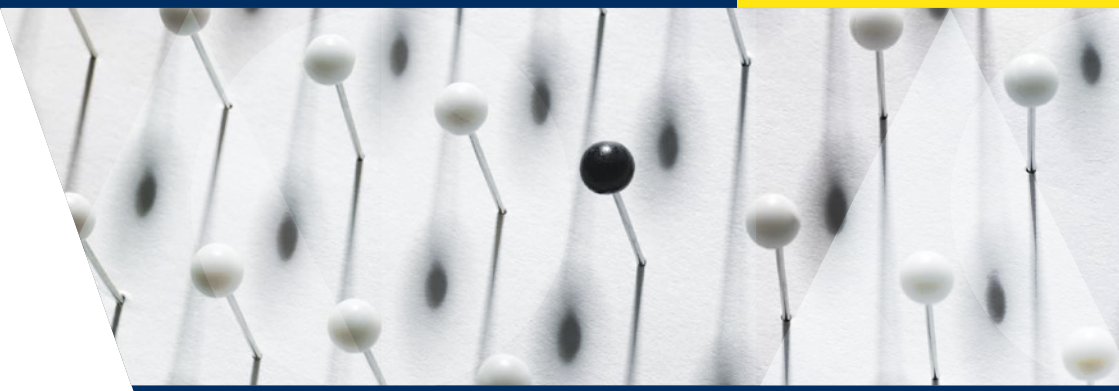
KÄSIRAAMAT



Euroopa andmekaitseõiguse käsiraamat

2018. aasta väljaanne

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

EDPS

Käsiraamatu käsikiri valmis 2018. aasta aprillis.

Uuendused avaldatakse Euroopa Liidu Põhiõiguste Ameti (FRA) veebilehel fra.europa.eu, Euroopa Nõukogu veebilehel coe.int/dataprotection, Euroopa Inimõiguste Kohtu veebilehe echr.coe.int kohtupraktika jaotises ja Euroopa Andmekaitseinspektori veebilehel edps.europa.eu.

Fotod (esilehel ja tekstis): © iStockphoto

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2020

Euroopa Nõukogu:	ISBN 978-92-871-9833-4		
FRA – Print:	ISBN 978-92-9474-441-8	doi:10.2811/627576	TK-05-17-225-ET-C
FRA – PDF:	ISBN 978-92-9474-446-3	doi:10.2811/383697	TK-05-17-225-ET-N

Euroopa andmekaitseõiguse käsiraamat

2018. aasta väljaanne

Eessõna

Ühiskond muutub üha digitaalsemaks. Tehnika arengu kiirus ja isikuandmete töötlemise viis mõjutab meid nende muutuste taustal iga päev ja igati. Euroopa Liidu (EL) ja Euroopa Nõukogu õigusraamistikud, millega tagatakse privaatsuse ja isikuandmete kaitse, vaadati hiljuti läbi.

Euroopa on kogu maailmas andmekaitse valdkonnas juhtpositsioonil. ELi andmekaitsestandardid põhinevad Euroopa Nõukogu konventsioonil nr 108, ELi õigusaktidel – sealhulgas isikuandmete kaitse üldmäärusel ning politseitöö ja kriminaalõigusasutuste andmekaitse direktiivil – ning Euroopa Inimõiguste Kohtu ja Euroopa Liidu Kohtu kohtupraktikal.

ELi ja Euroopa Nõukogu andmekaitsereformid on ulatuslikud ja mõnikord keerukad, nende kasu on laialdane ning mõju üksikisikutele ja ettevõtetele ulatuslik. Käsiraamatu eesmärk on teadvustada andmekaitse-eeskirju ja levitada teavet nende kohta, eriti üldjuristidele, kes peavad oma töös käsitlema andmekaitseküsimusi.

Käsiraamatu on koostanud Euroopa Liidu Põhiõiguste Amet (FRA) koos Euroopa Nõukoguga (koostöös Euroopa Inimõiguste Kohtu kantseleiga) ja Euroopa Andmekaitseinspektoriga. Sellega ajakohastatakse 2014. aasta väljaannet ning see kuulub FRA ja Euroopa Nõukogu ühistöös koostatud õiguskäsiraamatute sarja.

Soovime tänada Belgia, Eesti, Gruusia, Iirimaa, Itaalia, Monaco, Prantsusmaa, Šveitsi, Ungari ja Ühendkuningriigi andmekaitseasutusi abivalmis tagasiside eest käsiraamatu kavandile. Lisaks avaldame tunnustust Euroopa Komisjoni andmekaitseüksusele ning rahvusvaheliste andmevoogude ja andmekaitse üksusele.

Täname Euroopa Liidu Kohut käsiraamatu ettevalmistamisel antud dokumentaalse toetuse eest.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Euroopa Nõukogu inimõiguste ja õigusküsimuste peadirektor	Euroopa andmekaitseinspektor	Euroopa Liidu Põhiõiguste Ameti direktor

Sisukord

Lühendid

BCR	siduvad kontsernisisesed eeskirjad
C-SIS	Schengeni keskinfosüsteem
CCTV	videovalve
CETS	Euroopa Nõukogu lepingute sari
CIS	tolliinfosüsteem
CRM	kliendisuhtehaldus
DPA	andmekaitseasutus
DPO	andmekaitseametnik
EAW	Euroopa vahistamismäärus
EDPB	Euroopa Andmekaitsenõukogu
EDPS	Euroopa Andmekaitseinspektor
EFSA	Euroopa Toiduohutusamet
EFTA	Euroopa Vabakaubanduse Assotsiatsioon
EIK	Euroopa Inimõiguste Kohus
EIÕK	Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
EL	Euroopa Liit
ELi leping	Euroopa Liidu leping
ELK	Euroopa Liidu Kohus (enne detsembrit 2009 Euroopa Ühenduste Kohus)
ELT	Euroopa Liidu Teataja
ELTL	Euroopa Liidu toimimise leping
EMP	Euroopa Majanduspiirkond
EN	Euroopa Nõukogu
ENISA	Euroopa Liidu Võrgu- ja Infoturbeamet
ENU	Europoli riiklik üksus
EPPO	Euroopa Prokuratuur
ESMA	Euroopa Väärtpaberiturujärelevalve
eTEN	üleeuroopalised telekommunikatsioonivõrgud

eu-LISA	Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Amet
EuroPriSe	Euroopa eraelu puutumatuse märgiste süsteem
EÜ	Euroopa Ühendus
FRA	Euroopa Liidu Põhiõiguste Amet
GDPR	isikuandmete kaitse üldmäärus
GPS	globaalne positsioneerimissüsteem
Harta	Euroopa Liidu põhiõiguste harta
ICCPR	kodaniku- ja poliitiliste õiguste rahvusvaheline pakt
IKT	info- ja sidetehnoloogia
ISP	internetiteenuse osutaja
JSB	ühine järelevalveasutus
Konventsioon nr 108	Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (Euroopa Nõukogu). Taanis Elsinores (17.–18. mai 2018) toimunud 128. istungjärgul võttis Euroopa Nõukogu ministrite komitee vastu protokolli (CETS nr 223), millega muudetakse konventsiooni nr 108 (edaspidi „nüüdisajastatud konventsioon nr 108“). Tekstis tähendab „nüüdisajastatud konventsioon nr 108“ nimetatud konventsiooni, mida on muudetud protokolliga CETS nr 223.
N-SIS	riiklik Schengeni infosüsteem
NGO	vabaühendus
OECD	Majanduskoostöö ja Arengu Organisatsioon
PIN	isikukood
PNR	broneeringuinfo
SCG	järelevalve koordineerimisrühm
SEPA	ühtne euromaksete piirkond
SIS	Schengeni infosüsteem
SWIFT	Ülemaailmne Pankadevahelise Finantsinfo Ühing
UDHR	inimõiguste ülddeklaratsioon
VIS	viisainfosüsteem
ÜRO	Ühinenud Rahvaste Organisatsioon

Kuidas käsiraamatut kasutada?

