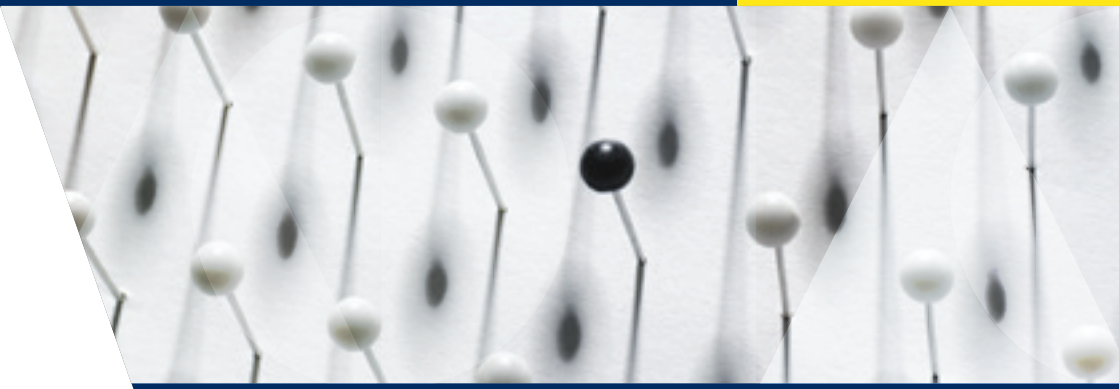
KÄSIRAAMAT



Euroopa andmekaitseõiguse käsiraamat

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Käsikiri valmis 2014. aasta aprillis.
Uuendusi hakatakse avaldama Euroopa Liidu Põhiõiguste Ameti (FRA) veebilehel (fra.europa.eu), Euroopa Nõukogu veebilehel (coe.int/dataprotection), ja Euroopa Inimõiguste Kohtu veebilehel (echr.coe.int) jaotises „Case-Law" („Kohtupraktika").

Europe Direct on teenistus, mis aitab leida vastused Euroopa Liitu käsitlevatele küsimustele

Tasuta infotelefon: (*)

00 800 6 7 8 9 10 11

(*) Antav teave on tasuta nagu ka enamik kõnesid (v.a mõne operaatori, hotelli ja telefonikabiini puhul).

Fotod: © iStockphoto

Lisateavet Euroopa Liidu kohta saab internetist Euroopa serverist (http://europa.eu).

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2015

ISBN 978-92-871-9947-8 (CoE)
ISBN 978-92-9239-331-1 (FRA)
doi:10.2811/53785

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Euroopa andmekaitseõiguse käsiraamat

Eessõna

Käesoleva Euroopa andmekaitseõiguse käsiraamatu on koostanud Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu koostöös Euroopa Inimõiguste Kohtu kantseleiga. See on Euroopa Liidu Põhiõiguste Ameti ja Euroopa Nõukogu ühistöös sündinud õiguskäsiraamatute sarja kolmas üllitis. 2011. aasta märtsis avaldati Euroopa võrdse kohtlemise õiguse käsiraamat ning 2013. aasta juunis Euroopa varjupaiga-, piirikontrolli- ja sisserändeõiguse käsiraamat.

Oleme otsustanud jätkata oma koostööd ühes ülimalt päevakajalises küsimuses, mis mõjutab igapäevaselt meid kõiki, nimelt võtsime tähelepanu alla isikuandmete kaitse. Euroopa isikuandmete kaitse süsteem on üks maailma tugevamaid, põhinedes Euroopa Nõukogu konventsioonil nr 108, Euroopa Liidu õigusaktidel ning samuti Euroopa Inimõiguste Kohtu (EIK) ja Euroopa Liidu Kohtu (ELK) praktikal.

Käesoleva käsiraamatu eesmärk on suurendada teadlikkust ja täiendada teadmisi andmekaitse-eeskirjadest Euroopa Liidu ja Euroopa Nõukogu liikmesriikides, pakkudes lugejatele selles valdkonnas peamist pidepunkti. Käsiraamat on välja töötatud õigusvaldkonna üldspetsialistidele, kohtunikele, riikide andmekaitseametnikele ning teistele andmekaitse valdkonnas töötavatele isikutele.

Lissaboni lepingu jõustumisega 2009. aasta detsembris muutus Euroopa Liidu põhiõiguste harta õiguslikult siduvaks ning sellega sai õigus isikuandmete kaitsele eraldi põhiõiguseks. Selle põhiõiguse kaitsmiseks on oluline aidata kõikidel paremini mõista Euroopa Nõukogu konventsiooni nr 108 ja asjaomaseid Euroopa Liidu õigusakte, mis ladusid Euroopas andmekaitsele vajaliku vundamendi, samuti Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktikat.

Soovime tänada Ludwig Boltzmanni nimelist inimõiguste instituuti panuse eest selle käsiraamatu valmimisse. Samuti tahame tänada Euroopa andmekaitseinspektori bürood panuse eest käsiraamatu kavandi koostamisse. Erilised tänuavaldused soovime edastada Euroopa Komisjoni andmekaitseüksusele käesoleva käsiraamatu koostamisel osutatud abi eest. Lõpetuseks, soovime tänada Eesti Andmekaitse Inspektsiooni käsiraaamatu tõlke toimetamise eest.

Philippe Boillat

Euroopa Nõukogu inimõiguste ja õigusküsimuste direktor

Morten Kjaerum

Euroopa Liidu Põhiõiguste Ameti direktor

Sisukord

Lühendid ja akronüümid

CETS	Euroopa Nõukogu lepingute seeria
EIK	Euroopa Inimõiguste Kohus
EL	Euroopa Liit
ELK	Euroopa Liidu Kohus (enne detsembrit 2009 Euroopa Ühenduste Kohus)
EMP	Euroopa Majanduspiirkond
ENISA	Euroopa Liidu Võrgu- ja Infoturbeamet
ESMA	Euroopa Väärtpaberiturujärelevalve
eTEN	Üleeuroopalised telekommunikatsioonivõrgud
eu-LISA	Vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimise Euroopa amet
EuroPriSe	Euroopa eraelu puutumatuse märgiste süsteem
FRA	Euroopa Liidu Põhiõiguste Amet
GPS	Globaalne asukoha määramise süsteem
Harta	Euroopa Liidu põhiõiguste harta
Konventsioon nr 108	Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (Euroopa Nõukogu)
OECD	Majanduskoostöö ja Arengu Organisatsioon
SEPA	Ühtne euromaksete piirkond
SIS	Schengeni infosüsteem
SWIFT	Ülemaailmne Pankadevahelise Finantstelekommunikatsiooni Ühing
TIS	Tolliinfosüsteem
ÜRO	Ühinenud Rahvaste Organisatsioon
VIS	Viisainfosüsteem

Käsiraamatu kasutamine

Käesolevas käsiraamatus esitatakse ülevaade Euroopa Liidu ja Euroopa Nõukogu tasandil andmekaitse valdkonnas kohaldatavatest õigusaktidest.

Käsiraamat on abiks õiguspraktikutele, kes ei ole spetsialiseerunud andmekaitse valdkonnale; see on ette nähtud juristidele, kohtunikele ja teistele spetsialistidele, samuti kõikidele muudes asutustes, sh vabaühendustes töötavatele isikutele, kellel tuleb tegeleda andmekaitsega seotud õigusküsimustega.

See on esmane teabeallikas andmekaitse kohta nii ELi õiguses kui ka Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis; käsiraamatus selgitatakse kõnealuse valdkonna reguleerimist ELi õiguses ja asjaomases konventsioonis, samuti Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (konventsioon nr 108) ja muude Euroopa Nõukogu dokumentide alusel. Iga peatüki alguses esitatakse üldtabel kohaldatavate õigussätetega, sealhulgas valitud tähtsamate näidetega Euroopa kahe eraldiseisva õigussüsteemi kohtupraktikast. Seejärel esitatakse Euroopa kahe õiguskorra asjakohased õigusaktid üksteise järel vastavalt igale käsitletavale teemale. Nii näeb lugeja, mis nüanssides süsteemid kokku langevad ja millistes lahknevad.

Peatükkide alguses esitatud tabelites loetletakse peatükis käsitletavad teemad, kohaldatavad õigussätted ja muud teemakohased allikad, näiteks kohtupraktika. Teemade järjestus võib peatüki teksti ülesehitusest erineda, kui see on asjaomase peatüki sisu täpse ja kokkuvõtliku esitamise seisukohalt vajalik. Tabelites käsitletakse nii Euroopa Nõukogu kui ka ELi õigust. See peaks võimaldama kasutajatel üles leida nende olukorraga seotud põhiteabe, eelkõige üksnes Euroopa Nõukogu õigusega seotud juhtudel.

Spetsialistid nendest ELi mittekuuluvatest riikidest, mis on Euroopa Nõukogu liikmesriigid ning ühinenud Euroopa põhiõiguste ja vabaduste kaitse konventsiooniga ning konventsiooniga nr 108, saavad oma riigi puhul asjakohast teavet vaadata otse Euroopa Nõukogu õiguse jaotistest. ELi liikmesriikides tegutsevad spetsialistid peavad kasutama mõlemat jaotist, sest nende riikide suhtes on siduvad mõlemad õiguskorrad. Nendele, kes sooviksid mõne küsimuse kohta rohkem teavet, on käsiraamatu jaotises „Lisalugemist" esitatud viited täiendavale materjalile.

Euroopa Nõukogu õigust tutvustatakse lühiviidetega teatavatele Euroopa Inimõiguste Kohtu (EIK) juhtumitele. Need on valitud suure hulga EIK otsuste seast, mis on seotud andmekaitseküsimustega.

ELi õigust tutvustatakse vastu võetud seadusandlike meetmete, lepingute asjakohaste sätete ja Euroopa Liidu põhiõiguste harta kaudu, lähtudes Euroopa Liidu Kohtu (ELK; enne 2009. aastat Euroopa Ühenduste Kohtu) praktikas kasutatud tõlgendustest.

Käesolevas käsiraamatus kirjeldatud või viidatud kohtupraktikaga esitatakse näiteid nii EIK kui ka ELK kohtupraktika laialdasest kogumist. Käsiraamatu lõpus esitatud suunised on abiks kohtupraktika otsimisel internetis.

Selleks et näitlikustada Euroopa andmekaitse-eeskirjade kohaldamist praktikas, eeskätt juhtudel, kui asjaomases küsimuses ei ole EIKs või ELKs konkreetset kohtupraktikat välja kujunenud, on tekstiboksides esitatud hüpoteetilised stsenaariumid elulistest olukordadest.

Käsiraamatu juhatab sisse lühiülevaade kahe õigussüsteemi rollist Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni ja ELi õigusaktide alusel (1. peatükk). 2.–8. peatükis käsitletakse järgmisi küsimusi:

- andmekaitseterminid;
- Euroopa andmekaitseõiguse peamised põhimõtted;
- Euroopa andmekaitseõiguse eeskirjad;
- andmesubjektide õigused ja nende õiguste jõustamine;
- andmete piiriülene liikumine;
- andmekaitse politsei ja kriminaalõiguse kontekstis;
- muud konkreetsed Euroopa andmekaitsealased õigusaktid.

1

Euroopa andmekaitseõiguse kontekst ja taust

EL	Käsitletavad teemad	Euroopa Nõukogu
Õigus andmekaitsele		
Direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (andmekaitsedirektiiv), EÜT L 281, 1995		Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 (õigus austusele era- ja perekonnaelu, kodu ja korrespondentsi vastu) Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (konventsioon nr 108)
Õiguste tasakaalustamine		
ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, 2010	Üldine	
ELK, C-73/07, *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy*, 2008	Sõnavabadus	EIK, *Axel Springer AG vs. Saksamaa*, 2012 EIK, *Mosley vs. Ühendkuningriik*, 2011
	Kunsti ja teaduse vabadus	EIK, *Vereinigung bildender Künstler vs. Austria*, 2007
ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 2008	Omandi kaitse	
ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*, 2010	Juurdepääs dokumentidele	EIK, *Társaság a Szabadságjogokért vs. Ungari*, 2009

1.1. Õigus isikuandmete kaitsele

Põhipunktid

- Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaselt kuulub era- ja perekonnaelu, kodu ja korrespondentsi puutumatuse austamise õiguse alla õigus kaitsele isikuandmete kogumise ja kasutamise vastu.
- Euroopa Nõukogu konventsioon nr 108 on esimene rahvusvaheline õiguslikult siduv dokument, mis käsitleb otseselt andmekaitset.
- ELi õiguses hakati andmekaitse valdkonda esmakordselt reguleerima andmekaitsedirektiiviga.
- ELi õiguses on andmekaitse talletatud eraldi põhiõigusena.

Üksikisiku eraelu puutumatuse kaitse teiste, eeskätt riigi sekkumise eest sätestati rahvusvahelises õigusaktis esmakordselt Ühinenud Rahvaste Organisatsiooni (ÜRO) 1948. aasta inimõiguste ülddeklaratsiooni artiklis 12, milles käsitletakse era- ja perekonnaelu austamist[1]. Inimõiguste ülddeklaratsioon mõjutas teiste inimõigusi käsitlevate dokumentide väljatöötamist Euroopas.

1.1.1. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon

Euroopa Nõukogu moodustati pärast Teist maailmasõda, et ühendada Euroopa riikide jõud õigusriigi, demokraatia, inimõiguste ja sotsiaalarengu edendamiseks. Sel eesmärgil võttis Euroopa Nõukogu 1950. aastal vastu Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni, mis jõustus 1953. aastal.

Rahvusvahelise kohustuse alusel peavad asjaomased riigid konventsiooni järgima. Nüüdseks on kõik Euroopa Nõukogu liikmesriigid konventsiooni oma õigusesse inkorporeerinud või selle jõustanud ning on seega kohustatud talitama kooskõlas konventsiooni sätetega.

Selleks et konventsiooniosalised täidaksid inimõiguste ja põhivabaduste kaitse konventsioonist tulenevaid kohustusi, asutati 1959. aastal Prantsusmaal Strasbourgis Euroopa Inimõiguste Kohus (EIK). EIK ülesanne on tagada, et riigid täidaksid

1 Ühinenud Rahvaste Organisatsioon (ÜRO), Inimõiguste ülddeklaratsioon, 10. detsember 1948.

konventsioonist tulenevaid kohustusi, ning selleks käsitleb kohus kaebusi, mille on esitanud üksikisikud, üksikisikute rühmad, vabaühendused või konventsiooni väidetavatest rikkumistest teatavad juriidilised isikud. 2013. aastal oli Euroopa Nõukogul 47 liikmesriiki, sealhulgas ELi 28 liikmesriiki. EIKsse saavad kaebuse esitada ka inimesed, kes ei ole asjaomaste riikide kodanikud. Samuti saab EIK käsitleda ühe või mitme Euroopa Nõukogu liikmesriigi algatatud kohtuasju teise liikmesriigi vastu.

Õigus isikuandmete kaitsele kuulub Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õiguse alla; artikliga 8 tagatakse kõikidele õigus era- ja perekonnaelu, kodu ja korrespondentsi puutumatuse austamisele ning kehtestatakse tingimused, mille puhul on põhjendatud kõnealuse õiguse piiramine[2].

Oma praktika jooksul on EIK hulganisti käsitlenud juhtumeid, milles on esile kerkinud andmekaitseküsimus, eeskätt teabevahetuse pealtkuulamine,[3] eri tüüpi jälgimine[4] ning kaitse isikuandmete säilitamise eest riigiasutustes[5]. Kohus on täpsustanud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 mitte üksnes ei kohusta liikmesriike hoiduma mis tahes toimingutest, millega võidakse rikkuda konventsiooniga tagatud õigust, vaid et teatavatel juhtudel peavad nad ka täitma positiivseid kohustusi inimeste era- ja perekonnaelu austamise igakülgseks tagamiseks[6]. Paljusid kõnealuseid kohtuasju käsitletakse täpsemalt asjaomastes peatükkides.

1.1.2. Euroopa Nõukogu konventsioon nr 108

Infotehnoloogia tärkamisega 1960. aastatel hakkas kasvama ka vajadus põhjalikumate eeskirjade järele, et pakkuda inimestele kaitset nende (isiku-)andmeid kaitstes. 1970. aastate keskpaigaks oli Euroopa Nõukogu ministrite komitee Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8 viidates vastu võtnud

2 Euroopa Nõukogu, Euroopa inimõiguste ja põhivabaduste kaitse konventsioon, CETS nr 005, 1950.

3 Vt nt EIK, *Malone vs. Ühendkuningriik*, nr 8691/79, 2. august 1984; EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 3. aprill 2007.

4 Vt nt EIK, *Klass jt vs. Saksamaa*, nr 5029/71, 6. september 1978; EIK, *Uzun vs. Saksamaa*, nr 35623/05, 2. september 2010.

5 Vt nt EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987; EIK, *S. ja Marper vs. Ühendkuningriik*, nr 30562/04, 4. detsember 2008.

6 Vt nt EIK, *I. vs. Soome*, nr 20511/03, 17. juuli 2008; EIK, *K.U. vs. Soome*, nr 2872/02, 2. detsember 2008.

mitu isikuandmete kaitset käsitlevat resolutsiooni[7]. 1981. aastal avati allkirjastamiseks isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (konventsioon nr 108)[8]. See konventsioon oli ja on praegugi andmekaitse valdkonnas ainus rahvusvaheline õiguslikult siduv dokument.

Konventsioon nr 108 kehtib igale andmetöötlusele, mis on tehtud era- või avaliku sektori poolt, nagu näiteks andmetöötlus kohtu- ja õiguskaitse organite poolt. Sellega kaitstakse üksikisikut kuritarvitamise eest, mis võib kaasneda isikuandmete kogumise ja töötlemisega, ning samal ajal on selle eesmärk reguleerida isikuandmete piiriülest liikumist. Isikuandmete kogumise ja töötlemise puhul käsitlevad konventsioonis sätestatud põhimõtted eeskätt andmete õiglast ja seaduslikku kogumist ja automaattöötlust ning nõuet, et andmeid säilitatakse kindlaks määratud õiguspärastel eesmärkidel ja mitte kõnealuste eesmärkidega vastuolus olevatel põhjustel, samuti ei säilitata andmeid kauem kui vajalik. Konventsiooni põhimõtetega reguleeritakse ka andmete kvaliteeti, eelkõige sätestatakse, et andmed peavad olema piisavad ja asjakohased ning et andmete hulk ei tohi ületada nende kogumise eesmärgi piire (proportsionaalsus), samuti peavad need olema täpsed.

Konventsiooniga nähakse ette isikuandmete kogumise ja töötlemisega seotud tagatised ning teisalt keelustatakse nõuetekohaste õiguslike tagatiste puudumisel tundlike andmete töötlemine, näiteks andmed rassi, poliitiliste vaadete, tervise, usutunnistuse, seksuaalelu või kriminaalmenetluste kohta.

Samuti talletatakse konventsioonis üksikisiku õigus teada, millist teavet tema kohta säilitatakse, ning lasta seda vajaduse korral parandada. Konventsioonis sätestatud õiguste puhul saab piiranguid kohaldada vaid juhul, kui see on vajalik ülekaalukate huvide seisukohalt, näiteks riigi julgeolek või -kaitse.

Kuigi konventsiooniga nähakse ette isikuandmete vaba liikumine konventsiooniga ühinenud riikide vahel, kehtestatakse sellise liikumise suhtes teatavad piirangud, juhul kui õigusraamistikuga ei ole tagatud võrdväärset kaitset.

7 Euroopa Nõukogu ministrite komitee, 1973, Resolutsioon (73) 22 üksikisikute eraelu puutumatuse kaitse kohta seoses erasektori elektrooniliste andmepankadega, 26. september 1973; Euroopa Nõukogu ministrite komitee, 1974, Resolutsioon (74) 29 üksikisikute eraelu puutumatuse kaitse kohta seoses avaliku sektori elektrooniliste andmepankadega, 20. september 1974.

8 Euroopa Nõukogu, Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, CETS nr 108, 1981.

Konventsioonis nr 108 kehtestatud üldpõhimõtete ja -eeskirjade täiendamiseks on Euroopa Nõukogu ministrite komitee vastu võtnud mitu soovitust, mis ei ole aga õiguslikult siduvad (vt 7. ja 8. peatükk).

Kõnealuse konventsiooni on ratifitseerinud kõik ELi liikmesriigid. 1999. aastal muudeti konventsiooni nr 108, et EL saaks sellega ühineda[9]. Peale selle võeti 2001. aastal vastu konventsiooni nr 108 lisaprotokoll, millega kehtestati sätted andmete piiriülese liikumise kohta riikidesse, mis ei ole konventsiooniga ühinenud, st kolmandatesse riikidesse, ning liikmesriikidele määrati kohustus asutada andmekaitse järelevalveasutused[10].

Väljavaated

Pärast otsust konventsiooni nr 108 ajakohastada kinnitati 2011. aastal korraldatud avaliku konsultatsiooni tulemuste põhjal selle protsessi kaks peamist eesmärki: eraelu puutumatuse kaitse tugevdamine digitaalajastul ja konventsiooni järelevalvemehhanismi täiendamine.

Konventsioon nr 108 on avatud ühinemiseks riikidele, mis ei kuulu Euroopa Nõukogusse, sh väljaspool Euroopat asuvatele riikidele. Kuna konventsiooni on võimalik rakendada üldstandardina ning see on avatud kõikidele riikidele, oleks see hea pidepunkt, millest lähtuda andmekaitse edendamisel ülemaailmsel tasandil.

Praegu on konventsiooni nr 108 46 osalisriigist 45 Euroopa Nõukogu liikmesriigid. Esimese väljaspool Euroopat asuva riigina ühines konventsiooniga Uruguay 2013. aasta augustis ning ministrite komitee kutsel konventsiooniga nr 108 ühineva Maroko puhul on käimas asjaomase protsessi viimased ettevalmistused.

1.1.3. Euroopa Liidu andmekaitseõigus

ELi õigus koosneb lepingutest ja teisestest ELi õigusaktidest. Lepingud, st Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu, on heaks kiitnud kõik ELi liikmesriigid ning neid nimetatakse ka esmasteks õigusaktideks. ELi määruseid, direktiive ja otsuseid võtavad vastu asjaomaste lepingute alusel selleks volitatud ELi

9 Euroopa Nõukogu, Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (ETS nr 108) muudatused, mis võimaldavad Euroopa Ühendustel konventsiooniga ühineda; vastu võetud ministrite komitees Strasbourgis 15. juunil 1999; konventsiooni nr 108 artikli 23 lõige 2 muudetud kujul.

10 Euroopa Nõukogu, Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni lisaprotokoll, mis käsitleb järelevalveasutusi ja andmete piiriülest liikumist, CETS nr 181, 2001.

institutsioonid ning nende puhul kasutatakse sageli üldnimetust „teisesed ELi õigusaktid".

Peamine ELi andmekaitsealane õigusakt on Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (andmekaitsedirektiiv)[11]. See võeti vastu 1995. aastal, kui mitu liikmesriiki olid juba vastu võtnud riigi tasandi andmekaitsealased õigusaktid. Kaupade, kapitali, teenuste ja isikute vaba liikumise võimaldamiseks siseturul oli vaja tagada ka andmete vaba liikumine, mille puhul tuli omakorda liikmesriikidele pakkuda ühtselt kõrget andmekaitsetaset.

Kuna andmekaitsedirektiiv võeti vastu riikide asjaomaste õigusaktide ühtlustamise[12] eesmärgil, on direktiivi üksikasjalikkuse tase võrreldav liikmesriikide (sel ajal kehtinud) andmekaitsealaste õigusaktide üksikasjalikkuse tasemega. Euroopa Liidu Kohtu jaoks on Direktiivi 95/46 mõte tagada, et kõikides liikmesriikides on ühtselt tagatud üksikisiku õigus isikuandmete kaitsele. Siin kohaldatavate riiklike seaduste ühtlustamine ei tohi kaasa tuua isikuandmete kaitse vähenemist, vaid vastupidi, see peab tagama ühtlaselt kõrge kaitse terves Euroopa Liidus. Riiklike seaduste ühtlustamine ei ole piiratud minimaalsele ühtlustamisele vaid kätkeb endas ühtlustamist, mis on üldiselt juba valmis." Seegaei ole liikmesriikidel direktiivi rakendamisel üleliia tegutsemisruumi[13].

Andmekaitsedirektiivi eesmärk on täpsustada konventsioonis nr 108 juba sätestatud põhimõtteid eraelu puutumatuse õiguse kohta ning laiendada nende sisu. Asjaolu, et 1995. aastal olid kõik ELi 15 liikmesriiki ka asjaomase konventsiooni osalised, välistab vastandlikud eeskirjad neis kahes õigusdokumendis. Andmekaitsedirektiivis on aga edasi arendatud konventsiooni nr 108 artikliga 11 ette nähtud võimalust pakkuda muid kaitsemeetmeid. Euroopa andmekaitseõiguse tulemusliku toimimise tagamisele on eriti tõhusalt kaasa aidanud sõltumatu järelevalve kehtestamine, et parandada andmekaitse-eeskirjade järgimist. (2001. aastal konventsiooni nr 108 lisaprotokolliga võeti sama põhimõte üle ka Euroopa Nõukogu õigusesse.)

11 Andmekaitsedirektiiv, EÜT L 281, 1995, lk 31.

12 Vt nt andmekaitsedirektiivi 1., 4., 7. ja 8. põhjendus.

13 ELK, ühine kohtuasi C-468/10 ja C469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) vs. Administración del Estado*, 24 November 2011, para. 28-29.

Andmekaitsedirektiivi territoriaalne kohaldamisala ulatub ELi 28st liikmesriigist kaugemale, hõlmates ka ELi mittekuuluvaid Euroopa Majanduspiirkonna (EMP)[14] riike, nimelt Islandit, Liechtensteini ja Norrat.

Selleks et andmekaitsedirektiivi kohaldataks liikmesriikides tulemuslikul ja ühtsel viisil, on Luxembourgis asuval ELK-l volitus välja selgitada, kas liikmesriik on täitnud direktiivist tulenevaid kohustusi, ning teha eelotsuseid direktiivi kehtivuse ja tõlgendamise küsimustes. Oluline erand andmekaitsedirektiivi kohaldamisel käsitleb kodust tegevust, st direktiivi ei kohaldata isikuandmete töötlemise suhtes, kui seda teeb füüsiline isik isiklikel või kodustel eesmärkidel[15]. See loetakse üldiselt üksikisiku vabaduste hulka.

Kooskõlas andmekaitsedirektiivi vastuvõtmise ajal jõus olnud ELi esmaste õigusaktidega piirdub direktiivi esemeline kohaldamisala siseturuga seotud küsimustega. Selle kohaldamisalasse ei kuulu eeskätt näiteks politsei- ja kriminaalõigusalane koostöö. Nende valdkondade andmekaitsesüsteem põhineb eri õigusaktidel, mida kirjeldatakse täpsemalt 7. peatükis.

Kuna andmekaitsedirektiiv oli suunatud üksnes ELi liikmesriikidele, tekkis vajadus täiendava õigusakti järele, et tagada andmekaitse isikuandmete töötlemisel ELi institutsioonides ja asutustes. Sel otstarbel võeti vastu määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (ELi institutsioonide andmekaitse määrus)[16].

Peale selle on isegi andmekaitsedirektiiviga hõlmatud valdkondades tihtipeale vaja täpsemaid andmekaitsesätteid, et tagada vajalik selgus muude õigustatud huvide tasakaalustamisel. Kaks asjakohast näidet on direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv),[17] ning direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üld-

14 Euroopa Majanduspiirkonna leping, mis jõustus 1. jaanuaril 1994. EÜT L 1, 1994.

15 Andmekaitsedirektiivi artikli 3 lõike 2 teine taane.

16 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, EÜT L 8, 2001.

17 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 2002.

kasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (andmete säilitamise direktiiv, kehtetuks tunnistatud 8 aprillil 2014.)[18]. Teisi näiteid käsitletakse 8. peatükis. Asjaomased sätted peavad olema kooskõlas andmekaitsedirektiiviga.

Euroopa Liidu põhiõiguste harta

Euroopa Ühenduste asutamislepingutes ei käsitletud mingil viisil inimõigusi ega nende kaitset. Kui aga toonasel Euroopa Ühenduste Kohtul tuli hakata tegelema inimõiguste väidetava rikkumise juhtumitega ELi õiguse kohaldamisalasse kuuluvates valdkondades, töötati välja uus lähenemisviis. Üksikisikute kaitsmiseks lülitati Euroopa õiguse üldpõhimõtetesse põhiõigused. ELK järgi kajastavad kõnealused üldpõhimõtted riikide põhiseadustes ja inimõigusi käsitlevates lepingutes, eeskätt Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis talletatud inimõiguste kaitse alustalasid. Kohus märkis, et võtab eesmärgiks tagada, et ELi õigusaktid oleks nende põhimõtetega kooskõlas.

Tunnistades, et ELi poliitikal võib olla mõju inimõigustele, ning püüdes lähendada kodanikke ELile, kuulutati 2000. aastal välja Euroopa Liidu põhiõiguste harta (edaspidi „harta"). Selles hartas sätestatakse hulk Euroopa kodanike kodaniku-, poliitilisi, majanduslikke ja sotsiaalseid õigusi, ühendades eri põhiseaduslikud tavad ja liikmesriikide ühised rahvusvahelised kohustused. Hartas kirjeldatud õigused on jagatud kuude valdkonda: väärikus, vabadused, võrdsus, solidaarsus, kodanike õigused ja õigusemõistmine.

Kuigi alguses oli harta vaid poliitiline dokument, muudeti see ELi esmase õigusaktina õiguslikult siduvaks[19] (vt ELi lepingu artikli 6 lõige 1) Lissaboni lepingu jõustumisega 1. detsembril 2009[20].

ELi esmased õigusaktid hõlmavad ka ELi üldpädevust võtta vastu andmekaitsealaseid õigusakte (ELi toimimise lepingu artikkel 16).

18 Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (andmete säilitamise direktiiv), ELT L 105, 2006, kehtetuks tunnistatud 8 aprillil 2014.

19 EL (2012), Euroopa Liidu põhiõiguste harta, ELT C 326, 2012.

20 Vt Euroopa Liidu lepingu konsolideeritud versioon (2012), ELT C 326, 2012, ja Euroopa Liidu toimimise lepingu konsolideeritud versioon (2012), ELT C 326, 2012.

Era- ja perekonnaelu austamise (artikkel 7) tagamise kõrval kehtestatakse hartaga ka õigus isikuandmete kaitsele (artikkel 8), mis tähendab, et sellega omistati isikuandmete kaitsele ELi õiguses sõnaselgelt põhiõiguse staatus. Seda õigust peavad austama ja kaitsma nii ELi institutsioonid kui ka liikmesriigid, sest harta artikli 51 kohaselt kehtib see kohustus liidu õiguse kohaldamise korral ka liikmesriikidele. Mitu aastat pärast andmekaitsedirektiivi vastuvõtmist koostatud harta artiklit 8 tuleb käsitada varem kehtestatud ELi andmekaitsealaste õigusaktide tulemina. Lisaks sellele, et artikli 8 lõikes 1 käsitletakse sõnaselgelt õigust andmekaitsele, on artikli 8 lõikes 2 kirjeldatud ka peamisi andmekaitsepõhimõtteid. Samuti on harta artikli 8 lõikega 3 ette nähtud, et nende põhimõtete rakendamist kontrollib sõltumatu asutus.

Väljavaated

2012. aasta jaanuaris tegi Euroopa Komisjon ettepaneku andmekaitse reformipaketi kohta, märkides, et praeguseid andmekaitse-eeskirju tuleks tehnoloogia kiiret arengut ja üleilmastumist silmas pidades ajakohastada. Reformipakett koosneb isikuandmete kaitse üldmäärusest,[21] mis peaks asendama andmekaitsedirektiivi, ning uuest andmekaitsedirektiivist,[22] milles käsitletakse andmekaitset kriminaalasjades tehtavas politseikoostöös ja õigusalases koostöös. Käesoleva käsiraamatu avaldamise ajal oli reformipakett veel arutlusel.

1.2. Õiguste tasakaalustamine

Põhipunkt

- Õigus isikuandmete kaitsele ei ole absoluutne õigus; selle puhul tuleb arvesse võtta ka teisi õigusi.

Põhiõiguste harta artiklis 8 sätestatud põhiõigus isikuandmete kaitsele „ei ole siiski absoluutne põhimõte, vaid sellega tuleb arvestada vastavalt selle ülesandele

21 Euroopa Komisjon (2012), *Ettepanek: Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus)*, COM(2012) 11 (final), Brüssel, 25. jaanuar 2012.

22 Euroopa Komisjon (2012), *Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta,* COM(2012) 10 (final), Brüssel, 25. jaanuar 2012.

ühiskonnas"[23]. Seepärast tunnistatakse harta artikli 52 lõikes 1, et muu hulgas artiklites 7 ja 8 sätestatud õiguste teostamist võib piirata, tingimusel et piirangud on ette nähtud seadusega, need arvestavad nimetatud õiguste ja vabaduste olemust ning need on proportsionaalsuse põhimõtte kohaselt vajalikud ja vastavad tegelikult Euroopa Liidu tunnustatud avalikku huvi teenivatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi[24].

Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis on andmekaitse tagatud artikli 8 alusel (õigus era- ja perekonnaelu austamisele) ja nagu ka harta puhul, tuleb seda õigust kohaldada paralleelselt teisi samaväärseid õigusi arvesse võttes. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 on sätestatud: „Võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik [...] kaasinimeste õiguste ja vabaduste kaitseks."

Sellest tulenevalt on nii EIK kui ka ELK korduvalt nentinud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 ja Euroopa Liidu põhiõiguste harta artikli 8 kohaldamisel ja tõlgendamisel tuleb samal ajal arvesse võtta teisi õigusi[25]. Mitu tähtsat näidet illustreerivad, kuidas saavutada nimetatud õiguste vahel tasakaalu.

1.2.1. Sõnavabadus

Õigusega andmekaitsele võib suure tõenäosusega konflikti sattuda muu hulgas õigus sõnavabadusele.

Sõnavabaduse kaitse põhineb harta artiklil 11 („Sõna- ja teabevabadus"). „See õigus kätkeb arvamusvabadust ning vabadust saada ja levitada teavet ja ideid avaliku võimu sekkumiseta ning sõltumata riigipiiridest." Artiklile 11 vastab Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 10. Harta artikli 52

23 Vt nt ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, 9. november 2010, punkt 48.

24 *Ibid.*, punkt 50.

25 EIK, *Von Hannover vs. Saksamaa (nr 2) [suurkoda]*, nr 40660/08 ja 60641/08, 7. veebruar 2012; ELK, liidetud kohtuasjad C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vs. Administración del Estado*, 24. november 2011, punkt 48; ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 29. jaanuar 2008, punkt 68. Vt ka Euroopa Nõukogu, 2013, Euroopa Inimõiguste Kohtu praktika isikuandmete kaitse valdkonnas, DP (2013) Case law, kättesaadav: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20%28final%29.pdf.

lõike 3 kohaselt on „selliste õiguste tähendus ja ulatus, mis vastavad Euroopa inimõiguste ja põhivabaduse kaitse konventsiooniga tagatud õigustele, [...] samad, mis neile nimetatud konventsiooniga ette on nähtud". Seega ei tohi piirangud, mida võidakse õiguspäraselt kohaldada harta artikliga 11 tagatud õiguse suhtes, ületada Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 lõikega 2 ette nähtud piiranguid, st need peavad olema fikseeritud seaduses ning „demokraatlikus ühiskonnas vajalikud [...] kaasinimeste reputatsiooni või õiguste kaitseks". See kontseptsioon hõlmab õigust andmekaitsele.

Isikuandmete kaitse ja sõnavabaduse suhet reguleeritakse andmekaitsedirektiivi artikliga 9 („Isikuandmete töötlemine ja sõnavabadus")[26]. Selle artikli kohaselt peavad liikmesriigid sätestama teatavad erandid või piirangud andmekaitse suhtes ja seega selle direktiivi II, IV ja VI peatükis ette nähtud eraelu puutumatuse põhiõiguse suhtes. Need erandid peavad olema tehtud üksnes ajakirjanduse jaoks või kunstilise või kirjandusliku eneseväljenduse huvides, mis on hõlmatud põhiõiguste hulka kuuluva sõnavabadusega, kui see on vajalik selleks, et ühitada eraelu puutumatuse õigus ja sõnavabadust reguleerivad eeskirjad.

Näide: kohtuasjas *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy*[27] paluti Euroopa Liidu Kohtul tõlgendada andmekaitsedirektiivi artiklit 9 ning määratleda andmekaitse ja ajakirjandusvabaduse seos. Kohus pidi analüüsima ligikaudu 1,2 miljoni füüsilise isiku maksuandmete levitamist Markkinapörssi ja Satamedia kaudu, kes kogusid need andmed seaduslikul alusel Soome maksuasutustelt. Eeskätt oli kohtul vaja selgeks teha, kas maksuasutuste avaldatud isikuandmete töötlemist, mis võimaldas mobiilikasutajatel tellida telefonile teiste füüsiliste isikutega seotud maksuandmeid, tuleb pidada isikuandmete töötlemiseks üksnes ajakirjanduse jaoks. Olles järeldanud, et Satakunnani toimingud võib lugeda isikuandmete töötlemiseks andmekaitsedirektiivi artikli 3 lõike 1 tähenduses, asus kohus tõlgendama direktiivi artiklit 9. Esiteks rõhutas kohus sõnavabaduse tähtsust igas demokraatlikus ühiskonnas ning märkis, et sellega seonduvaid mõisteid, sealhulgas ajakirjanduse mõistet, tuleb tõlgendada laialt. Seejärel nentis kohus, et kahe põhiõiguse vahelise tasakaalu tagamiseks tuleb seoses õigusega andmekaitsele tehtavate erandite ja piirangute puhul piirduda rangelt vajalikuga. Selles kontekstis järeldas kohus, et Markkinapörssi ja Satamedia toimingud liikmesriigi õigusnormide kohaselt

26 Andmekaitsedirektiivi artikkel 9.

27 ELK, C-73/07, *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy*, 16. detsember 2008, punktid 56, 61 ja 62.

avalikest dokumentidest pärit andmetega võib kvalifitseerida ajakirjanduslikuks tegevuseks, kui selle eesmärk on teabe, arvamuste ja mõtete avalikustamine, olenemata edastamise vahendist. Samuti otsustas kohus, et need toimingud ei puuduta üksnes meediaettevõtteid ning sellega võib seonduda kasu saamise eesmärk. Samal ajal jättis ELK liikmesriigi kohtu ülesandeks otsustada, kas see konkreetsel juhul kehtib.

Seoses sellega, kuidas ühitada õigust andmekaitsele ja õigust sõnavabadusele, on ka EIK teinud mitu olulist otsust.

Näide: kohtuasjas *Axel Springer AG vs. Saksamaa*[28] järeldas EIK, et kui siseriiklik kohus keelas ajalehe omanikul avaldada artiklit tuntud näitleja vahistamise ja süüdimõistmise kohta, rikuti sellega Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 10. Kohus kordas üle kriteeriume eelnevast kohtupraktikast seoses juhtumitega, kus on tulnud tasakaalustada õigust sõnavabadusele ja õigust eraelu puutumatusele:

- esiteks tuli kaaluda, kas avaldatud artiklis kajastatav sündmus pakkus avalikku huvi – isiku vahistamine ja süüdimõistmine oli kohtus kinnitatud ja üldsusele teada fakt ning pakkus seega avalikku huvi;
- teiseks tuli kaaluda, kas tegemist oli avaliku elu tegelasega – asjaomane isik oli näitlejana piisavalt tuntud, et teda loetaks avaliku elu tegelaseks;
- kolmandaks tuli kaaluda, kust teave saadi ning kas see oli usaldusväärne – teave pärines riigiprokuratuurilt ning selle üle, kas mõlemas artiklis avaldatud teave oli õige, pooled ei vaielnud.

Seepärast otsustas EIK, et äriühingule määratud avaldamispiirangud ei olnud mõistlikul määral proportsionaalsed kaebuse esitaja eraelu kaitsmise õiguspärase eesmärgiga. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 rikkumisega.

Näide: kohtuasjas *Von Hannover vs. Saksamaa (nr 2)*[29] leidis EIK pärast seda, kui Monaco printsess Caroline'il ei õnnestunud taotleda tõkendit, millega takis-

28 EIK, *Axel Springer AG vs. Saksamaa [suurkoda]*, nr 39954/08, 7. veebruar 2012, punktid 90 ja 91.

29 EIK, *Von Hannover vs. Saksamaa (nr 2) [suurkoda]*, nr 40660/08 ja 60641/08, 7. veebruar 2012, punkt 118 ja 124.

tada temast ja tema abikaasast suusapuhkusel tehtud foto avaldamist, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 tagatud õigust eraelu austamisele ei ole rikutud. Fotoga kaasnes artikkel, milles kajastati muude teemade hulgas prints Rainier' kehva terviseseisundit. EIK järeldas, et siseriiklikud kohtud olid põhjalikkusega kaalunud meediaväljaannete õigust sõnavabadusele ja kaebuse esitajate õigust eraelu austamisele. Asjaolu, et siseriiklikud kohtud pidasid prints Rainier' haigust tänapäeva ühiskonnas olulist rolli etendavaks sündmuseks, ei loetud ebamõistlikuks ning põhjendus, et koosluses artikliga panustas kõnealune foto vähemalt mingil määral ühiskondlikku huvi pakkuvasse arutellu, tundus EIK-le vastuvõetav. Kohus järeldas, et tegu ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

EIK kohtupraktikas on üks määrav kriteerium asjaomaste õiguste tasakaalustamisel see, kas kõne all olev teema on oluline avalikku huvi pakkuva arutelu seisukohalt.

Näide: kohtuasjas *Mosley vs. Ühendkuningriik*[30] arutati juhtumit, kus ühes nädalalehes avaldati kaebuse esitajast intiimsed fotod. Seejärel väitis ta, et tema suhtes on rikutud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8, arvestades, et tal ei olnud võimalust taotleda enne fotode avaldamist tõkendit, kuna väljaanne ei ole kohustatud teatama ette sellise materjali avaldamisest, mis võib ohtu seada üksikisiku õiguse eraelu puutumatusele. Kuigi kõnealust materjali levitati üldiselt pigem meelelahutuslikel kui hariduslikel eesmärkidel, loodeti selle puhul kahtlemata asjaomase konventsiooni artikliga 10 tagatavale kaitsele, mille võivad aga üles kaaluda artiklis 8 sätestatud nõuded, mille alusel ei tohiks teavet levitada juhul, kui see on eraelulise või intiimse sisuga ning kui selle levitamisel ei ole avalikku huvi pakkuvat mõõdet. Iseäranis delikaatselt tuli analüüsida piiranguid, mis võivad toimida teatavat laadi avaldamiseelse tsensuurina. Pidades silmas negatiivset mõju, mille materjali avaldamisest etteteatamise nõue võib kaasa tuua, kahtlusi selle tulemuslikkuse suhtes ning laia kaalutlusruumi kõnealuses valdkonnas, leidis EIK, et artiklist 8 ei tulene õiguslikult siduvat eelneva teavitamise kohustust. Vastavalt sellele otsustas kohus, et artiklit 8 ei ole rikutud.

Näide: kohtuasjas *Biriuk vs. Leedu*[31] nõudis kaebuse esitaja kahjuhüvitist päevalehelt, kuna selle ühes artiklis väideti, et ta on HIV positiivne. Väidetavalt olid

30 EIK, *Mosley vs. Ühendkuningriik*, nr 48009/08, 10. mai 2011, punktid 129 ja 130.

31 EIK, *Biriuk vs. Leedu*, nr 23373/03, 25. november 2008.

seda teavet kinnitanud kohaliku haigla meditsiinitöötajad. EIK arvates ei panustanud kõnealune artikkel avalikku huvi pakkuvasse arutellu ning kohus kinnitas, et isikuandmete, sealhulgas meditsiiniliste andmete kaitse on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 tagatud üksiksiku era- ja perekonnaelu austamise õiguse seisukohalt ülimalt oluline. Eriti imestusväärseks pidas kohus asjaolu, et ajalehes avaldatud andmete kohaselt pärines teave kaebuse esitaja haiguse kohta haigla meditsiinitöötajatelt, mis on ilmselgelt vastuolus arstisaladuse hoidmise kohustusega. Sellest tulenevalt ei suutnud riik kaitsta kaebuse esitaja õigust eraelu austamisele. Kohus otsustas, et tegu oli artikli 8 rikkumisega.

1.2.2. Juurdepääs dokumentidele

Põhiõiguste harta artiklis 11 ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 10 sätestatud teabevabadusega kaitstakse ühelt poolt õigust teavet edastada ja teisalt õigust teavet *saada*. Üha enam mõistame, et demokraatliku ühiskonna toimimise seisukohalt on oluline tagada valitsussüsteemi läbipaistvus. Seepärast on viimase 20 aasta jooksul otsustatud, et õigus tutvuda riigiasutustes säilitatavate dokumentidega peab olema kõikidel ELi kodanikel ja igal füüsilisel või juriidilisel isikul, kes elab või kelle registrijärgne asukoht on mõnes liikmesriigis.

Euroopa Nõukogu õiguse puhul saab viidata ametlikele dokumentidele juurdepääsu käsitlevas soovituses sätestatud põhimõtetele; see soovitus oli eeskuju ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooni koostamisel (konventsioon nr 205)[32]. **ELi õiguse** puhul on õigus tutvuda dokumentidega tagatud määrusega (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (dokumentidele juurdepääsu käsitlev määrus)[33]. Harta artikliga 42 ja ELi toimimise lepingu artikli 15 lõikega 3 on dokumentidega tutvumise õigust laiendatud liidu institutsioonide, organite ja asutuste mis tahes kandjal säilitatavatele dokumentidele. Kooskõlas harta artikli 52 lõikega 2 teostatakse õigust tutvuda dokumentidega ka ELi toimimise lepingu artikli 15 lõikes 3 määratletud tingimustel ja piires. Kõnealune õigus võib konflikti sattuda õigusega isikuandmete kaitsele, kui dokumendiga tutvumine hõlmaks teiste inimeste isikuandmete

32 Euroopa Nõukogu ministrite komitee (2002), Soovitus Rec(2002)2 liikmesriikidele ametlikele dokumentidele juurdepääsu kohta, 21. veebruar 2002; Euroopa Nõukogu, Ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon, CETS nr 205, 18. juuni 2009. Konventsioon ei ole veel jõustunud.

33 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1049/2001, 30. mai 2001, üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele, EÜT L 145, 2001.

avaldamist. Seetõttu tuleb riigiasutuste valduses olevate dokumentide või teabega tutvumise taotluste puhul arvesse võtta nende inimeste õigust isikuandmete kaitsele, kelle andmeid kõnealused dokumendid sisaldavad.

Näide: kohtuasjas *Euroopa Komisjon vs. Bavarian Lager*[34] määratles Euroopa Liidu Kohus ELi institutsioonide dokumentidele juurdepääsu puhul tagatava isikuandmete kaitse ulatuse ning määruse nr 1049/2001 (dokumentidele juurdepääsu käsitlev määrus) ja määruse nr 45/2001 (andmekaitsemäärus) vahelised seosed. 1992. aastal asutatud Bavarian Lager impordib saksa pudeliõlut Ühendkuningriiki, peamiselt alkohoolse joogi jaemüügi kohtadele. Sellega tekkis aga probleeme, sest Briti õigusaktid soosisid *de facto* kodumaiseid tootjaid. Bavarian Lageri kaebuse peale otsustas Euroopa Komisjon algatada Ühendkuningriigi vastu liikmesriigi kohustuste rikkumise menetluse, misjärel Ühendkuningriik muutis asjaomaseid sätteid ning ühtlustas neid ELi õigusega. Seejärel palus Bavarian Lager komisjonilt teiste dokumentide kõrval koopiat komisjoni, Ühendkuningriigi ametiasutuste ja ühisturu õlletootjate liidu (Confédération des Brasseurs du Marché Commun, CBMC) esindajate osalusel toimunud koosoleku protokollist. Komisjon nõustus avaldama teatavad dokumendid koosoleku kohta, aga kustutas koosoleku protokollist viis nime, kuna kaks isikut olid sõnaselgelt vastu oma isikuandmete avaldamisele ja veel kolmega ei olnud komisjonil õnnestunud ühendust saada. 18. märtsi 2004. aasta otsusega jättis komisjon rahuldamata Bavarian Lageri kordustaotluse protokolli täisversiooniga tutvumiseks, põhjendades seda eeskätt asjaomaste isikute eraelu kaitsega, mis on tagatud andmekaitsemäärusega. Kuna selline põhjendus ei olnud Bavarian Lagerile vastuvõetav, esitati hagiavaldus Esimese Astme Kohtusse, kes tühistas komisjoni otsuse 8. novembri 2007. aasta otsusega (kohtuasi T-194/04, *Bavarian Lager vs. komisjon),* arvestades, et ainuüksi asjaolu, et dokumendis oli asjaomaste asutuste esindajatena mainitud kõnealuste isikute nimesid, ei tähendanud tingimata eraelu austamise kohustuse rikkumist ning see ei seadnud ohtu nende eraelu.

Komisjoni apellatsioonkaebuse peale tühistas ELK Esimese Astme Kohtu otsuse. ELK leidis, et dokumentidele juurdepääsu käsitlev määrus „kehtestab erikorra ja tugevdab niisuguse isiku kaitset, kelle isikuandmeid võidakse vajaduse korral üldsusele edastada". ELK järeldas, et kui dokumentidele juurdepääsu käsitleva määruse alusel esitatud taotlusega soovitakse saada juurdepääsu isikuandmeid

34 ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*, 29. juuni 2010, punktid 60, 63, 76, 78 ja 79.

sisaldavatele dokumentidele, kohaldatakse kõiki dokumentidele juurdepääsu käsitleva määruse sätteid. Seejärel otsustas ELK, et komisjoni otsus jätta 1996. aasta oktoobris toimunud koosoleku protokolli täisversiooniga tutvumiseks esitatud taotlus rahuldamata oli õigustatud. Kuna komisjon ei olnud saanud viielt koosolekul osalenud isikult nõusolekut nende nimede avaldamiseks, täitis komisjon piisaval määral selguse ja arusaadavuse kohustust, avaldades dokumendist sellise versiooni, kust olid eemaldatud asjaomaste isikute nimed.

Peale selle leidis ELK, et kuna „Bavarian Lager ei esitanud ühtegi selget ja õiguspärast veenvat argumenti, mis tõendaks nende isikuandmete üleandmise vajadust, siis ei saanud komisjon kaaluda asjaomaste poolte erinevaid huve. Ta ei saanud ka kontrollida vastavalt [andmekaitsemäärusele], kas on põhjust arvata, et andmete üleandmine kahjustaks andmesubjektide õigustatud huve".

Selle kohtuotsuse alusel tohib isikuandmete kaitse õigusesse seoses dokumentidele juurdepääsuga sekkuda üksnes konkreetsel ja õigustatud põhjusel. Õigus tutvuda dokumentidega ei kaalu automaatselt üles õigust isikuandmete kaitsele[35].

Järgmises Euroopa Inimõiguste Kohtu otsuses käsitleti asjaomase juurdepääsutaotluse puhul üht konkreetset aspekti.

Näide: kohtuasjas *Társaság a Szabadságjogokért vs. Ungari*[36] oli kaebuse esitaja (inimõiguste eest seisev vabaühendus) taotlenud konstitutsioonikohtult juurdepääsu ühe menetluses olnud kohtuasjaga seotud teabele. Konstitutsioonikohus keeldus juurdepääsu lubamast põhjendusega, et kohtule esitatud kaebusi tohib välistele isikutele avaldada vaid kaebuse esitaja nõusolekul, kuigi asjaomase kohtuasja algatanud parlamendiliikmega ei olnud nõu peetud. Siseriiklikud kohtud pooldasid taotluse tagasilükkamist, sest selliste isikuandmete kaitset ei tohiks üles kaaluda muud õiguspärased huvid, sealhulgas avaliku teabe kättesaadavus. Kaebuse esitaja oli teatavas mõttes ühiskonna valvekoer, kelle tegevust võinuks kaitsta sarnasel viisil nagu ajakirjanduse puhul. Ajakirjandusvabaduse puhul oli EIK varasemas kohtupraktikas korduvalt järeldanud, et üldsusel on õigus saada avalikku huvi pakkuvat teavet. Kaebuse esitaja taotletud teave oli olemas ja kättesaadav ning eraldi andmete kogumist ei olnud selle puhul

35 Vt teisalt Euroopa andmekaitseinspektori (2011) üksikasjalikke kaalutlusi dokumendis „Public access to documents containing personal data after the Bavarian Lager ruling" (e k „Avalik juurdepääs isikuandmeid sisaldavatele dokumentidele Bavarian Lageri otsuses"), Brüssel, 24. märts 2011.

36 EIK, *Társaság a Szabadságjogokért vs. Ungari*, nr 37374/05, 14. aprill 2009; vt punktid 27, 36–38.

vaja. Sellistel tingimustel ei olnud riigil kohustust piirata kaebuse esitaja taotletud teabe avaldamist. Kokkuvõttes järeldas EIK, et meetmed, millega piiratakse juurdepääsu avalikku huvi pakkuvale teabele, võivad vähendada meediasfääris või muudes valdkondades tegutsevate isikute indu n-ö ühiskonna valvekoera ülesannete täitmisel. Kohus otsustas, et tegu oli artikli 10 rikkumisega.

ELi õiguses on selgusel ja arusaadavuseloluline koht. Selguse ja arusaadavuse põhimõte on talletatud ELi lepingu artiklites 1 ja 10 ning ELi toimimise lepingu artikli 15 lõikes 1[37]. Määruse (EÜ) nr 1049/2001 2. põhjenduse kohaselt võimaldab see kodanikel osaleda rohkem otsustamisprotsessis ja tagab juhtorganitele suurema legitiimsuse ning tulemuslikkuse ja suurema vastutuse kodanike ees demokraatlikus süsteemis[38].

Selle arutluskäigu alusel nõutakse nõukogu määrusega (EÜ) nr 1290/2005 ühise põllumajanduspoliitika rahastamise kohta ja komisjoni määrusega (EÜ) nr 259/2008, milles sätestatakse nõukogu määruse (EÜ) nr 1290/2005 kohaldamise üksikasjalikud eeskirjad, teabe avaldamist teatavatest põllumajandussektori ELi fondidest toetuse saajate kohta ja igale toetuse saajale makstud summade kohta[39]. Selle teabe avalikustamine peaks tugevdama avalikkuse kontrolli selle üle, et haldusasutused kasutaksid avaliku sektori rahalisi vahendeid otstarbekohaselt. Hulk toetuse saajaid aga vaidlustas kõnealuse avaldamiskohustuse proportsionaalsuse.

Näide: kohtuasjas *Volker und Markus Schecke ja Hartmut Eifert vs. Land Hessen*[40] pidi ELK otsustama, kas ELi õigusaktides sätestatud kohustus avalikustada ELi põllumajandustoetuste saajate nimed ja neile makstud toetussummad on proportsionaalne.

