tiettyjen yleisten etujen tai rekisteröidyn tai muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi ja se on välttämätöntä demokraattisessa yhteiskunnassa.<sup>160</sup> Tällaiset poikkeukset voivat olla tarpeellisia esimerkiksi rikosten tutkinnan yhteydessä, mutta ne voivat olla perusteltuja muissakin tilanteissa.

<sup>159</sup> Yleissopimus 108, 8 artiklan a alakohhta.

<sup>160</sup> *Ibid.*, 9 artiklan 2 kohta; ja tietosuojadirektiivi, 13 artiklan 1 kohta.

### 4.3.1. Informointi

**Sekä EN-oikeudessa että EU-oikeudessa** rekisterinpitäjillä on velvollisuus informoida rekisteröityjä ennalta suunnittelemaansa henkilötietojen käsittelystä.<sup>161</sup> Tämä velvollisuus ei edellytä pyyntöä rekisteröidyltä, vaan rekisterinpitäjän on täytettävä velvollisuus oma-aloitteisesti riippumatta siitä, osoittaako rekisteröity kiinnostusta tähän tietoon vai ei.

#### Annettavien tietojen sisältö

Tietoihin on sisällyttävä käsittelyn tarkoitus sekä rekisterinpitäjän henkilöllisyys ja yhteystiedot.<sup>162</sup> Tietosuojadirektiivissä vaaditaan antamaan lisätietoja, kun ”lisätiedot ovat tarpeen ottaen huomioon erityiset olosuhteet, joissa tiedot kerätään, rekisteröidyn kannalta asianmukaisen tietojenkäsittelyn takaamiseksi”. Direktiivin 10 ja 11 artiklassa mainitaan muun muassa käsiteltävät tietoryhmät ja tietojen vastaanottajat sekä rekisteröidyn oikeus saada itseään koskevia tietoja ja oikeus niiden oikaisuun. Silloin kun tietoja kerätään rekisteröidyiltä, informoinnissa tulisi tarkentaa, onko kysymyksiin vastaaminen pakollista vai vapaaehtoista, sekä vastaamatta jättämisen mahdolliset seuraukset.<sup>163</sup>

**EN-oikeuden** näkökulmasta tällaista informointia voidaan pitää tietojen asianmukaisen käsittelyn periaatteen mukaisesti hyvänä käytäntönä, ja se kuuluu siltä osin EN-oikeuteen.

Asianmukaisen käsittelyn periaate edellyttää, että rekisteröityjen on helppo ymmärtää annetut tiedot. Informoinnissa on käytettävä vastaanottajille sopivaa kieltä. Kielen tasossa ja lajissa on otettava huomioon esimerkiksi, onko tieto suunnattu aikuisille vai lapsille, suurelle yleisölle vai akateemisille asiantuntijoille.

Jotkut rekisteröidyt haluavat saada vain lyhyen kuvauksen siitä, miten ja miksi heidän henkilötietojaan käsitellään, kun taas toiset tarvitsevat yksityiskohtaisemman selonteon. Sitä, miten nämä asianmukaisen informoinnin eri tasot saatetaan tasapainoon, käsitellään tietosuojatyöryhmän lausunnossa, jossa kannatetaan ajatusta

161 Yleissopimus 108, 8 artiklan a alakohta; ja tietosuojadirektiivi, 10 ja 11 artikla.

162 Yleissopimus 108, 8 artiklan a alakohta; ja tietosuojadirektiivi, 10 artiklan a ja b alakohta.

163 Tietosuojadirektiivi, 10 artiklan c alakohta.

niin kutsutuista monitasoisista ilmoituksista,<sup>164</sup> jotka jättävät rekisteröidylle vapauden valita, miten yksityiskohtaista tietoa hän haluaa saada.

## Informoinnin ajankohta

Tietosuojadirektiivissä on hieman erilaiset säännökset informoinnin ajoituksen osalta riippuen siitä, kerätäänkö tiedot rekisteröidyltä (10 artikla) vai muualta (11 artikla). Jos tiedot kerätään rekisteröidyltä, informoinnin on tapahduttava viimeistään keräämisen yhteydessä. Jos tiedot kerätään muualta, informoinnin on tapahduttava viimeistään joko silloin, kun rekisterinpitäjä rekisteröi tiedot, tai ennen kuin tietoja luovutetaan sivulliselle ensimmäisen kerran.

## Poikkeukset informointivelvollisuudesta

**EU-oikeudessa** velvollisuudesta informoida rekisteröityjä voidaan yleisesti poiketa silloin, kun rekisteröity on jo saanut tiedot.<sup>165</sup> Tällä viitataan tilanteisiin, joissa rekisteröity – tilanteen olosuhteiden mukaan – on jo tietoinen siitä, että tietty rekisterinpitäjä tulee käsittelemään hänen henkilötietojaan tiettyä tarkoitusta varten.

Tietosuojadirektiivin 11 artiklassa säädetään rekisteröityjen informoinnista silloin, kun tiedot kerätään muualta kuin rekisteröidyltä itseltään. Informointivelvollisuudesta voidaan poiketa, erityisesti tilanteessa jossa henkilötietoja käsitellään tilastollisia tarkoituksia tai historiallista tai tieteellistä tutkimustarkoitusta varten, jos:

- tietojen antaminen osoittautuu mahdottomaksi; tai
- se vaatii kohtuutonta vaivaa; tai
- lainsäädännössä nimenomaisesti säädetään tietojen tallentamisesta tai luovuttamisesta.<sup>166</sup>

Ainoastaan tietosuojadirektiivin 11 artiklan 2 kohdassa todetaan, että rekisteröityjä ei tarvitse informoida käsittelytoimista, jos niistä säädetään lainsäädännössä. Otettaessa huomioon yleinen oikeudellinen oletus siitä, että lain kohteena olevat

<sup>164</sup> Tietosuojatyöryhmä (2004), *lausunto 10/2004 yhtenäisemmistä informointia koskevista säännöksistä*, WP 100, Bryssel, 25. marraskuuta 2004.

<sup>165</sup> Tietosuojadirektiivi, 10 artikla ja 11 artiklan 1 kohta.

<sup>166</sup> *Ibid.*, johdanto-osan 40 kappale ja 11 artiklan 2 kohta.

henkilöt tuntevat lain sisällön, olisi mahdollista väittää, että, rekisteröity on saanut vaaditut tiedot, kun henkilötietoja kerätään suoraan rekisteröidyltä direktiivin 10 artiklan nojalla. Koska lain sisällön tuntemus on pelkkä oletus, asianmukaisen käsittelyn periaate edellyttää 10 artiklan yhteydessä, että rekisteröityä informoidaan, vaikka käsittelystä olisi säädetty laissa. Etenkin, kun henkilötiedot kerätään suoraan rekisteröidyltä, ei informointi vaadi kohtuutonta vaivaa.

**EN-oikeudessa** yleissopimuksessa 108 määrätään nimenomaisesti, milloin 8 artiklasta voidaan poiketa. Tässäkin tietosuojadirektiivin 10 ja 11 artiklan poikkeuksia voidaan pitää esimerkkeinä hyvästä käytännöstä yleissopimuksen 9 artiklan soveltamisessa.

## Erilaisia tapoja tarjota tietoa

lhanteellinen tapa tarjota tietoa olisi esittää se erikseen jokaiselle rekisteröidylle suullisesti tai kirjallisesti. Jos henkilötiedot kerätään rekisteröidyltä, informoinnin tulisi tapahtua tiedonkeruun yhteydessä. Silloin kun henkilötiedot kerätään muualta, informointi voidaan kuitenkin tehdä – ottaen huomioon ilmeinen vaikeus tavoittaa rekisteröidyt henkilökohtaisesti – julkaisemalla tiedot asianmukaisesti.

Yksi tehokkaimmista tavoista tarjota tietoa, on esittää rekisterinpitäjän kotisivulla asianmukaiset tiedotuslausekkeet, kuten sivuston tietosuojaseloste Yrityksen tai viranomaisen on kuitenkin tiedotuskäytäntöä laatiessaan otettava huomioon, että osa väestöstä ei käytä internetiä.

### 4.3.2. Ilmoitusmenettely

Kansallisessa lainsäädännössä voidaan velvoittaa rekisterinpitäjät ilmoittamaan toimivaltaiselle valvontaviranomaiselle käsittelytoimista siten, että ne voidaan julkaista. Vaihtoehtoisesti kansallisessa lainsäädännössä voidaan säätää, että rekisterinpitäjä voi tietosuojavastaavan, joka ylläpitää rekisteriä rekisterinpitäjän henkilötietojen käsittelyä sisältävistä prosesseista.<sup>167</sup> Tällainen sisäinen rekisteri on saatettava pyynnöstä yleisön nähtäville.

Esimerkki: Ilmoituksessa, samoin kuin sisäisen tietosuojavastaavan laatimassa dokumentoinnissa, on kuvailtava asianomaisen tietojenkäsittelyn pääpiirteet.

<sup>167</sup> *Ibid.*, 18 artiklan 2 kohdan toinen luettelukohta.

Niihin kuuluvat tiedot rekisterinpitäjästä, käsittelyn tarkoitus, käsittelyn oikeudellinen peruste, käsiteltävät tietoryhmät, todennäköiset sivulliset vastaanottajat ja tieto siitä, aiotaanko henkilötietoja siirtää kolmansiin maihin ja, jos aiotaan, niin miten.

Valvontaviranomaisen on julkaistava ilmoitukset erityisen rekisterin muodossa. Jotta rekisteri täyttäisi tavoitteensa, siihen pitäisi voida tutustua helposti ja ilmaiseksi. Sama koskee tietosuojavastaavan henkilön ylläpitämää dokumentaatiota.

Kansallisessa lainsäädännössä voidaan myöntää poikkeuksia velvollisuuteen tehdä ilmoitus toimivaltaiselle valvontaviranomaiselle sekä velvollisuuteen nimetä tietosuojavastaava silloin, kun käsittelytoimet eivät todennäköisesti aiheuta erityistä riskiä rekisteröidyille tietosuojadirektiivin 18 artiklan 2 kohdassa luetelluissa tilanteissa.<sup>168</sup>

## 4.4. Sääntöjenmukaisuuden edistämistä koskevat säännöt

### Keskeiset kohdat

- Vastuullisuusperiaatteeseen nojaten tietosuojadirektiivissä mainitaan useita erimenpiteitä joilla sääntöjenmukaisuutta voidaan edistää:
  - kansallinen valvontaviranomainen tarkastaa ennalta suunnitellut käsittelytoimet;
  - tietosuojavastaavat tarjoavat rekisterinpitäjälle erityistä asiantuntemusta tietosuojan alalla;
  - käytännesäännöt, joissa tarkennetaan voimassa olevat tietosuojasäännöt, joita sovelletaan tietyllä alalla, erityisesti liiketoiminnassa.
- EN-oikeudessa ehdotetaan profilointia koskevissa suosituksissa samankaltaisia välineitä sääntöjenmukaisuuden edistämiseen.

### 4.4.1. Ennakkotarkastus

Ennen kuin henkilötietojen käsittely voidaan aloittaa, tietosuojadirektiivin 20 artiklan mukaan valvontaviranomaisen on tarkastettava käsittelytoimet, joista saattaa

<sup>168</sup> *Ibid.*, 18 artiklan 2 kohdan ensimmäinen luetelmakohta.

aiheutua erityisiä riskejä rekisteröityjen oikeuksien ja vapauksien suhteen, joko käsittelyn tarkoituksen tai olosuhteiden vuoksi. Kansallisessa lainsäädännössä on määriteltävä, mitkä käsittelytoimet vaativat ennakkotarkastuksen. Tarkastus voi johtaa siihen, että käsittelytoimet kielletään tai että ehdotettuihin käsittelytoimiin määrätään muutoksia. Direktiivin 20 artiklalla pyritään varmistamaan, ettei tarpeettoman riskialtista käsittelyä edes aloiteta, ja siksi valvontaviranomaisella on valta estää sellaiset toimet. Tällaisen mekanismin tehokkaan toiminnan edellytyksenä on, että valvontaviranomaiselle todellakin ilmoitetaan käsittelytoimista. Jotta varmistettaisiin, että rekisterinpitäjät täyttävät ilmoitusvelvollisuutensa, valvontaviranomaisella on oltava käytössään pakkokeinoja, kuten mahdollisuus määrätä sakkoja rekisterinpitäjille.

Esimerkki: Jos yritys toteuttaa käsittelytoimia, jotka on kansallisen lainsäädännön mukaan alistettava ennakkotarkastukselle, yrityksen on esitettävä valvontaviranomaiselle asiakirjat suunnitelluista käsittelytoimista. Yritys ei saa aloittaa käsittelytoimia, ennen kuin se on saanut myönteisen vastauksen valvontaviranomaiselta.

Joidenkin jäsenvaltioiden kansallisessa lainsäädännössä säädetään vaihtoehtoisesti, että käsittelytoimet voidaan aloittaa, jos valvontaviranomainen ei ole vastannut tietyn ajan puitteissa, esimerkiksi kolmen kuukauden kuluessa.

## 4.4.2. Tietosuojavastaavat

Tietosuojadirektiivissä annetaan mahdollisuus säätää kansallisessa lainsäädännössä, että rekisterinpitäjät voivat nimetä henkilön toimimaan tietosuojavastaavana.<sup>169</sup> Tällaisen henkilön tehtävänä on varmistaa, että käsittelytoimet eivät loukkaa rekisteröityjen oikeuksia ja vapauksia.<sup>170</sup>

Esimerkki: Saksassa liittovaltion tietosuojalain (*Bundesdatenschutzgesetz*) 4f §:n 1 momentin mukaan yksityisten yritysten on nimettävä sisäinen tietosuojavastaava, jos ne työllistävät vakituisesti vähintään 10 henkilöä automaattisessa henkilötietojen käsittelyssä.

<sup>169</sup> *Ibid.*, 18 artiklan 2 kohdan toinen luettelukohta.

<sup>170</sup> *Ibid.*

Tavoitteen saavuttaminen edellyttää, että tietosuojavastaavalla on tietty itsenäisyys rekisterinpitäjän organisaatiossa, kuten direktiivissä yksiselitteisesti todetaan. Lisäksi tehtävän toteuttamiseen tarvitaan vahvat työntekijän oikeudet, jotka suojaavat esimerkiksi perusteettomalta irtisanomiselta.

Kansallisen tietosuojalain noudattamisen edistämiseksi tietosuojavastaavan käsite on otettu käyttöön myös joissakin EN:n suosituksissa.<sup>171</sup>

### 4.4.3. Käytännesäännöt

Sääntöjen noudattamisen edistämiseksi yritykset ja eri toimialat voivat laatia omia tyyppillisiä käsittelytoimiaan varten yksityiskohtaisia sääntöjä, jotka heijastavat parhaita käytäntöjä. Alan edustajien asiantuntemusta hyödyntäen voidaan löytää käytännönläheisiä ratkaisuja, joita myös todennäköisemmin toteutetaan. Jäsenvaltioita – ja Euroopan komissiota – kannustetaan edistämään käytännesääntöjen laatimista, jolla tuetaan jäsenvaltioiden direktiivin mukaisesti antamien kansallisten säännösten asianmukaista täytäntöönpanoa kunkin alan erityispiirteet huomioiden.<sup>172</sup>

Jäsenvaltioiden on vahvistettava menettely, jolla ne varmistavat, että käytännesäännöt ovat yhdenmukaiset tietosuojadirektiivin nojalla annettujen kansallisten säännösten kanssa. Menettelyyn tulisi ottaa mukaan kansallinen viranomainen, ammatinharjoittajien yhdistyksiä ja muita rekisterinpitäjryhmiä edustavia muita järjestöjä.<sup>173</sup>

Yhteisön sääntöluonnokset ja olemassa olevien yhteisön sääntöjen muutokset tai laajennukset voidaan esittää tietosuojatyöryhmän arvioitaviksi. Kun tietosuojatyöryhmä on hyväksynyt ne, Euroopan komissio voi taata käytännesäännöille asianmukaisen julkisuuden.<sup>174</sup>

Esimerkki: Euroopan suoramarkkinointiliitto (Federation of European Direct and Interactive Marketing, FEDMA) kehitti eurooppalaiset käytännesäännöt henkilötietojen käyttöön suoramarkkinoinnissa. Säännöt esitettiin

171 Ks. esim. profiilointia koskeva suositus, 8 artiklan 3 kohta.

172 Ks. tietosuojadirektiivi, 27 artiklan 1 kohta.

173 *Ibid.*, 27 artiklan 2 kohta.

174 *Ibid.*, 27 artiklan 3 kohta.



tietosuojatyöryhmälle, joka hyväksyi ne. Käytännösääntöihin lisättiin vuonna 2010 verkkomarkkinointia koskeva liite.<sup>175</sup>

---

175 Tietosuojatyöryhmä (2010), *lausunto 4/2010 henkilötietojen käyttöä suoramarkkinoinnissa koskevista Euroopan suoramarkkinointiliiton (FEDMA) eurooppalaisista käytännösäännöistä*, WP 174, Bryssel, 13. heinäkuuta 2010.



# 5

## Rekisteröityjen oikeudet ja niiden valvonta

EU	Katetut aiheet	EN
<b>Tiedonsaantioikeus</b>		
Tietosuojadirektiivi, 12 artikla <i>Asia C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, EYTI 7.5.2009</i>	<b>Tarkastusoikeus</b>	Yleissopimus 108, 8 artiklan b alakohta
	<b>Oikeus saada virheellinen tieto korjatuksi</b>	Yleissopimus 108, 8 artiklan c alakohta <i>Asia nro 22427/04, Cemalettin Canli v. Turkki, EIT 18.11.2008</i> <i>Asia nro 62332/00, Segerstedt-Wiberg ym. v. Ruotsi, EIT 6.6.2006</i> <i>Asia nro 27138/04, Ciubotaru v. Moldova, EIT 27.4.2010</i>
<b>Oikeus vastustaa henkilötietojen käsittelyä</b>		
Tietosuojadirektiivi, 14 artiklan 1 kohdan a alakohta	<b>Oikeus vastustaa henkilötietojen käsittelyä rekisteröidyn tilanteeseen liittyvien syiden vuoksi</b>	Profilointia koskeva suositus, 5 artiklan 3 kohta
Tietosuojadirektiivi, 14 artiklan 1 kohdan b alakohta	<b>Oikeus vastustaa henkilötietojen käyttöä markkinointitarkoituksiin</b>	Suoramarkkinointia koskeva suositus, 4 artiklan 1 kohta

EU	Katetut aiheet	EN
Tietosuojadirektiivi, 15 artikla	Oikeus vastustaa automatisoituja päätöksiä	Profilointia koskeva suositus, 5 artiklan 5 kohta
<b>Riippumaton valvonta</b>		
Perusoikeuskirja, 8 artiklan 3 kohta Tietosuojadirektiivi, 28 artikla EU:n toimielinten Tietosuoja-asetus, 5 jakso Tietosuoja-asetus <i>Asia C-518/07, Euroopan komissio v. Saksan liittotasavalta</i> , EUTI 9.3.2010 <i>Asia C-614/10, Euroopan komissio v. Itävallan tasavalta</i> , EUTI 16.10.2012 <i>Asia C-288/12, Euroopan komissio v. Unkari</i> , EUTI, 8.4.2014	Kansalliset valvontaviranomaiset	Yleissopimus 108, lisäpöytäkirja, 1 artikla
<b>Oikeuskeinot ja sanktiot</b>		
Tietosuojadirektiivi, 12 artikla	Pyyntö rekisterinpitäjälle	Yleissopimus 108, 8 artiklan b alakohta
Tietosuojadirektiivi, 28 artiklan 4 kohta EU:n toimielinten tietosuoja-asetus, 32 artiklan 2 kohta	Valvontaviranomaiselle esitettävät vaateet	Yleissopimus 108, lisäpöytäkirja, 1 artiklan 2 kohdan b alakohta
Perusoikeuskirja, 47 artikla	Tuomioistuimet (yleisesti)	EIS, 13 artikla
Tietosuojadirektiivi, 28 artiklan 3 kohta	Kansalliset tuomioistuimet	Yleissopimus 108, lisäpöytäkirja, 1 artiklan 4 kohta
SEUT, 263 artiklan 4 kohta EU:n toimielinten tietosuoja-asetus, 32 artiklan 1 kohta SEUT, 267 artikla	EUTI	
	EIT	EIS, 34 artikla
<b>Oikeuskeinot ja sanktiot</b>		
Perusoikeuskirja, 47 artikla Tietosuojadirektiivi, 22 ja 23 artikla <i>Asia C-14/83, Sabine von Colson ja Elisabeth Kamann v. Land Nordrhein-Westfalen</i> , EYTI 10.4.1984 <i>Asia C-152/84, M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority</i> , EYTI 26.2.1986	Kansallisen tietosuojaoikeuden rikkominen	EIS, 13 artikla (vain EN:n jäsenvaltiot) Yleissopimus 108, 10 artikla <i>Asia nro 2872/02, K.U. v. Suomi</i> , EIT 2.3.2008 <i>Asia nro 23373/03, Biriuk v. Liettua</i> , EIT 25.11.2008
EU:n toimielinten tietosuoja-asetus, 34 ja 49 artikla <i>Asia C-28/08 P, Euroopan komissio v. The Bavarian Lager Co. Ltd</i> , EUTI 29.6.2010	EU:n toimielinten ja elinten EU-oikeuden vastainen toiminta	

Yleisesti oikeussääntöjen ja erityisesti rekisteröityjen oikeuksien vaikuttavuus riippuu merkittävässä määrin asianmukaisten valvontamekanismien olemassaolosta. Euroopan tietosuojasäännösten mukaan rekisteröidyllä on oltava kansallisen lainsäädännön nojalla oikeus suojata omia henkilötietojaan. Lisäksi kansallisessa lainsäädännössä on säädettävä riippumattoman valvontaviranomaisen perustamisesta auttamaan rekisteröityjä oikeuksiensa käyttämisessä ja valvomaan henkilötietojen käsittelyä. EIS:ssa ja perusoikeuskirjassa taattu oikeus tehokkaaseen oikeussuojakeinoon edellyttää vielä, että jokaisella on käytettävissään oikeussuojakeinoja.

## 5.1. Rekisteröityjen oikeudet

### Keskeiset kohdat

- Jokaisella on oltava kansallisen lainsäädännön nojalla oikeus pyytää kaikilta rekisterinpitäjiltä tietoa siitä, käsitteleeö rekisterinpitäjä hänen henkilötietojaan.
- Rekisteröidyllä on oltava kansallisen lainsäädännön nojalla oikeus
  - saada omat henkilötietonsa jokaiselta rekisterinpitäjältä, joka käsittelee näitä tietoja;
  - saada henkilötietoja käsittelevä rekisterinpitäjä oikaisemaan (tai tarvittaessa suojaamaan) hänen tietonsa, jos ne ovat virheelliset;
  - saada rekisterinpitäjä poistamaan tai tarvittaessa suojaamaan hänen henkilötietonsa, jos rekisterinpitäjä käsittelee niitä laittomasti.
- Lisäksi rekisteröidyllä on oltava oikeus vastustaa henkilötietojensa käsittelyä tietyissä tilanteissa
  - automaattisia päätöksiä (jotka on tehty käsittelemällä henkilötietoja ainoastaan automaattisesti);
  - henkilötietojensa käsittelyä, jos se johtaa suhteettomiin lopputuloksiin;
  - henkilötietojensa käsittelyä suoramarkkinointitarkoituksessa

### 5.1.1. Tarkastusoikeus

**EU-oikeudessa** tietosuojadirektiivin 12 artikla kattaa rekisteröidyn tarkastusoikeuden, mukaan lukien oikeuden saada rekisterinpitäjältä ”vahvistus siitä, käsitelläänkö häntä koskevia tietoja vai ei, sekä vähintään tiedot käsitellyn tarkoituksista,

käsiteltävistä tietoryhmistä ja tietojen vastaanottajista tai vastaanottajaryhmistä, joille tiedot luovutetaan” sekä saada ”sellaiset tiedot oikaistuiksi, poistetuiksi tai suojatuiksi, joiden käsittely ei ole tämän direktiivin mukaista, erityisesti tietojen puutteellisen tai virheellisen luonteen vuoksi”.

**EN-oikeudessa** nämä samat oikeudet ovat olemassa ja niistä on säädettävä kansallisessa lainsäädännössä (yleissopimus 108, 8 artikla). Useissa EN:n suosituksissa käsitellään tiedonsaantia sekä kuvaillaan tiedonsaantioikeuden eri näkökohtia ja ehdotetaan niiden täytäntöönpanoa kansallisessa lainsäädännössä edellisessä kapaleessa esitettyllä tavalla.

Yleissopimuksen 108 9 artiklan ja tietosuojadirektiivin 13 artiklan mukaan rekisteröidyn tarkastusoikeutta voidaan rajoittaa pakottavien muiden henkilöiden oikeutettujen etujen perusteella. Tällaiset tärkeämmät edut voivat liittyä yleiseen etuun, kuten kansalliseen turvallisuuteen, yleiseen turvallisuuteen tai syytetoimiin, tai yksityisiin etuihin, jotka menevät tietosuojaa koskevien etujen edelle. Poikkeusten ja rajoitusten on oltava välttämättömiä demokraattisessa yhteiskunnassa ja oikeassa suhteessa tavoitteeseen nähden. Erittäin poikkeuksellisissa tilanteissa, erimerkiksi lääkintähoidon yhteydessä, rekisteröidyn suojaaminen saattaa itsessään edellyttää avoimuuden rajoittamista; tämä koskee erityisesti rekisteröityjen yleisen tarkastusoikeuden rajoittamista.

Tietosuojadirektiivissä sallitaan tarkastusoikeuden rajoittaminen kansallisella lailla silloin, kun tietoja käsitellään yksinomaan tieteellistä tai tilastollista tutkimusta varten, kunhan asianmukaiset suojatoimet on toteutettu. Erityisesti on varmistettava, ettei tällaisen henkilötietojen käsittelyn yhteydessä tehdä yksittäistä henkilöä koskevia toimenpiteitä tai päätöksiä ja että ”siitä ei ilmeisesti aiheudu vaaraa yksityisyydelle”.<sup>176</sup> Samansuuntaisia määräyksiä annetaan yleissopimuksen 108 9 artiklan 3 kohdassa.

## Oikeus tutustua omiin henkilötietoihin

**EN-oikeudessa** oikeus tutustua omiin henkilötietoihin tunnustetaan nimenomaisesti yleissopimuksen 108 8 artiklassa. EIT on useasti todennut, että jokaisella on oikeus tutustua muiden hallussa tai käytössä oleviin henkilötietoihinsa ja että tämä oikeus

<sup>176</sup> Tietosuojadirektiivi, 13 artiklan 2 kohta.

perustuu velvollisuuteen kunnioittaa yksityiselämää.<sup>177</sup> Asiassa *Leander*<sup>178</sup> EIT kuitenkin katsoi, että oikeutta tutustua viranomaisten säilyttämiin henkilötietoihin voidaan tietyissä olosuhteissa rajoittaa.

**EU-oikeudessa** oikeus tutustua itseään koskeviin tietoihin on nimenomaisesti tunnustettu tietosuojadirektiivin 12 artiklassa, ja se on vahvistettu perusoikeudeksi perusoikeuskirjan 8 artiklan 2 kohdassa.

Tietosuojadirektiivin 12 artiklan a alakohdassa säädetään, että jäsenvaltioiden on taattava jokaiselle rekisteröidylle oikeus tutustua itseään koskeviin tietoihin ja saada tietoa. Erityisesti jokaisella rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö häntä koskevia tietoja vai ei, sekä vähintään seuraavat tiedot:

- käsittelyn tarkoitukset;
- käsiteltävät tietoryhmät;
- käsiteltävät tiedot;
- vastaanottajat tai vastaanottajaryhmät, joille tiedot luovutetaan;
- kaikki tietojen alkuperästä käytettävissä olevat tiedot;
- tiedot kyseessä olevien tietojen automaattiseen käsittelyyn liittyvästä logiikasta.

Kansallisessa lainsäädännössä voidaan määritellä muitakin tietoja, jotka rekisterinpitäjän on annettava, kuten tietojenkäsittelyn oikeudellinen peruste.

Esimerkki: Tarkastusoikeutta käyttämällä jokainen voi varmistaa, että tiedot pitävät paikkansa. Rekisteröidyn onkin ehdottomasti tiedettävä, mitä tietoryhmiä käsitellään ja mitä tiedot sisältävät. Tästä syystä ei riitä, että rekisterinpitäjä vain kertoo rekisteröidylle, että käsittely kattaa tämän nimen, osoitteen, syntymäajan ja kiinnostuksen kohteet. Rekisterinpitäjän on

<sup>177</sup> Asia nro 10454/83, *Gaskin v. Yhdistynyt kuningaskunta*, EIT 7.7.1989; asia nro 42326/98, *Odièvre v. Ranska* [suuri jaosto], EIT 13.2.2003; asia nro 32881/04, *K.H. ym. v. Slovakia*, EIT 28.4.2009; asia nro 33783/09, *Godelli v. Italia*, EIT 25.9.2012.

<sup>178</sup> Asia nro 9248/81, *Leander v. Ruotsi*, EIT 11.7.1985.

tarkennettava rekisteröidylle, että käsittely kattaa ”nimen: N.N.; osoitteen: 1040 Wien, Schwarzenbergplatz 11, Itävalta; syntymäajan: 10.10.1974; ja kiinnostuksen kohteet (rekisteröidyn ilmoituksen mukaan): klassinen musiikki.” Viimeinen kohta sisältää lisäksi henkilötiedon lähteen.

Tiedot käsiteltävistä henkilötiedoista ja niiden alkuperästä on annettava ymmärrettävässä muodossa, mikä tarkoittaa, että rekisterinpitäjä voi joutua selittämään tarkemmin käsittelyn kohteen rekisteröidylle. Esimerkiksi pelkät tekniset lyhenteet tai lääketieteelliset termit eivät yleensä riitä vastaukseksi tarkastusoikeutta koskevaan pyyntöön, vaikka ne olisivat ainoat säilytetyt tiedot.

Tarkastusoikeutta koskevaan pyyntöön annettavassa vastauksessa on kerrottava rekisterinpitäjän käsittelemien henkilötietojen alkuperä, jos se vain on mahdollista. Tässä yhteydessä on otettava huomioon asianmukaisen käsittelyn ja vastuullisuuden periaatteet. Rekisterinpitäjä ei saa tuhota tietoa henkilötietojen alkuperästä välttyäkseen sen paljastamiselta eikä laiminlyödä oman alansa tavanomaisia vaatimuksia tai tunnustettuja tarpeita dokumentoinnin osalta. Käsiteltävien henkilötietojen alkuperää koskevan dokumentaation puuttuminen tarkoittaa yleensä, ettei rekisterinpitäjä ole täyttänyt rekisteröidyn tarkastusoikeutta koskevia velvollisuuksiaan.

Kun tietoja arvioidaan automaattisesti, on automaattiseen arviointiin liittyvä yleinen logiikka – myös rekisteröidyn arvioinnissa käytetyt perusteet – selitettävä.

Direktiivissä ei tarkenneta, kattaako tarkastusoikeus myös menneisyyden ja jos kattaa, niin miltä aikaväliltä. Näin ollen, kuten EUTI:n oikeuskäytännössä on korostettu, oikeutta tutustua omiin henkilötietoihin ei voi perusteettomasti rajoittaa ajallisesti. Rekisteröidyillä on myös oltava kohtuulliset mahdollisuudet saada tietoa aiemmista henkilötietojen käsittelytoimista.

Esimerkki: Asiassa *Rijkeboer*<sup>179</sup> EYTI:ta pyydettiin selvittämään, voidaanko henkilön oikeus saada tietoja häntä koskevien henkilötietojen vastaanottajista tai vastaanottajaryhmistä sekä luovutettujen tietojen sisällöstä direktiivin 12 artiklan a alakohdan mukaan rajoittaa hänen tiedonsaantihakemustaan edeltävään vuoden jaksoon.

179 Asia C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, EYTI 7.5.2009.



Sen ratkaisemiseksi, mahdollistetaanko direktiivin 12 artiklan a alakohdassa tällainen ajallinen rajoittaminen, tuomioistuin päätti tulkita kyseistä artiklaa direktiivin tarkoituksia vasten. Tuomioistuin totesi ensinnäkin, että tarkastusoikeus on välttämätön, jotta rekisteröity voi käyttää oikeuttaan saada rekisterinpitäjä oikaisemaan, poistamaan tai suojaamaan hänen tietonsa (12 artiklan b alakohta) tai ilmoittamaan sivullisille, joille tietoja on luovutettu, näistä oikaisuista, poistamisista tai suojaamisista (12 artiklan c alakohta). Tarkastusoikeus on myös välttämätön, jotta rekisteröity voi käyttää oikeuttaan vastustaa henkilötietojensa käsittelyä (14 artikla) tai käyttää oikeussuojakeinoja kärsityn vahingon tapauksessa (22 ja 23 artikla).