Käsiraamatus kirjeldatakse Euroopa Liidu ja Euroopa Nõukogu andmekaitse õigusnorme. Käsiraamat on abiks töötajatele, kes ei ole spetsialiseerunud andmekaitse valdkonnale, sealhulgas juristidele, kohtunikele ja muudele õigustöötajatele, samuti kõigis muude asutuste ja ühingute (nt vabaühenduste) töötajatele, kellel tuleb käsitleda andmekaitsega seotud õigusküsimusi.

Käsiraamatus viidatakse asjakohasele ELi õigusele ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonile, samuti Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioonile (konventsioon nr 108) ja muudele Euroopa Nõukogu õigusaktidele.

Iga peatüki alguses on tabel, kus loetletakse peatüki teemadega seotud õigussätted. Tabel hõlmab nii Euroopa Nõukogu kui ka ELi õigust ning sisaldab valitud näiteid Euroopa Inimõiguste Kohtu (EIK) ja Euroopa Liidu Kohtu (ELK) praktikast. Seejärel loetletakse Euroopa mõlema õiguskorra asjakohased õigusaktid käsitletavate teemade järjestuses. Nii näeb lugeja, mis punktides õigussüsteemid ühtivad ja kus erinevad. See peaks võimaldama lugejatel leida ka nende olukorraga seotud põhiteabe, eriti siis, kui neile kehtib üksnes Euroopa Nõukogu õigus. Mõnes peatükis võib teemade järjestus tabelis ülevaatlikkuse huvides veidi erineda peatüki sisust. Käsiraamatus antakse lühiülevaade ka ÜRO raamistikust.

Nende ELi-väliste riikide õigusspetsialistid, mis on Euroopa Nõukogu liikmesriigid ning ühinenud Euroopa põhiõiguste ja vabaduste kaitse konventsiooniga ning konventsiooniga nr 108, saavad oma riigi kohta asjakohast teavet vaadata kohe Euroopa Nõukogu õiguse jaotistest. ELi-väliste riikide spetsialistid peavad ka meeles pidama, et alates ELi isikuandmete kaitse üldmääruse vastuvõtmisest kohaldatakse ELi andmekaitse-eeskirju väljaspool ELi asutatud organisatsioonide ja muude isikute suhtes, kui nad töötlevad isikuandmeid ning pakuvad kaupu ja teenuseid andmesubjektidele liidus või jälgivad selliste andmesubjektide käitumist.

ELi liikmesriikides tegutsevad spetsialistid peavad tutvuma mõlema jaotisega, sest nende riikide suhtes on siduvad mõlemad õiguskorrad. Tuleb märkida, et Euroopa andmekaitse-eeskirjade reformid ja nüüdisajastamine, mis toimub Euroopa Nõukogu raames (nüüdisajastatud konventsioon nr 108, mida on muudetud protokolliga CETS nr 223) ja ELi raamistikus (isikuandmete kaitse üldmääruse ja direktiivi (EL) 2016/680 vastuvõtmine), toimusid paralleelselt. Mõlema õigussüsteemi

seadusandjad on teinud kõik võimaliku, et tagada mõlema õigusraamistiku järjepidevus ja ühilduvus. Seega on reformid kooskõlastanud Euroopa Nõukogu ja ELi andmekaitseõigust senisest rohkem. Teemade lisateave on jaotises „Lisateave". Teave konventsiooni nr 108 ja selle 2001. aasta lisaprotokolli sätete kohta, mida kohaldatakse kuni muutmisprotokolli jõustumiseni, on käsiraamatu 2014. aasta väljaandes.

Euroopa Nõukogu õigust tutvustatakse lühiviidetega mõningatele Euroopa Inimõiguste Kohtu asjadele. Need on valitud Euroopa Inimõiguste Kohtu paljude andmekaitsega seotud otsuste seast.

Asjakohane ELi õigus hõlmab vastu võetud seadusandlikke meetmeid, aluslepingute asjakohaseid sätteid ja Euroopa Liidu põhiõiguste hartat, nagu seda tõlgendatakse Euroopa Liidu Kohtu praktikas. Käsiraamatus esitatakse ka arvamusi ja suuniseid, mille on vastu võtnud artikli 29 töörühm, mis on andmekaitsedirektiivi kohaselt ELi liikmesriikidele eksperdinõuannete andmise nõuandev organ, mida asendab alates 25. maist 2018 Euroopa Andmekaitsenõukogu. Olulist teavet ELi õiguse tõlgendamise kohta annavad ka Euroopa andmekaitseinspektori arvamused, mis on seega käsiraamatusse lisatud.

Käsiraamatus kirjeldatud või viidatud juhtumitega esitatakse näiteid nii Euroopa Inimõiguste Kohtu kui ka Euroopa Liidu Kohtu laialdasest kohtupraktikast. Käsiraamatu lõpus olevate suuniste eesmärk on abistada lugejaid kohtupraktika otsimisel veebis. Esitatud Euroopa Liidu Kohtu kohtupraktika on seotud varasema andmekaitsedirektiiviga. Euroopa Liidu Kohtu tõlgendusi saab siiski endiselt kohaldada isikuandmete kaitse üldmäärusega kehtestatud vastavate õiguste ja kohustuste suhtes.

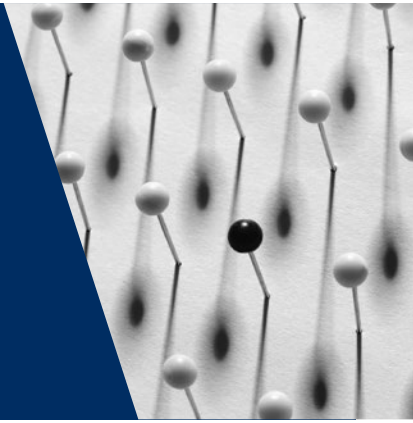
Sinise taustaga tekstikastides on hüpoteetilised eluliste olukordade stsenaariumid. Need näitlikustavad Euroopa andmekaitse-eeskirjade kohaldamist praktikas, eelkõige kui küsimuses puudub Euroopa Inimõiguste Kohtu või Euroopa Liidu Kohtu kohtupraktika. Teistes, halli taustaga tekstikastides on mujalt kui Euroopa Inimõiguste Kohtu või Euroopa Liidu Kohtu kohtupraktikast pärit näited – näiteks õigusaktidest ja artikli 29 töörühma arvamustest.