Märkides, et õigus isikuandmete kaitsele ei ole absoluutne põhimõte, leidis kohus, et kahest ELi põllumajandusfondist toetuse saajaid ja neile makstud

37 EL (2012), Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid, ELT C 326, 2012.

38 ELK, C-41/00 P, *Interporc Im- und Export GmbH vs. Euroopa Ühenduste Komisjon,* 6. märts 2003, punkt 39; ELK, C-28/08 P, *Euroopa Komisjon vs. Bavarian Lager Co. Ltd.,* 29. juuni 2010, punkt 54.

39 Nõukogu määrus (EÜ) nr 1290/2005, 21. juuni 2005, ühise põllumajanduspoliitika rahastamise kohta, ELT L 209, 2005; komisjoni määrus (EÜ) nr 259/2008, 18. märts 2008, milles sätestatakse nõukogu määruse (EÜ) nr 1290/2005 kohaldamise üksikasjalikud eeskirjad seoses Euroopa Põllumajanduse Tagatisfondi (EAGF) ja Maaelu Arengu Euroopa Põllumajandusfondi (EAFRD) vahenditest toetuse saajaid hõlmava teabe avaldamisega, ELT L 76, 2008.

40 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR (C-92/09) ja Hartmut Eifert (C-93/09) vs. Land Hessen*, 9. november 2010, punktid 47–52, 58, 66–67, 75, 86 ja 92.

täpseid summasid käsitlevate andmete avaldamisega veebilehel sekkutakse üldises plaanis toetusesaajate eraellu ning konkreetsemalt nende isikuandmete kaitsesse.

Kohus järeldas, et sellised põhiõiguste harta artiklites 7 ja 8 ette nähtud õiguste piirangud on ette nähtud seadusega ning vastavad ELi tunnustatud avalikku huvi pakkuvale eesmärgile, nimelt sealhulgas eesmärgile suurendada selgust ja arusaadavust ühenduse fondide kasutamisel. Sellegipoolest pidas ELK kahest ELi põllumajandusfondist toetust saavate füüsiliste isikute nimede ja neile makstud täpsete toetussummade avalikustamist ebaproportsionaalseks ning harta artikli 52 lõike 1 alusel õigustamatuks. Seega tunnistas kohus osaliselt kehtetuks asjaomaste ELi õigusaktide sätted, milles käsitleti Euroopa põllumajandusfondidest toetuse saajatega seotud teabe avaldamist.

1.2.3. Kunsti ja teaduse vabadus

Veel üks õigus, mida tuleb seoses õigusega eraelu austamisele ja isikuandmete kaitsele kaaluda, on kunsti ja teaduse vabadus, mille kaitsmisele viidatakse otsesõnu põhiõiguste harta artiklis 13. See õigus tuleneb peamiselt mõtte- ja sõnavabadusest ning selle teostamisel võetakse arvesse harta artiklit 1 („Inimväärikus"). Euroopa Inimõiguste Kohtu järgi on kunstivabaduse kaitse tagatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 10[41]. Harta artikliga 13 tagatud õiguse suhtes võidakse samal ajal kohaldada Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 10 lubatud piiranguid[42].

Näide: kohtuasjas *Vereinigung bildender Künstler vs. Austria*[43] käsitleti juhtumit, kus Austria kohtud keelasid kaebuse esitanud ühendusel eksponeerida maali, millel olid fotod eri avaliku elu tegelaste peadest kujutatud seksuaalaktides. Teosel fotol figureerinud Austria parlamendiliige pöördus kaebuse esitanud ühenduse vastu kohtusse ning taotles tõkendit, et maali enam ei eksponeeritaks. Siseriiklik kohus rahuldas tema taotluse ning seadis tõkendi. EIK toonitas, et selliste ideede puhul, mis solvavad, šokeerivad või häirivad riiki või mõnda elanikkonnarühma, kohaldatakse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 10. Kunstiteoseid loovad, esitavad, levitavad või

41 EIK, *Müller jt vs. Šveits*, nr 10737/84, 24. mai 1988.

42 Selgitused põhiõiguste harta kohta, ELT C 303, 2007.

43 EIK, *Vereinigung bildender Künstler vs. Austria*, nr 68345/01, 25. jaanuar 2007; vt eeskätt punktid 26 ja 34.

eksponeerivad isikud panustavad ideede ja arvamuste vahetamisse ning riik ei tohi nende väljendusvabadust üleliia piirata. Pidades silmas, et maal oli kollaažitehnikas, fotod olid üksnes asjaomaste isikute peadest ja kehad olid maalitud ebarealistlikult ja kunstilise liialdusega, millega ilmselgelt ei soovitud peegeldada tegelikku elu, isegi mitte vihjamisi, märkis EIK samuti, et on ebatõenäoline, et autori eesmärk oli jäljendada asjaomase isiku eraelu, vaid pigem soovis ta peegeldada tema avalikku seisust poliitikuna, ning et seda arvesse võttes peaks asjaomane isik üles näitama suuremat tolerantsust kriitika suhtes. Olles analüüsinud kaalul olnud eri huve, leidis EIK, et maali edasise eksponeerimise tähtajatu keeld oli ebaproportsionaalne. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 rikkumisega.

Euroopa andmekaitseõiguses tunnustatakse teaduse olulist rolli ühiskonnas. Seepärast on teadusega seotud eesmärkidel isikuandmete kasutamise üldpiirangud väiksemad. Nii andmekaitsedirektiivi kui ka konventsiooni nr 108 alusel on lubatud säilitada andmeid teaduslikel eesmärkidel ka siis, kui neid ei ole enam andmete kogumise esialgse otstarbe jaoks vaja. Peale selle ei peeta isikuandmete edasist kasutamist teadusuuringutes andmete kogumise esialgse eesmärgiga vastuolus olevaks. Üksikasjalikumad sätted määrab iga riik oma õiguses ise kindlaks, sealhulgas tagatised teadusuuringutest tuleneva huvi ühitamiseks õigusega isikuandmete kaitsele (vt ka jaotised 3.3.3 ja 8.4).

1.2.4. Omandi kaitse

Õigus omandi kaitsele on talletatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni esimese protokolli artiklis 1 ja põhiõiguste harta artikli 17 lõikes 1. Seoses õigusega omandile mängib olulist rolli intellektuaalomandi kaitse, millele on sõnaselgelt osutatud harta artikli 17 lõikes 2. ELi õiguskorras on mitu direktiivi, mille eesmärk on tagada intellektuaalomandi, eeskätt autoriõiguse tõhus kaitse. Intellektuaalomand hõlmab kirjandus- ja kunstiteoste kõrval ka patente, kaubamärke ja nendega seonduvaid õigusi.

Nagu on ilmnenud Euroopa Liidu Kohtu praktikast, tuleb põhiõigus omandi kaitsele viia tasakaalu teiste põhiõiguste kaitsega, eelkõige õigusega isikuandmete kaitsele[44]. On olnud juhtumeid, kus autoriõiguste kaitse asutused on nõudnud, et internetiteenuste osutajad avalikustaksid internetis failide jagamiseks ette nähtud platvormide kasutajate identiteedi. Selliste platvormide kaudu saavad internetikasu-

44 EIK, *Ashby Donald jt vs. Prantsusmaa,* nr 36769/08, 10. jaanuar 2013.

tajad tihtipeale tasuta alla laadida ka selliseid muusikapalasid, mis on autoriõigusega kaitstud.

Näide: kohtuasjas *Promusicae vs. Telefónica de España*[45] käsitleti juhtumit, kus üks Hispaania internetipakkuja (Telefónica) keeldus avaldamast Promusicaele (muusikaprodutsente ning heli- ja audiovisuaalsete salvestiste väljaandjaid koondav vabaühendus) isikuandmeid konkreetsete isikute kohta, kellele internetiteenuseid osutati. Promusicae taotles teabe avaldamist, et asjaomaste isikute vastu saaks algatada tsiviilmenetluse, sest vabaühenduse väitel kasutasid need isikud failivahetusprogrammi, mis võimaldas juurdepääsu fonogrammidele, mille varalised kasutusõigused kuulusid Promusicae liikmetele.

Hispaania kohus esitas küsimuse ELK-le, uurides, kas selliste isikuandmete edastamine tsiviilmenetluse raames on ühenduse õiguse alusel autoriõiguse tõhusa kaitse tagamiseks nõutav. Kohus viitas direktiividele 2000/31, 2001/29 ja 2004/48 koostoimes harta artiklitega 17 ja 47. ELK järeldas, et need kolm direktiivi, samuti eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv (direktiiv 2002/58/EÜ), ei välista liikmesriikide võimalust sätestada autoriõiguse tõhusa kaitse eesmärgil kohustust edastada tsiviilmenetluse raames isikuandmeid.

ELK rõhutas, et kohtuasi tõstatas seega küsimuse, kuidas saavutada vajalik kooskõla nõuete vahel, mis puudutavad selliste erinevate põhiõiguste kaitset nagu õigus eraelu puutumatusele ja õigus omandiõiguse kaitsele ning õigus tõhusale õiguskaitsele.

Kohus järeldas, et liikmesriigid peavad „eespool mainitud direktiivide ülevõtmisel jälgima, et nad tugineksid nende direktiivide sellisele tõlgendusele, mis võimaldab tagada tasakaalu erinevate ühenduse õiguskorras kaitstud põhiõiguste vahel. Järgmiseks, liikmesriikide ametiasutused ja kohtud ei pea nende direktiivide ülevõtmismeetmete rakendamisel mitte ainult tõlgendama oma siseriiklikku õigust kooskõlas nende direktiividega, vaid nad peavad ka jälgima, et nad ei tugineks asjaomaste direktiivide sellisele tõlgendusele, mis on vastuolus nende põhiõigustega või muude ühenduse õiguse üldpõhimõtetega, näiteks proportsionaalsuse põhimõttega"[46].

45 ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 29. jaanuar 2008, punktid 54 ja 60.

46 *Ibid.*, punktid 65 ja 68; vt ka ELK, C-360/10, *SABAM vs. Netlog N.V.*, 16. veebruar 2012.

2

Andmekaitseterminid

EL	Käsitletavad teemad	Euroopa Nõukogu
Isikuandmed		
Andmekaitsedirektiivi artikli 2 punkt a ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) vs. Land Hessen*, 9. november 2010 ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 29. jaanuar 2008	Õiguslik määratlus	Konventsiooni nr 108 artikli 2 punkt a EIK, *Bernh Larsen Holding AS jt vs. Norra*, nr 24117/08, 14. märts 2013
Andmekaitsedirektiivi artikli 8 lõige 1 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003	Isikuandmete eriliigid (tundlikud andmed)	Konventsiooni nr 108 artikkel 6
Andmekaitsedirektiivi artikli 6 lõike 1 punkt e	Anonüümseks muudetud ja pseudonüümi all esitatud andmed	Konventsiooni nr 108 artikli 5 punkt e Konventsiooni nr 108 seletuskiri, artikkel 42
Andmetöötlus		
Andmekaitsedirektiivi artikli 2 punkt b ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003	Mõisted	Konventsiooni nr 108 artikli 2 punkt c
Andmete kasutajad		
Andmekaitsedirektiivi artikli 2 punkt d	Vastutav töötleja	Konventsiooni nr 108 artikli 2 punkt d Profiilide koostamist käsitleva soovituse artikli 1 punkt g*

EL	Käsitletavad teemad	Euroopa Nõukogu
Andmekaitsedirektiivi artikli 2 punkt e ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003	**Volitatud töötleja**	Profiilide koostamist käsitleva soovituse artikli 1 punkt h*
Andmekaitsedirektiivi artikli 2 punkt g	**Vastuvõtja**	Konventsiooni nr 108 lisaprotokolli artikli 2 lõige 1
Andmekaitsedirektiivi artikli 2 punkt f	**Kolmas isik**	
Nõusolek		
Andmekaitsedirektiivi artikli 2 punkt h ELK, C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 5. mai 2011	**Kehtiva nõusoleku mõiste ja nõuded**	Meditsiiniliste andmete kaitset käsitleva soovituse artikkel 6 ja muud hilisemad soovitused

Märkus: **Euroopa Nõukogu ministrite komitee (2010), soovitus Rec(2010)13 liikmesriikidele üksikisikute kaitse kohta isikuandmete automaattöötlusel profiilide koostamise kontekstis (*profiilide koostamist käsitlev soovitus*), 23. november 2010.*

2.1. Isikuandmed

Põhipunktid

- Isikuandmetega on tegu juhul, kui andmed on seotud tuvastatud või vähemalt tuvastatava isikuga, st andmesubjektiga.
- Isik on tuvastatav, kui tema kohta on võimalik ilma ülemääraste jõupingutusteta saada lisateavet, mille alusel saab ta tuvastada.
- Autentimisega tõendatakse isiku identiteeti ja/või seda, et tal on luba mingeid kindlaid toiminguid teha.
- Teatavat liiki andmete, st tundlike andmete puhul, mis on loetletud konventsioonis nr 108 ja andmekaitsedirektiivis, on nõutav tugevdatud kaitse ning seega kehtib nende suhtes spetsiaalne õiguskord.
- Andmed on anonüümseks muudetud siis, kui need ei sisalda tuvastamist võimaldavaid tunnuseid; pseudonüümi all esitatakse andmed juhul, kui need tunnused on krüptitud.
- Erinevalt anonüümseks muudetud andmetest on pseudonüümi all esitatavate andmete puhul tegemist isikuandmetega.

2.1.1. Isikuandmete mõiste põhiaspektid

Nii **ELi** kui ka **Euroopa Nõukogu õiguses** mõistetakse isikuandmete all teavet tuvastatud või tuvastatava füüsilise isiku kohta,[47] st teavet inimese kohta, kelle identiteedi saab otseselt või lisateabe alusel kaudselt tuvastada.

Kui sellise isiku kohta töödeldakse andmeid, nimetatakse teda andmesubjektiks.

Isik

Õigus isikuandmete kaitsele põhineb õigusel eraelu austamisele. Eraelu mõiste seostub inimestega. Seega on andmekaitse suunatud peamiselt füüsilistele isikutele. Peale selle on andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamuse kohaselt Euroopa andmekaitseõiguses kaitse tagatud üksnes *elusolendile*[48].

EIK kohtupraktika seoses Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 näitab, et eraelu ja kutsetegevuse küsimuste eristamine võib osutuda keerukaks[49].

Näide: kohtuasjas *Amann vs. Šveits*[50] olid ametivõimud pealt kuulanud kaebuse esitajale tehtud äriteemalist telefonikõnet. Selle kõne alusel uurisid ametivõimud kaebuse esitaja tausta ning lisasid tema andmed riiklikusse turvakaartide registrisse. Kuigi pealt kuulati äriküsimustega seotud telefonikõnet, leidis EIK, et selle telefonikõne kohta säilitatud andmed olid seotud kaebuse esitaja eraeluga. Kohus juhtis tähelepanu asjaolule, et terminit „eraelu" ei tohiks tõlgendada kitsendavalt, pidades eeskätt silmas, et eraelu austamisega kaasneb õigus luua ja arendada suhteid kaasinimestega. Samuti ei olnud ühtki põhimõttelist põhjust, mis välistanuks termini „eraelu" mõiste hulgast kutsealase või äritegevuse. Sedalaadi lai tõlgendus vastas konventsiooni nr 108 puhul kasutatud tõlgendusele. EIK märkis ka, et kaebuse esitaja juhtumi puhul ei olnud sekkumine seadusega kooskõlas, kuna Šveitsi õigusaktides ei olnud kehtestatud üksikasjalikke erieeskirju teabe kogumise, salvestamise ja säilitamise kohta. Kohus järeldas,

47 Andmekaitsedirektiivi artikli 2 punkt a, konventsiooni nr 108 artikli 2 punkt a.

48 Andmekaitsedirektiivi artikli 29 alusel loodud töörühm, 2007, arvamus 4/2007 andmekaitse mõiste kohta, WP 136, 20. juuni 2007, lk 22.

49 Vt nt EIK, *Rotaru vs. Rumeenia [suurkoda]*, nr 28341/95, 4. mai 2000, punkt 43; EIK, *Niemitz vs. Saksamaa*, nr 13710/88, 16. detsember 1992, punkt 29.

50 EIK, *Amann vs. Šveits [suurkoda]*, nr 27798/95, 16. veebruar 2000, punkt 65.

et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Kui andmekaitse võib olla tagatud ka kutsetegevuse küsimustes, tekib küsimus, miks peaks kaitse hõlmama üksnes füüsilisi isikuid. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga ette nähtud õigused ei kehti ainuüksi füüsiliste isikute, vaid kõigi suhtes.

EIK kohtupraktikast võib välja tuua otsuse hagiavalduse kohta, milles juriidilised isikud väitsid, et nende puhul on rikutud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 ette nähtud õigust kaitsele andmete kasutamise vastu. Kohus aga lähtus selle juhtumi analüüsimisel õigusest kodu ja korrespondentsi austamisele, mitte õigusest eraelu austamisele.

Näide: kohtuasjas *Bernh Larsen Holding AS jt vs. Norra*[51] käsitleti kolme Norra ettevõtja kaebust maksuhalduri otsuse suhtes, mille alusel paluti neil esitada maksuaudiitoritele koopia kõikidest nende ühises kasutuses olnud serverarvutis sisaldunud andmetest.

EIK leidis, et kaebuse esitanud ettevõtjatele sellise kohustuse määramisega riivati nende õigusi seoses kodu ja korrespondentsi austamisega Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses. Samal ajal leidis kohus, et maksuasutustel olid väärkasutamise ärahoidmiseks paigas tõhusad ja piisavad kaitsemeetmed: kaebuse esitajaid teavitati aegsasti ette; nad viibisid kohapealse kontrolli juures ning neil oli võimalus ametnikega suhelda; materjal plaaniti pärast maksuauditi lõpetamist hävitada. Seda silmas pidades oli olemas õiglane tasakaal seoses ühelt poolt kaebuse esitanud ettevõtjate õigusega kodu ja korrespondentsi austamisele ning nende heaks töötavate inimeste eraelu puutumatuse kaitsmise huviga ja teiselt poolt avaliku huviga tagada tõhus kontroll maksuotsuse tegemiseks. Kohus otsustas, et tegu ei olnud seega artikli 8 rikkumisega.

Konventsiooni nr 108 kohaselt hõlmab andmekaitse peamiselt füüsiliste isikute andmete kaitset, kuid konventsiooniosalised võivad seda oma siseriiklikes õigusaktides laiendada juriidilistele isikutele, näiteks äriühingutele ja ühendustele. **ELi andmekaitseõigusega** üldiselt ei ole juriidilistele isikutele ette nähtud kaitset nende

51 EIK, *Bernh Larsen Holding AS jt vs. Norra*, nr 24117/08, 14. märts 2013. Vt ka EIK, *Liberty jt vs. Ühendkuningriik*, nr 58243/00, 1. juuli 2008.

kohta käivate andmete töötlemisel. Liikmesriikide seadusandjatel on aga vaba voli asjaomased sätted kehtestada[52].

Näide: kohtuasjas *Volker und Markus Schecke, Hartmut Eifert vs. Land Hessen*[53] leidis Euroopa Liidu Kohus põllumajandustoetuste saajate isikuandmete avaldamisele viidates, et „juriidilised isikud [saavad] sellise tuvastamise vastu harta artiklitele 7 ja 8 tugineda ainult siis, kui juriidilise isiku ametliku nime kaudu on võimalik tuvastada üks või mitu füüsilist isikut. [...H]arta artiklitega 7 ja 8 tunnustatud õigus eraelu puutumatusele isikuandmete töötlemisel [puudutab] igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta[...]"[54].

Isiku tuvastatavus

Nii **ELi** kui ka **Euroopa Nõukogu õiguses** hõlmab teave isikuandmeid juhul, kui:

- selles teabes tuvastatakse isik;
- üksikisikut, kes ei ole küll tuvastatud, kirjeldatakse kõnealuses teabes nii, et selle alusel saab lisauurimise abil välja selgitada andmesubjekti.

Mõlemat liiki teavet kaitstakse Euroopa andmekaitseõiguses samamoodi. EIK on korduvalt märkinud, et termini „isikuandmed" mõiste on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni puhul sama mis konventsioonis nr 108, eeskätt kattub neis tingimus, et andmed peavad olema seotud tuvastatud või tuvastatava isikuga[55].

Isikuandmete õiguslikes määratlustes ei täpsustata, millal loetakse isik tuvastatuks[56]. Tuvastamiseks peavad andmed sisaldama tunnuseid, mis kirjeldavad isikut nii, et ta eristub kõikidest teistest inimestest ning on üksikisikuna äratuntav. Selliste kirjeldavate tunnuste seas on esikohal isiku nimi. Teatavatel erijuhtudel võivad isikut

52 Andmekaitsedirektiivi 24. põhjendus.

53 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, 9. november 2010, punkt 53.

54 *Ibid.*, punkt 52.

55 EIK, *Amann vs. Šveits [suurkoda]*, nr 27798/95, 16. veebruar 2000, punkt 65 jt.

56 Vt ka EIK, *Odièvre vs. Prantsusmaa [suurkoda]*, nr 42326/98, 13. veebruar 2003; EIK, *Godelli vs. Itaalia*, nr 33783/09, 25. september 2012.

nime kõrval sarnasel viisil reeta ka muud tunnused. Näiteks võib avaliku elu tegelaste puhul piisata viitest isiku ametiseisundile (Euroopa Komisjoni president).

> Näide: kohtuasjas *Promusicae*[57] märkis Euroopa Liidu Kohus, et „[...] on vaieldamatu, et teatavate [konkreetse internetis failide jagamiseks kasutatava platvormi] kasutajate nimede ja aadresside edastamine, mida Promusicae taotles, tähendab, et käsutusse antakse isikuandmed, st teave tuvastatud või tuvastatava füüsilise isiku kohta vastavalt direktiivi 95/46 artikli 2 punktis a olevale määratlusele [...]. Sellise teabe edastamine, mida Telefónica Promusicae sõnul salvestab – mida Telefónica ei vaidlusta –, kujutab endast isikuandmete töötlemist direktiivi 2002/58 artikli 2 esimese lõigu tähenduses koosmõjus direktiivi 95/46 artikli 2 punktiga b".

Kuna paljud nimed ei ole kordumatud, võib isiku identiteedi kinnitamiseks vaja minna lisatunnuseid, et teda mitte kellegi teisega segi ajada. Sel puhul kasutatakse tihtipeale sünnikuupäeva ja -kohta. Peale selle on kodanike eristamise tõhustamiseks mitmes riigis kehtestatud isikukoodide süsteem. Tänapäeva tehnoloogiaajastul mängivad isikute tuvastamisel üha suuremat rolli biomeetrilised andmed, näiteks sõrmejäljekujutised, digitaalfotod ja silmaiirisekujutised.

Euroopa andmekaitseõiguse kohaldatavust silmas pidades aga ei ole andmesubjekti tuvastamiseks vaja kõrgema taseme tunnuseid; piisab sellest, kui asjaomane isik on tuvastatav. Isik on tuvastatav siis, kui teave sisaldab tunnuseid, mille alusel saab isiku otseselt või kaudselt tuvastada[58]. Andmekaitsedirektiivi 26. põhjenduse kohaselt tuleb arvesse võtta, kas teabe eeldatavate kasutajate jaoks on tõenäoliselt kättesaadavad mõistlikud vahendid isiku tuvastamiseks ning kas nad neid kasutavad; see hõlmab kolmandatest isikutest andmete vastuvõtjaid (vt jaotis 2.3.2).

> Näide: kohalik asutus otsustab hakata koguma andmeid kohalikel teedel kiirust ületavatest sõidukitest. Sõidukitest tehakse fotod, salvestades automaatselt aja ja asukoha, et anda need andmed üle pädevale asutusele kiirusepiirangut eiranud juhtide trahvimiseks. Üks andmesubjekt esitab kaebuse, väites, et kohalikul asutusel ei ole andmekaitseõiguse kohaselt õiguslikku alust selliste andmete kogumiseks. Kohalik asutus jääb seisukohale, et tegemist ei ole isikuandmete

57 ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 29. jaanuar 2008, punkt 45.

58 Andmekaitsedirektiivi artikli 2 punkt a.

kogumisega. Sõidukite registreerimismärgid on nende väitel andmed anonüümsete isikute kohta. Kohalikul asutusel ei ole seaduslikku juurdepääsu sõidukite üldregistrile, et kindlaks teha sõiduki omaniku või juhi identiteet.

Selline mõttekäik ei ole kooskõlas andmekaitsedirektiivi 26. põhjendusega. Pidades silmas, et andmete kogumise eesmärk on ilmselgelt kiiruseületajate kindlakstegemine ja trahvimine, võib eeldada, et selle jaoks üritatakse tuvastada isikuid. Kuigi kohalikel asutustel ei ole võimalust isikuid otseselt tuvastada, edastavad nad andmed pädevale asutusele, st politseile, kellel see võimalus on. 26. põhjendus hõlmab sõnaselgelt ka stsenaariumi, mille puhul võib arvata, et üksikisikut võivad andmete esmase kasutaja kõrval üritada tuvastada teised andmete vastuvõtjad. 26. põhjenduse kontekstis on kohaliku asutuse tegevus andmete kogumine tuvastatavate isikute kohta ning nõuab seega andmekaitseõigusega kooskõlas olevat õiguslikku alust.

Euroopa Nõukogu õiguses mõistetakse tuvastatavust sarnasel viisil. Näiteks makseandmeid käsitleva soovituse[59] artikli 1 lõikes 2 sätestatakse, et isikut ei loeta tuvastatavaks juhul, kui tuvastamine nõuab liiga palju aega, raha või tööjõudu.

Autentimine

Autentimisega kinnitab isik väidetavat identiteeti ja/või seda, et tal on õigus teatavaid toiminguid teha, näiteks turvaalale siseneda või pangakontolt raha välja võtta. Autentimine võib toimuda järgmistel viisidel: biomeetriliste andmete võrdlus, näiteks passifoto või sõrmejälgede võrdlemine selle isiku andmetega, kelle inimene väidab end olevat, näiteks sisserändekontrollis; sellise teabe küsimine, mida saab teada vaid teatava identiteedi või volitusega isik, näiteks isikukood või salasõna; konkreetse eseme esitamise nõudmine, mis peaks olema üksnes teatava identiteedi või volitusega isiku valduses, näiteks kiipkaart või pangaseifi võti. Peale salasõna või kiipkaardi on elektroonilises suhtluses eriti tõhus isikutuvastus- ja autentimisvahend elektrooniline allkiri, mõnikord koosluses isikukoodiga.

Andmete laad

Isikuandmete alla kuulub igasugune teave, mis on seotud teatava isikuga.

59 Euroopa Nõukogu ministrite komitee (1990), soovitus Rec(90) 19 maksete tegemisel ja muudes toimingutes kasutatavate isikuandmete kaitse kohta, 13. september 1990.

Näide: töötaja töötulemuste hinnang ülemuselt, mida säilitatakse töötaja isikutoimikus, kuulub töötaja isikuandmete alla, isegi kui selle sisu moodustab kas osaliselt või täies ulatuses üksnes ülemuse isiklik arvamus, näiteks „töötaja ei pühendu oma tööle", mitte faktid, näiteks „töötaja puudus viimase kuue kuu jooksul töölt viis nädalat".

Isikuandmete alla kuulub teave nii isiku eraelu kui ka kutsealase tegevuse ja seltskonnaelu kohta.

Amanni[60] kohtuasjas leidis EIK, et termini „isikuandmed" tähendus ei piirdu ainuüksi üksikisiku eraelu küsimustega (vt jaotis 2.1.1). Selline termini „isikuandmed" määratlus on asjakohane ka andmekaitsedirektiivi seisukohast.

Näide: kohtuasjas *Volker und Markus Schecke, Hartmut Eifert vs. Land Hessen*[61] märkis ELK: „Selles suhtes ei ole tähtsust asjaolul, et avaldatud andmed seonduvad kutsealase tegevusega [...]. Euroopa Inimõiguste Kohus on EIÕK artikli 8 tõlgendamisel sellega seoses otsustanud, et mõistet „eraelu" ei tuleks tõlgendada kitsalt ning et „ei ole ühtki põhimõttelist põhjust, mis välistaks „eraelu" mõiste hulgast kutsealase [...] tegevuse"[...]".

Andmed on isikuga seotud ka juhul, kui teabest selguvad kaudselt üksikasjad teatava inimese kohta. Mõnikord võidakse isikuandmetena käsitada ka teavet eseme või sündmuse kohta, juhul kui asjaomane ese või sündmus (nt mobiiltelefon, auto, õnnetus) on isikuga (nt eseme omanik, kasutaja, õnnetuses kannatanu) tihedalt seotud.

Näide: kohtuasjas *Uzun vs. Saksamaa*[62] käsitleti juhtumit, kus kaebuse esitajat ja üht teist meesterahvast hakati viimase autosse paigaldatud GPS-seadme abil jälgima, kuna neid kahtlustati pommirünnakutes osalemises. EIK leidis, et kaebuse esitaja jälgimisega GPSi kaudu sekkuti tema õigusesse eraelu austamisele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses. Jälgimine GPSi kaudu oli aga õigusaktidega kooskõlas, samuti vastas see mitme mõrvakatsejuhtumi uurimise õiguspärasele eesmärgile ning oli seega demokraatliku ühiskonna seisukohast vajalik. Kohus järeldas, et tegu

60 Vt EIK, *Amann vs. Šveits*, nr 27798/95, 16. veebruar 2000, punkt 65.

61 Liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen*, 9. november 2010, punkt 59.

62 EIK, *Uzun vs. Saksamaa*, nr 35623/05, 2. september 2010.

ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Andmete esitusviis

Andmekaitseõiguse kohaldatavuse seisukohast ei ole oluline, millisel kujul isikuandmeid säilitatakse või kasutatakse. Isikuandmeid võivad sisaldada nii kirjalik ja suuline suhtlus kui ka kujutised,[63] sealhulgas videovalve-[64] või helisalvestised[65]. Samuti võib isikuandmete alla kuuluda elektrooniliselt salvestatud teave ning paberkandjal esitatud teave, isegi inimkoest võetud rakuproovid, kuna nendega registreeritakse inimese DNA.

2.1.2. Isikuandmete eriliigid

Nii **ELi** kui ka **Euroopa Nõukogu õiguses** on teatavat liiki isikuandmeid, mille laadist tulenevalt võidakse nende töötlemise korral andmesubjekt ohtu seada ning mis seega vajavad tugevdatud kaitset. Selliste eriliiki andmete (nn tundlikud andmed) töötlemine peab seega olema lubatud üksnes konkreetsete kaitsemeetmete rakendamisel.

Tundlike andmete määratluses osutatakse nii konventsioonis nr 108 (artikkel 6) kui ka andmekaitsedirektiivis (artikkel 8) järgmistele kategooriatele:

- isikuandmed, mis paljastavad rassilise või etnilise päritolu;
- isikuandmed, mis paljastavad poliitilised vaated, usulised või muud veendumused;
- isikuandmed, mis käsitlevad tervislikku seisundit või seksuaalelu.

Näide: *Bodil Lindqvisti*[66] kohtuasjas märkis ELK, et „osutamine asjaolule, et isik vigastas oma jalga ja töötab haiguspuhkusel olles osalise tööajaga, sisaldab

63 EIK, *Von Hannover vs. Saksamaa*, nr 59320/00, 24. juuni 2004; EIK, *Sciacca vs. Itaalia*, nr 50774/99, 11. jaanuar 2005.

64 EIK, *Peck vs. Ühendkuningriik*, nr 44647/98, 28. jaanuar 2003; EIK, *Köpke vs. Saksamaa*, nr 420/07, 5. oktoober 2010.

65 Andmekaitsedirektiivi 16. ja 17. põhjendus; EIK, *P.G. ja J.H. vs. Ühendkuningriik*, nr 44787/98, 25. septemer 2001, punktid 59 ja 60; EIK, *Wisse vs. Prantsusmaa,* nr 71611/01, 20. detsember 2005.

66 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003, punkt 51.

tervislikku seisundit käsitlevaid isikuandmeid direktiivi 95/46 artikli 8 lõike 1 tähenduses".

Andmekaitsedirektiivi kohaselt kuuluvad tundlike andmete alla andmed, mis paljastavad ametiühingusse kuulumise, sest need võivad olulisel määral viidata inimese poliitilistele vaadetele või kuuluvusele.

Konventsiooni nr 108 kohaselt on tundlikud ka süüdimõistvaid otsuseid käsitlevad andmed.

Andmekaitsedirektiivi artikli 8 lõikes 7 antakse ELi liikmesriikidele volitus määrata „kindlaks tingimused, mille kohaselt võib töödelda siseriiklikku isikukoodi või muud üldkasutatavat tunnust".

2.1.3. Anonüümseks muudetud ja pseudonüümi all esitatud andmed

Kooskõlas põhimõttega, mille kohaselt ei tohi andmeid säilitada kauem kui asjaomase eesmärgi jaoks vajalik, mis on sätestatud nii andmekaitsedirektiivis kui ka konventsioonis nr 108 (täpsemalt on seda küsimust käsitletud 3 peatukis), tuleb andmeid säilitada „kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega"[67]. Kui vastutav töötleja tahab andmeid säilitada pärast nende aegumist ja nende kogumise esialgse eesmärgi täitmist, peab ta kõnealused andmed sellest tulenevalt anonüümseks muutma.

Anonüümseks muudetud andmed

Andmed on anonüümseks muudetud, kui teatavast isikuandmete kogumist on eemaldatud kõik tuvastamist võimaldavad tunnused. Teave ei tohi sisaldada ühtki tunnust, mille alusel võiks asjaomase(d) isiku(d) mõistlike jõupingutustega uuesti tuvastada[68]. Kui andmed on õnnestunud anonüümseks muuta, ei ole need enam isikuandmed.

Kui andmeid ei ole enam esialgse eesmärgi jaoks vaja, kuid neid tuleb personaliseeritud kujul säilitada kasutamiseks seoses ajaloo, statistika või teadusega, on see

67 Andmekaitsedirektiivi artikli 6 lõike 1 punkt e, konventsiooni nr 108 artikli 5 punkt e.

68 *Ibid.*, 26. põhjendus.

andmekaitsedirektiivi ja konventsiooni nr 108 alusel lubatud, tingimusel, et rakendatakse vajalikke tagatisi andmete väärkasutamise ärahoidmiseks[69].

Pseudonüümi all esitatud andmed

Isikuandmed sisaldavad isiku tuvastamist võimaldavaid tunnuseid, näiteks nimi, sünnikuupäev, sugu ja aadress. Kui isikuandmed esitatakse pseudonüümi all, asendatakse tunnused ühtse pseudonüümiga. Selle saavutamiseks on võimalik näiteks isikuandmetes sisalduvad tunnused krüpteerida.

Konventsioonis nr 108 ja andmekaitsedirektiivis esitatud õiguslikes määratlustes ei ole pseudonüümi all esitatud andmeid otseselt käsitletud. Konventsiooni nr 108 seletuskirja artiklis 42 aga sätestatakse, et isiku nime järgi tuvastamist võimaldavate andmete säilitamise tähtaegu käsitlev nõue ei tähenda, et andmetest tuleks teatava aja pärast lõplikult eemaldada asjaomase isiku nimi, vaid üksnes seda, et andmed ja tunnused ei tohiks olla hõlpsasti seostatavad. Sel eesmärgil saab andmed esitada pseudonüümi all. Ilma krüptovõtmeta onpseudonüümi all esitatud andmed raskelt tuvastatavad. Siiski püsib andmetes pseudonüümi ja krüptovõtme kombinatsiooni puhul teatav seos identiteediga. Isikutel, kellel on õigus krüptovõtit kasutada, on võimalus isik uuesti lihtsalt tuvastada. Seepärast tuleb iseäranis hoolsalt jälgida, et krüptovõtmeid ei saaks kasutada isikud, kellel ei ole selleks luba.

Kuna andmete esitamine pseudonüümi all on üldises plaanis üks olulisematest andmekaitse tagamise vahenditest, pidades silmas, et isikuandmete kasutamist ei saa alati täielikult välistada, tuleb selliste toimingute loogikat ja tagajärgi selgitada üksikasjalikumalt.

Näide: lause „Charles Spencer, sündinud 3. aprillil 1967, on nelja lapse (kahe poisi ja kahe tüdruku) isa" saab pseudonüümi all esitada näiteks järgmistel viisidel:

„C.S. 1967 on nelja lapse (kahe poisi ja kahe tüdruku) isa";

„324 on nelja lapse (kahe poisi ja kahe tüdruku) isa";

„YESz320l on nelja lapse (kahe poisi ja kahe tüdruku) isa".

69 *Ibid.*, andmekaitsedirektiivi artikli 6 lõike 1 punkt e, konventsiooni nr 108 artikli 5 punkt e.

Kasutajad, kes neid pseudonüümi all esitatud andmetele juurde pääsevad, ei saa üldjuhul tunnustest „324" või „YESz3201" tuletada tunnust „Charles Spencer, sündinud 3. aprillil 1967". Seega on pseudonüümi all esitatud andmed väärkasutamise eest tõenäoliselt paremini kaitstud.

Esimese näite puhul ei ole aga kaitse nii tõhus kui teiste puhul. Kui lauset „C.S. 1967 on nelja lapse (kahe poisi ja kahe tüdruku) isa" kasutatakse Charles Spenceri kodukülas, on härra Spencer hõlpsasti äratuntav. Viis, kuidas andmed pseudonüümi all esitatakse, mõjutab andmekaitse tõhusust.

Krüptitud tunnustega isikuandmeid kasutatakse isikute identiteedi salajas hoidmiseks mitmesugustes tingimustes. Eriti kasulik on see olukorras, kus vastutavad töötlejad peavad tagama, et nad käsitlevad samade andmesubjektide andmeid, kuid neil ei ole vaja teada või nad ei tohi teada andmesubjektide tegelikku identiteeti. See kehtib näiteks juhul, kui uurija analüüsib patsientide haiguskulgu ning patsientide identiteet on teada üksnes haiglale, kus neid ravitakse ning kust uurija asjaomased pseudonüümi all esitatud haiguslood sai. Isikuandmete esitamine pseudonüümi all on seega oluline lüli eraelu puutumatuse tugevdamiseks välja töötatud tehnoloogias. Samuti võib see olulist rolli mängida lõimitud eraelukaitse rakendamisel. Lõimitud eraelukaitse tähendab, et andmekaitse lõimitakse kõrgetasemelistesse andmetöötlussüsteemidesse juba nende kavandamisel.

2.2. Andmetöötlus

Põhipunktid

- Termin „töötlemine" viitab peamiselt automaatsele töötlemisele.
- ELi õiguses hõlmab termini „töötlemine" mõiste ka automatiseerimata töötlemist korrastatud kataloogides.
- Euroopa Nõukogu õiguses võivad riigid termini „töötlemine" mõistet oma õigusaktides laiendada automatiseerimata töötlemisele.

Konventsioonis nr 108 ja andmekaitsedirektiivis on andmekaitse peamiselt suunatud andmete automaatsele töötlemisele.

Euroopa Nõukogu õiguses selgub automaatse töötlemise määratlusest, et automaattoimingute vahepeal võidakse andmeid vajaduse korral käsitleda ka

automatiseerimata viisil. Nii on ka **ELi õiguses** andmete automaatne töötlemine määratletud kui isikuandmetega tehtavad toimingud, mis on kas täielikult või osaliselt automatiseeritud[70].

> Näide: *Bodil Lindqvisti*[71] kohtuasjas leidis ELK:
>
> „[...]toiming, mis seisneb veebilehel erinevatele isikutele osutamises ja nende individualiseerimises kas nime või muude vahendite, näiteks telefoninumbri või nende töötingimusi ja vaba aja harrastusi puudutava teabe alusel, on „isikuandmete täielikult või osaliselt automatiseeritud töötlemine" direktiivi 95/46 artikli 3 lõike 1 tähenduses."

Ka automatiseerimata andmetöötluse puhul tuleb tagada andmekaitse.

ELi õiguses ei ole andmekaitse mingil viisil piiratud üksnes automaatse andmetöötlusega. Sellest tulenevalt kehtib andmekaitse nõue ELi õiguses isikuandmete töötlemisele automatiseerimata kataloogis, st spetsiaalselt korrastatud andmekogumis[72]. Andmekaitse põhimõte laieneb sellisele andmetöötlusele järgmistel põhjustel:

- paberkandjaid on võimalik korrastada nii, et teavet saab üles leida kiiresti ja hõlpsalt;

- isikuandmete säilitamisel korrastatud paberkandjatel on lihtne kõrvale hiilida õigusaktides automaatse andmetöötluse suhtes sätestatud piirangutest[73].

Euroopa Nõukogu õiguses reguleeritakse konventsiooniga nr 108 peamiselt andmetöötlust automatiseeritud andmekogudes[74]. Samal ajal on konventsioonis ette nähtud võimalus, et riigid laiendavad kaitset oma siseriiklikes õigusaktides ka automatiseerimata töötlusele. Paljud konventsiooniosalised on seda võimalust kasutanud ning esitanud Euroopa Nõukogu peasekretärile asjakohased deklaratsioonid[75]. Andmekaitse põhimõtte laiendamine sedalaadi deklaratsiooni alusel peab hõlmama

70 Konventsiooni nr 108 artikli 2 punkt c; andmekaitsedirektiivi artikli 2 punkt b ja artikli 3 lõige 1.

71 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003, punkt 27.

72 Andmekaitsedirektiivi artikli 3 lõige 1.

73 *Ibid.*, 27. põhjendus.

74 Konventsiooni nr 108 artikli 2 punkt b.

75 Vt konventsiooni nr 108 artikli 3 lõike 2 punkti c alusel esitatud deklaratsioonid.

kõiki andmete automatiseerimata töötlemise vorme, mitte piirduma vaid andmete töötlemisega automatiseerimata kataloogides[76].

Hõlmatud andmetöötlustoimingute laadi silmas pidades on töötlemise mõiste **nii ELi kui ka Euroopa Nõukogu õiguses** laiahaardeline: „isikuandmete töötlemine [...] – iga isikuandmetega tehtav toiming [...], olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine"[77]. Termini „töötlemine" mõiste hõlmab ka toiminguid, mille puhul andmed loovutatakse ühelt vastutavalt töötlejalt teisele vastutavale töötlejale.

Näide: tööandjad koguvad ja töötlevad andmeid oma töötajate kohta, sealhulgas teavet palga kohta. Selliste toimingute õiguslik alus tuleneb töölepingust.

Tööandjad peavad oma töötajaskonna palgaandmed edastama maksuhaldurile. Ka selline andmete edastamine kuulub konventsiooni nr 108 ja andmekaitsedirektiivi tähenduses andmetöötluse alla. Palgaandmete avaldamise õiguslik alus ei seisne aga töölepingus. Töötlemistoiminguteks, mille puhul tööandja saadab maksuhaldurile palgaandmed, peab olema täiendav õiguslik alus. Tavaliselt on see ette nähtud riigi tasandi maksuõigusnormidega. Kui selliseid õigusnorme ei kohaldataks, loetaks kõnealuste andmete edastamine ebaseaduslikuks töötlemiseks.

2.3. Isikuandmete kasutajad

Põhipunktid

- Isik või üksus, kes otsustab töödelda teiste inimeste isikuandmeid, on andmekaitseõiguse seisukohalt vastutav töötleja; kui see otsus tehakse kollektiivselt, nimetatakse asjaomaseid isikuid ühisteks vastutavateks töötlejateks.
- Volitatud töötleja on juriidiliselt eraldiseisev isik või üksus, kes töötleb isikuandmeid vastutava töötleja nimel.

76 Vt konventsiooni nr 108 artikli 3 lõike 2 sõnastus.

77 Andmekaitsedirektiivi artikli 2 punkt b. Vt selle kohta ka konventsiooni nr 108 artikli 2 punkt c.

- Kui volitatud töötleja kasutab andmeid vastutava töötleja juhtnööre eirates isiklikel eesmärkidel, saab temast vastutav töötleja.
- Isik, kellele vastutav töötleja andmeid avaldab, on vastuvõtja.
- Kolmas isik on füüsiline või juriidiline isik, kes ei tegutse vastutava töötleja juhtnööre järgides (ning kes ei ole andmesubjekt).
- Kolmandast isikust vastuvõtja on vastutavast töötlejast juriidiliselt eraldiseisev isik või üksus, kellele vastutav töötleja avaldab isikuandmeid.

2.3.1. Vastutavad töötlejad ja volitatud töötlejad

Olulisim aspekt, mis vastutava töötleja või volitatud töötleja ülesandega kaasneb, on õiguslik vastutus andmekaitseõigusega ette nähtud asjaomaste kohustuste täitmise eest. Neid ülesandeid saavad seega täita üksnes isikud, keda saab kohaldatava õiguse alusel vastutusele võtta. Erasektoris on selles rollis tavaliselt füüsiline või juriidiline isik, avalikus sektoris aga ametiasutus. Muud üksused, näiteks õigusvõimeta asutused või institutsioonid, võivad vastutavad töötlejad või volitatud töötlejad olla üksnes juhul, kui see on ette nähtud teatavate õigussätetega.

Näide: kui ettevõtte Päikesekiir turundusosakond plaanib hakata töötlema andmeid turu-uuringu jaoks, on andmete töötlemisel vastutav töötleja ettevõte Päikesekiir, mitte selle turundusosakond. Turundusosakond ei saa olla vastutav töötleja, kuna sellel ei ole eraldi õigusvõimet.

Ettevõtjate gruppides loetakse valdusettevõtja ja kõik sidusettevõtjad eraldi vastutavateks töötlejateks või volitatud töötlejateks, sest nad on kõik eraldi juriidilised isikud. Kuna ettevõtjad on juriidiliselt eraldiseisvad, on andmete vahetamiseks ühte gruppi kuuluvate ettevõtjate vahel vaja asjakohast õiguslikku alust. Ettevõtjate gruppi kuuluvatel eraldiseisvatel õigussubjektidel ei ole mingit eesõigust, mis võimaldaks neil vahetada isikuandmeid kui selliseid.

Selles kontekstis tuleb jutuks võtta eraisikute roll. **ELi õiguses** ei kuulu teisi isikuid käsitlevaid andmeid üksnes isiklikel või kodustel eesmärkidel töötlevad eraisikud andmekaitsedirektiivi eeskirjade kohaldamisalasse; neid ei loeta vastutavateks töötlejateks[78].

78 Andmekaitsedirektiivi 12. põhjendus ja artikli 3 lõike 2 viimane taane.

Väljakujunenud kohtupraktikas on aga leitud, et andmekaitseõiguse eeskirjade kohaldamisalasse kuulub vaatamata sellele olukord, kus eraisik avaldab teisi inimesi käsitlevaid andmeid internetis.

Näide: *Bodil Lindqvisti*[79] kohtuasjas märkis ELK:

„toiming, mis seisneb veebilehel erinevatele isikutele osutamises ja nende individualiseerimises kas nime või muude vahendite [...] alusel, on „isikuandmete täielikult või osaliselt automatiseeritud töötlemine" direktiivi 95/46 artikli 3 lõike 1 tähenduses"[80].

Sellisel juhul ei ole isikuandmete töötlemise puhul tegemist üksnes isiklikel või kodustel eesmärkidel tehtavate toimingutega, mis ei kuulu andmekaitsedirektiivi kohaldamisalasse, arvestades, et seda erandit tuleb „tõlgendada nii, et see puudutab ainult tegevust, mis mahub isiku era- või perekonnaelu raamidesse, nagu see ilmselgelt ei ole siis, kui isikuandmete töötlemine seisneb nende internetis avaldamises, nii et andmed on tehtud kättesaadavaks määratlemata isikute ringile"[81].

Vastutav töötleja

ELi õiguses on vastutav töötleja isik või üksus, „kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid"[82]. Vastutava töötleja otsus määrab kindlaks, miks ja kuidas andmeid töödeldakse. **Euroopa Nõukogu õiguses** hõlmab vastutava töötleja mõiste ka seda, et vastutav töötleja otsustab, milliseid isikuandmete kategooriaid säilitatakse[83].

Konventsioonis nr 108 viidatakse termini „vastutav töötleja" määratluses veel ühele vastutusega kaasnevale aspektile, mida tuleb arvesse võtta. Kõnealune määratlus viitab küsimusele, kellel on õigus töödelda teatavaid andmeid teataval eesmärgil. Olukordades, kus on väidetavalt aset leidnud ebaseaduslik töötlemine ning tuleb välja selgitada vastutav töötleja, käsitatakse vastutava töötlejana sellegipoolest seda isikut või üksust, näiteks ettevõtjat või ametiasutust, kes otsustas, et andmeid

79 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003.

80 *Ibid.*, punkt 27.

81 *Ibid.*, punkt 47.

82 Andmekaitsedirektiivi artikli 2 punkt d.

83 Konventsiooni nr 108 artikli 2 punkt d.

tuleks töödelda, hoolimata sellest, kas tal oli seadusjärgne õigus seda otsust teha või mitte[84]. Taotlusega andmed kustutada tuleb seega alati pöörduda *de facto* vastutava töötleja poole.

Ühine vastutus

Andmekaitsedirektiivis viitab termini „vastutav töötleja" määratlus sellele, et mõnikord võivad vastutava töötlejana tegutseda ka mitu juriidiliselt eraldiseisvat üksust üheskoos. See tähendab, et nad otsustavad koos töödelda andmeid ühisel eesmärgil[85]. Kooskõlas õigusaktidega on see aga võimalik üksnes siis, kui andmete ühisel eesmärgil töötlemiseks on eraldi konkreetne õiguslik alus.

Näide: tüüpiline näide ühisest vastutusest on mitme krediidiasutuse hallatav ebausaldusväärsete klientide andmebaas. Kui ühiste vastutavate töötlejate hulka kuuluv pank saab taotluse krediidiliini saamiseks, kontrollitakse andmebaasi, et teha taotleja krediidivõimelisuse suhtes teadlik otsus.

Eeskirjades ei ole otseselt kindlaks määratud, kas ühine vastutus tähendab, et vastutavatel töötlejatel peab olema sama ühine eesmärk, või piisab sellest, kui nende eesmärgid kattuvad vaid mingil määral. Euroopa tasandil ei ole selles küsimuses aga välja kujunenud kohtupraktikat ning samuti ei ole täielikult selge, millised tagajärjed vastutusega kaasnevad. Andmekaitsedirektiivi artikli 29 alusel loodud töörühm tõlgendab ühise vastutuse mõistet laiemalt, et võimaldada tänapäeva andmekaitsevaldkonna üha suurenevat keerukust silmas pidades teatavat paindlikkust[86]. Töörühma seisukohta illustreerib üks Ülemaailmse Pankadevahelise Finantstelekommunikatsiooni Ühinguga (SWIFT) seotud juhtum.

Näide: nn SWIFTi juhtumis palkasid Euroopa pangad SWIFTi haldama andmete edastamise protsessi pangatehingutes, esialgu volitatud töötlejana. SWIFT avaldas asjaomased Ameerika Ühendriikides asuvas andmetöötluskeskuses talletatud andmed pangatehingute kohta USA rahandusministeeriumile, kuigi ühingu palganud Euroopa pangad ei olnud sellist korraldust otseselt andnud. Andmekaitsedirektiivi artikli 29 alusel loodud andmekaitse töörühm järeldas kõnealuse

84 Vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 15.

85 Andmekaitsedirektiivi artikli 2 punkt d.

86 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 19.

olukorra õiguspärasust analüüsides, et nii SWIFTi palganud Euroopa pankasid kui ka SWIFTi tuli käsitada ühiste vastutavate töötlejatena, kes mõlemad vastutasid Euroopa klientide ees nende andmete avaldamise eest USA ametiasutustele[87]. Otsustades andmed avaldada, oli SWIFT õigusvastaselt astunud vastutava töötleja rolli; pangad aga ei suutnud ilmselgelt täita oma kohustust volitatud töötleja tegevust kontrollida ning seega ei saanud neid vastutava töötleja kohustustest täienisti vabastada. Selles juhtumis oli lõppkokkuvõttes tegemist ühise vastutusega.

Volitatud töötleja

ELi õiguses on volitatud töötleja isik või üksus, kes töötleb isikuandmeid vastutava töötleja nimel[88]. Volitatud töötlejale usaldatud toimingud võivad olla piiratud väga spetsiifilise ülesande või valdkonnaga või siis üsna üldist laadi ja laiahaardelised.

Euroopa Nõukogu õiguses käsitatakse volitatud töötleja mõistet samamoodi kui ELi õiguses.

Teiste nimel andmete töötlemise kõrval on volitatud töötlejad nende enda eesmärkidel toimuva andmetöötluse kontekstis ka ise vastutava töötleja rollis, nt oma töötajate, müügi ja raamatupidamise haldamisel.

Näide: ettevõte Alati Valmis pakub teistele ettevõtetele personaliandmete haldamise andmetöötlusteenust. Seda ülesannet täites on Alati Valmis volitatud töötleja.

Enda töötajate andmeid töödeldes on Alati Valmis aga vastutav töötleja seoses tema suhtes tööandjana kehtivate kohustuste täitmiseks tehtavate andmetöötlustoimingutega.

Vastutava töötleja ja volitatud töötleja seos

Nagu näha, on vastutav töötleja isik või üksus, kes määrab kindlaks töötlemise eesmärgid ja vahendid.

87 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 10/2006 SWIFT-võrgus isikuandmete töötlemise kohta, WP 128, Brüssel, 22. november 2006.

88 Andmekaitsedirektiivi artikli 2 punkt e.

Näide: ettevõtte Päikesekiir direktor otsustab tellida turuanalüüsile spetsialiseerunud ettevõttelt Kuukiir Päikesekiire kliendiandmete turuanalüüsi. Kuigi töötlemise vahendite kindlaksmääramine usaldatakse Kuukiirele, on vastutav töötleja Päikesekiir ning Kuukiir on üksnes volitatud töötleja, kuna lepingu järgi võib Kuukiir Päikesekiire kliendiandmeid kasutada üksnes Päikesekiire määratud eesmärkidel.

Kui volitatud töötlejale antakse õigus kindlaks määrata töötlemise vahendid, peab vastutaval töötlejal sellegipoolest olema võimalus kõnealuste vahendite otsustamisel kaasa rääkida. Üldvastutus on ikkagi vastutaval töötlejal, kes peab jälgima, et volitatud töötlejate otsused oleksid kooskõlas andmekaitseõigusega. Leping, milles sätestatakse, et vastutav töötleja ei tohi volitatud töötleja otsustusprotsessi sekkuda, tooks seega kaasa tõenäoliselt ühise vastutuse ning pooled jagaksid vastutava töötleja õiguslikke kohustusi.

Kui volitatud töötleja ei pea andmete kasutamisel kinni vastutava töötleja kindlaks määratud andmekasutuse piirangutest, saab ka volitatud töötlejast vastutav töötleja, vähemalt seoses nende andmetega, mille puhul vastutava töötleja juhtnööre eiratakse. Tõenäoliselt saab sellest volitatud töötlejast ebaseaduslikult tegutsev vastutav töötleja. Algne vastutav töötleja peab seevastu selgitama, kuidas õnnestus volitatud töötlejal oma volitusi rikkuda. Andmekaitsedirektiivi artikli 29 alusel loodud töörühm kaldub sellistes juhtumites aga arvama, et tegemist on ühisvastutusega, sest see tagab andmesubjektide huvides kõrgeima kaitsetaseme[89]. Ühisvastutuse puhul peaks üks oluline tagajärg olema see, et pooled on kahjude eest solidaarselt vastutavad, mis laiendab andmesubjektidele kättesaadavate õiguskaitsevahendite valikut.