Edellä mainittujen säännösten tehokkaan vaikutuksen varmistamiseksi tuomioistuin katsoi, ” on välttämätöntä, että tämä oikeus koskee myös mennyttä aikaa. Jos näin ei olisi, rekisteröity ei voisi tehokkaalla tavalla käyttää oikeuttaan saada laittomiksi tai paikkansapitämättömiksi oletettuja tietoja oikaistuksi, poistetuksi tai suojatuksi tai käyttää oikeussuojakeinoja ja saada korvausta kärsimästään vahingosta.”

## Tiedon korjaaminen

”Kenellä tahansa henkilöllä on oltava oikeus tutustua itseään koskeviin käsiteltäviin tietoihin voidakseen varmistua erityisesti tietojen paikkansapitävyydestä ja niiden käsittelyn laillisuudesta.”<sup>180</sup> Näiden periaatteiden mukaisesti rekisteröidyillä on oltava kansallisen lainsäädännön nojalla oikeus vaatia rekisterinpitäjää oikaisemaan, poistamaan tai suojaamaan heidän henkilötietonsa, jos he uskovat, ettei käsittely ole direktiivin mukaista, erityisesti tietojen puutteellisen tai virheellisen luonteen vuoksi.<sup>181</sup>

Esimerkki: *Asiassa Cemalettin Canli v. Turkki*<sup>182</sup> EIT totesi, että poliisin virheellinen raportointi rikosoikeudenkäynnissä oli rikkonut EIS:n 8 artiklaa.

Kantaja oli ollut kaksi kertaa syytettynä laittoman järjestön jäsenyydestä, mutta häntä ei ollut koskaan tuomittu. Kun kantaja jälleen kerran pidätettiin ja asetettiin syytteeseen uudesta rikoksesta, poliisi toimitti rikostuomioistuimelle

180 Tietosuojadirektiivi, johdanto-osan 41 kappale.

181 *Ibid.*, 12 artiklan b alakohta.

182 Asia nro 22427/04, *Cemalettin Canli v. Turkki*, EIT 18.11.2008, 33, 42 ja 43 kohta; asia nro 964/07, *Dalea v. Ranska*, EIT 2.2.2010.

raportin, jonka otsikkona oli ”*tietoja muista rikoksista*” ja jossa kantaja esitettiin kahden laittoman järjestön jäsenenä. Kantajan pyyntö saada raportti ja poliisin rekisteritiedot muutettua evättiin. EIT katsoi, että poliisin raportin tiedot kuuluivat EIS:n 8 artiklan soveltamisalaan, sillä julkisetkin tiedot voivat kuulua ”yksityiselämän” piiriin, kun viranomaiset ovat keränneet ja säilyttäneet niitä järjestelmällisesti. Lisäksi poliisin raportti oli virheellinen ja se oli laadittu ja toimitettu rikostuomioistuimelle lainvastaisesti. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Segerstedt-Wiberg ym. v. Ruotsi*<sup>183</sup> kantajat olivat kuuluneet tiettyihin liberaaleihin ja kommunistisiin puolueisiin. He epäilivät, että heitä koskevia tietoja oli kirjattu turvallisuuspoliisin rekisteriin. EIT totesi, että tietojen tallentamisella oli ollut oikeudellinen peruste ja laillinen tarkoitus. EIT kuitenkin katsoi, että joidenkin kantajien kohdalla tietojen säilyttäminen loukkasi suhteettomasti heidän yksityiselämänsä. Esimerkiksi Schmid oli viranomaisten tietojen mukaan vuonna 1969 kannattanut poliisin väkivaltaista vastustamista mielenosoituksissa. EIT:n mielestä tällaisella tiedolla ei voinut olla suurta merkitystä kansalliselle turvallisuudelle, etenkin sen historiallisen luonteen vuoksi. EIT totesi, että EIS:n 8 artiklaa oli rikottu neljän kantajan kohdalla viidestä.

Joissakin tapauksissa riittää, että rekisteröity pyytää esimerkiksi nimen kirjoitusasun oikaisemista tai osoitteen tai puhelinnumeron muuttamista. Jos tällaiset pyynnöt liittyvät oikeudellisiin kysymyksiin, kuten rekisteröidyn oikeushenkilöllisyyteen tai oikeaan asuinpaikkaan oikeusasiakirjojen toimittamista varten, pelkkä oikaisu-  
pyyntö ei kuitenkaan välttämättä riitä ja rekisterinpitäjällä voi olla oikeus pyytää näyttöä väitetystä virheestä. Tällaisesta pyynnöstä ei saa aiheutua rekisteröidylle kohtuutonta todistustaakkaa, joka estäisi rekisteröityä saamasta tietoaan oikaisu-  
tuiksi. EIT on todennut, että EIS:n 8 artiklaa on rikottu monessa sellaisessa tapauksessa, jossa kantaja ei ole pystynyt kyseenalaistamaan salaisten rekisterien sisältämien tietojen täsmällisyyttä.<sup>184</sup>

Esimerkki: Asiassa *Ciubotaru v. Moldova*<sup>185</sup> kantajan pyyntö hänen etnistä alkuperäänsä koskevan merkinnän muuttamisesta virallisissa rekistereissä moldovalaisesta romanialaiseksi oli evätty sillä perusteella, ettei hän ollut esittänyt

183 Asia nro 62332/00, *Segerstedt-Wiberg ym. v. Ruotsi*, EIT 6.6.2006, 89 ja 90 kohta; ks. myös esim. asia nro 19522/09, *M.K. v. Ranska*, EIT 18.4.2013.

184 Asia nro 28341/95, *Rotaru v. Romania*, EIT 4.5.2000.

185 Asia nro 27138/04, *Ciubotaru v. Moldova*, EIT 27.4.2010, 51 ja 59 kohta.

todisteita pyyntönsä tueksi. EIT piti hyväksyttävänä sitä, että valtio pyytää rekisteröintiä varten objektiivista näyttöä henkilön etnisestä alkuperästä. Viranomaiset voisivat evätä pyynnön, joka perustuisi puhtaasti subjektiivisiin ja toteennäyttämättömiin väitteisiin. Kantajan pyyntö oli kuitenkin perustunut muuhunkin kuin subjektiiviseen näkemykseen omasta etnisyydestä; hän oli pystynyt esittämään objektiivisesti varmistettavissa olevia yhteyksiä romanialaisten etniseen ryhmään, kuten kielen, nimen ja yhteenkuuluvuuden tunteen. Kansallisen lain mukaan kantajan olisi kuitenkin pitänyt esittää todisteita siitä, että hänen vanhempansa olivat kuuluneet romanialaisten etniseen ryhmään. Moldovan historiallisen tilanteen takia tämä vaatimus oli muodostunut ylitsepääsemättömäksi esteeksi muun etnisen alkuperän rekisteröimiselle kuin sen, jonka Neuvostoliiton viranomaisen olivat kirjanneet kantajan vanhemmille. Epäämällä kantajalta mahdollisuuden hänen pyyntönsä tarkastelemiseen objektiivisesti varmistettavissa olevien todisteiden valossa valtio oli jättänyt noudattamatta positiivista velvollisuuttaan varmistaa kantajalle yksityiselämän kunnioitus. Tuomioistuimien totesi, että EIS:n 8 artiklaa oli rikottu.

Siviilioikeudenkäynneissä tai viranomaismenettelyissä, joissa selvitetään tietojen täsmällisyyttä, rekisteröity voi pyytää, että hänen tietoihinsa lisätään merkintä tai huomautus siitä, että hän on kiistänyt tietojen täsmällisyyden ja että asian käsittely on kesken. Tänä aikana rekisterinpitäjä ei saa esittää tietoja tosina tai lopullisina, etenkin sivullisille.

Rekisteröidyn pyyntö saada tiedot korjatuksi perustuu usein väitteeseen siitä, ettei henkilötietojen käsittelyllä ole oikeudellista perustetta. Tällaisia väitteitä esitetään usein silloin, kun suostumus on peruttu tai kun tiettyjä tietoja ei enää tarvita siihen tarkoitukseen, johon ne on kerätty. Rekisterinpitäjä on vastuussa tietojenkäsittelyn lainmukaisuudesta. Todistustaakka siitä, että tietoja käsitellään lainmukaisesti on rekisterinpitäjällä. Vastuullisuusperiaatteen mukaisesti rekisterinpitäjän on milloin tahansa voitava osoittaa, että tietojenkäsittelylle on asianmukainen oikeudellinen peruste, muuten käsittely on lopetettava.

Jos henkilötietojen käsittely on riitautettu sillä perusteella, että tietojen väitteeseen olevan virheellisiä tai laittomasti käsiteltyjä, rekisteröity voi – asianmukaisen käsittelyn periaatteeseen vedoten – vaatia riidanalaisten tietojen suojaamista. Se tarkoittaa, että tietoja ei poisteta, mutta rekisterinpitäjä ei saa käyttää tietoja sinä aikana, kun ne on suojattu. Tämä on erityisen tarpeellista silloin, kun virheellisten tai laittomasti säilytettyjen tietojen käytön jatkaminen voi vahingoittaa rekisteröityä.

Kansallisessa lainsäädännössä tulisi säätää yksityiskohtaisemmin siitä, milloin tietoja voidaan joutua suojaamaan ja miten suojaaminen toteutetaan.

Rekisterinpitäjällä on velvollisuus ilmoittaa tiedon korjaamisesta sille, jolle rekisterinpitäjä on luovuttanut virheellisen tiedon ennen tiedon korjaamista. Koska rekisterinpitäjän olisi pitänyt dokumentoida tietojen luovuttaminen sivullisille, tietojen vastaanottajat pitäisi voida tunnistaa ja niitä pitäisi voida pyytää poistamaan tiedot. Jos tiedot on kuitenkin ehditty jo julkaista, esimerkiksi internetissä, tietoja ei välttämättä voida poistaa joka paikasta, sillä tietojen vastaanottajia on mahdotonta löytää. Tietosuojadirektiivin mukaan tietojen vastaanottajia on pyydetävä oikaisemaan, poistamaan tai suojaamaan tiedot, ”paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa”.<sup>186</sup>

## 5.1.2. Oikeus vastustaa henkilötietojen käsittelyä

Oikeus vastustaa henkilötietojen käsittelyä kattaa oikeuden vastustaa automatisoituja yksittäispäätöksiä, oikeuden vastustaa henkilötietojen käsittelyä rekisteröidyn tilanteeseen liittyvien syiden vuoksi ja oikeuden vastustaa henkilötietojen käyttöä suoramarkkinointitarkoituksiin.

### Oikeus vastustaa automatisoituja yksittäispäätöksiä

Automatisoidut päätökset ovat päätöksiä, jotka on tehty käsittelemällä henkilötietoja ainoastaan automaattisesti. Jos tällaisella päätöksellä on todennäköisesti merkittävä vaikutus ihmisen elämään esimerkiksi siksi, että se liittyy luottokelpoisuuteen, ammatilliseen suoriutuskyykyyn, käyttäytymiseen tai luotettavuuteen, tarvitaan erityistä suojaa asiattomien seurausten välttämiseksi. Tietosuojadirektiivissä säädetään, että automatisoituja päätöksiä ei tulisi tehdä ihmisille tärkeissä asioissa ja että ihmisillä tulisi olla oikeus tutustua automatisoituihin päätöksiin.<sup>187</sup>

Esimerkki: Tärkeä käytännön esimerkki automatisoidusta päätöksenteosta on luottopisteytys. Tulevan asiakkaan luottokelpoisuuden nopeaa selvittämistä varten asiakkaalta pyydetään tietyt tiedot, kuten ammatti ja perhetilanne, ja nämä tiedot yhdistetään muista lähteistä, kuten luottotietojärjestelmistä, rekisteröidystä saataviin tietoihin. Tiedot syötetään pisteytysalgoritmiin, joka laskee mahdollisen asiakkaan luottokelpoisuutta kuvastavan kokonaisarvon. Näin

<sup>186</sup> Tietosuojadirektiivi, 12 artiklan c alakohdan virkkeen loppuosa.

<sup>187</sup> *Ibid.*, 15 artiklan 1 kohta.

työntekijä voi muutamassa sekunnissa päättää, voidaanko rekisteröity hyväksyä asiakkaaksi.

Direktiivin mukaan jäsenvaltioiden on kuitenkin säädettävä siitä, että henkilö voi joutua automatisoidun yksittäispäätöksen kohteeksi, jos rekisteröidyn edut eivät ole uhattuina, koska päätös on rekisteröidyn edun mukainen, tai rekisteröidyn edut on suojattu muilla asianmukaisilla tavoilla.<sup>188</sup> Oikeus vastustaa automatisoituja päätöksiä sisältyy myös **EN-oikeuteen**, kuten **profilointia koskevasta suosituksesta** ilmenee.<sup>189</sup>

## Oikeus vastustaa henkilötietojen käsittelyä rekisteröidyn tilanteeseen liittyvien syiden vuoksi, kuten virheellisen tiedon korjaaminen

Rekisteröidyillä ei ole yleistä oikeutta vastustaa henkilötietojensa käsittelyä.<sup>190</sup> Tietosuojadirektiivin 14 artiklan a alakohdassa annetaan kuitenkin rekisteröidyille oikeus vastustaa itseään koskevien tietojen käsittelyä tilanteeseensa liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi. EN:n profilointia koskevassa suosituksessa on tunnustettu samankaltainen oikeus.<sup>191</sup> Tällaisilla määräyksillä pyritään saattamaan tasapainoon rekisteröidyn oikeudet ja muiden lailliset oikeudet käsitellä rekisteröidyn henkilötietoja.

Esimerkki: Pankki säilyttää seitsemän vuoden ajan tiedot asiakkaistaan, jotka laininlyövät lainamaksujaan. Asiakas, jonka tiedot on tallennettu tähän tietokantaan, hakee uutta lainaa. Työntekijä tarkistaa tietokannan, arvioi taloudellisen tilanteen, ja epää asiakkaalta lainan. Asiakas voi kuitenkin vastustaa henkilötietojensa tallentamista tietokantaan ja pyytää tietojen poistamista, jos hän voi todistaa, että maksujen laininlyönti oli johtunut pelkästään virheestä, joka oli korjattu välittömästi sen jälkeen, kun se oli tullut asiakkaan tietoon.

188 *Ibid.*, 15 artiklan 2 kohta.

189 Profilointia koskeva suositus, 5 artiklan 5 kohta.

190 Ks. myös asia nro No. 20837/92, *M.S. v. Ruotsi*, EIT 27.8.1997, jossa terveystietoja oli luovutettu ilman suostumusta tai mahdollisuutta vastustaa; tai asia nro 9248/81, *Leander v. Ruotsi*, EIT 26.3.1987; tai asia nro 48009/08, *Mosley v. Yhdistynyt kuningaskunta*, EIT 10.5.2011.

191 Profilointia koskeva suositus, 5 artiklan 3 kohta.

Kun vastustus on hyväksytty, rekisterinpitäjä ei voi enää käsitellä kyseisiä henkilötietoja. Rekisteröidyn henkilötietoihin ennen vastustusta kohdistetut käsittelytoimet ovat kuitenkin edelleen lainmukaisia.

## Oikeus kieltää henkilötietojen käsittely suoramarkkinointitarkoituksiin

Tietosuojadirektiivin 14 artiklan b alakohdassa säädetään erityisestä mahdollisuudesta kieltää henkilötietojen käsittely suoramarkkinointitarkoituksessa. Samanlainen oikeus on vahvistettu EN:n suoramarkkinointia koskevassa suosituksessa.<sup>192</sup> Kielto on voitava esittää ennen kuin henkilötietoja ensi kerran luovutetaan sivulliselle tai käytetään sivullisen lukuun suoramarkkinointitarkoituksessa. Siksi rekisteröidylle on annettava mahdollisuus vastustaa henkilötietojen käsittelyä ennen tietojen luovuttamista.

## 5.2. Riippumaton valvonta

### Keskeiset kohdat

- Tehokkaan tietosuojan varmistamiseksi kansallisessa lainsäädännössä on säädettävä riippumattoman valvontaviranomaisen perustamisesta.
- Kansallisten valvontaviranomaisten on oltava toiminnassaan täysin riippumattomia. Tämä on taattava niiden perustamisesta annettavalla lailla ja tuotava esiin valvontaviranomaisen organisaatiorakenteessa.
- Valvontaviranomaisilla on erityisiä tehtäviä, joihin kuuluvat seuraavat:
  - tietosuojaan liittyvien asioiden seuraaminen ja edistäminen kansallisella tasolla;
  - rekisteröityjen ja rekisterinpitäjien sekä hallinnon ja suuren yleisön neuvominen;
  - valitusten vastaanottaminen ja rekisteröityjen avustaminen tietosuoja koskevien oikeuksien väitetyissä rikkomistapauksissa;
  - rekisterinpitäjien ja henkilötietojen käsittelijöiden valvominen;
  - tarvittaessa tilanteisiin puuttuminen

<sup>192</sup> EN, ministerineuvosto (1985), suositus Rec(85) 20 suoramarkkinoinnissa käytettävien henkilötietojen suojaamisesta, 25. lokakuuta 1985, 4 artiklan 1 kohta.

- antamalla rekisterinpitäjille ja henkilötietojen käsittelijöille huomautuksia tai varoituksia ja jopa sakkoja,
- määräämällä tietoja oikaistaviksi, suojattaviksi tai poistettaviksi,
- kieltämällä tietojen käsittely väliaikaisesti tai lopullisesti;
- asioiden saattaminen tuomioistuimien käsiteltäviksi.

Tietosuojadirektiivissä vaaditaan riippumatonta valvontaa tärkeänä mekanismina, jolla voidaan varmistaa tehokas tietosuojaa. Direktiivissä luotiin tietosuojan toteuttamista varten instituutio, jota ei alkuun ollut yleissopimuksessa 108 eikä OECD:n yksityisyyden suojaa koskevilla suuntaviivoilla.

Kun riippumaton valvonta osoittautui tehokkaan tietosuojan kehittämisen kannalta välttämättömäksi, [OECD:n yksityisyyden suojaa koskeviin suuntaviivoihin](#) lisättiin vuonna 2013 kohta, jossa jäsenvaltioita kehoitetaan perustamaan ja pitämään yksityisyyden suojan valvonnasta vastaavia viranomaisia, joiden hallinto, resurssit ja tekninen asiantuntemus riittävät tehtävien tehokkaaseen toteuttamiseen sekä objektiivisten, puolueettomien ja johdonmukaisten päätösten tekemiseen.<sup>193</sup>

**EN-oikeudessa** [yleissopimuksen 108 lisäpöytäkirjalla](#) valvontaviranomaisen perustamisesta tehtiin pakollista. Lisäpöytäkirjan 1 artikla sisältää riippumattomia valvontaviranomaisia koskevan oikeudellisen kehyksen, joka sopimuspuolien on pantava täytäntöön kansallisessa lainsäädännössä. Siinä kuvaillaan viranomaisten tehtäviä ja valtuuksia samankaltaisin sanamuodoin kuin tietosuojadirektiivissä. Valvontaviranomaisten tulisikin periaatteessa toimia samalla tavalla EU- ja EN-oikeuden puitteissa.

**EU-oikeudessa** valvontaviranomaisten valtuudet ja organisaatorakenne määriteltiin ensimmäisen kerran tietosuojadirektiivin 28 artiklan 1 kohdassa. EU:n toimielinten tietosuojasetuksessa<sup>194</sup> säädettiin, että Euroopan tietosuojavaltuutettu valvoo EU:n toimielinten ja elinten suorittamaa henkilötietojen käsittelyä. Tämän valvontaviranomaisen roolin ja vastuiden määrittelyssä on hyödynnetty tietosuojadirektiivin hyväksymisestä lähtien kerättyä kokemusta.

193 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, 19 artiklan c alakohta.

194 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001 L 8, 41–48 artikla.

Tietosuojaviranomaisten riippumattomuus on taattu SEUT 16 artiklan 2 kohdassa ja perusoikeuskirjan 8 artiklan 3 kohdassa. Jälkimmäisessä määräyksessä riippumattoman viranomaisen suorittama valvonta nähdään erityisesti olennaisena osana henkilötietojen suojaan perusoikeutena. Lisäksi tietosuojadirektiivissä veloitetaan jäsenvaltiot perustamaan täysin riippumattomat valvontaviranomaiset valvomaan direktiivin soveltamista.<sup>195</sup> Ei riitä, että valvontaelimen perustamisesta annettava laki sisältää erityiset säännökset, joilla taataan riippumattomuus, vaan viranomaisen organisaatorakenteen on ilmennettävä riippumattomuutta.

EUTI käsitteli vuonna 2010 ensimmäisen kerran tietosuojan valvontaviranomaisten riippumattomuutta koskevan vaatimuksen laajuutta.<sup>196</sup> Seuraavat esimerkit antavat kuvan sen tästä asiasta tekemästä tulkinnasta.

Esimerkki: Asiassa *komissio v. Saksa*<sup>197</sup> Euroopan komissio oli pyytänyt EUTI:ta toteamaan, että Saksa oli virheellisesti implementoinut tietosuojasta vastaavien valvontaviranomaisten ”täydellistä itsenäisyyttä” koskevan vaatimuksen ja siten jättänyt noudattamatta tietosuojadirektiivin 28 artiklan 1 kohdan mukaisia velvoitteitaan. Komission mielestä ongelmana oli, että Saksa oli asettanut valtion valvonnan alaiseksi viranomaiset, jotka valvovat henkilötietojen käsittelyä muualla kuin julkisella sektorilla eri osavaltioissa (*Länder*).

Kanteen perusteltavuus riippui tuomioistuimen mukaan säännöksessä tarkoitettun itsenäisyyden vaatimuksen ulottuvuudesta ja näin ollen säännöksen tulkinnasta.

Tuomioistuin toi esiin, että 28 artiklan 1 kohdassa käytetyn ilmaisun ”itsenäisesti” tulkinnassa oli otettava huomioon sekä säännöksen sanamuoto että tietosuojadirektiivin tavoitteet ja rakenne.<sup>198</sup> Tuomioistuin painotti, että valvontaviranomaiset ovat henkilötietojen käsittelyn alalla direktiivissä taattujen oikeuksien ”vartijoita” ja että niiden perustamista jäsenvaltioissa pidetään ”keskeisenä tekijänä yksilöiden suojelussa henkilötietojen käsittelyssä”.<sup>199</sup> Tuo-

195 Tietosuojadirektiivi, 28 artiklan 1 kohdan viimeinen virke; yleissopimus 108, lisäpöytäkirja, 1 artiklan 3 kohta.

196 Ks. FRA (2010), *Perusoikeudet: Haasteet ja saavutukset vuonna 2010*, Vuosikertomus 2010, s. 59. FRA on käsitellyt tätä asiaa yksityiskohtaisesti raportissaan: *Data protection in the European Union: the role of National Data Protection Authorities*, joka julkaistiin toukokuussa 2010.

197 Asia C-518/07, *Euroopan komissio v. Saksan liittotasavalta*, EUTI 9.3.2010, 27 kohta.

198 *Ibid.*, 17 ja 29 kohta.

199 *Ibid.*, 23 kohta.



mioistuin totesi, että ”valvontaviranomaisten on tehtäviään hoitaessaan toimitava objektiivisesti ja puolueettomasti. Tässä tarkoituksessa niiden on oltava suojattuna kaikelta ulkopuoliselta vaikuttamiselta, myös suoralta tai välilliseltä vaikuttamiselta valtion tai osavaltioiden taholta, ei ainoastaan valvottavien elinten taholta.”<sup>200</sup>

EUTI katsoi lisäksi, että ilmaisun ”itsenäisesti” tulkinnassa oli otettava huomioon Euroopan tietosuojavaltuutetun riippumattomuus, sellaisena kuin se määritellään EU:n toimielinten tietotuoja-asetuksessa. Kyseisen asetuksen 44 artiklan 2 kohdassa selvennetään riippumattomuuden käsitettä ja lisätään, että ”tehtäviään hoitaessaan Euroopan tietosuojavaltuutettu ei pyydä eikä ota ohjeita mitään taholta”. Tämä sulkee pois itsenäiseen tietosuojan valvontaviranomaiseen kohdistettavan valtion valvonnan.<sup>201</sup>

Edellä esitetyn perusteella EUTI totesi, että Saksan valtiolliset tietosuojaviranomaiset, jotka valvoivat muiden kuin julkisten elinten suorittamaa henkilötietojen käsittelyä, eivät olleet riittävän itsenäisiä, koska ne olivat valtion valvonnan alaisia.

Esimerkki: Asiassa *komissio v. Itävalta*<sup>202</sup> EUTI toi esiin samankaltaisia ongelmia Itävallan tietosuojaviranomaisen (Datenschutzkommission, DSK) tiettyjen jäsenten ja henkilöstön asemassa. Kyseisessä asiassa tuomioistuin katsoi, että Itävallan lainsäädäntö esti Itävallan tietosuojaviranomaista suorittamasta tehtäväänsä itsenäisesti tietosuojadirektiivissä tarkoitetulla tavalla. Itävallan tietosuojaviranomaisen riippumattomuutta ei ollut riittävästi turvattu, koska liittokanslerinvirasto palkkasi DSK:n työntekijät, valvoi DSK:ta ja sai milloin tahansa pyytää tietoja DSK:n työstä.

Esimerkki: Asiassa *komissio v. Unkari*<sup>203</sup> EUTI korosti, että ”vaatimus siitä, että jokainen valvontaviranomainen pystyy suoriutumaan sille osoitetuista tehtävistä täydellisen itsenäisesti, sisältää kyseessä olevalle jäsenvaltiolle osoitetun velvollisuuden sallia, että kyseinen viranomainen toimii koko toimikautensa ajan” ja katsoi, että ”päättämällä ennaikaisesti valvontaviranomaisen

200 *Ibid.*, 25 kohta.

201 *Ibid.*, 27 kohta.

202 Asia C-614/10, *Euroopan komissio v. Itävallan tasavalta*, EUTI 16.10.2012, 59 ja 63 kohta.

203 Asia C-288/12, *Euroopan komissio v. Unkari*, EUTI 8.4.2014, 50 ja 67 kohta

toimikauden, Unkari ei ole täyttänyt direktiivin 95/46/EY mukaisia velvoitteitaan [...]”

Valvontaviranomaisilla on kansallisen lainsäädännön nojalla valtuudet muun muassa<sup>204</sup>

- neuvoa rekisterinpitäjiä ja rekisteröityjä kaikissa tietosuojaan liittyvissä asioissa;
- tutkia käsittelytoimia ja puuttua niihin tarvittaessa;
- varoittaa tai huomauttaa rekisterinpitäjiä;
- määrätä tietoja oikaistaviksi, suojattaviksi poistettaviksi tai tuhottaviksi;
- kieltää henkilötietojen käsittely väliaikaisesti tai lopullisesti;
- saattaa asioita tuomioistuimien käsiteltäviksi.

Voidakseen hoitaa tehtäviään valvontaviranomaisella on oltava mahdollisuus tutustua kaikkiin selvityksen kannalta tarpeellisiin henkilötietoihin ja muihin tietoihin sekä päästä kaikkiin tiloihin, joissa rekisterinpitäjä säilyttää asiaa koskevia tietoja.

Kansallisissa lainsäädännöissä on merkittäviä eroja valvontaviranomaisen toteamiin poikkeamiin liittyvissä menettelyissä ja niiden oikeusvaikutuksissa. Seuraukset voivat vaihdella asiamiehen antamien suositusten kaltaisista ohjauksista välittömästi toimeenpantaviin päätöksiin. Tämän vuoksi, kun analysoidaan käytettävissä olevien oikeuskeinojen tehokkuutta, on otettava huomioon kyseessä olevan lainkäyttöalueen erityispiirteet.

## 5.3. Oikeuskeinot ja sanktiot

### Keskeiset kohdat

- Sekä yleissopimuksen 108 että tietosuojadirektiivin mukaan kansallisessa lainsäädännössä on säädettävä asianmukaiset oikeuskeinot ja sanktiot tietosuoja koskevien oikeuksien rikkomisen varalta.

<sup>204</sup> Tietosuojadirektiivi, 28 artikla; ks. myös yleissopimus 108, lisäpöytäkirja, 1 artikla.

- Oikeus tehokkaiisiin oikeussuojakeinoihin edellyttää EU-oikeudessa, että kansallisessa lainsäädännössä on vahvistettu oikeussuojakeinot tietosuojaoikeuksien rikkomisen varalta riippumatta mahdollisuudesta kääntyä valvontaviranomaisen puoleen.
- Kansallisessa lainsäädännössä on säädettävä sanktiot, jotka ovat tehokkaita, tasapuolisia, oikeasuhteisia ja varoittavia.
- Rekisterinpitäjään on oltava yhteydessä ennen asian viemistä tuomioistuimeen. Siitä, onko myös valvontaviranomaiseen oltava yhteydessä ennen asian saattamista tuomioistuimen käsiteltäväksi, säädetään kansallisessa lainsäädännössä.
- Rekisteröidyt voivat viimeisenä keinona ja tietyin edellytyksin saattaa henkilötietojen suojaa koskevat rikkomukset myös EIT:n käsiteltäväksi.
- Lisäksi rekisteröidyt voivat kääntyä EUT:n puoleen, mutta vain tarkoin määritellyissä tilanteissa.

Tietosuoja säännösten mukaisia oikeuksia voi käyttää ainoastaan se henkilö, jota oikeudet koskevat, eli henkilö, joka on – tai ainakin väittää olevansa – rekisteröity. Näitä henkilöitä voivat edustaa oikeuksien käytössä henkilöt, jotka täyttävät kansallisessa lainsäädännössä asetetut vaatimukset. Alaikäisiä edustavat heidän vanhempansa tai huoltajansa. Henkilöä voi valvontaviranomaisen edessä edustaa myös yhdistys, jonka laillisena tavoitteena on edistää tietosuojaan liittyviä oikeuksia.

### 5.3.1. Pyynnöt rekisterinpitäjälle

Edellä 3.2 kohdassa mainittuja oikeuksia on käytettävä ensin suhteessa rekisterinpitäjään. Asian vieminen suoraan valvontaviranomaisen tai tuomioistuimen käsiteltäväksi ei auta, sillä viranomaisen vain ohjaisi kääntymään ensin rekisterinpitäjän puoleen ja tuomioistuin toteaisi, ettei se voi ottaa kannetta tutkittavaksi. Rekisterinpitäjälle esitettävän oikeudellisesti pätevän pyynnön muotovaatimuksista, erityisesti siitä, onko pyynnön oltava kirjallinen, tulisi säätää kansallisessa lainsäädännössä.

Yhteisön, johon on otettu yhteyttä rekisterinpitäjänä, on vastattava pyyntöön, vaikkei se olisikaan rekisterinpitäjä. Rekisteröidylle on joka tapauksessa annettava vastaus kansallisessa lainsäädännössä asetetussa määräajassa, vaikka vastaus olisi vain se, ettei pyynnön esittäjää koskevia henkilötietoja käsitellä. Tietosujadirektiivin 12 artiklan a alakohdan ja yleissopimuksen 108 8 artiklan b alakohdan mukaan tällainen pyyntö on käsiteltävä ”ilman aiheetonta viivytystä”. Kansallisessa lainsäädännössä tulisikin määritellä vastausaika, joka on riittävän lyhyt, mutta jonka puitteissa rekisterinpitäjä ehtii käsitellä pyynnön asianmukaisesti.

Ennen pyyntöön vastaamista yhteisön, johon on otettu yhteyttä rekisterinpitäjänä, on selvítettävä pyynnön esittäjän henkilöllisyys ja varmistuttava siitä, että hän on se henkilö, joka hän väittää olevansa, salassapitovelvollisuuden vakavan rikkomisen välttämiseksi. Jos henkilöllisyyden selvittämistä koskevia vaatimuksia ei ole vahvistettu kansallisessa lainsäädännössä, rekisterinpitäjän on itse määriteltävä ne. Asianmukaisen käsittelyn periaate edellyttää joka tapauksessa, ettei rekisterinpitäjä aseta liian raskaita edellytyksiä henkilöllisyyden todistamiselle (ja pyynnön todentamiselle, kuten [2.1.1 kohdassa](#) esitettiin).