Käsiraamatu alguses on lühiülevaade mõlema õigussüsteemi rollist Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni ja ELi õigusaktide alusel (1. peatükk). 2.–10. peatükis käsitletakse järgmist:

- andmekaitse terminoloogia;
- Euroopa andmekaitseõiguse üldpõhimõtted;
- Euroopa andmekaitseõiguse eeskirjad;
- sõltumatu järelevalve;
- andmesubjektide õigused ja õiguste jõustamine;
- isikuandmete piiriülene edastamine ja liikumine;
- andmekaitse politsei ja kriminaalõiguse kontekstis;
- muud Euroopa andmekaitse-eeskirjad konkreetsetes valdkondades;
- isikuandmete kaitse nüüdisprobleemid.

1

Euroopa andmekaitseõiguse kontekst ja taust



EL	Teemad	EN
Õigus andmekaitsele		
Euroopa Liidu toimimise lepingu artikkel 16 Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artikkel 8 (õigus isikuandmete kaitsele) Direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (andmekaitsedirektiiv), EÜT 1995 L 281 (kehtib maini 2018) Nõukogu raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta, ELT 2008 L 350 (kehtib maini 2018) Määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), ELT 2016 L 119		Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 (õigus era- ja perekonnaelu ja kodu ning sõnumite saladuse austamisele)

EL	Teemad	EN
Direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (politsei- ja õigusasutuste andmekaitse), ELT 2016 L 119 Direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT 2002 L 201 Määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (ELi institutsioonide andmekaitse määrus), EÜT 2001 L 8		Isikuandmete automatiseeritud töötlemisel isiku kaitse nüüdisajastatud konventsioon (nüüdisajastatud konventsioon nr 108)
Isikuandmete kaitse õiguse piirangud		
Harta artikli 52 lõige 1 Isikuandmete kaitse üldmääruse artikkel 23 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen* [suurkoda], 2010		Inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõige 2 Nüüdisajastatud konventsiooni nr 108 artikkel 11 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 2008
Õiguste tasakaalustamine		
ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen* [suurkoda], 2010	Üldine	
ELK, C-73/07, *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy* [suurkoda], 2008 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 2014	Sõnavabadus	EIK, *Axel Springer AG vs. Saksamaa* [suurkoda], nr 39954/08, 2012 EIK, *Mosley vs. Ühendkuningriik*, nr 48009/08, 2011 EIK, *Bohlen vs. Saksamaa*, nr 53495/09, 2015

EL	Teemad	EN
ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd* [suurkoda], 2010 ELK, C-615/13P, *ClientEarth, PAN Europe vs. EFSA*, 2015	Juurdepääs dokumentidele	EIK, *Magyar Helsinki Bizottság vs. Ungari* [suurkoda], nr 18030/11, 2016
Isikuandmete kaitse üldmääruse artikkel 90	Kutsesaladus	EIK, *Pruteanu vs. Rumeenia*, nr 30181/05, 2015
Isikuandmete kaitse üldmääruse artikkel 91	Usu- ja veendumusvabadus	
	Kunsti ja teaduse vabadus	EIK, *Vereinigung bildender Künstler vs. Austria*, nr 68354/01, 2007
ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU* [suurkoda], 2008	Omandi kaitse	
ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 2014 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 2017	Majandusõigused	

1.1. Õigus isikuandmete kaitsele

Põhipunktid

- Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaselt kuulub era- ja perekonnaelu ja kodu ning sõnumi saladuse austamise õiguse alla isiku õigus kaitsele isikuandmete töötlemisel.
- Euroopa Nõukogu konventsioon nr 108 on esimene ja seni ainus rahvusvaheline õigusliku siduv dokument, mis käsitleb andmekaitset. Konventsiooni nüüdisajastati, mille tulemusel võeti vastu muutmisprotokoll CETS nr 223.
- ELi õiguses käsitatakse andmekaitset eraldi põhiõigusena. Seda kinnitatakse ka Euroopa Liidu toimimise lepingu artiklis 16 ja ELi põhiõiguste harta artiklis 8.
- ELi õiguses hakati andmekaitset esimest korda reguleerima andmekaitsedirektiiviga 1995. aastal.

- Tehnika kiire arengu tõttu võttis EL 2016. aastal vastu uue õigusakti, et kohandada andmekaitse-eeskirju digiajastuga. Isikuandmete kaitse üldmäärust, millega andmekaitsedirektiiv tunnistati kehtetuks, hakati kohaldama 2018. aasta mais.
- Koos isikuandmete kaitse üldmäärusega võttis EL vastu õigusakti riigiasutustes isikuandmete õiguskaitse eesmärgil töötlemise kohta. Direktiiviga (EL) 2016/680 kehtestatakse andmekaitse-eeskirjad ja põhimõtted, mis reguleerivad isikuandmete töötlemist süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil.

1.1.1. Õigus eraelu austamisele ja õigus isikuandmete kaitsele: lühike sissejuhatus

Kuigi õigus eraelu austamisele ja õigus isikuandmete kaitsele on tihedalt seotud, on need eraldi õigused. Õigus privaatsusele ehk eraelu puutumatusele – mida nimetatakse Euroopa õiguses õiguseks eraelu austamisele – ilmus inimõigusi käsitlevasse rahvusvahelisse õigusesse 1948. aastal inimõiguste ülddeklaratsiooni kaudu kui üks põhilisi kaitstud inimõigusi. Peagi pärast inimõiguste ülddeklaratsiooni vastuvõtmist kinnitas ka Euroopa seda õigust Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis, mis on lepinguosalistele õiguslikult siduv ja mis koostati 1950. aastal. Konventsioonis on sätestatud, et igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. Avaliku sektori asutuse sekkumine sellesse õigusesse on keelatud, v.a kooskõlas seadusega, kui sekkumine täidab olulisi ja õigustatud avalikke huve ning on demokraatlikus ühiskonnas vajalik.

Inimõiguste ülddeklaratsioon ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioon võeti vastu ammu enne arvutite ja interneti arengut ning infoühiskonna tekkimist. Selline areng on toonud üksikisikutele ja ühiskonnale suuri eeliseid, parandades elukvaliteeti, tõhusust ja tootlikkust. Samal ajal tekitab see uusi riske seoses õigusega eraelu austamisele. Vastuseks vajadusele isikuandmete kogumist ja kasutamist reguleerivate erisätete järele tekkis uus eraelu puutumatuse kontseptsioon, mida mõnes jurisdiktsioonis nimetatakse teabeprivaatsuseks ja mõnes teabelise enesemääramise õiguseks[1]. Selle kontseptsiooni tulemusel töötati välja eriõigusnormid, millega tagatakse isikuandmete kaitse.

1 Saksamaa föderaalne konstitutsioonikohus kinnitas teabelise enesemääramise õigust 1983. aastal otsuses kohtuasjas *Volkszählungsurteil*, BVerfGE Bd. 65, lk 1jj. Kohus leidis, et teabeline enesemääramine tuleneb isiksuse austamise põhiõigusest, mida kaitseb Saksamaa põhiseadus. Euroopa Inimõiguste Kohus tunnistas 2017. aasta kohtuotsuses, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 „sätestatakse õigus teabelisele enesemääramisele". Vt EIK, *Satakunnan Markkinapörssi Oy ja Satamedia Oy vs. Soome* [suurkoda], nr 931/13, 27. juuni 2017, punkt 137.