Samuti võib tekkida küsimusi seoses vastutuse jagunemisega olukorras, kus vastutav töötleja on väikeettevõtja ja volitatud töötleja suurettevõtja, kes määrab oma teenuse tingimused kindlaks ise. Sellegipoolest leiab andmekaitsedirektiivi artikli 29 alusel loodud töörühm selliseid tingimusi silmas pidades, et vastutuse ulatus ei tohiks läbirääkimisjõu ebavõrdse jaotumise tõttu väheneda ning et vastutava töötleja mõistet tuleb alati tõlgendada kindlaksmääratud viisil[90].

89 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 25; andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 10/2006 SWIFT-võrgus isikuandmete töötlemise kohta, WP 128, Brüssel, 22. november 2006.

90 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 26.

Selguse ja läbipaistvuse huvides tuleks vastutava töötleja ja volitatud töötleja suhted paika panna kirjalikus lepingus[91]. Kui sellist lepingut ei sõlmita, tähendab see, et vastutav töötleja rikub vastastikuseid kohustusi käsitlevate kirjalike dokumentide esitamise kohustust ning et talle võidakse määrata karistus[92].

Vahel määravad volitatud töötlejad teatavaid ülesandeid allhanke korras täitma teised volitatud töötlejad. See on õigusaktide alusel lubatud ning selle korralduse üksikasjad sõltuvad vastutava töötleja ja volitatud töötleja vahel sõlmitud lepingu tingimustest, sealhulgas sellest, kas vastutav töötleja peab selleks alati eraldi loa andma või piisab vaid tema teavitamisest.

Euroopa Nõukogu õiguses kehtib eespool kirjeldatud tõlgendus vastutava töötleja ja volitatud töötleja mõistetest täiel määral, nagu nähtub konventsiooni nr 108 alusel koostatud soovitustest[93].

2.3.2. Vastuvõtjad ja kolmandad isikud

Nende kahe andmekaitsedirektiivis määratletud isikute või üksuste kategooria erinevus seisneb peamiselt nende suhetes vastutava töötlejaga ning sellest tulenevalt nende õiguses vastutava töötleja valduses olevate isikuandmetega tutvuda.

Kolmas isik on vastutavast töötlejast juriidiliselt eraldiseisev isik või üksus. Andmete avaldamiseks kolmandale isikule on seega alati vaja konkreetset õiguslikku alust. Andmekaitsedirektiivi artikli 2 punkti f kohaselt kuuluvad kolmandate isikute alla „kõik füüsilised või juriidilised isikud, riigiasutused, esindused või muud organid, välja arvatud andmesubjekt, vastutav töötleja, volitatud töötleja ja isikud, kes võivad andmeid töödelda vastutava töötleja või volitatud töötleja otseses alluvuses". See tähendab, et vastutavast töötlejast juriidiliselt eraldiseisvas organisatsioonis töötavad isikud on kolmandad isikud (või kuuluvad kolmanda isiku juurde), isegi kui asjaomane organisatsioon kuulub samasse gruppi või valdusettevõttesse. Teisalt ei loetaks kolmandateks isikuteks peakorteri otseses alluvuses kliendikontosid töötlevaid panga harukontoreid[94].

91 Andmekaitsedirektiivi artikli 17 lõiked 3 ja 4.

92 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 27.

93 Vt nt profiilide koostamist käsitleva soovituse artikkel 1.

94 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta, WP 169, Brüssel, 16. veebruar 2010, lk 31.

Vastuvõtja mõiste on laiem kui kolmanda isiku mõiste. Andmekaitsedirektiivi artikli 2 punkti g tähenduses on vastuvõtja „füüsiline või juriidiline isik, riigiasutus, esindus või mõni muu organ, kellele andmed avaldatakse, olenemata sellest, kas tegemist on kolmanda isikuga või mitte". Vastuvõtja võib olla kas vastutavast töötlejast või volitatud töötlejast eraldiseisev isik, st seega kolmas isik, või vastutava töötleja või volitatud töötlejaga seotud isik, näiteks töötaja või sama ettevõtte või asutuse teine osakond.

Vastuvõtjaid ja kolmandaid isikuid on vaja eristada üksnes andmete õiguspärase avaldamise tingimusi silmas pidades. Vastutava töötleja või volitatud töötleja töötajad võivad isikuandmete vastuvõtjad olla ilma täiendava õigusliku aluseta, kui nad on kaasatud vastutava töötleja või volitatud töötleja andmetöötlustoimingutesse. Kolmandal isikul, kes on vastutavast töötlejast või volitatud töötlejast juriidiliselt eraldiseisev, seevastu ei ole õigust kasutada vastutava töötleja töödeldavaid isikuandmeid, välja arvatud teatavatel erijuhtudel, kus selleks on konkreetne õiguslik alus. Andmete kolmandast isikust vastuvõtjatel peab seega alati olema õiguslik alus isikuandmeid kooskõlas õigusaktidega vastu võtta.

Näide: volitatud töötleja töötaja, kes kasutab tööandja antud volituste alusel teatavaid isikuandmeid, on andmete vastuvõtja, kuid mitte kolmas isik, sest ta kasutab andmeid volitatud töötleja nimel ja tema juhtnööride järgi.

Kui aga kõnealune töötaja otsustab kasutada andmeid, millele tal on volitatud töötleja töötajana juurdepääs, omaenda eesmärkidel ning müüb neid teisele ettevõttele, tegutseb ta kolmanda isikuna. Ta ei järgi enam volitatud töötleja (tööandja) korraldusi. Kolmanda isikuna oleks asjaomasel töötajal andmete omandamiseks ja müümiseks vaja õiguslikku alust. Praegusel juhul töötajal sellist õiguslikku alust kahtlemata ei ole, mistõttu tegutseks ta ebaseaduslikult.

2.4. Nõusolek

Põhipunktid

- Isikuandmete töötlemise õigusliku alusena peab nõusolek olema vabatahtlik, teadlik ja konkreetne.

- Nõusolek peab olema antud ühemõtteliselt. Andmesubjekt võib nõusoleku anda kas otsesõnu või andes oma käitumisega selgelt mõista, et ta nõustub oma andmete töötlemisega.
- Tundlike andmete töötlemiseks nõusoleku alusel on vaja sõnaselget nõusolekut.
- Andmesubjekt võib nõusoleku mis tahes ajal tagasi võtta.

Nõusolek on „iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku"[95]. Paljudel juhtudel on see õiguspärase andmetöötluse õiguslik alus (vt jaotis 4.1).

2.4.1. Kehtiva nõusoleku tingimused

ELi õiguses peab kehtiva nõusoleku jaoks olema täidetud kolm tingimust, mille eesmärk on tagada, et andmesubjektid on igati nõus oma andmete kasutamisega:

- andmesubjektile ei tohtinud avaldada nõusoleku andmisel survet;
- andmesubjekti pidi nõuetekohaselt teavitatama nõusoleku andmise objektist ja tagajärgedest;
- nõusoleku ulatus peab olema mõistlikul määral konkreetne.

Andmekaitseõiguse seisukohalt on nõusolek kehtiv üksnes siis, kui kõik osutatud tingimused on täidetud.

Konventsioonis nr 108 nõusoleku määratlust sätestatud ei ole; see on jäetud riikide otsustada. Samal ajal vastavad kehtiva nõusoleku tingimused **Euroopa Nõukogu õiguses** eespool kirjeldatud tingimustele, nagu selgub konventsiooni nr 108 alusel koostatud soovitustest[96]. Nõusoleku tingimused kattuvad Euroopa tsiviilõiguses kehtiva tahteavalduse puhul rakendatavate tingimustega.

Kehtiva nõusoleku suhtes tsiviilõiguses kohaldatavad lisanõuded, näiteks õigus- ja teovõime, kehtivad loomulikult ka andmekaitse valdkonnas, kuna sellised nõuded on õiguslikus mõttes iseenesest mõistetavad eeltingimused. Õigus- ja teovõimeta isikute kehtetu nõusoleku puhul ei ole nende andmete töötlemiseks õiguslikku alust.

95 Andmekaitsedirektiivi artikli 2 punkt h.

96 Vt nt konventsioon nr 108, statistilisi andmeid käsitleva soovituse punkt 6.

Nõusolek võib olla sõnaselge[97] või kaudne. Esimese puhul ei jää mingit kahtlust andmesubjekti kavatsuste suhtes ning nõusolek võidakse anda kas suuliselt või kirjalikult; kaudne nõusolek tuletatakse tingimustest. Nõusolek peab alati olema antud ühemõtteliselt[98]. See tähendab, et ei tohiks olla põhjendatud kahtlust seoses sellega, et andmesubjekt tahtis väljendada nõustumist oma isikuandmete töötlemisega. Näiteks ei saa ühemõttelist nõusolekut eeldada ainuüksi sellest, kui andmesubjekt ei reageeri kuidagi. Tundlike andmete töötlemiseks on vaja andmesubjekti sõnaselget ja ühemõttelist nõusolekut.

Vabatahtlik nõusolek

Nõusolek on vabatahtlik üksnes juhul, kui andmesubjektil on reaalne valikuvõimalus ning teda ei ähvarda pettuse, hirmutamise või sundimise oht või olulised negatiivsed tagajärjed mittenõustumise korral[99].

Näide: paljudes lennujaamades peavad reisijad pardalemineku alale sisenemiseks läbima kehaskanneri[100]. Arvestades, et skannimisel töödeldakse reisijate andmeid, peab andmetöötlus vastama ühele andmekaitsedirektiivi artiklis 7 kirjeldatud õiguslikule alusele (vt jaotis 4.1.1). Vahel jäetakse reisijatele mulje, et kehaskanneri läbimine on vabatahtlik, vihjates sellele, et nende nõusolek võiks õigustada andmetöötlust. Samal ajal võivad reisijad karta, et sellest keeldumine võib tekitada kahtlust või anda põhjust täiendavaks turvakontrolliks, näiteks füüsiliseks läbiotsimiseks. Paljud reisijad nõustuvad skannimisega, kuna niiviisi püüavad nad vältida võimalikke probleeme või viivitusi. Eeldatavasti ei ole selline nõusolek piisavalt vabatahtlik.

Seega saab kindla õigusliku aluse tagada vaid seadusandja õigusaktiga andmekaitsedirektiivi artikli 7 punkti e alusel, mis kohustaks reisijaid ülimusliku avaliku huvi kaalutlusel koostööd tegema. Sellise õigusaktiga saaks siiski ette näha ka võimaluse valida skannimise ja läbiotsimise vahel, kuid üksnes osana teatavates tingimustes vajalikest täiendavatest piirikontrolli meetmetest. Neid

97 Andmekaitsedirektiivi artikli 8 lõige 2.

98 *Ibid.*, artikli 7 punkt a ja artikli 26 lõige 1.

99 Vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 15/2011 nõusoleku mõiste kohta, WP 187, Brüssel, 13. juuli 2011, lk 12.

100 Näide on pärit eelmisena viidatud allikast, lk 15.

aspekte käsitles Euroopa Komisjon kahes 2011. aasta määruses turvaskannerite kohta[101].

Nõusolek ei pruugi vabatahtlik olla ka alluvusega seotud juhtudel, kui nõusolekut taotlev vastutav töötleja ja nõusolekut andev andmesubjekt on majanduslikult olulisel määral ebavõrdsed[102].

Näide: suurettevõte kavatseb koostada kataloogi kõikide töötajate nimede, nende ametiülesannete ja tööaadressidega lihtsalt selleks, et parandada ettevõttesisest suhtlust. Personalijuht teeb ettepaneku lisada kataloogi ka igast töötajast foto, et kolleege oleks näiteks koosolekutel hõlpsam ära tunda. Töötajate esindajad nõuavad, et kataloogi lisataks fotod üksnes nendest töötajatest, kes selleks eraldi nõusoleku annavad.

Sellises olukorras tuleks töötaja nõusolekut käsitada õigusliku alusena fotode töötlemiseks kataloogis, kuna on selge, et foto avaldamisel kataloogis ei ole iseenesest negatiivseid tagajärgi, ning pealegi võib arvata, et töötajal ei teki tööandjaga probleeme, kui ta ei nõustu foto avaldamisega kataloogis.

See aga ei tähenda, et nõusolek ei saa kunagi olla kehtiv tingimustes, kus mittenõustumisel võib olla negatiivseid tagajärgi. Kui näiteks kaupluse kliendikaardi väljastamisega mittenõustumise tagajärg on üksnes see, et klient ei saa teatavatelt kaupadelt allahindlust, on nõusolek sellegipoolest kehtiv õiguslik alus kliendikaardi väljastamiseks nõusoleku andnud klientide isikuandmete töötlemiseks. Ettevõtte ja kliendi vahel ei ole alluvussuhet ning mittenõustumise tagajärjed ei ole andmesubjekti jaoks vaba valiku välistamiseks piisavalt tõsised.

Olukorras, kus teatavaid piisavalt olulisi kaupu või teenuseid saab osta ainult ja eranditult siis, kui avaldatakse isikuandmeid kolmandatele isikutele, ei ole andmesubjekti

101 Komisjoni määrus (EL) nr 1141/2011, 10. november 2011, millega muudetakse määrust (EÜ) nr 272/2009 (millega täiendatakse tsiviillennundusjulgestuse ühiseid põhistandardeid) seoses turvaskannerite kasutamisega ELi lennuväljadel, ELT L 293, 2011; komisjoni rakendusmäärus (EL) nr 1147/2011, 11. november 2011, millega muudetakse määrust (EL) nr 185/2010 (millega nähakse ette üksikasjalikud meetmed lennundusjulgestuse ühiste põhistandardite rakendamiseks) seoses turvaskannerite kasutamisega ELi lennuväljadel, ELT L 294, 2011.

102 Vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 8/2001 isikuandmete töötlemise kohta tööhõive valdkonnas, WP 48, Brüssel, 13. september 2001; andmekaitsedirektiivi artikli 29 alusel loodud töörühma 24. oktoobri 1995. aasta direktiivi 95/46/EÜ artikli 26 lõike 1 ühist tõlgendamist käsitlev töödokument, WP 114, Brüssel, 25. november 2005.

nõusolek oma andmete avaldamiseks üldiselt vabatahtlik ning seega ei ole see andmekaitseõiguse seisukohalt ka kehtiv.

Näide: olukorras, kus reisijad lubavad lennuettevõtjal edastada broneeringuinfot, st nende identiteeti, söömisharjumusi või terviseprobleeme käsitlevaid andmeid, teatava välisriigi sisseränd easutustele, ei ole andmekaitseõiguse alusel tegemist kehtiva nõusolekuga, kuna asjaomasesse riiki reisida soovivatel isikutel ei ole valikuvõimalust. Selleks et broneeringuinfo edastamine oleks õigusaktidega kooskõlas, on nõusoleku kõrval vaja täiendavat õiguslikku alust, tõenäoliselt eriotstarbelist õigusakti.

Teadlik nõusolek

Andmesubjektil peab enne otsuse tegemist olema piisavalt teavet. Esitatud teabe piisavuse üle saab otsustada ainult iga üksikjuhtumi puhul eraldi. Tavaliselt on teadlikuks nõusolekuks vaja täpset ja hõlpsasti mõistetavat kirjeldust nõusoleku objektist ning samuti teavet selle kohta, millised tagajärjed nõustumise või mittenõustumisega kaasnevad. Teave peaks olema selle eeldatavatele saajatele arusaadavas keeles.

Samuti peab kõnealune teave olema andmesubjektile hõlpsasti kättesaadav. Olulised tegurid on siinkohal teabe kättesaadavus ja nähtavus. Internetikeskkonnas võib hea lahendus olla nn kihiline teavitamine, mille puhul andmesubjekt saab teabe lühiülevaate kõrval tutvuda ka selle mahukama versiooniga.

Konkreetne nõusolek

Kehtiv nõusolek peab olema ka konkreetne. See käib käsikäes nõusoleku objekti kohta antava teabe kvaliteediga. Selles kontekstis mängivad rolli keskmise andmesubjekti õigustatud ootused. Kui andmetöötlustoiminguid kavatsetakse muuta või alustada uusi toiminguid, mida ei oleks mõistlikul alusel saanud algse nõusoleku andmise ajal ette näha, tuleb andmesubjektilt uuesti nõusolekut küsida.

Näide: *Deutsche Telekom AG*[103] kohtuasjas käsitles ELK küsimust, kas telekommunikatsiooniettevõtja, kellel oli vaja edastada abonentide isikuandmeid eraelu

103 ELK, C-543/09, *Deutsche Telekom AG vs. Saksamaa*, 5. mai 2011; vt eeskätt punktid 53 ja 54.

puutumatust ja elektroonilist sidet käsitleva direktiivi[104] artikli 12 alusel, pidi paluma andmesubjektidelt nõusoleku ülekinnitamist, arvestades, et andmete saajad ei olnud nõusoleku andmise ajal teada.

ELK leidis, et selle artikli alusel ei ole enne andmete edastamist tarvis abonendi uut nõusolekut, kuna andmesubjektid said kõnealuse sätte alusel nõustuda vaid töötlemise eesmärgiga, st nende andmete avaldamisega, ning ei saanud valida, millistes kataloogides lubada neid andmeid avaldada.

Kohus rõhutas, et „eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 12 kontekstipõhisest ja süstemaatilisest tõlgendusest [tuleneb], et selle artikli lõikes 2 käsitletud nõusolek on esmajoones seotud andmete üldkasutatavas kataloogis avaldamise eesmärgiga, mitte aga sellise kataloogi pakkuja isikuga"[105]. Peale selle võib „juba isikuandmete avaldamine teatava otstarbega kataloogis [...] osutuda abonenti kahjustavaks",[106] mitte andmete avaldaja.

2.4.2. Õigus võtta nõusolek mis tahes ajal tagasi

Andmekaitsedirektiiviga ei ole ette nähtud üldist õigust nõusolek mis tahes ajal tagasi võtta. Laiemas plaanis aga arvatakse, et selline õigus on olemas ning et andmesubjektil peab olema võimalik seda õigust omal äranägemisel kasutada. Tagasivõtmise korral ei tohiks andmesubjekti kohustada seda põhjendama ning andmete eelnevalt kokku lepitud kasutamisega seotud võimalikest eelistest ilmajäämise kõrval ei tohiks sellega kaasneda negatiivseid tagajärgi.

Näide: klient nõustub sellega, et talle saadetakse reklaamposti aadressile, mille ta vastutavale töötlejale esitab. Kui klient võtab nõusoleku tagasi, ei tohi vastutav töötleja talle enam reklaamposti saata. Nõusoleku tagasivõtmisega ei tohiks kaasneda karistusele viitavaid tagajärgi, näiteks mingeid tasusid.

Kui klient nõustus oma andmete kasutamisega reklaamposti saatmise eesmärgil ning sai vastutasuks hotellitoa hinnalt 5% allahindlust, ei tähenda hilisem nõusoleku tagasivõtmine, et ta peab kõnealuse allahindluse summa tagasi maksma.

104 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 2002.

105 ELK, C-543/09, *Deutsche Telekom AG vs. Saksamaa,* 5. mai 2011; vt eeskätt punkt 61.

106 *Ibid.*, eeskätt punkt 62.

3

Euroopa andmekaitseõiguse peamised põhimõtted

EL	Käsitletavad küsimused	Euroopa Nõukogu
Andmekaitsedirektiivi artikli 6 lõike 1 punktid a ja b ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) vs. Land Hessen*, 9. november 2010	**Seadusliku töötlemise põhimõte**	Konventsiooni nr 108 artikli 5 punktid a ja b EIK, *Rotaru vs. Rumeenia [suurkoda]*, nr 28341/95, 4. mai 2000 EIK, *Taylor-Sabori vs. Ühendkuningriik*, nr 47114/99, 22. oktoober 2002 EIK, *Peck vs. Ühendkuningriik*, nr 44647/98, 28. jaanuar 2003 EIK, *Khelili vs. Šveits*, nr 16188/07, 18. oktoober 2011 EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987
Andmekaitsedirektiivi artikli 6 lõike 1 punkt b	**Eesmärgi määratlemise ja piiritlemise põhimõte**	Konventsiooni nr 108 artikli 5 punkt b
	Andmekvaliteedi põhimõtted:	
Andmekaitsedirektiivi artikli 6 lõike 1 punkt c	**Andmete asjakohasus**	Konventsiooni nr 108 artikli 5 punkt c

EL	Käsitletavad küsimused	Euroopa Nõukogu
Andmekaitsedirektiivi artikli 6 lõike 1 punkt d	Andmete täpsus	Konventsiooni nr 108 artikli 5 punkt d
Andmekaitsedirektiivi artikli 6 lõike 1 punkt e	Andmete piiratud säilitamisaeg	Konventsiooni nr 108 artikli 5 punkt e
Andmekaitsedirektiivi artikli 6 lõike 1 punkt e	Erand teadusuuringute ja statistika puhul	Konventsiooni nr 108 artikli 9 lõige 3
Andmekaitsedirektiivi artikli 6 lõike 1 punkt a	Õiglase töötlemise põhimõte	Konventsiooni nr 108 artikli 5 punkt a EIK, *Haralambie vs. Rumeenia*, nr 21737/03, 27. oktoober 2009 EIK, *K.H. jt vs. Slovakkia*, nr 32881/04, 28. aprill 2009
Andmekaitsedirektiivi artikli 6 lõige 2	Vastutuse põhimõte	

Konventsiooni nr 108 artiklis 5 esitatud põhimõtetes peitub Euroopa andmekaitseõiguse tuumik. Samuti kajastuvad need põhimõtted andmekaitsedirektiivi artiklis 6 ning need on aluseks direktiivi järgnevates artiklites kehtestatud üksikasjalikumatele sätetele. Kõik Euroopa Nõukogu või ELi tasandi edaspidised andmekaitsealased õigusaktid peavad vastama asjaomastele põhimõtetele ning neid tuleb arvesse võtta kõnealuste õigusaktide tõlgendamisel. Riikide tasandil võidakse ette näha nende peamiste põhimõtete erandid ja piirangud[107]; need peavad olema kooskõlas õigusaktidega, neil peab olema õiguspärane eesmärk ning need peavad olema demokraatlikus ühiskonnas vajalikud. Kõik kolm tingimust peavad olema täidetud.

3.1. Seadusliku töötlemise põhimõte

Põhipunktid

- Seadusliku töötlemise põhimõtte mõistmiseks tuleks viidata tingimustele, mille puhul tohib õiguspärasel alusel piirata õigust isikuandmete kaitsele, pidades silmas Euroopa põhiõiguste harta artikli 52 lõiget 1, ning nõudeid seoses põhjendatud sekkumisega Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 alusel.
- Sellega seoses on isikuandmete töötlemine seaduslik ainult juhul, kui:

107 Konventsiooni nr 108 artikli 9 lõige 2; andmekaitsedirektiivi artikkel 13.

- see on kooskõlas õigusaktidega;
- sellel on õiguspärane eesmärk;
- see on demokraatlikus ühiskonnas vajalik õiguspärase eesmärgi saavutamiseks.

ELi ja Euroopa Nõukogu andmekaitseõiguses peab andmetöötlus esmajärjekorras olema seaduslik; see põhimõte on peaaegu samas sõnastuses talletatud konventsiooni nr 108 artiklis 5 ja andmekaitsedirektiivi artiklis 6.

Kummaski artiklis ei ole kirjeldatud, mida seaduslik töötlemine täpsemalt hõlmab. Selle õigustermini mõistmiseks tuleks viidata põhjendatud sekkumisele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni tähenduses ja EIK kohtupraktika tõlgenduses ning õiguspäraste piirangute tingimustele põhiõiguste harta artikli 52 alusel.

3.1.1. Nõuded seoses põhjendatud sekkumisega Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni alusel

Isikuandmete töötlemisega võidakse sekkuda andmesubjekti õigusesse eraelu austamisele. Õigus eraelu austamisele ei ole aga absoluutne õigus, vaid seda tuleb tasakaalustada ja kooskõlastada muude õiguspäraste huvidega, kas siis teiste inimeste huvidega (erahuvid) või kogu ühiskonna huvidega (avalikud huvid).

Alljärgnevalt kirjeldataksegi tingimusi, mille puhul riigi sekkumine on põhjendatud.

Kooskõla õigusaktidega

EIK kohtupraktikast lähtudes on sekkumine kooskõlas õigusaktidega, kui see põhineb teatavatele tingimustele vastaval riigi tasandi õigusnormil. Asjaomastel isikutel peaks olema juurdepääs kõnealusele õigusnormile ja selle mõju peaks olema prognoositav[108]. Prognoositav on eeskiri juhul, kui see on piisavalt täpselt sõnastatud ja võimaldab igal isikul – vajaduse korral asjakohase abiga – oma käitumist

108 EIK, *Amann vs. Šveits [suurkoda]*, nr 27798/95, 16. veebruar 2000, punkt 50; vt ka EIK, *Kopp vs. Šveits*, nr 23224/94, 25. märts 1998, punkt 55; EIK, *Iordachi jt vs. Moldova*, nr 25198/02, 10. veebruar 2009, punkt 50.

kohandada[109]. Õigusnormi puhul nõutav täpsuse aste sõltub konkreetsest kõne all olevast teemast[110].

Näide: kohtuasjas *Rotaru vs. Rumeenia*[111] tegi EIK kindlaks Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise, kuna Rumeenia õigusaktide alusel oli lubatud koguda, salvestada ja säilitada riigi julgeoleku seisukohalt olulist teavet salajastes toimikutes ning ei olnud samal ajal kehtestatud nende volituste kasutamise piiranguid, mistõttu ametiasutused said neid kasutada omal äranägemisel. Näiteks ei olnud riigi õigusaktides kindlaks määratud, millist liiki teavet võidakse töödelda, millistesse kategooriatesse kuuluvate isikute suhtes võidakse rakendada jälitusmeetmeid, millistes tingimustes selliseid meetmeid võidakse võtta või millist menetlust tuleb järgida. Nende puudujääkide tõttu järeldas kohus, et riigi õigusaktid ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 alusel kooskõlas prognoositavuse nõudega ning et tegemist oli selle artikli rikkumisega.

Näide: kohtuasjas *Taylor-Sabori vs. Ühendkuningriik*[112] käsitleti juhtumit, kus kaebuse esitaja oli politsei jälgimise all. Kaebuse esitaja piipari klooni abil sai politsei jälgida talle saadetud sõnumeid. Seejärel kaebuse esitaja vahistati ning talle esitati süüdistus kontrollitud uimastiga kaubitsemise vandenõus. Prokurör lähtus süüdistuse esitamisel muu hulgas jälgimise ajal tehtud kirjalikest märkmetest politsei transkribeeritud piiparisõnumite kohta. Kaebuse esitaja kohtuprotsessi ajal aga ei olnud Briti õiguses normi, millega oleks reguleeritud eraisikutele suunatud telekommunikatsioonisüsteemi kaudu toimuva suhtluse pealtkuulamist. Seega ei olnud sekkumine kaebuse esitaja õigustesse kooskõlas õigusaktidega. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

109 EIK, *Amann vs. Šveits [suurkoda]*, nr 27798/95, 16. veebruar 2000, punkt 56; vt ka EIK, *Malone vs. Ühendkuningriik*, nr 8691/79, 2. august 1984, punkt 66; EIK, *Silver jt vs. Ühendkuningriik*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. märts 1983, punkt 88.

110 EIK, *The Sunday Times vs. Ühendkuningriik*, nr 6538/74, 26. aprill 1979, punkt 49; vt ka EIK, *Silver jt vs. Ühendkuningriik*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. märts 1983, punkt 88.

111 EIK, *Rotaru vs. Rumeenia [suurkoda]*, nr 28341/95, 4. mai 2000, punkt 57; vt ka EIK, *Association for European Integration and Human Rights ja Ekimdzhiev vs. Bulgaaria*, nr 62540/00, 28. juuni 2007; EIK, *Shimovolos vs. Venemaa,* nr 30194/09, 21. juuni 2011; EIK, *Vetter vs. Prantsusmaa*, nr 59842/00, 31. mai 2005.

112 EIK, *Taylor-Sabori vs. Ühendkuningriik,* nr 47114/99, 22. oktoober 2002.

Õiguspärane eesmärk

Õiguspärane eesmärk võib olla kas mõni osutatud avalikest huvidest või teiste isikute õigused ja vabadused.

Näide: kohtuasjas *Peck vs. Ühendkuningriik*[113] käsitles kohus juhtumit, kus kaebuse esitaja üritas sooritada tänaval enesetappu, lõigates läbi oma veenid, seejuures teadmata, et teda filmis videovalvekaamera. Kui videovalvekaameraid jälginud politsei ta päästis, edastas politseiamet videosalvestise meediale, kus see avaldati ilma kaebuse esitaja nägu varjamata. EIK leidis, et ametivõimudel ei olnud asjakohaseid või piisavaid põhjuseid, mis oleks õigustanud salvestise otsest avaldamist avalikkusele ilma kaebuse esitaja nõusolekuta või tema identiteeti varjamata. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Vajalikkus demokraatlikus ühiskonnas

EIK kohaselt viitab vajalikkuse mõiste sellele, et sekkumine vastab tungivale sotsiaalsele vajadusele ning on eelkõige proportsionaalne õiguspäraselt taotletava eesmärgiga[114].

Näide: kohtuasjas *Khelili vs. Šveits*[115] käsitleti juhtumit, kus politsei kontrolli käigus leiti kaebuse esitajalt visiitkaardid, millel seisis tekst: „Meeldiv ja kena kolmekümnendate eluaastate teises pooles olev naine soovib kohtuda mehega, et võtta koos mõni klaasike või mõnikord välja minna. Telefoninumber: [...]". Kaebuse esitaja väitis, et pärast visiitkaartide leidmist sisestati ta andmebaasi prostituudina, kuigi ta märkis korduvalt, et ta ei ole prostituut. Kaebuse esitaja nõudis, et tema kirjest politsei andmebaasis kustutataks sõna „prostituut". EIK tunnistas üldjoontes, et üksikisiku isikuandmete säilitamine põhjusel, et ta võib toime panna uue kuriteo, võib teatavates tingimustes olla proportsionaalne. Kaebuse esitaja juhtumis aga tundus väide, et ta tegutseb ebaseadusliku prostitutsiooniga, liiga ebamäärane ja üldsõnaline ning selle tõendamiseks ei esitatud kindlaid fakte, kuna teda ei olnud kunagi ebaseaduslikus prostitutsioonis süüdi mõistetud, seega ei saanud sekkumine vastata tungivale sotsiaalsele

113 EIK, *Peck vs. Ühendkuningriik,* nr 44647/98, 28. jaanuar 2003, eeskätt punkt 85.

114 EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987, punkt 58.

115 EIK, *Khelili vs. Šveits*, nr 16188/07, 18. oktoober 2011.

vajadusele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses. Arvestades asjaolu, et ametivõimude ülesanne oli tõendada, et kaebuse esitaja kohta säilitatud andmed olid täpsed, ning kaebuse esitaja õigustesse sekkumise tõsidust, otsustas kohus, et demokraatlikus ühiskonnas ei olnud vajalik hoida politsei andmebaasis kaebuse esitaja kirjes mitu aastat sõna „prostituut". Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Näide: kohtuasjas *Leander vs. Rootsi*[116] otsustas EIK, et riigi julgeoleku seisukohalt olulistele ametikohtadele kandideerivate isikute salajane taustakontroll ei ole iseenesest vastuolus demokraatlikus ühiskonnas vajalikkuse nõudega. Lähtudes Rootsi õigusaktides andmesubjektide huvide kaitsmiseks kehtestatud konkreetsetest kaitsemeetmetest – näiteks kontroll parlamendi ja õiguskantsleri tasandil –, järeldas EIK, et Rootsi personalikontrolli süsteem vastas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 sätestatud nõuetele. Pidades silmas kostjaks olnud riigile jäetud suurt kaalutlusruumi, oli neil õigus arvestada, et kaebuse esitaja juhtumis kaaluvad riigi julgeoleku huvid üles üksikisiku huvid. Kohus järeldas, et tegu ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

3.1.2. Tingimused seoses õiguspäraste piirangutega ELi põhiõiguste harta alusel

Põhiõiguste harta on üles ehitatud ja sõnastatud teistmoodi kui Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Hartas ei käsitleta tagatud õigustesse sekkumist, vaid selles on kehtestatud säte hartaga tunnustatud õiguste ja vabaduste teostamise piiramise kohta.

Artikli 52 lõike 1 kohaselt tohib hartaga tunnustatud õiguste ja vabaduste teostamist ning sellest tulenevalt isikuandmete kaitse õiguse teostamist piirata, näiteks isikuandmeid töödeldes, üksnes juhul, kui:

- see on kooskõlas õigusaktidega;
- selle puhul arvestatakse isikuandmete kaitse õiguse olemust;
- see on vajalik ning vastab proportsionaalsuse põhimõttele;

116 EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987, punktid 59 ja 67.

- see vastab liidu tasandil tunnustatud avalikku huvi pakkuvatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi.

> Näide: *Volker und Markus Schecke*[117] kohtuasjas järeldas ELK, et nähes [teatavatest põllumajandusfondidest] toetust saanud füüsiliste isikute puhul ette iga toetusesaaja isikuandmete avaldamise, tegemata vahet asjaomaste kriteeriumide alusel, nagu toetuse saamise ajavahemikud, toetuse sagedus või liik ja summa, ületasid nõukogu ja komisjon piire, mida nõuab proportsionaalsuse põhimõtte järgimine.
>
> Seepärast järeldas ELK, et teatavad nõukogu määruse (EÜ) nr 1290/2005 sätted ja määrus (EÜ) nr 259/2008 tuleb kehtetuks tunnistada[118].

Hoolimata sõnastuse erinevustest sarnanevad põhiõiguste harta artikli 52 lõikest 1 tulenevad seadusliku töötlemise tingimused Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikest 2 tulenevate tingimustega. Harta artikli 52 lõikes 1 loetletud tingimused peavad kattuma konventsiooni artikli 8 lõikest 2 tulenevate tingimustega, pidades silmas, et harta artikli 52 lõike 3 esimeses lauses sätestatakse: „Hartas sisalduvate selliste õiguste tähendus ja ulatus, mis vastavad Euroopa inimõiguste ja põhivabaduse kaitse konventsiooniga tagatud õigustele, on samad, mis neile nimetatud konventsiooniga ette on nähtud".

Artikli 52 lõike 3 viimasest lausest selgub aga, et „[s]ee säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist". Kui võrrelda Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõiget 2 ja harta artikli 52 lõike 3 esimest lauset, võib see tähendada vaid seda, et konventsiooni artikli 8 lõike 2 kohased põhjendatud sekkumise tingimused on isikuandmete kaitse õiguse suhtes kooskõlas hartaga kohaldatavate õiguspäraste piirangute miinimumnõuded. Sellest tulenevalt on isikuandmete töötlemine ELi õiguses seaduslik, kui täidetud on vähemalt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 tingimused; samas võib liidu õiguses teatavateks juhtudeks kehtestada lisanõuded.

117 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, 9. november 2010, punktid 89 ja 86.

118 Nõukogu määrus (EÜ) nr 1290/2005, 21. juuni 2005, ühise põllumajanduspoliitika rahastamise kohta, ELT L 209, 2005; komisjoni määrus (EÜ) nr 259/2008, 18. märts 2008, milles sätestatakse nõukogu määruse (EÜ) nr 1290/2005 kohaldamise üksikasjalikud eeskirjad seoses Euroopa Põllumajanduse Tagatisfondi (EAGF) ja Maaelu Arengu Euroopa Põllumajandusfondi (EAFRD) vahenditest toetuse saajaid hõlmava teabe avaldamisega, ELT L 76, 2008.

ELi õigusega ette nähtud seadusliku töötlemise põhimõtte ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni asjakohaste sätete vastavust rõhutatakse ka ELi lepingu artikli 6 lõikes 3, milles sätestatakse, et „Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga tagatud [...] põhiõigused on liidu õiguse üldpõhimõtted".

3.2. Eesmärgi määratlemise ja piiritlemise põhimõte

Põhipunktid

- Enne andmete töötlemist peab olema selgelt kindlaks määratud töötlemise eesmärk.
- ELi õiguses peab töötlemise eesmärk olema selgelt määratletud; Euroopa Nõukogu õiguses on see küsimus riikide otsustada.
- Andmete töötlemine, mille puhul ei ole kindlaks määratud eesmärki, ei ole kooskõlas andmekaitseõigusega.
- Andmete täiendavaks kasutamiseks mõnel teisel eesmärgil on vaja täiendavat õiguslikku alust, juhul kui uus eesmärk ei lange kokku algse eesmärgiga.
- Andmete edastamine kolmandatele isikutele on uus eesmärk ning selleks on vaja täiendavat õiguslikku alust.

Sisuliselt tähendab eesmärgi määratlemise ja piiritlemise põhimõte seda, et isikuandmete töötlemise õiguspärasus sõltub töötlemise eesmärgist[119]. Enne andmete töötlemist peab vastutav töötleja kindlaks määrama ja täpsustama selle eesmärgi[120]. **ELi õiguses** võib eesmärki täpsustada kas asjaomasele järelevalveasutusele esitatavas deklaratsioonis, st teda teavitades, või vähemalt sisedokumendis, mille vastutav töötleja peab kättesaadavaks tegema järelevalveasutustele kontrollimiseks ja andmesubjektile tutvumiseks.

Isikuandmete töötlemine, mille puhul ei ole kindlaks määratud konkreetset ja/või piiritletud eesmärki, on ebaseaduslik.

119 Konventsiooni nr 108 artikli 5 punkt b; andmekaitsedirektiivi artikli 6 lõike 1 punkt b.

120 Vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 03/2013 eesmärgi piiramise kohta, WP 203, Brüssel, 2. aprill 2013.

Iga uue eesmärgi puhul on andmete töötlemiseks tarvis eraldi õiguslikku alust ning seejuures ei saa toetuda asjaolule, et andmed saadi või neid töödeldi esialgu muul õiguspärasel eesmärgil. Samamoodi piirdub seaduslik töötlemine selle algselt kindlaks määratud eesmärgiga ning igaks täiendavaks eesmärgiks on vaja eraldi õiguslikku alust. Eriti ettevaatlikult tuleb suhtuda andmete avaldamisse kolmandatele isikutele, kuna tavaliselt on selle puhul tegu uue eesmärgiga, mis nõuab andmete kogumise esialgsest õiguslikust alusest erinevat õiguslikku alust.

Näide: lennuettevõtja kogub reisijatelt broneeringute tegemisel teatavaid andmeid, et tagada nõuetekohane lennuteenus. Need andmed käsitlevad järgmisi küsimusi: reisijate istekoha numbrid; füüsilised eripiirangud, nt ratastoolis isikute puhul; toitlustamisega seotud erisoovid, nt koššer- või *halal*-toit. Kui lennuettevõtjal palutakse edastada kõnealused broneeringuinfos sisalduvad andmed sihtriigi sisserändeasutusele, kasutatakse neid seejärel sisserände kontrolli eesmärkidel, mis erinevad algsest andmete kogumise eesmärgist. Nende andmete edastamiseks sisserändeasutusele on seepärast vaja eraldi uut õiguslikku alust.

Konkreetse eesmärgi ulatuse ja piirangute puhul rakendatakse konventsioonis nr 108 ja andmekaitsedirektiivis kooskõla põhimõtet – andmete kasutamise eesmärgid peavad olema kooskõlas esialgse õigusliku alusega. Mida selline kooskõla aga täpsemalt hõlmab, ei ole kindlaks määratud, ning seda tõlgendatakse iga üksikjuhtumi puhul eraldi.

Näide: ettevõtte Päikesekiir kliendisuhete halduse eesmärgil kogutud kliendiandmete müümine otseturundusettevõttele Kuukiir, kes kavatseb neid andmeid kasutada kolmandate ettevõtete turunduskampaaniate edendamiseks, on uus eesmärk, mis ei ole kooskõlas ettevõtte Päikesekiir kliendiandmete kogumise esialgse eesmärgiga (kliendisuhete haldus). Seega on andmete müümiseks ettevõttele Kuukiir vaja eraldi õiguslikku alust.

Kui aga ettevõte Päikesekiir sooviks kõnealuseid kliendisuhete haldusega seotud andmeid kasutada omaenda turunduseesmärkidel, st ettevõtte tooteid käsitleva turundusteabe saatmiseks oma klientidele, oleks see üldiselt kooskõlas esialgse eesmärgiga.

Andmekaitsedirektiivis sätestatakse sõnaselgelt: „Täiendavat töötlemist ajaloo, statistika või teadusega seotud eesmärkidel ei peeta vastuolus olevaks tingimusel, et liikmesriigid kannavad hoolt vajalike tagatiste eest"[121].

Näide: ettevõte Päikesekiir on kogunud oma klientidelt kliendisuhete haldusega seotud andmeid ning säilitab neid. Kui Päikesekiir soovib neid andmeid hiljem kasutada statistilise analüüsi tegemiseks klientide ostuharjumuste kohta, on see lubatud, sest statistikaga seotud eesmärke ei peeta vastuolus olevaks. Selle jaoks ei ole vaja täiendavat õiguslikku alust, näiteks andmesubjektide nõusolekut.

Kui samu andmeid kavatsetakse edastada kolmandale isikule, ettevõttele Tähevalgus, üksnes statistilistel eesmärkidel, oleks ka see lubatud ilma täiendava õigusliku aluseta, kuid üksnes tingimusel, et kehtestatud on vajalikud tagatised, näiteks andmesubjektide identiteedi varjamine, sest statistikaga seotud eesmärkide puhul ei ole üldjuhul vaja teada andmesubjektide identiteeti.

3.3. Andmekvaliteedi põhimõtted

Põhipunktid

- Vastutav töötleja peab kõikides andmetöötlustoimingutes järgima andmete kvaliteeti käsitlevaid põhimõtteid.
- Andmete säilitamise tähtaja kindlaksmääramise põhimõttest lähtudes tuleb andmed kustutada kohe, kui neid ei ole enam nende kogumise esialgsete eesmärkide jaoks vaja.
- Andmete säilitamise tähtaja kindlaksmääramise põhimõtte erandid tuleb ette näha õigusaktidega ning tuleb tagada seejuures eritagatised andmesubjektide kaitsmiseks.

3.3.1. Andmete asjakohasuse põhimõte

Töödeldakse üksnes selliseid andmeid, mis on „piisavad, asjakohased ega ületa selle otstarbe piire, mille tarvis neid kogutakse ja/või hiljem töödeldakse"[122]. Töötlemisse

121 Üks näide sellistest riigi tasandi sätetest on Austria andmekaitseseadus (Datenschutzgesetz), Fed. Law Gazette I No. 165/1999, punkt 46, inglise keeles avaldatud: www.dsk.gv.at/DocView.axd?CobId=41936.

122 Konventsiooni nr 108 artikli 5 punkt c; andmekaitsedirektiivi artikli 6 lõike 1 punkt c.

hõlmatavad andmekategooriad peavad olema vajalikud andmetöötlustoimingute kindlaksmääratud üldeesmärgi saavutamiseks ning vastutav töötleja peaks andmete kogumisel piirduma üksnes sellise teabega, mis on töötlemise konkreetse eesmärgi seisukohalt asjakohane.

Tänapäeva ühiskonnas tuleb andmete asjakohasuse põhimõtte puhul arvesse võtta veel üht aspekti – eraelu puutumatust soodustavate tehnoloogiate abil ei ole teatavatel juhtudel üldse vaja isikuandmeid kasutada või on võimalik esitada andmed pseudonüümi all, mis tagab eraelu puutumatuse seisukohalt tõhusa lahenduse. See on eriti asjakohane laiaulatuslikumate andmetöötlussüsteemide puhul.

Näide: linnanõukogu pakub inimestele, kes kasutavad regulaarselt linna ühistransporti, teatava tasu eest kiipkaarti. Kaardile on kirjutatud kasutaja nimi ning kiip sisaldab isiku nime ka elektroonilises vormis. Bussi või trammi kasutades tuleb kiipkaarti lühidalt hoida ühissõidukitesse paigaldatud kaardilugejate ees. Lugejas tuvastatud andmeid võrreldakse elektrooniliselt, kasutades kõikide sõidukaardi ostnud inimeste nimesid sisaldavat andmebaasi.

Selle süsteemi puhul ei järgita asjakohasuse põhimõtet kuigi optimaalselt – selleks et kontrollida, kas isikul on õigus kasutada ühissõidukeid, ei ole tingimata vaja võrrelda kaardi kiibil sisalduvaid isikuandmeid andmebaasi kirjetega. Piisaks näiteks spetsiaalsest elektroonilisest kujutisest, näiteks triipkoodist kaardi kiibil, millega saaks kaarti kaardilugeja ees lühidalt hoides kinnitada kaardi kehtivust. Sellise süsteemi puhul ei salvestataks andmeid selle kohta, milliseid ühissõidukeid ja millal keegi on kasutanud. See ei hõlmaks isikuandmete kogumist, mis on asjakohasuse põhimõtet silmas pidades ka kõige optimaalsem lahendus, sest selle põhimõtte järgi peab andmete kogumine piirduma eesmärgi saavutamiseks minimaalselt vajalikuga.

3.3.2. Andmete täpsuse põhimõte

Vastutav töötleja võib tema käsutuses olevaid isikuandmeid kasutada üksnes juhul, kui ta saab mõistlikkuse piires kindel olla, et need andmed on täpsed ja ajakohased.

Andmete täpsuse tagamise kohustust tuleb vaadelda andmetöötluse eesmärki silmas pidades.

Näide: mööblimüügiga tegelev ettevõte kogus arve esitamiseks kliendilt andmeid, millest ilmnes tema identiteet ja aadress. Kuus kuud hiljem on samal ettevõttel plaanis käivitada turunduskampaania ning selle jaoks tahetakse ühendust võtta varasemate klientidega. Selleks et nendega ühendust võtta, tahab ettevõte kasutada rahvastikuregistrit, kus tõenäoliselt on olemas klientide kehtivad aadressid, kuna kodanikel on õigusaktide alusel kohustus teatada rahvastikuregistrile oma kehtiv aadress. Kõnealuse registri andmetega saavad tutvuda vaid need isikud ja üksused, kellel on selleks mõjuv põhjus.

Selles olukorras ei saa ettevõte väita, et tal on õigus saada rahvastikuregistrist ajakohastatud andmeid kõigi oma varasemate klientide aadresside kohta ettekäändel, et tal on vaja tagada andmete täpsus ja ajakohasus. Ettevõte kogus andmeid arvete esitamiseks; sel eesmärgil on asjakohane müügitehingu toimumise ajal kehtinud aadress. Ajakohastatud elukohaandmete kogumiseks ei ole õiguslikku alust, kuna turundusega seotud huvi ei kaalu üles õigust isikuandmete kaitsele ning seega ei ole see piisav alus registri andmetega tutvumiseks.

Mõnel juhul on õigusaktide alusel keelatud säilitatavaid andmeid ajakohastada, sest andmete säilitamise eesmärk on peaasjalikult sündmuste dokumenteerimine.

Näide: meditsiinilise operatsiooni protokolli ei tohi muuta, st ajakohastada isegi siis, kui hiljem selgub, protokollis esitatud leiud ei pidanud paika. Sellistel juhtudel võib protokollis tehtud tähelepanekuid üksnes täiendada ning seejuures tuleb selgelt märkida, et tegemist on hiljem tehtud täiendustega.

Teisalt tuleb ette olukordi, kus on andmete täpsust vaja ilmtingimata regulaarselt kontrollida, sh ajakohastada, sest kui andmed on ebatäpsed, võib see tekitada kahju andmesubjektile.

Näide: kui isik soovib sõlmida lepingu pangaga, kontrollib panktavaliselt võimaliku kliendi krediidivõimelisust. Selleks tarbeks on olemas eraldi andmebaasid, mis sisaldavad andmeid eraisikute varasemate laenude kohta. Kui sellise andmebaasi kaudu esitatakse üksikisiku kohta ebatäpseid või aegunud andmeid, võib sellel isikul tekkida tõsiseid probleeme. Selliste andmebaaside vastutavad töötlejad peavad seega rakendama erimeetmeid, et tagada andmete täpsuse põhimõtte järgimine.

Andmeid, mis ei käsitle fakte, vaid kahtlusi, näiteks kriminaaluurimiste kontekstis, võib koguda ja säilitada tingimusel, et vastutaval töötlejal on sellise teabe kogumiseks õiguslik alus ning tal on asjaomaseks kahtluseks piisav põhjus.

3.3.3. Andmete säilitamise tähtaja kindlaksmääramise põhimõte

Andmekaitsedirektiivi artikli 6 lõike 1 punkti e ja ka konventsiooni nr 108 artikli 5 punkti e kohaselt peavad liikmesriigid tagama, et „isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega". Kui eesmärgid on täidetud, tuleb andmed seega kustutada.

S. ja Marperi kohtuasjas otsustas EIK, et Euroopa Nõukogu asjakohaste dokumentidega ette nähtud peamiste põhimõtete ning teiste konventsiooniosaliste õigusaktide ja tavade kohaselt peab andmete säilitamine vastama nende kogumise eesmärgile ning sellel peab olema kindel tähtaeg, eeskätt politseis[123].

Isikuandmete säilitamise tähtaeg kehtib aga üksnes andmesubjektide tuvastamist võimaldavate andmete puhul. Andmeid, mida enam ei vajata, saaks seaduslikult säilitada juhul, kui need muudetakse anonüümseks või esitatakse pseudonüümi all.

Andmekaitsedirektiivis on sätestatud selge erand andmete säilitamise kohta edaspidiseks kasutamiseks teaduse, statistika või ajalooga seotud eesmärkidel[124]. Kui andmeid tahetakse säilitada ja kasutada pikema aja jooksul, peavad riigid seejuures oma õigusaktides kehtestama vajalikud tagatised.

3.4. Õiglase töötlemise põhimõte

Põhipunktid

- Õiglane töötlemine tähendab, et selle puhul tagatakse selgus ja arusaadavus, eelkõige andmesubjektide suhtes.

123 EIK, *S. ja Marper vs. Ühendkuningriik*, nr 30562/04 ja 30566/04, 4. detsember 2008; vt ka nt EIK, *M.M. vs. Ühendkuningriik*, nr 24029/07, 13. november 2012.

124 Andmekaitsedirektiivi artikli 6 lõike 1 punkt e.

- Vastutavad töötlejad peavad andmesubjekte teavitama nende andmete töötlemisest, avaldades vähemalt töötlemise eesmärgi ning vastutava töötleja andmed ja aadressi.
- Välja arvatud eraldi õigusaktidega ette nähtud juhtudel, ei tohi isikuandmete töötlemine toimuda salaja ega varjatult.
- Andmesubjektidel on õigus tutvuda oma andmetega, ükskõik kus neid töödeldakse.

Õiglase töötlemise põhimõte mõjutab peamiselt vastutava töötleja ja andmesubjekti suhet.

3.4.1. Selgus ja arusaadavus

Selle põhimõtte alusel peab vastutav töötleja teavitama andmesubjekte sellest, kuidas nende andmeid kasutatakse.

Näide: kohtuasjas *Haralambie vs. Rumeenia*[125] oli arutluse all juhtum, kus kaebuse esitaja taotles juurdepääsu tema kohta salateenistuses hoitud toimikule, kuid tema taotlus rahuldati alles viis aastat hiljem. EIK kinnitas, et inimestele, kelle kohta säilitatakse riigiasutustes isikutoimikuid, on väga oluline, et nad saaksid nende andmetega tutvuda. Ametiasutustel on kohustus tagada tõhus menetlus, mis võimaldaks andmesubjektil kõnealuse teabega tutvuda. EIK väitel ei saanud viieaastast viivitust kaebuse esitaja juurdepääsutaotluse rahuldamisel põhjendada ei liigutatud toimikute kogusega ega arhiivisüsteemi puudustega. Ametiasutused ei olnud taganud kaebuse esitajale tõhusat ja kättesaadavat menetlust, mis oleks tal võimaldanud tutvuda mõistliku aja jooksul oma isikutoimikuga. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Andmetöötlustoiminguid tuleb andmesubjektidele selgitada hõlpsasti mõistetaval viisil, et nad saaks aru, mis nende andmetega tegema hakatakse. Andmesubjektil on samuti õigus sellele, et vastutav töötleja teavitab teda taotluse korral sellest, kas tema andmeid töödeldakse ning milliseid andmeid.

3.4.2. Usalduse loomine

Vastutavad töötlejad peaksid andmesubjektidele ja laiemale avalikkusele konkreetses dokumendis lubama, et nad töötlevad andmeid õiguspärasel ja läbipaistval viisil.

125 EIK, *Haralambie vs. Rumeenia*, nr 21737/03, 27. oktoober 2009.

Andmetöötlustoimingud ei tohi olla salajased ning neil ei tohi olla ettenägematut negatiivset mõju. Vastutavad töötlejad peaksid tagama, et kliente või kodanikke teavitataks nende andmete kasutamisest. Lisaks sellele peavad vastutavad töötlejad võimaluse piires püüdma ilma viivitusteta täita andmesubjekti soove, eeskätt juhul, kui asjaomase andmetöötluse õiguslik alus on andmesubjekti nõusolek.

Näide: kohtuasjas *K.H. jt vs. Slovakkia*[126] esitasid kaebuse kaheksa romast naist, kes viibisid raseduse ja sünnituse ajal ravil kahes Ida-Slovakkia haiglas. Hiljem ei õnnestunud kellelgi neist enam rasestuda, hoolimata korduvatest püüetest. Riigi tasandi kohtud otsustasid, et haiglad peavad lubama kaebuse esitajatel ja nende esindajatel tutvuda asjaomaste meditsiiniandmetega ning teha neist käsitsi väljavõtteid, kuid ei rahuldanud taotlust teha dokumentidest koopiaid, väidetavalt selleks, et vältida nende väärkasutamist. Riikidele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 alusel ette nähtud positiivsed kohustused hõlmavad ilmtingimata ka kohustust tagada andmesubjektidele koopiad nende andmetest. Riik otsustab ise, millisel viisil isikuandmeid sisaldavaid toimikuid kopeeritakse, ning vajaduse korral põhjendab koopiate tegemisest keeldumist. Kaebuse esitajate juhtumis põhjendasid riigi tasandi kohtud meditsiiniandmetest koopiate tegemise keeldu peamiselt sellega, et asjaomast teavet tuleb kaitsta väärkasutamise eest. EIK aga ei mõistnud, kuidas oleksid kaebuse esitajad, kellel lubati igal juhul tutvuda kõikide oma meditsiiniandmetega, saanud väärkasutada iseennast käsitlevat teavet. Peale selle ei olnud kõnealuse väärkasutamise riski ärahoidmiseks vaja tingimata kaebuse esitajad andmete koopiatest ilma jätta, vaid seda oleks saanud teha ka muudel viisidel, näiteks piirates andmetele juurde pääsevate isikute ringi. Riik ei esitanud piisavalt mõjuvaid põhjuseid, miks kaebuse esitajatele ei võimaldatud igakülgset juurdepääsu nende tervist käsitlevatele andmetele. Kohus otsustas, et tegu oli artikli 8 rikkumisega.