Kansallisessa lainsäädännössä on myös otettava kantaa siihen, voiko rekisterinpitäjä vaatia, että pyynnön esittäjä suorittaa maksun ennen pyyntöön vastaamista: Tietosuojadirektiivin 12 artiklan a alakohdan ja yleissopimuksen 108 8 artiklan b alakohdan mukaan tarkastusoikeutta koskevaan pyyntöön on saatava vastaus ”ilman – aiheettomia kustannuksia”. Monissa Euroopan maissa on kansallisessa lainsäädännössä säädetty, että henkilötietojen käsittelyyn liittyviin pyyntöihin on vastattava ilmaiseksi, kunhan vastaamisesta ei aiheudu kohtuutonta ja tavatonta vaivaa; rekisterinpitäjät on vuorostaan yleensä suojattu kansallisessa lainsäädännössä vastauksen saamista koskevan oikeuden väärinkäytöltä.

Jos henkilö, toimielin tai elin, johon on otettu yhteyttä rekisterinpitäjänä, ei kiellä olevansa rekisterinpitäjä, sen on kansallisessa lainsäädännössä asetettuun määräaikaan mennessä

- joko hyväksyttävä pyyntö ja ilmoitettava pyynnön esittäneelle henkilölle, miten pyyntö on täytetty; tai
- tiedotettava pyynnön esittäjälle, miksi hänen pyyntöään ei tulla täyttämään.

## 5.3.2. Valvontaviranomaiselle esitettävät vaateet

Jos henkilö on esittänyt tarkastusoikeutta koskevan pyyntönsä tai vastustuksensa rekisterinpitäjälle, mutta ei saa siihen kohtuullisessa ajassa tyydyttävästi vastausta, hän voi käännyä kansallisen tietosuojaviranomaisen puoleen ja pyytää tältä apua. Valvontaviranomaisen menettelyn aikana tulisi selvittää, oliko henkilöllä, toimielimellä tai elimellä, johon pyynnön esittäjä oli yhteydessä, velvollisuus vastata pyyntöön ja käsitteillä se pyynnön asianmukaisella ja riittävällä tavalla. Valvontaviranomaisen on tiedotettava asianosaiselle tämän vaateen käsittelyn tuloksesta.<sup>205</sup>

205 Tietosuojadirektiivi, 28 artiklan 4 kohta.

Kansallisen valvontaviranomaisen menettelyn tulosten oikeusvaikutukset riippuvat kansallisesta lainsäädännöstä: viranomaisen päätökset voivat olla suoraan täytäntöönpanokelpoisia, tai rekisterinpitäjää vastaan voidaan joutua nostamaan kanne, jos se ei noudata valvontaviranomaisen päätöksiä (lausuntoa, huomautusta tms.).

Jos EU:n toimielimen tai elimen väitetään rikkoneen SEUT 16 artiklassa taattuja tietosuoja-oikeuksia, rekisteröity voi tehdä kantelun Euroopan tietosuoja-valtuutetulle,<sup>206</sup> riippumattomalle tietosuojan valvontaviranomaiselle, jonka perustamisesta, velvollisuuksista ja valtuuksista säädetään EU:n toimielinten tietosuoja-asetuksessa. Jos Euroopan tietosuoja-valtuutettu ei ole antanut vastausta kuuden kuukauden kuluessa, kantelu katsotaan hylätyksi.

Kansallisen valvontaviranomaisen päätöksistä on voitava valittaa tuomioistuimeen. Tämä koskee sekä rekisteröityjä että rekisterinpitäjiä, jotka ovat olleet osallisina valvontaviranomaisen menettelyssä.

Esimerkki: Yhdistyneen kuningaskunnan tietosuoja-valtuutettu teki 24. heinäkuuta 2013 päätöksen, jossa se pyysi Hertfordshiren poliisia luopumaan ajoneuvojen rekisterikilpien jäljitysjärjestelmästä, jota se piti laittomana. Kameroilla kerättyjä tietoja säilytettiin sekä paikallispoliisin tietokannassa että keskustietokannassa. Rekisterikilvistä otettuja valokuvia säilytettiin kaksi vuotta ja autoista otettuja valokuvia 90 päivää. Tällaista kameroiden ja muiden valvontamuotojen laajamittaista käyttöä pidettiin suhteettomana sillä käsiteltyyn ongelmaan nähden.

### 5.3.3. Tuomioistuimelle esitettävät vaateet

Tietosuojadirektiivin mukaan henkilön, joka on esittänyt tietosuojasäännöksissä tarkoitetun pyynnön rekisterinpitäjälle, mutta ei ole tyytyväinen saamaansa vastaukseen, on voitava tehdä valitus kansalliseen tuomioistuimeen.<sup>207</sup>

Siitä, onko valvontaviranomaiseen oltava yhteydessä ennen vetoamista tuomioistuimeen, säädetään kansallisessa lainsäädännössä. Useimmissa tapauksissa on kuitenkin hyvä lähestyä ensin valvontaviranomaista, joka käsittelee sille esitetyt

206 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001 L 8.

207 Tietosuojadirektiivi, 22 artikla.

vaateet vaivattomasti ja ilmaiseksi. Valvontaviranomaisen päätöksessä (lausunnossa, huomautuksessa tms.) esitetyt perustelut voivat lisäksi auttaa rekisteröityä saamaan oikeutensa tunnustetuksi tuomioistuimissa.

**EN-oikeudessa** tietosuojaoikeuksien rikkomukset, joiden väitetään olevan paitsi EIS:n sopimuspuolen kansallisen lainsäädännön vastaisia myös EIS:n 8 artiklan vastaisia, voidaan lisäksi saattaa EIT:n käsiteltäviksi sen jälkeen, kun kaikki kansalliset oikeuskeinot on käytetty. Jotta EIT voisi ratkaista EIS:n 8 artiklan rikkomisen, on muidenkin tutkittavaksi ottamisen edellytysten täytyttävä (EIS:n 34–37 artikla).<sup>208</sup>

Kanteen voi EIT:ssa nostaa vain sopimuspuolta vastaan, mutta asioissa voidaan välillisesti käsitellä myös yksityisten osapuolten toimia tai laiminlyöntejä, siinä määrin kuin sopimuspuoli on jättänyt noudattamatta positiivisia velvollisuuksiaan eikä ole vahvistanut kansallisessa lainsäädännössä riittävää turvaa tietosuojaoikeuksien rikkomisia vastaan.

Esimerkki: Asiassa *K.U. v. Suomi*<sup>209</sup> kantajana ollut alaikäinen henkilö valitti, että hänestä oli julkaistu internetin seuranhakupalstalla seksuaalisuonteinen ilmoitus. Palveluntarjoaja kieltäytyi paljastamasta tiedon julkaisseen henkilön henkilöllisyyttä vedoten Suomen lain mukaiseen salassapitovelvollisuuteen. Kantaja väitti, että Suomen laki ei tarjonnut riittävää suojaa tilanteessa, jossa yksityishenkilö julkaisi laittomasti tietoja internetissä. EIT katsoi, että valtioilla on paitsi velvollisuus olla puuttumatta mielivaltaisesti ihmisten yksityiselämää myös positiivisia velvollisuuksia, joihin kuuluu yksityiselämää suojaavien toimenpiteiden toteuttaminen myös yksilöiden välisten suhteiden alalla. Kantajan tapauksessa hänen tosiasiallinen ja tehokas suojaamisensa edellytti toimia rikosten tekijän tunnistamiseksi ja asettamiseksi syytteeseen. Valtio ei kuitenkaan ollut tarjonnut tällaista suojaa, ja siksi tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Köpke v. Saksa*<sup>210</sup> kantajaa oli epäilty varkaudesta hänen työpaikallaan ja siksi hänet oli asetettu salaa videovalvontaan. EIT katsoi, ettei mikään viitannut siihen, että kansalliset viranomaiset eivät olisi harkintavaltansa puitteissa pyrkineet saattamaan kantajan 8 artiklan mukaista oikeutta

208 EIS, 34–37 artikla, saatavana osoitteessa [http://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063/19990063\\_2](http://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063/19990063_2).

209 Asia nro 2872/02, *K.U. v. Suomi*, EIT 2.3.2009.

210 Asia nro 420/07, *Köpke v. Saksa*, EIT 5.10.2010.

nauttia yksityiselämän kunnioitusta tasapainoon työnantajan omistusoikeuden suojaamiseen liittyvien etujen ja asianmukaista oikeudenkäyttöä koskevan yleisen edun kanssa. Kanne jätettiin näin ollen tutkimatta.

Jos EIT toteaa, että sopimuspuoli on rikkonut jotain EIS:lla suojattua oikeutta, sopimusvaltion on pantava täytäntöön EIT:n tuomio. Täytäntöönpanotoimenpiteiden ensisijaisena vaikutuksena on oltava kyseessä olevan rikkomuksen lopettaminen ja sen jälkeen mahdollisuuksien mukaan kantajalle aiheutuneiden haitallisten seurausten korjaaminen. Tuomioiden täytäntöönpano saattaa edellyttää myös yleisiä toimenpiteitä, joilla ehkäistään tuomioistuimen toteamien rikkomusten toistumista lainsäädännön muutosten, oikeuskäytännön tai muiden toimenpiteiden kautta.

Kun EIT toteaa, että EIS:ta on rikottu, se voi EIS:n 41 artiklan nojalla määrätä sopimusvaltion maksamaan kantajalle hyvityksen.

**EU-oikeudessa**<sup>211</sup> Jos kansallisesti implementoitu tietosuojalaki rikkoo kansalaisen oikeuksia, voi asian tietyin edellytyksin saattaa EUTI:n käsiteltäväksi. Rekisteröidyn väite hänen tietosuojaa koskevien oikeuksiensa rikkomisesta voi päättyä EUTI:n käsiteltäväksi kahdessa tapauksessa.

Ensimmäisessä tapauksessa rekisteröidyn on täytynyt kärsiä suoraan EU:n hallinto- tai sääntelytoimesta, joka on rikkonut hänen oikeuttaan tietosuojaan. SEUT 263 artiklan 4 kohdassa määrätään seuraavasti:

*”Luonnollinen henkilö tai oikeushenkilö voi – – nostaa kanteen hänelle osoitetusta säädöksestä tai säädöksestä, joka koskee häntä suoraan ja erikseen, sekä sääntelytoimesta, joka koskee häntä suoraan ja joka ei edellytä täytäntöönpanotoimenpiteitä.”*

Täten EU:n elinten toteuttaman laittoman henkilötietojen käsittelyn uhrin voivat vedota suoraan unionin yleiseen tuomioistuimeen, jolla on toimivalta ratkaista EU:n toimielinten tietosuoja-asetukseen liittyviä asioita. EUTI:een voi vedota suoraan myös silloin, kun jokin EU:n säännös vaikuttaa suoraan henkilön oikeudelliseen tilanteeseen.

<sup>211</sup> EU (2007), Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, allekirjoitettu Lissabonissa 13 päivänä joulukuuta 2007, EUVL 2007 C 306. Ks. myös Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidut versiot, EUVL 2012 C 326.

Toinen tapaus liittyy EUTI:n (unionin tuomioistuimen) toimivaltaan antaa ennakkoratkaisuja SEUT 267 artiklan nojalla.

Rekisteröidyt voivat kansallisten menettelyjen yhteydessä esittää, että kansallinen tuomioistuin pyytää unionin tuomioistuinta selventämään EU:n perussopimusten tulkintaa sekä ottamaan kantaa EU:n toimielinten, elinten, laitosten tai virastojen toimien pätevyYTEEN. Tällaisia selvennyksiä kutsutaan ennakkoratkaisuuksi. Kyseessä ei ole valituksen tekijän näkökulmasta välitön oikeuskeino, mutta näin kansalliset tuomioistuimet voivat varmistaa, että ne tulkitsevat oikein EU:n lainsäädäntöä.

Jos kansallisen tuomioistuinmenettelyn osapuoli ehdottaa ennakkoratkaisupyynnön esittämistä EUTI:lle, siihen on suostuttava ainoastaan, jos kansallinen tuomioistuin on ylin oikeusaste eikä sen päätöksistä ole mahdollista valittaa.

Esimerkki: Asiassa *Kärntner Landesregierung ym.*<sup>212</sup> Itävallan perustuslakituomioistuin kysyi EUTI:lta, oliko direktiivin 2006/24/EY (*tietojen säilyttämistä koskeva direktiivi*) 3–9 artiklaa pidettävä pätevinä perusoikeuskirjan 7, 9 ja 11 artiklan valossa ja olivatko tietyt Itävallan liittovaltion televiestintälain säännökset, joilla tietojen säilyttämistä koskeva direktiivi oli saatettu osaksi kansallista lainsäädäntöä, yhdenmukaisia tiettyjen tietosuojadirektiivin ja EU:n toimielinten tietosuoja-asetuksen näkökohtien kanssa.

Yksi perustuslakituomioistuimen menettelyn kantajista, Seitlinger, totesi, että hän käyttää puhelinta, internetiä ja sähköpostia sekä työssään että yksityiselämässään. Tiedot, joita hän lähettää ja vastaanottaa, kulkevat julkisten televiestintäverkkojen kautta. Itävallan vuoden 2003 televiestintälain nojalla hänen televiestintäpalvelujen tarjoajallaan on lakisääteinen velvollisuus kerätä ja säilyttää tietoja hänen verkon käytöstään. Seitlinger ymmärsi, ettei tällainen hänen henkilötietojensa keruu ja säilytys ollut mitenkään välttämätöntä siihen tekniseen tarkoitukseen, joka oli tietojen siirtäminen verkossa A:lta B:lle. Henkilötietojen keruu ja säilytys ei ollut edes mitenkään tarpeellista laskutus-tarkoituksiin. Seitlinger ei totisesti ollut antanut suostumustaan tällaiseen henkilötietojensa käyttöön. Ainoa syy kaikkien ylimääräisten tietojen keruulla ja säilytyksellä oli Itävallan vuoden 2003 televiestintälaki.

212 Yhdistetyt asiat C-293/12 ja C-594/12 *Digital Rights Ireland ja Seitling ja muut*, EUTI 8.4.2014



Seitlinger nosti näin ollen Itävallan perustuslakituomioistuimessa kanteen, jossa hän väitti, että televiestintäpalvelujen tarjoajan lakisääteiset velvollisuudet rikkoivat hänen EU:n perusoikeuskirjan 8 artiklan mukaisia perusoikeuksiaan.

EUTI ottaa kantaa ainoastaan sille esitetyn ennakkoratkaisupyynnön tunnusmerkistöön. Kansallinen tuomioistuin ratkaisee pääasian.

Unionin tuomioistuimen on periaatteessa vastattava sille esitettyihin kysymyksiin. Se ei voi kieltäytyä antamasta ennakkoratkaisua sillä perusteella, että sen vastaus ei olisi merkityksellinen eikä oikea-aikainen pääasian kannalta. Se voi kuitenkin jättää vastaamatta, jos kysymys ei kuulu sen toimivaltaan.

Lopuksi, jos EU:n toimielimen tai elimen väitetään rikkoneen SEUT 16 artiklassa taatuja tietosuojaoikeuksia henkilötietojen käsittelyn yhteydessä, rekisteröity voi saattaa asian unionin yleisen tuomioistuimen käsiteltäväksi (EU:n toimielinten tietosuoja-asetuksen 32 artiklan 1 ja 4 kohta). Sama koskee Euroopan tietosuojavaltuutetun tällaisista rikkomuksista tekemiä päätöksiä (EU:n toimielinten tietosuoja-asetuksen 32 artiklan 3 kohta).

Unionin yleinen tuomioistuin on toimivaltainen ratkaisemaan EU:n toimielinten tietosuoja-asetukseen liittyviä asioita, mutta jos henkilö haluaa käyttää oikeuskeinoa EU:n toimielimen tai elimen työntekijänä, hänen on nostettava kanne EU:n virkamiestuomioistuimessa.

Esimerkki: Asiassa *Euroopan komissio v. The Bavarian Lager Co. Ltd*<sup>213</sup> tuodaan esiin erilaiset EU:n toimielinten tai elinten tietosuojaan liittyviä toimia tai päätöksiä vastaan käytettävissä olevat oikeuskeinot.

Bavarian Lager oli pyytänyt Euroopan komissiolta täydellisen pöytäkirjan komission pitämästä kokouksesta, jonka se väitti liittyneen yritystä koskeneisiin oikeudellisiin kysymyksiin. Komissio oli hylännyt pyynnön yksityiselämän- ja henkilötietojen suojaan liittyvien ensisijaisten etujen perusteella.<sup>214</sup> Bavarian Lager valitti tästä päätöksestä EU:n toimielinten tietosuoja-asetuk-

<sup>213</sup> Asia C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd.*, EUTI 29.6.2010.

<sup>214</sup> Ks. perustelujen analyysi asiakirjassa EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bryssel, saatavana osoitteessa: [www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24\\_Bavarian\\_Lager\\_EN.pdf](http://www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf).

sen 32 artiklan nojalla EUTI:een, tarkemmin ottaen ensimmäisen oikeusasteen tuomioistuimeen (joka oli unionin yleisen tuomioistuimen edeltäjä). Asiassa T-194/04, *Bavarian Lager v. komissio*, ensimmäisen oikeusasteen tuomioistuin kumosi päätöksen, jolla komissio hylkäsi asiakirjapyyntö. Euroopan komissio valitti päätöksestä unionin tuomioistuimeen. Unionin tuomioistuin (suuri jaosto) kumosi ensimmäisen oikeusasteen tuomioistuimen tuomion ja vahvisti Euroopan komission asiakirjapyyntö hylkäyksen.

### 5.3.4. Sanktiot

**EN-oikeudessa** yleissopimuksen 108 10 artiklassa määrätään, että sopimuspuolten on toteutettava asianmukaiset rangaistukset ja oikeuskeinot sen kansallisen lainsäädännön rikkomisesta, jolla yleissopimuksessa 108 mainitut tietosuojan peruseriaatteen toteutetaan.<sup>215</sup> **EU-oikeudessa** tietosuojadirektiivin 24 artiklassa säädetään, että ”jäsenvaltioiden on toteutettava tarvittavat toimenpiteet tämän direktiivin säännösten täydellisen soveltamisen varmistamiseksi ja määriteltävä erityisesti sanktiot, joita sovelletaan tämän direktiivin mukaisesti säädettyjen säännösten rikkomistapauksissa”.

Molemmissa instrumenteissa on jätetty jäsenvaltioille paljon harkintavaltaa asianmukaisten sanktioiden ja oikeuskeinojen valintaan. Kummassakaan ei anneta erityisiä ohjeita asianmukaisten sanktioiden luonteen tai tyyppin osalta eikä esimerkkejä erilaisista sanktioista.

Kuitenkin:

*”Vaikka EU:n jäsenvaltioilla on tietty harkintavalta, kun ne määrittelevät asianmukaisimmat toimenpiteet EU-oikeudesta johdettujen oikeuksien suojaamiseksi, niiden tulisi SEU 4 artiklan 3 kohdassa tarkoitetun vilpittömän yhteistyön periaatteen mukaisesti kunnioittaa tehokkuuden, tasapuolisuuden, oikeasuhteisuuden ja varoittavuuden vähimmäisvaatimuksia”.*<sup>216</sup>

EUTI on useasti todennut, että kansallisessa lainsäädännössä ei voida täysin vapaasti määritellä sanktioita.

<sup>215</sup> Asia nro 20511/03, *I. v. Suomi*, EIT 17.7.2008; asia nro 2872/02, *K.U. v. Suomi*, EIT 2.12.2008.

<sup>216</sup> FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, 2/2012, Wien, 1.10.2012, 27 s.

Esimerkki: Asiassa *Von Colson ja Kamann v. Land Nordrhein-Westfalen*<sup>217</sup> EYTI totesi, että kaikkien jäsenvaltioiden, joille direktiivi on osoitettu, on toteuttava kansallisessa oikeusjärjestyksessään ja direktiivissä asetettujen tavoitteiden mukaisesti kaikki direktiivin täyden vaikutuksen varmistamiseksi tarvittavat toimenpiteet. Tuomioistuin totesi, että vaikka jäsenvaltioilla on vapaus valita tavat ja keinot direktiivin täytäntöönpanon varmistamiseksi, vapaus ei vaikuta niitä koskevaan velvoitteeseen. Yksilöillä on erityisesti oltava tehokkaat oikeuskeinot, joilla he voivat vaatia ja käyttää oikeuksiaan niiden täydessä laajuudessa. Todellisen ja tehokkaan suojan saavuttamiseksi oikeuskeinoihin on liityttävä rangaistus- ja/tai korvausmenettelyjä, jotka johtavat sanktioihin, joilla on ennaltaehkäisevä vaikutus.

EU:n toimielimille ja elimille voidaan määrätä EU:n tietosuojalainsäädännön rikkomuksista sanktioina vain kurinpitoseuraamuksia EU:n toimielinten tietosuoja-asetuksen erityisen soveltamisalan vuoksi. Asetuksen 49 artiklassa säädetään, että ”jos Euroopan yhteisöjen palveluksessa oleva virkamies tai muu toimihenkilö tahallaan tai tuottamuksellisesti jättää täyttämättä tämän asetuksen mukaiset velvollisuutensa, hänelle voidaan määrätä kurinpitoseuraamus –”.

<sup>217</sup> Asia C-14/83, *Sabine Von Colson ja Elisabeth Kamann v. Land Nordrhein-Westfalen*, EYTI 10.4.1984.



# 6

## Rajan yli tapahtuva henkilötietojen siirto



EU	Katetut aiheet	EN
<b>Rajan yli tapahtuva tietojen siirto</b>		
Tietosuojadirektiivi, 25 artiklan 1 kohta Asia C-101/01, <i>Bodil Lindqvist</i> , EYTI 6.11.2003	Määritelmä	Yleissopimus 108, lisäpöytäkirja, 2 artiklan 1 kohta
<b>Vapaa tietojen siirto</b>		
Tietosuojadirektiivi, 1 artiklan 2 kohta	EU:n jäsenvaltioiden välillä	
	Yleissopimuksen 108 osapuolien välillä	Yleissopimus 108, 12 artiklan 2 kohta
Tietosuojadirektiivi, 25 artikla	Kolmansiin maihin, joissa on riittävä tietosuojan taso	Yleissopimus 108, lisäpöytäkirja, 2 artiklan 1 kohta
Tietosuojadirektiivi, 26 artiklan 1 kohta	Kolmansiin maihin erityisissä tapauksissa	Yleissopimus 108, lisäpöytäkirja, 2 artiklan 2 kohdan a alakohta
<b>Rajoitettu tietojen siirto kolmansiin maihin</b>		
Tietosuojadirektiivi, 26 artiklan 2 kohta Tietosuojadirektiivi, 26 artiklan 4 kohta	Sopimuslausekkeet	Yleissopimus 108, lisäpöytäkirja, 2 artiklan 2 kohdan b alakohta  Sopimuslausekkeiden laatimista koskeva opas
Tietosuojadirektiivi, 26 artiklan 2 kohta	Konsernin sisäiset sitovat tietosuojasäännöt	

EU	Katetut aiheet	EN
<p>Esimerkkejä:                      EU:n ja Yhdysvaltojen välinen matkustajarekisterisopimus                      EU:n ja Yhdysvaltojen välinen SWIFT-sopimus</p>	<p>Erityiset kansainväliset sopimukset</p>	

Tietosuojadirektiivissä ei ainoastaan säädetä vapaasta tietojen siirrosta jäsenvaltioiden välillä, vaan siinä myös asetetaan vaatimuksia henkilötietojen siirrolle EU:n ulkopuolisiin kolmansiin maihin. EN on myös tunnustanut kolmansiin maihin raja yli tapahtuvaa tietojen siirtoa koskevien täytäntöönpanosääntöjen tärkeyden, ja se hyväksyi vuonna 2001 yleissopimuksen 108 lisäpöytäkirjan. Lisäpöytäkirjaan sisällytettiin sopimuspuolien ja EU:n jäsenvaltioiden tärkeimmät rajan yli tapahtuvaa tietojen siirtoa koskevat määräykset.

## 6.1. Rajan yli tapahtuvan tietojen siirron luonne

### Keskeiset kohdat

- Rajan yli tapahtuvalla tietojen siirrolla tarkoitetaan henkilötietojen siirtoa vastaanottajalle, joka on vieraan lainkäyttövallan alainen.

Yleissopimuksen 108 lisäpöytäkirjan 2 artiklan 1 kohdassa määritellään rajan yli tapahtuva tietojen siirto henkilötietojen siirroksi yleissopimuksen osapuoliin kuulumattoman valtion tai järjestön vastaanottajalle, joka on vieraan lainkäyttövallan alainen. Tietosuojadirektiivin 25 artiklan 1 kohdassa säännellään ”käsiteltävien tai siirron jälkeen käsiteltäviksi tarkoitettujen henkilötietojen siirtoa kolmanteen maahan”. Tällainen tietojen siirto on sallittu ainoastaan, jos siinä noudatetaan yleissopimuksen 108 lisäpöytäkirjan 2 artiklassa ja EU:n jäsenvaltioiden osalta lisäksi tietosuojadirektiivin 25 ja 26 artiklassa asetettuja sääntöjä.

Esimerkki: Asiassa *Bodil Lindqvist*<sup>218</sup> EYTI totesi, että ”sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumerosa tai antamalla tietoja heidän työ-

<sup>218</sup> Asia C-101/01, *Bodil Lindqvist*, EYTI 6.11.2003, 27, 68 ja 69 kohta.

suhteestaan ja harrastuksistaan, on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä”.

Tämän jälkeen tuomioistuin toi esiin, että direktiivi sisältää myös erityiset säännöt, joilla sallitaan jäsenvaltioiden valvoa henkilötietojen siirtoa kolmansiin maihin.

Kuitenkin, kun otetaan huomioon internetin kehitysaste silloin, kun direktiiviä laadittiin, sekä se, että direktiivissä ei ole internetin käyttöön soveltuvia kriteerejä, ”ei voida olettaa yhteisöjen lainsäätäjän aikoneen tulevaisuuden varalta sisällyttää käsitteeseen ’henkilötietojen siirto kolmansiin maihin’ tilannetta, jossa – henkilö laittaa henkilötietoja Internet-sivulle, vaikka tiedot saatetaankin tällä tavoin sellaisten kolmansissa maissa olevien henkilöiden saataville, joilla on tähän tarvittavat tekniset välineet”.

Toisin sanoen, jos direktiiviä ”tulkittaisiin siten, että kyse on henkilötietojen siirrosta kolmanteen maahan aina kun henkilötietoja ladataan Internet-sivulle, kyse olisi välttämättä siirrosta kaikkiin sellaisiin kolmansiin maihin, joissa on Internetiin pääsyn edellyttämät tekniset välineet. [Direktiivissä] säädetty erityinen järjestelmä muuttuisi näin välttämättä Internetissä suoritettujen toimenpiteiden osalta soveltamisalaltaan yleiseksi järjestelmäksi. Kun komissio toteaisi – –, että jo yhdessä kolmannessa maassa ei kyetä turvaamaan riittävää tietosuojaa, jäsenvaltioilla olisi nimittäin heti velvollisuus estää kaikki henkilötietojen laittaminen Internetiin.”

Periaate, jonka mukaan pelkkää (henkilö)tietojen julkaisemista ei pidetä rajan yli tapahtuvana tietojen siirtona, sovelletaan myös tietoverkossa saatavilla oleviin julkisiin rekistereihin ja joukkotiedotusvälineisiin, kuten (sähköisiin) sanomalehtiin ja televisioon. Ainoastaan viestintää, joka on suunnattu tarkoin määritellyille vastaanottajille, voidaan pitää ”rajan yli tapahtuvana tietojen siirtona”.

## 6.2. Vapaa tietojen siirto jäsenvaltioiden tai sopimuspuolien välillä

### Keskeiset kohdat

- Henkilötietojen siirtoa toiseen Euroopan talusalueen jäsenvaltioon tai toiseen yleissopimuksen 108 osapuolena olevaan valtioon ei saa rajoittaa.

**EN-oikeudessa** yleissopimuksen 12 artiklan 2 kohdassa määrätään, että henkilötietoja on voitava siirtää vapaasti yleissopimuksen osapuolina olevien valtioiden välillä. Kansallisessa lainsäädännössä ei saa rajoittaa henkilötietojen vientiä toisen sopimuspuolen alueelle, paitsi jos

- tietojen erityinen luonne edellyttää sitä,<sup>219</sup> tai
- tarkoituksena on välttää tietojen siirtoa kolmansiin maihin koskevien kansallisten säännösten kiertäminen.<sup>220</sup>

**EU-oikeudessa** tietojen vapaan liikkuvuuden rajoittaminen tai estäminen jäsenvaltioiden välillä tietosuojan nojalla on kielletty tietosuojadirektiivin 1 artiklan 2 kohdassa. Tietojen vapaan liikkuvuuden aluetta laajennettiin **Euroopan talusalueetta (ETA) koskevalla sopimuksella**,<sup>221</sup> jolla Islanti, Liechtenstein ja Norja liitettiin sisämarkkinoihin.

Esimerkki: Jos sellaisen kansainvälisen yritysryhmän tytäryhtiö, jolla on toimipaikkoja useissa EU:n jäsenvaltioissa, muun muassa Sloveniassa ja Ranskassa, siirtää henkilötietoja Sloveniasta Ranskaan, tällaista tietojen siirtoa ei saa rajoittaa eikä kieltää Slovenian kansallisessa lainsäädännössä.

Mutta jos sama slovenialainen tytäryhtiö haluaa siirtää samat henkilötiedot emoyhtiölleen Yhdysvaltoihin, slovenialaisen tietojen viejän on noudatettava

<sup>219</sup> Yleissopimus 108, 12 artiklan 3 kohdan a alakohta.

<sup>220</sup> *Ibid.*, 12 artiklan 3 kohdan b alakohta.

<sup>221</sup> Neuvoston ja komission päätös, tehty 13 päivänä joulukuuta 1993, Euroopan yhteisöjen ja niiden jäsenvaltioiden sekä Itävallan tasavallan, Suomen tasavallan, Islannin tasavallan, Liechtensteinin ruhtinaskunnan, Norjan kuningaskunnan, Ruotsin kuningaskunnan ja Sveitsin valaliiton välisen Euroopan talusalueetta koskevan sopimuksen tekemisestä, EYVL 1994 L 1.



tietojen siirrosta sellaisiin kolmansiin maihin, joissa ei ole riittävää tietosuojaa, annetussa Slovenian laissa määriteltyä menettelyä, ellei emoyhtiö ole sitoutunut noudattamaan yksityisyyden suojaa koskevia safe harbour -periaatteita, vapaaehtoisia käytännesääntöjä, joilla turvataan riittävä tietosuojan taso (ks. 6.3.1 kohta).

ETA-maihin muilla kuin sisämarkkinoiden piiriin kuuluvilla aloilla, esimerkiksi rikosten tutkinnan alalla, tapahtuvaan tietojen siirtoon ei kuitenkaan sovelleta tietosuojadi-  
rektiivin säännöksiä eikä tietojen vapaan liikkuvuuden periaate näin ollen koske sitä. EN-oikeudessa kaikki alat kuuluvat yleissopimus 108 ja sen lisäpöytäkirjan sovelta-  
misalaa, joskin sopimuspuolet voivat määrätä poikkeuksia. Kaikki ETA:n jäsenval-  
tiot ovat myös yleissopimuksen 108 osapuolia.

## 6.3. Vapaa tietojen siirto kolmansiin maihin

### Keskeiset kohdat

- Tietojen siirtoa kolmansiin maihin ei saa rajoittaa kansallisella lainsäädännöllä, jos
  - vastaanottajan tietosuojan tason riittävyys on varmistettu; tai
  - se on tarpeellista rekisteröidyn erityisten etujen tai muiden henkilöiden oikeutet-  
tujen etujen, erityisesti tärkeiden yleisten etujen, vuoksi.
- Tietosuojan tason riittävyys kolmannessa maassa tarkoittaa, että kyseisen maan kansallisessa lainsäädännössä on pantu tehokkaasti täytäntöön tietosuojan pääperiaatteet.
- EU-oikeudessa kolmannen maan tietosuojan tason riittävyyden arvioi Euroopan komissio. EN-oikeudessa riittävyyden arviointi on jätetty kansallisen lainsäädännön piiriin.

### 6.3.1. Vapaa tietojen siirto riittävän suojan takia

**EN-oikeuden** nojalla kansallisessa lainsäädännössä voidaan sallia vapaa tietojen siirto muihin kuin sopimusmaihiin, jos vastaanottava valtio tai järjestö takaa aiotulle tietojen siirrolle riittävän suojan tason.<sup>222</sup> Kansallisessa lainsäädännössä päätetään, miten tietosuojan taso toisessa maassa arvioidaan ja kuka sen arvioi.

<sup>222</sup> Yleissopimus 108, lisäpöytäkirja, 2 artiklan 1 kohta.