Euroopas algas andmekaitse 1970. aastatel, kui mõni riik võttis vastu õigusaktid, et reguleerida isikuandmete töötlemist riigiasutustes ja suurettevõtetes[2]. Seejärel kehtestati andmekaitse õigusaktid Euroopa tasandil[3] ja aastate jooksul on andmekaitse kujunenud omaette väärtuseks, mis eristub õigusest eraelu austamisele. ELi õiguskorras tunnustatakse andmekaitset kui põhiõigust, mis on eraldi põhiõigusest eraelu austamisele. Selline eraldamine tekitab küsimuse kummagi õiguse seostest ja erinevustest.

Õigus eraelu austamisele ja õigus isikuandmete kaitsele on omavahel tihedalt seotud. Mõlema eesmärk on kaitsta sarnaseid väärtusi – üksikisikute sõltumatust ja inimväärikust –, tagades neile isikliku ala, kus nad saavad vabalt arendada isiksust, mõelda ja kujundada arvamusi. Seega on need teiste põhivabaduste, näiteks sõnavabaduse, rahumeelse kogunemise ja ühinemise vabaduse ning usuvabaduse teostamise olulised eeldused.

Kummalgi õigusel on eri sõnastus ja kohaldamisala. Õigus eraelu puutumatusele seisneb üldises sekkumiskeelus, mille suhtes kehtivad teatud avaliku huvi kriteeriumid, mis võivad teatud juhtudel õigustada sekkumist. Isikuandmete kaitset peetakse nüüdisaegseks ja aktiivseks õiguseks,[4] millega luuakse kontrolli- ja tasakaalusüsteem, et kaitsta isikuid nende isikuandmete töötlemisel. Töötlemine peab olema vastavuses isikuandmete kaitse oluliste elementidega, nimelt sõltumatu järelevalve ja andmesubjekti õiguste austamisega[5].

Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artiklis 8 kinnitatakse õigust isikuandmete kaitsele ja nimetatakse selle õigusega seotud põhiväärtused. Artiklis sätestatakse, et isikuandmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul

2 Saksamaa Hesseni liidumaa võttis 1970. aastal vastu esimese andmekaitseseaduse, mis kehtis ainult nimetatud liidumaal. 1973. aastal võttis Rootsi vastu maailma esimese riikliku andmekaitseseaduse. 1980. aastate lõpuks olid andmekaitse õigusaktid vastu võtnud ka mitu muud Euroopa riiki (Madalmaad, Prantsusmaa, Saksamaa ja Ühendkuningriik).

3 Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (konventsioon nr 108) võeti vastu 1981. aastal. EL võttis oma esimese ulatusliku andmekaitseõigusakti vastu 1995. aastal: direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.

4 Kohtujurist Sharpston kirjeldas juhtumit nii, et see hõlmab kaht eri õigust: nn klassikalist õigust eraelu puutumatuse kaitsele ja nn nüüdisaegsemat õigust ehk õigust andmekaitsele. Vt ELK, liidetud kohtuasjad C-92/09 ja C-93/02, *Volker und Markus Schecke GbR vs. Land Hessen*, *kohtujurist Sharpstoni ettepanek*, 17. juuni 2010, punkt 71.

5 Hustinx, P., Euroopa andmekaitseinspektori kõned ja artiklid, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, juuli 2013.

alusel. Isikutel peab olema õigus tutvuda oma isikuandmetega ja nõuda nende parandamist ning selle õiguse järgimist peab kontrollima sõltumatu asutus.

Õigust isikuandmete kaitsele on vaja isikuandmete töötlemisel, seega on see laiem kui õigus eraelu austamisele. Isikuandmete mis tahes töötlemisel kohaldatakse asjakohast kaitset. Andmekaitse on seotud mis tahes isikuandmete ja andmetöötlusega, olenemata seosest eraelu puutumatusega ning mõjust sellele. Nagu allpool esitatud näidetest nähtub, võidakse isikuandmete töötlemisel riivata ka õigust eraelule. Andmekaitse-eeskirjade kohaldamiseks ei ole vaja tõendada eraeluga seotud rikkumist.

Õigus eraelu puutumatusele on seotud olukordadega, kus kahjustatakse isiku erahuvi ehk eraelu. Nagu käesolevas käsiraamatus näidatud, tõlgendatakse kohtupraktikas eraelu mõistet väga mitmeti, sest see hõlmab intiimseid olukordi, delikaatset või konfidentsiaalset teavet, teavet, mis võib kahjustada avalikkuse suhtumist isikusse, ning isegi isiku tööelu aspekte ja avalikku käitumist. Hinnang, kas eraellu sekkutakse või on sellesse sekkutud või mitte, oleneb siiski iga juhtumi taustast ja asjaoludest.

Seevastu võivad isikuandmete töötlemisega seotud toimingud kuuluda andmekaitse-eeskirjade kohaldamisalasse ja tingida õiguse isikuandmete kaitsele. Kui näiteks tööandja registreerib töötajate nimede ja makstud töötasu teavet, ei saa üksnes selle teabe registreerimist pidada eraellu sekkumiseks. Sellise sekkumise olemasolu võib siiski väita, kui näiteks tööandja edastas töötajate isikuandmed kolmandatele isikutele. Tööandjad peavad igal juhul järgima andmekaitse-eeskirju, sest töötajate andmete registreerimine on andmetöötlus.

Näide: kohtuasjas *Digital Rights Ireland*[6] paluti Euroopa Liidu Kohtul otsustada direktiivi 2006/24/EÜ kehtivuse üle, arvestades isikuandmete kaitse ja eraelu austamise põhiõigust, mida kinnitab Euroopa Liidu põhiõiguste harta. Direktiiviga nõuti, et üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujad säilitaksid kodanike sideandmeid kuni kaks aastat, et tagada andmete kättesaadavus raskete kuritegude ennetamisel, uurimisel ja nende eest vastutusele võtmisel. Meede oli seotud ainult metaandmete, asukohaandmete ja andmetega, mida on vaja abonendi või kasutaja tuvastamiseks. Seda ei kohaldatud elektroonilise side sisu suhtes.

6 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

ELK leidis, et direktiiv riivab põhiõigust isikuandmete kaitsele, „sest direktiiv näeb ette isikuandmete töötlemise“[7]. Lisaks leidis kohus, et direktiiv riivas õigust eraelu austamisele[8]. Direktiivi kohaselt võivad säilitatavad isikuandmed, millele võib pädevatel asutustel olla juurdepääs, koosvõetuna võimaldada „teha väga täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse, näiteks nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad“[9]. Mõlema õiguse riive oli ulatuslik ja väga raske.

ELK tunnistas direktiivi 2006/24/EÜ kehtetuks, leides, et kuigi sellega taotletakse õiguspärast eesmärki, riivab see raskelt õigust isikuandmete kaitsele ja eraelu puutumatusele ega piirdu rangelt vajalikuga.