Internetiteenuste puhul peavad andmetöötlussüsteemide funktsioonid olema sellised, et andmesubjektid täielikult mõistaksid, mis nende andmetega tehakse.

Õiglane töötlemine tähendab ka seda, et vastutavad töötlejad on valmis minema kaugemale andmesubjektidele teenuste tagamisel õigusaktide alusel kohustuslikest miinimumnõuetest, kui see on andmesubjekti õiguspärastes huvides vajalik.

126 EIK, *K.H. jt vs. Slovakkia*, nr 32881/04, 28. aprill 2009.

3.5. Vastutuse põhimõte

Põhipunktid

- Vastutuse põhimõte tähendab, et vastutavad töötlejad peavad rakendama aktiivselt meetmeid andmekaitse tagamiseks ja edendamiseks andmetöötlustoimingutes.
- Vastutavad töötlejad vastutavad selle eest, et nende andmetöötlustoimingud oleksid kooskõlas andmekaitseõigusega.
- Vastutaval töötlejal peaks olema võimalik mis tahes ajal andmesubjektile, laiemale avalikkusele ja järelevalveasutustele tõendada, et tema andmetöötlustoimingud on kooskõlas andmekaitsealaste õigusnormidega.

Majanduskoostöö ja Arengu Organisatsioon (OECD) võttis 2013. aastal vastu eraelu puutumatust käsitlevad suunised, milles rõhutati, et vastutavad töötlejad mängivad olulist rolli andmekaitse toimimise tagamisel. Suunistes on talletatud vastutuse põhimõte, sätestades, et vastutav töötleja peaks vastutama suunistes kehtestatud põhimõtete jõustamiseks ette nähtud meetmete võtmise eest[127].

Samal ajal kui konventsioonis nr 108 ei viidata vastutavate töötlejate vastutusele, jättes selle küsimuse riikide otsustada, sätestatakse andmekaitsedirektiivi artikli 6 lõikes 2, et andmekvaliteedi põhimõtete (esitatud lõikes 1) järgimise peaks tagama vastutav töötleja.

Näide: õigusaktidest võib vastutuse põhimõtte rõhutamisega seoses esile tõsta eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi 2002/58/EÜ 2009. aasta muutmisdirektiivi[128]. Muudetud artiklis 4 sätestatakse direktiivis turvapoliitika rakendamise kohustus („tagatakse isikuandmete töötlemise turvapoliitika rakendamine"). Seega otsustas seadusandja, et kõnealuses direktiivis käsitletavate turvalisusega seotud sätete puhul on vaja paika panna sõnaselge nõue turvapoliitika kehtestamise ja rakendamise kohta.

127 OECD (2013), „Guidelines on governing the Protection of Privacy and transborder flows of personal data" (e k „Eraelu puutumatuse kaitset ja isikuandmete piiriülest liikumist käsitlevad suunised"), artikkel 14.

128 Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, 25. november 2009, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta, ELT L 337, 2009, lk 11.

Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamuse[129] kohaselt seisneb vastutuse põhiolemus selles, et vastutav töötleja peab:

- võtma meetmed, mis tagaksid tavapärastes tingimustes andmekaitsealaste eeskirjade täitmise andmetöötlustoimingutes;

- tagama dokumendid, millega näidatakse andmesubjektidele ja järelevalveasutustele, milliseid meetmeid on andmekaitsealaste eeskirjade täitmiseks võetud.

Vastutuse põhimõtte alusel peavad vastutavad töötlejad seega aktiivselt üles näitama, et nende tegevus on kooskõlas asjaomaste põhimõtetega, ning mitte üksnes ootama, et andmesubjektid või järelevalveasutused puudustele osutavad.

129 Andmekaitsedirektiivi artikli 29 alusel loodud töörühm, arvamus 3/2010 vastutuse põhimõtte kohta, WP 173, Brüssel, 13. juuli 2010.

4

Euroopa andmekaitseõiguse eeskirjad

EL	Käsitletavad teemad	Euroopa Nõukogu
Eeskirjad mittetundlike andmete seadusliku töötlemise kohta		
Andmekaitsedirektiivi artikli 7 punkt a	Nõusolek	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b ja punkt 3.6
Andmekaitsedirektiivi artikli 7 punkt b	Lepinguline (lepingueelne) suhe	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b
Andmekaitsedirektiivi artikli 7 punkt c	Vastutava töötleja seadusjärgsed kohustused	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt a
Andmekaitsedirektiivi artikli 7 punkt d	Andmesubjekti elulised huvid	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b
Andmekaitsedirektiivi artikli 7 punkt e ja artikli 8 lõige 4 ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008	Avalikud huvid ja avaliku võimu teostamine	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b
Andmekaitsedirektiivi artikkel 7 (f), artikli 8 lõiked 2 ja 3 ELK, liidetud kohtuasjad 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) vs. Administración del Estado*, 24. november 2011	Kaasinimeste õigustatud huvid	Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b

EL	Käsitletavad teemad	Euroopa Nõukogu
Eeskirjad tundlike andmete seadusliku töötlemise kohta		
Andmekaitsedirektiivi artikli 8 lõige 1	Üldine töötlemiskeeld	Konventsiooni nr 108 artikkel 6
Andmekaitsedirektiivi artikli 8 lõiked 2–4	Üldise keelu erandid	Konventsiooni nr 108 artikkel 6
Andmekaitsedirektiivi artikli 8 lõige 5	Süüdimõistvate kohtuotsustega seotud andmete töötlemine	Konventsiooni nr 108 artikkel 6
Andmekaitsedirektiivi artikli 8 lõige 7	Isikukoodide töötlemine	
Eeskirjad turvalise töötlemise kohta		
Andmekaitsedirektiivi artikkel 17	Kohustus tagada töötlemise turvalisus	Konventsiooni nr 108 artikkel 7
		EIK, *I. vs. Soome*, nr 20511/03, 17. juuli 2008
Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 4 lõige 2	Andmetega seotud rikkumistest teavitamine	
Andmekaitsedirektiivi artikkel 16	Kohustus tagada konfidentsiaalsus	
Eeskirjad töötlemise selguse ja arusaadavuse kohta		
	Selgus ja arusaadavus üldises plaanis	Konventsiooni nr 108 artikli 8 punkt a
Andmekaitsedirektiivi artiklid 10 ja 11	Teave	Konventsiooni nr 108 artikli 8 punkt a
Andmekaitsedirektiivi artiklid 10 ja 11	Teatamiskohustuse erandid	Konventsiooni nr 108 artikkel 9
Andmekaitsedirektiivi artiklid 18 ja 19	Teatamine	Profiilide koostamist käsitleva soovituse punkti 9.2 alapunkt a
Eeskirjad nõuetele vastavuse edendamise kohta		
Andmekaitsedirektiivi artikkel 20	Eelkontroll	
Andmekaitsedirektiivi artikli 18 lõige 2	Isikuandmete kaitsega tegelevad ametiisikud	Profiilide koostamist käsitleva soovituse punkt 8.3
Andmekaitsedirektiivi artikkel 27	Tegevusjuhendid	

Põhimõtted on alati üldist laadi. Nende rakendamine konkreetsetes olukordades jätab teatava tõlgendamisruumi ning võimaldab valida eri abinõude vahel. **Euroopa Nõukogu õiguses** saavad konventsiooni nr 108 osalised oma siseriiklike õigusaktidega ise kindlaks määrata, kui suur see tõlgendamisruum täpselt on. **ELi õiguses** on asjad teisiti – selleks et panna siseturul alus andmekaitsele, otsustati, et juba ELi tasandil tuleks rakendada üksikasjalikumaid eeskirju, et liikmesriikide õigusaktidega tagatud andmekaitse tase oleks ühtlane. Andmekaitsedirektiivi artiklis 6 esitatud põhimõtetes kehtestatakse rida üksikasjalikke eeskirju, mida riigid peavad oma õigusaktides aktiivselt rakendama. Seepärast on alljärgnevalt esitatud tähelepanekud Euroopa tasandi üksikasjalike andmekaitsealaste eeskirjade kohta peamiselt seotud ELi õigusega.

4.1. Eeskirjad seadusliku töötlemise kohta

Põhipunktid

- Isikuandmete töötlemine on seaduslik, kui:
  - see põhineb andmesubjekti nõusolekul;
  - see on vajalik andmesubjekti eluliste huvide kaitsmiseks;
  - see on vajalik teiste inimeste õigustatud huvide elluviimiseks, kui selliseid huve ei kaalu üles andmesubjektide põhiõiguste kaitsmisega seotud huvid.
- Tundlike isikuandmete töötlemise seaduslikkuse tagamiseks peab töötlemine vastama rangematele erinõuetele.

Andmekaitsedirektiivis on andmete seaduslikku töötlemist käsitlevad eeskirjad jagatud kahte rühma: mittetundlike andmete töötlemise eeskirjad artiklis 7 ja tundlike andmete töötlemise eeskirjad artiklis 8.

4.1.1. Mittetundlike andmete seaduslik töötlemine

Direktiivi 95/46/EÜ II peatükis „Üldised eeskirjad isikuandmete töötlemise seaduslikkuse kohta" sätestatakse, et isikuandmete töötlemine peab esiteks vastama andmekaitsedirektiivi artiklis 6 esitatud põhimõtetele andmekvaliteedi kohta ning teiseks ühele artiklis 7 esitatud andmetöötluse seaduslikkuse kriteeriumile, juhul kui

artikliga 13 ette nähtud eranditest ei tulene teisiti[130]. See selgitab, millistel juhtudel on mittetundlike isikuandmete töötlemine seaduslik.

Nõusolek

Euroopa Nõukogu õiguses ei ole nõusolekut käsitletud ei Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 ega konventsioonis nr 108. Küll aga on sellele osutatud EIK kohtupraktikas ning mitmes Euroopa Nõukogu soovituses. **ELi õiguses** on nõusolek seadusliku andmetöötluse alusena kehtestatud andmekaitsedirektiivi artikli 7 punktis a ning sellele on sõnaselgelt viidatud ka põhiõiguste harta artiklis 8.

Lepinguline suhe

Veel üks isikuandmete seadusliku töötlemise alus on **ELi õiguses** see, kui „töötlemine on vajalik sellise lepingu täitmiseks, mille osapool andmesubjekt on, või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele" (andmekaitsedirektiivi artikli 7 punkt b). See säte hõlmab ka lepingueelseid suhteid. Näide: üks pool kavatseb sõlmida lepingu, kuid ei ole seda veel teinud, võibolla sellepärast, et teatavad kontrollid on veel lõpetamata. Kui tal on vaja selleks tarbeks töödelda andmeid, on selline töötlemine seaduslik, kui see on vajalik „lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele".

Euroopa Nõukogu õiguses on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 sätestatud, et isikuandmete kaitse õiguse kasutamisse ei sekkuta muidu, kui see on vajalik muu hulgas kaasinimeste õiguste ja vabaduste kaitseks.

Vastutava töötleja seadusjärgsed kohustused

ELi õiguses osutatakse sõnaselgelt veel ühele andmetöötluse seaduslikkuse kriteeriumile: „töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks" (andmekaitsedirektiivi artikli 7 punkt c). See säte hõlmab erasektoris tegutsevaid vastutavaid töötlejaid; avaliku sektori vastutavate töötlejate seadusjärgsed

130 ELK, liidetud kohtuasjad C-465/00, C-138/01 ja C-139/01, *Österreichischer Rundfunk jt*, 20. mai 2003, punkt 65; ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008, punkt 48; ELK, liidetud kohtuasjad 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) vs. Administración del Estado*, 24. november 2011, punkt 26.

kohustused kuuluvad direktiivi artikli 7 punkti e kohaldamisalasse. Tihti on erasektori vastutavad töötlejad õigusaktide alusel kohustatud töötlema teiste inimeste andmeid; näiteks on arstidel ja haiglatel seadusjärgne kohustus säilitada mitme aasta jooksul patsientide raviandmeid, tööandjad peavad oma töötajaid käsitlevaid andmeid töötlema sotsiaalkindlustuse ja maksustamisega seotud eesmärkidel ning ettevõtjad peavad töötlema oma kliente käsitlevaid andmeid maksustamisega seotud eesmärkidel.

Seoses sellega, et lennuettevõtjad peavad edastama reisijaandmeid teiste riikide sisserände kontrolli asutustele, on tekkinud küsimus, kas *välisriigi* õigusaktidest tulenevad kohustused tagavad õigusliku aluse andmetöötluseks ELi õigusaktide alusel (seda küsimust käsitletakse üksikasjalikumalt jaotises 6.2).

Ka **Euroopa Nõukogu õiguses** käsitletakse vastutava töötleja seadusjärgseid kohustusi andmetöötluse õigusliku alusena. Nagu juba eespool osutatud, on erasektori vastutavate töötlejate seadusjärgsete kohustuste puhul tegu vaid ühe konkreetse kaasinimeste õigustatud huvide alla kuuluva juhtumiga Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 tähenduses. Seepärast kehtib esitatud näide ka Euroopa Nõukogu õiguse puhul.

Andmesubjekti elulised huvid

ELi õiguses sätestatakse andmekaitsedirektiivi artikli 7 punktis d, et isikuandmeid võib töödelda juhul, kui „töötlemine on vajalik andmesubjekti eluliste huvide kaitsmiseks". Sellised huvid, mis on tihedalt seotud andmesubjekti elu ja surmaga, võivad anda õigusliku aluse näiteks terviseandmete ja kadunud isikuid käsitlevate andmete kasutamiseks.

Euroopa Nõukogu õiguses ei kuulu andmesubjekti elulised huvid Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 osutatud põhjuste alla, mille puhul on sekkumine isikuandmete kaitse õigusesse põhjendatud. Mõnes konventsiooni nr 108 alusel konkreetsetes küsimustes avaldatud Euroopa Nõukogu soovituses aga on andmesubjekti elulisi huvisid seevastu ühemõtteliselt käsitletud andmetöötluse õigusliku alusena[131]. Arvatakse, et andmesubjekti elulised huvid peaksid ilmselgelt kuuluma andmetöötlust põhjendavate aluste alla – põhiõiguste kaitsmisel ei tohiks kunagi ohtu seada kaitstava isiku elulisi huvisid.

131 Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b.

Avalikud huvid ja avaliku võimu teostamine

Pidades silmas võimalusterohkust avalike suhete korraldamisel, sätestatakse andmekaitsedirektiivi artikli 7 punktis e, et isikuandmeid võib töödelda juhul, kui see „on vajalik üldiste huvidega seotud ülesande täitmiseks või sellise avaliku võimu teostamiseks, mis on tehtud ülesandeks volitatud töötlejale või andmeid saavale kolmandale isikule[...]"[132].

Näide: kohtuasjas *Huber vs. Saksamaa*[133] käsitleti juhtumit, kus Saksamaal elanud Austria kodanik (Huber) esitas föderaalsele migratsiooni- ja pagulasametile taotluse kustutada välismaalaste keskregistrist tema andmed. Selles registris hoitakse isikuandmeid teistest ELi riikidest pärit inimeste kohta, kes ei ole Saksamaa kodanikud, kuid elavad Saksamaal kauem kui kolm kuud; seda kasutatakse statistika eesmärgil ning seda kasutavad ka õiguskaitseasutused ja kohtud kuritegelike või avalikku julgeolekut ohustavate tegude uurimisel ja lahendamisel. Eelotsusetaotluse esitanud kohus küsis, kas isikuandmete töötlemine sellises registris nagu välismaalaste keskregister, millele on juurdepääs ka teistel riigiasutustel, on kooskõlas ELi õigusega, võttes arvesse, et Saksamaa kodanike puhul sellist registrit ei kasutata.

Esiteks leidis ELK, et andmekaitsedirektiivi artikli 7 punkti e alusel on isikuandmete töötlemine õiguspärane üksnes juhul, kui töötlemine on vajalik avalike huvidega või avaliku võimu teostamisega seotud ülesande täitmiseks.

Kohus märkis, et „arvestades eesmärki tagada kõigis liikmesriikides võrdne kaitse, ei või direktiivi 95/46 artikli 7 punktis e sisalduval vajalikkuse mõistel [...] olla sõltuvalt liikmesriigist erinev sisu. Järelikult on see ühenduse õiguse autonoomne mõiste, mida tuleb tõlgendada nii, et see oleks täielikult kooskõlas nimetatud direktiivi eesmärgiga, mis on määratletud selle artikli 1 lõikes 1"[134].

Kohus märkis, et liidu kodaniku õigus elada liikmesriigis, mille kodanik ta ei ole, ei ole tingimusteta, vaid võib olla allutatud asutamislepinguga ja selle rakendamiseks võetud meetmetega kehtestatud piirangutele ja tingimustele. Kui sellise välismaalaste keskregistri taolise registri kasutamine elamisõigust käsitlevate õigusnormide kohaldamise eest vastutavate ametiasutuste abistamiseks

132 Andmekaitsedirektiivi 32. põhjendus.

133 ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008.

134 *Ibid.*, punkt 52.

on põhimõtteliselt õiguspärane, ei tohi selline register sisaldada muud teavet peale selle, mis on vajalik asjaomasel eesmärgil. Kohus järeldas, et selline isikuandmete töötlemise süsteem on ELi õigusega kooskõlas üksnes juhul, kui see sisaldab asjaomaste õigusnormide kohaldamiseks vajalikku teavet ning kui selle tsentraliseeritus võimaldab neid õigusnorme tõhusamalt kohaldada. Eelotsusetaotluse teinud kohtule määrati ülesandeks kontrollida, kas kõnealuses kohtuasjas on need tingimused täidetud. Kui need tingimused ei ole täidetud, ei saa sellises registris nagu välismaalaste keskregister isikuandmete säilitamist ja töötlemist statistika eesmärgil mingil juhul pidada vajalikuks direktiivi 95/46/EÜ artikli 7 lõike e tähenduses[135].

Seoses registris sisalduvate andmete kasutamisega kuritegevusevastase võitluse eesmärgil leidis kohus, et kõnealune eesmärk on „kindlasti toimepandud kuritegude ja muude õigusrikkumiste lahendamine, sõltumata nende toimepanijate kodakondsusest". Välismaalaste keskregister ei sisalda asjaomase liikmesriigi kodanike isikuandmeid ning sellise erineva kohtlemise puhul on tegu ELi toimimise lepingu artikli 18 alusel keelatud diskrimineerimisega. Järelikult tuleb seda sätet kohtu sõnul tõlgendada nii, et „sellega on vastuolus liikmesriigi poolt kuritegevuse vastase võitluse eesmärgil spetsiaalse välismaalastest liidu kodanike isikuandmete töötlemise süsteemi rajamine"[136].

Isikuandmete kasutamise suhtes avalikus sfääris tegutsevate ametiasutuste poolt kohaldatakse ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Vastutava töötleja või kolmanda isiku õigustatud huvid

Õigustatud huvisid ei ole ainult andmesubjektidel. Andmekaitsedirektiivi artikli 7 punkti f kohaselt võib isikuandmeid töödelda juhul, kui „töötlemine on vajalik vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide elluviimiseks, kui selliseid huve ei kaalu üles [...] kaitstavate andmesubjekti põhiõiguste ja -vabadustega seotud huvid".

Järgmisena kirjeldatud kohtuotsuses põhines ELK otsus otseselt direktiivi artikli 7 punktil f.

135 *Ibid.*, punktid 54, 58, 59, 66–68.

136 *Ibid.*, punktid 78 ja 81.

Näide: *ASNEFi ja FECEMDi*[137] kohtuasjas täpsustas ELK, et liikmesriigid ei tohi oma õigusaktidega lisada andmekaitsedirektiivi artikli 7 punktis f esitatud kriteeriumidele uusi andmetöötluse seaduslikkust käsitlevaid kriteeriume. See oli ajendatud juhtumist, kus Hispaania andmekaitseõigus hõlmas sätet, mille alusel teised eraõiguslikud isikud said seoses isikuandmete töötlemisega tugineda õigustatud huvile, kui selline teave oli juba avaldatud avalikkusele kättesaadavates allikates.

Esiteks märkis kohus, et direktiivi 95/46/EÜ eesmärk on viia isikuandmete töötlemisega seonduv üksikisikute õiguste ja vabaduste kaitse kõigis liikmesriikides samale tasemele. Samuti lisati, et selle valdkonna õigusaktide ühtlustamise tagajärjel ei tohi nendega pakutav kaitse väheneda. Selle asemel peab liidus tagatava kaitstuse tase olema kõrgem[138]. ELK järeldas, et „[s]eega tuleneb eesmärgist tagada kõigis liikmesriikides võrdväärne kaitstuse tase, et direktiivi 95/46 artikkel 7 näeb ette ammendava ja piirava loetelu juhtudest, millal isikuandmete töötlemist võib pidada seaduslikuks". Peale selle järeldub sellest, „et liikmesriigid ei saa lisada direktiivi 95/46 artiklile 7 uusi isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume ega kehtestada täiendavaid nõudeid, mis muudavad selles artiklis sätestatud kuuest kriteeriumist mõne kriteeriumi ulatust"[139]. Kohus tunnistas, et „[m]is puudutab vajalikku kaalumist direktiivi 95/46 artikli 7 punkti f alusel, siis on võimalik võtta arvesse asjaolu, et nimetatud töötlemisega andmesubjekti põhiõigustele kaasneva riive raskus võib sõltuda sellest, kas asjaomased andmed on juba esitatud avalikkusele kättesaadavates allikates või ei ole seda tehtud".

Seevastu on „selle direktiivi artikli 7 punktiga f vastuolus, kui liikmesriik välistab kategooriliselt ja üldiselt teatud isikuandmete kategooriate töötlemise, ilma et lubatud oleks kaaluda konkreetsel juhtumil vastanduvaid õigusi ja huve".

Nende tähelepanekute põhjal otsustas kohus, et „direktiivi 95/46/EÜ [...] artikli 7 punkti f tuleb tõlgendada nii, et sellega on vastuolus siseriiklikud õigusnormid, mis nõuavad selleks, et ilma andmesubjekti nõusolekut küsimata võiks

137 ELK, liidetud kohtuasjad 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) vs. Administración del Estado*, 24. november 2011.

138 *Ibid.*, punkt 28. Andmekaitsedirektiivi 8. ja 10. põhjendus.

139 ELK, liidetud kohtuasjad 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) vs. Administración del Estado*, 24. november 2011, punktid 30 ja 32.

tema isikuandmeid töödelda, mis on vajalik vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huvide elluviimiseks, lisaks sellele, et ei tohi rikkuda andmesubjekti põhiõigusi ja -vabadusi, ka seda, et kõnealused andmed oleksid avalikkusele kättesaadavates allikates, välistades seega kategooriliselt ja üldiselt kõikide nende andmete töötlemise, mis ei sisaldu sellistes allikates"[140].

Sarnaseid tähelepanekuid on tehtud ka Euroopa Nõukogu soovitustes. Profiilide koostamist käsitleva soovituse järgi on isikuandmete töötlemine profiilide koostamise eesmärgil õiguspärane, kui see on vajalik kaasinimeste õigustatud huvide seisukohalt, kui selliseid huve ei kaalu üles andmesubjektide põhiõigused ja vabadused[141].

4.1.2. Tundlike andmete seaduslik töötlemine

Euroopa Nõukogu õiguses võivad riigid seoses tundlike andmete kasutamisega ise otsustada asjakohaste kaitsemeetmete üle, samal ajal kui **ELi õiguses** on andmekaitsedirektiivi artikliga 8 ette nähtud üksikasjalik süsteem selliste andmekategooriate töötlemiseks, mis paljastavad rassilise või etnilise päritolu, poliitilised vaated, usulised või filosoofilised veendumused, ametiühingusse kuulumise või tervislikku seisundit või seksuaalelu käsitlevad andmed. Põhimõtteliselt on tundlike andmete töötlemine keelatud[142]. Direktiivi artikli 8 lõigetes 2 ja 3 on aga esitatud täielik loetelu selle põhimõtte eranditest. Need erandid hõlmavad andmesubjekti sõnaselget nõusolekut, andmesubjekti elulisi huvisid, teiste inimeste õigustatud huvisid ning avalikku huvi.

Erinevalt mittetundlike andmete töötlemisest ei saa tundlike andmete töötlemise seaduslikkuse puhul tugineda üldjoontes lepingulisele suhtele andmesubjektiga. Kui andmesubjektiga sõlmitud lepingu raamistikus soovitakse töödelda tundlikke andmeid, peab andmesubjekt seega lepingu sõlmimisega nõustumise kõrval andma eraldi nõusoleku kõnealuste andmete kasutamiseks. Kui andmesubjekt avaldab sõnaselgelt soovi teatavate kaupade või teenuste järele, mis paljastavad ilmtingimata tundlikke andmeid, peaks selline olukord aga olema sõnaselge nõusolekuga samaväärne.

140 *Ibid.*, punktid 40, 44, 48 ja 49.

141 Profiilide koostamist käsitleva soovituse punkti 3.4 alapunkt b.

142 Andmekaitsedirektiivi artikli 8 lõige 1.

Näide: kui lennureisija palub lendu broneerides lennuettevõtjalt ratastooli ja košš er-toitlustamist, võib lennuettevõtja neid andmeid kasutada ka juhul, kui reisija ei andnud eraldi kirjalikku nõusolekut, millega ta oleks lubanud kasutada oma tervislikku seisundit ja usulisi veendumusi käsitlevaid üksikasju sisaldavaid andmeid.

Andmesubjekti sõnaselge nõusolek

Andmetöötluse seaduslikkuse peamine tingimus on – hoolimata andmete tundlikkusest või mittetundlikkusest – andmesubjekti nõusolek. Tundlike andmete puhul peab andmesubjekti nõusolek olema antud sõnaselgelt. Riigid võivad aga oma õigusaktidega ette näha, et tundlike andmete kasutamisega nõustumine ei ole piisav õiguslik alus nende töötlemise lubamiseks[143] näiteks olukorras, kus andmetöötlus võib andmesubjektile erandjuhtudel kaasa tuua tavapäratuid riske.

Ühel konkreetsel juhul käsitatakse tundlike andmete töötlemise õigusliku alusena isegi kaudset nõusolekut. Andmekaitsedirektiivi artikli 8 lõike 2 punkti e kohaselt ei ole töötlemine keelatud, kui töödeldakse andmeid, mille andmesubjekt on ilmselgelt avalikustanud. Selle sätte puhul lähtutakse endastmõistetavalt eeldusest, et kui andmesubjekt on ise oma andmed avalikustanud, vihjab see sellele, et ta on nõus oma andmete kasutamisega.

Andmesubjekti elulised huvid

Nagu mittetundlike andmete puhul, võib ka tundlikke andmeid töödelda juhul, kui see on andmesubjekti elulistes huvides[144].

Tundlike andmete töötlemine andmesubjekti elulistes huvides on õiguspärane juhul, kui andmesubjektilt ei olnud võimalik küsida nõusolekut, kuna ta oli näiteks teadvusetu, teda ei olnud kohal või teda ei õnnestunud kätte saada.

Kaasinimeste õigustatud huvid

Nagu mittetundlike andmete puhul, võib ka tundlike andmete töötlemise õigusliku alusena käsitada teiste inimeste õigustatud huvisid. Tundlike andmete puhul kehtib see andmekaitsedirektiivi artikli 8 lõike 2 kohaselt aga üksnes järgmistel juhtudel:

143 *Ibid.*, artikli 8 lõike 2 punkt a.

144 *Ibid.*, artikli 8 lõike 2 punkt c.

- töötlemine on vajalik selleks, et kaitsta mõne teise isiku elulisi huve,[145] kui andmesubjekt on füüsiliselt või õiguslikult võimetu oma nõusolekut andma;

- tundlikke andmeid on vaja töödelda tööõiguse valdkonnas, näiteks terviseandmeid, kui tegu on eriti ohtliku töökeskkonnaga, või andmeid usuliste veendumuste kohta seoses puhkustega[146];

- poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega sihtasutused, ühendused või muud mittetulunduslikud asutused töötlevad andmeid oma liikmete, toetajate või teiste huvitatud isikute kohta (need andmed on tundlikud seepärast, et need võivad paljastada asjaomaste isikute usulised või poliitilised veendumused)[147];

- tundlikke andmeid kasutatakse kohtu- või haldusasutuste menetlustes õigusnõude koostamiseks, esitamiseks või kaitsmiseks[148].

- Peale selle hõlmavad erandid andmekaitsedirektiivi artikli 8 lõike 3 kohaselt ka tervishoiuteenuste juhtimist, mille puhul tervishoiuteenuste pakkujad kasutavad terviseandmeid meditsiinilise läbivaatuse ja ravi jaoks. Eritagatisena käsitatakse isikuid tervishoiuteenuste pakkujatena üksnes juhul, kui nad täidavad teatavaid konfidentsiaalsusega seotud kutsealaseid kohustusi.

Avalik huvi

Samuti tuleks märkida, et andmekaitsedirektiivi artikli 8 lõike 4 kohaselt võivad liikmesriigid kehtestada täiendavaid eesmärke, mille jaoks võib töödelda tundlikke andmeid, juhul kui:

- töötlemine on seotud märkimisväärse avaliku huviga;

- need kehtestatakse siseriikliku õiguse või järelevalveasutuse otsusega;

145 *Ibid.*

146 *Ibid.*, artikli 8 lõike 2 punkt b.

147 *Ibid.*, artikli 8 lõike 2 punkt d.

148 *Ibid.*, artikli 8 lõike 2 punkt e.

- siseriiklik õigus või järelevalveasutuse otsus hõlmab sobivaid tagatisi, mis võimaldavad tõhusalt kaitsta andmesubjektide huvisid[149].

Hea näide on sellega seoses elektroonilised terviseregistrid, mis paljudes liikmesriikides peagi luuakse. Selliste süsteemide kaudu saavad tervishoiuteenuste pakkujad teha patsiendi ravi ajal kogutud terviseandmed kättesaadavaks teistele tervishoiuteenuste pakkujatele, kes asjaomase patsiendiga tegelevad; süsteem võimaldab laiahaardelist ja enamasti riigiülest andmete edastamist.

Andmekaitsedirektiivi artikli 29 alusel loodud töörühm järeldas, et praegused andmekaitsedirektiivi artikli 8 lõike 3 alusel toimuvat patsiendiandmete töötlemist käsitlevad õigusnormid selliste süsteemide loomist ei võimalda. Kuna kõnealused elektroonilised terviseregistrid pakuvad olulist avalikku huvi, võiks nende loomisel lähtuda direktiivi artikli 8 lõikest 4, mille kohaselt peaks süsteemide loomiseks olema otsene õiguslik alus ning seejuures tuleks ette näha vajalikud tagatised, mis kindlustaks süsteemi turvalise rakendamise[150].

4.2. Eeskirjad turvalise töötlemise kohta

Põhipunktid

- Andmetöötluse turvalisust käsitlevad eeskirjad hõlmavad vastutava töötleja ja volitatud töötleja kohustust võtta sobivaid tehnilisi ja korralduslikke meetmeid, et hoida andmetöötlustoimingute puhul ära mis tahes ebaseaduslikke sekkumisi.
- Andmete turvalisuse vajaliku taseme määravad ära:
  - konkreetse andmetöötlusliigi puhul turul saadaolevad turvafunktsioonid;
  - kulud;
  - töödeldavate andmete tundlikkus.
- Andmete töötlemise turvalisuse tagab ka kõikidele isikutele, vastutavatele töötlejatele või volitatud töötlejatele määratud üldkohustus hoida andmeid konfidentsiaalsena.

149 *Ibid.*, artikli 8 lõige 4.

150 Andmekaitsedirektiivi artikli 29 alusel loodud töörühm, 2007, töödokument, milles käsitletakse elektroonilisele tervisekaardile kantavate tervisealaste isikuandmete töötlemist, WP 131, Brüssel, 15. veebruar 2007.

Seega on vastutavate töötlejate ja volitatud töötlejate kohustus võtta asjakohaseid meetmeid andmeturbe tagamiseks sätestatud nii **Euroopa Nõukogu** kui ka **ELi andmekaitseõiguses**.

4.2.1. Andmeturbe elemendid

ELi asjakohastes õigusnormides on sätestatud:

> *„Liikmesriigid näevad ette, et vastutav töötleja peab rakendama vajalikke tehnilisi ja organisatsioonilisi meetmeid kaitsmaks isikuandmeid juhusliku või ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest, eelkõige juhul, kui töötlemine hõlmab andmete edastamist võrgu kaudu, ning igasuguse muu võimaliku ebaseadusliku töötlemise eest"*[151].

Sarnane säte on talletatud ka **Euroopa Nõukogu õiguses**:

> *„Automatiseeritud andmekogudes säilitatavate isikuandmete tahtmatu või tahtliku hävitamise, kaotsimineku, aga ka omavolilise juurdepääsu, muutmise või levitamise eest kaitsmiseks võetakse kasutusele kohased turvameetmed"*[152].

Sageli on andmete turvalise töötlemise tagamiseks kehtestatud ka tööstus-, riikide tasandi ja rahvusvahelisi standardeid. Näiteks uuritakse ELi üleeuroopaliste telekommunikatsioonivõrkude (eTEN) projektide hulka kuuluva Euroopa eraelu puutumatuse märgiste süsteemi (EuroPriSe) raamistikus toodete, eeskätt tarkvara sertifitseerimise võimalusi Euroopa andmekaitseõiguse nõuete alusel. Selleks et suurendada ELi, selle liikmesriikide ja ettevõtjaskonna suutlikkust võrgu- ja infoturbe probleemide ärahoidmisel, käsitlemisel ja lahendamisel, loodi Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA)[153]. ENISA avaldab regulaarselt analüüse ähvardavate turvariskide kohta ning annab nõu, kuidas nendega tegeleda.

151 Andmekaitsedirektiivi artikli 17 lõige 1.

152 Konventsiooni nr 108 artikkel 7.

153 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 460/2004, 10. märts 2004, millega luuakse Euroopa Võrgu- ja Infoturbeamet, ELT L 77, 2004.

Andmeturbe jaoks ei ole vaja üksnes õigeid vahendeid, st riist- ja tarkvara. Vaja on ka asjakohaseid organisatsioonilisi sisekorraeeskirju. Sellised sisekorraeeskirjad võiksid ideaalis hõlmata järgmist:

- kõikide töötajate regulaarne teavitamine andmeturvet käsitlevatest eeskirjadest ning nende kohustustest andmekaitseõiguse alusel, eeskätt konfidentsiaalsusega seotud kohustustest;
- selge vastutuse jaotus ja volituste kirjeldus andmekaitseküsimustes, eeskätt isikuandmete töötlemist ja nende kolmandatele isikutele edastamist käsitlevates otsustes;
- isikuandmete kasutamine üksnes kooskõlas pädeva isiku juhtnööridega või organisatsioonis kehtestatud üldeeskirjadega;
- meetmed, millega kaitstakse ligipääsu vastutava töötleja või volitatud töötleja asjaomastele asukohtadele ning riist- ja tarkvarale, sealhulgas juurdepääsuloa olemasolu kontrollimine;
- veendumine, et isikuandmetega tutvumiseks on loa andnud pädev isik ning et esitatud on vajalikud dokumendid;
- automaattoimingud seoses elektroonilise juurdepääsuga isikuandmetele ning selliste toimingute regulaarne kontroll organisatsioonisisese järelevalveisiku vastutusel;
- põhjalikud dokumendid sellise andmete avaldamise kohta, mille puhul ei ole juurdepääs olnud automatiseeritud, eesmärgiga näidata, et ei ole toimunud andmete ebaseaduslikku edastamist.

Tõhusate turvalisusega seotud ettevaatusabinõude tagamisel mängib olulist rolli ka töötajatele andmeturbe küsimustes asjakohase koolituse ja õppe pakkumine. Samuti tuleb paika panna kontrollimenetlused, mille abil tagada kindlaksmääratud asjakohaste meetmete võtmine ja toimimine praktikas (nt sise- või välisauditid).

Vastutav töötleja või volitatud töötleja saab turvalisust parandada ka järgmiste meetmete abil: isikuandmete kaitsega tegelevate ametiisikute määramine, töötajate turvalisuskoolitus, korrapärased auditid, turvaaukude otsimise testid ja kvaliteedimärgised.

Näide: kohtuasjas *I. vs. Soome*[154] käsitleti juhtumit, kus kaebuse esitajal ei õnnestunud tõendada, et tema terviseandmeid olid ebaseaduslikult vaadanud tema kolleegid haiglast, kus ta töötas. Seepärast ei rahuldanud riigi tasandi kohtud tema kaebust selle kohta, et tema õigust isikuandmete kaitsele oli rikutud. EIK otsustas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega, kuna haigla terviseandmete registreerimise süsteem oli üles ehitatud nii, et tagantjärele ei olnud võimalik patsiendiandmete kasutamist kindlaks teha, sest süsteem näitas üksnes viit kõige viimast kasutuskorda, ning pealegi kustutati see teave kohe, kui asjaomane toimik arhiivi tagasi viidi. Kohtu arvates oli otsustav tegur asjaolu, et haiglas kasutusel olnud registreerimissüsteem ei olnud ilmselgelt kooskõlas Soome õigusnormidega, kusjuures riigi tasandi kohtud ei olnud sellele nüansile piisaval määral tähelepanu pööranud.

Andmetega seotud rikkumistest teavitamine

Mitme Euroopa riigi andmekaitseõiguses on kasutusele võetud uus vahend andmeturbe rikkumise probleemiga tegelemiseks – elektroonilise side teenuse osutajad peavad andmetega seotud rikkumistest teatama tõenäolistele ohvritele ja järelevalveasutustele. Elektroonilise side teenuse osutajatele on see ELi õiguse alusel kohustuslik[155]. Andmesubjektidele tuleb andmetega seotud rikkumistest teavitada, sest rikkumistest ja nende võimalikest tagajärgedest teada andmine vähendab andmesubjektidele avalduva kahjuliku mõju riski. Raske hooletuse korral võidakse teenuseosutajaid ka trahvida.

Teenuseosutajad peavad ennetavalt kehtestama sisemenetlused turvarikkumiste tõhusaks haldamiseks ja nendest teavitamiseks, kuna andmesubjektidele ja/või järelevalveasutusele tuleb siseriiklike õigusaktide alusel teada anda üldiselt üsna aegsasti.

154 EIK, *I. vs. Soome*, nr 20511/03, 17. juuli 2008.

155 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 2002, artikli 4 lõige 3, mida on muudetud Euroopa Parlamendi ja nõukogu direktiiviga 2009/136/EÜ, 25. november 2009, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta, ELT L 337, 2009.

4.2.2. Konfidentsiaalsus

ELi õiguses tagab andmete töötlemise turvalisuse ka kõikidele isikutele, vastutavatele töötlejatele või volitatud töötlejatele määratud üldkohustus hoida andmeid konfidentsiaalsena.

Näide: kindlustusettevõtte töötajale helistab tööl isik, kes väidab, et ta on klient ning nõuab teavet enda kindlustuslepingu kohta.

Kuna töötaja peab hoidma klientide andmeid konfidentsiaalsena, peab ta enne isikuandmete avaldamist kasutusele võtma vähemalt minimaalsed turvameetmed. Näiteks võib kõnealusele isikule välja pakkuda, et teenindaja helistab tagasi kliendi toimikus esitatud telefoninumbrile.

Andmekaitsedirektiivi artiklis 16 käsitletakse konfidentsiaalsust üksnes vastutava töötleja ja volitatud töötleja suhte seisukohalt. Seda, kas vastutavad töötlejad peavad hoidma andmeid konfidentsiaalsena, st ei tohi neid avaldada kolmandatele isikutele, käsitletakse direktiivi artiklites 7 ja 8.

Konfidentsiaalsuskohustus ei kehti olukordades, kus isik tutvub andmetega eraisikuna ning mitte vastutava töötleja või volitatud töötleja töötajana. Sel juhul andmekaitsedirektiivi artikkel 16 ei kehti, sest olukord, kus isikuandmeid kasutab eraisik, ei kuulu andmekaitsedirektiivi kohaldamisalasse, kui see mahub nn koduse kasutamise erandi alla[156]. See erand kehtib juhul, kui isikuandmeid kasutab „füüsiline isik isiklikel või kodustel eesmärkidel"[157]. Alates ELK otsusest *Bodil Lindqvisti*[158] kohtuasjas tuleb seda erandit aga tõlgendada kitsendavalt, eeskätt seoses andmete avaldamisega. Eeskätt ei laiene kõnealune erand isikuandmete avaldamisele internetis piiramatule arvule vastuvõtjatele (seda kohtuasja on täpsemalt käsitletud jaotistes 2.1.2, 2.2, 2.3.1 ja 6.1).

Euroopa Nõukogu õiguses vihjatakse konfidentsiaalsuskohustusele konventsiooni nr 108 artiklis 7 andmeturbe käsitlemisel.

Volitatud töötlejate puhul tähendab konfidentsiaalsuskohustus, et nad võivad vastutavalt töötlejalt saadud isikuandmeid kasutada ainult kooskõlas tolle juhtnööridega.

156 Andmekaitsedirektiivi artikli 3 lõike 2 teine taane.

157 *Ibid.*

158 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003.

Ka vastutava töötleja või volitatud töötleja töötajad võivad isikuandmeid konfidentsiaalsusnõuete alusel kasutada üksnes oma pädeva ülemuse juhtnööre järgides.

Konfidentsiaalsuskohustus tuleb hõlmata kõikidesse vastutavate töötlejate ja nende volitatud töötlejate vahel sõlmitavatesse lepingutesse. Samuti peavad vastutavad töötlejad ja volitatud töötlejad võtma konkreetseid meetmeid oma töötajatele konfidentsiaalsuskohustuse kindlaksmääramiseks juriidilisel tasandil, tavaliselt töölepingutesse konfidentsiaalsusklauslite lisamisega.

Konfidentsiaalsusega seotud töökohustuste rikkumine on kriminaalkorras karistatav paljudes ELi riikides ja konventsiooni nr 108 osalisriikides.

4.3. Eeskirjad töötlemise selguse ja arusaadavuse kohta

Põhipunktid

- Enne isikuandmete töötlemist peab vastutav töötleja avaldama andmesubjektidele vähemalt vastutava töötleja andmed ja andmetöötluse eesmärgi, kui andmesubjekt ei ole sellest veel teadlik.
- Kui andmed on pärit kolmandalt isikult, ei kehti teabe avaldamise kohustus juhul, kui:
  - andmetöötlus on sätestatud õigusaktidega;
  - sellise teabe andmine osutub võimatuks või eeldab ülemääraseid jõupingutusi.
- Enne isikuandmete töötlemist peab vastutav töötleja samuti:
  - teatama järelevalveasutusele kavandatavatest andmetöötlustoimingutest;
  - tagama, et isikuandmete kaitsega tegelev sõltumatu ametiisik koostab andmetöötlust käsitlevad sisedokumendid, kui selline menetlus on õigusaktidega ette nähtud.

Õiglase töötlemise põhimõtte kohaselt peab andmetöötlus olema selge ja arusaadav. Sellega seoses on **Euroopa Nõukogu õiguses** kehtestatud, et isikule peab olema võimaldatud teha kindlaks andmetöötlusfailide olemasolu, nende eesmärk ja vastutav töötleja[159]. Kuidas see täpselt toimuma peaks, otsustavad riigid oma õigusakti-

159 Konventsiooni nr 108 artikli 8 punkt a.

des ise. **ELi õigus** on selles küsimuses konkreetsem – selguse ja arusaadavuse tagab andmesubjektile vastutava töötleja kohustus talle teavet anda ning laiema üldsuse puhul tagab selguse ja arusaadavuse teavitamine.

Mõlemas õiguskorras võivad riigid oma õiguses kohaldada vastutavate töötlejate suhtes selguse ja arusaadavusega seoses kehtivate kohustuste erandeid ja piiranguid, kui seda on vaja, et kaitsta avalikke huvisid, andmesubjekti või teiste isikute õigusi ja vabadusi ning need on demokraatlikus ühiskonnas vajalikud[160]. Sellised erandid võivad vajalikuks osutuda näiteks kuritegude uurimisel, kuid võivad olla põhjendatud ka muudel tingimustel.

4.3.1. Teave

Nii Euroopa Nõukogu kui ka ELi õiguses peavad andmetöötlustoimingute vastutavad töötlejad andmesubjektile kavandatavast töötlemisest ette teatama[161]. Seda kohustust ei täideta andmesubjekti taotlusel, vaid vastutav töötleja peab seda täitma proaktiivselt, sõltumata sellest, kas andmesubjekt tunneb kõnealuse teabe vastu huvi või mitte.

Teabe sisu

Asjaomases teabes tuleb avaldada töötlemise eesmärk, samuti andmed vastutava töötleja isiku kohta ja tema kontaktandmed[162]. Andmekaitsedirektiivi kohaselt peab esitama lisateavet, kui „selline täiendav teave on vajalik, et tagada andmesubjekti suhtes õiglane andmete töötlemine, võttes arvesse andmete kogumise konkreetseid asjaolusid". Direktiivi artiklites 10 ja 11 osutatakse muu hulgas töödeldavate andmete liigile ja selliste andmete vastuvõtjate kategooriatele, samuti isikuandmetega tutvumise ja nende parandamise õiguse olemasolule. Kui andmeid kogutakse andmesubjektidelt, tuleks asjaomases teabes täpsustada, kas küsimustele vastamine on kohustuslik või vabatahtlik ja millised on vastamata jätmise võimalikud tagajärjed[163].

160 *Ibid.*, artikli 9 lõige 2; andmekaitsedirektiivi artikli 13 lõige 1.

161 Konventsiooni nr 108 artikli 8 punkt a; andmekaitsedirektiivi artiklid 10 ja 11.

162 Konventsiooni nr 108 artikli 8 punkt a; andmekaitsedirektiivi artikli 10 punktid a ja b.

163 Andmekaitsedirektiivi artikli 10 punkt c.

Euroopa Nõukogu õiguse seisukohast võib kõnealuse teabe avaldamist käsitada õiglase andmetöötluse põhimõttega kaasneva hea tavana ning sellega seoses kuulub see ka Euroopa Nõukogu õiguse alla.

Õiglase andmetöötluse põhimõtte kohaselt peab teave olema andmesubjektidele hõlpsasti mõistetav. Keelekasutus peab vastama sihtrühmale. Keelekasutuse laad ja tase sõltub näiteks sellest, kas sihtrühm koosneb lastest või täiskasvanutest, laiema üldsuse või teadusringkonna esindajatest.

Mõni andmesubjekt soovib oma andmete töötlemise põhjusest ja viisist teavet saada vaid kokkuvõtlikus vormis, samal ajal kui teised eelistavad üksikasjalikku selgitust. Seda, kuidas saavutada õiglase teavitamise puhul vajalik tasakaal, käsitletakse andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamuses, kus tuuakse esile nn mitmekihilised teated,[164] mis võimaldavad andmesubjektil valida teate üksikasjalikkuse taseme.

Teabe andmise aeg

Andmekaitsedirektiivis on seoses teabe andmise ajaga kehtestatud eri sätted sõltuvalt sellest, kas andmeid kogutakse andmesubjektilt (artikkel 10) või kolmandalt isikult (artikkel 11). Kui andmeid kogutakse andmesubjektilt, tuleb talle teave edastada hiljemalt andmete kogumise ajal. Kui andmeid kogutakse kolmandatelt isikutelt, tuleb teave edastada hiljemalt kas siis, kui vastutav töötleja salvestab andmed, või enne andmete esmakordset avaldamist kolmandale isikule.

Teatamiskohustuse erandid

ELi õiguses kohaldatakse andmesubjektile teatamise kohustuse ülderandit juhul, kui andmesubjektil juba on see teave[165]. See viitab olukordadele, kus andmesubjekt sõltuvalt asjaoludest juba teab, et teatav vastutav töötleja asub tema andmeid konkreetsel eesmärgil töötlema.

Direktiivi artiklis 11, milles käsitletakse andmesubjektile teatamise kohustust juhul, kui andmed ei ole saadud andmesubjektilt, on samuti sätestatud, et eeskätt

164 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 10/2004 teabesätete suurema ühtlustatuse kohta, WP 100, Brüssel, 25. november 2004.

165 Andmekaitsedirektiivi artikkel 10 ja artikli 11 lõige 1.

statistika, ajaloo- või teadusuuringutega seotud eesmärkidel toimuva töötlemise puhul ei kehti teatamiskohustus siis, kui:

- sellise teabe andmine osutub võimatuks;
- see eeldab ülemääraseid jõupingutusi;
- selliste andmete salvestamine või avalikustamine on õigusaktides selgelt sätestatud[166].

Üksnes andmekaitsedirektiivi artikli 11 lõikes 2 sätestatakse, et andmesubjekte ei pea andmetöötlustoimingutest teavitama juhul, kui need on õigusaktides selgelt sätestatud. Lähtudes õiguslikust oletusest, et andmesubjektid tunnevad asjaomaseid õigusakte, võib eeldada, et juhul, kui andmeid kogutakse andmesubjektilt, nagu ette nähtud direktiivi artikliga 10, on andmesubjektil vajalik teave juba olemas. Kuna aga andmesubjektid ei pruugi olla nendest õigusaktidest teadlikud, tuleks artikli 10 alusel õiglase põhimõtte kohaselt andmesubjektile teatada ka siis, kui töötlemine on ette nähtud õigusaktidega, eeskätt sellepärast, et kui andmeid kogutakse otse andmesubjektilt, ei nõua talle teabe andmine ülemääraseid jõupingutusi.

Euroopa Nõukogu õiguses sätestatakse konventsioonis nr 108 sõnaselgelt erandid konventsiooni artiklist 8. Taas kord tuleks märkida, et andmekaitsedirektiivi artiklites 10 ja 11 kirjeldatud erandeid võib lugeda konventsiooni nr 108 artikli 9 kohaste eranditega seotud hea tava näideteks.

Teabe andmise eri viisid

Ideaalsel juhul pöördutakse teabe andmiseks iga andmesubjekti poole eraldi, kas suulises või kirjalikus vormis. Kui andmeid kogutakse andmesubjektilt, tuleks teave edastada kogumise ajal. Vahel võib teabe aga edastada ka asjakohaste avalduste kaudu, iseäranis sellistel juhtudel, kus andmeid kogutakse kolmandatelt isikutelt, arvestades, et praktilises mõttes on isiklik pöördumine andmesubjektide poole ilmselgelt keerukas.

Üks tõhusamaid teabe andmise viise on vastutava töötleja kodulehel asjakohaste teavitamist käsitlevate klauslite esitamine, näiteks veebilehe privaatsuspoliitika.

166 *Ibid.*, 40. põhjendus ja artikli 11 lõige 2.

Paljud inimesed aga ei kasuta internetti ning seda tuleb ettevõtja või riigiasutuse teavitamispoliitikas arvesse võtta.

4.3.2. Teatamine

Vastutavad töötlejad võivad riigi õigusaktide alusel olla kohustatud teatama andmetöötlustoimingutest järelevalveasutusele, et viimane saaks avalikustada teabe nende kohta. Teise võimalusena võib riigi õigusaktidega olla ette nähtud, et vastutavad töötlejad võivad ametisse määrata isikuandmete kaitsega tegeleva ametiisiku, kelle peamine ülesanne on pidada registrit vastutava töötleja tehtavatest andmetöötlustoimingutest[167]. Selle registriga peavad taotluse korral tutvuda saama üldsuse esindajad.

Näide: teatamisel, samuti isikuandmete kaitsega tegeleva ametiisiku koostatavates dokumentides tuleb kirjeldada asjaomase andmetöötlustoimingu peamisi aspekte. See hõlmab teavet vastutava töötleja, andmetöötluse eesmärgi ja õigusliku aluse, töödeldavate andmete liikide, tõenäoliste kolmandast isikust vastuvõtjate kohta ning selle kohta, kas plaanis on andmete piiriülene liikumine, ja kui on, siis millisel viisil.

Järelevalveasutus avaldab teateid konkreetses registris. Eesmärgi täitmiseks peaks kõnealune register olema hõlpsasti ja tasuta kättesaadav. Sama kehtib vastutava töötleja valduses olevate ja isikuandmete kaitsega tegeleva ametiisiku säilitatavate dokumentide kohta.

Riigid võivad oma õigusaktides sätestada erandeid pädevale järelevalveasutusele teatamise või andmekaitsega tegeleva organisatsioonisisese ametiisiku ametisse määramise kohustustest andmetöötlustoimingute puhul, mis tõenäoliselt ei ohusta andmesubjekti, andmekaitsedirektiivi artikli 18 lõikes 2 loetletud juhtudel[168].

167 *Ibid.*, artikli 18 lõike 2 teine taane.

168 *Ibid.*, artikli 18 lõike 2 esimene taane.

4.4. Eeskirjad nõuetele vastavuse edendamise kohta

Põhipunktid

- Vastutuse põhimõtet käsitlevates sätetes osutatakse andmekaitsedirektiivis mitmele nõuete järgimist toetavale meetmele:
  - kavandatavate andmetöötlustoimingute eelkontroll riigi tasandi järelevalveasutuses;
  - isikuandmete kaitsega tegelevad ametiisikud, kes pakuvad vastutavale töötlejale andmekaitsevaldkonna oskusteavet;
  - tegevusjuhendid, milles täpsustatakse kehtivate andmekaitsealaste eeskirjade kohaldamist teatavas ühiskonna, eeskätt ettevõtlusvaldkonna harus.
- Euroopa Nõukogu õiguses pakutakse profiilide koostamist käsitlevas soovituses nõuetele vastavuse edendamiseks välja sarnaseid vahendeid.

4.4.1. Eelkontroll

Andmekaitsedirektiivi artikli 20 kohaselt peab järelevalveasutus andmetöötlustoiminguid, mis võivad kas eesmärgi või tingimuste tõttu tõenäoliselt ohustada andmesubjektide õigusi ja vabadusi, enne töötlemise alustamist kontrollima. See, milliste töötlemistoimingute puhul eelkontrolli rakendatakse, määratakse kindlaks riikide õigusaktides. Sellise kontrollimise tulemusena võidakse mõni toiming keelata või nõuda toimingu kavandatava ülesehituse teatavate omaduste muutmist. Direktiivi artikli 20 eesmärk on tagada, et tarbetute riskidega seotud töötlemist isegi mitte ei alustataks, sest järelevalveasutusel on õigus sellised toimingud keelata. Selle mehhanismi toimimise tagamiseks on tarvis, et järelevalveasutusi tõepoolest teavitataks. Selleks et vastutavad töötlejad täidaksid oma teatamiskohustust, peab järelevalveasutustel olema õigus rakendada sunnimeetmeid, näiteks määrata vastutavatele töötlejatele trahve.

Näide: kui ettevõtja teostab andmetöötlustoiminguid, mille suhtes kohaldatakse riigi õigusaktide alusel eelkontrolli, peab ettevõtja esitama järelevalveasutusele dokumendid kavandatavate töötlemistoimingute kohta. Ettevõtja ei või kõnealuseid toiminguid alustada enne, kui on saanud järelevalveasutuselt positiivse vastuse.