**EU-oikeudessa** vapaasta tietojen siirrosta kolmansiin maihin, joissa tietosuojan taso on riittävä, säädetään tietosuojadirektiivin 25 artiklan 1 kohdassa. Kun tason ei tarvitse olla sama vaan riittävä, tietosuoja voidaan panna täytäntöön eri tavoin. Direktiivin 25 artiklan 6 kohdan mukaan Euroopan komissio on toimivaltainen arvioimaan tietosuojan tason riittävyyttä kolmannessa maassa tekemällä tietosuojan riittävyyden toteavia päätöksiä ja kuulemalla arvioinnista tietosuojatyöryhmää, joka on tehnyt merkittävää työtä 25 ja 26 artiklan tulkinnan selkeyttämiseksi.<sup>223</sup>

Komission tekemä tietosuojan riittävyyden toteavalla päätöksellä on sitova vaikutus. Jos komissio julkaisee Euroopan unionin virallisessa lehdessä tiettyä maata koskevan tietosuojan riittävyyden toteavan päätöksen, kaikkien ETA:n jäsenvaltioiden ja niiden elinten on noudatettava päätöstä, eli tietoja on voitava siirtää kyseiseen maahan ilman kansallisten viranomaisten tarkistus- tai lupamenettelyä.<sup>224</sup>

Euroopan komissio voi myös arvioida osia maan oikeusjärjestelmästä tai keskittyä vain tiettyihin aiheisiin. Komissio on esimerkiksi tehnyt tietosuojan riittävyyden toteavan päätöksen yksinomaan Kanadan yksityisestä kauppalainsäädännöstä.<sup>225</sup> Lisäksi on paljon tietosuojan riittävyyden toteavia päätöksiä, jotka perustuvat EU:n ja kolmansien maiden välisiin sopimuksiin. Nämä päätökset koskevat yksinomaan tietyn tyyppistä tietojen siirtoa, kuten matkustajarekisterien siirtoa lentoyhtiöiltä muiden maiden rajavalvontaviranomaisille silloin, kun lentoyhtiö lentää EU:sta tiettyihin ulkomaankohteisiin (ks. 6.4.3 kohta). Viime vuosina EU:n ja kolmansien maiden välillä tehtyjen erityisten sopimusten perusteella tapahtunut tietojen siirto ei yleensä ole edellyttänyt tietosuojan riittävyyden toteavaa päätöstä, koska sopimusten on oletettu takaavan samantasoisien tietosuojan tason.<sup>226</sup>

223 Ks. esim. tietosuojatyöryhmä (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers*, WP 74, Bryssel, 3. kesäkuuta 2003; ja tietosuojatyöryhmä (2005), *valmistelusiakirja 24 päivänä lokakuuta 1995 annettun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25. marraskuuta 2005.

224 Jatkuvasti päivitettävä luettelo maista, joissa tietosuoja on todettu riittäväksi, julkaistaan Euroopan komission oikeusasiodien pääosaston verkkosivustolla osoitteessa [http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm).

225 Euroopan komissio (2002), 20 päivänä joulukuuta 2001 tehty päätös 2002/2/EY henkilötietojen suojaaja ja sähköisiä asiakirjoja koskevan Kanadassa voimassaolevan lain tarjoaman tietosuojan riittävyydestä Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti, EYVL 2002 L 2.

226 Esimerkiksi matkustajarekisteritietojen käyttöä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskeva Amerikan yhdysvaltojen ja Euroopan unionin sopimus (EUVL 2012 L 215, s. 5–14) tai terrorismin rahoituksen jäljittämisohjelmia varten tapahtuvaa rahaliikenteen sanomanvälitystietojen käsittelyä ja siirtämistä Euroopan unionista Yhdysvaltoihin koskeva Euroopan unionin ja Amerikan yhdysvaltojen välinen sopimus, (EUVL 2010 L 8, s. 11–16).

Yksi tärkeimmistä tietosuojan riittävyyden toteavista päätöksistä ei oikeastaan liity lainkaan säännöksiin,<sup>227</sup> vaan se koskee käytännesääntöjen kaltaisia sääntöjä, joita kutsutaan safe harbor periaatteiksi. EU ja Yhdysvallat laativat nämä periaatteet yhdysvaltalaisia liikeyrityksiä varten. Safe harbour järjestelmään liitytään antamalla Yhdysvaltojen kauppaministeriölle vapaaehtoinen sitoumus, joka liitetään ministeriön julkaisemaan luetteloon. Koska yksi riittävän tietosuojan tärkeistä edellytyksistä on tietosuojan täytäntöönpanon tehokkuus, safe harbour järjestelmään liittyy myös tiettyä valtiollista valvontaa: safe harbour järjestelmään voivat liittyä ainoastaan ne yritykset, jotka ovat Yhdysvaltojen liittovaltion kauppakomission valvonnan alaisia.

### 6.3.2. Vapaa tietojen siirto erityisissä tapauksissa

**EN-oikeudessa** yleissopimuksen 108 lisäpöytäkirjan 2 artiklan 2 kohdassa sallitaan henkilötietojen siirto kolmansiin maihin, joissa ei ole riittävää tietosuojaa, jos siirto on kansallisessa lainsäädännössä sallittu ja se on tarpeellista:

- rekisteröidyn erityisen edun perusteella; tai
- muiden henkilöiden oikeutetun ja erityisesti merkittävän yleisen edun perusteella.

**EU-oikeudessa** tietosuojadirektiivin 26 artiklan 1 kohta sisältää samansuuntaisia säännöksiä kuin yleissopimuksen 108 lisäpöytäkirja.

Direktiivin mukaan rekisteröidyn edut voivat oikeuttaa vapaan tietojen siirron kolmanteen maahan, jos:

- rekisteröity on yksiselitteisesti antanut suostumuksensa suunniteltuun siirtoon; tai
- rekisteröity tekee – tai aikoo tehdä – sopimuksen, joka selkeästi edellyttää tietojen siirtoa ulkomaiselle vastaanottajalle; tai
- rekisterinpitäjä on tehnyt sivullisen kanssa sopimuksen rekisteröidyn edun mukaisesti; tai

<sup>227</sup> Euroopan komissio (2000), komission päätös, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä, EYVL 2000 L 215.

- siirto on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi; tai
- siirto tehdään julkisesta rekisteristä; tämä tapaus liittyy yleiseen etuun saada tietoa julkisista rekistereistä.

Muiden henkilöiden oikeudet edut voivat riittää perusteeksi maan rajan yli tapahtuvalle tietojen siirrolle.<sup>228</sup>

- tärkeän yleisen edun turvaamiseksi, kun kyseessä ei ole kansallinen tai yleinen turvallisuus, sillä ne eivät kuulu tietosuojadirektiivin soveltamisalaan; tai
- oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Edellä esitetyt tapaukset ovat poikkeuksia sääntöön, jonka mukaan tietojen siirto muihin maihin edellyttää, että vastaanottavassa maassa on riittävä tietosuojan taso. Poikkeuksia on aina tulkittava suppeasti. Tietosuojatyöryhmä on painottanut tätä toistuvasti tietosuojadirektiivin 26 artiklan 1 kohdan osalta, erityisesti silloin, kun tietojen siirron perusteena on suostumus.<sup>229</sup> Tietosuojatyöryhmä on todennut, että suostumuksen oikeudellista merkitystä koskevat yleiset säännöt pätevät myös direktiivin 26 artiklan 1 kohdan yhteydessä. Jos esimerkiksi työsuhtetilanteessa on epäselvää, ovatko työntekijät todellakin antaneet suostumuksensa vapaaehtoisesti, tietojen siirron perusteena ei voida käyttää direktiivin 26 artiklan 1 kohdan a alakohtaa. Tällöin sovelletaan 26 artiklan 2 kohtaa, jossa edellytetään, että kansalliset tietosuojaviranomaiset antavat luvan tietojen siirtoon.

## 6.4. Rajoitettu tietojen siirto kolmansiin maihin

### Keskeiset kohdat

- Ennen tietojen viemistä kolmansiin maihin, joissa ei ole taattu riittävää tietosuojan tasoa, rekisterinpitäjän on voi olla tarpeen esittää tietojen siirtoa koskeva suunnitelman valvontaviranomaiselle tutkintaa varten.

<sup>228</sup> Tietosuojadirektiivi, 26 artiklan 1 kohdan d alakohta.

<sup>229</sup> Ks. erityisesti tietosuojatyöryhmä (2005), *valmisteluasiakirja 24 päivänä lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25. marraskuuta 2005.

- Rekisterinpitäjän, joka haluaa viedä tietoja maasta, on selvitettävä tutkinnan aikana kaksi asiaa:
  - tietojen siirrolle kyseiselle vastaanottajalle on oikeudellinen peruste; ja
  - vastaanottaja on toteuttanut toimenpiteitä riittävän tietosuojan tason varmistamiseksi.
- Vastaanottajan tietosuojan riittävä taso voidaan osoittaa muun muassa
  - tietoja vievän rekisterinpitäjän ja ulkomaisen tietojen vastaanottajan välisillä sopimusehdoilla; tai
  - konsernin sisäisillä sitovilla tietosuojasäännöillä (BCR), joita sovelletaan yleensä tietojen siirtoon monikansallisessa yritysryhmässä.
- Tietojen siirtoa ulkomaisille viranomaisille voidaan myös säännellä erityisellä kansainvälisellä sopimuksella.

Tietosuojadirektiivin ja yleissopimuksen 108 lisäpöytäkirjan nojalla kansallisen lainsäädännön puitteissa on mahdollista luoda järjestelmiä tietojen siirtoon kolmansiin maihin, joissa ei ole taattu riittävää tietosuojan tasoa, kunhan rekisterinpitäjä varmistaa erityisillä järjestelyillä, että vastaanottaja toteuttaa riittävät suojatoimet, ja kunhan rekisterinpitäjä voi todistaa tämän toimivaltaiselle viranomaiselle. Tämä vaatimus mainitaan selkeästi vain yleissopimuksen 108 lisäpöytäkirjassa, mutta sitä pidetään myös tietosuojadirektiivin nojalla tavallisena menettelynä.

### 6.4.1. Sopimuslausekkeet

Sekä **EN-oikeudessa** että **EU-oikeudessa** mainitaan tietoja vievän rekisterinpitäjän ja kolmannessa maassa sijaitsevan vastaanottajan väliset sopimuslausekkeet keinona taata siirron riittävä tietosuojan taso.

**EU:ssa** Euroopan komissio on laatinut tietosuojatyöryhmän avulla mallisopimuslausekkeet, jotka on komission päätöksellä virallisesti hyväksytty näytöksi tietosuojan riittävästä tasosta.<sup>230</sup> Koska komission päätökset ovat kaikilta osiltaan velvoittavia jäsenvaltioissa, rajan yli tapahtuvan tietojen siirron valvonnasta vastaavien kansallisten viranomaisten on tunnustettava nämä mallisopimuslausekkeet omissa menettelyissään.<sup>231</sup> Näin ollen, jos tietoja vievä rekisterinpitäjä ja kolmannessa

230 Tietosuojadirektiivi, 26 artiklan 4 kohta.

231 SEUT, 288 artikla.

maassa sijaitseva vastaanottaja sopivat ja allekirjoittavat nämä lausekkeet, valvontaviranomaisen kuuluu pitää sitä riittävänä näyttönä asianmukaisista suojaustoimista.

Se, että EU:n oikeudellisessa kehityksessä on mallisopimuslausekkeet, ei estä rekisterinpitäjiä muotoilemasta muita tilanteeseen sopivia sopimuslausekkeitä. Niillä on kuitenkin tuotettava samantasoinen suoja kuin mallisopimuslausekkeilla. Mallisopimuslausekkeiden tärkeimmät ominaisuudet ovat seuraavat:

- kolmatta osapuolta suojaava edunsaajalauseke, jonka nojalla rekisteröidyt voivat käyttää sopimusoikeuksia, vaikka he eivät olisi sopimuksen osapuolia;
- tietojen vastaanottajan tai maahantuojan suostuminen tietoja vievän rekisterinpitäjän kansallisen valvontaviranomaisen ja/tai tuomioistuimen menettelyyn riitapauksissa.

Rekisterinpitäjien välistä tietojen siirtoa varten on olemassa kaksi mallisopimuslausekesarjaa, joista rekisterinpitäjät voivat valita.<sup>232</sup> Rekisterinpitäjien ja henkilötietojen käsittelijöiden välistä tietojen siirtoa varten on vain yksi sarja mallisopimuslausekkeitä.<sup>233</sup>

**EN-oikeudessa** yleissopimuksen 108 nojalla perustettu neuvoa-antava komitea on laatinut oppaan sopimuslausekkeiden laatimiseen.<sup>234</sup>

---

232 Näistä 1. sarja esitetään Euroopan komission (2001) päätöksen liitteessä: komission päätös, tehty 15 päivänä kesäkuuta 2001, direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen kolmansiin maihin siirtoa varten, EYVL 2001 L 181; ja 2. sarja esitetään Euroopan komission päätöksen (2004) liitteessä: komission päätös, tehty 27 päivänä joulukuuta 2004, päätöksen 2001/497/EY muuttamisesta vaihtoehtoisten mallisopimuslausekkeiden ottamiseksi käyttöön henkilötietojen kolmansiin maihin siirtoa varten, EUVL 2004 L 385.

233 Euroopan komissio (2010), komission päätös, annettu 5 päivänä helmikuuta 2010, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen siirtoa varten kolmansiin maihin sijoittautuneille henkilötietojen käsittelijöille, EUVL 2010 L 39.

234 EN, yleissopimuksen 108 nojalla perustettu neuvoa-antava komitea (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data*.

## 6.4.2. Konsernin sisäiset sitovat tietosuojasäännöt

Monenvälisiin konsernin sisäisiin sitoviin tietosuojasääntöihin (BCR) osallistuu hyvin usein monta eurooppalaista tietosuojaviranomaista yhtä aikaa.<sup>235</sup> Ennen kuin yrityksiä sitovat säännöt voidaan hyväksyä, niiden luonnos on lähetettävä vakiomuotoisten hakulomakkeiden kanssa johtavalle viranomaiselle.<sup>236</sup> Johtava viranomainen nimetään vakiomuotoisessa hakulomakkeessa. Tämä viranomainen välittää tiedon kaikille valvontaviranomaisille niissä ETA-maissa, joissa yritysryhmällä on tytäryhtiöitä, joskin niiden osallistuminen yrityksiä sitovien sääntöjen arviointiprosessiin on vapaaehtoista. Vaikka arvioinnin tulos ei olekaan sitova, kaikkien asianomaisten tietosuojaviranomaisten tulisi liittää se virallisiin lupamenettelyihinsä.

## 6.4.3. Erityiset kansainväliset sopimukset

EU on sopinut erityisistä järjestelyistä kahdenlaisten tietojen siirtoa varten:

### Matkustajarekisterit

Lentoyhtiöt keräävät varausprosessin yhteydessä matkustajarekisteritietoja (engl. Passenger Name Records, PNR), joihin kuuluvat nimet, osoitteet, luottokorttitiedot ja matkustajien istuinpaikat. Yhdysvaltojen lainsäädännön mukaan lentoyhtiöiden on saatettava nämä tiedot sisäisen turvallisuuden ministeriön saataville, ennen kuin matkustajat lähtevät lennolle. Tämä koskee sekä lentoja Yhdysvaltoihin että lentoja sieltä pois.

Jotta turvataan riittävä matkustajarekisterien siirron tietosuojantasoa direktiivin 95/46/EY mukaisesti, vuonna 2004 hyväksyttiin ns. PNR -paketti<sup>237</sup>, joka sisälsi lausunnon yhdysvaltain sisäisen turvallisuuden ministeriön tietojen käsittelyn tietosuojan tason riittävydestä.

235 Asianmukaisten yrityksiä sitovien sääntöjen sisältö ja rakenne selitetään asiakirjoissa tietosuojatyöryhmä (2008), *Working document setting up a framework for the structure of Binding Corporate Rules*, WP 154, Bryssel, 24. kesäkuuta 2008; ja tietosuojatyöryhmä (2008), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*, WP 153, Bryssel, 24. kesäkuuta 2008.

236 Tietosuojatyöryhmä (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data*, WP 133, Bryssel, 10. tammikuuta 2007.

237 *Neuvoston päätös 2004/496/EY* 17,5,2004 Lentoyhtiöiden PNR eli matkustajarekisteritietojen käsittelimestä ja siirtämisestä Yhdysvaltojen sisäisen turvallisuus ministeriön alaiselle tulli- ja rajavartiolaitokselle koskevan Euroopan yhteisön ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä, EUVL L 183, s 83 ja *Komission päätös 2004/535/EY*, 14.05.2004 Yhdysvaltojen tulli- ja rajavartiolaitokselle toimitettavien lentomatikustajista koskevaan matkustajarekisteriin sisältyvien henkilötietojen suojan riittävästä tasosta, EUVL L 235 s. 11-22.

EYTI kumosi PNR paketin<sup>238</sup>, jonka seurauksena EU ja Yhdysvallat allekirjoittivat kaksi erillistä sopimusta, joilla oli samankaltaiset tarkoitukset: ensinnäkin muodostaa oikeudellisen perusteen matkustajarekisteritietojen luovuttamiselle yhdysvaltojen viranomaisille ja toiseksi riittävän tietosuojan tason varmistaminen vastaanottavassa maassa.

Vuonna 2012 solmittiin ensimmäinen sopimus tietojen jakamisesta ja hallinnoinnista EU:n jäsenvaltioiden ja Yhdysvaltojen välillä. Sopimus sisälsi useita puutteita, joten se korvattiin samana vuonna uudella sopimuksella, jossa oikeusvarmuus taataan paremmin<sup>239</sup>. Uudessa sopimuksessa on merkittäviä parannuksia. Siinä rajoitetaan ja selvennetään tarkoituksia, joihin tietoja voidaan käyttää, joita ovat muun muassa vakavan kansainvälisen rikollisuuden ja terrorismin torjuminen. Sopimuksessa vahvistetaan myös tietojen säilytysaika: kuuden kuukauden jälkeen, tiedot on tehtävä tunnistettomiksi. Jos tietoja käytetään väärin, on jokaisella oikeus Yhdysvaltojen lainsäädännön mukaisesti hallinnollisiin ja oikeudellisiin muutoksenhakuineihin. Jokaisella on myös oikeus tarkastaa omat matkustajarekisteritietonsa ja pyytää sisäisen turvallisuuden ministeriöltä niiden korjaamista, jos tiedot ovat virheellisiä.

Sopimus tuli voimaan 1. heinäkuuta 2012, ja se on voimassa seitsemän vuotta eli vuoteen 2019 asti.

Euroopan unionin neuvosto hyväksyi joulukuussa 2011 EU:n ja Australian välisen sopimuksen matkustajarekisteritietojen käsittelemisestä ja siirtämisestä.<sup>240</sup> EU:n ja Australian välillä matkustajarekisteritiedoista tehty sopimus on osa EU:n toimintaohjelmaa, johon kuuluvat kokonaisvaltaiset ohjeet matkustajarekisteritietojen

238 Yhdistetyt asiat C-317/04 ja C-318/04, *Euroopan parlamentti v. Euroopan unionin neuvosto ja Euroopan yhteisöjen komissio*, EYTI 30.5.2006 57, 58 ja 59 kohdat, joiden mukaan henkilötietojen suoja riittävästä tasosta tehty päätös ja sopimus tietojen käsittelystä ovat suljettu tietosuojadirektiivin soveltamisalan ulkopuolelle.

239 *Council Decision 2012/472/EU*, annettu 26.4.2012, matkustajarekisteritietojen käyttöä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriölle koskevan Amerikan yhdysvaltojen ja Euroopan unionin sopimuksen tekemisestä EUVL 2012 L 215/4. Sopimuksen teksti on liitetty tähän päätökseen, EUVL 2012 L 215 s. 5-14.

240 *Neuvoston päätös 2012/381/EU*, annettu 13 päivänä joulukuuta 2011, lentoliikenteen harjoittajien PNR- eli matkustajarekisteritietojen käsittelemistä ja siirtämistä Australian tulli- ja rajavartiolaitokselle koskevan Euroopan unionin ja Australian välisen sopimuksen tekemisestä, joka korvasi aikaisemman sopimuksen vuodelta 2008, EUVL 2012 L 186/3. Sopimuksen teksti on liitetty tähän päätökseen, EUVL 2012 L 186, s. 4-16.



siirtoon,<sup>241</sup> EU:n matkustajarekisteritietoja koskevan järjestelmän luominen<sup>242</sup> ja sopimusten neuvottelemine kolmansien maiden kanssa.<sup>243</sup>

## Rahaliikenteen sanomanvälitystiedot

Belgiaan sijoittautunut Society for Worldwide Interbank Financial Telecommunication (SWIFT), joka hoitaa suurimman osan eurooppalaisten pankkien maailmanlaajuisista rahansiirroista, pitää yhtä tietojenkäsittelykeskusta Yhdysvalloissa, ja Yhdysvaltojen valtiovarainministeriö pyysi sitä luovuttamaan tietoja terrorismin tutkintaa varten.<sup>244</sup>

EU:n näkökulmasta näiden pohjimmiltaan eurooppalaisten tietojen luovuttamiselle ei ollut oikeudellista perustetta. Ne olivat saatavilla Yhdysvalloissa vain siksi, että yksi SWIFTin tietojenkäsittelykeskuksista sijaitsi Yhdysvalloissa.

EU ja Yhdysvallat tekivät vuonna 2010 erityisen sopimuksen, niin kutsutun SWIFT-sopimuksen, jolla luotiin tarvittava oikeudellinen peruste ja taattiin riittävä tietosuojaja.<sup>245</sup>

- 
- 241 Ks. erityisesti komission tiedonanto matkustajarekisteritietojen (PNR) siirtoa kolmansiin maihin koskevasta kokonaisvaltaisesta lähestymistavasta, KOM(2010) 492 lopullinen, Bryssel, 21. syyskuuta 2010. Katso myös WP 29 tietosuojaryhmän (2010), *lausunto 7/2010 matkustajarekisteritietojen (PNR) siirtoa kolmansiin maihin koskevasta kokonaisvaltaisesta lähestymistavasta annetusta komission tiedonannosta*, WP 178, Brysselissä 12. marraskuuta 2010.
- 242 Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden ehkäisemistä, paljastamista, tutkimista ja syytteesenpanoa varten, KOM(2011) 32 lopullinen, Bryssel, 2. helmikuuta 2011. Euroopan parlamentti pyysi huhtikuussa 2011 FRA:ta antamaan lausunnon tästä ehdotuksesta ja sen yhdenmukaisuudesta Euroopan unionin perusoikeuskirjan kanssa. Ks. FRA (2011), *Opinion 1/2011 – Passenger Name Record*, Wien, 14. kesäkuuta 2011.
- 243 EU neuvottelee parhaillaan uudesta matkustajarekisteritietoja koskevavasta sopimuksesta a Kanadan kanssa, jolla tullaan korvaamaan tällä hetkellä voimassa oleva sopimus vuodelta 2006 sopimus.
- 244 Ks. tässä yhteydessä tietosuojatyöryhmä (2011), *lausunto 14/2011 rahanpesun ja terrorismin rahoituksen estämiseen liittyvistä tietosuojakysymyksistä*, WP 186, Bryssel, 13. kesäkuuta 2011; tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22. marraskuuta 2006; Commission de la protection de la vie privée (2008), *Control and recommendation procedure initiated with respect to the company SWIFT srl*, päätös, 9. joulukuuta 2008.
- 245 *Neuvoston päätös 2010/412/EU*, annettu 13 päivänä heinäkuuta 2010, terrorismin rahoituksen jäljittämisohjelmaa varten tapahtuvaa rahaliikenteen sanomanvälitystietojen käsittelyä ja siirtämistä Euroopan unionista Yhdysvaltoihin koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä, EUVL 2010 L 195, s. 3 ja 4. Sopimuksen teksti on liitetty tähän päätökseen, EUVL 2010 L 195, s. 5–14.

Tämän sopimuksen mukaan SWIFT:n säilyttämiä rahataloudellisia tietoja luovutetaan myös jatkossa Yhdysvaltojen valtiovarainministeriölle terrorismin tai terrorismin rahoituksen ennaltaehkäisyä, tutkintaa, paljastamista tai syytteesenpanoa varten. Yhdysvaltojen valtiovarainministeriö voi pyytää SWIFT:ltä tietoja, kunhan pyyntö täyttää seuraavat vaatimukset:

- siinä yksilöidään mahdollisimman selvästi rahataloudelliset tiedot;
- siinä perustellaan selkeästi tietojen tarpeellisuus;
- se on rajattu mahdollisimman tarkasti pyydettävien tietojen määrän minimoimiseksi;
- siinä ei pyydetä mitään yhtenäiseen euromaksualueeseen liittyviä tietoja (SEPA).

Europolin on saatava kopio Yhdysvaltojen valtiovarainministeriön esittämästä pyynnöstä ja tarkistettava, onko SWIFT-sopimuksen periaatteita noudatettu<sup>246</sup>. Jos on, niin SWIFT:n on toimitettava rahataloudelliset tiedot suoraan Yhdysvaltojen valtiovarainministeriölle. Ministeriön on säilytettävä rahataloudellisia tietoja suojatussa fyysisessä ympäristössä, jossa niihin on pääsy vain terrorismia tai sen rahoitusta tutkivilla analyytikoilla. Rahataloudellisia tietoja ei myöskään saa liittää mihinkään muuhun tietokantaan. Yleisesti ottaen SWIFT:n toimittamat tiedot on poistettava viimeistään viiden vuoden kuluttua niiden vastaanottamisesta. Yksittäisiä tutkinta- tai syytetoimia koskevia rahataloudellisia tietoja voidaan säilyttää niin kauan kuin niitä tarvitaan kyseisiä toimia varten.

Yhdysvaltojen valtiovarainministeriö voi siirtää SWIFT:ltä saamia tietoja Yhdysvalloissa tai sen ulkopuolella toimiville lainvalvonnasta, yleisestä turvallisuudesta tai terrorismin torjunnasta vastaaville viranomaisille yksinomaan terrorismin tai sen rahoituksen tutkintaa, paljastamista, ennaltaehkäisyä tai syytteesenpanoa varten. Jos edelleen siirrettävät rahataloudelliset tiedot koskevat jonkin EU:n jäsenvaltion kansalaista tai asukasta, tietoja voidaan jakaa kolmannen maan viranomaisille ainoastaan kyseisen jäsenvaltion viranomaisen etukäteen antamalla suostumuksella. Edellä esitetystä voidaan poiketa, jos tietojen jakaminen on välttämätöntä yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhan vuoksi.

<sup>246</sup> Europolin yhteisen valvontaviranomaisen tarkastuksissa on käsitelty Europolin toimintaa tällä alalla. Tarkastusten tulokset ovat saatavilla osoitteessa: <http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=fi>.

Riippumattomat valvojat, mukaan lukien Euroopan komission nimittämä henkilö, seuraavat SWIFT-sopimuksen periaatteiden noudattamista.

Rekisteröidyillä on oikeus saada toimivaltaiselta EU:n tietosuojaviranomaiselta vahvistus siitä, onko heidän henkilötietojen suoja koskevia oikeuksiaan kunnioitettu. Rekisteröidyillä on myös oikeus saada Yhdysvaltojen valtiovarainministeriön SWIFT-sopimuksen nojalla keräämät ja säilyttämät henkilötietonsa oikaistuiksi, poistetuiksi tai suojatuiksi. Rekisteröityjen tiedonsaantioikeuteen voidaan kuitenkin soveltaa tiettyjä oikeudellisia rajoituksia. Jos henkilötietojen antaminen evätään, rekisteröidylle on annettava kirjallinen selvitys epäämisestä ja kerrottava Yhdysvalloissa käytettävissä olevista hallinnollisista ja oikeudellisista oikeussuojakeinoista.

SWIFT-sopimus on voimassa viisi vuotta elokuuhun 2015 asti. Sen voimassaoloa jatketaan ilman eri toimenpiteitä aina yhdellä vuodella kerrallaan, jollei jompikumpi osapuoli ilmoita toiselle osapuolelle ainakin kuusi kuukautta etukäteen aikomuksesta olla jatkamatta sopimusta.



# 7

## Tietosuoja poliisi- ja rikosasioissa

EU	Katetut aiheet	EN
	Yleisesti	Yleissopimus 108
	Poliisiasiat	Poliisiasioita koskeva suositus Asia nro 5335/06, <i>B.B. v. Ranska</i> , EIT 17.12.2009 Asiat nro 30562/04 ja 30566/04, <i>S. ja Marper v. Yhdistynyt kuningaskunta</i> , EIT 4.12.2008 Asia nro 59842/00, <i>Vetter v. Ranska</i> , EIT 31.5.2005
	Tietoverkkorikollisuus	Tietoverkkorikollisuutta koskeva yleissopimus
<b>Tietosuoja poliisi- ja oikeusviranomaisten rajat ylittävän yhteistyön puiteissa</b>		
Tietosuojaa koskeva puitepäätös	Yleisesti	Yleissopimus 108 Poliisiasioita koskeva suositus
Prüm-päätös	Erityiset henkilötiedot: sormenjäljet, dna, huliganismi jne.	Yleissopimus 108 Poliisiasioita koskeva suositus
Europol-päätös Eurojust-päätös Frontex-asetus	Erityisvirastot	Yleissopimus 108 Poliisitietoja koskeva suositus
Schengen II -päätös VIS-asetus Eurodac-asetus CIS-päätös	Erityiset yhteiset tietojärjestelmät	Yleissopimus 108 Poliisiasioita koskeva suositus Asia nro 964/07, <i>Dalea v. Ranska</i> , EIT 2.2.2010

EN ja EU ovat panneet täytäntöön erityisiä oikeudellisia instrumentteja, joilla saataan tasapainoon yksilöiden tietosuojaan liittyvät edut ja yhteiskunnan edut, jotka liittyvät tietojen keräämiseen rikosten torjumiseksi sekä kansallisen ja yleisen turvallisuuden varmistamiseksi.

## 7.1. Tietosuojaa poliisi- ja rikosasioissa käsittelevä EN-oikeus

### Keskeiset kohdat

- Yleissopimus 108 ja EN:n poliisiasioita koskeva suositus kattavat tietosuojan kaikilla poliisityön alueilla.
- Tietoverkkorikollisuutta koskeva yleissopimus (*Budapestin yleissopimus*) on velvoittava kansainvälinen oikeudellinen asiakirja, joka koskee sähköisiä verkkoja vastaan ja niiden kautta tehtyjä rikoksia.

Euroopan tasolla yleissopimus 108 kattaa kaikki henkilötietojen käsittelyn alueet ja sen määräyksillä on tarkoitus säännellä henkilötietojen käsittelyä yleisesti. Näin ollen yleissopimusta 108 sovelletaan tietosuojaan poliisi- ja rikosasioissa, mutta sopimuspuolet voivat rajoittaa sen soveltamisalaa.

Poliisi- ja oikeusviranomaisten oikeudelliset tehtävät usein edellyttävät henkilötietojen käsittelyä, jolla saattaa olla vakavia seurauksia asianosaisille. EN:n vuonna 1987 hyväksymässä poliisitietoja koskevassa suosituksessa annetaan sopimuspuolille ohjeita siihen, miten niiden tulisi panna yleissopimuksen 108 periaatteet täytäntöön poliisiviranomaisten suorittaman henkilötietojen käsittelyn yhteydessä.<sup>247</sup>

### 7.1.1. Poliisiasioita koskeva suositus

EIT on toistuvasti todennut, että poliisiviranomaiset ja kansalliset turvallisuusviranomaiset puuttuvat EIS:n 8 artiklan 1 kohdassa vahvistettuun oikeuteen, kun ne tallentavat ja säilyttävät henkilötietoja. Monessa EIT:n tuomiossa käsitellään tällaisen puuttumisen oikeutusta.<sup>248</sup>

247 EN, ministerineuvosto (1987), suositus Rec(87)15, poliisitoimen tietosuojaa koskeva suositus, 17. syyskuuta 1987.

248 Ks. esim. asia nro 9248/81, *Leander v. Ruotsi*, EIT 26.3.1987; asia nro 24029/07, *M.M. v. Yhdistynyt kuningaskunta*, 13.11.2012; asia nro 19522/09, *M.K. v. Ranska*, EIT 18.4.2013.

Esimerkki: Asiassa *B.B. v. Ranska*<sup>249</sup> EIT päätti, että tuomitun seksuaalirikollisen tietojen kirjaaminen kansalliseen oikeudelliseen tietokantaan kuului EIS:n 8 artiklan soveltamisalaan. Kilpailevat yksilön ja yleiset edut oli kuitenkin pystytty saattamaan tasapainoon toteuttamalla riittävät tietosuojan suojatoimet, kuten rekisteröidyn oikeus pyytää tietojen poistamista, tietojen rajallinen säilytysaika ja tietoihin pääsyn rajaaminen. Tuomioistuin totesi, ettei EIS:n 8 artiklaa ollut rikottu.