1.1.2. Rahvusvaheline õigusraamistik: ÜRO

ÜRO raamistikus ei tunnustata isikuandmete kaitset põhiõigusena, kuigi õigus eraelu puutumatusele on juba ammu rahvusvahelises õiguskorras põhiõigus. Inimõiguste ülddeklaratsiooni artikkel 12 era- ja perekonnaelu austamise kohta[10] oli esimene kord, kui rahvusvahelise õigusaktiga sätestati isiku õigus oma eraelu kaitsele teiste, eriti riigi sekkumise eest. Kuigi inimõiguste ülddeklaratsioon on mittesiduv, on inimõigustega seotud rahvusvahelise õiguse alusaktina sellel oluline staatus ning see on mõjutanud inimõiguste muude õigusaktide arengut Euroopas. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt jõustus 1976. aastal. Selles kuulutatakse, et kellegi eraelu, kodu või sõnumite saladust ei tohi meelevaldselt ega ebaseaduslikult riivata ning kellegi au ja mainet ei tohi seadusevastaselt rünnata. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt on 169 osalisega rahvusvaheline leping, mis kohustab osalisi austama ja tagama üksikisikute kodanikuõigusi, sealhulgas eraelu puutumatust.

Vastusena uute tehnoloogiate arengule ja paljastustele mõnes riigis toimuva massijälgimise kohta (Snowdeni paljastused) on ÜRO võtnud alates 2013. aastast eraelu puutumatuse kohta vastu kaks resolutsiooni pealkirjaga „Õigus eraelu

7 *Ibid.*, punkt 36.

8 *Ibid.*, punktid 32–35.

9 *Ibid.*, punkt 27.

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

puutumatusele digitaalajastul“[11]. Resolutsioonides mõistetakse hukka massiline jälgimine ja juhitakse tähelepanu sellise jälgimise mõjule eraelu puutumatusele ja sõnavabadusele kui põhiõigustele ning elujõulise ja demokraatliku ühiskonna toimimisele. Kuigi resolutsioonid ei ole õiguslikult siduvad, tekitasid need olulise rahvusvahelise kõrgetasemelise poliitilise arutelu eraelu puutumatuse, uute tehnoloogiate ja jälgimise üle. Samuti alustas nende tulemusena tegevust eraelu puutumatuse õiguse eriraportöör, kellel on volitused seda õigust edendada ja kaitsta. Raportööri eriülesanded hõlmavad teabe kogumist riikide tavade ja kogemuste kohta seoses eraelu puutumatusega ning uute tehnoloogiatega seotud probleemidega, parimate tavade vahetamise ja edendamisega ning võimalike takistuste tuvastamisega.

Kui varasemates resolutsioonides keskenduti massilise jälgimise negatiivsele mõjule ja riikide vastutusele luureasutuste volituste piiramisel, kajastavad hiljutised resolutsioonid eraelu puutumatuse kohta ÜROs toimuva arutelu olulist arengut[12]. 2016. ja 2017. aastal vastu võetud resolutsioonides kinnitatakse taas vajadust piirata luureasutuste volitusi ja mõista hukka massiline jälgimine. Samas märgitakse neis selge sõnaga, et „ettevõtete suurenev suutlikkus isikuandmete kogumisel, töötlemisel ja kasutamisel võib ohustada eraelu puutumatuse õiguse kasutamist digiajastul“. Seega osutatakse resolutsioonides lisaks riigiasutuste vastutusele ka erasektori kohustusele austada inimõigusi ning kutsutakse ettevõtteid üles teavitama kasutajaid isikuandmete kogumisest, kasutamisest, jagamisest ja säilitamisest ning kehtestama läbipaistvaid töötlemispõhimõtteid.

1.1.3. 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.

Lepinguosalistel on rahvusvaheline kohustus järgida konventsiooni. Praeguseks on kõik Euroopa Nõukogu liikmesriigid konventsiooni oma riiklikku õigusse üle võtnud

11 Vt ÜRO Peaassamblee, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18. detsember 2013 ja ÜRO Peaassamblee, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/69/L.26/Rev.1, New York, 19. november 2014.

12 ÜRO Peaassamblee, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/71/L.39/Rev.1, New York, 16. november 2016; ÜRO Inimõiguste Nõukogu, *The right to privacy in the digital age*, A/HRC/34/L.7/Rev.1, 22. märts 2017.

või selle riiklike õigusaktidega jõustanud ning on seega kohustatud tegutsema kooskõlas konventsiooni sätetega. Lepinguosalised peavad mis tahes tegevuse või võimu teostamisel austama konventsioonis sätestatud õigusi. See hõlmab ka riigi julgeolekuga seotud tegevust. Euroopa Inimõiguste Kohtu (EIK) põhimõttelistes otsustes on käsitletud riigi tegevust riigi julgeoleku õigusaktide ja -tava tundlikes valdkondades[13]. Kohus on kindla sõnaga kinnitanud, et jälgimistegevus on eraelu austamise riive[14].

Tagamaks et lepinguosalised täidavad konventsioonist tulenevaid kohustusi, asutati 1959. aastal Prantsusmaal Strasbourgis Euroopa Inimõiguste Kohus (EIK). EIK tagab, et riigid täidavad konventsioonist tulenevaid kohustusi, arutades isikute, isikurühmade, vabaühenduste või juriidiliste isikute kaebusi konventsiooni väidetava rikkumise kohta. Samuti saab EIK käsitleda ühe või mitme Euroopa Nõukogu liikmesriigi algatatud kohtuasju teise liikmesriigi vastu.

2018. aastal on Euroopa Nõukogus 47 lepinguosalist, sealhulgas 28 ELi liikmesriiki. Euroopa Inimõiguste Kohtusse hagi esitaja ei pea olema lepinguosalise riigi kodanik, kuigi väidetavad rikkumised peavad toimuma ühe lepinguosalise jurisdiktsioonis.

Õigus isikuandmete kaitsele kuulub Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õiguse alla; artikliga 8 tagatakse kõigile õigus era- ja perekonnaelu ja kodu ning sõnumite saladuse austamisele ning kehtestatakse selle õiguse piiramise tingimused[15].

Euroopa Inimõiguste Kohus on uurinud palju olukordi, mis on seotud andmekaitse küsimustega. Need on näiteks sõnumisaladuse rikkumine[16], mitmesugused era- ja avaliku sektori poolse jälgimise vormid[17] ning kaitse isikuandmete säilitamise eest riigiasutustes[18]. Õigus eraelu austamisele ei ole absoluutne õigus, sest eraelu puutumatuse õiguse teostamine võib kahjustada muid õigusi, näiteks sõnavabadust ja

13 Vt näiteks EIK, *Klass jt vs. Saksamaa*, nr 5029/71, 6. september 1978; EIK, *Rotaru vs. Rumeenia* [suurkoda], nr 28341/95, 4. mai 2000; EIK, *Szabó ja Vissy vs. Ungari*, nr 37138/14, 12. jaanuar 2016.

14 *Ibid*.