Mõne liikmesriigi õigusaktide alusel võib aga andmetöötlustoiminguid alustada juhul, kui järelevalveasutus ei ole kindla ajavahemiku, näiteks kolme kuu jooksul oma vastust andnud.

4.4.2. Isikuandmete kaitsega tegelevad ametiisikud

Andmekaitsedirektiivi alusel võib siseriiklike õigusaktidega ette näha, et vastutav töötleja võib ametisse määrata isikuandmete kaitsega tegeleva ametiisiku[169]. Selle ametikoha eesmärk on tagada, et töötlemistoimingute käigus tõenäoliselt ei kahjustataks andmesubjektide õigusi ja vabadusi[170].

Näide: Saksamaa föderaalse andmekaitseseaduse (*Bundesdatenschutzgesetz*) jaotise 4f 1. alajaotise kohaselt peavad eraettevõtjad määrama ametisse isikuandmete kaitsega tegeleva ametiisiku, kui ettevõttes tegeleb isikuandmete automatiseeritud töötlemisega kümme või enam alalist töötajat.

Kõnealuse eesmärgi saavutamiseks peab asjaomasel isikul oma töökohustuste täitmisel vastutava töötleja organisatsioonis olema teatav sõltumatus, nagu direktiivis otsesõnu sätestatud. Selleks et tagada kõnealuse ametikoha toimimine, on tarvis tugevaid tööalaseid õigusi, mis tagaks kaitse selliste tagajärgede vastu nagu põhjendamatu vallandamine.

Riikide andmekaitseõiguse nõuetele vastavuse edendamiseks on isikuandmete kaitsega tegelevate organisatsioonisiseste ametiisikute kontseptsiooni kasutatud ka mõnes Euroopa Nõukogu soovituses[171].

4.4.3. Tegevusjuhendid

Nõuetele vastavuse edendamiseks võib ettevõtlussektoris ja muudes valdkondades välja töötada üksikasjalikke eeskirju tüüpiliste andmetöötlustoimingute reguleerimiseks, talletades parima tava. Sektori asjaomaste liikmete oskusteabe abil leitakse lahendused, mis on praktilised ning leiaks seepärast ka laiemat järgimist. Sellega seoses julgustatakse liikmesriike ja ka Euroopa Komisjoni toetama tegevusjuhendite koostamist, mille eesmärk on aidata kaasa liikmesriikides andmekaitsedirektiivi

169 *Ibid.*, artikli 18 lõike 2 teine taane.

170 *Ibid.*

171 Vt nt profiilide koostamist käsitleva soovituse punkt 8.3.

alusel vastu võetud sätete nõuetekohasele rakendamisele, võttes arvesse sektorite eriomadusi[172].

Selleks et need tegevusjuhendid oleksid kooskõlas liikmesriikides andmekaitsedirektiivi alusel vastu võetud sätetega, peavad liikmesriigid kehtestama menetluse juhendite hindamiseks. Üldiselt peaks sellises menetluses osalema riigi tasandi järelevalveasutus, kutseühingud ja vastutavate töötlejate teisi kategooriaid esindavad muud organid[173].

Ühenduse tegevusjuhendite projektid ja olemasolevate ühenduse tegevusjuhendite muudatused või laiendused võib esitada hindamiseks andmekaitsedirektiivi artikli 29 alusel loodud töörühmale. Kui töörühm on dokumendi heaks kiitnud, võib Euroopa Komisjon tagada tegevusjuhendite asjakohase avalikustamise[174].

Näide: Euroopa otse- ja interaktiivse turunduse föderatsioon (*Federation of European Direct and Interactive Marketing, FEDMA*) töötas välja Euroopa tegevusjuhendi isikuandmete kasutamise kohta otseturunduses. Tegevusjuhendi kiitis heaks andmekaitsedirektiivi artikli 29 alusel loodud töörühm. 2010. aastal koostati tegevusjuhendi lisa elektroonilise turunduskommunikatsiooni kohta[175].

172 Andmekaitsedirektiivi artikli 27 lõige 1.

173 *Ibid.*, artikli 27 lõige 2.

174 *Ibid.*, artikli 27 lõige 3.

175 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 4/2010, mis käsitleb FEDMA Euroopa tegevusjuhendit isikuandmete kasutamiseks otseturunduses, WP 174, Brüssel, 13. juuli 2010.

5

Andmesubjektide õigused ja nende õiguste jõustamine

EL	Käsitletavad teemad	Euroopa Nõukogu
Õigus andmetega tutvuda		
Andmekaitsedirektiivi artikkel 12 ELK, C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer*, 7. mai 2009	Õigus tutvuda enda isikuandmetega	Konventsiooni nr 108 artikli 8 punkt b
	Õigus lasta andmed parandada, kustutada või sulgeda	Konventsiooni nr 108 artikli 8 punkt c EIK, *Cemalettin Canli vs. Türgi*, nr 22427/04, 18. november 2008 EIK, *Segerstedt-Wiberg jt vs. Rootsi*, nr 62332/00, 6. juuni 2006 EIK, *Ciubotaru vs. Moldova*, nr 27138/04, 27. aprill 2010
Õigus esitada vastuväiteid		
Andmekaitsedirektiivi artikli 14 lõike 1 punkt a	Õigus esitada vastuväiteid andmesubjekti konkreetse olukorraga seoses	Profiilide koostamist käsitleva soovituse punkt 5.3
Andmekaitsedirektiivi artikli 14 lõike 1 punkt b	Õigus esitada vastuväiteid andmete edasise kasutamise kohta turundusees-märkidel	Otseturundust käsitleva soovituse artikkel 4.1

EL	Käsitletavad teemad	Euroopa Nõukogu
Andmekaitsedirektiivi artikkel 15	Õigus esitada vastuväiteid automatiseeritud otsuste kohta	Profiilide koostamist käsitleva soovituse punkt 5.5
Sõltumatu järelevalveasutus		
Põhiõiguste harta artikli 8 lõige 3 Andmekaitsedirektiivi artikkel 28 ELi institutsioonide andmekaitse määruse V peatükk Andmekaitsemäärus ELK, C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik*, 9. märts 2010 ELK, C-614/10, *Euroopa Komisjon vs. Austria Vabariik*, 16. oktoober 2012 ELK, C-288/12, *8. juunil 2012 esitatud hagi – Euroopa Komisjon vs. Ungari*, 8. aprill 2014	Riikide järelevalveasutused	Konventsiooni nr 108 lisaprotokolli artikkel 1
Õiguskaitsevahendid ja karistused		
Andmekaitsedirektiivi artikkel 12	Vastutavale töötlejale esitatav taotlus	Konventsiooni nr 108 artikli 8 punkt b
Andmekaitsedirektiivi artikli 28 lõige 4 ELi institutsioonide andmekaitse määruse artikli 32 lõige 2	Järelevalveasutusele esitatavad kaebused	Konventsiooni nr 108 lisaprotokolli artikli 1 lõike 2 punkt b
Põhiõiguste harta artikkel 47	Kohtud (üldiselt)	Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 13
Andmekaitsedirektiivi artikli 28 lõige 3	Riigi tasandi kohtud	Konventsiooni nr 108 lisaprotokolli artikli 1 lõige 4
ELi toimimise lepingu artikli 263 lõige 4 ELi institutsioonide andmekaitse määruse artikli 32 lõige 1 ELi toimimise lepingu artikkel 267	ELK	
	EIK	Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 34

EL	Käsitletavad teemad	Euroopa Nõukogu
Õiguskaitsevahendid ja karistused		
Põhiõiguste harta artikkel 47 Andmekaitsedirektiivi artiklid 22 ja 23 ELK, C-14/83, *Sabine von Colson ja Elisabeth Kamann vs. Land Nordrhein-Westfalen*, 10. aprill 1984 ELK, C-152/84, *M.H. Marshall vs. Southampton ja South-West Hampshire Area Health Authority*, 26. veebruar 1986	**Riigi tasandi andmekaitseõiguse rikkumiste puhul**	Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 13 (ainult Euroopa Nõukogu liikmesriikide puhul) Konventsiooni nr 108 artikkel 10 EIK, *K.U. vs. Soome*, nr 2872/02, 2. detsember 2008 EIK, *Biriuk vs. Leedu*, nr 23373/03, 25. november 2008
ELi institutsioonide andmekaitse määruse artiklid 34 ja 49 ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*, 29. juuni 2010	**ELi õiguse rikkumised ELi institutsioonides ja asutustes**	

See, kas laiemalt õigusnormide ja kitsamalt andmesubjektide õiguste rakendamine vilja kannab, sõltub olulisel määral asjaolust, kas nende jõustamiseks on olemas asjakohased mehhanismid. Euroopa andmekaitseõiguses peab andmesubjektil riigi õigusaktide alusel olema õigus kaitsta oma andmeid. Selleks et tagada isikuandmete töötlemise järelevalve ning aidata andmesubjektidel oma õigusi rakendada, tuleb riikide õigusaktidega luua ka sõltumatud järelevalveasutused. Peale selle tähendab Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ja põhiõiguste hartas sätestatud õigus tõhusale õiguskaitsevahendile, et kõikidel inimestel peab olema võimalus pöörduda kohtu poole.

5.1. Andmesubjektide õigused

Põhipunktid

- Igal inimesel on riikide õigusaktide alusel õigus taotleda mis tahes vastutavalt töötlejalt teavet selle kohta, kas isikut ennast käsitlevaid andmeid töödeldakse.
- Riigi tasandi õigusaktide alusel peab andmesubjektidel olema õigus:
  - tutvuda andmetega, mida mis tahes vastutav töötleja nendega seoses töötleb;

- lasta oma andmeid töötleval vastutaval töötlejal andmeid parandada (või vajaduse korral need sulgeda), kui andmed on ebaõiged;
- lasta vastutaval töötlejal oma andmed vajaduse korral kustutada või sulgeda, kui vastutav töötleja töötleb kõnealuseid andmeid ebaseaduslikult.

- Peale selle on andmesubjektidel õigus esitada vastutavatele töötlejatele vastuväiteid järgmise kohta:
  - automatiseeritud otsused (tehakse isikuandmete alusel täielikult automatiseeritult);
  - nende andmete töötlemine, kui sellel on ebaproportsionaalsed tulemused;
  - nende andmete kasutamine otseturunduse eesmärkidel.

5.1.1. Isikuandmetega tutvumise õigus

ELi õiguses on andmekaitsedirektiivi artiklis 12 kirjeldatud andmesubjektide õigust isikuandmetega tutvuda, sealhulgas õigust nõuda vastutavalt töötlejalt „kinnitust selle kohta, kas isikut ennast käsitlevaid andmeid töödeldakse, ja teavet vähemalt töötlemise eesmärkide, asjaomaste andmete liikide ja nende vastuvõtjate või vastuvõtjate kategooriate kohta, kellele andmed avalikustatakse", samuti „võimalust [...] parandada, kustutada või sulgeda need andmed, mille töötlemine ei vasta käesoleva direktiivi sätetele, eelkõige seetõttu, et andmed on ebatäielikud või ebaõiged".

Euroopa Nõukogu õiguskorras kehtivad samad õigused ning need tuleb sätestada riigi õigusaktides (konventsiooni nr 108 artikkel 8). Mitmes Euroopa Nõukogu soovituses kasutatakse terminit „tutvumine (juurdepääs)" ning kõnealuse õigusega seotud eri aspekte kirjeldatakse ja soovitatakse siseriiklikes õigusaktides rakendada samamoodi nagu eespool osutatud sättes.

Konventsiooni nr 108 artikli 9 ja andmekaitsedirektiivi artikli 13 kohaselt võib vastutavate töötlejate kohustust vastata andmesubjekti taotlusele andmetega tutvuda piirata kaasinimeste ülimuslike õiguslike huvide kaitsmiseks. Ülimuslikud õiguslikud huvid võivad olla avalikud, nt riigi julgeolek, avalik kord ja kuritegude eest vastutusele võtmine, ning ka isiklikud, mis kaaluvad üles andmekaitsega seotud huvid. Kõik erandid ja piirangud peavad olema demokraatlikus ühiskonnas vajalikud ning vastama taotletavale eesmärgile. Väga erandlikel juhtudel, näiteks meditsiinilisel näidustusel, tuleb juba omaette andmesubjekti kaitsmiseks piirata selguse ja arusaadavuse kohustuse täitmist; see on eelkõige seotud piirangutega kõikide andmesubjektide õigusele isikuandmetega tutvuda.

Kui andmeid töödeldakse ainult teadusuuringutega seotud eesmärgil või statistika tegemiseks, võivad liikmesriigid andmekaitsedirektiivi kohaselt andmetega tutvumise õigusi oma õigusaktidega piirata, aga sel juhul peavad olemas olema piisavad õiguslikud tagatised. Eeskätt tuleb tagada, et sellistes andmetöötlustoimingutes ei võetaks konkreetset üksikisikut puudutavaid meetmeid või ei tehtaks temaga seotud otsuseid ning et „ilmselt puudub oht sekkuda andmesubjekti eraellu"[176]. Sarnased sätted on kehtestatud konventsiooni nr 108 artikli 9 lõikes 3.

Õigus tutvuda oma isikuandmetega

Euroopa Nõukogu õiguses on õigus isikuandmetega tutvuda sõnaselgelt talletatud konventsiooni nr 108 artiklis 8. EIK on korduvalt kinnitanud, et inimesel on õigus tutvuda teiste inimeste valduses oleva või kasutatava teabega, mis sisaldab tema isikuandmeid, ning et see õigus tuleneb eraelu austamise nõudest[177]. *Leanderi*[178] kohtuasjas järeldas EIK, et õigust tutvuda riigiasutustes säilitatavate isikuandmetega võidakse aga teatavatel tingimustel piirata.

ELi õiguses sätestatakse õigus tutvuda isikuandmetega sõnaselgelt andmekaitsedirektiivi artiklis 12 ning põhiõiguste harta artikli 8 lõikes 2 on see talletatud ka põhiõigusena.

Andmekaitsedirektiivi artikli 12 punkti a kohaselt peavad liikmesriigid igale andmesubjektile tagama õiguse tutvuda oma isikuandmetega ning asjaomase teabega. Eeskätt on igal andmesubjektil õigus saada vastutavalt töötlejalt kinnitust selle kohta, kas isikut ennast käsitlevaid andmeid töödeldakse, ning teavet vähemalt järgmistes küsimustes:

- töötlemise eesmärgid;
- asjaomaste andmete liigid;
- töödeldavad andmed;
- vastuvõtjad või vastuvõtjate kategooriad, kellele andmed avalikustatakse;

176 Andmekaitsedirektiivi artikli 13 lõige 2.

177 EIK, *Gaskin vs. Ühendkuningriik*, nr 10454/83, 7. juuli 1989; EIK, *Odièvre vs. Prantsusmaa [suurkogu]*, nr 42326/98, 13. veebruar 2003; EIK, *K.H. jt vs. Slovakkia*, nr 32881/04, 28. aprill 2009; EIK, *Godelli vs. Itaalia*, nr 33783/09, 25. september 2012.

178 EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987.

- mis tahes kättesaadav teave töödeldavate andmete allika kohta;
- automatiseeritud otsuste puhul andmete automatiseeritud töötlemise loogika.

Riigid võivad oma õigusaktidega ette näha veel küsimusi, milles vastutavad töötlejad peavad teavet andma, näiteks andmetöötlust võimaldav õiguslik alus.

Näide: oma andmetega tutvudes saab isik kindlaks teha, kas andmed on täpsed. Seepärast tuleb andmesubjekti igal juhul teavitada töödeldavate andmete liikidest ning ka andmete sisust. Nii ei piisa sellest, kui vastutav töötleja teatab andmesubjektile üksnes seda, et ta töötleb tema nimele, aadressile, sünnikuupäevale ja huvialale viitavaid andmeid. Vastutav töötleja peab andmesubjektile teatama ka seda, et ta töötleb järgmisi andmeid: „nimi: N.N; aadress: 1040 Viin, Schwarzenbergplatz 11, Austria; sünnikuupäev 10.10.1974; huviala (andmesubjekti avalduse kohaselt): klassikaline muusika". Viimane osa sisaldab lisaks ka teavet andmete allika kohta.

Andmesubjektile tuleb töödeldavatest andmetest ning mis tahes teabest andmete allika kohta teatada arusaadaval kujul, mis tähendab, et vastutav töötleja peab andmesubjektile vajaduse korral täpsemalt selgitama, milliseid andmeid töödeldakse. Andmetega tutvumise taotlusele üksnes tehnilistele lühenditele või meditsiiniterminitele viitamisest näiteks ei piisa, isegi kui säilitatavate andmete puhul ongi tegemist selliste lühendite või terminitega.

Andmetega tutvumise taotlusele vastates tuleb olemasolu korral esitada teave vastutava töötleja töödeldavate andmete allika kohta. Seda sätet tuleb käsitada õiglase töötlemise ja vastutuse põhimõtte taustal. Vastutav töötleja ei tohi andmete allikat käsitlevat teavet hävitada, et selle avaldamisest hoiduda, ega eirata tema tegevusvaldkonnas seoses dokumentatsiooniga kehtivaid üldnõudeid ja tunnustatud nõudmisi. Kui vastutaval töötlejal ei ole dokumente töödeldavate andmete allika kohta, ei täida ta isikuandmetega tutvumise õigusega seotud kohustusi.

Automatiseeritud hindamise puhul tuleb selgitada hindamise üldloogikat, sealhulgas konkreetseid kriteeriume, mille alusel andmesubjekti hinnati.

Direktiivist ei selgu, kas õigus teabega tutvuda ulatub minevikku ning kui jah, siis kui kaugele minevikku. Sellega seoses ei tohiks isiku õigusel enda andmetega tutvuda olla põhjendamatuid ajapiiranguid, nagu nähtub alljärgnevast ELK kohtuasjast.

Samuti peab andmesubjektidele tagama mõistliku võimaluse saada teavet varasemate andmetöötlustoimingute kohta.

Näide: *Rijkeboeri*[179] kohtuasjas paluti ELK-l välja selgitada, kas direktiivi artikli 12 punkti a alusel võis isiku õigust tutvuda teabega isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta ning avalikustatud andmete sisu kohta piirata andmetega tutvumise taotluse esitamisele eelnenud aastaga.

Selleks et välja selgitada, kas direktiivi artikli 12 punkti a alusel on selline ajapiirang lubatud, otsustas kohus tõlgendada kõnealust artiklit direktiivi eesmärke arvestades. Esmalt märkis kohus, et isikuandmetega tutvumise õigus on vajalik selleks, et võimaldada andmesubjektil kasutada õigust nõuda, et vastutav töötleja parandab, kustutab või sulgeb andmed (artikli 12 punkt b) või et ta teavitab parandustest, kustutamistest või sulgemistest kolmandaid isikuid, kellele need andmed avalikustati (artikli 12 punkt c). Isikuandmetega tutvumise õigus on vajalik ka selleks, et andmesubjekt saaks kasutada õigust esitada vastuväiteid tema isikuandmete töötlemisele (artikkel 14) või õiguskaitsevahendeid, kui ta on kandnud kahju (artiklid 22 ja 23).

Kohus leidis, et eespool „viidatud sätete kasuliku mõju tagamiseks peab kõnealune õigus tingimata minevikku puudutama. Kui see nii ei oleks, siis ei saaks nimelt andmesubjekt kasutada tõhusalt oma õigust nõuda, et parandataks, kustutataks või sulgetaks andmed, mis on eeldatavalt ebaseaduslikud või väärad, ning esitada kaebus ja saada kahjuhüvitist".

Õigus lasta andmeid parandada, kustutada ja sulgeda

„[I]gaühel peab olema võimalik kasutada õigust tutvuda teda käsitlevate töödeldavate andmetega, et kontrollida eelkõige andmete õigsust ja töötlemise seaduslikkust"[180]. Kooskõlas nende põhimõtetega peab andmesubjektidel olema riigi õigusaktide alusel õigus nõuda, et vastutav töötleja parandaks, kustutaks või sulgeks nende andmed, mille töötlemine ei vasta andmesubjektide arvates andmekaitsedirektiivi sätetele, eelkõige seetõttu, et andmed on ebatäielikud või ebaõiged[181].

179 ELK, C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer*, 7. mai 2009.

180 Andmekaitsedirektiivi 41. põhjendus.

181 *Ibid.*, artikli 12 lõige b.

Näide: kohtuasjas *Cemalettin Canli vs. Türgi*[182] tegi EIK kindlaks Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise seoses ebaõigete politseiaruannetega kriminaalmenetlustes.

Kaebuse esitaja oli kahel korral kaasatud kriminaalmenetlustesse kahtlustatuna ebaseaduslikult tegutsevatesse rühmitustesse kuulumises, ent teda ei olnud kunagi süüdi mõistetud. Kui kaebuse esitaja taas kord vahistati ja teda süüdistati veel ühes kuriteos, esitas politsei kriminaalkohtule aruande pealkirjaga „Teabevorm teiste kuritegude kohta", millest võis välja lugeda, et kaebuse esitaja on kahe ebaseaduslikult tegutseva rühmituse liige. Kaebuse esitaja palus asjaomast aruannet ja politsei registrikirjeid muuta, kuid tema taotlust ei rahuldatud. EIK leidis, et politseiaruandes esitatud teave kuulus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaldamisalasse, kuna ka avalik teave võib kuuluda eraelu alla, arvestades, et sellist teavet koguti süstemaatiliselt ja säilitati ametiasutuste registrites. Peale selle ei olnud politseiaruandes sisalduv teave õige ning aruande koostamine ja esitamine kriminaalkohtule ei olnud kooskõlas õigusaktidega. Kohus otsustas, et tegu oli artikli 8 rikkumisega.

Näide: kohtuasjas *Segerstedt-Wiberg jt vs. Rootsi*[183] arutati juhtumit, kus kaebuse esitajaid seostati teatavate liberaalsete ja kommunistlike erakondadega. Kaebuse esitajad kahtlustasid, et nende teave oli kantud kaitsepolitsei registrisse. EIK leidis, et kõnealuste andmete säilitamisel oli õiguslik alus ning põhjendatud eesmärk. Teatavate kaebuse esitajate puhul märkis EIK, et nende andmete jätkuva säilitamisega sekkuti ülemäära nende eraellu. Näiteks härra Schmidi puhul säilitasid ametivõimud teavet selle kohta, et 1969. aastal oli ta väidetavalt õhutanud meeleavaldustel vägivaldset vastuhakku politseile. EIK leidis, et selle teabe puhul ei saanud mängus olla asjakohast riigi julgeoleku kaitsmisega seotud huvi, arvestades eeskätt, et teave käsitles aastatetaguseid kahtlustusi. EIK järeldas, et kaebuse esitajate suhtes oli nelja isiku puhul viiest rikutud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Mõnel juhul piisab sellest, kui andmesubjekt esitab lihtsalt taotluse näiteks nime kirjapildi parandamiseks või aadressi või telefoninumbri muutmiseks. Kui aga sellised taotlused on seotud juriidiliste küsimustega, näiteks andmesubjekti õigusliku staatusega või kehtiva elukoha aadressiga õigusdokumentide kättetoimetamiseks,

182 EIK, *Cemalettin Canli vs. Türgi*, nr 22427/04, 18. november 2008, punktid 33, 42 ja 43; EIK, *Dalea vs. Prantsusmaa,* nr 964/07, 2. veebruar 2010.

183 EIK, *Segerstedt-Wiberg jt vs. Rootsi*, nr 62332/00, 6. juuni 2006, punktid 89 ja 90; vt ka nt EIK, *M.K. vs. Prantsusmaa*, nr 19522/09, 18. aprill 2013.

ei pruugi parandamistaotlusest piisata ning vastutaval töötlejal on õigus nõuda tõendeid väidetava ebatäpsuse põhjendamiseks. Selliste nõudmistega ei tohi andmesubjektile määrata liiga suurt tõendamiskoormist ning seetõttu nad andmete parandamise võimalusest ilma jätta. EIK on mitmes kohtuasjas, kus kaebuse esitajal ei ole õnnestunud esitada vastuväiteid salajastes registrites hoitava teabe õigsuse kohta, kindlaks teinud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise[184].

Näide: kohtuasjas *Ciubotaru vs. Moldova*[185] ei olnud kaebuse esitajal õnnestunud lasta ametlikes registrikannetes muuta oma etnilist päritolu moldovlasest rumeenlaseks, kuna leiti, et ta ei suutnud oma taotlust põhjendada. EIK leidis, et riikidel on õigus nõuda üksikisiku etnilise identiteedi registreerimisel objektiivseid tõendeid. Kui selline taotlus põhineb vaid subjektiivsetel ja põhjendamata alustel, on ametiasutustel õigus see rahuldamata jätta. Kaebuse esitaja taotlus ei põhinenud aga vaid sellel, kuidas asjaomane isik ise oma etnilist päritolu tajus; ta osutas objektiivselt kontrollitavatele seostele rumeenlaste etnilise rühmaga, nagu keel, nimi, samastumine rühmaga jms. Riigi õigusaktide alusel aga pidi kaebuse esitaja esitama tõendeid selle kohta, et tema vanemad kuulusid rumeenlaste etnilisse rühma. Pidades silmas Moldova ajalugu, seadis kõnealune nõue ületamatuid takistusi olukorras, kus isik soovis tema vanematele nõukogude ametivõimude määratud etnilise identiteedi järgi tehtud registrikannet muuta. Kuna kaebuse esitajale ei võimaldatud tema taotluse hindamist objektiivselt kontrollitavate tõendite alusel, ei täitnud riik oma positiivset kohustust tagada kaebuse esitaja eraelu austamine. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Tsiviilkohtumenetlustes või riigiasutuse juhitavates menetlustes saab andmesubjekt oma andmete õigsuse kontrollimiseks taotleda, et tema andmetele lisataks kirje või märge, milles märgitakse, et andmete täpsus on küsimärgi all ning ametlikku otsust ei ole veel tehtud. Sellel perioodil ei tohi vastutav töötleja jätta muljet, et andmed on täielikud ja lõplikud, eriti kolmandatele isikutele.

Kui andmesubjekt taotleb andmete kustutamist, väidetakse tavaliselt, et andmete töötlemisel ei ole õiguslikku alust. Sageli tõstatatakse selliseid väiteid olukorras, kus nõusolek on tagasi võetud või teatavaid andmeid ei ole andmete kogumise eesmärgi saavutamise jaoks enam vaja. Andmetöötluse seaduslikkuse tõendamise

184 EIK, *Rotaru vs. Rumeenia*, nr 28341/95, 4. mai 2000.

185 EIK, *Ciubotaru vs. Moldova*, nr 27138/04, 27. aprill 2010, punktid 51 ja 59.

koormis on vastutaval töötlejal, sest just tema vastutab töötlemise õiguspärasuse eest. Vastutuse põhimõttest lähtudes peab vastutaval töötlejal ükskõik millal olema võimalik näidata, et tema andmetöötlustoimingutel on nõuetekohane õiguslik alus, ning kui ta seda teha ei suuda, tuleb töötlemine peatada.

Kui andmete töötlemise suhtes esitatakse vastuväide sellepärast, et arvatavalt on andmed ebaõiged või neid töödeldakse ebaseaduslikult, võib andmesubjekt kooskõlas õiglase töötlemise põhimõttega nõuda, et asjaomased andmed sulgetaks. See tähendab, et andmeid mitte ei kustutata, vaid vastutav töötleja ei tohi andmeid sulgemisperioodil kasutada. See on eriti vajalik juhtudel, kui ebaõigete või ebaseaduslikult säilitatavate andmete jätkuv kasutamine võib andmesubjekti ohtu seada. Seda, millistel tingimustel ja kuidas tuleb andmete kasutamine sulgeda, tuleks täpsustada riikide õigusaktides.

Samuti on andmesubjektidel õigus nõuda, et vastutav töötleja saadaks mis tahes sulgemisest, parandamisest või kustutamisest teatise kolmandatele isikutele, kellele andmeid enne kõnealuseid töötlemistoiminguid avalikustati. Kuna vastutav töötleja peab andmete avalikustamist kolmandatele isikutele dokumenteerima, peaks olema võimalik andmete vastuvõtjad kindlaks teha ning taotleda andmete kustutamist. Kui aga asjaomased andmed on vahepeal avaldatud näiteks internetis, ei pruugi olla võimalik kõiki asjaomaseid andmeid kustutada, sest andmete vastuvõtjaid ei saa tuvastada. Andmekaitsedirektiivi kohaselt peab paranduste, kustutamiste või sulgemiste asjus ühendust võtma andmete vastuvõtjatega, „kui see ei ole võimatu või kui sellega ei kaasne ülemääraseid jõupingutusi"[186].

5.1.2. Õigus esitada vastuväiteid

Õigus esitada vastuväiteid hõlmab õigust esitada vastuväiteid automatiseeritud üksikotsuste kohta, õigust esitada vastuväiteid andmesubjekti konkreetse olukorraga seoses ning õigust esitada vastuväiteid andmete edasise kasutamise kohta otseturunduse eesmärkidel.

Õigus esitada vastuväiteid automatiseeritud üksikotsuste kohta

Automatiseeritud otsused tehakse töödeldud isikuandmete alusel täielikult automatiseeritult. Olukorras, kus sellised otsused võivad olulisel määral mõjutada üksikisikute elu, kuna need on seotud näiteks krediidivõimelisuse, tööviljakuse, käitumise

186 Andmekaitsedirektiivi artikli 12 punkt c, lause viimane pool.

või usaldusväärsusega, on ebasoovitavate tagajärgede vältimiseks tarvis konkreetseid kaitsemeetmeid. Andmekaitsedirektiivi kohaselt ei tohi automatiseeritud otsustes olla kindlaks määratud üksikisiku seisukohalt olulisi küsimusi ning tal peab olema õigus automatiseeritud otsus üle vaadata[187].

Näide: oluline praktiline näide automatiseeritud otsusest on krediidihindamine. Selleks et määrata kiiresti kindlaks tulevase kliendi krediidivõimelisus, kogutakse kliendilt teatavaid andmeid, näiteks elukutse ja perekonnaseisu kohta, ning need pannakse kokku kliendi kohta teistest allikatest, näiteks krediidiinfosüsteemidest kättesaadavate andmetega. Nende andmete peal rakendatakse automaatselt hindamisalgoritmi, mille abil arvutatakse üldväärtus, st potentsiaalse kliendi krediidivõimelisus. Nii saab ettevõtte töötaja sekunditega otsustada, kas andmesubjekt sobib kliendiks või mitte.

Vaatamata sellele peavad liikmesriigid kooskõlas andmekaitsedirektiiviga tagama, et isiku kohta võib teha automatiseeritud üksikotsuse, kui andmesubjekti huvid ei ole arutluse all, kuna otsus tehakse andmesubjekti kasuks, või kui neid kaitstakse muude sobivate meetmete abil[188]. Õigus esitada vastuväiteid automatiseeritud otsuste kohta on olemas ka **Euroopa Nõukogu õiguses**, nagu nähtub profiilide koostamist käsitlevast soovitusest[189].

Õigus esitada vastuväiteid andmesubjekti konkreetse olukorraga seoses

Andmesubjektidele ei ole ette nähtud üldõigust esitada vastuväiteid nende andmete töötlemise kohta[190]. Andmekaitsedirektiivi artikli 14 punkti a alusel on aga andmesubjektil õigus esitada vastuväiteid tema konkreetse olukorraga seotud õigustatud ja veenvatel põhjustel. Sarnast õigust on tunnustatud Euroopa Nõukogu soovituses profiilide koostamise kohta[191]. Sedalaadi sätete eesmärk on leida andmesubjekti andmete töötlemisel õige tasakaal andmesubjekti andmekaitsega seotud õiguse ja teistele inimestele õigusaktidega tagatud õiguste vahel.

187 *Ibid.*, artikli 15 lõige 1.

188 *Ibid.*, artikli 15 lõige 2.

189 Profiilide koostamist käsitleva soovituse punkt 5.5.

190 Vt ka EIK, *M.S. vs. Rootsi*, nr 20837/92, 27. august 1997, mille puhul edastati meditsiinilisi andmeid ilma andmesubjekti nõusolekuta või võimaluseta vastuväiteid esitada; EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987; või EIK *Mosley vs. Ühendkuningriik*, nr 48009/08, 10. mai 2011.

191 Profiilide koostamist käsitleva soovituse punkt 5.3.

Näide: pangas säilitatakse seitsme aasta jooksul andmeid klientide kohta, kellel on esinenud laenumaksete häireid. Klient, kelle andmed on kõnealusesse andmebaasi kantud, taotleb uut laenu. Andmebaasist saadud andmete ja kliendi rahalise olukorra hinnangu põhjal otsustatakse kliendile laenu mitte anda. Samal ajal saab klient esitada vastuväite tema isikuandmete säilitamise kohta kõnealuses andmebaasis ning paluda andmed kustutada, kui ta suudab tõendada, et maksehäire tekkis üksnes teatava vea tõttu, mille klient sellest teada saades kohe parandas.

Kui vastuväide rahuldatakse, tähendab see seda, et vastutav töötleja ei tohi asjaomaseid andmeid enam töödelda. Andmesubjekti andmetega enne vastuväite esitamist tehtud töötlemistoimingud aga jäävad jõusse.

Õigus esitada vastuväiteid andmete edasise kasutamise kohta otseturunduse eesmärkidel

Andmekaitsedirektiivi artikli 14 punktis b sätestatakse andmesubjektidele konkreetne õigus esitada vastuväiteid oma andmete kasutamise kohta otseturunduse eesmärkidel. Selline õigus on ette nähtud ka Euroopa Nõukogu soovitusega otseturunduse kohta[192]. Vastuväide tuleb esitada enne seda, kui andmed avalikustatakse otseturunduse eesmärgil kolmandatele isikutele. Seepärast peab andmesubjektil olema võimalus vastuväiteid esitada enne andmete edastamist.

5.2. Sõltumatu järelevalve

Põhipunktid

- Selleks et andmekaitse oleks tõhus, tuleb riikide õigusaktide alusel luua sõltumatud järelevalveasutused.
- Riikide järelevalveasutustel peab tegutsemisel olema täielik sõltumatus, mis peab olema tunnustatud nende asutamist käsitlevates õigusaktides ning kajastuma järelevalveasutuse konkreetses organisatsioonilises struktuuris.
- Järelevalveasutuste konkreetsed ülesanded on muu hulgas:
  - andmekaitse järelevalve ja edendamine riigi tasandil;

192 Euroopa Nõukogu ministrite komitee (1985) soovitus Rec(85)20 liikmesriikidele otseturunduse eesmärkidel kasutatavate isikuandmete kaitse kohta, 25. oktoober 1985, artikli 4 lõige 1.

- andmesubjektidele, vastutavatele töötlejatele ning samuti valitsusele ja kogu avalikkusele nõu andmine;
- kaebuste läbivaatamine ning andmesubjektidele abi osutamine juhtumites, kus väidetavalt on rikutud andmekaitsega seotud õigusi;
- vastutavate töötlejate ja volitatud töötlejate juhendamine;
- vajaduse korral sekkumine:
  - hoiatades, noomides või lausa trahvides vastutavaid töötlejaid või volitatud töötlejaid;
  - nõudes andmete parandamist, sulgemist või kustutamist;
  - keelates andmete töötlemise;
- küsimuste suunamine kohtule.

Andmekaitsedirektiivi kohaselt on sõltumatu järelevalve oluline mehhanism andmekaitse tõhususe tagamisel. Kõnealune direktiivis andmekaitse jõustamise eesmärgil sätestatud instrument ei kajastunud algselt konventsioonis nr 108 ega eraelu puutumatust käsitlevates OECD suunistes.

Kuna sõltumatu järelevalve osutus tõhusa andmekaitsesüsteemi väljatöötamisel asendamatuks meetmeks, kehtestati 2013. aastal vastu võetud muudetud OECD suunistes eraelu puutumatuse kohta uus säte, et liikmesriigid peaksid looma eraelu puutumatuse kaitsega tegelevad ametiasutused, kelle sõltumatus, ressursid ja tehniline oskusteave võimaldavad tulemuslikult kasutada neile määratud volitusi ning teha otsuseid objektiivselt, erapooletult ja järjekindlalt, ning tagama selliste asutuste toimimise[193].

Euroopa Nõukogu õiguses on järelevalveasutuste loomise kohustus sätestatud konventsiooni nr 108 lisaprotokollis. Selle dokumendi artiklis 1 on kirjeldatud sõltumatute järelevalveasutuste õigusraamistikku, mida konventsiooniosalised peavad oma õigusaktides rakendama. Järelevalveasutuste ülesannete ja volituste kirjeldamisel kasutatakse selles dokumendis sarnast sõnastust nagu andmekaitsedirektiivis. Põhimõtteliselt peaksid järelevalveasutused seega Euroopa Nõukogu õiguskorras tegutsema samamoodi nagu ELi õiguskorras.

193 OECD (2013), „Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data" (e k „Suunised eraelu puutumatuse kaitse ja isikuandmete piiriülese liikumise kohta"), punkti 19 alapunkt c.

ELi õiguses kirjeldati järelevalveasutuste pädevust ja organisatsioonilist struktuuri esmakordselt andmekaitsedirektiivi artikli 28 lõikes 1. ELi institutsioonide andmekaitse määruses[194] määratakse ELi asutustes ja institutsioonides toimuva andmetöötluse järelevalve eest vastutavaks Euroopa andmekaitseinspektor. Asjaomase järelevalveasutuse ülesannete ja vastutusalade piiritlemisel lähtuti määruses andmekaitsedirektiivi väljakuulutamisest alates saadud kogemustest.

Andmekaitseasutuste sõltumatus on tagatud ELi toimimise lepingu artikli 16 lõikega 2 ja põhiõiguste harta artikli 8 lõikega 3. Viimase sätte alusel moodustab sõltumatu ametiasutuse kontroll olulise osa põhiõigusest isikuandmete kaitsele. Lisaks sellele peavad liikmesriigid andmekaitsedirektiivi kohaselt looma direktiivi sätete kohaldamise üle järelevalve teostamiseks järelevalveasutused, kes tegutsevad täiesti sõltumatult[195]. Järelevalveasutuse loomist käsitlev õigusakt peab sisaldama sätteid, millega tagatakse asutuse sõltumatus, kuid seejuures peab sõltumatus kajastuma ka asutuse eriomases organisatsioonilises struktuuris.

2010. aastal käsitles ELK esimest korda andmekaitse järelevalveasutuste sõltumatuse nõude ulatuse küsimust[196]. Kohtu lähenemisviisi illustreerivad järgmised näited.

Näide: kohtuasjas *Euroopa Komisjon vs. Saksamaa*[197] oli Euroopa Komisjon palunud ELK-l tuvastada, et Saksamaa oli ebaõigelt üle võtnud andmekaitse tagamise eest vastutavate asutuste täieliku sõltumatuse nõude ning seega rikkunud andmekaitsedirektiivi artikli 28 lõikest 1 tulenevaid kohustusi. Komisjoni arvamuse kohaselt seisnes probleem selles, et Saksamaa allutas riiklikule järelevalvele asutused, kes olid eri liidumaades pädevad teostama järelevalvet isikuandmete töötlemise üle erasektoris.

Asjaomase hagi põhjendatuse hindamine sõltus kohtu väitel kõnealuses sättes sisalduva sõltumatuse nõude ulatusest ning seega nimetatud sätte tõlgendamisest.

194 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, EÜT L 8, 2001, artiklid 41–48.

195 Andmekaitsedirektiivi artikli 28 lõike 1 viimane lause; konventsiooni nr 108 lisaprotokolli artikli 1 lõige 3.

196 FRA (2010), „Põhiõigused: peamised õiguslikud ja poliitilise arengusuunad 2010. aastal", aastaaruanne 2010, lk 59. FRA käsitles seda küsimust üksikasjalikumalt oma 2010. aasta mais avaldatud aruandes „Data protection in the European Union: the role of National Data Protection Authorities" (e k „Andmekaitse Euroopa Liidus – riikide andmekaitseasutuste roll").

197 ELK, C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik*, 9. märts 2010, punkt 27.

Kohus rõhutas, et direktiivi artikli 28 lõikes 1 esitatud väljendit „täiesti sõltumatult" tuleb tõlgendada selle sätte tavapärasest tähendusest ning andmekaitsedirektiivi eesmärkidest ja ülesehitusest lähtudes[198]. Kohus märkis, et järelevalveasutused on isikuandmete töötlemise puhul direktiivis sätestatud õiguste kaitsjad ning et nende loomist liikmesriikides peetakse „oluliseks teguriks üksikisikute kaitsmisel seoses isikuandmete töötlemisega"[199]. Kohus järeldas, „et oma ülesannete täitmisel peavad järelevalveasutused tegutsema objektiivselt ja erapooletult. Selleks peavad nad olema kaitstud mitte ainult nende kontrollile allutatud asutuste mõju eest, vaid igasuguse välise mõju eest, kaasa arvatud riigi või liidumaade otsene või kaudne mõju"[200].

Samuti leidis ELK, et väljendit „täiesti sõltumatult" tuleks tõlgendada Euroopa andmekaitseinspektori sõltumatust arvesse võttes, nagu on kirjeldatud ELi institutsioonide andmekaitse määruses. ELK märkis, et määruse artikli 44 lõikes 2 „lisatakse sõltumatuse mõiste selgitamiseks, et oma kohustuste täitmisel ei taotle ega võta Euroopa andmekaitseinspektor vastu juhendeid teistelt isikutelt". Seega ei tohiks andmekaitse sõltumatu järelevalveasutus kuuluda riigi järelevalve alla[201].

Seda silmas pidades leidis ELK, et liidumaa tasandil tegutsevad Saksamaa andmekaitseasutused, kes teevad järelevalvet eraõiguslikes asutustes toimuva isikuandmete töötlemise üle, ei olnud piisavalt sõltumatud, kuna nad olid allutatud riigi järelevalvele.

Näide: kohtuasjas *Euroopa Komisjon vs. Austria*[202] tõstis ELK esile sarnaseid probleeme seoses Austria andmekaitseasutuse (andmekaitsekomisjoni) liikmete ja töötajate ametikohtadega. Selles kohtuasjas järeldas kohus, et Austria andmekaitseasutus ei saanud Austria õigusnormide alusel tegutseda oma ülesannete täitmisel andmekaitsedirektiivi tähenduses täiesti sõltumatult. Austria andmekaitseasutusele ei olnud tagatud piisavat sõltumatust, kuna föderaalkantselei vastutas andmekaitsekomisjoni personaliküsimuste eest, korraldas järelevalvet komisjoni üle ning föderaalkantsleril oli mis tahes ajal võimalik saada teavet komisjoni töö kohta.

198 *Ibid.*, punktid 17 ja 29.

199 *Ibid.*, punkt 23.

200 *Ibid.*, punkt 25.

201 *Ibid.*, punkt 27.

202 ELK, C-614/10, *Euroopa Komisjon vs. Austria Vabariik*, 16. oktoober 2012, punktid 59 ja 63.

Näide: kohtuasjas *Euroopa Komisjon vs. Ungari*[203] tõi ELK välja, et "nõue tagada, et andmekaitseasutus suudaks teostada ülesandeid, mis on talle usaldatud, täielikult iseseisvalt, kaasneb liikmesriikidele kohustus lubada sellel asutusel teenida terve ametiaeg" ja leidis, et "enneaegselt lõpetades andmekaitseasutuse töö, Ungari ei ole täitnud oma kohustust, lähtuvalt direktiivist 95/46/EC."

Järelevalveasutustel on riikide õigusaktide alusel muu hulgas järgmised pädevused ja volitused[204]:

- vastutavate töötlejate ja andmesubjektide nõustamine kõikides andmekaitsega seotud küsimustes;
- töötlemistoimingute uurimine ja sekkumine vastavalt vajadusele;
- vastutavate töötlejate hoiatamine või neile märkuse tegemine;
- andmete parandamiseks, sulgemiseks, kustutamiseks või hävitamiseks korralduse andmine;
- ajutiselt või lõplikult töötlemise keelamine;
- küsimuse suunamine kohtule.

Oma ülesannete täitmiseks peab järelevalveasutusel olema võimalus tutvuda kõikide järelepärimise jaoks vajalike isikuandmete ja teabega, samuti peab tal olema ligipääs kõikidele ruumidele, kus vastutav töötleja asjakohast teavet hoiab.

Riikide jurisdiktsioonides esineb järelevalveasutuste tehtud järeldustega seotud menetluste ja nende õigusliku mõju puhul märkimisväärseid erinevusi. Need varieeruvad ombudsmanidele omastest soovitustest viivitamata täidetavate otsusteni. Seega tuleb teatavas jurisdiktsioonis kättesaadavate õiguskaitsevahendite tõhususe hindamisel arvesse võtta asjaomaseid tingimusi.

203 ELK, C-288/12, *Euroopa Komisjon vs. Ungari*, 8 aprill 2014, punktid 50 ja 67.

204 Andmekaitsedirektiivi artikkel 28; konventsiooni nr 108 lisaprotokolli artikkel 1.

5.3. Õiguskaitsevahendid ja karistused

Põhipunktid

- Konventsiooni nr 108 ja ka andmekaitsedirektiivi kohaselt tuleb riigi õigusaktidega ette näha asjakohased õiguskaitsevahendid ja karistused juhtudeks, kui rikutakse õigust isikuandmete kaitsele.
  - Õigus tõhusale õiguskaitsevahendile tähendab ELi õiguskorras, et riigi õigusaktides tuleb sätestada õiguskaitsevahendid seoses juhtumitega, kus on rikutud andmekaitsega seotud õigusi, sõltumata järelevalveasutuse poole pöördumise võimalusest.
  - Riikide õigusaktidega tuleb ette näha tõhusad, proportsionaalsed ja hoiatavad karistused, mis kehtivad kõikidele võrdsetel alustel.
- Enne kohtu poole pöördumist tuleb esmalt pöörduda vastutava töötleja poole. See, kas enne kohtusse hagi esitamist tuleb pöörduda ka järelevalveasutuse poole, määratakse kindlaks riigi õigusaktides.
- Andmesubjektid võivad andmekaitseõiguse rikkumiste asjus viimase abinõuna ja teatavatel tingimustel pöörduda EIK poole.
- Peale selle saavad nad pöörduda ka ELK poole, kuid üksnes väga piiratud ulatuses.

Andmekaitseõigusest tulenevaid õigusi saab kasutada üksnes see isik, kelle õigused on kõne all, st isik, kes on või vähemalt väidab end olevat andmesubjekt. Andmesubjekte võivad nende õiguste kasutamisel esindada isikud, kes vastavad riigi õigusaktide alusel teatavatele nõuetele. Alaealisi esindavad nende vanemad või eestkostjad. Järelevalveasutuste poole pöördumisel võivad andmesubjekti esindada ka ühendused, kelle õiguspärane eesmärk on seista andmekaitsega seotud õiguste eest.

5.3.1. Vastutavale töötlejale esitatavad taotlused

Jaotises 3.2 kirjeldatud õiguste kasutamiseks tuleb esmajärjekorras pöörduda vastutava töötleja poole. Kohe riigi tasandi järelevalveasutuse või kohtu poole pöördumisest ei oleks abi, sest järelevalveasutus soovitaks esmalt ühendust võtta vastutava töötlejaga ning kohus tunnistaks asjaomase hagiavalduse vastuvõetamatuks. Vastutavale töötlejale esitatavate juriidilises mõttes asjakohaste taotluste vorminõuded, eriti asjaolu, kas need peavad olema kirjalikus vormis, tuleks kindlaks määrata riigi õigusaktidega.

Üksus või isik, kellele taotlus on vastutava töötlejana suunatud, peab taotlusele vastama, isegi juhul, kui ta ei ole vastutav töötleja. Andmesubjekt peab vastuse saama igal juhul õigusaktidega kindlaksmääratud tähtaja jooksul, ka olukorras, kus teatatakse, et taotlejat käsitlevaid andmeid ei töödelda. Kooskõlas andmekaitsedirektiivi artikli 12 punktis a ja konventsiooni nr 108 artikli 8 punktis b esitatud sätetega tuleb taotlust käsitleda ilma liigsete viivitusteta. Seepärast tuleks riigi õigusaktides taotlusele vastamise puhul kindlaks määrata tähtaeg, mis on piisavalt lühike, kuid võimaldab samal ajal vastutaval töötlejal taotlusega asjakohasel viisil tegeleda.

Enne taotlusele vastamist peab isik või üksus, kelle poole vastutava töötlejana pöörduti, konfidentsiaalsusnõuete tõsise rikkumise vältimiseks kindlaks tegema, kas taotleja on ka päriselt see isik, kelle ta väidab end olevat. Kui isiku tuvastamise nõuded ei ole eraldi kindlaks määratud riigi õigusaktides, peab nende küsimuses otsuse tegema vastutav töötleja. Õiglase töötlemise põhimõtte kohaselt ei tohiks aga vastutavad töötlejad rakendada isiku tuvastamise puhul (ning taotluse autentsuse puhul, nagu kirjeldatud jaotises 2.1.1) liigselt koormavaid tingimusi.

Riikide õigusaktides tuleb kindlaks määrata ka see, kas vastutavad töötlejad võivad enne taotlusele vastamist nõuda taotlejalt teatava tasu maksmist – direktiivi artikli 12 punkti a ja konventsiooni nr 108 artikli 8 punkti b kohaselt peab andmetega tutvumist taotlev isik saama vastuse ilma liigsete kulutusteta. Paljude Euroopa riikide õigusaktides on sätestatud, et andmekaitseõiguse alusel esitatavatele taotlustele vastamise eest ei küsita tasu, kui vastamine ei nõua ülemääraseid ja tavapäratuid jõupingutusi; teisalt kaitsevad riikide õigusaktid tavaliselt vastutavaid töötlejaid taotlusele vastuse saamise õiguse kuritarvitamise eest.

Kui isik, institutsioon või asutus, kelle poole vastutava töötlejana pöörduti, ei lükka tagasi, et ta on vastutav töötleja, võib ta riigi õigusaktidega kindlaks määratud tähtaja jooksul:

- taotluse rahuldada ning teatada taotlejale, kuidas taotluses esitatud nõudmised täideti; või
- teatada taotlejale, miks taotluses esitatud nõudmisi ei täideta.

5.3.2. Järelevalveasutusele esitatavad avaldused

Kui vastutavale töötlejale andmetega tutvumise taotluse või vastuväite esitanud isik ei saa kindlaksmääratud tähtaja jooksul rahuldavat vastust, on tal võimalus taotleda

abi järelevalveasutuselt. Järelevalveasutuse algatatud menetluses tuleks välja selgitada, kas isik, institutsioon või asutus, kelle poole taotleja algselt pöördus, oli üldse kohustatud taotlusele vastama ning kas vastus oli õige ja piisav. Järelevalveasutus peab asjaomasele isikule teatama avalduse käsitlemiseks algatatud menetluse tulemusest[205]. Järelevalveasutuste algatatud menetluste tulemuste õiguslik tagajärg sõltub riigi õigusaktidest, kus määratakse kindlaks, kas järelevalveasutuse otsuseid saab ellu viia õiguslikul tasandil, st kas neid jõustavad avaliku võimu kandjad, või kas on vajadust pöörduda kohtu poole, kui vastutav töötleja ei täida järelevalveasutuse otsust (arvamus, märkus jms).

Olukorras, kus ELi institutsioonid või asutused on väidetavalt rikkunud ELi toimimise lepingu artikliga 16 tagatud andmekaitsega seotud õigusi, võib andmesubjekt esitada kaebuse Euroopa andmekaitseinspektorile,[206] kes määrati andmekaitsevaldkonna sõltumatuks järelevalveasutuseks ELi institutsioonide andmekaitse määrusega, milles sätestatakse Euroopa andmekaitseinspektori kohustused ja volitused. Kui Euroopa andmekaitseinspektor ei ole kuue kuu jooksul vastanud, tähendab see, et kaebus on tagasi lükatud.

Riigi järelevalveasutuse otsuste puhul peab olema võimalus kaevata need edasi kohtusse. See võimalus peab olema nii andmesubjektidel kui ka vastutavatel töötlejatel, kes on osalenud teatavas järelevalveasutuse algatatud menetluses.

Näide: 24. juulil 2013 avaldas Ühendkuningriigi teabevolinik otsuse, mille kohaselt ei tohtinud Hertfordshire'i politsei enam kasutada sõidukite registreerimismärkide jälgimise süsteemi, mis tunnistati ebaseaduslikuks. Kaamerate abil kogutud andmeid säilitati nii kohaliku politsei andmebaasides kui ka keskandmebaasis. Fotosid sõidukite registreerimismärkidest hoiti andmebaasides kahe aasta jooksul ning fotosid sõidukitest 90 päeva jooksul. Kokkuvõttes leiti, et kaamerate ja muude jälgimisvahendite laiaulatuslik kasutamine ei olnud proportsionaalne probleemiga, mida selle abil lahendada püüti.

205 Andmekaitsedirektiivi artikli 28 lõige 4.

206 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, EÜT L 8, 2001.

5.3.3. Kohtule esitatav avaldus

Kui isik, kes on esitanud vastutavale töötlejale andmekaitseõiguse alusel taotluse, ei ole vastutava töötleja vastusega rahul, peab taotlejal andmekaitsedirektiivi kohaselt olema õigus esitada kaebus riigi tasandi kohtule[207].

See, kas enne kohtusse hagiavalduse esitamist tuleb esmajärjekorras pöörduda ka järelevalveasutuse poole, määratakse kindlaks riigi õigusaktides. Enamikul juhtudel aga tuleb kasuks, kui isik pöördub andmekaitsega seotud õiguste kasutamisel esmalt järelevalveasutuse poole, sest nendelt abi taotlemine peaks olema tasuta ning ei tohiks olla üleliia bürokraatlik. Järelevalveasutuse otsuses (arvamus, märkus jms) sisalduvad eksperdihinnangud võivad andmesubjektile abiks olla ka oma õiguste kasutamiseks kohtu poole pöördumisel.

Euroopa Nõukogu õiguses võib juhtudel, kus väidetavalt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni osalisriigi tasandil on rikutud andmekaitsega seotud õigusi ning samal ajal on tegemist Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega, peale selle pöörduda ka EIK poole, kui riigi tasandi õiguskaitsevahenditest ei ole abi olnud. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise suunamiseks Euroopa Inimõiguste Kohtusse peab kaebus vastama teatavatele vastuvõetavuse kriteeriumidele (Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklid 34–37)[208].

Kuigi Euroopa Inimõiguste Kohtule võib avaldusi esitada vaid konventsiooniosaliste vastu, võidakse nendes kaudselt käsitleda ka eraõiguslike isikute tegevust või tegevusetust, juhul kui konventsiooniosaline ei ole täitnud Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist tulenevaid positiivseid kohustusi ning taganud oma õigusaktidega piisavat kaitset andmekaitsega seotud õiguste rikkumiste eest.