Esimerkki: Asiassa *S. ja Marper v. Yhdistynyt kuningaskunta*<sup>250</sup> molemmat kantajat oli asetettu syytteeseen rikoksista, mutta heitä ei ollut tuomittu. Poliisi oli kuitenkin tallentanut ja säilyttänyt heidän sormenjälkensä, dna-tunnisteensa ja solunäytteensä. Säädöksen nojalla henkilön, jota epäiltiin rikoksesta, biometrisiä tietoja voitiin säilyttää rajattomasti, vaikka epäilty olisi myöhemmin julistettu syyttömäksi tai syytteistä olisi luovuttu. EIT katsoi, että yleinen ja valikoimaton henkilötietojen säilyttäminen ilman mitään aikarajaa siten, että syyttömiksi todetuilla henkilöillä oli vain rajoitettu mahdollisuus pyytää henkilötietojensa poistamista, muodosti suhteettoman puuttumisen kantajien oikeuteen nauttia yksityiselämäänsä kohdistuvaa kunnioitusta. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

Useissa muissakin EIT:n tuomioissa käsitellään mahdollisuutta puuttua tietosuojajoikeuteen seurannan kautta.

Esimerkki: Asiassa *Allan v. Yhdistynyt kuningaskunta*<sup>251</sup> viranomaiset olivat salaa tallentaneet vangin yksityisiä keskusteluja hänen ystävänsä kanssa vankilan vierailualueella ja toisen syytetyn kanssa vankilan sellissä. EIT katsoi, että äänen ja kuvan tallennuslaitteiden käyttö kantajan sellissä, vankilan vierailualueella ja toisen vangin päällä rikkoi kantajan oikeutta nauttia yksityiselämäänsä kohdistuvaa kunnioitusta. Koska millään lakiperusteisella järjestelmällä ei tuolloin säännelty poliisin mahdollisuutta käyttää salaisia tallennuslaitteita, kyseinen oikeuteen puuttuminen ei ollut lainmukaista. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

249 Asia nro 5335/06, *B.B. v. Ranska*, EIT 17.12.2009.

250 Asiat nro 30562/04 ja 30566/04, *S. ja Marper v. Yhdistynyt kuningaskunta*, EIT 4.12.2008, 119 ja 125 kohta.

251 Asia nro 48539/99, *Allan v. Yhdistynyt kuningaskunta*, EIT 5.11.2002.

Esimerkki: Asiassa *Klass ym. v. Saksa*<sup>252</sup> kantajat väittivät, että monet Saksan säädökset, joilla sallittiin sähköpostin, postin ja televiestinnän salainen seuranta, rikkoivat EIS:n 8 artiklaa erityisesti siksi, että asianosaisille ei kerrottu valvontatoimenpiteistä eivätkä he voineet vedota tuomioistuimiin sen jälkeen, kun toimenpiteet oli saatettu päätökseen. EIT katsoi, että seurannan uhka väistämättä rajoitti vapaata viestintää posti- ja televiestintäpalvelujen käyttäjien välillä. Tuomioistuin kuitenkin katsoi, että väärinkäytöksiä vastaan oli toteutettu riittävät suojaustoimenpiteet. Saksan lainsäätäjät oli oikeutetusti pitänyt käsiteltäviä toimenpiteitä välttämättöminä demokraattisessa yhteiskunnassa kansallisen turvallisuuden säilyttämiseksi sekä epäjärjestyksen ja rikosten torjumiseksi. Tuomioistuin totesi, ettei EIS:n 8 artiklaa ollut rikottu.

Koska poliisiviranomaisten suorittamalla henkilötietojen käsittelyllä voi olla merkittäviä seurauksia asianosaisille, ovat yksityiskohtaiset tietosuojasäännöt tietokantojen pitämiseksi tällä alalla erityisen tarpeellisia. EN:n poliisiasioita koskevassa suosituksessa käsitellään tätä näkökohtaa antamalla ohjeita siihen, miten tietoja tulisi kerätä poliisityötä varten; miten tiedostoja tulisi säilyttää tällä alalla; kenelle tulisi antaa pääsy näihin tiedostoihin, mukaan lukien edellytykset tietojen luovuttamiselle muiden maiden poliisiviranomaisille; miten rekisteröityjen tulisi voida käyttää tietosuojaoikeuksiaan; ja miten riippumattomien viranomaisten suorittama valvonta tulisi panna täytäntöön. Myös velvollisuutta turvata riittävä tietoturva on käsitelty.

Suosituksessa ei sallita poliisiviranomaisten kerätä rajoittamattomasti kaikenlaisia tietoja. Poliisiviranomaisten oikeus kerätä henkilötietoja on rajoitettu siihen, mikä on tarpeellista todellisen vaaran ehkäisemiseksi tai erityisen rikollisen teon torjumiseksi. Kaiken muun tietojen keruun on perustuttava erityiseen kansalliseen lainsäädäntöön. Arkaluonteisia henkilötietoja tulisi käsitellä vain siinä määrin, kuin se on välttämätöntä tietyn tutkinnan yhteydessä.

Jos henkilötietoja kerätään rekisteröidyn tietämättä, rekisteröidylle tulisi kertoa tiedonkeruusta heti, kun asian paljastaminen ei enää haittaa tutkintaa. Myös teknisellä tarkkailulla tai muuten automatisoidusti tapahtuvan tietojen keräämisen tulisi perustua erityisiin säännöksiin.

Esimerkki: Asiassa *Vetter v. Ranska*<sup>253</sup> nimettömät todistajat olivat syyttäneet kantajaa henkirikoksesta. Kantaja vieraili säännöllisesti ystävänsä kotona,

252 Asia nro 5029/71, *Klass ym. v. Saksa*, EIT 6.9.1978.

253 Asia nro 59842/00, *Vetter v. Ranska*, EIT 31.5.2005.



minne poliisi asensi kuuntelulaitteet tutkintatuomarin luvalla. Tallennettujen keskustelujen perusteella kantaja pidätettiin ja asetettiin syytteeseen henkirikoksesta. Hän vaati tallenteen hylkäämistä todisteena erityisesti siksi, että se ei ollut laillinen. EIT:n mielestä olennaista oli se, oliko kuuntelulaitteiden käyttö ollut ”lainmukaista”. Kuuntelulaitteiden asentaminen yksityisasuntoon ei selkeästikään kuulunut rikosprosessilain 100 pykälän ja sitä seuraavien pykälien soveltamisalaan, sillä niissä käsiteltiin puhelujen salakuuntelua. Lain 81 pykälässä ei määritelty kohtuullisen selkeästi viranomaisten harkintavallan laajuutta tai käyttöä yksityisten keskustelujen tarkkailun sallimisessa. Näin ollen kantaja ei ollut nauttinut vähimmäissuojaa, johon kansalaiset olivat oikeusvaltioperiaatteen nojalla oikeutettuja demokraattisessa yhteiskunnassa. Tuomioistuinin totesi, että EIS:n 8 artiklaa oli rikottu.

Suosituksessa todetaan, että henkilötietoja säilytettäessä tulisi seuraavat tietoryhmät erottaa selkeästi toisistaan: hallinnolliset tiedot ja poliisitiedot; erilaiset rekisteröidyt, kuten epäillyt, tuomitut, uhrit ja todistajat; sekä tosiseikat ja epäilyt tai olettamukset.

Poliisitietojen käyttötarkoitus tulisi olla tarkkaan rajattu. Tämä asia vaikuttaa poliisitietojen luovuttamiseen sivullisille: henkilötietojen luovuttamista tai välittämistä poliisialalla tulisi säännellä sen pohjalta, liittyykö tietojen jakamiseen oikeutettua etua. Henkilötietojen siirtäminen poliisialan ulkopuolelle tulisi sallia vain, kun siihen on selkeä laillinen velvollisuus tai lupa. Tietoja tulisi voida siirtää tai välittää rajojen yli vain muiden maiden poliisiviranomaisille ja erityisten säännösten, mahdollisesti kansainvälisten sopimusten, nojalla, ellei tietojen luovuttaminen olisi välttämätöntä vakavan ja välittömän vaaran torjumiseksi.

Riippumattoman valvojan on varmistettava, että poliisi noudattaa tietojen käsittelyssä kansallista tietosuojalainsäädäntöä. Rekisteröidyillä on oltava kaikki yleissopimuksessa 108 taatut tiedonsaantioikeudet. Jos rekisteröityjen tiedonsaantioikeuksia on rajoitettu yleissopimuksen 108 9 artiklan nojalla tehokkaiden poliisitutkintojen turvaamiseksi, rekisteröidyille on annettava kansallisessa lainsäädännössä mahdollisuus valittaa kansalliselle tietosuojaviranomaiselle tai muulle riippumattomalle elimelle.

## 7.1.2. Tietoverkkorikollisuutta koskeva Budapestin yleissopimus

Rikollisen toiminnan välineenä ja kohteena ovat yhä useammin sähköiset tietojenkäsittelyjärjestelmät, ja siksi tämän haasteen käsittelemiseksi tarvitaan uusia rikos-oikeudellisia säännöksiä. EN onkin laatinut kansainvälisen oikeudellisen instrumentin, [tietoverkkorikollisuutta koskevan yleissopimuksen](#) – eli niin kutsutun Budapestin yleissopimuksen –, jolla puututaan sähköisiä verkkoja vastaan ja niiden kautta tehtyihin rikoksiin.<sup>254</sup> Yleissopimukseen voivat liittyä myös muut kuin EN:n jäsenmaat, ja vuoden 2013 puoliväliin mennessä neljä EN:n ulkopuolista maata – Australia, Dominikaaninen tasavalta, Japani ja Yhdysvallat – oli liittynyt yleissopimukseen ja 12 muuta EN:n ulkopuolista maata oli allekirjoittanut yleissopimuksen tai saanut kutsun liittyä siihen.

Tietoverkkorikollisuutta koskeva yleissopimus on vaikutusvaltaisin kansainvälinen sopimus, jossa käsitellään [internetin](#) tai muun [tietoverkon](#) kautta tehtäviä rikoksia. Siinä vaaditaan sopimuspuolia ajantasaistamaan ja yhdenmukaistamaan rikoslainsäädäntöään seuraavilla aloilla: [tietomurrot](#) ja muut turvallisuusrikkomukset, mukaan lukien [tekijänoikeusrikkokset](#), [tietokoneavusteiset petokset](#), [lapsipornografia](#) ja muut laittomat tietoverkkotoiminnot. Yleissopimuksessa määrätään myös valtuuksista suorittaa tietoverkkoihin kohdistuvia etsintöjä ja telepakkokeinoja tietoverkkorikollisuuden torjumisen yhteydessä. Lopuksi se mahdollistaa tehokkaan kansainvälisen yhteistyön. Yleissopimuksen lisäpöytäkirjassa käsitellään tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisviihamielisten tekojen kriminalisointia.

Vaikka yleissopimus ei ole varsinaisesti tarkoitettu tietosuojan edistämiseen, sillä tehdään rangaistavaksi toimintoja, jotka todennäköisesti rikkovat rekisteröityjen oikeutta henkilötietojensa suojaan. Se myös velvoittaa sopimuspuolet varmistamaan yleissopimuksen täytäntöönpanon yhteydessä riittävän suojan ihmisoikeuksille ja vapauksille, mukaan lukien EIS:n nojalla taatut oikeudet, kuten tietosuojaoikeus.<sup>255</sup>

254 Euroopan neuvosto, ministerikomitea (2001), tietoverkkorikollisuutta koskeva yleissopimus, CETS nro 185, Budapest, 23. marraskuuta 2001. Yleissopimus tuli voimaan 1. heinäkuuta 2004.

255 *Ibid.*, 15 artiklan 1 kohta.

## 7.2. Tietosuoja poliisi- ja rikosasioissa käsittelevä EU-oikeus

### Keskeiset kohdat

- EU:n tasolla tietosuoja poliisi- ja rikosasioissa säännellään ainoastaan poliisi- ja oikeusviranomaisten rajat ylittävän yhteistyön alalla.
- Euroopan poliisivirastolla (Europol) ja Euroopan oikeudellisen yhteistyön yksiköllä (Eurojust), jotka ovat rajat ylittävää lainvalvontaa tukevia ja edistäviä EU:n elimiä, on omat erityiset tietosuojajärjestelynsä.
- Erityisiä tietosuojajärjestelyjä on luotu myös toimivaltaisten poliisi- ja oikeusviranomaisten rajat ylittävään tiedonvaihtoon EU:ssa käytettäviä yhteisiä tietojärjestelmiä varten. Näistä huomionarvoisia ovat erityisesti Schengen II, viisumitietojärjestelmä VIS ja Eurodac, keskitetty järjestelmä, johon on tallennettu sormenjälkitiedot kolmansien maiden kansalaisilta, jotka ovat hakeneet turvapaikkaa jossakin EU:n jäsenvaltiossa.

Tietosujadirektiiviä ei sovelleta poliisi- ja rikosoikeusasioissa. Oppaan 7.2.1 kohdassa kuvaillaan tärkeimpiä tätä alaa koskevia oikeudellisia välineitä.

### 7.2.1. Tietosuoja koskeva puitepäättös

Rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta annetun [neuvoston puitepäättöksen 2008/977/YOS \(tietosuoja koskeva puitepäättös\)](#)<sup>256</sup> tavoitteena on suojata luonnollisten henkilöiden henkilötietoja silloin, kun näitä tietoja käsitellään rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi. Jäsenvaltioiden tai EU:n puolesta toimivat poliisi- ja oikeusalaalla työskentelevät toimivaltaiset viranomaiset. Nämä viranomaiset ovat EU:n virastoja tai elimiä sekä jäsenvaltioiden viranomaisia.<sup>257</sup> Puitepäättöksen soveltamisala rajoittuu tietosuojan turvaamiseen näiden viranomaisten välisessä rajat ylittävässä yhteistyössä – se ei kata kansallista turvallisuutta.

Tietosujaa koskeva puitepäättös nojautuu pitkälti yleissopimuksen 108 ja tietosujadirektiivin sisältämiin periaatteisiin ja määritelmiin.

<sup>256</sup> Euroopan unionin neuvosto (2008), neuvoston puitepäättös 2008/977/YOS, tehty 27 päivänä marraskuuta 2008, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, (*tietosujaa koskeva puitepäättös*), EUVL 2008 L 350.

<sup>257</sup> *Ibid.*, 2 artiklan h alakohhta.

Henkilötietoja saavat käsitellä vain toimivaltaiset viranomaiset, ja niitä voidaan käsitellä vain niihin tarkoituksiin, joihin ne on siirretty tai asetettu saataville. Vastaanottavan jäsenvaltion on noudatettava kaikkia henkilötiedot siirtäneen jäsenvaltion lainsäädännössä tietojenvaihtoa varten säädettyjä rajoituksia. Vastaanottava jäsenvaltio voi kuitenkin tietyin edellytyksin käyttää tietoja muihinkin tarkoituksiin. Toimivaltaisten viranomaisten erityisenä tehtävänä on kirjata ja dokumentoida siirrot, jotta vastuut olisi helpompi selvittää valitustapauksissa. Rajat ylittävässä yhteistyössä saatujen henkilötietojen siirtäminen edelleen kolmansiin maihin edellyttää sen jäsenvaltion suostumusta, josta tiedot ovat peräisin. Tästä säännöstä voidaan tosin poiketa hätätapauksissa.

Toimivaltaisten viranomaisten on toteutettava tarvittavat turvatoimet henkilötietojen suojaamiseksi kaikenlaiselta laittomalta käsittelyltä.

Jokaisen jäsenvaltion on varmistettava, että yhden tai useamman kansallisen valvontaviranomaisen tehtävänä on toimia neuvojana ja valvojana tietosuojaa koskevan puitepäätöksen nojalla annettujen säännösten soveltamisessa. Kuka tahansa henkilö voi myös esittää näille valvontaviranomaisille oikeuksiensa ja vapauksiensa suojelua varten vaateen, joka koskee toimivaltaisten viranomaisten suorittamaa henkilötietojen käsittelyä.

Rekisteröidyllä on oikeus saada informaatioita henkilötietojensa käsittelystä ja tarkastusoikeus omiin tietoihinsa sekä oikeus saada henkilötietonsa oikaistuksi, poistetuiksi tai suojatuiksi. Jos näiden oikeuksien harjoittaminen kielletään pakottavista syistä, rekisteröidyllä on oltava oikeus valittaa toimivaltaiselle kansalliselle valvontaviranomaiselle ja/tai tuomioistuimelle. Jos henkilölle aiheutuu vahinkoa tietosuojaa koskevan puitepäätöksen täytäntöönpanemiseksi annetun kansallisen lain vastaisesta toiminnasta, hänellä on oikeus saada korvaus rekisterinpitäjältä.<sup>258</sup> Yleisesti ottaen rekisteröidyllä on oltava oikeus käyttää oikeussuojakeinoja, jos heille tietosuojaa koskevan puitepäätöksen täytäntöönpanemiseksi annetussa kansallisessa laissa taattuja oikeuksia rikotaan.<sup>259</sup>

---

258 *Ibid.*, 19 artikla.

259 *Ibid.*, 20 artikla.

Euroopan komissio on ehdottanut uudistusta, joka koostuu yleisestä tietosuoja-asetuksesta<sup>260</sup> ja yleisestä tietosuojadirektiivistä.<sup>261</sup> Uusi direktiivi korvaa nykyisen tietosuoja-asetuksen, ja siinä säädetään poliisiyhteistyöhön ja rikosasioissa tehtävään oikeudelliseen yhteistyöhön sovellettavat yleiset periaatteet ja säännöt.

## 7.2.2. Erityiset oikeudelliset instrumentit , joilla säännellään tietosuoja- ja oikeusviranomaisten rajat ylittävän yhteistyön puitteissa

Tietosuoja-asetuksen lisäksi tiettyjen jäsenvaltioiden hallussa olevien tietojen vaihtoa säännellään erilaisilla muilla oikeudellisilla instrumenteilla, kuten jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä tehdyllä neuvoston puitteillä 2009/315/YOS ja neuvoston päätöksellä jäsenvaltioiden rahanpesun selvittelykeskusten välistä yhteistyötä koskevista järjestelyistä, joita noudatetaan tietojenvaihdossa.<sup>262</sup>

Toimivaltaisten viranomaisten rajat ylittävään yhteistyöhön<sup>263</sup> liittyy yhä useammin maahanmuuttotietojen vaihtoa. Tämä oikeuden ala ei kuulu poliisi- ja rikosoikeusasioiden piiriin, mutta se on monella tavalla olennaista poliisi- ja oikeusviranomaisten työn kannalta. Sama koskee tietoja EU:hun tuotavista ja sieltä vietävistä tavaroista. Valvonnan poistuminen EU:n sisäisiltä rajoilta on kasvattanut petosten riskiä ja ajanut jäsenvaltiot tehostamaan yhteistyötä erityisesti kehittämällä rajat ylittävää

260 Euroopan komissio (2012), ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), KOM(2012) 11 lopullinen, Bryssel, 25. tammikuuta 2012.

261 Euroopan komissio (2012), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuojadirektiivi), KOM(2012) 10 lopullinen, Bryssel, 25. tammikuuta 2012.

262 Euroopan unionin neuvosto (2009), neuvoston puitteillä 2009/315/YOS, tehty 26 päivänä helmikuuta 2009, jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä, EUVL 2009 L 93; Euroopan unionin neuvosto (2000), neuvoston päätös 2000/642/YOS, tehty 17 päivänä lokakuuta 2000, jäsenvaltioiden rahanpesun selvittelykeskusten välistä yhteistyötä koskevista järjestelyistä, joita noudatetaan tietojenvaihdossa, EYVL 2000 L 271.

263 Euroopan komissio (2012), komission tiedonanto Euroopan parlamentille ja neuvostolle, lainvalvontayhteistyön vahvistaminen EU:ssa: eurooppalainen tiedonvaihtomalli (EIXM), KOM(2012) 735 lopullinen, Bryssel, 7. joulukuuta 2012.

tiedonsiirtoa jäsenvaltioiden ja EU:n tullilainsäädännön vastaisen toiminnan havaitsemisen ja syyteomien käynnistämisen helpottamiseksi.

## Prüm-päätös

Merkittävä esimerkki virallisesta kansallisten tietojen vaihdon muodossa tapahtuvasta rajat ylittävästä yhteistyöstä on [neuvoston päätös 2008/615/YOS](#) rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajat ylittävän rikollisuuden torjumiseksi (*Prüm-päätös*), jolla Prümin sopimus sisällytettiin EU-oikeuteen vuonna 2008.<sup>264</sup> Prümin sopimus oli kansainvälistä poliisiyhteistyötä koskenut sopimus, jonka Itävalta, Belgia, Ranska, Saksa, Luxemburg, Alankomaat ja Espanja allekirjoittivat vuonna 2005.<sup>265</sup>

Prüm-päätöksen tavoitteena oli auttaa jäsenvaltioita kehittämään tiedonvaihtoa rikollisuuden ehkäisemiseksi ja torjumiseksi kolmella alueella, jotka ovat terrorismi, rajat ylittävä rikollisuus ja laitton maahanmuutto. Tätä varten päätöksessä käsitellään seuraavia asioita:

- automaattinen pääsy dna-tunnisteisiin, sormenjälkitietoihin ja tiettyihin kansallisiin ajoneuvorekisteritietoihin;
- tietojen toimittaminen sellaisten suurtapahtumien yhteydessä, joilla on rajat ylittäviä ulottuvuuksia;
- terrorismirikosten estämiseen tarkoitettujen tietojen toimittaminen;
- muut toimenpiteet rajat ylittävän poliisiyhteistyön tehostamiseksi.

Prüm-päätöksen nojalla käyttöön tarjottavia tietokantoja säännellään yksinomaan kansallisella lainsäädännöllä, mutta tiedonvaihtoon sovelletaan lisäksi Prüm-päätöstä ja nykyään myös tietosuojaa koskevaa puitepäätöstä. Päätöksen nojalla tapahtuvan tietojen siirron valvonnasta vastaavat kansalliset tietosuojaviranomaiset.

<sup>264</sup> Euroopan unionin neuvosto (2008), neuvoston päätös 2008/615/YOS, tehty 23 päivänä kesäkuuta 2008, rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi, EUVL 2008 L 210.

<sup>265</sup> Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Ranskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehty sopimus; saatavilla osoitteessa: <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.

## 7.2.3. Tietosuojat Europolissa ja Eurojustissa

### Eupropol

EU:n lainvalvontavirastolla, Europolilla, on päämaja Haagissa ja kansalliset yksiköt (ENU:t) kaikissa jäsenvaltioissa. Europol perustettiin vuonna 1998; sen nykyinen oikeudellinen asema EU:n toimielimenä perustuu [neuvoston päätökseen Euroopan poliisiviraston perustamisesta \(Europol-päätös\)](#).<sup>266</sup> Europolin tehtävänä on auttaa vähintään kahteen jäsenvaltioon vaikuttavan järjestäytyneen rikollisuuden, terrorismin ja muiden vakavan rikollisuuden muotojen ehkäisemisessä ja tutkinnassa.

Saavuttaakseen tavoitteensa Europol on perustanut Europolin tietojärjestelmän, joka tarjoaa jäsenvaltioille tietokannan, jonka kautta ENU:t voivat vaihtaa rikoksiin liittyviä tiedostelu- ja muita tietoja. Europolin tietojärjestelmän kautta voidaan tarjota saataville tietoja, jotka liittyvät henkilöihin, joita epäillään tai jotka on tuomittu Europolin toimivaltaan kuuluvasta rikoksesta, tai henkilöihin, joiden osalta on tosiasioihin perustuvaa näyttöä siitä, että he aikovat tehdä Europolin toimivaltaan kuuluvia rikoksia. Europol ja ENU:t voivat tallentaa tietoja suoraan Europolin tietojärjestelmään ja hakea sieltä tietoja. Ainoastaan tiedot järjestelmään tallentaneella osapuolella on oikeus muuttaa, oikaista tai poistaa näitä tietoja.

Europol voi, jos se on sen tehtävien suorittamisen kannalta tarpeen, säilyttää, muuttaa ja käyttää analyysitietokannoissa olevia tietoja rikoksista. Analyysitietokantoja perustetaan sellaista tietojen keräämistä, käsittelyä tai käyttöä varten, jonka tarkoituksena on avustaa Europolin yhdessä EU:n jäsenvaltioiden kanssa toteuttamissa rikostutkinnoissa.

Uusien haasteiden edessä Europoliin perustettiin 1. tammikuuta 2013 Euroopan verkkorikostorjuntakeskus.<sup>267</sup> Keskus toimii verkkorikollisuutta koskevan tiedon solmukohtana EU:ssa. Se auttaa reagoimaan nopeasti tietoverkoissa tapahtuviin rikoksiin, kehittää ja ottaa käyttöön digitaalisia tutkintakeinoja ja levittää verkkorikolli-

<sup>266</sup> Euroopan unionin neuvosto (2009), neuvoston päätös, tehty 6 päivänä huhtikuuta 2009, Euroopan poliisiviraston (Europol) perustamisesta, EUVL 2009 L 121 (Europol). Ks. myös komission asetusehdotus, jossa esitetään oikeudellinen kehys uudelle Europolille, joka korvaa nykyisen Europolin, joka on perustettu Euroopan poliisiviraston (Europol) perustamisesta 6 päivänä huhtikuuta 2009 tehdyllä neuvoston päätöksellä 2009/371/YOS, ja Euroopan poliisiakatemia, joka on perustettu Euroopan poliisiakatemia (CEPOL) perustamisesta tehdyllä [neuvoston päätöksellä 2005/681/YOS](#), KOM(2013) 173 lopullinen.

<sup>267</sup> Ks. myös EDPS (2012), *Euroopan tietosuojavaltuutetun lausunto Euroopan komission neuvostolle ja Euroopan parlamentille osoittamasta tiedonannosta "Rikostentorjunta digitaali- ja verkko-rikosten torjuntakeskuksen perustaminen"*, Bryssel, 29. kesäkuuta 2012.

suuden tutkinnan alalla hyväksi todettuja toimintatapoja. Keskuksessa on asetettu painopisteeseen seuraavat verkkorikollisuuden muodot:

- järjestäytyneiden rikollisryhmien tekemät verkkorikokset, jotka tuottavat merkittävää rikoshyötyä, kuten verkkopetokset;
- verkkorikokset, jotka aiheuttavat uhreille vakavaa haittaa, kuten verkossa tapahtuva lasten seksuaalinen hyväksikäyttö;
- verkkorikokset, jotka kohdistuvat unionin elintärkeisiin infrastruktuureihin ja tietojärjestelmiin.

Europolin toimintaan sovelletaan tehostettua tietosuojaa. Europol-päätöksen 27 artiklassa määrätään, että yleissopimuksessa 108 ja poliisitietoja koskevassa suosituksessa automaattisesti käsiteltävien sekä muiden kuin automaattisesti käsiteltävien tietojen käsittelyn osalta vahvistettuja periaatteita on noudatettava. Europolin ja jäsenvaltioiden välisessä tiedonsiirrossa on lisäksi noudatettava tietosuojaa koskevassa puitepäätöksessä asetettuja sääntöjä.

Riippumaton Europolin yhteinen valvontaviranomainen (Europol Joint Supervisory Body) valvoo ja seuraa Europolin toimintaa sen varmistamiseksi, että se on sovellettavan tietosuojalainsäädännön mukaista ja erityisesti että tietojen käsittely ei loukkaa yksilöiden oikeuksia.<sup>268</sup> Jokaisella on tarkastusoikeus Europolin ylläpitämiin henkilörekistereihin sekä oikeus tarvittaessa pyytää henkilötietojensa tarkistamista, korjaamista tai poistamista. Jos henkilö ei tyydy Europolin päätökseen näiden oikeuksien käyttämisestä, hän voi valittaa yhteisen valvontaviranomaisen muutoksenhakukomitealle.

Jos Europolissa säilytettyjen tai käsiteltyjen tietojen oikeudellisista tai asiavirheistä aiheutuu vahinkoja, vahingon kärsinyt voi käyttää oikeussuojakeinoja vain sen jäsenvaltion toimivaltaisessa tuomioistuimessa, jossa vahinko on tapahtunut.<sup>269</sup> Jos vahinko on johtunut siitä, että Europol ei ole täyttänyt velvollisuuksiaan, Europol hyvittää jäsenvaltiolle sen maksamat korvaukset.

---

<sup>268</sup> Europol-päätös, 34 artikla.

<sup>269</sup> *Ibid.*, 52 artikla.



## Eurojust

Vuonna 2002 perustettu Eurojust, on Haagissa päämajaa pitävä EU:n elin, joka edistää oikeudellista yhteistyötä vähintään kahteen jäsenvaltioon vaikuttavien vakavien rikosten tutkinta- ja syytetoimissa.<sup>270</sup> Eurojustilla on toimivalta

- edistää ja parantaa tutkinta- ja syytetoimien koordinoitua jäsenvaltioiden toimivaltaisten kansallisten viranomaisten välillä;
- helpottaa oikeudelliseen yhteistyöhön liittyvien pyyntöjen ja päätösten täytäntöönpanoa.

Eurojustin tehtävien toteuttaminen on kansallisten jäsenten vastuulla. Jokainen jäsenvaltio nimeää Eurojustiin yhden tuomarin tai syyttäjän, jonka asema määräytyy kansallisen lainsäädännön mukaan ja jolla on tarvittava toimivalta suorittaa oikeudellisen yhteistyön edistämiseksi ja parantamiseksi tarvittavat tehtävät. Lisäksi kansalliset jäsenet täyttävät yhdessä kollegiona erityisiä Eurojustin tehtäviä.

Eurojust voi käsitellä henkilötietoja siinä määrin kuin se on tarpeen sen tavoitteiden toteuttamiseksi. Tämä mahdollisuus kattaa kuitenkin vain tarkoin määritellyt tiedot henkilöistä, joita epäillään Eurojustin toimivaltaan kuuluvasta rikoksesta tai osallisuudesta tällaiseen rikokseen tai jotka on tuomittu tällaisesta rikoksesta. Eurojust voi myös käsitellä tiettyjä tietoja, jotka koskevat Eurojustin toimivaltaan kuuluvien rikosten todistajia tai uhreja.<sup>271</sup> Poikkeustapauksissa Eurojust voi käsitellä rajoitetun ajan myös muita rikoksen tekohetken olosuhteisiin liittyviä henkilötietoja, jos niillä on välitöntä merkitystä meneillään oleville tutkintatoimille. Eurojust voi toimivaltansa puitteissa tehdä yhteistyötä muiden EU:n toimielinten, elinten ja virastojen kanssa ja vaihtaa niiden kanssa henkilötietoja. Eurojust voi myös tehdä yhteistyötä ja vaihtaa henkilötietoja kolmansien maiden ja järjestöjen kanssa.

270 Euroopan unionin neuvosto (2002), *neuvoston päätös 2002/187/YOS*, tehty 28 päivänä helmikuuta 2002, Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi, EYVL 2002 L 63; Euroopan unionin neuvosto (2003), *neuvoston päätös 2003/659/YOS*, tehty 18 päivänä kesäkuuta 2003, Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi tehdyn päätöksen 2002/187/YOS muuttamisesta, EUVL 2003 L 44; Euroopan unionin neuvosto (2009), *neuvoston päätös 2009/426/YOS*, tehty 16 päivänä joulukuuta 2008, Eurojustin vahvistamisesta sekä Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi tehdyn päätöksen 2002/187/YOS muuttamisesta, EUVL 2009 L 138 (*Eurojust-päätökset*).

271 *Konsolidoitu versio neuvoston päätöksestä 2002/187/YOS* sellaisena kuin se on muutettuna neuvoston päätöksellä 2003/659/YOS ja neuvoston päätöksellä 2009/426/YOS, 15 artiklan 2 kohta.

Tietosuojan osalta Eurojustin on taattava vähintään Euroopan neuvoston yleissopimuksen 108 ja siihen myöhemmin tehtyjen muutosten periaatteita vastaava tietosuojan taso. Tietojen vaihdossa on noudatettava erityisiä sääntöjä ja rajoituksia, joista on sovittu joko yhteistyösopimuksessa tai käytännön järjestelyissä Eurojustia koskevien neuvoston päätösten ja Eurojustin tietosuojasääntöjen mukaisesti.<sup>272</sup>

Eurojustiin on perustettu riippumaton yhteinen valvontaviranomainen, jonka tehtävänä on valvoa Eurojustin suorittamaa henkilötietojen käsittelyä. Yksityishenkilö voi valittaa yhteiselle valvontaviranomaiselle, jos hän ei tyydy Eurojustin vastaukseen tiedonsaantia tai henkilötietojen korjaamista, suojaamista tai poistamista koskeneeseen pyyntöön. Jos Eurojust käsittelee henkilötietoja lainvastaisesti, se on vastuussa sen jäsenvaltion lainsäädännön mukaisesti, jossa sen päätoimipaikka sijaitsee, eli Alankomaiden lainsäädännön mukaisesti kaikista rekisteröidylle aiheutuneista vahingoista.