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

16 Vt näiteks EIK, *Malone vs. Ühendkuningriik*, nr 8691/79, 2. august 1984; EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 3. aprill 2007 või EIK, *Mustafa Sezgin Tanrıkulu vs. Türgi*, nr 27473/06, 18. juuli 2017.

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

18 Vt näiteks EIK, *Roman Zakharov vs. Venemaa* [suurkoda], nr 47143/06, 4. detsember 2015; EIK, *Szabó ja Vissy vs. Ungari*, nr 37138/14, 12. jaanuar 2016.

juurdepääsu teabele, ning vastupidi. Seega püüab kohus leida asjaomaste õiguste tasakaalu. Kohus on selgitanud, et peale selle, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 kohustab riike hoiduma kõigist meetmetest, mis võivad konventsiooni kohast õigust rikkuda, on neil teatud tingimustel ka positiivsed kohustused tagada aktiivselt era- ja pereelu tegelik austamine[19]. Asjakohastes peatükkides kirjeldatakse paljusid neid juhtumeid üksikasjalikult.

1.1.4. Euroopa Nõukogu konventsioon nr 108

Infotehnoloogia tekkides 1960. aastatel suurenes ka põhjalikumate eeskirjade vajadus, et kaitsta inimesi nende isikuandmete kaitsmise kaudu. 1970. aastate keskpaigaks võttis Euroopa Nõukogu ministrite komitee vastu mitu resolutsiooni isikuandmete kaitse kohta, viidates Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8[20]. 1981. aastal avati allkirjastamiseks isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (konventsioon nr 108)[21]. See konventsioon oli ja on praegugi andmekaitse valdkonnas ainus rahvusvaheline õiguslikult siduv dokument.

Konventsiooni nr 108 kohaldatakse kogu era- ja avaliku sektori tehtava andmetöötluse suhtes, sealhulgas andmetöötluse suhtes kohtu- ja õiguskaitseasutustes. Sellega kaitstakse isikuid kuritarvitamise eest, mis võib kaasneda isikuandmete töötlemisega, ning ühtlasi on selle eesmärk reguleerida isikuandmete piiriülest liikumist. Isikuandmete töötlemise suhtes käsitlevad konventsioonis sätestatud põhimõtted eelkõige andmete õiglast ja seaduslikku kogumist ning automaatset töötlemist kindlaksmääratud õiguspärastel eesmärkidel. See tähendab, et andmeid ei tohi kasutada nende eesmärkidega sobimatutel eesmärkidel ja andmeid ei tohi säilitada kauem kui vaja. Konventsiooni põhimõtetega reguleeritakse ka andmete kvaliteeti, eelkõige sätestatakse, et andmed peavad olema piisavad ja asjakohased ning andmete hulk ei tohi ületada nende kogumise eesmärgi piire (proportsionaalsus), samuti peavad andmed olema õiged.

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

20 Euroopa Nõukogu ministrite komitee (1973), *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, 26. september 1973; Euroopa Nõukogu ministrite komitee (1974), *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, 20. september 1974.

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

Konventsiooniga nähakse ette isikuandmete töötlemise tagatised ja andmeturbe tagamise kohustused ning teisalt keelatakse nõuetekohaste õiguslike tagatiste puudumisel töödelda delikaatseid andmeid, näiteks rassi, poliitiliste vaadete, tervise, usutunnistuse, seksuaalelu või karistusregistri kannete andmeid.

Samuti on konventsioonis jäädvustatud isiku õigus teada, mis teavet tema kohta säilitatakse, ning õigus lasta seda vajaduse korral parandada. Konventsioonis sätestatud õiguste suhtes saab piiranguid kohaldada ainult siis, kui seda on vaja ülekaalukate huvide tõttu, näiteks riigi julgeoleku või riigikaitse huvides. Konventsiooniga sätestatakse ka isikuandmete vaba liikumine lepinguosaliste vahel ja kehtestatakse andmete liikumise suhtes teatud piirangud, kui õigusraamistikuga ei ole võrdväärset kaitset tagatud.

Konventsioon nr 108 on selle ratifitseerinud riikidele siduv. See ei kuulu Euroopa Inimõiguste Kohtu kohtujärelevalve alla, kuid Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kontekstis on Euroopa Inimõiguste Kohus seda kohtupraktikas arvestanud. Aastate jooksul on kohus otsustanud, et isikuandmete kaitse on eraelu austamise õiguse (artikkel 8) oluline osa, ja on juhindunud selle põhiõiguse riive olemasolu üle otsustamisel konventsiooni nr 108 põhimõtetest[22].

Konventsioonis nr 108 sätestatud üldpõhimõtete ja eeskirjade edasiarendamiseks võttis Euroopa Nõukogu ministrite komitee vastu mitu mittesiduvat soovitust. Need soovitused on mõjutanud andmekaitseõiguse arengut Euroopas. Euroopas oli näiteks aastaid ainus õigusakt, mis reguleerib isikuandmete kasutamist politseivaldkonnas, politseisoovitus[23]. Soovituse põhimõtteid, näiteks andmefailide säilitamise vahendeid ja vajadust rakendada selged eeskirjad isikute kohta, kellel on nendele failidele juurdepääs, arendati edasi ja need kajastuvad ELi hilisemates õigusaktides[24]. Hilisemate soovitustega püütakse lahendada digiajastu probleeme: näiteks seoses andmete töötlemisega töösuhete kontekstis (vt 9. peatükk).

Konventsiooni nr 108 on ratifitseerinud kõik ELi liikmesriigid. 1999. aastal tehti konventsiooni nr 108 muudatusettepanekud, et EL võiks saada konventsiooni osaliseks,

22 Vt näiteks EIK, *Z vs. Soome*, nr 22009/93, 25. veebruar 1997.

23 Euroopa Nõukogu ministrite komitee (1987), *Recommendation Rec(87)15 to Member States regulating the use of personal data in the police sector*, Strasbourg, 17. september 1987.

24 Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT L 281, 23. november 1995.

kuid need ei ole jõustunud[25]. 2001. aastal võeti vastu konventsiooni nr 108 lisaprotokoll. Selles kehtestati sätted andmete piiriülese liikumise kohta mitteosalistele (kolmandatele riikidele) ja riiklike andmekaitse järelevalveasutuste loomise kohta[26].

Konventsioon nr 108 on avatud ühinemiseks Euroopa Nõukogu liikmetele, kes ei ole lepinguosalised. Konventsioonil on avatud olemuse tõttu potentsiaali saada ülemaailmseks standardiks ja seepärast on see alus andmekaitse edendamisel ülemaailmsel tasandil. Praeguseks on konventsiooniga nr 108 ühinenud 51 riiki, sealhulgas kõik Euroopa Nõukogu liikmesriigid (47 riiki); Uruguay, esimene Euroopa-väline riik, kes ühines 2013. aasta augustis, ning Mauritius, Senegal ja Tuneesia, kes ühinesid 2016. ja 2017. aastal.