> Näide: kohtuasjas *K.U. vs. Soome*[209] väitis kaebuse esitaja (alaealine), et tema kohta oli internetis ühel tutvumissaidil avaldatud seksuaalse alatooniga kuulutus. Soome õigusaktidest tulenevate konfidentsiaalsuskohustuste tõttu ei avalikustanud internetiteenuse osutaja teabe üles laadinud isiku identiteeti. Kaebuse esitaja väitis, et olukorras, kus eraisik avaldas tema kohta internetis süüstavaid

207 Andmekaitsedirektiivi artikkel 22.

208 Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklid 34–37, kättesaadav: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 EIK, *K.U. vs. Soome*, nr 2872/02, 2. detsember 2008.

andmeid, ei olnud talle Soome õigusaktidega tagatud piisavat kaitset. EIK leidis, et riikidel ei ole mitte üksnes kohustust hoiduda meelevaldsest sekkumisest üksikisikute eraellu, vaid neil on ka positiivsed kohustused, mis hõlmavad selliste meetmete vastuvõtmist, mille eesmärk on tagada eraelu austamine ka üksikisikute omavaheliste suhete valdkonnas. Kaebuse esitaja juhtumi puhul tulnuks selleks, et teda reaalselt ja tulemuslikult kaitsta, võtta tõhusaid meetmeid rikkuja isiku tuvastamiseks ning tema süüdimõistmiseks. Riik aga sellist kaitset ei pakkunud ning kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Näide: kohtuasjas *Köpke vs. Saksamaa*[210] käsitleti juhtumit, kus kaebuse esitajat kahtlustati varguses töökohal ning teda asuti seetõttu varjatud videovalve abil jälgima. EIK järeldas, et kõnealuses juhtumis ei olnud mingeid märke sellest, et riigi ametiasutused ei olnud suutnud oma kaalutlusruumi piires tagada kaebuse esitajale tema õigust eraelu austamisele artikli 8 tähenduses ning võtta seejuures samaväärselt arvesse nii tööandja huvi kaitsta oma õigust omandile kui ka avalikku huvi tagada nõuetekohane õigusemõistmine. Seepärast tunnistati avaldus vastuvõetamatuks.

Kui EIK teeb kindlaks, et teatav osalisriik on rikkunud ükskõik millist Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga kaitstavat õigust, peab asjaomane riik EIK otsust täitma. Täitemeetmete rakendamisel tuleb esmalt peatada rikkumine ja võimaluse piires hüvitada kaebuse esitajale tekkinud negatiivsed tagajärjed. Kohtuotsuste täitmiseks võib vaja minna ka üldmeetmeid, et edaspidi selliseid kohtu avastatud juhtumitega sarnanevaid rikkumisi vältida, kas siis õigusaktide muutmise kaudu, kohtupraktika või muude meetmete abil.

Kui EIK teeb kindlaks Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni rikkumise, võib kohus konventsiooni artikli 41 kohaselt määrata kaebuse esitajale asjaomase osalisriigi kulul õiglase hüvitise.

ELi õiguses[211] saavad riikides ELi andmekaitsealaste õigusaktide rakendamiseks kehtestatud õigusaktide rikkumiste ohvrid teatavatel juhtudel pöörduda ELK poole. On kaks võimalikku stsenaariumi seoses sellega, kuidas andmesubjekti väide, et tema andmekaitsega seotud õigusi on rikutud, võib jõuda ELK menetlusse.

210 EIK, *Köpke vs. Saksamaa* (vastuvõetavuse otsus), nr 420/07, 5. oktoober 2010.

211 EL (2007), Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut, sõlmitud Lissabonis 13. detsembril 2007, ELT C 306, 2007. Vt ka Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioone (ELT C 326, 2012).

Esimese stsenaariumi puhul peab andmesubjekt olema otseselt kannatada saanud teatava ELi haldusdokumendi või õigusakti tagajärjel, millega rikutakse asjaomase üksikisiku õigust isikuandmete kaitsele. ELi toimimise lepingu artikli 263 lõikes 4 sätestatakse:

> *„Iga füüsiline või juriidiline isik võib [...] esitada hagi temale adresseeritud või teda otseselt ja isiklikult puudutava akti vastu ning üldkohaldatava akti vastu, mis puudutab teda otseselt ja ei sisalda rakendusmeetmeid."*

Seega võib isik, kelle andmeid on ebaseaduslikult töödelnud teatav ELi asutus, esitada edasikaebuse otse Euroopa Liidu Üldkohtule, mis on pädev tegema otsuseid ELi institutsioonide andmekaitse määrusega seotud küsimustes. Võimalus esitada hagiavaldus otse ELK-le on isikul siis, kui tema õiguslikku seisundit mõjutab otseselt mõni ELi õigusnorm.

Teine stsenaarium on seotud ELK (Euroopa Kohtu) pädevusega teha eelotsuseid, nagu on ette nähtud ELi toimimise lepingu artikliga 267.

Riigi tasandi kohtumenetlustes võivad andmesubjektid paluda liikmesriigi kohtul esitada Euroopa Kohtule taotlus selgituste saamiseks aluslepingute tõlgendamise või ELi institutsioonide, organite või asutuste õigusaktide kehtivuse ja tõlgendamise kohta. Selliseid selgitusi nimetatakse eelotsusteks. Need ei ole mõeldud otsese õiguskaitsevahendina kaebuse esitajale, ent eelotsuste abil saavad liikmesriikide kohtud veenduda, et nad tõlgendavad ELi õigusakte õigesti.

Kui riigi tasandi kohtumenetlusse kaasatud pool nõuab ELK-le eelotsusetaotluse esitamist, peavad seda tegema üksnes liikmesriigi kõrgeima astme kohtud, mille otsuseid ei saa edasi kaevata.

Näide: kohtuasjas *Kärntner Landesregierung jt*[212] esitas Austria konstitutsioonikohus eelotsusetaotluse ELK-le, küsides, kas direktiivi 2006/24/EÜ (andmete säilitamise direktiivi) artiklid 3–9 on kooskõlas põhiõiguste harta artiklitega 7, 9 ja 11 ning kas teatavad Austria föderaalse telekommunikatsiooniseaduse sätted, mis kehtestati andmete säilitamise direktiivi ülevõtmiseks, vastavad andmekaitsedirektiivi ja ELi institutsioonide andmekaitse määruse aspektidele või mitte.

212 ELK liidetud kohtuasjades C-293/12 ja C594/12, *Digital Right Ireland ja Seitling jt*, 8 aprill 2014.

Üks konstitutsioonikohtu menetluses osalenud kaebuse esitaja, härra Seitlinger, märkis, et kasutab telefoni, internetti ja e-posti nii tööga seotud eesmärkidel kui ka eraviisiliselt. Sellest tulenevalt liigub tema saadetav ja vastu võetav teave avalikes telekommunikatsioonivõrkudes. Austria 2003. aasta telekommunikatsiooniseaduse alusel on teenuseosutajal, kellelt ta asjaomast teenust ostab, õiguslik kohustus koguda ja säilitada andmeid tema võrgukasutuse kohta. Seitlingeri arvates ei olnud tema isikuandmete kogumine ja säilitamine mingil viisil vajalik võrgus teabe punktist A punkti B toimetamisega seotud tehnilistel eesmärkidel. Samuti ei olnud nende andmete kogumine ja säilitamine isegi mitte kaudsel viisil vajalik arvete esitamiseks. Kindlasti ei olnud Seitlinger andnud nõusolekut oma isikuandmete kasutamiseks. Kõnealuseid lisaandmeid koguti ja säilitati ainuüksi Austria 2003. aasta telekommunikatsioonseaduse tõttu.

Seepärast esitas Seitlinger hagiavalduse Austria konstitutsioonikohtule, väites, et tema telekommunikatsiooniteenuse osutajale määratud kohustuste täitmisega rikutakse talle põhiõiguste harta artikliga 8 tagatud põhiõigusi.

ELK teeb otsuse üksnes talle suunatud eelotsusetaotluses esitatud küsimustes. Algses kohtuasjas langetab otsuse ikkagi riigi tasandi kohus.

Põhimõtteliselt peab ELK vastama talle esitatud küsimustele. Kohus ei saa eelotsuse tegemisest keelduda põhjusel, et asjaomane vastus ei oleks algset kohtuasja arvesse võttes ei asjakohane ega esitatud õigeaegselt. Keeldumiseks on alust aga juhul, kui küsimus ei kuulu ELK pädevusvaldkonda.

Lõpetuseks võib märkida, et juhtudel, kui ELi institutsioon või asutus on isikuandmete töötlemisel väidetavalt rikkunud ELi toimimise lepingu artikliga 16 tagatud andmekaitsega seotud õigusi, võib andmesubjekt anda asja Euroopa Liidu Üldkohtusse (ELi institutsioonide andmekaitse määruse artikli 32 lõiked 1 ja 4). Sama kehtib selliste rikkumiste küsimuses Euroopa andmekaitseinspektori tehtud otsuste puhul (ELi institutsioonide andmekaitse määruse artikli 32 lõige 3).

Kuigi ELi institutsioonide andmekaitse määrusega seotud küsimustes otsuste tegemine kuulub Euroopa Liidu Üldkohtu pädevusvaldkonda, peab ELi institutsiooni või asutuse töötaja volituste alusel tegutsev isik aga õiguskaitse taotlemiseks esitama edasikaebuse Euroopa Liidu Avaliku Teenistuse Kohtusse.

Näide: näide õiguskaitsevahenditest, mida ELi institutsioonides ja asutustes seoses andmekaitseküsimustega tehtud toimingute või otsuste vastu on võimalik kasutada, on kohtuasi *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*[213].

Bavarian Lager esitas Euroopa Komisjonile taotluse, et tutvuda komisjoni korraldatud ning väidetavalt asjaomasesse ettevõttesse puutunud juriidiliste küsimustega seotud koosoleku protokolli täisversiooniga. Komisjon ei rahuldanud ettevõtte taotlust andmetega tutvuda, põhjendades seda ülimuslike andmekaitsega seotud huvidega[214]. Bavarian Lager esitas selle otsuse kohta ELi institutsioonide andmekaitse määruse artiklile 32 tuginedes kaebuse ELK-le, täpsemalt Esimese Astme Kohtule (nüüdne Euroopa Liidu Üldkohus). Oma otsusega kohtuasjas T-194/04, *Bavarian Lager vs. komisjon,* tühistas Esimese Astme Kohus komisjoni otsuse, millega jäeti kaebuse esitaja taotlus andmetega tutvuda rahuldamata. Euroopa Komisjon kaebas selle otsuse edasi ELK alla kuuluvale Euroopa Kohtule. Euroopa Kohtu (suurkoda) otsustas Esimese Astme Kohtu otsuse tühistada ning kinnitas, et Euroopa Komisjonil oli õigus andmetega tutvumise taotlus rahuldamata jätta.

5.3.4. Karistused

Euroopa Nõukogu õiguses sätestatakse konventsiooni nr 108 artiklis 10, et iga osalisriik peab ette nägema asjakohased karistused ja õiguskaitsevahendid juhuks, kui rikutakse neid siseriikliku õiguse sätteid, mille alusel rakendatakse konventsioonis sätestatud peamisi andmekaitsepõhimõtteid[215]. **ELi õiguses** on andmekaitsedirektiivi artikliga 24 ette nähtud, et „liikmesriigid võtavad sobivaid meetmeid, et tagada käesoleva direktiivi sätete täielik rakendamine, ja sätestavad eelkõige sanktsioonid, mida kohaldatakse [...] sätete rikkumise puhul".

Mõlemas õigusaktis on liikmesriikidele jäetud suur kaalutlusruum asjakohaste karistuste ja õiguskaitsevahendite valikul. Kummaski õigusaktis ei anta täpsemaid suuniseid selle kohta, millised peaksid asjakohased karistused olema, ega esitata näiteid karistustest.

213 ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*, 29. juuni 2010.

214 Põhjenduse analüüsi vt: Euroopa andmekaitseinspektor (2011), „Public access to documents containing personal data after the Bavarian Lager ruling" (e k „Avalikkuse juurdepääs isikuandmeid sisaldavatele dokumentidele pärast Bavarian Lageri otsust"), Brüssel, Euroopa andmekaitseinspektor, kättesaadav: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 EIK, *I. vs. Soome*, nr 20511/03, 17. juuli 2008; EIK, *K.U. vs. Soome*, nr 2872/02, 2. detsember 2008.

Samal ajal tuleb silmas pidada järgmist:

> *„kuigi ELi liikmesriikidele on jäetud suur kaalutlusruum otsustada üksikisikutele ELi õigusaktidega tagatud õiguste kaitsmiseks kõige asjakohasemate meetmete üle, tuleks kooskõlas ELi lepingu artikli 4 lõikes 3 sätestatud lojaalse koostöö põhimõttega järgida tõhususe, võrdväärsuse, proportsionaalsuse ja mõjususega seotud miinimumnõudeid*[216]*."*

ELK on mitmel korral kinnitanud, et liikmesriigil ei ole karistuste kindlaksmääramisel oma õigusaktides täienisti vabad käed.

Näide: kohtuasjas *Von Colson ja Kamann vs. Land Nordrhein-Westfalen*[217] märkis ELK, et kõikidel teatava direktiivi adressaadiks olevatel liikmesriikidel on kohustus võtta siseriiklikus õiguses kõik vajalikud meetmed, et tagada direktiivi täielik mõju vastavalt selles sätestatud eesmärkidele. Kohus leidis, et kuigi liikmesriikidele on antud valikuvabadus direktiivi rakendamiseks võetavate meetmete ja vahendite puhul, ei tohi selline valikuvabadus mõjutada neile määratud kohustust. Eeskätt peab üksiksikul tõhusa õiguskaitsevahendi abil olema võimalus asjaomast õigust kogu selle sisu ulatuses kasutada ja jõustada. Reaalse ja tõhusa kaitse saavutamiseks tuleb õiguskaitsevahendite kasutamisel algatada karistus- ja/või kompensatsioonimenetlus, mille tulemusena määratakse rikkujale hoiatav karistus.

Kui ELi institutsioonid või asutused rikuvad ELi õigusakte, karistatakse neid ELi institutsioonide andmekaitse määruses sätestatud erivolituste tõttu üksnes distsiplinaarmenetluse kaudu. Määruse artikli 49 kohaselt kohaldatakse „[k]äesoleva määrusega ettenähtud kohustuste ettekavatsetud või hooletusest tingitud täitmatajätmise korral [...] Euroopa ühenduste ametniku või teenistuja suhtes distsiplinaarmenetlust [...]".

216 FRA, 2012, Euroopa Liidu Põhiõiguste Ameti arvamus andmekaitse reformipaketi ettepaneku kohta, 2/2012, Viin, 1. oktoober 2012, lk 27.

217 ELK, C-14/83, *Sabine von Kolson ja Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10. aprill 1984.

6

Andmete piiriülene liikumine

EL	Käsitletavad teemad	Euroopa Nõukogu
Andmete piiriülene liikumine		
Andmekaitsedirektiivi artikli 25 lõige 1 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003	Määratlus	Konventsiooni nr 108 lisaprotokolli artikli 2 lõige 1
Andmete vaba liikumine		
Andmekaitsedirektiivi artikli 1 lõige 2	ELi liikmesriikide vahel	
	Konventsiooni nr 108 osalisriikide vahel	Konventsiooni nr 108 artikli 12 lõige 2
Andmekaitsedirektiivi artikkel 25	Kolmandatesse riikidesse, kus on piisav andmekaitse tase	Konventsiooni nr 108 lisaprotokolli artikli 2 lõige 1
Andmekaitsedirektiivi artikli 26 lõige 1	Erandina kolmandatesse riikidesse	Konventsiooni nr 108 lisaprotokolli artikli 2 lõike 2 punkt a
Andmete piiratud liikumine kolmandatesse riikidesse		
Andmekaitsedirektiivi artikli 26 lõige 2 Andmekaitsedirektiivi artikli 26 lõige 4	Lepingutingimused	Konventsiooni nr 108 lisaprotokolli artikli 2 lõike 2 punkt b Lepingutingimuste koostamise juhend
Andmekaitsedirektiivi artikli 26 lõige 2	Siduvad kontsernisisesed eeskirjad	
Näited: ELi ja USA broneeringuinfo leping ELi ja USA SWIFT-leping	Spetsiaalsed rahvusvahelised lepingud	

Andmekaitsedirektiiviga ei nähta ainuüksi ette andmete vaba liikumist liikmesriikide vahel, vaid see hõlmab ka sätteid nõuete kohta, mida kohaldatakse isikuandmete edastamise suhtes väljaspool ELi asuvatesse kolmandatesse riikidesse. Ka Euroopa Nõukogu tunnistas, kui oluline on rakendada andmete piiriülese liikumise suhtes kolmandatesse riikidesse konkreetseid eeskirju, ning võttis seoses sellega 2001. aastal vastu konventsiooni nr 108 lisaprotokolli. Sellesse protokolli võeti üle konventsiooniosaliste ja ELi liikmesriikide õigusraamistikus andmete piiriülese liikumise puhul rakendatud peamised sätted.

6.1. Andmete piiriülese liikumise olemus

Põhipunktid

- Andmete piiriülene liikumine tähendab isikuandmete edastamist vastuvõtjale, kes on teises kohtualluvuses.

Konventsiooni nr 108 lisaprotokolli artikli 2 lõike 1 kohaselt on andmete piiriülene liikumine isikuandmete edastamine vastuvõtjale, kes on teises kohtualluvuses. Andmekaitsedirektiivi artikli 25 lõikes 1 käsitletakse „töödeldavate või pärast edastamist töötlemiseks kavandatud isikuandmete [edastamist] kolmandatesse riikidesse […]". Selline andmete edastamine peab toimuma täies kooskõlas konventsiooni nr 108 lisaprotokolli artiklis 2 ning ELi liikmesriikide puhul ka andmekaitsedirektiivi artiklites 25 ja 26 sätestatud eeskirjadega.

Näide: *Bodil Lindqvisti*[218] kohtuasjas märkis ELK, et „[…]toiming, mis seisneb veebilehel erinevatele isikutele osutamises ja nende individualiseerimises kas nime või muude vahendite, näiteks telefoninumbri või nende töötingimusi ja vaba aja harrastusi puudutava teabe alusel, on „isikuandmete täielikult või osaliselt automatiseeritud töötlemine" direktiivi 95/46 artikli 3 lõike 1 tähenduses".

Seejärel nentis kohus, et direktiivis sätestatakse ka erieeskirjad, mille eesmärk on tagada liikmesriikide tehtav kontroll isikuandmete edastamisel kolmandatesse riikidesse.

218 ELK, C-101/01, *Bodil Lindqvist*, 6. november 2003, punktid 27, 68 ja 69.

Arvestades aga esiteks interneti arengutaset direktiivi väljatöötamise ajal ja teiseks seda, et selles puuduvad interneti kasutamisele kohaldatavad sätted, „ei saa eeldada, et ühenduse seadusandja soovis mõistega „andmete edastamine kolmandatesse riikidesse" tulevikus hõlmata andmete sisestamist veebilehele isiku poolt [...], isegi kui andmed muutuvad seeläbi kättesaadavaks kolmandates riikides isikutele, kellel on nendega tutvumiseks vajalikud tehnilised vahendid".

„Kui tõlgendada direktiivi [...] nii, et „andmete edastamine kolmandatesse riikidesse" on toimunud iga kord, kui isikuandmed on sisestatud veebilehele, oleks selle edastamise puhul paratamatult tegu edastamisega kõikidesse kolmandatesse riikidesse, kus on interneti kasutamiseks vajalikud tehnilised vahendid. [Direktiivis] ette nähtud erikord muutuks seega internetitoimingute osas paratamatult üldiseks korraks. Niipea, kui komisjon [...] sedastab, et üksainus kolmas riik ei taga kaitse piisavat taset, oleksid liikmesriigid kohustatud tõkestama kõigi isikuandmete internetti paneku."

Põhimõte, et pelgalt (isiku)andmete avalikustamine ei kuulu andmete piiriülese liikumise alla, kehtib ka internetis kättesaadavate avalike registrite või meedia, näiteks (elektrooniliste) ajalehtede ja televisiooni kohta. Andmete piiriülese liikumise mõiste alla kuulub üksnes konkreetsetele vastuvõtjatele suunatud teabevahetus.

6.2. Andmete vaba liikumine liikmesriikide vahel või konventsiooniosaliste vahel

Põhipunktid

- Isikuandmete edastamist teise Euroopa Majanduspiirkonna liikmesriiki või teise konventsiooni nr 108 osalisriiki ei tohi piirata.

Euroopa Nõukogu õiguses peab konventsiooni nr 108 artikli 12 lõike 2 kohaselt konventsiooniosaliste vahel toimuma isikuandmete vaba liikumine. Riigi õigusaktidega ei tohi isikuandmete edastamist teisele konventsiooniosalisele kitsendada, välja arvatud juhul, kui:

- see on vajalik andmete eriomast laadi silmas pidades[219]; või

219 Konventsiooni nr 108 artikli 12 lõike 3 punkt a.

- see on vajalik selleks, et vältida andmete piiriülest liikumist kolmandatesse riikidesse käsitlevate riigi tasandi õigusnormide rikkumist[220].

ELi õiguses on andmekaitsedirektiivi artikli 1 lõikes 2 sätestatud, et isikuandmete vaba liikumist liikmesriikide vahel ei tohi piirata ega keelata põhjustel, mis on seotud andmekaitsega. Andmete vaba liikumise piirkonda laiendati Euroopa Majanduspiirkonna lepinguga,[221] mille alusel ühinesid siseturuga Island, Liechtenstein ja Norra.

Näide: kui mitmes ELi liikmesriigis, sealhulgas Sloveenias ja Prantsusmaal, asutatava rahvusvahelise ettevõtjate kontserni sidusettevõtja edastab isikuandmeid Sloveeniast Prantsusmaale, ei tohi sellist andmete liikumist Sloveenia õigusaktidega piirata ega keelata.

Kui aga sama Sloveenias tegutsev sidusettevõtja tahab neid isikuandmeid edastada USAs asuvale valdusettevõtjale, peab asjaomane andmeeksportija läbima Sloveenia õigusaktides kindlaks määratud menetlused seoses andmete piiriülese edastamisega kolmandatele riikidele, kus ei ole tagatud piisav andmekaitse tase, välja arvatud juhul, kui valdusettevõtja rakendab programmi Safe Harbour põhimõtteid (tegemist on vabatahtliku tegevusjuhendiga andmekaitse piisava taseme tagamiseks; vt jaotis 6.3.1).

Andmete piiriülese liikumise puhul EMP liikmesriikidesse eesmärkidel, mis ei ole seotud siseturuga, näiteks kuritegude uurimiseks, aga andmekaitsedirektiivi sätteid ei kohaldata ning seega ei kuulu see andmete vaba liikumise põhimõtte alla. Euroopa Nõukogu õiguses kuuluvad konventsiooni nr 108 ja selle lisaprotokolli kohaldamisalasse kõik valdkonnad, kuigi konventsiooniosalised võivad teha teatavaid erandeid. Kõik EMP liikmed on ühinenud ka konventsiooniga nr 108.

220 *Ibid.*, artikli 12 lõike 3 punkt b.

221 Nõukogu ja komisjoni otsus, 13. detsember 1993, Euroopa Majanduspiirkonna lepingu sõlmimise kohta Euroopa ühenduste, nende liikmesriikide ja Austria Vabariigi, Soome Vabariigi, Islandi Vabariigi, Liechtensteini Vürstiriigi, Norra Kuningriigi, Rootsi Kuningriigi ja Šveitsi Konföderatsiooni vahel, EÜT L 1, 1994.

6.3. Andmete vaba liikumine kolmandatesse riikidesse

Põhipunktid

- Isikuandmete edastamist kolmandatesse riikidesse ei tohi riigi tasandi andmekaitseõiguse alusel piirata juhul, kui:
  - vastuvõtja puhul on kindlaks tehtud, et tagatud on piisav andmekaitse tase;
  - see on vajalik andmesubjekti erihuvide tõttu või kaasinimeste ülekaalukate õigustpäraste huvide, eelkõige oluliste avalike huvide tõttu.
- Andmekaitse tase on kolmandas riigis piisav siis, kui selle riigi õigusaktides rakendatakse tõhusalt peamisi andmekaitsepõhimõtteid.
- ELi õiguses määrab teatava kolmanda riigi andmekaitse taseme piisavuse kindlaks Euroopa Komisjon. Euroopa Nõukogu õiguses võivad riigid oma õigusaktides ise otsustada, kuidas see kindlaks määratakse.

6.3.1. Andmete vaba liikumine piisava kaitse tingimustes

Euroopa Nõukogu õiguses võivad riigid oma õigusaktidega ette näha andmete vaba liikumise konventsiooniga ühinemata riikidesse, kui vastuvõtjariigis või organisatsioonis on andmete kavandatava edastamise puhul tagatud kaitse piisav tase[222]. See, kuidas välisriigi andmekaitse taset hinnatakse ning kes selle hindamise eest vastutab, otsustatakse riikide õigusaktides.

ELi õiguses käsitletakse andmekaitsedirektiivi artikli 25 lõikes 1 andmete vaba liikumist kolmandatesse riikidesse, kui kõnealune kolmas riik tagab andmekaitse piisava taseme. Asjaolu, et andmekaitse tase peab olema piisav, mitte samaväärne, tähendab, et andmekaitse rakendamise puhul on aktsepteeritavad eri meetmed. Andmekaitsedirektiivi artikli 25 lõike 6 kohaselt kuulub välisriikide andmekaitse taseme kindlaksmääramine Euroopa Komisjoni pädevusse; sel eesmärgil teeb komisjon andmekaitse taseme piisavuse otsuseid ja peab hindamisel nõu andmekaitsedirektiivi

222 Konventsiooni nr 108 lisaprotokolli artikli 2 lõige 1.

artikli 29 alusel loodud töörühmaga, kes on andnud olulise panuse artiklite 25 ja 26 tõlgendamisse[223].

Euroopa Komisjoni otsus andmekaitse taseme piisavuse kohta on siduva toimega. Kui komisjon avaldab *Euroopa Liidu Teatajas* otsuse teatava riigi andmekaitse taseme piisavuse kohta, peavad seda otsust järgima kõik EMP liikmesriigid ja nende asutused, mis tähendab, et asjaomasesse riiki võib andmeid edastada ilma riigi tasandi ametiasutustelt järele küsimata või luba taotlemata[224].

Euroopa Komisjonil on võimalus hinnata üksnes kindlaid osi riigi õigussüsteemist või piirduda teatava teemavaldkonnaga. Näiteks tegi komisjon andmekaitse taseme piisavuse otsuse Kanadas erasektori tulundustegevuse suhtes kohaldatavate õigusaktide puhul[225]. Samuti on mitu andmekaitse taseme piisavuse otsust tehtud andmete edastamise kohta ELi ja välisriikide vahel sõlmitud lepingute alusel. Nendes otsustes käsitletakse üksnes konkreetset tüüpi andmeedastust, näiteks broneeringuinfo edastamist lennuettevõtjatelt välisriikide piirikontrolliasutustele EList teatavatesse välisriikidesse suunduvatel lendudel (vt jaotis 6.4.3). Viimasel ajal ei nähta ELi ja kolmandate riikide vaheliste erilepingute alusel toimuval andmete edastamisel andmekaitse taseme piisavuse otsusteks üldiselt vajadust, kuna eeldatavasti tagab juba leping iseenesest andmekaitse piisava taseme[226].

223 Vt nt andmekaitsedirektiivi artikli 29 alusel loodud töörühm (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" (e k „Töödokument isikuandmete edastamise kohta kolmandatesse riikidesse – ELi andmekaitsedirektiivi artikli 26 lõike 2 kohaldamine andmete rahvusvahelist edastamist käsitlevate siduvate kontsernisiseste eeskirjade suhtes"), WP 74, Brüssel, 3. juuni 2003; andmekaitsedirektiivi artikli 29 alusel loodud töörühma 24. oktoobri 1995. aasta direktiivi 95/46/EÜ artikli 26 lõike 1 ühist tõlgendamist käsitlev töödokument, WP 114, Brüssel, 25. november 2005.

224 Korrapäraselt ajakohastatav loetelu riikidest, mille andmekaitse tase on tunnistatud piisavaks, on kättesaadav Euroopa Komisjoni õigusküsimuste peadirektoraadi kodulehel: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Euroopa Komisjon, 2002, komisjoni otsus 2002/2/EÜ, 20. detsember 2001, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ isikuandmete piisava kaitse kohta, nagu on ette nähtud Kanada isikuandmete kaitse ja elektrooniliste dokumentide seadusega, EÜT L 2, 2002.

226 Nt Ameerika Ühendriikide ja Euroopa Liidu vaheline leping, milles käsitletakse broneeringuinfo kasutamist ja edastamist USA Sisejulgeolekuministeeriumile (ELT L 215, 2012, lk 5–14), või Euroopa Liidu ja Ameerika Ühendriikide vaheline leping, mis käsitleb Euroopa Liidust pärinevate finantstehinguid käsitlevate sõnumiandmete töötlemist ja edastamist terroristide rahastamise jälgimisprogrammi raames (ELT L 8, 2010, lk 11–16).

Ühes kõige olulisemas andmekaitse taseme piisavuse otsuses ei käsitleta tegelikult konkreetselt õigusnorme[227]. Selle asemel on see seotud pigem tegevusjuhendi tasandil eeskirjadega, mida nimetatakse programmi Safe Harbour põhimõteteks. EL ja USA leppisid need põhimõtted kokku USA äriühingute puhul kasutamiseks. Programmiga Safe Harbour liitumiseks peab äriühing vabatahtlikult võtma USA kaubandusministeeriumi ees kohustuse põhimõtteid järgida ning kaubandusministeerium kannab äriühingu asjaomasesse nimekirja. Kuna andmekaitse taseme piisavuse üks olulisi osi on andmekaitse rakendamise tõhusus, on programmis Safe Harbour ette nähtud ka teatav riigi järelevalve – programmiga saavad ühineda ainult need ettevõtjad, kelle tegevust kontrollib USA föderaalne kaubanduskomisjon.

6.3.2. Andmete vaba liikumine erijuhtudel

Euroopa Nõukogu õiguses võib isikuandmeid konventsiooni nr 108 lisaprotokolli artikli 2 lõike 2 kohaselt edastada kolmandatesse riikidesse, kus andmekaitse tase ei ole piisav, juhul, kui andmete edastamine on ette nähtud riigi õigusaktidega ning see on vajalik:

- andmesubjekti erihuvide tõttu; või
- kaasinimeste ülekaalukate õiguspäraste huvide, eelkõige oluliste avalike huvide tõttu.

ELi õiguses hõlmab konventsiooni nr 108 lisaprotokolli sätetega sarnanevaid sätteid andmekaitsedirektiivi artikli 26 lõige 1.

Direktiivi alusel on andmete vaba liikumine kolmandasse riiki andmesubjekti huvides põhjendatud juhul, kui:

- andmesubjekt on andmete eksportimiseks andnud ühemõttelise nõusoleku;
- andmesubjekt sõlmib või kavatseb sõlmida lepingu, milles kehtestatakse otsesõnu, et andmeid edastatakse välismaal asuvale vastuvõtjale;
- vastutav töötleja ja kolmas isik sõlmisid andmesubjekti huvides lepingu;

227 Euroopa Komisjon (2000), komisjoni otsus 2000/520/EÜ, 26. juuli 2000, vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium, EÜT L 215, 2000.

- andmeid on vaja edastada andmesubjekti eluliste huvide kaitsmiseks;

- andmeid edastatakse avalikest registritest; sellisel juhul on tegemist ülimusliku huviga tagada laiema avalikkuse juurdepääs avalikes registrites säilitatavale teabele.

Kaasinimeste õigustatud huvides on andmete vaba piiriülene liikumine põhjendatud[228]:

- oluliste avalike huvidega seotud eesmärkidel, v.a riigi- või avaliku julgeoleku tagamine, mis ei kuulu andmekaitsedirektiivi kohaldamisalasse; või

- õigusnõuete koostamiseks, esitamiseks või kaitsmiseks.

Eespool osutatud juhtumeid tuleb käsitada eranditena eeskirjast, mille kohaselt peab andmete piiranguteta edastamiseks teistesse riikidesse asjaomases vastuvõtjariigis olema tagatud piisav andmekaitse tase. Erandeid tuleb alati tõlgendada kitsendavalt. Seda on korduvalt rõhutanud andmekaitsedirektiivi artikli 29 alusel loodud töörühm andmekaitsedirektiivi artikli 26 lõike 1 tõlgendamisel, eeskätt juhul, kui andmete edastamise arvatav õiguslik alus on andmesubjekti nõusolek[229]. Töörühm on järeldanud, et nõusoleku õiguslikku tähendust käsitlevad üldpõhimõtted kehtivad ka direktiivi artikli 26 lõike 1 kohta. Näiteks kui töösuhete puhul ei ole selge, et töötajad andsid oma nõusoleku vabatahtlikult, ei saa andmete edastamisel tugineda direktiivi artikli 26 lõike 1 punktile a. Sellisel juhul kehtib artikli 26 lõige 2, mille kohaselt peavad riikide andmekaitseasutused väljastama andmete edastamiseks loa.

228 Andmekaitsedirektiivi artikli 26 lõike 1 punkt d.

229 Vt eeskätt andmekaitsedirektiivi artikli 29 alusel loodud töörühma 24. oktoobri 1995. aasta direktiivi 95/46/EÜ artikli 26 lõike 1 ühist tõlgendamist käsitlev töödokument, WP 114, Brüssel, 25. november 2005.

6.4. Andmete piiratud edastamine kolmandatesse riikidesse

Põhipunktid

- Enne andmete eksportimist kolmandatesse riikidesse, kus ei ole tagatud piisav andmekaitse tase, peaks vastutav töötleja laskma kavandatavat andmeedastustoimingut kontrollida järelevalveasutusel.
- Andmete eksportimist kavandav vastutav töötleja peab selle kontrolli käigus näitama, et:
  - andmete edastamiseks vastuvõtjale on olemas õiguslik alus;
  - rakendatakse meetmeid, et tagada andmete asjakohane kaitse pärast nende üleandmist vastuvõtjale.
- Vastuvõtja piisava andmekaitse taseme tagamiseks võetavad meetmed võivad hõlmata järgmist:
  - andmeid eksportiva vastutava töötleja ja teisest riigist pärit vastuvõtja vahel sõlmitud lepingu tingimused;
  - siduvad kontsernisisesed eeskirjad, mis tavaliselt kehtivad andmete edastamise suhtes hargmaises ettevõtjate kontsernis.
- Andmete edastamist välisriikide ametiasutustele võidakse reguleerida ka rahvusvahelise erilepingute alusel.

Andmekaitsedirektiivis ja konventsiooni nr 108 lisaprotokollis on riikidele jäetud võimalus luua oma õigusaktidega süsteeme seoses andmete piiriülese liikumisega kolmandatesse riikidesse, kus ei ole tagatud piisav andmekaitse tase, juhul kui vastutav töötleja on võtnud erimeetmeid, mille eesmärk on tagada, et andmed oleksid pärast vastuvõtjale üleandmist piisaval määral kaitstud, ning kui vastutav töötleja suudab seda pädevale ametiasutusele tõendada. Seda nõuet on otsesõnu mainitud vaid konventsiooni nr 108 lisaprotokollis, ent ka andmekaitsedirektiivi puhul peetakse seda normiks.

6.4.1. Lepingutingimused

Nii **Euroopa Nõukogu** kui ka **ELi õiguses** käsitatakse võimaliku abinõuna vastuvõtja piisava andmekaitse taseme tagamiseks andmeid eksportiva vastutava töötleja ja kolmandas riigis asuva vastuvõtja vahel sõlmitud lepingu tingimusi.

ELi tasandil töötas Euroopa Komisjon andmekaitsedirektiivi artikli 29 alusel loodud töörühma abiga välja lepingu tüüptingimused, mis tunnistati komisjoni otsusega ametlikult tõendiks piisavast andmekaitse tasemest[230]. Kuna komisjoni otsused on liikmesriikidele täies ulatuses siduvad, peavad riikides andmete piiriülese liikumise järelevalve eest vastutavad ametiasutused neid lepingu tüüptingimusi oma menetlustes arvesse võtma[231]. Kui andmeid eksportiv vastutav töötleja ja kolmandas riigis asuv vastuvõtja lepivad kokku ja allkirjastavad kõnealused tüüptingimused, peaks see andma järelevalveasutusele küllalt tõendeid selle kohta, et andmekaitse tagamiseks rakendatakse piisavaid meetmeid.

Lepingu tüüptingimuste olemasolu ELi õigusraamistikus ei takista vastutavatel töötlejatel paika panemast muid ajutisi lepingutingimusi. Sellegipoolest tuleks nendega lõppkokkuvõttes tagada sama kaitsetase nagu lepingu tüüptingimuste puhul. Lepingu tüüptingimuste kõige olulisemad osad on järgmised:

- soodustatud kolmanda isiku säte, mis võimaldab andmesubjektidel kasutada lepingust tulenevaid õigusi, kuigi nad ise ei ole lepingut sõlminud;

- andmete vastuvõtja või importija nõustub andmeid eksportiva vastutava töötleja riigi järelevalveasutuse menetlusega ja/või kohtumenetlusega, kui peaks tekkima vaidlus.

Vastutavalt töötlejalt vastutavale töötlejale andmete edastamise puhul saab andmeid eksportiv vastutav töötleja nüüd valida kahe tüüptingimuste kogumi vahel[232]. Andmete edastamiseks vastutavalt töötlejalt volitatud töötlejale on ainult üks lepingu tüüptingimuste kogum[233].

230 Andmekaitsedirektiivi artikli 26 lõige 4.

231 ELi toimimise lepingu artikkel 288.

232 I kogum on esitatud järgmise otsuse lisas: Euroopa Komisjon (2001), komisjoni otsus 2001/497/EÜ, 15. juuni 2001, kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste kohta direktiivi 95/46/EÜ alusel, EÜT L 181, 2001; II kogum on esitatud järgmise otsuse lisas: Euroopa Komisjon (2004), komisjoni otsus 2004/915/EÜ, 27. detsember 2004, millega muudetakse otsust 2001/497/EÜ kolmandatesse riikidesse isikuandmete edastamise lepingu alternatiivsete tüüptingimuste kogumi kasutuselevõtu kohta, ELT L 385, 2004.

233 Euroopa Komisjon (2010), komisjoni otsus 2010/87/EL, 5. veebruar 2010, kolmandates riikides asuvatele volitatud töötlejatele isikuandmete edastamise lepingu tüüptingimuste kohta nõukogu ja Euroopa Parlamendi direktiivi 95/46/EÜ alusel, ELT L 39, 2010.

Euroopa Nõukogu õiguse puhul võib märkida, et konventsiooni nr 108 nõuandekomitee töötas välja lepingutingimuste koostamise juhendi[234].

6.4.2. Siduvad kontsernisisesed eeskirjad

Mitmepoolsed siduvad kontsernisisesed eeskirjad hõlmavad sageli samal ajal mitut Euroopa andmekaitseasutust[235]. Siduvatele kontsernisisestele eeskirjadele heakskiidu saamiseks tuleb nende projekt saata koos standarditud taotlusvormidega juhtivale ametiasutusele[236]. Juhtiva ametiasutuse saab kindlaks teha standarditud taotlusvormilt. See ametiasutus teavitab seejärel kõiki järelevalveasutusi nendes EMP liikmesriikides, kus on asutatud kontserni sidusettevõtjad, kuigi järelevalveasutuste osalus siduvate kontsernisiseste eeskirjade hindamise protsessis on vabatahtlik. Kuigi see ei ole kohustuslik, peaksid kõik asjaomased andmekaitseasutused kasutama hindamise tulemust oma ametlikes loamenetlustes.

6.4.3. Rahvusvahelised erilepingud

EL on sõlminud erilepingud kahte tüüpi andmeedastustoimingute puhul, mida kirjeldatakse alljärgnevalt.

Broneeringuinfo

Broneeringuinfot koguvad lennuettevõtjad lennupiletite broneerimisel ning see hõlmab lennureisija nime, aadressi, krediitkaardiandmeid ja istekoha numbrit. USA õiguskorras peavad lennuettevõtjad need andmed enne reisijate väljalendu

234 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (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" (e k „Juhend, milles käsitletakse lepingutingimuste koostamist andmekaitse tagamiseks isikuandmete edastamisel kolmandatesse riikidesse, kus ei ole tagatud andmekaitse piisav tase").

235 Asjakohaste siduvate kontsernisiseste eeskirjade sisu ja ülesehitust selgitatakse järgmistes dokumentides: andmekaitsedirektiivi artikli 29 alusel loodud töörühm (2008), „Working document setting up a framework for the structure of Binding Corporate Rules" (e k „Töödokument, milles luuakse siduvate kontsernisiseste eeskirjade ülesehituse raamistik"), WP 154, Brüssel, 24. juuni 2008; andmekaitsedirektiivi artikli 29 alusel loodud töörühm (2008), „Working document setting up a table with the elements and principles to be found in Binding Corporate Rules" (e k „Töödokument, milles esitatakse siduvates kontsernisisestes eeskirjades sisalduvate elementide ja põhimõtete tabel"), WP 153, Brüssel, 24. juuni 2008.

236 Andmekaitsedirektiivi artikli 29 alusel loodud töörühm (2007), „Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data" (e k „Soovitus 1/2007 isikuandmete edastamist käsitlevate siduvate kontsernisiseste eeskirjade heakskiitmise standardtaotlus"), WP 133, Brüssel, 10. jaanuar 2007.

avaldama sisejulgeolekuministeeriumile. See kehtib USAsse saabuvate või USAst väljuvate lendude puhul.

Et tagada lendude broneeringuinfo[237] turvalisus ja kooskõla direktiiviga 95/46/EU võeti 2004 aastal vastu "lendude broneeringuinfo paket", mis koosnes Ameerika Ühendriikide sisejulgeolekuministeeriumi soovitusdest.

Järgnevalt tühistati lendude broneeringuinfo pakett kohtu[238] poolt, mille tulemusena sõlmiti kaks eraldi kokkulepet. Esimeses lepingus, milles reguleeriti andmete jagamist ning haldamist ELi liikmesriikide ja USA vahel, mis allkirjastati 2007.

Sellel lepingul oli aga nii mõnigi puudus ning see asendati 2012 aastal õiguskindluse parandamiseks uue lepinguga[239]. Uues lepingus on tehtud olulisi täiendusi. Selles piiritletakse ja täpsustatakse eesmärke, milleks teavet võib kasutada, näiteks raske piiriülese kuritegevuse ja terrorismi vastu võitlemine. Broneeringuinfo säilitamise ja kasutamise tähtaega on rahvusvahelise raske kuritegevuse puhul lühendatud 15 aastalt 10 aastale (terrorismi puhul jäi tähtajaks 15 aastat) ning sätestatud on nõue, et kõik andmed tuleks kuue kuu möödudes anonüümseks muuta. Samuti on üksikisikutel lepingu alusel võimalus tutvuda oma broneeringuinfoga, mida USA ametiasutustes säilitatakse. Kui teave ei ole õige, tuleb seda muuta või see kustutada – varem sellist võimalust ei olnud. Andmete väärkasutamise korral on kõigil õigus taotleda haldus- ja õiguskaitset kooskõlas USA õigusaktidega. Samuti on neil õigus oma broneeringuinfoga tutvuda ning taotleda sisejulgeolekuministeeriumilt andmete parandamist, seahulgas kustutamist, kui andmed ei ole õiged.

1. juulil 2012 jõustunud leping kehtib seitse aastat, st 2019. aastani.

2011. aasta detsembris kiitis Euroopa Liidu Nõukogu heaks ELi ja Austraalia vahelise uuendatud broneeringuinfo töötlemist ja edastamist käsitleva lepingu[240]. ELi ja

237 Euroopa Ülemkogu otsus 2004/496/EU, 17 mai 2014 ja otsus 2004/535/EU, 14 mai 2004.

238 ELK liidetud kohtuasjad C-317/04 ja C-318/04, *Euroopa Parlament vs.Euroopa Komirjon*, 30 mai 2006, par. 57,58 ja 59.

239 Nõukogu otsus 2012/472/EL, 26. aprill 2012, Ameerika Ühendriikide ja Euroopa Liidu vahelise lepingu (milles käsitletakse broneeringuinfo kasutamist ja edastamist USA Sisejulgeolekuministeeriumile) sõlmimise kohta, ELT L 215, 2012, lk 4. Lepingu tekst on lisatud sellele otsusele, ELT L 215, 2012, lk 5–14.

240 Nõukogu otsus 2012/381/EL, 13. detsember 2011, mis asendas aasta 2008 kokkulepet, Euroopa Liidu ja Austraalia vahelise lepingu (milles käsitletakse lennuettevõtjate poolt broneeringuinfo töötlemist ja edastamist Austraalia Tolli- ja Piirivalveametile) sõlmimise kohta, ELT L 186, 2012, lk 3. Lepingu tekst on lisatud sellele otsusele, ELT L 186, 2012, lk 4–16.

Austraalia vaheline broneeringuinfot käsitlev leping on järjekordne edusamm ELi tegevuskavas, mis hõlmab broneeringuinfo üldsuuniseid,[241] ELi broneeringuinfo süsteemi loomist[242] ja lepinguläbirääkimisi kolmandate riikidega[243].

Finantstehinguid käsitlevad sõnumiandmed

Enamiku Euroopa pankadest tehtavate ülemaailmsete rahaülekannete puhul volitatud töötlejana tegutseva Ülemaailmse Pankadevahelise Finantstelekommunikatsiooni Ühingu (SWIFT; peakorter asub Belgias) üks peegelandmetöötluskeskus asusUSAs ning USA rahandusministeerium nõudis neilt andmete avaldamist terrorismivastaste uurimiste jaoks[244].

ELi seisukohalt ei olnud SWIFTil õiguslikku alust avaldada neid olulisel määral Euroopa-keskseid andmeid, millega USA rahandusministeerium sai tutvuda ainult seepärast, et kõnealune SWIFTi andmetöötluskeskus asus USAs.

2010. aastal sõlmisid EL ja USA erilepingu, SWIFT-lepingu, et luua vajalik õiguslik alus ning tagada piisav andmekaitse tase[245].

Selle lepingu alusel edastatakse siiani SWIFTi säilitatavaid finantsandmeid USA rahandusministeeriumile terrorismi või selle rahastamise tõkestamise, uurimise või

241 Vt eeskätt komisjoni teatis broneeringuinfo kolmandatele riikidele edastamist käsitleva üldise lähenemisviisi kohta, KOM(2010) 492 (lõplik), Brüssel, 21. september 2010.

242 Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks, KOM(2011) 32 (lõplik), Brüssel, 2. veebruar 2011. 2011. aasta aprillis palus Euroopa Parlament Euroopa Liidu Põhiõiguste Ametil avaldada arvamust kõnealuse ettepaneku ja selle kooskõla kohta Euroopa Liidu põhiõiguste hartaga. Vt: FRA, 2011, Arvamus 1/2011 – broneeringuinfo, Viin, 14. juuni 2011.

243 Praegu peab EL läbirääkimisi broneeringuinfot käsitleva lepingu sõlmimiseks Kanadaga, mis jõustumisel asendaks praaegu jõus oleva kokkuleppe.

244 Vt sellega seoses: andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 14/2011 rahapesu ja terrorismi rahastamise tõkestamisega seotud andmekaitseküsimuste kohta, WP 186, Brüssel, 13. juuni 2011; andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 10/2006 SWIFT-võrgus isikuandmete töötlemise kohta, WP 128, Brüssel, 22. november 2006; Commission de la protection de la vie privée (2008), „Control and recommendation procedure initiated with respect to the company SWIFT scrl" (e k „Kontrollimenetlus ja soovituse avaldamine äriühingu SWIFT scrl puhul", otsus, 9. detsember 2008.

245 Nõukogu otsus 2010/412/EL, 13. juuli 2010, Euroopa Liidu ja Ameerika Ühendriikide vahelise lepingu (mis käsitleb finantstehinguid käsitlevate sõnumiandmete töötlemist ja edastamist Euroopa Liidust Ameerika Ühendriikidesse terroristide rahastamise jälgimise programmi raames) sõlmimise kohta, ELT L 195, 2010, lk 3–4. Lepingu tekst on lisatud sellele otsusele, ELT L 195, 2010, lk 5–14.

avastamise või nende eest kohtulikule vastutusele võtmise eesmärgil. USA rahandusministeerium võib SWIFTilt finantsandmeid küsida, kui taotluses:

- määratakse võimalikult selgelt kindlaks, milliseid finantsandmeid on vaja;
- põhjendatakse selgelt, miks neid andmeid on vaja;
- täpsustatakse võimalikult täpselt taotluse eesmärki, et nõutavate andmete kogus oleks võimalikult väike;
- ei nõuta ühtse euromaksete piirkonnaga (SEPA) seotud andmeid.

USA kaubandusministeerium saadab igast taotlusest koopia Europolile, kes teeb kindlaks, kas taotlus on kooskõlas SWIFT-lepingu põhimõtetega[246]. Kui Europol kinnitab, et kõik on korras, peab SWIFT finantsandmed edastama otse USA kaubandusministeeriumile. Ministeerium peab asjaomaseid finantsandmeid säilitama turvalises füüsilises keskkonnas, kus neile pääsevad ligi üksnes terrorismi või selle rahastamise uurimisega tegelevad analüütikud, ning neid andmeid ei tohi ühendada mõne muu andmebaasiga. Üldiselt kustutatakse SWIFTilt saadud finantsandmed hiljemalt viie aasta möödudes andmete vastuvõtmisest. Konkreetse uurimise või kohtulikule vastutusele võtmise jaoks vajalikke finantsandmeid võib säilitada nii kaua kui uurimise või kohtulikule vastutusele võtmise puhul tarvis.

USA rahandusministeerium võib SWIFTilt saadud andmetest pärit teavet edastada teatavatele USAs või mujal asuvatele õiguskaitse, avaliku julgeoleku või terrorismivastase võitlusega tegelevatele asutustele üksnes terrorismi või selle rahastamise tõkestamise, uurimise või avastamise või nende eest kohtulikule vastutusele võtmise eesmärgil. Kui edasi kavatsetakse saata finantsandmeid, mis on seotud ELi liikmesriigi kodaniku või alalise elanikuga, tohib selliseid andmeid kolmanda riigi ametiasutustega jagada üksnes asjaomase liikmesriigi pädevate asutuste eelneval nõusolekul. Erandid on lubatud juhul, kui andmete jagamine on äärmiselt vajalik avalikku julgeolekut ähvardava vahetu ja tõsise ohu vältimiseks.

SWIFT-lepingu põhimõtetest kinnipidamise üle teevad järelevalvet sõltumatud järelevaatajad, sealhulgas Euroopa Komisjoni määratud isik.

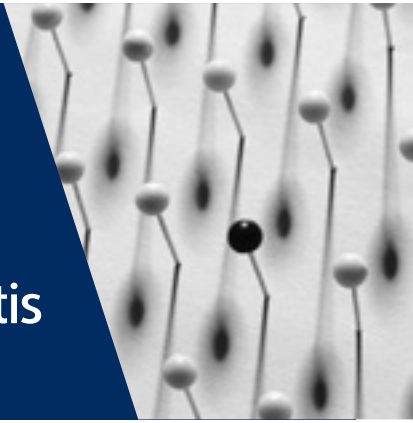
246 Europoli ühine järelvalveorgan on läbi vvinud audited Europoli tegevuse kohta antud valdkonnas, tulemused on kättesaadavad leheküljel: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

Andmesubjektidel on õigus saada pädevalt ELi andmekaitseasutuselt kinnitus selle kohta, kas andmete kasutamisel on austatud nende isikuandmete kaitsega seotud õigusi. Samuti on andmesubjektidel õigus lasta parandada, kustutada või sulgeda andmed, mida USA rahandusministeerium nende kohta SWIFT-lepingu alusel on kogunud ja säilitab. Andmesubjektide õiguse suhtes andmetega tutvuda võidakse teatavatel juhtudel kohaldada õiguslikke piiranguid. Kui andmetega tutvumise taotlust ei rahuldata, tuleb andmesubjekti sellest kirjalikult teavitada, sealhulgas sellest, et tal on õigus taotleda haldus- ja õiguskaitset USAs.

SWIFT-leping kehtib viis aastat, st 2015. aasta augustini. See pikeneb järgnevalt automaatselt üheaastate ajavahemike kaupa, kui üks lepinguosalistest ei anna teisele lepinguosalisele kirjalikult vähemalt kuus kuud enne teada, et ta ei kavatse lepingut enam pikendada.

7

Andmekaitse politsei ja kriminaalõiguse kontekstis



EL	Käsitletavad teemad	Euroopa Nõukogu
	Üldine	Konventsioon nr 108
	Politsei	Politseid käsitlev soovitus
		EIK, *B.B. vs. Prantsusmaa*, nr 5335/06, 17. detsember 2009
		EIK, *S. ja Marper vs. Ühendkuningriik*, nr 30562/04 ja 30566/04, 4. detsember 2008
		EIK, *Vetter vs. Prantsusmaa*, nr 59842/00, 31. mai 2005
	Küberkuritegevus	Küberkuritegevuse konventsioon
Andmekaitse politsei- ja kriminaalõigusasutuste piiriüleses koostöös		
Andmekaitse raamotsus	**Üldine**	Konventsioon nr 108
		Politseid käsitlev soovitus
Prümi otsus	**Eriliiki andmed: sõrmejäljed, DNA, huligaansus jne**	Konventsioon nr 108
		Politseid käsitlev soovitus
Europoli käsitlev otsus	**Eriagentuurid**	Konventsioon nr 108
Eurojusti käsitlev otsus		Politseiandmeid käsitlev soovitus
Frontexi määrus		
Teise põlvkonna Schengeni infosüsteemi käsitlev otsus	**Eriotstarbelised ühised infosüsteemid**	Konventsioon nr 108
		Politseid käsitlev soovitus
Viisainfosüsteemi käsitlev määrus		EIK, *Dalea vs. Prantsusmaa*, nr 964/07, 2. veebruar 2010
Eurodaci määrus		
Tolliinfosüsteemi käsitlev otsus		

Selleks et tasakaalustada üksikisiku huvi oma andmeid kaitsta ning ühiskonna huvi seoses andmete kogumisega kuritegevuse vastu võitlemiseks ning riigi- ja avaliku julgeoleku tagamiseks, on Euroopa Nõukogu ja EL kehtestanud konkreetsed õigusaktid.

7.1. Politsei- ja kriminaalõigusvaldkonna andmekaitsega seotud Euroopa Nõukogu õigusaktid

Põhipunktid

- Kõikide politsei tööga seotud valdkondade andmekaitset käsitletakse konventsioonis nr 108 ja Euroopa Nõukogu soovituses politsei kohta.
- Küberkuritegevuse (Budapesti) konventsioon on siduv rahvusvaheline õigusakt, milles käsitletakse elektrooniliste võrkude abil või selliste võrkude vastu toime pandud kuritegusid.

Euroopa tasandil hõlmab konventsioon nr 108 kõiki isikuandmete töötlemise valdkondi ning konventsiooni sätete eesmärk on reguleerida isikuandmete töötlemist üldises mõttes. Sellest tulenevalt kohaldatakse konventsiooni nr 108 politsei- ja kriminaalõiguse valdkonnaga seotud andmekaitsele, kuigi konventsiooniosalised võivad selle kohaldamisala piirata.