## 7.2.4. Tietosuojaja EU-tason yhteisissä tietojärjestelmissä

Sen lisäksi, että jäsenvaltiot voivat vaihtaa keskenään tietoja ja että EU:hun on perustettu erityisiä viranomaisia torjumaan rajat ylittävää rikollisuutta, EU:ssa on otettu käyttöön erilaisia yhteisiä tietojärjestelmiä, joiden kautta toimivaltaiset kansalliset ja EU:n viranomaiset voivat vaihtaa tietoja tiettyihin lainvalvontaan liittyviin tarkoituksiin, kuten maahanmuutto- ja tullilainsäädännön valvontaa varten. Osa näistä järjestelmistä, kuten Schengenin tietojärjestelmä, viisumitietojärjestelmä, Eurodac, Eurosur tai tullitietojärjestelmä, perustuu monenvälisiin sopimuksiin, joita on myöhemmin täydennetty EU:n oikeudellisilla välineillä ja järjestelmillä.

Vuonna 2012 perustettu tietotekniikkavirasto (eu-LISA)<sup>273</sup> vastaa toisen sukupolven Schengenin tietojärjestelmän (SIS II), viisumitietojärjestelmän (VIS) ja Eurodac-järjestelmän operatiivisesta hallinnoinnista pitkällä aikavälillä. Eu-LISA:n päätehtävänä on varmistaa tietojärjestelmien tehokas, turvallinen ja jatkuva toiminta. Se vastaa myös tarvittavien toimenpiteiden toteuttamisesta järjestelmien ja tietojen turvaamiseksi.

272 Säännökset henkilötietojen käsittelyä ja tietosuojaa Eurojustissa koskevasta työjärjestyksestä, EUVL 2005 C 68/01, 19.3.2005, s. 1.

273 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1077/2011, annettu 25 päivänä lokakuuta 2011, vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston perustamisesta, EUVL 2011 L 286.

## Schengenin tietojärjestelmä

Vuonna 1985 Euroopan yhteisöihin kuuluneet Benelux-maat, Saksa ja Ranska tekivät sopimuksen tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla (*Schengenin sopimus*). Sopimuksella oli tarkoitus luoda Schengenin alue, jolla henkilöt voisivat liikkua vapaasti ilman rajatarkastuksia.<sup>274</sup> Rajojen avaamisesta yleiselle turvallisuudelle aiheutuvan uhan vastapainoksi rajatarkastuksia Schengenin alueen ulkorajoilla vahvistettiin ja kansallisten poliisi- ja oikeusviranomaisten välistä yhteistyötä tiivistettiin.

Uusien valtioiden liittyttyä Schengenin sopimukseen koko järjestelmä sisällytettiin lopulta EU:n oikeudelliseen kehykseen *Amsterdamin sopimuksella*.<sup>275</sup> Päätös pantiin täytäntöön vuonna 1999. Schengenin tietojärjestelmän uusin versio, niin kutsuttu SIS II, otettiin käyttöön 9. huhtikuuta 2013. Se palvelee nykyään kaikkien EU:n jäsenvaltioiden lisäksi Islantia, Liechtensteinia, Norjaa ja Sveitsiä.<sup>276</sup> Myös Europol and Eurojust voivat käyttää SIS II järjestelmää.

SIS II sisältää keskusjärjestelmän (C-SIS), kansallisen järjestelmän (N-SIS) jokaisessa jäsenvaltiossa, sekä keskusjärjestelmän ja kansallisten järjestelmien välisen viestintäinfrastruktuurin. C-SIS sisältää tiettyjä jäsenvaltioiden henkilöistä ja esineistä tallentamia tietoja. C-SIS-järjestelmää käyttävät kansalliset rajavalvonta-, poliisi-, tulli-, viisumi- ja oikeusviranomaiset eri puolilla Schengen-alueetta. Jokainen jäsenvaltio käyttää C-SIS:stä kansallista kopiota, jota kutsutaan kansalliseksi Schengenin tietojärjestelmäksi (N-SIS), ja päivittää sitä säännöllisesti siten, että samalla myös C-SIS päivittyy. N-SIS:stä voidaan hakea tietoja ja se antaa kuulutuksen, jos

- henkilöllä ei ole oikeutta tulla Schengen-alueelle tai oleskella siellä; tai
- oikeus- tai lainvalvontaviranomaiset etsivät kyseistä henkilöä tai esinettä; tai

274 Benelux-taloussiiton valtioiden, Saksan liittotasavallan ja Ranskan tasavallan hallitusten välinen sopimus tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla, EYVL 2000 L 239.

275 Euroopan yhteisöt (1997), Amsterdamin sopimus Euroopan unionista tehdyn sopimuksen, Euroopan yhteisöjen perustamissopimusten ja niihin liittyvien tiettyjen asiakirjojen muuttamisesta, EYVL 1997 C 340.

276 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, annettu 20 päivänä joulukuuta 2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL 2006 L 381 (SIS II) ja Euroopan unionin neuvosto (2007), neuvoston päätös 2007/533/YOS, tehty 12 päivänä kesäkuuta 2007, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL 2007 L 205.

- henkilö on ilmoitettu kadonneeksi; tai
- tavarat, kuten setelit, autot, perävaunut, aseet tai henkilötodistukset on ilmoitettu varastetuiksi tai kadonneiksi.

Kun kuulutus on annettu, kansallisten Schengen-tietojärjestelmien kautta käynnistetään jatkotoimet.

SIS II:ssa on uusina toimintoina muun muassa mahdollisuus tallentaa biometrisiä tietoja, kuten sormenjälkiä ja valokuvia; uusia kuulutusluokkia, kuten varastetut veneet, ilma-alukset, kontit tai maksuvälineet; entistä tarkempia kuulutuksia henkilöistä ja esineistä; kopioita eurooppalaisista pidätysmääräyksistä henkilöistä, joita etsitään kiinniottoa tai luovuttamista varten.

Toisen sukupolven Schengenin tietojärjestelmän perustamisesta, toiminnasta ja käytöstä tehty [neuvoston päätös 2007/533/YOS](#) (Schengen II -päätös) kattaa yleissopimuksen 108: ”Tämän päätöksen nojalla käsitellyt henkilötiedot on suojattava Euroopan neuvoston [yleissopimuksen 108] mukaisesti”.<sup>277</sup> Jos kansalliset poliisiviranomaiset käyttävät henkilötietoja Schengen II päätöksen nojalla, yleissopimuksen 108 ja poliisitietoja koskevan suosituksen määräykset on täytynyt saattaa osaksi kansallista lainsäädäntöä.

Toimivaltainen kansallinen valvontaviranomainen kussakin jäsenvaltiossa valvoo kansallista N-SIS-järjestelmää. Sen on erityisesti tarkistettava niiden tietojen laatu, jotka jäsenvaltio tallentaa C-SIS-järjestelmään N-SIS:n kautta. Kansallisen valvontaviranomaisen on varmistettava, että N-SIS:ssä tapahtuva tietojenkäsittely tarkastetaan vähintään joka neljäs vuosi. Kansalliset valvontaviranomaiset ja Euroopan tietosuojavaltuutettu tekevät yhteistyötä ja varmistavat SIS:n koordinoitun valvonnan, kun taas C-SIS:n valvonnasta vastaa Euroopan tietosuojavaltuutettu. Avoimuuden vuoksi ne toimittavat joka toinen vuosi Euroopan parlamentille, neuvostolle ja eu-LISALLE yhteisen toimintaselvityksen.

Yksilöiden oikeutta saada tietoa SIS II:sta voidaan käyttää kaikissa jäsenvaltioissa, sillä jokainen N-SIS on tarkka kopio C-SIS:stä.

<sup>277</sup> Euroopan unionin neuvosto (2007), neuvoston päätös 2007/533/YOS, tehty 12 päivänä kesäkuuta 2007, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL 2007 L 205, 57 artikla.

Esimerkki: Asiassa *Dalea v. Ranska*<sup>278</sup> kantajalta evättiin viisumi Ranskaan, koska Ranskan viranomaiset olivat ilmoittaneet Schengenin tietojärjestelmään, ettei häntä tulisi päästää maahan. Kantaja käytti tarkastusoikeuttaan sekä oikeutta saada ne korjatuiksi tai poistetuiksi ensin Ranskan tietosuojaviranomaiselta ja lopuksi korkeimmasta hallinto-oikeudesta, mutta pyyntö evättiin. EIT katsoi, että kantaja oli kirjattu Schengenin tietojärjestelmään lainmukaisesti ja että kirjaamisen laillisena tarkoituksena oli ollut kansallisen turvallisuuden suojaaminen. Koska kantaja ei ollut osoittanut kärsineensä vahinkoa sen johdosta, että häneltä oli evätty pääsy Schengen-alueelle, ja koska hänen suojaamiseksi mielivaltaisilta päätöksiltä oli toteutettu riittävät toimenpiteet, puuttuminen oikeuteen nauttia yksityiselämään kohdistuvaa kunnioitusta oli ollut oikeasuhteista. Kantajan 8 artiklaan perustuvaa valitusta ei näin ollen otettu tutkittavaksi.

## Viisumitietojärjestelmä

Viisumitietojärjestelmä (VIS), joka on niin ikään eu-LISAn hallinnoima, kehitettiin EU:n yhteisen viisumipolitiikan täytäntöönpanon tueksi.<sup>279</sup> VIS:n avulla Schengen-maat voivat vaihtaa viisumitietoja sellaisen järjestelmän kautta, joka yhdistää Schengen-maiden EU:n ulkopuolella sijaitsevat konsulaatit kaikkien Schengen-maiden ulkorajojen ylityspaikkoihin. VIS käsittelee lyhytaikaista oleskelua tai kauttakulkua varten Schengen-alueelle haettavien viisumien tietoja. VIS:n avulla rajavalvontaviranomaiset voivat tarkistaa biometrisiä tietoja käyttäen, onko viisumin esittävä henkilö sen oikea haltija, ja tunnistaa henkilöt, joilla ei ole asiakirjoja tai joiden asiakirjat ovat väärennetyjä.

Viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 767/2008 (*VIS-asetus*) mukaan VIS:ään voidaan tallentaa vain hakijaa ja hänen viisumejaan koskevia tietoja, valokuvia, sormenjälkiä, linkkejä aiempiin hakemuksiin sekä hakijan mukana matkustavien

<sup>278</sup> Asia nro 964/07, *Dalea v. Ranska*, EIT 2.2.2010.

<sup>279</sup> Euroopan unionin neuvosto (2004), neuvoston päätös, tehty 8 päivänä kesäkuuta 2004, viisumitietojärjestelmän (VIS) perustamisesta, EUVL 2004 L 213; Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008, annettu 9 päivänä heinäkuuta 2008, viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (*VIS-asetus*), EUVL 2008 L 218; Euroopan unionin neuvosto (2008), neuvoston päätös 2008/633/YOS, tehty 23 päivänä kesäkuuta 2008, jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi, EUVL 2008 L 218.

henkilöiden hakemustiedostoja.<sup>280</sup> Ainoastaan jäsenvaltioiden viisumiviranomaiset pääsevät VIS:ään tallentamaan, muuttamaan tai poistamaan tietoja, mutta tietoja voivat hakea viisumiviranomaisten lisäksi myös viranomaiset, joilla on valtuudet tehdä tarkastuksia ulkorajojen ylityspaikoilla sekä maahanmuuttoon ja turvapaikkaan liittyviä tarkastuksia. Kansalliset toimivaltaiset poliisiviranomaiset ja Europol voivat tietyin edellytyksin pyytää päästä VIS:ään tallennettuihin tietoihin terrorismirikosten ja muiden vakavien rikosten torjumista, havaitsemista ja tutkimista varten.<sup>281</sup>

## Eurodac

Eurodacin nimi viittaa englanninkieliseen sanaan dactylogram eli sormenjälkeen. Kyseessä on keskitetty järjestelmä, joka sisältää niiden kolmansien maiden kansalaisten sormenjälkitiedot, jotka ovat hakeneet turvapaikkaa jossakin EU:n jäsenvaltiossa.<sup>282</sup> Järjestelmä on ollut toiminnassa tammikuusta 2003 lähtien, ja sen tarkoituksena on auttaa määrittämään jäsenvaltio, joka on vastuussa turvapaikkahakemuksen käsittelystä niiden perusteiden ja menettelyjen vahvistamisesta, joiden mukaisesti määritetään kolmannen maan kansalaisen johonkin jäsenvaltioon jättämän turvapaikkahakemuksen käsittelystä vastuussa oleva jäsenvaltio, annetun neuvoston asetuksen (EY) N:o 343/2003 (*Dublin II asetus*) mukaisesti.<sup>283</sup> Eurodacin sisältämiä henkilötietoja voidaan käyttää vain Dublin II asetuksen soveltamisen helpottamiseksi; kaikista muista käytöistä rangaistaan.

Eurodac koostuu eu-LISA:n hallinnoimasta keskusyksiköstä, joka on tarkoitettu sormenjälkien tallentamiseen ja vertailemiseen, sekä jäsenvaltioiden ja

280 Viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (VIS-asetus) 9 päivänä heinäkuuta 2008 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 767/2008 5 artikla, EUVL 2008 L 218.

281 Euroopan unionin neuvosto (2008), neuvoston päätös 2008/633/YOS, tehty 23 päivänä kesäkuuta 2008, jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi, EUVL 2008 L 218.

282 Neuvoston asetus (EY) N:o 2725/2000, annettu 11 päivänä joulukuuta 2000, Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten Dublinin yleissopimuksen tehokkaaksi soveltamiseksi, EYVL 2000 L 316; neuvoston asetus (EY) N:o 407/2002, annettu 28 päivänä helmikuuta 2002, tietyistä säännöistä Eurodac-järjestelmän perustamisesta sormenjälkien vertailemista varten Dublinin yleissopimuksen tehokkaaksi soveltamiseksi annetun asetuksen (EY) N:o 2725/2000 täytäntöönpanemiseksi, EYVL 2002 L 62 (*Eurodac-asetukset*).

283 Neuvoston asetus (EY) N:o 343/2003, annettu 18 päivänä helmikuuta 2003, niiden perusteiden ja menettelyjen vahvistamisesta, joiden mukaisesti määritetään kolmannen maan kansalaisen johonkin jäsenvaltioon jättämän turvapaikkahakemuksen käsittelystä vastuussa oleva jäsenvaltio, EUVL 2003 L 50 (*Dublin II -asetus*).

keskustietokannan välisestä sähköisestä tiedonsiirtojärjestelmästä. Jäsenvaltiot ottavat ja siirtävät keskusyksikköön sormenjäljet kaikilta vähintään 14-vuotiailta EU:n ulkopuolisten maiden kansalaisilta ja kansalaisuudettomilta henkilöiltä, jotka hakevat turvapaikkaa niiden alueella tai jotka pidätetään maan ulkorajojen luvattoman ylittämisen takia. Jäsenvaltiot voivat myös ottaa ja siirtää keskusyksikköön sormenjälkiä EU:n ulkopuolisten maiden kansalaisilta ja kansalaisuudettomilta henkilöiltä, jotka tavattu oleskelemasta luvottomasti sen alueelta.

Sormenjälkitiedot tallennetaan Eurodacin tietokantaan salanimetyssä muodossa. Jos tietokannasta löytyy vastaavuus, salanimi ja sormenjälkitiedon ensimmäisenä tallentaneen jäsenvaltion nimi luovutetaan toiselle jäsenvaltiolle. Tämä toinen jäsenvaltio kääntyy sen jälkeen ensimmäisen jäsenvaltion puoleen, koska Dublin II asetuksen nojalla ensimmäinen jäsenvaltio vastaa turvapaikkahakemuksen käsittelemisestä.

Turvapaikanhakijoihin liittyviä henkilötietoja säilytetään Eurodacissa 10 vuotta siitä päivästä lähtien, jolloin sormenjäljet on otettu, paitsi jos rekisteröity saa jonkin EU:n jäsenvaltion kansalaisuuden. Silloin tiedot on välittömästi poistettava. Ulkorajan luvattoman ylittämisen takia pidätettyjen ulkomaalaisten tietoja säilytetään kaksi vuotta. Nämä tiedot on poistettava välittömästi, jos rekisteröity saa oleskeluluvan, poistuu EU:n alueelta tai saa jäsenvaltion kansalaisuuden.

EU:n jäsenvaltioiden lisäksi myös Islanti, Norja, Liechtenstein ja Sveitsi käyttävät Eurodacia kansainvälisten sopimusten pohjalta.

## Eurosur

**Euroopan rajavalvontajärjestelmän (Eurosur)**<sup>284</sup> tarkoituksena on tukea Schengen-alueen ulkorajojen valvontaa havaitsemalla, estämällä ja torjumalla laitonta maahanmuuttoa ja rajat ylittävää rikollisuutta. Se tehostaa tiedonvaihtoa ja operatiivista yhteistyötä kansallisten koordinoitikeskusten ja Frontexin, uuden yhdennetyn rajaturvallisuuden periaatteen kehittämisestä ja soveltamisesta vastaavan EU-viraston,<sup>285</sup> välillä. Sen yleiset tavoitteet ovat seuraavat:

284 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1052/2013, annettu 22 päivänä lokakuuta 2013, Euroopan rajavalvontajärjestelmän (Eurosur) perustamisesta, EUVL 2013 L 295.

285 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1168/2011, annettu 25 päivänä lokakuuta 2011, Euroopan unionin jäsenvaltioiden operatiivisesta ulkorajayhteistyöstä huolehtivan viraston perustamisesta annetun neuvoston asetuksen (EY) N:o 2007/2004 muuttamisesta (*Frontex-asetus*), EUVL 2011 L 394.

- EU:hun laittomasti päässeiden maahanmuuttajien määrän vähentäminen;
- laittomien maahanmuuttajien kuolemantapausten määrän vähentäminen pelastamalla ihmisiä merellä;
- sisäisen turvallisuuden parantaminen koko EU:ssa ehkäisemällä rajat ylittävää rikollisuutta.<sup>286</sup>

Järjestelmä otettiin käyttöön 2. joulukuuta 2013 kaikissa jäsenvaltioissa, joilla on ulkorajoja, ja se otetaan muissa jäsenvaltioissa käyttöön 1. joulukuuta 2014. Asetusta sovelletaan jäsenvaltioiden maarajojen, meriulkorajojen ja ilmarajojen valvontaan.

## Tullitietojärjestelmä

Toinen tärkeä EU:n tasolla käyttöön otettu yhteinen tietojärjestelmä on **tullitietojärjestelmä (TTJ)**.<sup>287</sup> Sisämarkkinoiden perustamisen yhteydessä poistettiin kaikki tavaroiden liikkumiseen EU:n alueella kohdistuneet tarkastukset ja muodollisuudet, mikä kasvatti petosten riskiä. Riskin vastapainoksi tehostettiin jäsenvaltioiden tullihallintojen välistä yhteistyötä. TTJ:n tavoitteena on auttaa jäsenvaltioita kansallisen ja EU:n tulli- ja maatalouslainsäädännön vakavien rikkomusten estämisessä, tutkimuksessa ja syytteenpanossa.

TTJ:n sisältämiin tietoihin kuuluu henkilötietoja, jotka liittyvät tuotteisiin, kuljetusvälineisiin, yrityksiin, henkilöihin sekä pidätettyihin, takavarikoituihin tai menetetyksi tuomittuihin tavaroihin ja käteisvaroihin. Näitä tietoja voidaan käyttää ainoastaan tullisäädännön rikkomisesta epäiltyjen henkilöiden havainnointia, ilmoittamista tai erityistarkastuksia sekä strategista tai operatiivista analyysia varten.

<sup>286</sup> Ks. myös: Euroopan komissio (2008), komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle Euroopan rajavalvontajärjestelmän (Eurosur) luomisesta, KOM(2008) 68 lopullinen, Bryssel, 13.2.2008; Euroopan komissio (2011), Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur), Staff working paper, SEC(2011) 1536 final, Bryssel, 12.12.2011, s. 18.

<sup>287</sup> Euroopan unionin neuvosto (1995), neuvoston säädös, annettu 26 päivänä heinäkuuta 1995, yhteisöjen taloudellisten etujen suojaamista koskevan yleissopimuksen tekemisestä, EYVL 1995 C 316, sellaisena kuin se on muutettuna neuvoston päätöksellä 2009/917/YOS, tehty 30 päivänä marraskuuta 2009, tietotekniikan käytöstä tullialalla (*TTJ-päätös*), EUVL 2009 L 323. Neuvoston asetus N:o 515/97, annettu 13 päivänä marraskuuta 1997, jäsenvaltioiden hallintoviranomaisten keskinäisestä avunannosta sekä jäsenvaltioiden hallintoviranomaisten ja komission yhteistyöstä tulli- ja maatalousasioita koskevan lainsäädännön moitteettoman soveltamisen varmistamiseksi.



TTJ:n tietoihin pääsevät vain kansalliset tulli-, vero-, maatalous-, kansanterveys- ja poliisiviranomaiset sekä Europol ja Eurojust.

Henkilötietojen käsittelyssä on noudatettava asetusta N:o 515/97 sekä TTJ-yleissopimuksessa asetettuja erityisiä sääntöjä<sup>288</sup> sekä tietosuojadirektiivin, EU:n toimielinten tietosuoja-asetuksen, yleissopimuksen 108 ja poliisitietoja koskevan suosituksen säännöksiä ja määräyksiä Euroopan tietosuojavaltuutettu valvoo, että TTJ:n tietojen käsittelyssä noudatetaan asetusta (EY) No 45/2011. Euroopan tietosuojavaltuutettu järjestää vähintään kerran vuodessa tapaamisen kaikkien niiden kansallisten tietosuojaviranomaisten kanssa, jotka ovat toimivaltaisia valvomaan TTJ:ään liittyviä asioita.

---

288 *Ibid.*



# 8

## Muut erityiset Euroopan tietosuojasäädökset

EU	Katetut aiheet	EN
Tietosuojadirektiivi Sähköisen viestinnän tietosuojadirektiivi	Sähköinen viestintä	Yleissopimus 108 Televiestintäpalveluja koskeva suositus
Tietosuojadirektiivi, 8 artiklan 2 kohdan b alakohta	Työelämän suhteet	Yleissopimus 108 Työelämää koskeva suositus Asia nro 62617/00, <i>Copland v. Yhdistynyt kuningaskunta</i> , EIT 3.4.2007
Tietosuojadirektiivi, 8 artiklan 3 kohta	Lääketieteelliset tiedot	Yleissopimus 108 Lääketieteellisiä tietoja koskeva suositus Asia nro 22009/93, <i>Z. v. Suomi</i> , EIT 25.2.1997
Kliinisiä tutkimuksia koskeva direktiivi	Kliiniset tutkimukset	
Tietosuojadirektiivi, 6 artiklan b ja e alakohta, 13 artiklan 2 kohta	Tilastotiedot	Yleissopimus 108 Tilastotietoja koskeva suositus
Asetus (EY) N:o 223/2009 Euroopan tilastoista Asia C-524/01, <i>Huber v. Saksa</i> , EYTI 16.12.2008	Viralliset tilastot	Yleissopimus 108 Tilastotietoja koskeva suositus

EU	Katetut aiheet	EN
Direktiivi 2004/39/EY rahoitusvälineiden markkinoista Asetus (EU) N:o 648/2012 OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä Asetus (EY) N:o 1060/2009 luottoluokituslaitoksista Direktiivi 2007/64/EY maksupalveluista sisämarkkinoilla	Rahataloudelliset tiedot	Yleissopimus 108 Maksutapahtumia ja niihin liittyviä toimintoja koskeva suositus 90(19) Asia nro 12323/11, <i>Michaud v. Ranska</i> , EIT 6.12.2012

Monissa paikoin on Euroopan tasolla hyväksytty erityisiä oikeudellisia välineitä, joilla yleissopimuksen 108 ja tietosuojadirektiivin yleisiä sääntöjä sovelletaan yksityiskohdaisemmin tarkoin määritellyillä aloilla.

## 8.1. Sähköinen viestintä

### Keskeiset kohdat

- EN:n vuonna 1995 antama suositus sisältää erityisiä tietosuojasääntöjä televiestintää ja etenkin puhelinpalveluja varten.
- Viestintäpalveluihin EU:n tasolla liittyvää henkilötietojen käsittelyä säännellään sähköisen viestinnän tietosuojadirektiivillä.
- Sähköisen viestinnän luottamuksellisuus ei kata ainoastaan viestin sisältöä vaan myös liikennetiedot, kuten tiedon viestinnän osapuolista, ajankohdasta ja kestosta, ja paikannustiedot, kuten sen, mistä viesti on lähetetty.

Viestintäverkoissa on tavallista suurempi riski siitä, että käyttäjien oikeutta nauttia yksityisyyden suojaa loukataan, koska niissä tapahtuvan viestinnän kuunteluun ja seurantaan on enemmän teknisiä mahdollisuuksia. Siksi on katsottu tarpeelliseksi antaa erityisiä tietosuojasetuksia, joilla torjutaan viestintäpalvelujen käyttäjille aiheutuvia riskejä.

**EN antoi vuonna 1995 suosituksen** henkilötietojen suojasta televiestintäpalveluiden alalla ja erityisesti puhelinpalveluiden alalla.<sup>289</sup> Suosituksen mukaan henkilötietoja tulisi televiestinnän alalla kerätä ja käsitellä ainoastaan seuraaviin

<sup>289</sup> EN, ministerineuvosto (1995), [suositus Rec\(95\)4](#) henkilötietojen suojasta televiestintäpalveluiden alalla ja erityisesti puhelinpalveluiden alalla, 7. helmikuuta 1995.

tarkoituksiin: käyttäjän yhdistäminen verkkoon, tietyn televiestintäpalvelun tarjoaminen käyttöön, laskutus, varmennus, tekniikan mahdollisimman hyvän toiminnan varmistaminen sekä verkon ja palvelun kehittäminen.

Televiestintäverkkojen käyttöön suoramarkkinoinnissa kiinnitettiin erityistä huomiota. Yleissääntönä on, että suoramarkkinointiviestejä ei saa lähettää tilaajalle, joka on tehnyt selväksi, että hän ei halua vastaanottaa mainosviestejä. Automaattisia soittolaitteita, jotka lähettävät valmiiksi tallennettuja viestejä, voidaan käyttää vain, jos tilaaja on nimenomaisesti antanut suostumuksensa. Kansallisessa lainsäädännössä säädetään alalla sovellettavat yksityiskohtaiset säännöt.

**EU:n oikeuskehityksessä sähköisen viestinnän tietosuojadirektiiviä** ehdotettiin ensimmäisen kerran vuonna 1997, mutta se hyväksyttiin lopulta vasta vuonna 2002. Direktiiviä muutettiin vuonna 2009 tietosuojadirektiivin säännösten täydentämiseksi ja täsmentämiseksi televiestinnän osalta.<sup>290</sup> Sähköisen viestinnän tietosuojadirektiiviä sovelletaan ainoastaan julkisissa sähköisissä verkoissa tarjottaviin viestintäpalveluihin.

Sähköisen viestinnän tietosuojadirektiivissä on jaettu viestinnän aikana tuotetut tiedot kolmeen pääluokkaan:

- viestinnän aikana lähetettyjen viestien sisällön muodostavat tiedot, jotka ovat täysin luottamuksellisia;
- viestinnän muodostamiseen ja ylläpitämiseen tarvittavat niin kutsutut tunnistamistiedot, kuten tiedot viestinnän osapuolista, ajankohdasta ja kestosta;
- tunnistamistietojen osana tiedot, jotka liittyvät viestintävälineen sijaintiin, eli niin kutsutut paikkatiedot; nämä tiedot kertovat myös viestintälaitteiden *käyttäjien* sijainnin ja ne ovat erityisen tärkeitä kannettavien viestintälaitteiden käyttäjien osalta.

<sup>290</sup> Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (*sähköisen viestinnän tietosuojadirektiivi*), EYVL 2002 L 201, sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY muuttamisesta ja Euroopan parlamentin ja neuvoston asetus (EY) N:o 2006/2004, annettu 27 päivänä lokakuuta 2004, kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä, EUVL 2009 L 337.

Palvelun tarjoaja voi käyttää tunnistamistietoja ainoastaan laskutusta ja palvelun teknistä tarjoamista varten. Rekisteröidyn suostumuksella nämä tiedot voidaan kuitenkin luovuttaa muille rekisterinpitäjille, jotka tarjoavat lisäarvopalveluja, kuten kertovat käyttäjälle lähimmän metroaseman tai apteekin tai kyseisen alueen sääennusteen.

Kaiken muun sähköisissä verkoissa tapahtuvaa viestintää koskevan tiedon käytön, esimerkiksi rikosten tutkintaa varten, on sähköistä viestintää koskevan tietosuojadirektiivin 15 artiklan nojalla täytettävä EIS:n 8 artiklan 2 kohdassa asetetut ja perusoikeuskirjan 8 ja 52 artiklassa vahvistetut vaatimukset oikeutetulle puuttumiselle henkilön tietosuojaan.

Sähköisen viestinnän tietosuojadirektiiviin vuonna 2009 tehdyillä muutoksilla<sup>291</sup> direktiiviin lisättiin seuraavat säännöt:

- Sähköpostiviestien lähettämistä suoramarkkinointitarkoituksiin koskevat rajoitukset ulotettiin kattamaan tekstiviesti- ja multimediatelevisiopalvelut sekä muut vastaavat sovellukset. Sähköisen suoramarkkinoinnin lähettäminen on kiellettyä ilman ennalta saatua suostumusta ilman ennakkosuostumusta sähköistä suoramarkkinointia voidaan kohdentaa omaan asiakkaaseen, jos yhteystieto on saatu tuotteen tai palvelun myynnin yhteydessä ja sitä käytetään omien vastaavien tuotteiden tai palveluiden markkinoinnissa. Suomen tietosuojavaltuutettu on katsonut, että yhteystieto on saatu edellä mainitulla tavalla, jos tuote on ostettu kyseistä viestintävälinettä käyttämällä. Lisäksi asiakasta on informoitava yhteystiedon käytöstä sähköisessä suoramarkkinointi tarkoituksessa ja oikeudesta kieltää suoramarkkinointi tietoja kerätessä sekä jokaisen suoramarkkinointiviestin yhteydessä. Kaikkien ehtojen on täyttyvä.
- Jäsenvaltiot veloitettiin varmistamaan oikeussuojakeinot tilanteisiin, joissa ei-toivotun viestinnän kieltoa rikotaan.<sup>292</sup>
- Evästeiden, eli tietokoneen käyttäjän toimia seuraavien ja tallentavien ohjelmistojen, asentaminen ilman tietokoneen käyttäjän lupaa kiellettiin. Kansallisessa

291 Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispuhelinpalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta, EUVL 2009 L 337.

292 Ks. muutettu direktiivi, 13 artikla.

lainsäädännössä tulisi yksityiskohtaisesti määritellä, miten suostumus annetaan riittävän suojan varmistamiseksi.<sup>293</sup>

Jos luvaton käyttö tai tietojen häviäminen tai tuhoaminen aiheuttaa tietoturvaloukkauksen, asiasta on välittömästi ilmoitettava toimivaltaiselle valvontaviranomaiselle. Tilajille on kerrottava, jos tietoturvaloukkauksesta saattaa aiheutua heille vahinkoa.<sup>294</sup>

Tietojen säilyttämistä koskeva direktiivi<sup>295</sup> (kumottu 8. Huhtikuuta 2014), velvoitti viestintäpalvelujen tarjoajat pitämään tunnistamistiedot saatavilla, erityisesti vakavien rikosten torjuntaa varten, vähintään kuuden kuukauden ja enintään kahden vuoden ajan, riippumatta siitä, tarvitsiko palvelun tarjoaja itse tietoja laskutusta tai palvelun teknistä tarjoamista varten.

EU:n jäsenvaltioiden on nimettävä riippumattomat viranomaiset valvomaan säilytetyjen tietojen turvallisuutta.

Televiestintätietojen säilyttäminen on selkeästi puuttumista tietosuojaoikeuteen.<sup>296</sup> Tämän puuttumisen oikeutus on kiistetty lukuisissa oikeudenkäyntimenettelyissä EU:n jäsenvaltioissa.<sup>297</sup>

Esimerkkejä: *Digital Rights Ireland ja Seitlinger ja Muut*<sup>298</sup>, EUTI totesi päätöksensä, että tietojen säilyttämistä koskeva direktiivi on pätemätön. EUTI:n mukaan ” kyseisellä direktiivillä puututaan yksityiselämän suojaa ja henkilötietojen suojaa koskeviin perusoikeuksiin laajamittaisesti ja erityisen vakavasti. Tätä puuttu-

293 *Ibid.*, 5 artikla, ks. myös tietosuojatyöryhmä (2012), *lausunto 04/2012 evästeisiin liittyvää suostumusta koskevasta vapautuksesta*, WP 194, Bryssel, 7. kesäkuuta 2012.