Hiljuti konventsiooni nüüdisajastati. 2011. aastal korraldatud avalik arutelu kinnitas nüüdisajastamise mõlemat põhieesmärki: eraelu puutumatuse kaitse tugevdamine digitaalvaldkonnas ja konventsiooni järelevalvemehhanismi tugevdamine. Nüüdisajastamisel keskenduti nendele eesmärkidele ja selle lõpus võeti vastu protokoll, millega muudeti konventsiooni nr 108 (protokoll CETS nr 223). See toimus paralleelselt teiste rahvusvaheliste andmekaitse õigusaktide reformidega ja koos 2012. aastal algatatud ELi andmekaitse-eeskirjade reformiga. Euroopa Nõukogu ja ELi tasandi seadusandjad on teinud kõik võimaliku, et tagada mõlema õigusraamistiku järjepidevus ja ühilduvus. Nüüdisajastamisel säilitati konventsiooni üldine ja paindlik olemus ning tugevdati selle potentsiaali universaalse andmekaitse õigusaktina. Kinnitati ja stabiliseeriti olulisi põhimõtteid ning anti üksikisikutele uusi õigusi, ühtlasi suurendades isikuandmete töötlejate vastutust ja tagades suurema vastutusvõime. Näiteks on isikutel, kelle isikuandmeid töödeldakse, õigus saada teavet andmetöötluse põhjuste kohta ja õigus esitada töötlemise kohta vastuväiteid. Veebimaailmas sagenenud profiilianalüüsi tõkestamiseks sätestatakse konventsioonis ka üksikisiku õigus, et tema suhtes ei tehtaks otsust üksnes andmete automaattöötlemise põhjal, arvestamata tema seisukohti. Konventsiooni praktilisel rakendamisel on kesksel kohal andmekaitse-eeskirjade tõhus jõustamine lepinguosaliste sõltumatute järelevalveasutuste poolt. Selleks rõhutatakse nüüdisajastatud konventsioonis vajadus anda järelevalveasutustele tõhusad volitused ja ülesanded ning tagada neile ülesannete täitmisel tõeline sõltumatus.

25 Euroopa Nõukogu, konventsiooni üksikisikute kaitse kohta isikuandmete automaattöötlusel (CETS nr 108) muudatused, mille võttis ministrite komitee vastu 15. juunil 1999 Strasbourgis.

26 Euroopa Nõukogu, isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni lisaprotokoll, mis käsitleb järelevalveasutusi ja andmete piiriülest liikumist, CETS nr 181, 2001. Konventsiooni nr 108 nüüdisajastamise tõttu seda protokolli enam ei kohaldata, sest selle sätteid on ajakohastatud ja need on hõlmatud nüüdisajastatud konventsioonis nr 108.

1.1.5. Euroopa Liidu andmekaitseõigus

ELi õigus koosneb esmastest ja teisestest ELi õigusaktidest. Lepingud – Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu – on ratifitseerinud kõik ELi liikmesriigid; need on esmased ELi õigusaktid. ELi määruseid, direktiive ja otsuseid võtavad nimetatud lepingute alusel vastu selleks volitatud ELi institutsioonid; need on teisesed ELi õigusaktid.

Andmekaitse esmastes ELi õigusaktides

Algsetes Euroopa ühenduste asutamislepingutes ei mainitud inimõigusi ega nende kaitset, sest Euroopa Majandusühendus oli esialgu kavandatud piirkondliku organisatsioonina, mis keskendub majanduse lõimimisele ja ühisturu loomisele. Euroopa ühenduste loomise ja arendamise aluspõhimõte – mis on ka praegu kehtiv – on pädevuse andmise põhimõte. Selle põhimõtte kohaselt tegutseb EL ainult liikmesriikide poolt talle antud pädevuse piires, mida on kajastatud ELi lepingutes. Vastupidiselt Euroopa Nõukogule, ei ole ELi lepingutes selgesõnalist pädevust põhiõiguste küsimustes.

Kuna Euroopa Liidu Kohtusse jõudsid kohtuasjad inimõiguste väidetavate rikkumiste kohta ELi õigusaktide kohaldamisala valdkondades, andis Euroopa Liidu Kohus Euroopa Liidu lepingute olulise tõlgenduse. Isikute kaitsmiseks lisati Euroopa õiguse üldpõhimõtetesse põhiõigused. ELK järgi kajastavad need üldpõhimõtted inimõiguste kaitse sisu riikide põhiseadustes ja inimõiguste lepingutes, eelkõige Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis. Kohus märkis, et ta tagab, et ELi õigusaktid oleksid 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"). Hartas sätestatakse arvukalt Euroopa kodanike kodaniku-, poliitika-, majandus- ja sotsiaalõigusi, ühendades liikmesriikide põhiseaduslikud tavad ja ühised rahvusvahelised kohustused. Harta õigused jagunevad kuude valdkonda: väärikus, vabadused, võrdsus, solidaarsus, kodanike õigused ja õigusemõistmine.

Harta, mis oli algselt ainult poliitiline dokument, muutus õiguslikult siduvaks[27] ELi esmase õigusaktina (vt Euroopa Liidu lepingu artikli 6 lõige 1), kui 1. detsembril 2009

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

jõustus Lissaboni leping[28]. Harta sätted on suunatud ELi institutsioonidele ja asutustele, kohustades neid oma ülesannete täitmisel austama hartas loetletud õigusi. Harta sätted on liikmesriikidele siduvad ka ELi õiguse rakendamisel.

Hartaga tagatakse nii era- ja perekonnaelu austamine (artikkel 7) kui ka kehtestatakse õigus isikuandmete kaitsele (artikkel 8). Hartaga tõstetakse selle kaitse tase selge sõnaga ELi õiguses kehtestatud põhiõiguse tasemele. ELi institutsioonid ja asutused peavad austama ja kaitsma seda õigust, nagu ka liikmesriigid liigu õiguse kohaldamisel (harta artikkel 51). Mitu aastat pärast andmekaitsedirektiivi vastuvõtmist koostatud harta artiklit 8 tuleb käsitada varem kehtestatud ELi andmekaitseõigusaktide tulemina. Peale selle, et artikli 8 lõikes 1 käsitletakse selge sõnaga õigust andmekaitsele, on artikli 8 lõikes 2 kirjeldatud ka peamisi andmekaitsepõhimõtteid. Samuti nõutakse harta artikli 8 lõikes 3, et nende põhimõtete rakendamist kontrolliks sõltumatu asutus.

Lissaboni lepingu vastuvõtmine on andmekaitseõiguse arengus teetähis, sest lisaks harta tõstmisele siduva õigusdokumendi staatusesse esmase õiguse tasandil, kehtestas see ka isikuandmete kaitse õiguse. See õigus on konkreetselt sätestatud Euroopa Liidu toimimise lepingu artiklis 16, mis on osa ELi üldpõhimõtetele pühendatud lepingust. Artiklis 16 luuakse ka uus õiguslik alus, mis annab ELile pädevuse võtta vastu andmekaitse õigusakte. See on oluline areng, sest ELi andmekaitse-eeskirjad – eelkõige andmekaitsedirektiiv – põhinesid esialgu siseturu õiguslikul alusel ja vajadusel ühtlustada riikide õigusakte, et mitte takistada andmete vaba liikumist ELis. Nüüd on Euroopa Liidu toimimise lepingu artiklis 16 sätestatud andmekaitse ELi pädevuse kõik küsimused, sealhulgas kriminaalasjades toimuva politsei- ja õiguskoostööd hõlmava nüüdisaegse tervikliku käsitlusviisi sõltumatu õiguslik alus. Euroopa Liidu toimimise lepingu artiklis 16 kinnitatakse ka, et selle alusel vastu võetud andmekaitse-eeskirjade järgimist peab kontrollima sõltumatu järelevalveasutus. Artikkel 16 oli 2016. aastal andmekaitse-eeskirjade põhjaliku reformi, st isikuandmete kaitse üldmääruse ning politsei- ja kriminaalõigusasutuste andmekaitse direktiivi (vt allpool) vastuvõtmise õiguslik alus.