Politsei- ja kriminaalõigusasutustel on oma õigusjärgseid ülesandeid täites tihti vaja töödelda isikuandmeid, mis võib asjaomastele üksikisikutele kaasa tuua tõsiseid tagajärgi. Euroopa Nõukogu 1987. aastal vastu võetud soovituses politseiandmete kohta antakse konventsiooniosalistele suuniseid selle kohta, kuidas jõustada konventsiooni nr 108 põhimõtteid isikuandmete töötlemise puhul politseiasutustes[247].

7.1.1. Politseid käsitlev soovitus

EIK on mitmes kohtuasjas järeldanud, et isikuandmete salvestamise ja säilitamisega politsei- ja riiklikes julgeolekuasutustes sekkuti Euroopa inimõiguste ja

247 Euroopa Nõukogu ministrite komitee (1987), soovitus Rec(87)15 liikmesriikidele isikuandmete kasutamise kohta politseisektoris, 17. september 1987.

põhivabaduste kaitse konventsiooni artikli 8 lõikega 1 tagatud õiguste kasutamisse. Paljudes EIK otsustes käsitletakse selliste sekkumiste põhjendusi[248].

Näide: kohtuasjas *B.B. vs. Prantsusmaa*[249] otsustas EIK, et süüdimõistetud seksuaalkurjategija kandmine riigi kohtuandmebaasi kuulus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaldamisalasse. Kuna aga rakendati piisavaid andmekaitsega seotud tagatisi, näiteks andmesubjekti õigust taotleda andmete kustutamist, andmete säilitamise tähtaja piiramist ning piiratud juurdepääsu asjaomastele andmetele, saavutati kaalul olnud konkureerivate isiklike huvide ja avalike huvide vahel õiglane tasakaal. Kohus järeldas, et tegu ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Näide: kohtuasjas *S. ja Marper vs. Ühendkuningriik*[250] käsitleti juhtumit, kus mõlemat kaebuse esitajat süüdistati kuritegudes, kuid neid ei mõistetud süüdi. Sellegipoolest hoidis politsei alles nende sõrmejäljed, DNA-profiilid ja rakuproovid ning säilitas neid andmeid. Biomeetrilisi andmeid oli võimalik tähtajatult säilitada seaduse tõttu, mille järgi kahtlustati isikut kuriteos isegi siis, kui ta hiljem õigeks mõisteti või vabastati. EIK leidis, et isikuandmete üldise ja vahettegematu säilitamisega, mille puhul ei olnud kindlaks määratud selget tähtaega ja süüdistustest vabastatud üksikisikutel oli keeruline taotleda andmete kustutamist, sekkuti ebaproportsionaalselt kaebuse esitajate õigusesse eraelu austamisele. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Nii mõneski teises EIK otsuses on arutluse all olnud varjatud jälgimise kaudu isikuandmete kaitse õigusesse sekkumise põhjendused.

Näide: kohtuasjas *Allan vs. Ühendkuningriik*[251] käsitleti juhtumit, kus ametivõimud salvestasid salaja ühe kinnipeetu isiklikke vestlusi sõbraga vangla külastusalal ning kaassüüdistatavaga vangikambris. EIK leidis, et heli- ja videosalvestusseadmete kasutamist kaebuse esitaja kambris ja vangla külastusalal ning

248 Vt nt EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987; EIK, *M.M. vs. Ühendkuningriik*, nr 24029/07, 13. november 2012; EIK, *M.K. vs. Prantsusmaa*, nr 19522/09, 18. aprill 2013.

249 EIK, *B.B. vs. Prantsusmaa*, nr 5335/06, 17. detsember 2009.

250 EIK, *S. ja Marper vs. Ühendkuningriik*, nr 30562/04 ja 30566/04, 4. detsember 2008, punktid 119 ja 125.

251 EIK, *Allan vs. Ühendkuningriik*, nr 48539/99, 5. november 2002.

kaasvangi abiga võib käsitada sekkumisena kaebuse esitaja õigusesse eraelu austamisele. Kuna tol ajal ei olnud konkreetset õigusraamistikku seoses varjatud salvestusseadmete kasutamisega politseis, ei olnud kõnealune sekkumine kooskõlas õigusaktidega. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Näide: kohtuasjas *Klass jt vs. Saksamaa*[252] väitsid kaebuse esitajad, et mitu Saksamaa õigusakti, mis võimaldasid kirjade, postisaadetiste ja sidepidamise varjatud jälgimist, olid vastuolus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8, eeskätt sellepärast, et asjaomast isikut ei teavitatud jälgimismeetmetest ning et tal ei oleks olnud võimalust pärast jälgimismeetmete peatamist kohtusse pöörduda. EIK leidis, et jälgimise oht tähendas kindlasti sekkumist posti- ja telekommunikatsiooniteenuste kasutajate suhtlusvabaduse kasutamisse. Samal ajal märgiti, et kehtestatud olid piisavad kaitsemeetmed kuritarvitamise vältimiseks. On põhjendatud, et Saksamaa õigusaktides peeti selliseid meetmeid vajalikuks demokraatlikus ühiskonnas riigi julgeoleku tagamisel ning korratuse ja kuritegevuse vältimisel. Kohus järeldas, et tegu ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Kuna andmete töötlemine politseiasutustes võib asjaomaseid isikuid olulisel määral mõjutada, on üksikasjalikud andmekaitse-eeskirjad politseiandmebaaside haldamise kohta iseäranis vajalikud. Euroopa Nõukogu soovituses politsei kohta anti selle teema käsitlemiseks suuniseid järgmise kohta: kuidas koguda andmeid politsei töö tarbeks; kuidas tuleb selles valdkonnas andmefaile hoida; kellel peaks olema juurdepääs nendele andmetele, sealhulgas andmete välisriikide politseiasutustele edastamise tingimused; kuidas andmesubjektid peaksid saama kasutada andmekaitsega seotud õigusi; kuidas tuleks rakendada sõltumatute ametiasutuste tehtavat kontrolli. Samuti käsitletakse soovituses kohustust tagada piisav andmeturve.

Soovitusega ei nähta ette, et politseiasutused võivad andmeid koguda piiramatult ja valimatult. Selles on esitatud nõue, et politseiasutuste kogutavad isikuandmed peavad piirduma nende andmetega, mida on vaja reaalse ohu vältimiseks või konkreetse kuriteo tõkestamiseks. Täiendavaks andmete kogumiseks peab see olema ette nähtud konkreetsete riigi tasandi õigusaktidega. Tundlike andmete töötlemine peaks piirduma teatava uurimise kontekstis absoluutselt vajalike andmetega.

252 EIK, *Klass jt vs. Saksamaa*, nr 5029/71, 6. september 1978.

Kui isikuandmeid kogutakse andmesubjekti teadmata, tuleb andmesubjekti sellest teavitada kohe, kui andmete avaldamine ei ole enam uurimisele takistuseks. Andmete kogumine tehniliste valvesüsteemide või muude automatiseeritud vahendite abil peaks samuti põhinema konkreetsetel õigusnormidel.

Näide: kohtuasjas *Vetter vs. Prantsusmaa*[253] olid anonüümsed tunnistajad süüdistanud kaebuse esitajat mõrvas. Kuna kaebuse esitaja käis sageli ühel sõbral külas, pani politsei uuriva kohtuniku loal sõbra elukohta üles pealtkuulamisseadmed. Salvestatud vestlustele toetudes kaebuse esitaja vahistati ning talle esitati süüdistus mõrvas. Kaebuse esitaja esitas taotluse, et salvestis tunnistataks tõendusmaterjalina vastuvõetamatuks, põhjendades, et see ei olnud õigusaktidega ette nähtud. EIK arvates seisnes küsimus selles, kas pealtkuulamisseadmete kasutamine oli kooskõlas õigusaktidega. Eravalduste pealtkuulamine ei kuulunud ilmselgelt kriminaalmenetluse seadustiku artikli 100 ja järgnevate artiklite kohaldamisalasse, kuna nendes sätetes käsitleti telefoniliinide pealtkuulamist. Seadustiku artiklist 81 ei selgu piisaval määral, kui suures ulatuses või kuidas võivad ametivõimud isiklike vestluste pealtkuulamist lubada. Seda silmas pidades ei olnud kaebuse esitajale tagatud minimaalset kaitset, millele kodanikel on demokraatlikus ühiskonnas õigusnormide alusel õigus. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Soovituses järeldatakse, et isikuandmete säilitamisel tuleb selgelt eristada administratiivandmeid ja politseiandmeid, andmesubjektide eri kategooriaid, nt kahtlustatavad, süüdimõistetud, ohvrid ja tunnistajad, ning konkreetseteks faktideks ja kahtlustel või spekulatsioonidel põhinevateks loetavaid andmeid.

Politseiandmete puhul peab olema kindlalt piiritletud eesmärk. See mängib rolli seoses politseiandmetest teatamisega kolmandatele isikutele – selliste andmete edastamine või nendest teatamine politseisektoris peaks sõltuma sellest, kas teabe jagamiseks on õigustatud huvi. Selliste andmete edastamine või nendest teatamine väljaspool politseisektorit peaks olema lubatud üksnes juhul, kui selleks on sõnaselge õiguslik kohustus või luba. Rahvusvaheline andmete edastamine või andmetest teavitamine peaks piirduma üksnes välisriikide politseiasutustega ning põhinema konkreetsetel õigusnormidel, võib-olla ka rahvusvahelistel lepingutel, välja arvatud juhul, kui see on vajalik tõsise ja vahetu ohu vältimiseks.

253 EIK, *Vetter vs. Prantsusmaa*, nr 59842/00, 31. mai 2005.

Andmete töötlemist politseis peab riikide andmekaitseõiguse järgimise tagamiseks kontrollima sõltumatu järelevaataja. Andmesubjektidel peavad olema kõik konventsioonis nr 108 sätestatud õigused andmetega tutvuda. Kui andmesubjektide õigust andmetega tutvuda on piiratud konventsiooni nr 108 artikli 9 alusel tõhusa politseiuurimise huvides, peab andmesubjektil kooskõlas riigi õigusaktidega olema õigus esitada kaebus riigi andmekaitse järelevalveasutusele või mõnele muule sõltumatule asutusele.

7.1.2. Küberkuritegevuse Budapesti konventsioon

Ajal, kui kuritegevuses kasutatakse üha rohkem ära või mõjutatakse elektroonilisi andmetöötlussüsteeme, on probleemi käsitlemiseks vaja uusi kriminaalõigusnorme. Seepärast võttis Euroopa Nõukogu elektrooniliste võrkude vastu ja nende kaudu toime pandud kuritegude probleemiga tegelemiseks vastu rahvusvahelise õigusakti – küberkuritegevuse konventsiooni (nimetatakse ka Budapesti konventsiooniks)[254]. Selle konventsiooniga võivad ühineda ka muud riigid kui Euroopa Nõukogu liikmesriigid, kusjuures 2013. aasta keskpaigaks olid sellega ühinenud neli Euroopa Nõukogusse mitte kuuluvat riiki (Austraalia, Dominikaani Vabariik, Jaapan ja USA) ning veel 12 sellist riiki olid konventsiooni allkirjastanud või kutsutud sellega ühinema.

Küberkuritegevuse konventsioon on siiani kõige olulisem rahvusvaheline leping, milles käsitletakse internetis või muudes teabevõrkudes toime pandud õigusrikkumisi. Selle alusel peavad konventsiooniosalised oma kriminaalõigust ajakohastama ja ühtlustama häkkimist ja muid turvarikkumisi, sealhulgas autoriõiguste rikkumisi, arvuti abil sooritatud pettusi, lapspornot ja muud ebaseaduslikku kübertegevust silmas pidades. Samuti nähakse konventsiooniga ette menetluspädevused arvutivõrkude läbiotsimiseks ja sidepidamise pealtkuulamiseks küberkuritegevuse vastu võitlemise eesmärgil. Viimaks võiks märkida, et konventsioon võimaldab rahvusvahelist koostööd. Konventsiooni lisaprotokollis tunnistatakse kuritegelikuks rassistlik ja ksenofoobiline propaganda arvutivõrkudes.

Kuigi konventsiooni eesmärk ei ole õigupoolest andmekaitse edendamine, tunnistatakse sellega kuritegelikuks tegevus, millega võidakse rikkuda andmesubjekti õigust isikuandmete kaitsele. Samuti on konventsiooniga osalisriikidele ette nähtud kohustus, et konventsiooni rakendamisel tuleb tagada inimõiguste ja vabaduste,

254 Euroopa Nõukogu ministrite komitee (2001), Küberkuritegevuse konventsioon, CETS nr 185, Budapest, 23. november 2001, jõustus 1. juulil 2004.

sealhulgas Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist tulenevate õiguste piisav kaitse, nagu õigus isikuandmete kaitsele[255].

7.2. Politsei- ja kriminaalõigusvaldkonna andmekaitsega seotud ELi õigusaktid

Põhipunktid

- ELi tasandil reguleeritakse politsei- ja kriminaalõigusvaldkonna andmekaitset üksnes politsei- ja õigusasutuste piiriülese koostöö kontekstis.
- Eraldi andmekaitsekord on kahel piiriülest õiguskaitset toetaval ja edendaval ELi asutusel – Euroopa Politseiametil (Europol) ja ELi õigusalase koostöö üksusel (Eurojust).
- Eriotstarbelist andmekaitsekorda rakendatakse ka ELi tasandil pädevate politsei- ja õigusasutuste vahelise piiriülese teabevahetuse võimaldamiseks loodud ühiste teabesüsteemide puhul. Olulised näited sellistest süsteemidest on teise põlvkonna Schengeni infosüsteem, viisainfosüsteem ning Eurodac (tsentraliseeritud süsteem, milles säilitatakse ELi liikmesriikides varjupaika taotlevate kolmandate riikide kodanike sõrmejälgede andmeid).

Politsei- ja kriminaalõigusvaldkond ei kuulu andmekaitsedirektiivi kohaldamisalasse. Selle valdkonnaga seotud olulisimaid õigusakte kirjeldatakse jaotises 7.2.1.

7.2.1. Andmekaitse raamotsus

Kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitset käsitleva nõukogu raamotsuse 2008/977/JSK (andmekaitse raamotsus)[256] eesmärk on tagada füüsiliste isikute isikuandmete kaitse tingimustes, kus pädevad asutused koguvad või töötlevad nende isikuandmeid kuritegude vältimise, uurimise, avastamise või kuritegude eest vastutusele võtmise või kriminaalkaristuste täideviimise eesmärgil. Liikmesriikide või ELi nimel tegutsevad politsei- ja kriminaalõigusvaldkonna pädevad asutused. Need on ELi asutused või organid, samuti

255 *Ibid.*, artikli 15 lõige 1.

256 Euroopa Liidu Nõukogu (2008), nõukogu raamotsus 2008/977/JSK, 27. november 2008, kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta (andmekaitse raamotsus), ELT L 350, 2008.

liikmesriikide asutused[257]. Raamotsuse kohaldamisala hõlmab üksnes andmekaitse tagamist nende asutuste piiriüleses koostöös ning see ei laiene riigi julgeolekule.

Andmekaitse raamotsuses lähtutakse suures osas konventsioonis nr 108 ja andmekaitsedirektiivis esitatud põhimõtetest ja määratlustest.

Andmeid võib kasutada üksnes pädev asutus ning ainult sellel eesmärgil, mille jaoks need edastati või kättesaadavaks tehti. Vastuvõttev liikmesriik peab kinni pidama kõikidest andmeid edastava liikmesriigi õigusaktides andmete vahetamise puhul kehtestatud piirangutest. Teatavatel tingimustel võib aga vastuvõttev liikmesriik kasutada andmeid muudel eesmärkidel. Pädevatel asutustel on konkreetne kohustus registreerida ja dokumenteerida igasugune andmete edastamine, et aidata selgeks teha, milline vastutus kaasneb kaebustega. Piiriülese koostöö käigus saadud andmeid võib kolmandatele isikutele edasi saata üksnes selle liikmesriigi nõusolekul, kellelt andmed saadi, kuigi pakilistel juhtudel võidakse teha erandeid.

Pädevad asutused peavad võtma asjakohaseid turvameetmeid, et kaitsta isikuandmeid mis tahes ebaseadusliku töötlemise eest.

Iga liikmesriik peab tagama, et andmekaitse raamotsuse kohaselt vastu võetud sätete kohaldamise üle teeks järelevalvet ning pakuks asjakohast nõustamist üks või mitu riigi tasandi sõltumatut järelevalveasutust. Need asutused vaatavad samuti läbi kõigi isikute esitatud kaebused oma õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega pädevates asutustes.

Andmesubjektil on õigus saada teavet oma isikuandmete töötlemise kohta ja nende andmetega tutvuda ning õigus lasta andmed parandada, kustutada või sulgeda. Kui selliste õiguste kasutamist on vaja tungivatel põhjustel piirata, peab andmesubjektil olema õigus esitada kaebus pädevale riiklikule järelevalveasutusele ja/või kohtule. Kui isikule on tekitatud kahju andmekaitse raamotsuse rakendamiseks vastu võetud riigi tasandi õigusnormide rikkumisega, on tal õigus saada vastutavalt töötlejalt hüvitist[258]. Üldiselt peavad andmesubjektid saama kasutada õiguskaitsevahendeid, kui neile andmekaitse raamotsuse rakendamiseks vastu võetud riigi tasandi õigusnormidega tagatud õigusi rikutakse[259].

257 *Ibid.*, artikli 2 punkt h.

258 *Ibid.*, artikkel 19.

259 *Ibid.*, artikkel 20.

Euroopa Komisjon esitas ettepaneku reformipaketi kohta, mis hõlmab andmekaitse üldmäärust[260] ja andmekaitse ülddirektiivi[261]. Kõnealuse uue direktiiviga asendatakse andmekaitse raamotsus ning kriminaalasjades tehtava politsei- ja õigusalase koostöö puhul kohaldatakse üldpõhimõtteid ja -eeskirju.

7.2.2. Konkreetsemad õigusaktid seoses andmekaitsega politsei- ja õiguskaitseasutuste piiriüleses koostöös

Andmekaitse raamotsuse kõrval reguleeritakse liikmesriikide valduses oleva teabe vahetamist konkreetsetes valdkondades eri õigusaktidega, näiteks nõukogu raamotsusega 2009/315/JSK, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu, ning nõukogu otsusega liikmesriikide rahapesu andmebüroode vahelise koostöö korra kohta teabe vahetamisel[262].

On oluline märkida, et pädevate asutuste piiriülene koostöö[263] hõlmab järjest enam sisserändeandmete vahetamist. See õigusvaldkond ei kuulu politsei- ja kriminaalõigusküsimuste alla, ent on politsei- ja õigusasutuste töös nii mõneski aspektis asjakohane. Sama kehtib ELi imporditavaid või EList teistesse riikidesse eksporditavaid kaupu käsitlevate andmete kohta. Piirikontrolli kaotamine ELi sisepiiridel on suurendanud pettuste riski, mis tähendab, et liikmesriigid peavad tugevdama omavahelist koostööd, edendades eeskätt piiriülest teabevahetust, et tagada riikide ja ELi tasandi tollieeskirjade rikkumiste kiire avastamine ja nende eest vastutusele võtmine.

260 Euroopa Komisjon (2012), Ettepanek: Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), COM(2012) 11 (final), Brüssel, 25. jaanuar 2012.

261 Euroopa Komisjon (2012), Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv üksikisikute kaitse kohta seoses pädevates asutustes isikuandmete töötlemisega kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumise kohta, COM(2012) 10 (final), Brüssel, 25. jaanuar 2012.

262 Euroopa Liidu Nõukogu (2009), Nõukogu raamotsus 2009/315/JSK, 26. veebruar 2009, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu, ELT L 93, 2009; Euroopa Liidu Nõukogu (2009), Nõukogu otsus 2000/642/JSK, 17. oktoober 2000, liikmesriikide rahapesu andmebüroode vahelise koostöö korra kohta teabe vahetamisel, EÜT L 271, 2000.

263 Euroopa Komisjon (2012), komisjoni teatis Euroopa Parlamendile ja nõukogule: „Õiguskaitsekoostöö tugevdamine ELis: Euroopa teabevahetusmudel (EIXM)", COM(2012) 735 (final), Brüssel, 7. detsember 2012.

Prümi otsus

Oluline näide piiriülesest institutsioonilisest koostööst liikmesriikide valduses oleva teabe vahetamise kaudu on nõukogu otsus 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega (Prümi otsus), millega inkorporeeriti 2008. aastal ELi õigusesse Prümi leping[264]. Prümi leping on rahvusvahelise politseikoostöö leping, mille sõlmisid 2005. aastal Austria, Belgia, Prantsusmaa, Saksamaa, Luksemburg, Madalmaad ja Hispaania[265].

Prümi otsuse eesmärk on aidata liikmesriikidel parandada teabe jagamist kuritegevuse tõkestamiseks ja selle vastu võitlemiseks kolmes valdkonnas: terrorism, piiriülene kuritegevus ja ebaseaduslik ränne. Sel otstarbel on otsuses kehtestatud sätted järgmise kohta:

- automatiseeritud juurdepääs DNA-profiilidele, sõrmejälgede andmetele ja teatavatele riiklikele sõidukite registreerimisandmetele;
- andmete esitamine seoses piiriülese mõõtmega suursündmustega;
- teabe edastamine terroriaktide ärahoidmiseks;
- muud piiriülese politseikoostöö tõhustamise meetmed.

Prümi otsuse alusel kättesaadavaks tehtavaid andmebaase hallatakse üksnes riikide õigusaktide alusel, ent andmete vahetamist reguleeritakse täiendavalt ka kõnealuse otsusega ning viimasel ajal andmekaitse raamotsusega. Selliste andmevoogude järelevalve eest vastutavad pädevad asutused on riikide andmekaitse järelevalveasutused.

264 Euroopa Liidu Nõukogu (2008), nõukogu otsus 2008/615/JSK, 23. juuni 2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega, ELT L 210, 2008.

265 Konventsioon Belgia Kuningriigi, Saksamaa Liitvabariigi, Hispaania Kuningriigi, Prantsuse Vabariigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi ja Austria Vabariigi vahel piiriülese koostöö tõhustamiseks eelkõige seoses terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastase võitlusega; kättesaadav: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Andmekaitse Europolis ja Eurojustis

Europol

ELi õiguskaitseasutuse Europoli peakorter asub Haagis ning igal liikmesriigil on Europoli siseriiklik üksus. Europol asutati 1998. aastal; selle praegune õiguslik staatus ELi asutusena põhineb nõukogu otsusel, millega asutatakse Euroopa Politseiamet (Europoli käsitlev otsus)[266]. Europoli eesmärk on aidata kaasa organiseeritud kuritegevuse, terrorismi ja muude kahte või enamat liikmesriiki mõjutavate raskete kuriteovormide, mis on loetletud Europoli käsitleva otsuse lisas, ennetamisel ja nende uurimisel.

Eesmärkide saavutamiseks on Europolis loodud Europoli infosüsteem, mis pakub liikmesriikidele andmebaasi kriminaalteabe ja muu teabe vahetamiseks siseriiklike üksuste kaudu. Europoli infosüsteemi võib kasutada selliste andmete avaldamiseks, mis on seotud isikutega, keda kahtlustatakse või kes on süüdi mõistetud Europoli pädevusse kuuluva kuriteo toimepanemises, või isikutega, kelle kohta on faktilisi tõendeid selle kohta, et nad panevad toime Europoli pädevusse kuuluvaid kuritegusid. Europol ja siseriiklikud üksused võivad andmeid vahetult Europoli infosüsteemi sisestada ja nende kohta sealt väljavõtteid teha. Andmeid tohib muuta, parandada või kustutada üksnes andmed sisestanud pool.

Kui see on Europoli ülesannete täitmiseks vajalik, võib asutus säilitada, muuta ja kasutada kuritegusid käsitlevaid andmeid analüüsimiseks koostatud tööfailides. Analüüsimiseks koostatud tööfailid avatakse andmete kogumiseks, töötlemiseks või kasutamiseks kindlate Europoli ja ELi liikmesriikide koostöös uuritavate kriminaalasjade tarbeks.

Uute suundumuste arvessevõtmiseks loodi Europoli juurde 1. jaanuaril 2013 küberkuritegevuse vastase võitluse Euroopa keskus[267]. Keskus toimib ELi teabepunktina küberkuritegevuse valdkonnas, aidates kiiremini reageerida internetikuritegude korral, arendades ja rakendades digitaalkriminalistika suutlikkust ning luues pari-

266 Euroopa Liidu Nõukogu (2009), Nõukogu otsus, 6. aprill 2009, millega asutatakse Euroopa Politseiamet (Europol), ELT L 121, 2009. Vt ka komisjoni ettepanek määruse kohta, mis annab õigusraamistiku uuele Europolile, mis asendab nõukogu 6. aprilli 2009. aasta otsusega 2009/371/JSK asutatud Euroopa Politseiameti (Europoli) ja on selle õigusjärglane, ning nõukogu otsusega 2005/681/JSK asutatud politseikolledži ((CEPOLi), COM(2013) 173 (final).

267 Vt ka Euroopa andmekaitseinspektor (2012), Euroopa andmekaitseinspektori arvamuse kokkuvõte – komisjoni teatis nõukogule ja Euroopa Parlamendile: küberkuritegevuse vastase võitluse Euroopa keskuse loomine, Brüssel, 29. juuni 2012.

mat tava küberkuritegude uurimisel. Kõnealune asutus keskendub järgmistele küberkuritegudele:

- kuriteod, mille on toime pannud organiseeritud rühmitused suure kriminaaltulu saamise eesmärgil, näiteks internetipettused;
- kuriteod, mis põhjustavad ohvritele tõsist kahju, näiteks laste seksuaalne ärakasutamine internetikeskkonnas;
- kuriteod, mis häirivad elutähtsaid taristuid ja infosüsteeme ELis.

Europoli tegevust reguleerivat andmekaitsekorda täiustatakse pidevalt. Europoli käsitleva otsuse artiklis 27 on sätestatud, et Europol kohaldab konventsioonis nr 108 ja politseiandmeid käsitlevas soovituses esitatud põhimõtteid automatiseeritud ja mitteautomatiseeritud andmete töötlemise kohta. Andmete edastamisel Europoli ja liikmesriikide vahel tuleb järgida ka andmekaitse raamotsuses sätestatud eeskirju.

Selleks et tagada kohaldatavate andmekaitsealaste õigusaktide järgimine ning eeskätt see, et isikuandmete töötlemisel ei rikutaks üksikisiku õigusi, kontrollib ja jälgib Europoli tegevust sõltumatu Europoli ühine järelevalveasutus[268]. Igal üksikisikul on õigus tutvuda mis tahes isikuandmetega, mida võidakse Europolis tema kohta säilitada, samuti nõuda nende isikuandmete kontrollimist, parandamist või kustutamist. Kui isik ei ole rahul Europoli otsusega kõnealuste õiguste kasutamise küsimuses, võib ta otsuse edasi kaevata ühise järelevalveasutuse apellatsioonikomiteele.

Kahjude eest, mis tulenevad õiguslikest või faktivigadest Europoli säilitatavates või töödeldavates andmetes, võib kannatanud isik hüvitist taotleda üksnes selle liikmesriigi pädeva kohtu poole pöördudes, kus leidis aset kahju tekitanud juhtum[269]. Kui kahju tekkis seetõttu, et Europol ei täitnud oma õiguslikke kohustusi, maksab Europol hüvitisena makstava summa liikmesriigile tagasi.

268 Europoli käsitleva otsuse artikkel 34.

269 *Ibid.*, artikkel 52.

Eurojust

2002. aastal asutatud Eurojust on ELi asutus (peakorter Haagis), mis edendab õigusalast koostööd vähemalt kaht liikmesriiki mõjutavate raskete kuritegude uurimisel ja kohtu alla andmisel[270]. Eurojust täidab järgmisi ülesandeid:

- edendab ja parandab uurimiste ja kohtu alla andmise koordineerimist eri liikmesriikide pädevate asutuste vahel;

- toetab õigusalase koostööga seotud taotluste ja otsuste täitmist.

Eurojust täidab oma ülesandeid liikmesriikide kaudu. Iga liikmesriik lähetab Eurojusti ühe kohtuniku või prokuröri, kelle staatuse puhul kohaldatakse riigi õigusakte ning kellele on antud volitused täita ülesandeid eesmärgiga edendada ja parandada õigusalast koostööd. Peale selle tegutsevad liikmesriiki esindavad liikmed Eurojusti teatavate eriülesannete täitmiseks üheskoos kolleegiumina.

Eurojust võib töödelda isikuandmeid üksnes oma eesmärkide saavutamiseks. See piirdub konkreetse teabega inimeste kohta, keda kahtlustatakse Eurojusti pädevusse kuuluva kuriteo toimepanemises või selles osalemises või kes on sellise kuriteo eest süüdi mõistetud. Samuti võib Eurojust töödelda teavet Eurojusti pädevusse kuuluvate kuritegude tunnistajate või ohvrite kohta[271]. Erandjuhtudel võib Eurojust piiratud aja jooksul töödelda täiendavaid isikuandmeid, mis on seotud süüteo asjaoludega, kui need andmed on otseselt asjassepuutuvad ja seotud käimasoleva uurimisega. Oma pädevusala piires võib Eurojust koostööd teha teiste ELi institutsioonide, asutuste ja organitega ning nendega isikuandmeid vahetada. Samuti võib Eurojust koostööd teha ja isikuandmeid vahetada kolmandate riikide ja organisatsioonidega.

Seoses andmekaitsega peab Eurojust tagama sellise kaitse taseme, mis on vähemalt samaväärne tasemega, mis on ette nähtud Euroopa Nõukogu konventsiooni nr 108 ja sellesse hiljem tehtud muudatuste põhimõtetega. Andmete

270 Euroopa Liidu Nõukogu (2002), nõukogu otsus 2002/187/JSK, 28. veebruar 2002, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, EÜT L 63, 2002; Euroopa Liidu Nõukogu (2003), nõukogu otsus 2003/659/JSK, 18. juuni 2003, millega muudetakse nõukogu otsust 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, ELT L 44, 2003; Euroopa Liidu Nõukogu (2009), nõukogu otsus 2009/426/JSK, 16. detsember 2008, millega tugevdatakse Eurojusti ja muudetakse otsust 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, ELT L 138, 2009 (Eurojusti käsitlevad otsused).

271 Nõukogu otsus 2002/187/JSK, mida on muudetud nõukogu otsusega 2003/659/JSK ja nõukogu otsusega 2009/426/JSK, konsolideeritud versioon, artikli 15 lõige 2.

vahetamisel tuleb järgida erieeskirju ja -piiranguid, mis kehtestatakse kas koostöölepingus või töökorras kooskõlas Eurojusti käsitlevate nõukogu otsustega ja Eurojusti andmekaitse-eeskirjadega[272].

Eurojustis on loodud sõltumatu ühine järelevalveasutus, kes kontrollib isikuandmete töötlemist Eurojustis. Üksikisikud võivad esitada ühisele järelevalveasutusele kaebuse, kui nad ei ole rahul andmetega tutvumise või andmete parandamise, sulgemise või kustutamise taotlusele antud vastusega. Kui Eurojust töötleb isikuandmeid ebaseaduslikult, vastutab ta kooskõlas selle liikmesriigi õigusega, kus Eurojusti peakontor asub, (Madalmaad) kõigi andmesubjektile tekitatud kahjude eest.

7.2.4. Andmekaitse ELi tasandi ühistes infosüsteemides

Lisaks andmevahetusele liikmesriikide vahel ja piiriülese kuritegevuse vastu võitlemiseks ELi eriasutuste loomisele on ELi tasandil käivitatud mitu ühist infosüsteemi, mis oleks platvormiks andmete vahetamisele liikmesriikide pädevate asutuste ja ELi ametiasutuste vahel konkreetsetel õiguskaitsega, sealhulgas sisserändeõiguse ja tollieeskirjadega seotud eesmärkidel. Mõni neist süsteemidest põhineb mitmepoolsetel lepingutel, mida on hiljem täiendatud ELi õigusaktide ja süsteemidega, näiteks Schengeni infosüsteemi, viisainfosüsteemi, Eurodaci, Eurosuri või tolliinfosüsteemiga.

Teise põlvkonna Schengeni infosüsteemi, viisainfosüsteemi ja Eurodaci pikaajalise operatiivjuhtimise eest vastutab 2012. aastal asutatud Euroopa suuremahuliste IT-süsteemide amet (eu-LISA)[273]. Selle ameti põhiülesanne on tagada kõnealuste IT-süsteemide tõhus, turvaline ja pidev toimimine. Samuti vastutab see süsteemide ja andmete turvalisuse tagamiseks vajalike meetmete vastuvõtmise eest.

Schengeni infosüsteem

1985. aastal sõlmisid mitu tolleaegsete Euroopa ühenduste liikmesriiki lepingu Beneluxi Majandusliidu, Saksamaa ja Prantsusmaaga kontrolli järkjärgulise

272 Eurojusti isikuandmete töötlemist ja kaitset käsitleva töökorra sätted, ELT C 68, 2005, lk 1, 19. märts 2005.

273 Euroopa Parlamendi ja nõukogu määrus (EL) nr 1077/2011, 25. oktoober 2011, millega asutatakse Euroopa amet vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimiseks, ELT L 286, 2011.

kaotamise kohta nende ühispiiridel (Schengeni leping), et tagada isikute vaba liikumine ja kaotada piirikontroll Schengeni alal[274]. Selleks et tasakaalustada avalikku julgeolekut ohustavat mõju, mis avatud piiride tõttu tekkida võib, tugevdati piirikontrolli Schengeni ala välispiiridel ning samuti hakkasid tihedamat koostööd tegema riikide politsei- ja õigusasutused.

Kuna Schengeni lepinguga liitus veel mitu riiki, lõimiti Schengeni süsteem Amsterdami lepinguga[275]. lõplikult ELi õigusraamistikku. Seda otsust hakati rakendama 1999. aastal. Schengeni infosüsteemi uusim versioon, teise põlvkonna Schengeni infosüsteem, käivitati 9. aprillil 2013. Nüüd kasutavad seda kõik ELi liikmesriigid ning Island, Liechtenstein, Norra ja Šveits[276]. Teise põlvkonna Schengeni infosüsteemi saavad kasutada ka Europol ja Eurojust.

Teise põlvkonna Schengeni infosüsteem koosneb keskinfosüsteemist ja liikmesriikide süsteemidest ning keskinfosüsteemi ja liikmesriikide süsteemide vahelisest sideinfrastruktuurist. Keskinfosüsteem sisaldab teatavaid liikmesriikide sisestatud andmeid isikute ja esemete kohta. Seda kasutavad riikide piirivalve-, politsei-, tolli-, viisa- ja kohtuasutused kogu Schengeni alal. Igal liikmesriigil on oma versioon keskinfosüsteemist, st riiklik Schengeni infosüsteem; seda ajakohastatakse pidevalt ja selle kaudu ajakohastatakse seega ka keskinfosüsteemi. Liikmesriikide süsteeme kontrollitakse ja hoiatusteade esitatakse juhul, kui:

- isikul ei ole õigust Schengeni alale siseneda või seal viibida;
- kohtu- või õiguskaitseasutused on isiku või eseme kuulutanud tagaotsitavaks;
- isik on kuulutatud kadunuks;
- esemed, näiteks paberraha, autod, kaubikud, tulirelvad ja isikut tõendavad dokumendid, on registreeritud varastatud või kadunud varana.

274 Beneluxi Majandusliidu riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vaheline leping kontrolli järkjärgulise kaotamise kohta nende ühispiiridel, EÜT L 239, 2000.

275 Euroopa ühendused, 1997, Amsterdami leping, millega muudetakse Euroopa Liidu lepingut, Euroopa ühenduste aluslepinguid ja teatavaid nendega seotud akte, EÜT C 340, 1997.

276 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT L 381, 2006; Euroopa Liidu Nõukogu, 2007, nõukogu otsus 2007/533/JSK, 12. juuni 2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT L 205, 2007.

Hoiatusteate korral tuleb riiklike Schengeni infosüsteemide kaudu käivitada järelmeetmed.

Teise põlvkonna Schengeni infosüsteemil on teatavaid uusi funktsioone, näiteks võimaldab see sisestada järgmist: biomeetrilised andmed, näiteks sõrmejäljed ja fotod; uut tüüpi hoiatusteated, näiteks varastatud laevade, õhusõidukite, konteinerite või maksevahendite kohta; täiendatud hoiatusteated isikute ja esemete kohta; vahistamise, üleandmise või väljasaatmise eesmärgil tagaotsitavate isikutega seotud Euroopa vahistamismääruste koopiad.

Nõukogu otsuses 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist (teise põlvkonna Schengeni infosüsteemi otsus), osutatakse konventsioonile nr 108: „Käesoleva otsuse kohaldamisel töödeldud isikuandmeid kaitstakse Euroopa Nõukogu […] konventsiooni […] alusel"[277]. Kui politseiasutused kasutavad isikuandmeid teise põlvkonna Schengeni infosüsteemi otsuse kohaldamise raamistikus, tuleb riigi tasandi õiguses rakendada konventsioonis nr 108, samuti politseiandmeid käsitlevas soovituses esitatud sätteid.

Riikliku Schengeni infosüsteemi järelevalve eest vastutab iga liikmesriigi pädev järelevalveasutus. Eeskätt peab järelevalveasutus kontrollima riikliku süsteemi kaudu keskinfosüsteemi sisestatavate andmete kvaliteeti. Riigi järelevalveasutus peab tagama, et vähemalt kord iga nelja aasta tagant korraldataks riikliku Schengeni infosüsteemi andmetöötlustoimingute audit. Riikide järelevalveasutused teevad koostööd Euroopa andmekaitseinspektoriga ning tagavad keskinfosüsteemi koordineeritud järelevalve ning Euroopa andmekaitseinspektor vastutab keskinfosüsteemi järelevalve üle. Selguse ja arusaadavuse huvides saadetakse Euroopa Parlamendile, nõukogule ja eu-LISA-le iga kahe aasta tagant ühine tegevusaruanne.

Teise põlvkonna Schengeni infosüsteemi puhul üksikisikutele tagatud juurdepääsuõigusi saab kasutada ükskõik millises liikmesriigis, kuna iga riiklik Schengeni infosüsteem on keskinfosüsteemi täpne koopia.

Näide: kohtuasjas *Dalea vs. Prantsusmaa*[278] käsitleti juhtumit, kus kaebuse esitajale ei antud viisat Prantsusmaale reisimiseks, kuna Prantsusmaa ametiasutused

277 Euroopa Liidu Nõukogu (2007), nõukogu otsus 2007/533/JSK, 12. juuni 2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT L 205, 2007, artikkel 57.

278 EIK, *Dalea vs. Prantsusmaa,* nr 964/07, 2. veebruar 2010.

olid Schengeni infosüsteemi teatanud, et teda ei tohiks riiki lubada. Kaebuse esitaja püüdis Prantsusmaa andmekaitsekomisjoni ja lõpuks riiginõukogu kaudu taotleda andmetega tutvumist ja andmete parandamist või kustutamist, kuid tulutult. EIK leidis, et kaebuse esitajast Schengeni infosüsteemi teatamine oli kooskõlas õigusaktidega ning et sellel oli õiguspärane eesmärk kaitsta riigi julgeolekut. Kuna kaebuse esitaja ei tõendanud, et ta oli Schengeni alale pääsemisest keeldumise tõttu kannatanud reaalset kahju, ning kuna ametiasutused rakendasid piisavaid meetmeid, mille abil kaitsta asjaomast isikut meelevaldsete otsuste eest, oli sekkumine kaebuse esitaja õigusesse eraelu austamisele proportsionaalne. Kaebuse esitaja artikli 8 alusel esitatud kaebus tunnistati seega vastuvõetamatuks.

Viisainfosüsteem

Viisainfosüsteem (VIS), mida haldab samuti eu-LISA, loodi ELi ühise viisapoliitika rakendamise toetamiseks[279]. Viisainfosüsteem võimaldab Schengeni riikidel vahetada viisaandmeid süsteemi kaudu, mis ühendab Schengeni riikide ELi mittekuuluvates riikides asuvaid konsulaate kõikide liikmesriikide välispiiridel asuvate piiripunktidega. Süsteemis töödeldakse Schengeni riikide lühiajaliste viisade või transiitviisade taotlusi käsitlevaid andmeid. Tänu viisainfosüsteemile saavad piirikontrolliasutused biomeetriliste andmete abil välja selgitada, kas viisa esitanud isik on selle seaduslik kasutaja, ning kindlaks teha isikud, kelle dokumendid on võltsitud või kellel ei ole dokumente.

Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 767/2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), on sätestatud, et viisainfosüsteemi võib salvestada üksnes andmeid taotleja ja tema viisade kohta, fotosid, sõrmejälgede andmeid ning linke varasemate taotluste ja koos reisivate isikute taotlustoimikute juurde[280]. Juurdepääs viisainfosüsteemile andmete sisestamiseks, muutmiseks või kustutamiseks on üksnes

279 Euroopa Liidu Nõukogu (2004), nõukogu otsus, 8. juuni 2004, viisainfosüsteemi (VIS) kehtestamise kohta, ELT L 213, 2004; Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), ELT L 218, 2008; Euroopa Liidu Nõukogu, 2008, nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel, ELT L 218, 2008.

280 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), ELT L 218, 2008, artikkel 5.

liikmesriikides viisasid väljastavatel asutustel, samal ajal kui päringuid võivad viisasid väljastavate asutuste kõrval süsteemis teha ka välispiiridel asuvates piiripunktides kontrolle ja sisserändekontrolle tegevad asutused ning varjupaigataotlustega tegelevad asutused. Teatavatel tingimustel võivad riikide pädevad politseiasutused ja Europol taotleda viisainfosüsteemi sisestatud andmetega tutvumist terroriaktide ja kuritegude vältimise, avastamise ja uurimise eesmärgil[281].

Eurodac

Eurodaci nimi viitab terminile daktülogramm (ehk sõrmejälg). Tegemist on keskse süsteemiga, mis sisaldab sõrmejälgede andmeid kolmandate riikide kodanike kohta, kes taotlevad varjupaika mõnes ELi liikmesriigis[282]. Süsteem on kasutuses olnud alates 2003. aasta jaanuarist ning selle eesmärk on aidata kindlaks määrata, milline liikmesriik vastutab konkreetse varjupaigataotluse läbivaatamise eest kooskõlas nõukogu määrusega (EÜ) nr 343/2003, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku esitatud varjupaigataotluse läbivaatamise eest (Dublini II määrus)[283]. Eurodacis sisalduvaid isikuandmeid tohib kasutada ainult Dublini II määruse kohaldamise hõlbustamiseks, igasugune muu kasutus on karistatav.

Eurodac koosneb eu-LISA hallatavast keskküksusest sõrmejälgede säilitamiseks ja võrdlemiseks ning liikmesriikide ja keskandmebaasi vahelise elektroonilise andmeedastuse süsteemist. Liikmesriigid võtavad sõrmejäljed kõikidelt vähemalt 14aastastelt välismaalastelt või kodakondsuseta isikutelt, kes taotlevad nende territooriumil varjupaika või kes on kinni peetud välispiiride ebaseadusliku ületamise tõttu, ning edastavad need keskküksusele. Samuti võivad liikmesriigid võtta ja edastada nende välismaalaste või kodakondsuseta isikute sõrmejäljed, kelle puhul avastatakse, et nad viibivad riigi territooriumil ebaseaduslikult.

281 Euroopa Liidu Nõukogu (2008), nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel, ELT L 218, 2008.

282 Nõukogu määrus (EÜ) nr 2725/2000, 11. detsember 2000, mis käsitleb sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist Dublini konventsiooni tõhusa kohaldamise eesmärgil, EÜT L 316, 2000; nõukogu määrus (EÜ) nr 407/2002, 28. veebruar 2002, millega nähakse ette sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist Dublini konventsiooni tõhusa kohaldamise eesmärgil käsitleva määruse (EÜ) nr 2725/2000 teatavad rakenduseeskirjad, EÜT L 62, 2002, (Eurodaci käsitlevad määrused).

283 Nõukogu määrus (EÜ) nr 343/2003, 18. veebruar 2003, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku esitatud varjupaigataotluse läbivaatamise eest, ELT L 50, 2003, (Dublini II määrus).

Sõrmejälgede andmeid säilitatakse Eurodaci andmebaasis üksnes pseudonüümide all. Kokkulangevuse korral avaldatakse pseudonüüm koos sõrmejälgede andmed edastanud esimese liikmesriigi nimega teisele liikmesriigile. Kõnealune teine liikmesriik pöördub seejärel esimese liikmesriigi poole, kuna Dublini II määruse kohaselt vastutab varjupaigataotluse töötlemise eest esimene liikmesriik.

Eurodacis varjupaigataotlejatega seoses säilitatavaid isikuandmeid hoitakse kümne aasta jooksul pärast sõrmejälgede võtmist, välja arvatud juhul, kui andmesubjekt saab mõne ELi liikmesriigi kodakondsuse. Sellisel juhul tuleb andmed otsekohe kustutada. Välispiiri ebaseaduslikul ületamisel kinni peetud välismaalastega seotud andmeid säilitatakse kahe aasta jooksul. Kui andmesubjektile antakse välja elamisluba, ta lahkub ELi territooriumilt või on saanud mõne liikmesriigi kodakondsuse, tuleb need andmed kohe kustutada.

Kõikide ELi liikmesriikide kõrval rakendavad Eurodaci rahvusvaheliste lepingute alusel ka Island, Norra, Liechtenstein ja Šveits.

Eurosur

Euroopa piiride valvamise süsteem (Eurosur)[284] on välja töötatud eesmärgiga tugevdada Schengeni välispiiride kontrolli ebaseadusliku sisserände ja piiriülese kuritegevuse avastamise, tõkestamise ja nende vastu võitlemise kaudu. See on ette nähtud riiklike koordinatsioonikeskuste ja uue integreeritud piirihalduse kontseptsiooni väljatöötamise ja kohaldamise eest vastutava ELi asutuse, Frontexi teabevahetuse ja operatiivkoostöö edendamiseks[285]. Eurosuri üldeesmärgid on järgmised:

- vähendada ELi märkamatult sisenevate ebaseaduslike rändajate arvu;
- vähendada surmajuhtumite arvu ebaseaduslike rändajate seas, vältides inimeste hukkumist merel;

284 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1052/2013, 22. oktoober 2013, millega luuakse Euroopa piiride valvamise süsteemRohke (EUROSUR), ELT L 295, 2013.

285 Euroopa Parlamendi ja nõukogu määrus (EL) nr 1168/2011, 25. oktoober 2011, millega muudetakse määrust (EÜ) nr 2007/2004 Euroopa Liidu liikmesriikide välispiiril tehtava operatiivkoostöö juhtimise Euroopa agentuuri asutamise kohta (Frontexi määrus), ELT L 394, 2011.

- suurendada kogu ELi sisejulgeolekut, aidates kaasa piiriülese kuritegevuse tõkestamisele[286].

Eurosur alustas tööd 2. detsembril 2013 kõikides välispiiridega liikmesriikides ning teistes liikmesriikides hakatakse seda rakendama 1. detsembrist 2014. Määrust hakatakse kohaldama liikmesriikide väliste maa- ja merepiiride ning õhupiiride valvamise suhtes.

Tolliinfosüsteem

Veel üks oluline ELis loodud ühine infosüsteem on tolliinfosüsteem (TIS)[287]. Siseturu loomise käigus kaotati ELi territooriumil liikuvate kaupade puhul kõik kontrollid ja formaalsused, mis aga suurendas pettuste riski. Seda riski tasakaalustati liikmesriikide tolliametite koostöö tugevdamise kaudu. Tolliinfosüsteemi eesmärk on aidata liikmesriike ELi tolli- ja põllumajanduseeskirjade raskete rikkumiste tõkestamisel, uurimisel ja nende eest vastutusele võtmisel.

Tolliinfosüsteemis sisalduv teave koosneb isikuandmetest viidetega kaupadele, transpordivahenditele, äriühingutele, isikutele ning kinnipeetud, arestitud või konfiskeeritud esemetele ja sularahale. Seda teavet võib kasutada üksnes vaatluste, aruannete, erikontrolli ja strateegilise või tegevusanalüüsi jaoks tollieeskirjade rikkumises kahtlustatavate isikute puhul.

Tolliinfosüsteemile pääsevad ligi riikide tolli-, maksu-, põllumajandus-, rahvatervise- ja politseiasutused, samuti Europol ja Eurojust.

286 Vt ka: Euroopa Komisjon (2008), komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele – Euroopa piiride valvamise süsteemi (EUROSUR) loomise analüüs, KOM(2008) 68 (lõplik), Brüssel, 13. veebruar 2008; Euroopa Komisjon (2011), mõjuhinnang, mis on lisatud ettepanekule võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega luuakse Euroopa piiride valvamise süsteem (EUROSUR), komisjoni talituste töödokument, SEK(2011) 1536 (lõplik), Brüssel, 12. detsember 2011, lk 18.

287 Euroopa Liidu Nõukogu (1995), nõukogu akt, 26. juuli 1995, millega koostatakse infotehnoloogia tolliotstarbelise kasutamise konventsioon, EÜT C 316, 1995, mida on muudetud järgmise otsusega: Euroopa Liidu Nõukogu, 2009, Regulatsioon nr 515/97, 13dal märtsil 1997 ühise abistamise regulatsioon liikmesriikide haldusasutuste vahel ja koostöö eelmainitud organisatsioonide ja Komisjoni vahel, et tagada tolli ja põllumajanduse valdkonna seaduste õige kohaldamine. Nõukogu otsus 2009/917/JSK, 30. november 2009, infotehnoloogia tollialase kasutamise kohta (tolliinfosüsteemi käsitlev otsus), ELT L 323, 2009.

Isikuandmete töötlemine peab toimuma kooskõlas regulatsiooniga nr 515/97 ja TIS-konventsiooniga,[288] samuti andmekaitsedirektiivis, ELi institutsioonide andmekaitse määruses, konventsioonis nr 108 ja politseiandmeid käsitlevas soovituses esitatud sätetega. Euroopa andmekaitseinspektor vastutab tolliinfosüsteemi järelevalve üle regulatsiooniga nr 45/2001 ning kutsub kokku vähemalt ühe korra aastas kõikide andmekaitseasutuste pädevad isikud seoses tolliinfosüsteemi järelevalvega.

288 *Ibid.*

8

Muud konkreetsed Euroopa andmekaitsealased õigusaktid

EL	Käsitletavad teemad	Euroopa Nõukogu
Andmekaitsedirektiiv Eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv	Elektrooniline side	Konventsioon nr 108 Telekommunikatsioonitee-nuseid käsitlev soovitus
Andmekaitsedirektiivi artikli 8 lõike 2 punkt b	Töösuhted	Konventsioon nr 108 Tööhõivet käsitlev soovitus
		EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 3. aprill 2007
Andmekaitsedirektiivi artikli 8 lõige 3	Meditsiinilised andmed	Konventsioon nr 108 Meditsiinilisi andmeid käsitlev soovitus
		EIK, *Z. vs. Soome*, nr 22009/93, 25. veebruar 1997
Kliinilisi uuringuid käsitlev direktiiv	Kliinilised uuringud	
Andmekaitsedirektiivi artikli 6 lõike 1 punktid b ja e ning artikli 13 lõige 2	Statistika	Konventsioon nr 108 Statistilisi andmeid käsitlev soovitus
Määrus (EÜ) nr 223/2009 Euroopa statistika kohta ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008	Ametlik statistika	Konventsioon nr 108 Statistilisi andmeid käsitlev soovitus

Direktiiv 2004/39/EÜ finantsinstrumentide turgude kohta Määrus (EÜ) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta Määrus (EÜ) nr 1060/2009 reitinguagentuuride kohta Direktiiv 2007/64/EÜ makseteenuste kohta siseturul	**Finantsandmed**	Konventsioon nr 108 Soovitus 90(19) maksete ja muude seonduvate tehingute eesmärgil kasutatavate isikuandmete kaitse kohta EIK, *Michaud vs. Prantsusmaa*, nr 12323/11, 6. detsember 2012

Paljudel juhtudel on Euroopa tasandil vastu võetud eriotstarbelised õigusaktid, mille alusel kohaldatakse konventsiooni nr 108 või andmekaitsedirektiivi üldpõhimõtteid teatavate olukordade suhtes suurema üksikasjalikkusega.

8.1. Elektrooniline side

Põhipunktid

- Erieeskirjad andmekaitse kohta telekommunikatsioonisektoris, eeskätt telefoniteenuste puhul, on esitatud Euroopa Nõukogu 1995. aasta soovituses.
- Isikuandmete töötlemist elektroonilise side teenuste osutamise puhul ELi tasandil reguleeritakse eraelu puutumatust ja elektroonilist sidet käsitleva direktiiviga.
- Elektroonilise side konfidentsiaalsus ei ole seotud mitte üksnes side sisuga, vaid ka andmeliiklusandmetega, näiteks teave selle kohta, kelle vahel side toimus, millal ja kui pikalt, ning asukohaandmetega, näiteks teave selle kohta, kust andmed edastati.

Sidevõrkude puhul valitseb suurem risk põhjendamatuks sekkumiseks kasutajate eraelu sfääri, kuna nendesse on sisse ehitatud tehnilised võimalused võrkudes toimuva side pealtkuulamiseks ja jälgimiseks. Sellest tulenevalt peeti sideteenuste kasutajaid ähvardavate riskide käsitlemise eesmärgil vajalikuks kehtestada konkreetsed andmekaitse-eeskirjad.

1995. aastal andis Euroopa Nõukogu välja soovituse andmekaitse kohta telekommunikatsioonisektoris, eeskätt telefoniteenuste puhul[289]. Selle soovituse kohaselt peaks isikuandmete kogumine ja töötlemine telekommunikatsioonisektoris piirduma järgmiste eesmärkidega: kasutaja ühendamine võrguga, konkreetse telekom-

289 Euroopa Nõukogu ministrite komitee (1995), soovitus R(95) 4 liikmesriikidele isikuandmete kaitse kohta telekommunikatsiooniteenuste, eeskätt telefoniteenuste valdkonnas, 7. veebruar 1995.

munikatsiooniteenuse kasutamise võimaldamine, arvete koostamine, kontrollimine, optimaalse tehnilise toimimise tagamine ning võrgu- ja teenusearendus.

Eritähelepanu pöörati ka sidevõrkude kasutamisele otseturundusteadete saatmise eesmärgil. Üldiselt ei tohi otseturundusteateid saata ühelegi abonendile, kes on reklaamiteadete saamisest sõnaselgelt loobunud. Automaatkõneseadmeid võib eelsalvestatud reklaamiteadete saatmiseks kasutada üksnes juhul, kui abonent on selleks andnud sõnaselge nõusoleku. Kõnealuse valdkonnaga seotud üksikasjalikumad eeskirjad määratakse kindlaks riigi õigusaktides.

ELi õigusraamistikus võeti pärast 1997. aastal tehtud esmakordset katset 2002. aastal vastu eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv (muudetud 2009. aastal), mille eesmärk on täiendada ja täpsustada andmekaitsedirektiivi sätteid telekommunikatsioonisektori puhul[290]. Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi kohaldamisala hõlmab üldkasutatavate elektrooniliste võrkude sideteenuseid.