294 Ks. myös tietosuojatyöryhmä (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Bryssel, 5. huhtikuuta 2011.

295 Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL 2006 L 105.

296 EDPS (2011), *lausunto komission arviointikertomuksesta neuvostolle ja Euroopan parlamentille – tietojen säilyttämistä koskeva direktiivi (direktiivi 2006/24/EY)*, 31. toukokuuta 2011.

297 Saksan liittovaltion perustuslakituomioistuin (*Bundesverfassungsgericht*), 1 BvR 256/08, 2.3.2010; Romanian liittovaltion perustuslakituomioistuin (*Curtea Constituțională a României*), No. 1258, 8.11.2009; Tšekin perustuslakituomioistuin (*Ústavní soud České republiky*), 94/2011 Coll., 22.3.2011.

298 Yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland ja Seitlinger ja Muut*.

mista ei myöskään ole riittävästi rajattu sen varmistamiseksi, että puuttuminen tosiasiallisesti rajoittuu vain siihen, mikä on ehdottoman välttämätöntä.”

Ollennainen kysymys sähköisen viestinnän yhteydessä on viranomaisten mahdollisuus puuttua kyseiseen viestintään. Viestinnän valvonta tai sieppaus esimerkiksi kuuntelu- tai salakuuntelulaitteilla, on sallittua vain, jos siitä on säädetty lailla ja se on välttämätöntä demokraattisessa yhteiskunnassa valtion turvallisuuden, yleisen turvallisuuden, valtion taloudellisen edun tai rekisteröidyn tai muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi tai rikosten torjumiseksi.

Esimerkki: Asiassa *Malone v. Yhdistynyt kuningaskunta*<sup>299</sup> kantaja oli asetettu syytteeseen lukuisista rikoksista, jotka liittyivät varastettujen tavaroiden epärehelliseen käsittelyyn. Oikeudenkäynnin aikana ilmeni, että eräs kantajan puhe- luvu oli kuunneltu sisäministerin antaman luvan nojalla. Vaikka kantajan viestintä oli kansallisen lainsäädännön mukaan kuunneltu laillisesti, EIT katsoi, että viranomaisten tällä alalla nauttiman harkintavallan laajuutta ja käyttöä ei ollut mitenkään rajoitettu oikeussäännöillä ja että kyseisestä käytännöstä seuraava puuttuminen tietosuojaan ei siten ollut ”lainmukaista”. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

## 8.2. Työsuhdetta koskevat tiedot

### Keskeiset kohdat

- EN:n työelämää koskevassa suosituksessa esitetään erityiset säännöt työsuhdetta koskevien tietojen suojalle.
- Tietosuojadirektiivissä työsuhdetta käsitellään nimenomaisesti vain arkaluonteisten tietojen käsittelyn yhteydessä.
- Suostumuksen, joka on annettava vapaaehtoisesti, jotta se voisi toimia oikeudellisenä perusteena työntekijän tietojen käsittelylle, pätevyys voidaan kyseenalaistaa, kun otetaan huomioon työnantajan ja työntekijöiden välinen taloudellinen epätasapaino. Suostumuksen antamisen olosuhteet on arvioitava huolellisesti.

EU:n säädöksissä ei oteta erityisesti kantaan henkilötietojen käsittelyyn työsuhhteissa. Tietosuojadirektiivissä työsuhdetta käsitellään nimenomaisesti vain

<sup>299</sup> Asia nro 8691/79, *Malone v. Yhdistynyt kuningaskunta*, EIT 2.8.1984.



direktiivin 8 artiklan 2 kohdassa, joka koskee arkaluonteisten tietojen käsittelyä. EN antoi puolestaan vuonna 1989 työelämää koskevan suosituksen, jota ollaan parhailaan saattamassa ajan tasalle.<sup>300</sup>

Tietosuojatyöryhmän valmisteluasiakirjassa esitetään katsaus yleisimpiin tietosuojaongelmiin työelämässä.<sup>301</sup> Työryhmä analysoi suostumuksen merkitystä työsuhdetta koskevien tietojen käsittelyn oikeudellisena perusteena.<sup>302</sup> Työryhmä totesi, että taloudellinen epätasapaino suostumusta pyytävän työnantajan ja suostumuksen antavan työntekijän välillä herättää usein epäilyjä siitä, onko suostumus annettu vapaaehtoisesti. Siksi olosuhteita, joissa suostumusta on pyydetty, tulisi arvioida huolellisesti, kun selvitetään suostumuksen pätevyyttä työsuhteessa.

Nykyään tavallinen tietosuojaongelma tyypillisellä työpaikalla liittyy oikeuteen valvoa työntekijöiden sähköistä viestintää työpaikalla. Usein esitetään, että ongelma olisi helppo ratkaista kieltämällä viestintävälineiden käyttö yksityisiin tarkoituksiin työpaikalla. Tällainen yleinen kieltö voisi kuitenkin olla suhteeton ja epärealistinen. Seuraava EIT:n tuomio on erityisen kiinnostava tässä yhteydessä:

Esimerkki: Asiassa *Copland v. Yhdistynyt kuningaskunta*<sup>303</sup> korkeakoulun työntekijän puhelimen, sähköpostin ja internetin käyttöä oli seurattu sen selvittämiseksi, käyttikö hän korkeakoulun palveluja liian paljon henkilökohtaisiin tarkoituksiin. EIT katsoi, että työpaikalla soitetut puhelut kuuluivat yksityiselämän ja kirjesalaisuuden piiriin. Siksi tällaiset työpaikalla soitetut puhelut ja kirjoitetut sähköpostiviestit samoin kuin yksityisen internetin käytön seurannasta saadut tiedot olivat suojattuja EIS:n 8 artiklan nojalla. Kantajan tapauksessa ei ollut olemassa mitään säännöksiä, joilla olisi säädetty, missä olosuhteissa työnantajat voivat seurata työntekijöiden puhelimen, sähköpostin ja internetin käyttöä. Oikeuteen puuttuminen ei siten ollut lainmukaista. Tuomioistuin totesi, että EIS:n 8 artiklaa oli rikottu.

300 Euroopan neuvosto, ministerikomitea (1989), *suositus Rec(89)2 jäsenvaltioille työsuhteen hoitamiseksi käytettävien henkilötietojen suojaamisesta*, 18. tammikuuta 1989. Ks. myös yleissopimuksen 108 nojalla perustettu neuvoo-antava komitea, *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation*, 9. syyskuuta 2011.

301 Tietosuojatyöryhmä (2001), *lausunto 8/2001 henkilötietojen käsittelystä työpaikoilla*, WP 48, 13. syyskuuta 2001.

302 Tietosuojatyöryhmä (2005), *valmisteluasiakirja 24 päivänä lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25. marraskuuta 2005.

303 Asia nro 62617/00, *Copland v. Yhdistynyt kuningaskunta*, EIT 3.4.2007.

EN:n työelämää koskevan suosituksen mukaan työntekijää koskevat henkilötiedot olisi kerättävä suoraan työntekijältä itseltään. varten kerättävät henkilötiedot tulisi saada suoraan yksittäiseltä työntekijältä.

Rekrytointia varten kerättävien henkilötietojen on rajoitettava tietoihin, joita tarvitaan hakijoiden soveltuvuuden ja uramahdollisuuksien arviointiin.

Suosituksessa myös nimenomaisesti mainitaan yksittäisten työntekijöiden työsuoritukseen tai mahdollisuuksiin liittyvät arviointitiedot. Arviointitietojen on perustuttava oikeudenmukaisiin ja rehellisiin arviointeihin, eikä niitä saa laatia loukkaavaan muotoon. Tätä edellyttävät tietojen asianmukaisen käsittelyn ja täsmällisyyden periaatteet.

Erityinen tietosuojalainsäädäntöön liittyvä näkökohta työnantajan ja työntekijän välisessä suhteessa on työntekijöiden edustajien asema. Nämä edustajat voivat saada työntekijöiden henkilötietoja vain siinä määrin, kuin he tarvitsevat niitä voidakseen ajaa työntekijöiden etuja.

Työsuhteen hoitamista varten kerättyjä arkaluonteisia henkilötietoja voidaan käsitellä vain tarkoin määritellyissä tapauksissa ja kansallisessa lainsäädännössä asetettujen suojatoimien puitteissa. Työnantajat voivat kysyä työntekijöiltä tai työnhakijoilta tietoja heidän terveydentilastaan tai suorittaa heille lääkärintarkastuksen vain, jos se on tarpeen työtehtäviin soveltuvuuden ratkaisemiseksi, ennalta ehkäisevän terveydenhuollon vaatimusten täyttämiseksi tai sosiaaliturvaetuuksien myöntämiseksi. Terveydentilaa koskevia tietoja ei saa kerätä muualta kuin työntekijältä itseltään, ellei hän ole antanut tälle nimenomaisesti tietoista suostumustaan tai ellei asiasta ole säädetty lailla.

Työelämää koskevan suosituksen mukaan työntekijöille tulisi informoida, mitä tarkoitusta varten heidän henkilötietojaan käsitellään, millaisia tietoja heistä säilytetään ja keille tietoja säännöllisesti luovutetaan sekä tällaisen luovuttamisen tarkoitus ja oikeudellinen peruste. Työnantajien tulisi lisäksi kertoa ennalta työntekijöille, jos työntekijöiden henkilötietojen käsittelyä tai kulunvalvontaa tai tuottavuuden tarkkailua varten otetaan käyttöön tai mukautetaan automaattisia tietojenkäsittelyjärjestelmiä.

Työntekijöillä on oltava oikeus tarkastaa itseään koskevat tiedot sekä oikeus pyytää virheellisten tietojen korjaamista. Jos arviointitietoja käsitellään, työntekijöillä on lisäksi oltava oikeus kiistää arvion oikeellisuus. Näitä oikeuksia voidaan kuitenkin

tilapäisesti rajoittaa sisäisten tutkimusten suorittamista varten. Jos työnantaja kieltäytyy tarkastusoikeuden toteuttamisesta tai korjaamasta tietoja työntekijän vaatimuksen mukaisesti, kansallisessa lainsäädännössä on säädettävä asianmukaiset menettelyt tämän epäämisen riittauttamiseen.

## 8.3. Terveydentilaa koskevat tiedot

### Keskeiset kohdat

- Terveydentilaa koskevat tiedot ovat arkaluonteisia ja siksi niitä suojellaan erityisen tarkasti.

Rekisteröidyn terveydentilaa koskevat henkilötiedot määritellään tietosuojadirektiivin 8 artiklan 1 kohdassa ja yleissopimuksen 108 6 artiklassa arkaluonteisiksi. Terveydentilaa koskeviin tietoihin sovelletaankin tiukempaa tietosuojajärjestelmää kuin tietoihin, jotka eivät ole arkaluonteisia.

Esimerkki: Asiassa *Z. v. Suomi*<sup>304</sup> kantajan entinen aviomies, jolla oli HIV-tartunta, oli syyllistynyt lukuisiin seksuaalirikoksiin. Hänet tuomittiin taposta sillä perusteella, että hän oli tietoisesti asettanut uhrinsa alttiiksi HIV-tartunnalle. Kansallinen tuomioistuin määräsi tuomion koko tekstin ja asiaan liittyvät asiakirjat pidettäväksi salassa 10 vuotta, vaikka kantaja pyysi pidempää salassapitoaikaa. Muutoksenhakutuomioistuin eväsi pyynnön ja esitti tuomiossaan sekä kantajan että hänen entisen aviomiehensä koko nimet. EIT katsoi, ettei oikeuden puuttuminen ollut ollut välttämätöntä demokraattisessa yhteiskunnassa, koska terveydentilaa koskevien tietojen suojaaminen on olennainen edellytys mahdollisuudelle nauttia oikeudesta yksityis- ja perhe-elämään kohdistuvaa kunnioitusta, erityisesti silloin kun on kyse HIV-tartunnasta, johon liittyy monissa yhteiskunnassa vahva leima. Näin ollen tuomioistuin totesi, että kantajan henkilöllisyyttä ja terveydentilaa koskevien tietojen saattaminen saataville muutoksenhakutuomioistuimen tuomiossa esitetyllä tavalla vain 10 vuoden kuluttua tuomiosta, rikkoisi EIS:n 8 artiklaa.

304 Asia nro 22009/93, *Z. v. Suomi*, EIT 25.2.1997, 94 ja 112 kohta; ks. myös asia nro 20837/92, *M.S. v. Ruotsi*, EIT 27.8.1997; asia nro 7508/02, *L.L. v. Ranska*, EIT 10.10.2006; asia nro 20511/03, *I. v. Suomi*, EIT 17.7.2008; asia nro 32881/04, *K.H. ym. v. Slovakia*, EIT 28.4.2009; asia nro 36936/05, *Szuluk v. Yhdistynyt kuningaskunta*, EIT 2.6.2009.

Tietosuojadirektiivin 8 artiklan 3 kohdassa sallitaan terveydentilaa koskevien tietojen käsittely silloin, kun se on tarpeen ennalta ehkäisevää lääketiedettä, lääketieteellisiä diagnooseja, hoidon suorittamista tai terveydenhuollon palvelujen hallintoa varten. Ehtona on kuitenkin, että käsittelyn suorittaa terveydenhuollon ammattikoulutuksen saanut henkilö, jota koskee salassapitovelvollisuus, tai muu henkilö, jolla on vastaava velvoite.<sup>305</sup>

EN:n vuonna 1997 antamassa terveydentilaa koskevia tietoja koskevassa suosituksessa sovelletaan yleissopimuksen 108 periaatteita erityisesti lääketieteen alalla.<sup>306</sup> Ehdotetut säännöt ovat yhdenmukaisia tietosuojadirektiivin sääntöjen kanssa terveydentilaa koskevien tietojen käsittelyn laillisten tarkoitusten, terveydentilaa koskevia tietoja käsittelevien henkilöiden salassapitovelvollisuuden sekä tietojenkäsittelyn avoimuutta, tarkastusoikeutta ja tietojen korjaamista ja poistamista koskevien oikeuksien osalta. Lisäksi terveydenhuollon ammattilaisten laillisesti käsittelemiä tietoja ei voida luovuttaa lainvalvontaviranomaisille, ellei ole toteutettu riittäviä suojatoimia EIS:n 8 artiklassa taattua yksityiselämän kunnioitusta rikkovan luovuttamisen estämiseksi.<sup>307</sup>

Terveydentilaa koskevia tietoja koskeva suositus sisältää vielä erityisiä sääntöjä syntymättömien lasten ja vajaakykyisten henkilöiden terveydentilaa koskevia tietoja sekä geneettisten tietojen käsittelyä varten. Tieteellinen tutkimus tunnustetaan selkeästi syyksi säilyttää tietoja pidempään kuin on tarpeen, mutta tiedot on sitä varten yleensä tehtävä anonyymeiksi. Terveydentilaa koskevia tietoja koskevan suosituksen 12 artiklassa ehdotetaan yksityiskohtaisia sääntöjä tilanteisiin, joissa tutkijat tarvitsevat henkilötietoja, eivätkä anonyymit tiedot riitä.

Pseudonymisoinnin avulla voi olla mahdollista täyttää tieteelliset tarpeet siten, että potilaiden edut pysyvät suojattuina. Tietojen pseudonymisointia tietosuojan edistämiseksi käsitellään tarkemmin [2.1.3 kohdassa](#).

Kansallisella ja Euroopan tasolla on käyty kiivasta keskustelua suunnitelmista tallentaa potilaiden hoitotietoja sähköiseen terveystietojärjestelmään.<sup>308</sup> Valtakunnallisten terveystietojärjestelmien erityisenä piirteenä on, että tiedot olisivat saatavilla yli

305 Ks. myös asia nro 23373/03, *Biriuk v. Liettua*, 25.11.2008.

306 EN, ministerineuvosto (1997), suositus Rec(97)5 jäsenvaltioille lääketieteellisten tietojen tietosuojasta, 13. helmikuuta 1997.

307 Asia nro 1585/09, *Avilkina ym. v. Venäjä*, EIT 6.6.2013, 53 kohta (ei lopullinen).

308 Tietosuojatöryhmä (2007), *valmisteluasiakirja potilastietojen käsittelystä sähköisissä potilastietokannoissa*, WP 131, Bryssel, 15. helmikuuta 2007.

rajojen: tämä näkökohta on erityisen kiinnostava EU:n rajat ylittävän terveydenhuollon kannalta.<sup>309</sup>

Toinen aihe, jonka sääntelystä käydään keskustelua, koskee kliinisiä tutkimuksia, eli uusien lääkkeiden testaamista potilailla dokumentoidussa tutkimusympäristössä; tähänkin aiheeseen liittyy merkittäviä tietosuojakysymyksiä. Ihmisille tarkoitettujen lääkkeiden kliinisiä tutkimuksia säännellään 4 päivänä huhtikuuta 2012 annetulla Euroopan parlamentin ja neuvoston **direktiivillä 2001/20/EY** hyvän kliinisen tutkimustavan noudattamista ihmisille tarkoitettujen lääkkeiden kliinisissä tutkimuksissa koskevien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämisestä (*kliinisiä tutkimuksia koskeva direktiivi*).<sup>310</sup> Euroopan komissio antoi joulukuussa 2012 ehdotuksen asetukseksi, joka korvasi kliinisiä tutkimuksia koskevan direktiivin ja yhtenäistäisi ja tehostaisi tutkimusmenetelmiä.<sup>311</sup>

EU:ssa on lukuisia muitakin lainsäädännöllisiä ja muita aloitteita, jotka liittyvät henkilötietojen käyttöön terveydenhoitoalalla.<sup>312</sup>

## 8.4. Tietojen käsittely tilastollisiin tarkoituksiin

### Keskeiset kohdat

- Tilastollisiin tarkoituksiin kerättyjä tietoja ei voida käyttää mihinkään muuhun tarkoitukseen.
- Muihin tarkoituksiin laillisesti kerättyjä tietoja voidaan käyttää tilastollisiin tarkoituksiin, mikäli käyttäjät noudattavat kansallisessa lainsäädännössä säädettyjä riittäviä suoja-toimia. Tätä varten tulisi erityisesti harkita tietojen tekemistä anonyymeiksi tai pseudonyymeiksi ennen niiden luovuttamista sivullisille.

309 Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU, annettu 9 päivänä maaliskuuta 2011, potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa, EUVL 2011 L 88.

310 Euroopan parlamentin ja neuvoston direktiivi 2001/20/EY, annettu 4 päivänä huhtikuuta 2001, hyvän kliinisen tutkimustavan noudattamista ihmisille tarkoitettujen lääkkeiden kliinisissä tutkimuksissa koskevien jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämisestä, EYVL 2001 L 121.

311 Euroopan komissio (2012), ehdotus Euroopan parlamentin ja neuvoston asetukseksi ihmisille tarkoitettujen lääkkeiden kliinisistä lääketutkimuksista ja direktiivin 2001/20/EY kumoamisesta, KOM(2012) 369 lopullinen., Bryssel, 17. heinäkuuta 2012.

312 EDPS (2013), *Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21<sup>st</sup> century'*, Bryssel, 27. maaliskuuta 2013.

Tietosuojadirektiivissä tietojen käsittely tilastollisiin tarkoituksiin mainitaan siinä yhteydessä, kun käsitellään mahdollisuutta poiketa joistain tietosuojaperiaatteista. Direktiivin 6 artiklan 1 kohdan b alakohdan mukaan käyttötarkoitussidonnaisuuden periaatteesta voidaan poiketa kansallisen lainsäädännön nojalla tietojen myöhemmä tilastollista käsittelyä varten, mutta kansallisessa lainsäädännössä on vahvistettava kaikki tarpeelliset suojatoimet. Direktiivin 13 artiklan 2 kohdassa sallitaan tarkastusoikeuden rajoittaminen kansallisella lainsäädännöllä silloin, kun tietoja käsitellään yksinomaan tilastollisiin tarkoituksiin; tätäkin varten kansallisessa lainsäädännössä on oltava riittävät suojatoimet. Tässä yhteydessä tietosuojadirektiivissä asetetaan erityiseksi vaatimukseksi, että mitään tilastollisiin tarkoituksiin kerättyjä tai luotuja tietoja ei voida käyttää rekisteröityjä koskevien päätösten tekemiseen.

Rekisterinpitäjä voi käyttää laillisesti keräämiään tietoja omiin tilastollisiin tarkoituksiinsa, vaikka tämä poikkeaisikin alkuperäisestä tietojenkäsittely tarkoituksesta. Jos rekisterinpitäjä luovuttaa tietoja tilastollisiin tarkoituksiin sivullisille, tiedot on ennen luovutusta, tapauksesta riippuen, tehtävä joko anonyymeiksi tai pseudonyymeiksi „, ellei rekisteröity ole antanut suostumustaan tai tietojenkäsittelystä ei ole nimenomaisesti säädetty lailla. Tämä perustuu tietosuojadirektiivin 6 artiklan 1 kohdan b alakohdassa esitettyyn vaatimukseen toteuttaa tarpeelliset suojatoimet.

Tietoja käytetään tilastollisiin tarkoituksiin erityisesti silloin, kun kansalliset ja EU:n tilastolaitokset laativat virallisia tilastoja kansallisten ja EU:n säädösten nojalla. Kyseiset säädökset usein velvoittavat kansalaiset ja yritykset luovuttamaan tietoja tilastoviranomaisille. Tilastolaitoksissa työskenteleviä virkamiehiä sitoo salassapitovelvollisuus, jota noudatetaan huolellisesti. Korkea tasoinen salassapitovelvollisuus on edellytys kansalaisten luottamukselle ja sille, että tietoja saataisiin tilastoviranomaisten käyttöön.

[Euroopan tilastoista annettu asetus \(EY\) N:o 223/2009](#) sisältää virallisten tilastojen tietosuojaa koskevat keskeiset säännöt, ja sillä on siten vaikutusta myös virallisten tilastojen sääntelyyn kansallisella tasolla.<sup>313</sup> Asetuksessa vahvistetaan periaate,

313 Euroopan parlamentin ja neuvoston asetus (EY) N:o 223/2009, annettu 11 päivänä maaliskuuta 2009, Euroopan tilastoista sekä salassapidettävien tilastotietojen luovuttamisesta Euroopan yhteisöjen tilastotoimistolle annetun Euroopan parlamentin ja neuvoston asetuksen (EY, Euratom) N:o 1101/2008, yhteisön tilastoista annetun neuvoston asetuksen (EY) N:o 322/97 ja Euroopan yhteisöjen tilasto-ohjelmakomitean perustamisesta tehdyn neuvoston päätöksen 89/382/ETY, Euratom kumoamisesta, EUVL 2009 L 87.

jonka mukaan virallisten tilastojen käsittelyyn on oltava riittävän tarkoin määritelty oikeudellinen peruste.<sup>314</sup>

Esimerkki: Asiassa *Huber v. Saksa*<sup>315</sup> EYTI katsoi, ettei viranomaisen suorittama henkilötietojen keruu ja tallennus tilastollisiin tarkoituksiin ollut itsessään riittävä peruste käsittelyn laillisuudelle. Henkilötietojen käsittelyä säätelevän lain oli lisäksi täytettävä tarpeellisuuden vaatimus, mutta käsiteltävänä olleessa asiassa näin ei ollut.

EN:n vuonna 1997 antama [tilastotietoja koskeva suositus](#) kattaa tilastojen laadinnan niin julkisella kuin yksityiselläkin sektorilla.<sup>316</sup> Suosituksessa esitetyt periaatteet vastaavat edellä kuvattuja tietosuojadirektiivin tärkeimpiä sääntöjä. Suosituksessa annetaan yksityiskohtaisia sääntöjä seuraavilla aihealueilla.

Tietoja, jotka rekisterinpitäjä on kerännyt tilastollisiin tarkoituksiin, ei voida käyttää muihin tarkoituksiin, mutta tietoja, jotka on kerätty muihin tarkoituksiin, voidaan saattaa tilastolliseen käyttöön. Tilastotietoja koskevassa suosituksessa sallitaan jopa tietojen luovuttaminen sivullisille silloin, kun se tapahtuu yksinomaan tilastollisiin tarkoituksiin. Tällöin osapuolien tulisi sopia ja dokumentoida laillisen tilastokäytön laajuus. Koska tällä tavalla ei voida ohittaa rekisteröidyn suostumusta, on oletettava, että kansallisessa lainsäädännössä on lisäksi vahvistettava riittävät suojoimet henkilötietojen väärinkäytön riskien minimoimiseksi, kuten velvollisuus tehdä tiedot anonyymeiksi tai pseudonyymeiksi ennen niiden luovuttamista.

Tilastotutkimusta ammattimaisesti harjoittaville henkilöille tulisi asettaa kansallisessa lainsäädännössä salassapitovelvollisuus – kuten virallisten tilastojen kohdalla yleensä on tehty. Salassapitovelvollisuus tulisi ulottaa myös haastattelijoihin, jotka osallistuvat tietojen keräämiseen rekisteröidyltä tai muilta henkilöiltä.

Jos henkilötietoja käsitellään tilastollisessa tarkoituksessa ja tästä ei ole säädetty lailla, vaaditaan tällaisen tilastollisentutkimuksen lailliseen tekemiseen, joko rekisteröidyn suostumus tai vähintään oikeus kieltää tietojen käsittely tässä tarkoituksessa.

314 Tätä periaatetta tarkennetaan Euroopan tilastoja koskevissa käytännössä, joissa annetaan Euroopan tilastoista annetun asetuksen 11 artiklan mukaisesti eettisiä ohjeita virallisten tilastojen laadintaan, mukaan lukien henkilötietojen harkitsevainen käyttö. Asiakirja on saatavilla osoitteessa: [http://epp.eurostat.ec.europa.eu/portal/page/portal/about\\_eurostat/introduction](http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction).

315 Asia C-524/06, *Huber v. Saksa*, EYTI 16.12.2008, ks. erityisesti 68 kohta.

316 EN, ministerineuvosto (1997), suositus Rec(97)18 tilastollisiin tarkoituksiin kerättyjen ja käsiteltyjen henkilötietojen suojelusta, 30. syyskuuta 1997.

Jos henkilötietoja kerätään tilastollisiin tarkoituksiin haastattelemalla, henkilöille on selkeästi kerrottava, onko tietojen luovuttaminen kansallisen lain mukaan pakollista. Arkaluonteisia tietoja ei tulisi koskaan kerätä niin, että henkilö voidaan tunnistaa, ellei kansallisessa laissa nimenomaisesti sallita sitä.

Jos tilastotutkimusta ei voida toteuttaa anonyymeillä tiedoilla, vaan tarvitaan henkilötietoja, tätä tarkoitusta varten kerätyt tiedot tulisi tehdä anonyymeiksi heti, kun se on mahdollista. Tilastotutkimuksen tuloksista ei ainakaan pidä voida tunnistaa yhtään rekisteröityä, ellei se ole selvästi täysin riskitöntä.

Kun tilastoanalyysi on tehty, siinä käytetyt henkilötiedot tulisi joko poistaa tai tehdä anonyymeiksi. Tilastotietoja koskevassa suosituksessa ehdotetaan, että jälkimmäisessä tapauksessa tunnistetiedot säilytettäisiin erillään muista henkilötiedoista. Tämä tarkoittaa esimerkiksi, että tiedot käsitellään pseudonyymeiksi ja joko salauksen avain tai luettelo tunnistetiedoista tallennettaisiin eri paikkaan kuin pseudonyymit tiedot.

## 8.5. Rahataloudelliset tiedot

### Keskeiset kohdat

- Vaikka rahataloudelliset tiedot eivät ole arkaluonteisia tietoja yleissopimuksessa 108 tai tietosuojadirektiivissä tarkoitetulla tavalla, niiden käsittelyssä on noudatettava erityisiä suoja-toimia tietojen täsmällisyyden ja tietoturvan varmistamiseksi.
- Sähköisissä maksujärjestelmissä on oltava sisäänrakennettuna yksityisyyden suoja.
- Asianmukaisten todentamisjärjestelmien tarve aiheuttaa tällä alalla erityisiä tietosuoaongelmia.

Esimerkki: Asiassa *Michaud v. Ranska*<sup>317</sup> kantaja, ranskalainen asianajaja, riitautti hänelle Ranskan lainsäädännössä asetetun velvollisuuden ilmoittaa hänen asiakkaidensa mahdollista rahanpesutoimintaa koskevista epäilyistä. EIT:n näkemyksen mukaan se, että asianajajia vaaditaan ilmoittamaan hallintoviranomaisille muita henkilöitä koskevia tietoja, jotka he ovat saaneet yhteydenpidossaan näiden henkilöiden kanssa, rajoittaa asianajajien EIS:n 8 artik-

317 Asia nro 12323/11, *Michaud v. Ranska*, EIT 6.12.2012; ks. myös asia nro 13710/88, *Niemietz v. Saksa*, EIT 16.12.1992, 29 kohta, ja asia nro 20605/92, *Halford v. Yhdistynyt kuningaskunta*, EIT 25.6.1997, 42 kohta.



lan mukaista oikeutta nauttia kirjeenvaihtoon ja yksityiselämään kohdistuvaa kunnioitusta, joka kattaa ammatti- ja liiketoiminnan. Oikeuden rajoittaminen oli kuitenkin lainmukaista ja sillä oli laillinen tarkoitus, joka oli epäjärjestyksen ja rikosten ehkäiseminen. Koska asianajajilla oli velvollisuus ilmoittaa epäilyistään vain tarkoin rajatuissa tilanteissa, EIT katsoi, että velvollisuus oli oikeasuhteinen. Näin ollen se totesi, ettei 8 artiklaa ollut rikottu.

Yleissopimukseen 108 sisältyvää tietosuojan yleistä oikeudellista kehystä on sovellettu maksujen alalla vuonna 1990 annetussa EN:n suosituksessa Rec(90)19.<sup>318</sup> Suosituksessa selvennetään tietojen laillisen keruun ja käytön rajoja maksujen ja erityisesti maksukorteille tehtävien maksujen yhteydessä. Lisäksi siinä ehdotetaan kansallisille lainsäätäjille yksityiskohtaisia sääntöjä, jotka koskevat maksutietojen luovuttamista sivullisille, tietojen säilytysaikoja, avoimuutta, tietoturvaa ja rajan yli tapahtuvaa tietojen siirtoa sekä lopuksi valvontaa ja oikeussuojakeinoja. Ehdotetut ratkaisut vastaavat myöhemmin tietosuojadirektiivissä vahvistettua EU:n yleistä tietosuojakehystä.

Rahoitusvälineiden markkinoiden sekä luottolaitosten ja sijoituspalveluyritysten toiminnan säätelemiseksi ollaan parhaillaan valmistelemassa erilaisia oikeudellisia instrumentteja.<sup>319</sup> Toisilla oikeudellisilla instrumenteilla tuetaan sisäpiirikauppojen ja markkinoiden manipuloinnin torjuntaa.<sup>320</sup> Tärkeimmät tietosuojaan liittyvät kysymykset näillä aloilla ovat seuraavat:

- rahataloustoimia koskevien asiakirjojen säilytys;
- henkilötietojen siirto kolmansiin maihin;

318 EN, ministerineuvosto (1990), suositus R Rec(90)19 henkilötietojen suojaamisesta maksutapahtumissa, 13. syyskuuta 1990.

319 Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi rahoitusvälineiden markkinoista ja Euroopan parlamentin ja neuvoston direktiivin 2004/39/EY kumoamisesta, KOM(2011) 656 lopullinen, Bryssel, 20. lokakuuta 2011; Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston asetukseksi rahoitusvälineiden markkinoista sekä OTC-johdannaisista, keskussvastapuolista ja kauppatietorekistereistä annetun asetuksen [Euroopan markkinarakenneseetus] muuttamisesta, KOM(2011) 652 lopullinen, Bryssel, 20. lokakuuta 2011; Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi oikeudesta harjoittaa luottolaitostoimintaa sekä luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta ja finanssiryhmittymään kuuluvien luottolaitosten, vakuutusyritysten ja sijoituspalveluyritysten lisävalvonnasta annetun Euroopan parlamentin ja neuvoston direktiivin 2002/87/EY muuttamisesta, KOM(2011) 453 lopullinen, Bryssel, 20. heinäkuuta 2011.

320 Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston asetukseksi sisäpiirikaupoista ja markkinoiden manipuloinnista (markkinoiden väärinkäyttö), KOM(2011) 651 lopullinen, Bryssel, 20. lokakuuta 2011; Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi sisäpiirikaupoista ja markkinoiden manipuloinnista määrättävistä rikosoikeudellisista seuraamuksista, KOM(2011) 654 lopullinen, Bryssel, 20. lokakuuta 2011.

- puhelinkeskustelujen ja sähköisen viestinnän tallentaminen, mukaan lukien toimivaltaisten viranomaisten valtuus pyytää puhelin- ja televiestintätietoja;
- henkilötietojen luovuttaminen, mukaan lukien seuraamusten julkaiseminen;
- toimivaltaisten viranomaisten valvonta- ja tutkintavaltuudet, mukaan lukien paikan päällä tehtävät tarkastukset ja pääsy yksityisiin tiloihin asiakirjojen takavarikointia varten;
- rikkomuksista ilmoittamisen mekanismit, ts. ilmiantamisjärjestelmät; ja
- jäsenvaltioiden toimivaltaisten viranomaisten ja Euroopan arvopaperimarkkina-  
viranomaisen (EAMV) välinen yhteistyö.

Näillä aloilla on muitakin kysymyksiä, joita on käsitelty tarkemmin, kuten tietojen kerääminen rekisteröityjen taloudellisesta tilanteesta<sup>321</sup> tai rajat ylittävät tilisiirrot, jotka väistämättä johtavat henkilötietojen siirtoon.<sup>322</sup>

---

321 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1060/2009, annettu 16 päivänä syyskuuta 2009, luottoluokituslaitoksista, EUVL 2009 L 302; Euroopan komission, ehdotus Euroopan parlamentin ja neuvoston asetukseksi luottoluokituslaitoksista annetun asetuksen (EY) N:o 1060/2009 muuttamisesta, KOM(2010) 289 lopullinen, Bryssel, 2. kesäkuuta 2010.

322 Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 päivänä marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta, EUVL 2007 L 319.

# Kirjallisuutta

## Luku 1

Araceli Mangas, M. (toim.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

EDRI, *An introduction to data protection*, Bryssel, saatavana osoitteessa [www.edri.org/files/paper06\\_datap.pdf](http://www.edri.org/files/paper06_datap.pdf).

Frowein, J. ja Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berliini, N. P. Engel Verlag.

Grabenwarter, C. ja Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. ja Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. ja Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. ja Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bryssel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, nro 5, s. 281–288.

Warren, S. ja Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review*, nide 4, nro 5, s. 193–220, saatavana osoitteessa [www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf](http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf).

White, R. ja Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

## Luku 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Pariisi, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. ja Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, nide 57, nro 6, s. 1701–1777.

Tinnefeld, M., Buchner, B. ja Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, saatavana osoitteessa [www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/anonymisation](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation).

## Luvut 3-5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. ja Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Euroopan perusoikeusvirasto) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Euroopan unionin julkaisutoimisto (Julkaisutoimisto).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Wien, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Julkaisutoimisto.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, saatavana osoitteessa [www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_impact\\_assessment](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment).

## Luku 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. ja Nouwt, S. (2009), *Reinventing data protection?*, Berliini, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

## Luku 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Julkaisutoimisto, saatavana osoitteessa [www.europol.europa.eu/sites/default/files/publications/europol\\_dpo\\_booklet\\_0.pdf](http://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf).

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime*, ERA Forum, nide 13, nro 3, s. 381–395.

Gutwirth, S., Poullet, Y. ja De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. ja Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, nide 36, nro 5, s. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2, saatavana osoitteessa [www.asser.nl/upload/documents/20130226T013310-cleer\\_13-2\\_web.pdf](http://www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf).

## Luku 8

Büllesbach, A., Gijrath, S., Poulet, Y. ja Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. ja Poulet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y. ja De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y., De Hert, P. ja Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, nide 36, nro 5, s. 722–776.

Rosemary, J. ja Hamilton, A. (2012), *Data protection law and practice*, Lontoo, Sweet & Maxwell.





# Oikeuskäytäntö

## Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöä

### Henkilötietojen saanti

*Gaskin v. Yhdistynyt kuningaskunta*, nro 10454/83, 7.7.1989

*Godelli v. Italia*, nro 33783/09, 25.9.2012

*K.H. ym. v. Slovakia*, nro 32881/04, 28.4.2009

*Leander v. Ruotsi*, nro 9248/81, 26.3.1987

*Odièvre v. Ranska* [suuri jaosto], nro 42326/98, 13.2.2003

### Tietosuojaan saattaminen tasapainoon ilmaisunvapauden kanssa

*Axel Springer AG v. Saksa* [suuri jaosto], nro 39954/08, 7.2.2012

*Von Hannover v. Saksa*, nro 59320/00, 24.6.2004

*Von Hannover v. Saksa (nro 2)* [suuri jaosto], nro 40660/08 ja 60641/08, 7.2.2012

### Tietosuojaan haasteet sähköisessä ympäristössä

*K.U. v. Suomi*, nro 2872/02, 2.12.2008

### Kirjeenvaihto

*Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 16.2.2000

*Bernh Larsen Holding AS ym. v. Norja*, nro 24117/08, 14.3.2013

*Cemalettin Canli v. Turkki*, nro 22427/04, 18.11.2008

*Dalea v. Ranska*, nro 964/07, 2.2.2010  
*Gaskin v. Yhdistynyt kuningaskunta*, nro 10454/83, 7.7.1989  
*Haralambie v. Romania*, nro 21737/03, 27.10.2009  
*Khelili v. Sveitsi*, nro 16188/07, 18.10.2011  
*Leander v. Ruotsi*, nro 9248/81, 26.3.1987  
*Malone v. Yhdistynyt kuningaskunta*, nro 8691/79, 26.4.1985  
*McMichael v. Yhdistynyt kuningaskunta*, nro 16424/90, 24.2.1995  
*M.G. v. Yhdistynyt kuningaskunta*, nro 39393/98, 24.9.2002  
*Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000  
*S. ja Marper v. Yhdistynyt kuningaskunta*, nro 30562/04 ja 30566/04, 4.12.2008  
*Shimovolos v. Venäjä*, nro 30194/09, 21.6.2011  
*Turek v. Slovakia*, nro 57986/00, 14.2.2006

### **Rikosrekisteritietokannat**

*B.B. v. Ranska*, nro 5335/06, 17.12.2009  
*M.M. v. Yhdistynyt kuningaskunta*, nro 24029/07, 13.11.2012

### **DNA-tietokannat**

*S. ja Marper v. Yhdistynyt kuningaskunta*, nro 30562/04 ja 30566/04, 4.12.2008.

### **GPS-tiedot**

*Uzun v. Saksa*, nro 35623/05, 2.9.2010

### **Terveystiedot**

*Biriuk v. Liettua*, nro 23373/03, 25.11.2008  
*I. v. Suomi*, nro 20511/03, 17.7.2008  
*L.L. v. Ranska*, nro 7508/02, 10.10.2006  
*M.S. v. Ruotsi*, nro 34209/96, 2.7.2002  
*Szuluk v. Yhdistynyt kuningaskunta*, nro 36936/05, 2.6.2009  
*Z. v. Suomi*, nro 22009/93, 25.2.1997

### **Henkilöllisyys**

*Ciubotaru v. Moldova*, nro 27138/04, 27.4.2010  
*Godelli v. Italia*, nro 33783/09, 25.9.2012  
*Odièvre v. Ranska* [suuri jaosto], nro 42326/98, 13.2.2003

**Ammattitoimintaa koskevat tiedot**

*Michaud v. Ranska*, nro 12323/11, 6.12.2012

*Niemietz v. Saksa*, nro 13710/88, 16.12.1992

**Viestinnän sieppaus**

*Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 16.2.2000

*Copland v. Yhdistynyt kuningaskunta*, nro 62617/00, 3.4.2007

*Cotlet v. Romania*, nro 38565/97, 3.6.2003

*Kruslin v. Ranska*, nro 11801/85, 24.4.1990

*Lambert v. Ranska*, nro 23618/94, 24.8.1998

*Liberty ym. v. Yhdistynyt kuningaskunta*, nro 58243/00, 1.7.2008

*Malone v. Yhdistynyt kuningaskunta*, nro 8691/79, 26.4.1985

*Halford v. Yhdistynyt kuningaskunta*, nro 20605/92, 25.6.1997

*Zsuluk v. Yhdistynyt kuningaskunta*, nro 36936/05, 2.6.2009

**Vastuullisten henkilöiden velvollisuudet**

*B.B. v. Ranska*, nro 5335/06, 17.12.2009

*I. v. Suomi*, nro 20511/03, 17.7.2008

*Mosley v. Yhdistynyt kuningaskunta*, nro 48009/08, 10.5.2011

**Valokuvat**

*Sciacca v. Italia*, nro 50774/99, 11.1.2005

*Von Hannover v. Saksa*, nro 59320/00, 24.6.2004

**Oikeus tulla unohdetuksi**

*Segerstedt-Wiberg ym. v. Ruotsi*, nro 62332/00, 6.6.2006

**Oikeus vastustaa tietojen käsittelyä**

*Leander v. Ruotsi*, nro 9248/81, 26.3.1987

*Mosley v. Yhdistynyt kuningaskunta*, nro 48009/08, 10.5.2011

*M.S. v. Ruotsi*, nro 34209/96, 2.7.2002

*Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000

**Arkaluonteiset tietoluokat**

*I. v. Suomi*, nro 20511/03, 17.7.2008

*Michaud v. Ranska*, nro 12323/11, 6.12.2012

*S. ja Marper v. Yhdistynyt kuningaskunta*, nro 30562/04 ja 30566/04, 4.12.2008

### **Valvonta ja täytäntöönpano (eri toimijoiden roolit, mukaan lukien tietosuojaviranomaiset)**

*I. v. Suomi*, nro 20511/03, 17.7.2008

*K.U. v. Suomi*, nro 2872/02, 2.12.2008

*Von Hannover v. Saksa*, nro 59320/00, 24.6.2004

*Von Hannover v. Saksa (nro 2)* [suuri jaosto], nro 40660/08 ja 60641/08, 7.2.2012

### **Tarkkailumenetelmät**

*Allan v. Yhdistynyt kuningaskunta*, nro 48539/99, 5.11.2002

*Association "21 Décembre 1989" ym. v. Romania*, nro 33810/07 ja 18817/08, 24.5.2011

*Bykov v. Venäjä* [suuri jaosto], nro 4378/02, 10.3.2009

*Kennedy v. Yhdistynyt kuningaskunta*, nro 26839/05, 18 May 2010

*Klass ym. v. Saksa*, nro 5029/71, 6.9.1978

*Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000

*Taylor-Sabori v. Yhdistynyt kuningaskunta*, nro 47114/99, 22.10.2002

*Uzun v. Saksa*, nro 35623/05, 2.9.2010

*Vetter v. Ranska*, nro 59842/00, 31.5.2005

### **Videovalvonta**

*Köpke v. Saksa*, nro 420/07, 5.10.2010

*Peck v. Yhdistynyt kuningaskunta*, nro 44647/98, 28.1.2003

### **Ääninäytteet**

*P.G. ja J.H. v. Yhdistynyt kuningaskunta*, nro 44787/98, 25.9.2001

*Wisse v. Ranska*, nro 71611/01, 20.12.2005

# Euroopan unionin oikeuskäytäntöä

## Tietosuojadirektiiviin liittyvä oikeuskäytäntö

Asia C-73/07, *Tietosuojavalvutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy*, 16.12.2008

[Tietosuojadirektiivin 9 artiklassa tarkoitetun journalistisen toiminnan käsite]

Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen*, 9.11.2010

[Tiettyjen EU:n maatalousrahastojen tuensaajia koskevien henkilötietojen julkaisemista koskevan laillisen velvoitteen oikeasuhteisuus]

Asia C-101/01, *Bodil Lindqvist*, 6.11.2003

[Yksityishenkilön oikeus julkaista muiden henkilöiden yksityiselämää koskevia tietoja internetissä]

C-131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Audiencia Nacionalin (Espanja) 9.3.2012 esittämä ennakkoratkaisupyynnö, 25.5.2012, asian käsittely on kesken

[Hakuohjelmien tarjoajien velvollisuus pitäytyä rekisteröidyn pyynnöstä näyttämästä henkilötietoja hakutuloksissa]

Asia C-270/11, *Euroopan komissio v. Ruotsin kuningaskunta*, 30.5.2013

[Sakko direktiivin täytäntöönpanon laiminlyönnistä]

Asia, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29.1.2008

[Internetyhteyspalvelujen tarjoajien velvollisuus paljastaa KaZaA-ohjelman käyttäjien henkilöllisyys teollis- ja tekijänoikeuksia suojelevalle yhdistykselle]

Asia C-288/12, *Euroopan komissio v. Unkari*, 8.4.2014

[Kansallisen tietosuojavalvutetun virasta poistamisen laillisuus]

C-291/12, *Michael Schwarz v. Stadt Bochum*, julkisasiamiehen ratkaisuehdotus, 13.6.2013

[EU:n primaarioikeuden rikkominen asetuksella (EY) 2252/2004, jossa säädetään, että passeihin on tallennettava sormenjälkitiedot]

Yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland ja Seitlinger ja Muut*, 8.4.2014

[EU:n primaarioikeuden rikkominen tietojen säilyttämistä koskevalla direktiivillä]

C-360/10, *SABAM v. Netlog N.V.*, 16.2.2012

[Sosiaalisten verkkopalvelujen tarjoajien velvollisuus estää verkon käyttäjiä käyttämästä laittomasti musiikkiteoksia ja audiovisuaalisia teoksia]

Yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, *Rechnungshof v. Österreichischer Rundfunk ym. sekä Neukomm ja Lauer mann v. Österreichischer Rundfunk*, 20.5.2003

[Tiettyjen julkiseen sektoriin liittyvien virastojen työntekijöiden palkkatietojen julkaisemista koskevan laillisen velvoitteen oikeasuhteisuus]

Yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24.11.2011

[Tietosuojadirektiivin 7 artiklan f kohdan – ”sivullisen oikeutettu intressi” – asianmukainen täytäntöönpano kansallisessa lainsäädännössä]

Asia C-518/07, *Euroopan komissio v. Saksan liittotasavalta*, 9.3.2010

[Kansallisen valvontaviranomaisen riippumattomuus]

Asia C-524/01, *Huber v. Saksa*, 16.12.2008

[Ulkomaalaisia koskevien tietojen tilastollisessa rekisterissä säilyttämisen laillisuus]

Asia C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5.5.2011

[Suostumuksen uusimisen tarpeellisuus]

Asia C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, 7.5.2009

[Rekisteröidyn tiedonsaantioikeus]

Asia C-614/10, *Euroopan komissio v. Itävallan tasavalta*, 16.10.2012

[Kansallisen valvontaviranomaisen riippumattomuus]

**EU:n toimielinten tietosuojasetukseen liittyvä oikeuskäytäntö**

Asia C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd*, 29.6.2010

[Asiakirjojen saatavuus]

Asia C-41/00 P, *Interporc Im- und Export GmbH v. Euroopan yhteisöjen komissio*,  
6.3.2003

[Asiakirjojen saatavuus]

Asia F-35/08, *Pachtitis v. komissio ja EPSO*, 15.6.2010

[Henkilötietojen käyttö EU:n toimielinten palvelukseenoton yhteydessä]

F-46/09, *V. v. parlamentti*, 5.7.2011

[Henkilötietojen käyttö EU:n toimielinten palvelukseenoton yhteydessä]





# Luettelo oikeustapauksista

## **Euroopan yhteisöjen tuomioistuimen oikeuskäytäntö**

<i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado</i> , Yhdistetyt asiat C-468/10 ja C-469/10, 24.11.2011 .....	18, 22, 79, 82, 86, 196
<i>Bodil Lindqvist</i> , Asia C-101/01, 6.11.2003.....	33, 34, 42, 45, 48, 95, 131, 132, 195
<i>College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer</i> , Asia C-553/07, 7.5.2009 .....	105, 110, 196
<i>Deutsche Telekom AG v. Bundesrepublik Deutschland</i> , Asia C-543/09, 5.5.2011 .....	34, 58, 196
<i>Digital Rights Ireland ja Seitlinger ja Muut</i> , Yhdistetyt asiat C-293/12 ja C-594/12, 8.4.2014.....	126, 173, 196
<i>Euroopan komissio v. Itävallan tasavalta</i> , Asia C-614/10, 16.10.2012.....	106, 119, 196
<i>Euroopan komissio v. Ruotsin kuningaskunta</i> , Asia C-270/11, 30.5.2013.....	195
<i>Euroopan komissio v. Saksan liittotasavalta</i> , Asia C-518/07, 9.3.2010 .....	106, 118, 196
<i>Euroopan komissio v. The Bavarian Lager Co. Ltd</i> , Asia C-28/08 P, 29.6.2010 .....	13, 26, 29, 106, 127, 197
<i>Euroopan komissio v. Unkari</i> , Asia C-288/12, 8.4.2014.....	106, 119, 195

<i>Euroopan parlamentti v. Euroopan unionin neuvosto ja Euroopan yhteisöjen komissio</i> , Yhdistetyt asiat C-317/04 ja C-318/04, 30.5.2006.....	142
<i>Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González</i> , Audiencia Nacionalin (Espanja) 9.3.2012 esittämä ennakkoratkaisupyyntö, C-131/12, 25.5.2012, asian käsittely on kesken.....	195
<i>Huber v. Saksa</i> , Asia C-524/01, 16.12.2008 .....	61, 79, 82, 84, 169, 181, 196
<i>Interporc Im- und Export GmbH v. Euroopan yhteisöjen komissio</i> , Asia C-41/00 P, 6.3.2003 .....	29, 197
<i>M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority</i> , Asia C-152/84, 26.2.1986.....	106
<i>Michael Schwarz v. Stadt Bochum</i> , julkisasiamiehen ratkaisuehdotus, C-291/12, 3.6.2013 .....	195
<i>Pachitis v. komissio ja EPSO</i> , Asia F-35/08, 15.6.2010 .....	197
<i>Productores de Música de España (Promusicae) v. Telefónica de España SAU</i> , Asia, C-275/06, 29.1.2008.....	13, 22, 31, 33, 38, 195
<i>Rechnungshof v. Österreichischer Rundfunk ym. sekä Neukomm ja Lauer mann v. Österreichischer Rundfunk</i> , Yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, 20.5.2003 .....	82, 196
<i>SABAM v. Netlog N.V.</i> , C-360/10, 16.2.2012.....	32, 196
<i>Sabine von Colson ja Elisabeth Kamann v. Land Nordrhein-Westfalen</i> , Asia C-14/83, 10.4.1984.....	106, 129
<i>Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy</i> , Asia C-73/07, 16.12.2008 .....	13, 23, 195
<i>V. v. parlamentti</i> , F-46/09, 5.7.2011 .....	197
<i>Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen</i> , Yhdistetyt asiat C-92/09 ja C-93/09, 9.11.2010 .....	13, 21, 29, 33, 37, 40, 61, 66, 195

**Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö**

<i>Allan v. Yhdistynyt kuningaskunta</i> , nro 48539/99, 5.11.2002 .....	149, 194
<i>Amann v. Sveitsi</i> [suuri jaosto], nro 27798/95, 16.2.2000 .....	35, 37, 40, 63, 191, 193
<i>Ashby Donald ym. v. Ranska</i> , nro 36769/08, 10.1.2013 .....	31
<i>Association "21 Décembre 1989" ym. v. Romania</i> , nro 33810/07 ja 18817/08, 24.5.2011 .....	194
<i>Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria</i> , nro 62540/00, 28.6.2007 .....	64
<i>Avilkina ym. v. Venäjä</i> , nro 1585/09, 6.6.2013 .....	178
<i>Axel Springer AG v. Saksa</i> [suuri jaosto], nro 39954/08, 7.2.2012 .....	13, 24, 191
<i>B.B. v. Ranska</i> , nro 5335/06, 17.12.2009 .....	147, 149, 192, 193
<i>Bernh Larsen Holding AS ym. v. Norja</i> , nro 24117/08, 14.3.2013 .....	33, 36, 191
<i>Biriuk v. Liettua</i> , nro 23373/03, 25.11.2008 .....	25, 106, 178, 192
<i>Bykov v. Venäjä</i> [suuri jaosto], nro 4378/02, 10.3.2009 .....	194
<i>Cemalettin Canli v. Turkki</i> , nro 22427/04, 18.11.2008 .....	105, 111, 191
<i>Ciubotaru v. Moldova</i> , nro 27138/04, 27.4.2010 .....	105, 112, 192
<i>Copland v. Yhdistynyt kuningaskunta</i> , nro 62617/00, 3.4.2007 .....	15, 169, 175, 193
<i>Cotlet v. Romania</i> , nro 38565/97, 3.6.2003 .....	193
<i>Dalea v. Ranska</i> , nro 964/07, 2.2.2010 .....	111, 147, 163, 192
<i>Gaskin v. Yhdistynyt kuningaskunta</i> , nro 10454/83, 7.7.1989 .....	109, 191, 192
<i>Godelli v. Italia</i> , nro 33783/09, 25.9.2012 .....	37, 109, 191, 192
<i>Halford v. Yhdistynyt kuningaskunta</i> , nro 20605/92, 25.6.1997 .....	182, 193
<i>Haralambie v. Romania</i> , nro 21737/03, 27.10.2009 .....	62, 74, 192
<i>I. v. Suomi</i> , nro 20511/03, 17.7.2008 .....	15, 80, 93, 128, 177, 192, 193, 194
<i>lordachi ym. v. Moldova</i> , nro 25198/02, 10.2.2009 .....	63
<i>K.H. ym. v. Slovakia</i> , nro 32881/04, 28.4.2009 .....	62, 75, 109, 177, 191
<i>K.U. v. Suomi</i> , nro 2872/02, 2.12.2008 .....	15, 106, 124, 128, 191, 194
<i>Kennedy v. Yhdistynyt kuningaskunta</i> , nro 26839/05, 18 May 2010 .....	194

<i>Khelili v. Sveitsi</i> , nro 16188/07, 18.10.2011 .....	61, 65, 192
<i>Klass ym. v. Saksa</i> , nro 5029/71, 6.9.1978 .....	15, 150, 194
<i>Köpke v. Saksa</i> , nro 420/07, 5.10.2010.....	41, 124, 194
<i>Kopp v. Sveitsi</i> , nro 23224/94, 25.3.1998.....	63
<i>Kruslin v. Ranska</i> , nro 11801/85, 24.4.1990.....	193
<i>L.L. v. Ranska</i> , nro 7508/02, 10.10.2006.....	177, 192
<i>Lambert v. Ranska</i> , nro 23618/94, 24.8.1998.....	193
<i>Leander v. Ruotsi</i> , nro 9248/81, 26.3.1987.....	15, 61, 65, 109, 115, 148, 191, 192, 193
<i>Liberty ym. v. Yhdistynyt kuningaskunta</i> , nro 58243/00, 1.7.2008.....	36, 193
<i>M.G. v. Yhdistynyt kuningaskunta</i> , nro 39393/98, 24.9.2002 .....	192
<i>M.K. v. Ranska</i> , nro 19522/09, 18.4.2013 .....	112, 148
<i>M.M. v. Yhdistynyt kuningaskunta</i> , nro 24029/07, 13.11.2012.....	73, 148, 192
<i>M.S. v. Ruotsi</i> , nro 34209/96, 2.7.2002.....	115, 177, 192, 193
<i>Malone v. Yhdistynyt kuningaskunta</i> , nro 8691/79, 26.4.1985.....	15, 63, 174, 192, 193
<i>McMichael v. Yhdistynyt kuningaskunta</i> , nro 16424/90, 24.2.1995.....	192
<i>Michaud v. Ranska</i> , nro 12323/11, 6.12.2012.....	170, 182, 193, 194
<i>Mosley v. Yhdistynyt kuningaskunta</i> , nro 48009/08, 10.5.2011 .....	13, 25, 115, 193
<i>Müller ym. v. Sveitsi</i> , nro 10737/84, 24.5.1988.....	30
<i>Niemietz v. Saksa</i> , nro 13710/88, 16.12.1992.....	35, 182, 193
<i>Odièvre v. Ranska</i> [suuri jaosto], nro 42326/98, 13.2.2003.....	37, 109, 191, 192
<i>P.G. ja J.H. v. Yhdistynyt kuningaskunta</i> , nro 44787/98, 25.9.2001.....	41, 194
<i>Peck v. Yhdistynyt kuningaskunta</i> , nro 44647/98, 28.1.2003.....	41, 61, 64, 194
<i>Rotaru v. Romania</i> [suuri jaosto], nro 28341/95, 4.5.2000.....	35, 61, 64, 112, 192, 193, 194
<i>S. ja Marper v. Yhdistynyt kuningaskunta</i> , nro 30562/04 ja 30566/04, 4.12.2008.....	15, 73, 147, 149, 192, 194
<i>Sciacca v. Italia</i> , nro 50774/99, 11.1.2005.....	41, 193
<i>Segerstedt-Wiberg ym. v. Ruotsi</i> , nro 62332/00, 6.6.2006.....	105, 112, 193

<i>Shimovolos v. Venäjä</i> , nro 30194/09, 21.6.2011 .....	64, 192
<i>Silver ym. v. Yhdistynyt kuningaskunta</i> , nro 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25.3.1983.....	63
<i>Szuluk v. Yhdistynyt kuningaskunta</i> , nro 36936/05, 2.6.2009.....	177, 192, 193
<i>Társaság a Szabadságjogokért v. Unkari</i> , nro 37374/05, 14.4.2009 .....	13, 28
<i>Taylor-Sabori v. Yhdistynyt kuningaskunta</i> , nro 47114/99, 22.10.2002 .....	61, 64, 194
<i>The Sunday Times v. Yhdistynyt kuningaskunta</i> , nro 6538/74, 26.4.1979 .....	63
<i>Turek v. Slovakia</i> , nro 57986/00, 14.2.2006.....	192
<i>Uzun v. Saksa</i> , nro 35623/05, 2.9.2010.....	15, 41, 192, 194
<i>Vereinigung bildender Künstler v. Itävalta</i> , nro 68345/01, 25.1.2007 .....	13, 30
<i>Vetter v. Ranska</i> , nro 59842/00, 31.5.2005.....	64, 147, 150, 194
<i>Von Hannover v. Saksa (nro 2)</i> [suuri jaosto], nro 40660/08 ja 60641/08, 7.2.2012.....	22, 24, 191, 194
<i>Von Hannover v. Saksa</i> , nro 59320/00, 24.6.2004 .....	41, 191, 193, 194
<i>Wisse v. Ranska</i> , nro 71611/01, 20.12.2005 .....	41, 194
<i>Z. v. Suomi</i> , nro 22009/93, 25.2.1997.....	169, 177, 192

### Kansallisten tuomioistuinten oikeuskäytäntö

Saksan liittovaltion perustuslakituomioistuin ( <i>Bundesverfassungsgericht</i> ), 1 BvR 256/08, 2.3.2010 .....	173
Romanian liittovaltion perustuslakituomioistuin ( <i>Curtea Constituțională a României</i> ), No. 1258, 8.11.2009.....	173
Tšekin perustuslakituomioistuin ( <i>Ústavní soud České republiky</i> ), 94/2011 Coll., 22.3.2011.....	173



Euroopan unionin perusoikeusvirasto  
Euroopan neuvosto - Euroopan ihmisoikeustuomioistuin

## Käsikirja Euroopan tietosuojaoikeudesta

2014 – 204 p. – 14,8 × 21 cm

ISBN 978-92-871-9946-1 (Euroopan neuvosto)

ISBN 978-92-9239-496-7 (FRA)

doi:10.2811/73623

Paljon Euroopan unionin perusoikeusvirastoa koskevaa tietoa on saatavilla Internetissä, perusoikeusviraston (FRA) verkkosivuilla ([fra.europa.eu](http://fra.europa.eu)).

Lisätietoja Euroopan neuvostosta on saatavilla osoitteessa [hub.coe.int](http://hub.coe.int).

Lisätietoa Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä on saatavilla tuomioistuimen verkkosivuilla [www.echr.coe.int](http://www.echr.coe.int). HUDOC-hakusivustolta on pääsy englannin- ja ranskankielisiin tuomioihin ja päätöksiin, muunkielisiin käännöksiin, kuukausittain ilmestyviin oikeuskäytännön tietoisuuksiin, lehdistötiedotteisiin sekä muuhun tuomioistuimen toimintaa koskevaan tietoon.

### MISTÄ EU:N JULKAISUJA SAA?

#### Maksuttomat julkaisut:

- yksi kappale:  
EU Bookshopista (<http://bookshop.europa.eu>);
- enemmän kuin yksi kappale tai julisteet/kartat:  
Euroopan unionin edustustoista ([http://ec.europa.eu/represent\\_fi.htm](http://ec.europa.eu/represent_fi.htm)),  
muissa kuin EU-maissa sijaitsevista lähetystöistä ([http://eeas.europa.eu/delegations/index\\_fi.htm](http://eeas.europa.eu/delegations/index_fi.htm)),  
ottamalla yhteyttä Europe Direct -palveluun ([http://europa.eu/europedirect/index\\_fi.htm](http://europa.eu/europedirect/index_fi.htm))  
tai soittamalla 00 800 6 7 8 9 10 11 (maksuton numero koko EU:n alueella) (\*).

#### Maksulliset julkaisut:

- EU Bookshopista (<http://bookshop.europa.eu>);

#### Maksulliset tilaukset:

- Euroopan unionin julkaisu toimiston myyntiedustajalta ([http://publications.europa.eu/others/agents/index\\_fi.htm](http://publications.europa.eu/others/agents/index_fi.htm)).

(\* ) Saat pyytämäsi tiedot maksutta. Myös useimmat puhelut ovat maksuttomia, joskin jotkin operaattorit, puhelinkioskit tai hotellit voivat periä puhelusta maksun.

### Miten hankkia Euroopan neuvoston julkaisuja?

Euroopan neuvoston kustantamo julkaisee teoksia kaikilta organisaation eri osa-alueilta, kuten ihmisoikeuksista, oikeustieteestä, terveydestä, etiikasta, sosiaalialioista, ympäristöstä, koulutuksesta, kulttuurista, urheilusta, nuorisosta ja kulttuuriperinnöstä. Kirjoja ja elektronisia julkaisuja voi tilata laajasta luettelosta osoitteesta (<http://book.coe.int/>).

Virtuaalilukuhuoneessa käyttäjät voivat maksutta tutustua hiljattain ilmestyneiden tärkeimpien teosten lyhennelmiin tai tiettyihin virallisiin asiakirjoihin kokonaisuudessaan.

Tietoa Euroopan neuvoston yleissopimuksista sekä niiden tekstit kokonaisuudessaan ovat saatavilla sopimustoimiston verkkosivuilla <http://conventions.coe.int/>.

Tieto- ja viestintäteknikoiden nopea kehitys on kasvattanut vankan tietosuojan tarvetta. Euroopan unioni (EU) ja Euroopan neuvosto (EN) ovat hyväksyneet välineitä tämän oikeuden turvaksi. Tekniikan kehittymisen myötä esimerkiksi tarkkailun, viestinnän sieppauksen ja tietojen säilyttämisen rajat ovat väljentyneet asettaen merkittäviä haasteita tietosuojaoikeudelle. Tämän käsikirjan tarkoituksena on tarjota tietosuojaoikeuteen liittyvää tietoa oikeusalan ammattilaisille, jotka eivät ole erikoistuneet tähän oikeuden alaan. Siinä luodaan yleiskatsaus EU:n ja EN:n voimassa oleviin oikeuskehyksiin ja oikeuskäytäntöön, jonka osalta esitellään lyhyesti sekä Euroopan ihmisoikeustuomioistuimen (EIT) että Euroopan unionin tuomioistuimen (EUTI) tärkeimpiä tuomioita. Tilanteista, joista ei ole vielä olemassa oikeuskäytäntöä, käsikirjassa esitetään käytännön esimerkkejä ja kuviteltuja skenaarioita. Lyhyesti sanoen tällä käsikirjalla pyritään varmistamaan, että oikeutta tietosuojaan vaalitaan tarmokkaasti ja määrätietoisesti.

---

#### **EUROOPAN UNIONIN PERUSOIKEUSVIRASTO**

Schwarzenbergplatz 11 – 1040 Wien – Itävalta  
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693  
[fra.europa.eu](http://fra.europa.eu) – [info@fra.europa.eu](mailto:info@fra.europa.eu)

#### **EUROOPAN NEUVOSTO EUROOPAN IHMISOIKEUSTUOMIOISTUIN**

67075 Strasbourg Cedex – Ranska  
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30  
[echr.coe.int](http://echr.coe.int) – [publishing@echr.coe.int](mailto:publishing@echr.coe.int)



Julkaisutoimisto

ISBN 978-92-871-9946-1 (Euroopan neuvosto)  
ISBN 978-92-9239-496-7 (FRA)