Direktiivis eristatakse peamiselt kolme liiki andmeid, mis side käigus luuakse:

- side käigus saadetavate teadete sisu moodustavad andmed; need andmed on rangelt konfidentsiaalsed;

- side alustamiseks ja hoidmiseks vajalik teave, st andmeliiklusandmed, näiteks sidepartnerite ning side toimumise aja ja kestuse kohta;

- andmeliiklusandmed hõlmavad andmeid, mis on täpsemalt seotud sidevahendi asukohaga, st asukohaandmeid; need andmed käsitlevad samal ajal sidevahendi *kasutaja* asukohta ning on eriti asjakohased mobiilsidevahendite kasutajate puhul.

Teenuseosutaja võib andmeliiklusandmeid kasutada üksnes arvete koostamise ja teenuse tehnilise poole toimimise eesmärgil. Andmesubjekti nõusolekul võib neid

290 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 2001, mida on muudetud Euroopa Parlamendi ja nõukogu direktiiviga 2009/136/EÜ, 25. november 2009, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta, ELT L 337, 2009.

andmeid aga avaldada teistele vastutavatele töötlejatele, kes osutavad lisaväärtusteenuseid, näiteks kasutaja asukohaga seotud teabe andmine lähima metroojaama või apteegi kohta või ilmaolude kohta selles asupaigas.

Muu juurdepääs elektroonilistes võrkudes toimuva side andmetele, näiteks kuritegude uurimise eesmärgil, peab eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 15 kohaselt olema kooskõlas nõuetega põhjendatud sekkumise kohta õigusesse isikuandmete kaitsele, mis on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 ning kinnitatud põhiõiguste harta artiklitega 8 ja 52.

Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi 2009. aasta muudatused[291] hõlmavad järgmist.

- Otseturundusotstarbelise elektronposti saatmise suhtes kehtivaid piiranguid laiendati lühisõnumiteenustele, multimeediateenustele ja muudele sellistele rakendustele; turunduse eesmärkidel ei tohi elektronposti saata, kui selleks ei ole saadud eelnevat nõusolekut. Ilma sellise nõusolekuta võib turunduse eesmärgil elektronposti saata vaid varasematele klientidele, kui nad on oma e-posti aadressi avaldanud ning kui neil ei ole selle saamise kohta vastuväiteid.

- Liikmesriikidele määrati kohustus tagada õiguskaitsevahendid kaitseks pealesunnitud teabe saatmise keelu rikkumiste eest[292].

- Arvuti kasutaja toiminguid jälgivate küpsiste ja tarkvara rakendamine ei ole ilma arvuti kasutaja nõusolekuta enam lubatud. Nõusoleku esitamise ja saamise viisi tuleks piisava kaitse tagamiseks reguleerida riigi õigusaktidega[293].

Andmetega seotud rikkumiste puhul ebaseadusliku juurdepääsu või andmete kaotsimineku või hävimise tõttu tuleb viivitamata teavitada pädevat järelevalveasutust.

291 Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, 25. november 2009, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta, ELT L 337, 2009.

292 Vt muudetud direktiivi artikkel 13.

293 *Ibid.*, artikkel 5; vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 04/2012, mis käsitleb vabastust küpsiste kasutamiseks nõusoleku saamise kohustusest, WP 194, Brüssel, 7. juuni 2012.

Abonente tuleb teavitada, kui andmetega seotud rikkumise tagajärjel on võimalik, et nad kannavad selle tõttu kahju[294].

Andmete säilitamise direktiivi[295], mis tunnistati kehtetuks 8dal aprillil 2014, kohaselt pidid sideteenuste osutajad säilitama andmeliiklusandmeid, eeskätt raskete kuritegude vastu võitlemise eesmärgil, mitte vähem kui kuue kuu ja kõige rohkem kahe aasta jooksul, sõltumata sellest, kas teenuseosutajal oli neid andmeid enam vaja arvete koostamiseks või teenuse osutamise tehnilise poole toimimise tagamiseks.

ELi liikmesriigid määravad sõltumatud ametiasutused, kes vastutavad säilitatavate andmete turvalisuse järelevalve eest.

Telekommunikatsiooniliikluse andmete säilitamine on ilmselgelt vastuolus inimeste õigusega isikuandmete kaitsele[296]. Sellise sekkumise põhjendatus on küsimuse alla seatud nii mõneski ELi liikmesriikide[297] tasandi kohtumenetluses.

Asjas *Digital Rights Ireland ja Seitlinger ning teised,*[298] Euroopa Liidu kohus tunnistas andmete säilitamise direktiivi kehtetuks. Kohtu hinnangul, "laiaulatuslik ja tõsine sekkumine direktiivi poolt, kui teemaks on fundamentaalsed õigused, ei ole piisavalt piiritletud, et oleks tagatud vajaduse korral piisav sekkumine.

Oluline küsimus elektroonilise side puhul on ametiasutuste sekkumine. Side jälgimine või pealtkuulamine, näiteks pealtkuulamisseadmete kasutamine, on lubatud üksnes juhul, kui see on õigusaktidega ette nähtud ning osutub demokraatlikus ühiskonnas vajalikuks, et kaitsta riigi julgeolekut, avalikku korda, riigi rahalisi

294 Vt ka andmekaitsedirektiivi artikli 29 alusel loodud töörühma töödokument 01/2011 ELi kehtiva isikuandmetega seotud rikkumisi käsitleva raamistiku kohta ning soovituste kohta tulevasteks poliitikasuundumusteks, WP 184, Brüssel, 5. aprill 2011.

295 Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, ELT L 105, 2006.

296 Euroopa andmekaitseinspektor, 2011, Euroopa andmekaitseinspektori arvamus komisjoni hindamisaruande kohta nõukogule ja Euroopa Parlamendile seoses andmete säilitamise direktiiviga (direktiiv 2006/24/EÜ), 31. mai 2011.

297 Saksamaa föderaalne konstitutsioonikohus (Bundesverfassungsgericht), 1 BvR 256/08, 2. märts 2010; Rumeenia konstitutsioonikohus (Curtea Constituțională a României), nr 1258, 8. oktoober 2009; Tšehhi Vabariigi konstitutsioonikohus (Ústavní soud České republiky), 94/2011 Coll., 22. märts 2011.

298 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland ja Seitlinger ning teised,* 8 aprill 2014, par 65.

huve, võidelda kuritegevuse vastu või kaitsta andmesubjekti või muu isiku õigusi ja vabadusi.

Näide: kohtuasjas *Malone vs. Ühendkuningriik*[299] käsitleti juhtumit, kus kaebuse esitajat oli süüdistatud mitmes kuriteos, mis olid seotud ebaausa kauplemisega varastatud esemetega. Kohtuprotsessi käigus ilmnes, et ühte kaebuse esitaja telefonivestlust kuulati siseministri (Secretary of State for the Home Department) väljastatud määruse alusel pealt. Ehkki kaebuse esitaja suhtluse pealtkuulamine oli oma meetodi poolest riigi õigusaktidest lähtudes seaduslik, leidis EIK, et Ühendkuningriigi õigusaktides puudusid õigusnormid, mis oleksid reguleerinud ametiasutustele selles valdkonnas võimaldatud kaalutlusõiguse kasutamise ulatust ja meetodit, ning et seepärast ei olnud kõnealusest toimingust põhjustatud sekkumine „õigusaktidega kooskõlas". Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

8.2. Tööhõiveandmed

Põhipunktid

- Erieeskirjad andmekaitse kohta töösuhetes on esitatud tööhõiveandmeid käsitlevas Euroopa Nõukogu soovituses.
- Andmekaitsedirektiivis viidatakse konkreetselt töösuhetele vaid tundlike andmete töötlemist käsitlevates sätetes.
- Arvestades, et nõusoleku andmine peab olema vabatahtlik, on selle kehtivus õigusliku alusena töötajate isikuandmete töötlemiseks kaheldav, pidades silmas tööandja ja töötajate majanduslikku ebavõrdsust. Nõusoleku andmise tingimusi tuleb hoolikalt kaaluda.

ELis ei ole isikuandmete töötlemise puhul tööhõive valdkonnas kehtestatud konkreetset õigusraamistikku. Andmekaitsedirektiivis viidatakse töösuhetele sõnaselgelt vaid artikli 8 lõikes 2, milles käsitletakse tundlike andmete töötlemist. Euroopa

299 EIK, *Malone vs. Ühendkuningriik*, nr 8691/79, 2. august 1984.

Nõukogu tasandil võeti 1989. aastal vastu tööhõiveandmeid käsitlev soovitus, mida praegu ajakohastatakse[300].

Ülevaade tööhõive valdkonnaga seotud peamistest andmekaitseprobleemidest on esitatud andmekaitsedirektiivi artikli 29 alusel loodud töörühma töödokumendis[301]. Töörühm analüüsis nõusoleku rolli tööhõiveandmete töötlemise õigusliku alusena[302]. Selle töö käigus jõuti järeldusele, et nõusolekut taotleva tööandja ja nõusolekut andva töötaja vaheline majanduslik ebavõrdsus tõstatab sageli kahtlusi selle suhtes, kas nõusolek antakse ikka vabatahtlikult. Seepärast tuleb tööhõivetingimustes antud nõusoleku kehtivuse hindamisel hoolikalt kaaluda nõusoleku taotlemise tingimusi.

Üks levinud andmekaitseprobleem tänapäeva töökeskkonnas on seotud sellega, millises ulatuses on töötajate elektroonilise side jälgimine töökohas seaduslik. Tihtipeale väidetakse, et lihtne lahendus sellele probleemile oleks keelata töökohal sidevahendite kasutamine isiklikel eesmärkidel. Selline üldine keeld võib aga osutuda ebaproportsionaalseks ja raskesti teostatavaks. Selles küsimuses on iseäranis asjakohane järgmine EIK otsus.

Näide: kohtuasjas *Copland vs. Ühendkuningriik*[303] käsitleti juhtumit, kus ühe kolledžitöötaja telefoni-, e-posti ja internetikasutust jälgiti salaja, et välja selgitada, kas ta kasutab kolledži ressursse liiga palju isiklikel eesmärkidel. EIK leidis, et töökohalt tehtud telefonikõned kuuluvad eraelu ja korrespondentsi mõiste alla. Seepärast kaitstakse selliseid töökohal tehtavaid kõnesid ja töökohalt saadetavaid e-kirju, samuti isiklikel eesmärkidel interneti kasutamise jälgimisest saadavat teavet Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8. Kaebuse esitaja juhtumi puhul leiti, et riigi õigusaktides ei olnud kehtestatud sätteid, millega oleks reguleeritud seda, millistel tingimustel võib tööandja jälgida töötajate telefoni-, e-posti ja internetikasutust. Seega ei olnud

300 Euroopa Nõukogu ministrite komitee (1989), soovitus R(89) 2 liikmesriikidele tööhõive eesmärkidel kasutatavate isikuandmete kaitse kohta, 18. jaanuar 1989. Vt ka: konventsiooni nr 108 nõuandekomitee, uuring tööhõive eesmärkidel kasutatavate isikuandmete kaitset käsitleva soovituse R(89) 2 kohta ja ettepanekud kõnealuse soovituse läbivaatamise kohta, 9. september 2011.

301 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma arvamus 8/2001 isikuandmete töötlemise kohta tööhõive valdkonnas, WP 48, Brüssel, 13. september 2001.

302 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma 24. oktoobri 1995. aasta direktiivi 95/46/EÜ artikli 26 lõike 1 ühist tõlgendamist käsitlev töödokument, WP 114, Brüssel, 25. november 2005.

303 EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 3. aprill 2007.

sekkumine kooskõlas õigusaktidega. Kohus järeldas, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

Tööhõivet käsitleva Euroopa Nõukogu soovituse kohaselt peavad tööhõive eesmärkidel kogutud isikuandmed olema saadud otse asjaomaselt töötajalt.

Töölevõtmise otstarbel võib isikuandmeid koguda üksnes kandidaatide sobivuse ja karjääripotentsiaali hindamiseks vajalikus ulatuses.

Soovituses käsitletakse konkreetselt ka selliseid andmeid, mis sisaldavad hinnanguid töötaja töötulemuste või potentsiaali kohta. Sedalaadi andmed peavad põhinema õiglastel ja ausatel hinnangutel ning need ei tohi olla solvavad. See tuleb tagada ka andmete õiglase töötlemise ja andmete täpsuse põhimõtetest lähtudes.

Üks andmekaitseõigusega seotud eriküsimus tööandja ja töötaja suhte puhul on töötajate esindajate roll. Töötajate esindajad võivad töötajate isikuandmeid vastu võtta üksnes nende esindamiseks vajalikus ulatuses.

Tööhõivega seotud eesmärkidel kogutud tundlikke andmeid võib töödelda ainult erijuhtudel ning riigi õigusaktides sätestatud tagatiste alusel. Tööandjad võivad töötajatelt või töölesoovijatelt küsida nende tervisliku seisundi kohta või paluda neid meditsiinilisele läbivaatusele üksnes selleks, et selgitada välja, kas nad sobivad töökohale, et täita haiguste ennetamisega seotud nõudeid või tagada isikule sotsiaaltoetuste määramine. Terviseandmeid ei tohi koguda muudest allikatest, vaid ainult asjaomaselt töötajalt endalt, välja arvatud juhul, kui töötaja on andnud selleks sõnaselge ja teadliku nõusoleku, või kui see on ette nähtud riigi õigusaktidega.

Tööhõivet käsitleva soovituse kohaselt tuleb töötajaid teavitada sellest, millisel eesmärgil nende isikuandmeid töödeldakse, mis liiki isikuandmeid säilitatakse, millistele üksustele neid andmeid regulaarselt edastatakse ning mis eesmärgil ja õiguslikul alusel selline andmete edastamine toimub. Tööandjad peaksid töötajaid ette teavitama ka töötajate isikuandmete töötlemiseks või nende tegevuse või töötulemuste jälgimiseks automatiseeritud süsteemide loomisest või sellistes süsteemides tehtavatest muudatustest.

Töötajatel peab olema õigus tutvuda nendega seotud tööhõiveandmetega ning lasta need vajaduse korral parandada või kustutada. Hinnanguid sisaldavate andmete töötlemise puhul peab töötajatel olema ka õigus esitada asjaomaste hinnangute kohta vastuväiteid. Neid õigusi võib aga ajutiselt piirata sisejuurdluste eesmärgil.

Kui töötajale ei võimaldata tööhõivega seotud isikuandmetega tutvumist või nende parandamist või kustutamist, peab tal riigi õigusaktides sätestatud asjakohaste menetluste abil olema võimalik esitada keeldumise kohta vastuväide.

8.3. Meditsiinilised andmed

Põhipunkt

- Meditsiinilised andmed kuuluvad tundlike andmete alla ning seega kohaldatakse nende suhtes erikaitset.

Andmesubjekti tervislikku seisundit käsitlevad isikuandmed kuuluvad andmekaitsedirektiivi artikli 8 lõike 1 ja konventsiooni nr 108 artikli 6 alusel tundlike andmete hulka. See tähendab, et meditsiiniliste andmete suhtes kohaldatakse rangemaid andmetöötlusnõudeid kui mittetundlike andmete puhul.

Näide: kohtuasjas *Z. vs. Soome*[304] käsitleti juhtumit, kus kaebuse esitaja endine abikaasa, kes oli HI-viiruse kandja, oli toime pannud mitu seksuaalkuritegu. Hiljem mõisteti ta süüdi tapmises, kuna ta ei olnud oma ohvreid hoiatanud HI-viirusesse nakatumise riskist. Soome kohus otsustas, et kohtuotsust ja kohtutoimikuid tuleb hoida konfidentsiaalsena kümme aastat, hoolimata sellest, et kaebuse esitaja taotles pikemat tähtaega. Apellatsioonikohus ei rahuldanud neid taotlusi ning selle otsus sisaldas nii kaebuse esitaja kui ka tema endise abikaasa täisnime. EIK leidis, et kõnealust sekkumist ei saa pidada demokraatlikus ühiskonnas vajalikuks, sest era- ja perekonnaelu austamisega seotud õiguse kasutamise puhul on meditsiiniliste andmete kaitse väga oluline, eeskätt juhul, kui tegu on HIV-nakkust käsitleva teabega, pidades silmas, et paljudes ühiskondades peetakse seda diagnoosi häbimärgiks. Seepärast järeldas kohus, et kui apellatsioonikohtu otsust hoitakse konfidentsiaalsena ainult kümme aastat pärast otsuse tegemist ning seega võimaldatakse selle tähtaja möödumisel juurdepääsu otsuses sisalduvale teabele, milles viidatakse kaebuse esitaja isikule ning tervislikule seisundile, on tegu Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

304 EIK, *Z. vs. Soome*, nr 22009/93, 25. veebruar 1997, punktid 94 ja 112; vt ka EIK, *M.S. vs. Rootsi*, nr 20837/92, 27. august 1997; EIK, *L.L. vs. Prantsusmaa*, nr 7508/02, 10. oktoober 2006; EIK, *I. vs. Soome*, nr 20511/03, 17. juuli 2008; EIK, *K.H. jt vs. Slovakkia*, nr 32881/04, 28. aprill 2009; EIK, *Szuluk vs. Ühendkuningriik*, nr 36936/05, 2. juuni 2009.

Andmekaitsedirektiivi artikli 8 lõike 3 kohaselt võib meditsiinilisi andmeid töödelda juhul, kui see on vajalik ennetava meditsiini, meditsiinilise diagnoosi, meditsiinilise abi või ravi võimaldamise või tervishoiuteenuste juhtimise jaoks. Neid andmeid võib aga töödelda üksnes ametisaladuse hoidmise kohustusega tervishoiutöötaja või mõni teine isik, kelle suhtes kehtib samaväärne saladuse hoidmise kohustus[305].

Konventsiooni nr 108 põhimõtete rakendamist meditsiinivaldkonnas toimuva andmetöötluse suhtes käsitletakse üksikasjalikumalt Euroopa Nõukogu 1997. aasta soovituses meditsiiniliste andmete kohta[306]. Selles soovitatud eeskirjad on kooskõlas andmekaitsedirektiivis esitatud sätetega, mis käsitlevad meditsiiniliste andmete töötlemise õiguspäraseid eesmärke, terviseandmeid kasutavate isikute ametisaladuse hoidmise kohustust ning andmesubjektide õigusi selguse ja arusaadavuse, andmetega tutvumise ning andmete parandamise ja kustutamise puhul. Lisaks sellele ei tohi meditsiinilisi andmeid, mida tervishoiutöötajad seaduslikult töötlevad, edastada õiguskaitseasutustele, välja arvatud juhul, kui kehtestatud on piisavad tagatised, et vältida andmete sellist avaldamist, millega rikutakse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 tagatud õigust eraelu austamisele[307].

Meditsiinilisi andmeid käsitlevas soovituses on esitatud ka erisätted sündimata laste ja piiratud teovõimega isikute meditsiiniliste andmete kohta ning geeniandmete töötlemise kohta. Soovituses on sõnaselgelt viidatud sellele, et andmeid võib vajadusest pikema aja jooksul säilitada teadusuuringute eesmärkidel, kuigi tavaliselt tuleb andmed selleks anonüümseks muuta. Meditsiinilisi andmeid käsitleva soovituse artiklis 12 soovitatakse üksikasjalikke eeskirju juhtudeks, kus uurijatel on vaja kasutada isikuandmeid ning anonüümsetest andmetest ei piisa.

Selleks et täita teadustööga seotud vajadusi ja samal ajal kaitsta asjaomaste patsientide huve, võib kasu olla andmete pseudonüümi all esitamisest. Pseudonüümide kasutamist andmekaitsevaldkonnas käsitletakse üksikasjalikumalt jaotises 2.1.3.

Riikide ja Euroopa tasanditel on tuliselt arutletud algatuste üle, mille eesmärk on hakata säilitama patsientide raviandmeid elektroonilistel tervisekaartidel[308].

305 Vt ka EIK, *Biriuk vs. Leedu*, nr 23373/03, 25. november 2008.

306 Euroopa Nõukogu ministrite komitee (1997), soovitus R(97) 5 liikmesriikidele meditsiiniliste andmete kaitse kohta, 13. veebruar 1997.

307 EIK, nr 1585/09, *Avilkina jt vs. Venemaa*, 6. juuni 2013, punkt 53 (pooleliolev).

308 Andmekaitsedirektiivi artikli 29 alusel loodud töörühma töödokument, milles käsitletakse elektroonilisele tervisekaardile kantavate tervisealaste isikuandmete töötlemist, WP 131, Brüssel, 15. veebruar 2007.

Üleriigiliste elektrooniliste tervisekaardisüsteemide puhul mängib erilist rolli nende piiriülene kättesaadavus, mis on ELis oluline küsimus piiriülese tervishoiu kontseptsioonis[309].

Veel üks valdkond, mida uute õigusnormide käsitlemisel arutatakse, on kliinilised uuringud, st ravimite katsetamine patsientidel dokumenteeritud uurimiskeskkonnas; ka see küsimus on andmekaitse seisukohalt väga oluline. Inimravimite kliinilisi uuringuid reguleeritakse Euroopa Parlamendi ja nõukogu 4. aprilli 2001. aasta direktiiviga 2001/20/EÜ liikmesriikide õigus- ja haldusnormide ühtlustamise kohta, mis käsitlevad hea kliinilise tava rakendamist inimtervishoius kasutatavate ravimite kliinilistes uuringutes (kliiniliste uuringute direktiiv)[310]. 2012. aasta detsembris tegi Euroopa Komisjon ettepaneku kliiniliste uuringute direktiiv asendada, et kliiniliste uuringutega seotud menetlusi ühtlustada ja tõhustada[311].

ELi tasandil on isikuandmete ja tervishoiusektori seoste küsimuses pooleli ka palju teisi seadusandlikke ja muid algatusi[312].

8.4. Andmete töötlemine statistilistel eesmärkidel

Põhipunktid

- Statistika eesmärkidel kogutud andmeid ei tohi kasutada muudel eesmärkidel.
- Teataval eesmärgil seaduslikult kogutud andmeid võib täiendavalt kasutada statistika eesmärkidel tingimusel, et andmete kasutajad esitavad riigi õigusaktides sätestatud piisavad tagatised. Sel otstarbel tuleks ette näha, et enne andmete kolmandatele isikutele edastamist tuleb need muuta anonüümseks või kasutada pseudonüüme.

309 Euroopa Parlamendi ja nõukogu direktiiv 2011/24/EL, 9. märts 2011, patsiendiõiguste kohaldamise kohta piiriüleses tervishoius, ELT L 88, 2011.

310 Euroopa Parlamendi ja nõukogu direktiiv 2001/20/EÜ, 4. aprill 2001, liikmesriikide õigus- ja haldusnormide ühtlustamise kohta, mis käsitlevad hea kliinilise tava rakendamist inimtervishoius kasutatavate ravimite kliinilistes uuringutes, EÜT L 121, 2001.

311 Euroopa Komisjon (2012), Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse inimtervishoius kasutatavate ravimite kliinilisi katseid ja millega tunnistatakse kehtetuks direktiiv 2001/20/EÜ, COM(2012) 369 (final), Brüssel, 17. juuli 2012.

312 Euroopa andmekaitseinspektor (2013), Euroopa andmekaitseinspektori arvamus komisjoni teatise „E-tervise 2012.–2020. aasta tegevuskava: innovatiivne tervishoid 21. sajandil" kohta, Brüssel, 27. märts 2013.

Andmekaitsedirektiivis viidatakse andmete töötlemisele statistikaga seotud eesmärkidel andmekaitsepõhimõtete võimalike erandite kontekstis. Direktiivi artikli 6 lõike 1 punkti b kohaselt ei pea eesmärgi piiramise põhimõtet riigi õigusaktide alusel järgima, kui andmeid on vaja täiendavalt kasutada statistilistel eesmärkidel, kuigi riigi õigusaktidega tuleb ette näha kõik vajalikud tagatised. Artikli 13 lõike 2 kohaselt võib andmetega tutvumise õigust riigi õigusaktide alusel piirata, kui andmeid töödeldakse ainult statistika tegemiseks; ka sel juhul peavad riigi õigusaktides olema kehtestatud piisavad tagatised. Selles küsimuses on andmekaitsedirektiivis sätestatud erinõue, et statistilise uurimistöö käigus saadud või loodud andmeid ei tohi mingil juhul kasutada andmesubjekti kohta konkreetsete otsuste tegemiseks.

Kuigi vastutav töötleja võib andmeid, mille ta seaduslikul alusel teataval eesmärgil kogus, uuesti kasutada omaenda statistilistel eesmärkidel (nn sekundaarne statistika), tuleb andmed enne kolmandale isikule statistika eesmärgil edastamist, olenevalt kontekstist, muuta anonüümseks või esitada need pseudonüümi all, välja arvatud juhul, kui andmesubjekt on andnud vastava nõusoleku või see on sätestatud riigi õigusaktides. See nõue põhineb andmekaitsedirektiivi artikli 6 lõike 1 punktis b sätestatud vajalike tagatiste nõudel.

Peamine valdkond, kus andmeid kasutatakse statistilistel eesmärkidel, on riikide ja ELi statistikaasutuste tehtav ametlik statistika asjaomaste ametlikku statistikat käsitlevate riigi tasandi ja ELi õigusaktide alusel. Nende õigusaktide kohaselt on kodanikud ja ettevõtjad üldiselt kohustatud statistikaasutustele andmeid avaldama. Statistikaasutuste töötajatel on konkreetsed ametisaladuse hoidmise kohustused, mille täitmist põhjalikult kontrollitakse, arvestades, et see on väga oluline statistikaasutustele andmeid avaldavate kodanike usalduse seisukohalt.

Määrus (EÜ) nr 223/2009 Euroopa statistika kohta (Euroopa statistika määrus) hõlmab olulisi eeskirju andmekaitse kohta ametliku statistika valdkonnas ning seepärast võib see asjakohane olla ka riikide tasandil ametliku statistika puhul kehtestatud õigusnormide küsimuses[313]. Määruses tuginetakse põhimõttele, et ametliku statistika toiminguteks on vaja piisavalt täpset õiguslikku alust[314].

313 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 223/2009, 11. märts 2009, Euroopa statistika kohta ning Euroopa Parlamendi ja nõukogu määruse (EÜ, Euratom) nr 1101/2008 (konfidentsiaalsete statistiliste andmete Euroopa Ühenduste Statistikaametile edastamise kohta), nõukogu määruse (EÜ) nr 322/97 (ühenduse statistika kohta) ja nõukogu otsuse 89/382/EMÜ, Euratom (millega luuakse Euroopa ühenduste statistikaprogrammi komitee) kehtetuks tunnistamise kohta, ELT L 87, 2009.

314 Seda põhimõtet on plaanis täpsemalt käsitleda Eurostati Euroopa statistika tegevusjuhises, milles antakse Euroopa statistika määruse artikli 11 alusel eetilisi suuniseid ametliku statistika tegemise kohta, sealhulgas isikuandmete vastutustundliku kasutamise kohta; kättesaadav: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

Näide: kohtuasjas *Huber vs. Saksamaa*[315] leidis ELK, et kui ametiasutus kogub ja säilitab isikuandmeid statistika eesmärkidel, ei tähenda see iseenesest, et andmete töötlemine on seaduslik. Õigusakt, millega nähakse ette isikuandmete töötlemine, peab vastama ka vajalikkuse nõudele – kõnealuses kohtuasjas see nii ei olnud.

Euroopa Nõukogu õigusraamistikus käsitletakse avalikus ja erasektoris tehtavat statistikat 1997. aastal avaldatud soovituses statistiliste andmete kohta[316]. Selles soovituses on kirjeldatud põhimõtteid, mis vastavad andmekaitsedirektiivi eespool osutatud peamistele eeskirjadele. Soovituses esitatakse üksikasjalikumad eeskirjad alljärgnevalt osutatud küsimuste kohta.

Samal ajal kui andmeid, mille vastutav töötleja on kogunud statistikaga seotud eesmärkidel, ei tohi kasutada muudel eesmärkidel, tuleb statistikavälistel eesmärkidel kogutud andmed teha kättesaadavaks juhul, kui neid on vaja täiendavalt kasutada statistika jaoks. Statistilisi andmeid käsitleva soovitusega on isegi ette nähtud, et andmeid võib edastada kolmandatele isikutele, kui seda tehakse üksnes statistikaga seotud eesmärkidel. Sellistel juhtudel peaksid pooled kokku leppima ja kirjalikult vormistama, millises ulatuses on andmete kasutamine statistilistel eesmärkidel seaduslik. Kuna see ei asenda andmesubjekti nõusolekut, eeldatakse, et riigi õigusaktides on sätestatud vajalikud tagatised, et isikuandmete väärkasutamise risk oleks võimalikult väike; selline tagatis võiks näiteks olla kohustus muuta andmed enne edastamist anonüümseks või esitada need pseudonüümide all.

Ametialaselt statistiliste uuringutega tegelevate isikute suhtes tuleks riigi õigusaktide alusel kohaldada ametisaladuse hoidmise erikohustusi, nagu on tavaks ametliku statistika puhul. Need kohustused peaksid kehtima ka küsitlejate suhtes, kelle tööülesanne on koguda andmeid andmesubjektidelt või teistelt isikutelt.

Kui statistiline uuring, mille käigus kasutatakse isikuandmeid, ei ole ette nähtud õigusaktidega, peab selleks, et andmete kasutamine oleks seaduslik, saama andmesubjektide nõusoleku või vähemalt tuleb anda neile võimalus esitada vastuväiteid. Kui küsitlejad koguvad statistilistel eesmärkidel isikuandmeid, tuleb neile konkreetselt selgeks teha, kas andmete avaldamine on riigi õigusaktide alusel kohustuslik või mitte. Tundlikke andmeid ei tohiks mitte kunagi koguda viisil, mis

315 ELK, C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008, vt eeskätt punkt 68.

316 Euroopa Nõukogu ministrite komitee (1997), soovitus Rec(97)18 liikmesriikidele statistilistel eesmärkidel kogutavate ja töödeldavate isikuandmete kaitse kohta, 30. september 1997.

võimaldab tuvastada üksikisiku, välja arvatud juhul, kui see on sõnaselgelt lubatud riigi õigusaktidega.

Kui statistilist uuringut ei saa teha anonüümsete andmetetaning isikuandmeid on tõepoolest vaja, tuleks sel otstarbel kogutud andmed anonüümseks muuta kohe, kui see on võimalik. Miinimumtingimusena ei tohi sellise statistilise uuringu tulemustest olla võimalik tuvastada andmesubjekte, välja arvatud juhul, kui on ilmselge, et sellega ei kaasne riske.

Kui statistiline analüüs on tehtud, tuleks isikuandmed kas kustutada või muuta need anonüümseks. Selleks puhuks tehakse statistilisi andmeid käsitlevas soovituses ettepanek, et identifitseerimist võimaldavaid andmeid tuleks hoida muudest isikuandmetest eraldi. See tähendab näiteks, et andmed tuleks esitada pseudonüümi all ning krüptimisvõtit või tuvastamist võimaldavate sünonüümide loendit tuleks säilitada kõnealustest andmetest eraldi.

8.5. Finantsandmed

Põhipunktid

- Kuigi finantsandmed ei ole konventsiooni nr 108 ega andmekaitsedirektiivi tähenduses tundlikud andmed, peab nende töötlemisel täpsuse ja andmeturbe tagamiseks rakendama eritagatisi.
- Elektroonilistesse maksesüsteemidesse peab andmekaitse olema sisse ehitatud – seda nimetatakse lõimitud eraelukaitseks.
- Kõnealusele valdkonnale omased andmekaitseprobleemid tulenevad eeskätt sobivate autentimismehhanismide nõudest.

Näide: kohtuasjas *Michaud vs. Prantsusmaa*[317] seadis kaebuse esitaja (Prantsusmaal tegutsev advokaat) kahtluse alla advokaatide suhtes Prantsuse õigusaktide alusel kohaldatava kohustuse teatada kahtlustest võimaliku rahapesuga seotud tegevuse kohta tema klientide seas. EIK täheldas, et advokaatidele määratud kohustusega edastada haldusasutustele teise isiku kohta teavet, mis on

317 EIK, *Michaud vs. Prantsusmaa*, nr 12323/11, 6. detsember 2012; vt ka EIK, *Niemietz vs. Saksamaa*, nr 13710/88, 16. detsember 1992, punkt 29, ja EIK, *Halford vs. Ühendkuningriik*, nr 20605/92, 25. juuni 1997, punkt 42.

saadud teabevahetuses selle isikuga, sekkutakse advokaatide õigusesse nende korrespondentsi ja eraelu austamisele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses, kuna kõnealune õigus hõlmab ka kutsealast või ärilist tegevust. Samal ajal on sekkumine kooskõlas õigusaktidega ning sellel on õiguspärane eesmärk, st rikkumiste ja kuritegude tõkestamine. Pidades silmas, et advokaadid peavad kahtlustest teada andma üksnes väga piiratud asjaoludel, leidis EIK, et kõnealune kohustus on proportsionaalne, järeldades, et tegu ei olnud artikli 8 rikkumisega.

Konventsioonis nr 108 sätestatud üldist andmekaitse õigusraamistikku hakati maksete valdkonna suhtes kohaldama Euroopa Nõukogu 1990. aasta soovitusega R(90) 19[318]. Selles soovituses selgitatakse, millises ulatuses on andmete kogumine maksete otstarbel, eeskätt maksekaartide puhul seaduslik. Soovituses tehakse riikide seadusandjatele ettepanek rakendada üksikasjalikke õigusnorme järgmistes küsimustes: makseandmete kolmandatele isikutele edastamise piirangud, andmete säilitamise tähtajad, selgus ja arusaadavus, andmeturve, andmete piiriülene liikumine ning järelevalve ja õiguskaitsevahendid. Kavandatud lahendused vastavad hiljem andmekaitsedirektiivis sätestatud üldisest ELi andmekaitseraamistikust tulenevatele lahendustele.

Praegu on koostamisel mitu krediidiasutuste ja investeerimisühingute tegevuse ning finantsinstrumentide turgude reguleerimiseks ette nähtud õigusakti[319]. Arutluse all on ka siseringitehingute ja turuga manipuleerimise vastu võitlemisele suunatud

318 Euroopa Nõukogu ministrite komitee (1990), soovitus R(90) 19 maksete tegemisel ja muudes toimingutes kasutatavate isikuandmete kaitse kohta, 13. september 1990.

319 Euroopa Komisjon (2011), Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv finantsinstrumentide turgude kohta, millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2004/39/EÜ, KOM(2011) 656 (lõplik), Brüssel, 20. oktoober 2011; Euroopa Komisjon (2011), Ettepanek: Euroopa Parlamendi ja nõukogu määrus finantsinstrumentide turgude kohta ning millega muudetakse määrust [Euroopa turu infrastruktuuri määrus] börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta, KOM(2011) 652 (lõplik), Brüssel, 20. oktoober 2011; Euroopa Komisjon (2011), Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet ning millega muudetakse Euroopa Parlamendi ja nõukogu direktiivi 2002/87/EÜ, milles käsitletakse finantskonglomeraati kuuluvate krediidiasutuste, kindlustusseltside ja investeerimisühingute täiendavat järelevalvet, KOM(2011) 453 (lõplik), Brüssel, 20. juuli 2011.

õigusakte[320]. Kõnealuste valdkondade olulisemad andmekaitset mõjutavad probleemid on järgmised:

- finantstehingute andmete säilitamine;
- isikuandmete edastamine kolmandatesse riikidesse;
- telefonivestluste või elektroonilise side salvestamine, sealhulgas pädevate ametiasutuste õigus nõuda telefoni- ja andmeliiklusandmeid;
- isikuandmete avaldamine, sealhulgas karistusi käsitleva teabe avaldamine;
- pädevate ametiasutuste järelevalve- ja uurimisvolitused, seahulgas kohapealsed kontrollid ja eravaldustesse sisenemine dokumentide kaasavõtmiseks;
- rikkumistest teavitamise mehhanismid (süsteemid);
- liikmesriikide pädevate ametiasutuste ning Euroopa Väärtpaberiturujärelevalve koostöö (ESMA).

Kõnealustes valdkondades on ka muid küsimusi, millega sihipäraselt tegeletakse, sealhulgas andmesubjektide finantsseisundi kohta andmete kogumine[321] või välismaksed pangaülekannete kaudu, mille käigus paratamatult edastatakse isikuandmeid[322].

320 Euroopa Komisjon (2011), Ettepanek: Euroopa Parlamendi ja nõukogu määrus siseringitehingute ja turuga manipuleerimise (turu kuritarvitamise) kohta, KOM(2011) 651 (lõplik), Brüssel, 20. oktoober 2011; Euroopa Komisjon (2011), Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv siseringitehingute ja turuga manipuleerimise korral kohaldatavate kriminaalkaristuste kohta, KOM(2011) 654 (lõplik), Brüssel, 20. oktoober 2011.

321 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1060/2009, 16. september 2009, reitinguagentuuride kohta, ELT L 302, 2009; Euroopa Komisjon, ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EÜ) nr 1060/2009 reitinguagentuuride kohta, KOM(2010) 289 (lõplik), Brüssel, 2. juuni 2010.

322 Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ, 13. november 2007, makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja 2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta, ELT L 319, 2007.

Lisalugemist

1. peatükk

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*, Viin, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brüssel, kättesaadav: www.edri.org/files/paper06_datap.pdf.

Frowein, J. ja Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berliin, 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*, Brüssel, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, nr 5, lk 281–288.

Warren, S. ja Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* 4. väljaanne, nr 5, lk 193–220, kättesaadav: 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.

2. peatükk

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*, Pariis, 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*, Vol. 57, nr 6, lk 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*, kättesaadav: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

3.–5. peatükk

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" järgmises väljaandes: Grabitz, E., Hilf, M. ja Nettesheim, M. (toim.), *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 (Euroopa Liidu Põhiõiguste amet) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Euroopa Liidu Väljaannete Talitus.

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konverentsi versioon), Viin, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Euroopa Liidu Väljaannete Talitus.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, kättesaadav: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

6. peatükk

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. ja Nouwt, S. (2009), *Reinventing data protection?*, Berliin, 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.

7. peatükk

Europol (2012), *Data Protection at Europol*, Luxembourg, Euroopa Liidu Väljaannete Talitus, kättesaadav: 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, Vol. 13, nr 3, lk 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, Vol. 36, nr 5, lk 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, kättesaadav: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

8. peatükk

Büllesbach, A., Gijrath, S., Poullet, Y. ja Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. ja Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

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*, Vol. 36, nr 5, lk 722–776.

Rosemary, J. ja Hamilton, A, 2012, *Data protection law and practice*, London, Sweet & Maxwell.

Kohtupraktika

Valitud kohtuasjad Euroopa Inimõiguste Kohtu praktikast

Juurdepääs isikuandmetele

Gaskin vs. Ühendkuningriik, nr 10454/83, 7. juuli 1989
Godelli vs. Itaalia, nr 33783/09, 25. september 2012
K.H. jt vs. Slovakkia, nr 32881/04, 28. aprill 2009
Leander vs. Rootsi, nr 9248/81, 26. märts 1987
Odièvre vs. Prantsusmaa [suurkoda], nr 42326/98, 13. veebruar 2003

Andmekaitse ja sõnavabaduse tasakaalustamine

Axel Springer AG vs. Saksamaa [suurkoda], nr 39954/08, 7. veebruar 2012
Von Hannover vs. Saksamaa, nr 59320/00, 24. juuni 2004
Von Hannover vs. Saksamaa (nr 2) [suurkoda], nr 40660/08 ja 60641/08, 7. veebruar 2012

Andmekaitseprobleemid internetis

K.U. vs. Soome, nr 2872/02, 2. detsember 2008

Korrespondents

Amann vs. Šveits [suurkoda], nr 27798/95, 16. veebruar 2000
Bernh Larsen Holding AS jt vs. Norra, nr 24117/08, 14. märts 2013

Cemalettin Canli vs. Türgi, nr 22427/04, 18. november 2008
Dalea vs. Prantsusmaa, nr 964/07, 2. veebruar 2010
Gaskin vs. Ühendkuningriik, nr 10454/83, 7. juuli 1989
Haralambie vs. Rumeenia, nr 21737/03, 27. oktoober 2009
Khelili vs. Šveits, nr 16188/07, 18. oktoober 2011
Leander vs. Rootsi, nr 9248/81, 26. märts 1987
Malone vs. Ühendkuningriik, nr 8691/79, 2. august 1984
McMichael vs. Ühendkuningriik, nr 16424/90, 24. veebruar 1995
M.G. vs. Ühendkuningriik, nr 39393/98, 24. september 2002
Rotaru vs. Rumeenia [suurkoda], nr 28341/95, 4. mai 2000
S. ja Marper vs. Ühendkuningriik, nr 30562/04 ja 30566/04, 4. detsember 2008
Shimovolos vs. Venemaa, nr 30194/09, 21. juuni 2011
Turek vs. Slovakkia, nr 57986/00, 14. veebruar 2006

Karistusregistri andmebaasid

B.B. vs. Prantsusmaa, nr 5335/06, 17. detsember 2009
M.M. vs. Ühendkuningriik, nr 24029/07, 13. november 2012

DNA-andmebaasid

S. ja Marper vs. Ühendkuningriik, nr 30562/04 ja 30566/04, 4. detsember 2008

GPS-andmed

Uzun vs. Saksamaa, nr 35623/05, 2. september 2010

Terviseandmed

Biriuk vs. Leedu, nr 23373/03, 25. november 2008
I. vs. Soome, nr 20511/03, 17. juuli 2008
L.L. vs. Prantsusmaa, nr 7508/02, 10. oktoober 2006
M.S. vs. Rootsi, nr 20837/92, 27. august 1997
Szuluk vs. Ühendkuningriik, nr 36936/05, 2. juuni 2009
Z. vs. Soome, nr 22009/93, 25. veebruar 1997

Identiteet

Ciubotaru vs. Moldova, nr 27138/04, 27. aprill 2010
Godelli vs. Itaalia, nr 33783/09, 25. september 2012
Odièvre vs. Prantsusmaa [suurkoda], nr 42326/98, 13. veebruar 2003

Kutsetegevust käsitlev teave

Michaud vs. Prantsusmaa, nr 12323/11, 6. detsember 2012
Niemietz vs. Saksamaa, nr 13710/88, 16. detsember 1992

Side pealtkuulamine

Amann vs. Šveits [suurkoda], nr 27798/95, 16. veebruar 2000
Copland vs. Ühendkuningriik, nr 62617/00, 3. aprill 2007
Cotlet vs. Rumeenia, nr 38565/97, 3. juuni 2003
Kruslin vs. Prantsusmaa, nr 11801/85, 24. aprill 1990
Lambert vs. Prantsusmaa, nr 23618/94, 24. august 1998
Liberty jt vs. Ühendkuningriik, nr 58243/00, 1. juuli 2008
Malone vs. Ühendkuningriik, nr 8691/79, 2. august 1984
Halford vs. Ühendkuningriik, nr 20605/92, 25. juuni 1997
Szuluk vs. Ühendkuningriik, nr 36936/05, 2. juuni 2009

Õiguste kohaldajate kohustused

B.B. vs. Prantsusmaa, nr 5335/06, 17. detsember 2009
I. vs. Soome, nr 20511/03, 17. juuli 2008
Mosley vs. Ühendkuningriik, nr 48009/08, 10. mai 2011

Fotod

Sciacca vs. Itaalia, nr 50774/99, 11. jaanuar 2005
Von Hannover vs. Saksamaa, nr 59320/00, 24. juuni 2004

Õigus olla unustatud

Segerstedt-Wiberg jt vs. Rootsi, nr 62332/00, 6. juuni 2006

Õigus esitada vastuväiteid

Leander vs. Rootsi, nr 9248/81, 26. märts 1987
Mosley vs. Ühendkuningriik, nr 48009/08, 10. mai 2011
M.S. vs. Rootsi, nr 20837/92, 27. august 1997
Rotaru vs. Rumeenia [suurkoda], nr 28341/95, 4. mai 2000

Tundlikud andmed

I. vs. Soome, nr 20511/03, 17. juuli 2008

Michaud vs. Prantsusmaa, nr 12323/11, 6. detsember 2012
S. ja Marper vs. Ühendkuningriik, nr 30562/04 ja 30566/04, 4. detsember 2008

Järelevalve ja nõuete täitmise kontrollimine (eri osaliste, sealhulgas andmekaitseasutuste roll)

I. vs. Soome, nr 20511/03, 17. juuli 2008
K.U. vs. Soome, nr 2872/02, 2. detsember 2008
Von Hannover vs. Saksamaa, nr 59320/00, 24. juuni 2004
Von Hannover vs. Saksamaa (nr 2) [suurkoda], nr 40660/08 ja 60641/08, 7. veebruar 2012

Jälgimismeetodid

Allan vs. Ühendkuningriik, nr 48539/99, 5. november 2002
Ühendus 21 Décembre 1989 jt vs. Rumeenia, nr 33810/07 ja 18817/08,24. mai 2011
Bykov vs. Venemaa [suurkoda], nr 4378/02, 10. märts 2009
Kennedy vs. Ühendkuningriik, nr 26839/05, 18. mai 2010
Klass jt vs. Saksamaa, nr 5029/71, 6. september 1978
Rotaru vs. Rumeenia [suurkoda], nr 28341/95, 4. mai 2000
Taylor-Sabori vs. Ühendkuningriik, nr 47114/99, 22. oktoober 2002
Uzun vs. Saksamaa, nr 35623/05, 2. september 2010
Vetter vs. Prantsusmaa, nr 59842/00, 31. mai 2005

Videovalve

Köpke vs. Saksamaa, nr 420/07, 5. oktoober 2010
Peck vs. Ühendkuningriik, nr 44647/98, 28. jaanuar 2003

Kõnesalvestus

P.G. ja J.H. vs. Ühendkuningriik, nr 44787/98, 25. september 2001
Wisse vs. Prantsusmaa, nr 71611/01, 20. detsember 2005

Valitud kohtuasjad Euroopa Liidu Kohtu praktikast

Andmekaitsedirektiiviga seotud kohtupraktika

C-73/07, *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy*, 16. detsember 2008
[Ajakirjandusliku tegevuse mõiste andmekaitsedirektiivi artikli 9 tähenduses]

Liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) vs. Land Hessen*, 9. november 2010
[Teatavatest ELi põllumajandusfondidest toetust saavate isikute isikuandmete avaldamisega seotud õigusliku kohustuse proportsionaalsus]

C-101/01, *Bodil Lindqvist*, 6. november 2003
[Olukord, kus eraisik avaldab internetis teiste isikute eraelu kohta andmeid, ning selle õiguspärasus]

C-131/12, *Google Spain ja S.L., Google Inc. vs. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, eelotsusetaotlus, mille on esitanud Audiencia Nacional (Hispaania)* 9. märtsil 2012, 25. mai 2012, pooleliolev
[Otsingumootorite haldajate kohustus tagada andmesubjekti taotlusel, et tema isikuandmeid ei näidataks otsingutulemustes]

C-270/11, *Euroopa Komisjon vs. Rootsi Kuningriik*, 30. mai 2013
[Rahaline karistus direktiivi rakendamata jätmise eest]

C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU*, 29. jaanuar 2008
[Internetiteenuste osutajate kohustus avaldada failivahetusprogrammi KaZaA kasutajate identiteet intellektuaalomandi kaitsega tegelevale ühendusele]

C-288/12, *Euroopa Komisjon vs. Ungari,* 8. aprill 2014 esitatud hagi
[Riigi andmekaitseinspektori ametist kõrvaldamise õiguspärasus]

C-291/12, *Michael Schwarz vs. Stadt Bochum*, kohtujuristi ettepanek, 13. juuni 2013
[ELi esmaste õigusaktide rikkumine määrusega (EÜ) nr 2252/2004, millega nähakse ette sõrmejälgede andmete säilitamine passides]

Liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland ja Seitling ja Others*, 8. aprill 2014
[Euroopa Liidu esmase õiguse rikkumine andmete säilitamise direktiivi poolt]

C-360/10, *SABAM vs. Netlog N.V.*, 16. veebruar 2012
[Suhtlusvõrgustike haldajate kohustus hoida võrgustike kasutajate seas ära muusika- ja audiovisuaalteoste ebaseaduslikku kasutamist]

Liidetud kohtuasjad C-465/00, C-138/01 ja C-139/01, *Rechnungshof vs. Österreichischer Rundfunk jt ning Neukomm ja Lauermann vs. Österreichischer Rundfunk*, 20. mai 2003
[Õiguslik kohustus avaldada avaliku sektoriga seotud asutustes töötavate ja teatavatesse kategooriatesse kuuluvate isikute palgaandmeid ja selle õiguspärasus]

Liidetud kohtuasjad C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vs. Administración del Estado*, 24. november 2011
[Andmekaitsedirektiivi artikli 7 punkti f (teiste isikute õigustatud huvid) nõuetekohane rakendamine riigi õigusaktides]

C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik,* 9. märts 2010
[Liikmesriigi järelevalveasutuse sõltumatus]

C-524/06, *Huber vs. Saksamaa*, 16. detsember 2008
[Välismaalastega seotud andmete säilitamine statistilises registris ja selle õiguspärasus]

C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 5. mai 2011
[Uue nõusoleku vajalikkus]

C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M.E.E. Rijkeboer*, 7. mai 2009
[Andmesubjekti õigus isikuandmetega tutvuda]

C-614/10, *Euroopa Komisjon vs. Austria Vabariik*, 16. oktoober 2012
[Liikmesriigi järelevalveasutuse sõltumatus]

ELi institutsioonide andmekaitse määrusega seotud kohtupraktika

C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd*, 29. juuni 2010
[Juurdepääs dokumentidele]

C-41/00 P, *Interporc Im- und Export GmbH vs. Euroopa Ühenduste Komisjon*, 6. märts 2003
[Juurdepääs dokumentidele]

F-35/08, *Pachtitis vs. komisjon ja EPSO*, 15. juuni 2010
[Isikuandmete kasutamine ELi institutsioonides töötamise korral]

F-46/09, *V. vs. parlament*, 5. juuli 2011
[Isikuandmete kasutamine ELi institutsioonides töötamise korral]

Kohtuasjade loetelu

Euroopa Kohtu kohtupraktika

Euroopa Inimõiguste Kohtu kohtupraktika

Riikide kohtute kohtupraktika

Euroopa Liidu Põhiõiguste Amet
Euroopa Nõukogu – Euroopa Inimõiguste Kohus

Euroopa andmekaitseõiguse käsiraamat

2015 — 199 lk — 14,8 × 21 cm

ISBN 978-92-871-9947-8 (CoE)
ISBN 978-92-9239-331-1 (FRA)
doi:10.2811/53785

Euroopa Liidu Põhiõiguste Ameti kohta on Internetis saadaval rohkesti lisateavet. Teave on kättesaadav FRA kodulehel (fra.europa.eu).

Lisateave Euroopa Nõukogu kohta on Internetis kättesaadav veebilehel: hub.coe.int

Lisainfo Euroopa Inimõiguste Kohtu praktikast on kättesaadav Kohtu veebilehel: www.echr.coe.int. HUDOC-i otsinguportaal võimaldab juurdepääsu otsustele inglise ja/või prantsuse keeles, otsuste tõlgetele teistesse keeltesse, kohtupraktika igakuulistele ülevaadetele, pressiteadetele ja muule kohtu tööd puudutavale informatsioonile.

KUST SAAB ELi VÄLJAANDEID?

Tasuta väljaanded:
- üksikeksemplarid:
  EU Bookshopi kaudu (http://bookshop.europa.eu);
- rohkem eksemplare ning plakatid ja kaardid:
  Euroopa Liidu esindustest (http://ec.europa.eu/represent_et.htm), delegatsioonidest väljaspool ELi (http://eeas.europa.eu/delegations/index_et.htm), kasutades Europe Direct'i teenistust (http://europa.eu/europedirect/index_et.htm) või helistades infotelefonile 00 800 6 7 8 9 10 11 (kõikjalt EList helistades tasuta) (*).

Tasulised väljaanded:
- EU Bookshopi kaudu (http://bookshop.europa.eu);

Tasulised tellimused:
- Euroopa Liidu Väljaannete Talituse edasimüüjate kaudu (http://publications.europa.eu/others/agents/index_et.htm).

(*) Antav teave on tasuta nagu ka enamik kõnesid (v.a mõne operaatori, hotelli ja telefonikabiini puhul).

Kuidas hankida Euroopa Nõukogu väljaandeid?

Euroopa Nõukogu kirjastus avaldab materjale kõigis organisatsiooni töövaldkondades, mis hõlmavad inimõigusi, õigusteadust, tervishoidu, eetikat, sotsiaalvaldkonda, keskkonda, haridust, kultuuri, sporti, noorsugu ja arhitektuuripärandit. Laias valikus raamatuid ja elektroonilisi väljaandeid saab tellida internetist (http://book.coe.int/).

Virtuaalne lugemistuba võimaldab kasutajatel tasuta tutvuda väljavõtetega värskelt avaldatud põhiteostest või teatavate ametlike dokumentide täistekstidega.

Teave Euroopa Nõukogu konventsioonide kohta koos lepingutekstidega on kättesaadav lepingubüroo veebilehel http://conventions.coe.int/.

10.2811/53785 TK-01-13-772-ET-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Info- ja kommunikatsioonitehnoloogia hoogsa arengu taustal on üha olulisem tugevdada ka isikuandmete kaitset, pidades silmas, et õigus isikuandmete kaitsele on talletatud nii Euroopa Liidu (ELi) kui ka Euroopa Nõukogu õigusaktides. Tehnoloogia areng laiendab ka näiteks jälgimistegevuse, side pealtkuulamise ja andmete säilitamise piire, tõstatades kõnealuse õiguse puhul olulisi probleeme. Käsiraamat on välja töötatud õigustöötajatele, kes ei ole spetsialiseerunud andmekaitsevaldkonnale, ent soovivad end nende küsimustega kurssi viia. Selles antakse ülevaade ELi ja Euroopa Nõukogu tasandil kohaldatavatest õigusraamistikest. Käsiraamatus selgitatakse peamist kohtupraktikat, kirjeldades kokkuvõtlikult nii Euroopa Inimõiguste Kohtu (EIK) kui ka Euroopa Liidu Kohtu (ELK) olulisi kohtuotsuseid. Selliste olukordade puhul, kus kohtupraktikat ei ole veel välja kujunenud, kirjeldatakse käsiraamatus oletatavaid stsenaariume. Lühidalt öeldes on andmekaitseõiguse käsiraamatu eesmärk aidata tagada, et õigust isikuandmete kaitsele aktiivselt ja otsustavalt toetatakse.

EUROOPA LIIDU PÕHIÕIGUSTE AMET
Schwarzenbergplatz 11 – 1040 Viin – Austria
Tel +43 (1) 580 30-60 – Faks +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EUROOPA NÕUKOGU
EUROOPA INIMÕIGUSTE KOHUS
67075 Strasbourg Cedex – Prantsusmaa
Tel +33 (0) 3 88 41 20 18 – Faks +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Väljaannete talitus
ISBN 978-92-871-9947-8 (CoE)
ISBN 978-92-9239-331-1 (FRA)