Isikuandmete kaitse üldmäärus

1995. aastast kuni 2018. aasta maini oli andmekaitse peamine ELi õigusakt Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

28 Vt järgmiste õigusaktide konsolideeritud versioonid: Euroopa ühendused (2012), Euroopa Liidu leping, ELT 2012 C 326, ja Euroopa ühendused (2012), Euroopa Liidu toimimise leping, ELT 2012 C 326.

(andmekaitsedirektiiv)[29]. See võeti vastu 1995. aastal, ajal, mil mitu liikmesriiki oli juba vastu võtnud riikliku andmekaitseseaduse,[30] ja tulenes vajadusest neid seadusi ühtlustada, et tagada kõrgel tasemel kaitse ja isikuandmete vaba liikumine liikmesriikide vahel. Kaupade, kapitali, teenuste ja isikute vaba liikumise võimaldamiseks siseturul oli vaja tagada ka andmete vaba liikumine, mis eeldas, et liikmesriigid saavad kasutada ühtselt kõrget andmekaitsetaset.

Andmekaitsedirektiiv kajastas andmekaitsepõhimõtteid, mis olid olemas juba riigisisestes õigusaktides ja konventsioonis nr 108, laiendades neid sageli. Direktiivis arendati edasi konventsiooni nr 108 artiklis 11 sätestatud võimalust pakkuda muid kaitsemeetmeid. Euroopa andmekaitseõiguse tulemusliku toimimise tagamisele on eriti tõhusalt kaasa aidanud sõltumatu järelevalve kehtestamine direktiivis, et parandada andmekaitse-eeskirjade järgimist. 2001. aastal lisati konventsiooni nr 108 lisaprotokolliga sama põhimõte ka Euroopa Nõukogu õigusesse. See näitab, kuidas mõlemad vahendid on aastate jooksu teineteist vastastikku mõjutanud ja soodustanud.

Andmekaitsedirektiiviga loodi ELis üksikasjalik ja terviklik andmekaitsesüsteem. ELi õigussüsteemi kohaselt ei kohaldata direktiive vahetult ja need tuleb üle võtta liikmesriikide riiklikku õigusse. Paratamatult on liikmesriikidel direktiivi sätete ülevõtmisel kaalutlusõigus. Kuigi direktiiv pidi tagama täieliku ühtlustamise[31] (ja täieliku kaitse), võeti see liikmesriikides üle tegelikult erinevalt. Nii kehtestati kõikjal ELis erinevad andmekaitse-eeskirjad, kusjuures riiklikes õigusaktides tõlgendati mõisteid ja eeskirju erinevalt. Liikmesriigiti erinevad ka jõustamine ja karistused. Infotehnoloogia on alates direktiivi koostamisest 1990. aastate keskel oluliselt muutunud. Kõik need põhjused koos tingisid ELi andmekaitse õigusaktide reformi.

Reformi tulemusena võeti 2016. aasta aprillis pärast aastaid kestnud elavat arutelu vastu isikuandmete kaitse üldmäärus. ELi andmekaitse-eeskirjade ajakohastamise vajaduse arutelud algasid 2009. aastal, kui komisjon algatas isikuandmete kaitse

29 Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT 1995 L 281.

30 Saksamaa Hesseni liidumaa võttis 1970. aastal vastu maailma esimese andmekaitseseaduse, mida kohaldati ainult sellel liidumaal. Rootsi võttis 1973. aastal vastu seaduse *Datalagen*, Saksamaa 1976. aastal seaduse *Bundesdatenschutzgestez* ja Prantsusmaa 1977. aastal seaduse *Loi relatif à l'informatique, aux fichiers et aux libertés*. Ühendkuningriigis võeti 1984. aastal vastu andmekaitseseadus *Data Protection Act*. Madalmaad võtsid 1989. aastal vastu seaduse *Wet Persoonregistraties*.

31 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 29.

põhiõiguse tulevase õigusraamistiku avaliku arutelu. Komisjon avaldas määruse ettepaneku 2012. aasta jaanuaris, algatades Euroopa Parlamendi ja Euroopa Liidu Nõukogu vaheliste läbirääkimiste pika õigusloomeprotsessi. Pärast isikuandmete kaitse üldmääruse vastuvõtmist algas kaheaastane üleminekuperiood. Määrust hakati täielikult kohaldama 25. mail 2018, mil andmekaitsedirektiiv tühistati.

Isikuandmete kaitse üldmääruse vastuvõtmisega 2016. aastal ajakohastati ELi andmekaitse õigusakte, kohandades need digiajastu majandus- ja sotsiaalprobleemide kontekstis põhiõiguste kaitsmiseks. Isikuandmete kaitse üldmääruses säilitatakse andmekaitsedirektiivis sätestatud kesksed põhimõtted ja andmesubjekti õigused ning arendatakse neid edasi. Lisaks kehtestati sellega uued kohustused, mille kohaselt peavad organisatsioonid rakendama lõimitud andmekaitset ja vaikimisi andmekaitset, nimetama teatud asjaoludel ametisse andmekaitseametniku ning järgima uut andmete ülekandmise õigust ja vastutuse põhimõtet. ELi õiguse kohaselt on määrused vahetult kohaldatavad ja riiklikku rakendamist ei ole vaja. Seega sätestatakse isikuandmete kaitse üldmäärusega kogu ELis ühtne andmekaitse-eeskirjade kogum. Sellega kehtestatakse kogu ELis ühtsed andmekaitse-eeskirjad, luues õiguskindla keskkonna, millest ettevõtjad ja üksikisikud saavad andmesubjektidena kasu.

Kuigi isikuandmete kaitse üldmäärus on vahetult kohaldatav, eeldatakse, et liikmesriigid ajakohastavad oma olemasolevaid riiklikke andmekaitseseadusi, et viia need määrusega täielikku vastavusse, kuid kajastades ka kaalutlusruumi põhjenduse 10 erisätete korral. Määruses sätestatud põhieeskirjad ja põhimõtted ning üksikisikutele antud tugevad õigused moodustavad suure osa käsiraamatust ja on esitatud järgmistes peatükkides. Määruses on terviklikud eeskirjad territoriaalse kohaldamisala kohta. Seda kohaldatakse nii ELis asuvate ettevõtete suhtes kui ka väljaspool ELi asuvate vastutavate töötlejate või volitatud töötlejate suhtes, kes pakuvad kaupu või teenuseid andmesubjektidele ELis või jälgivad nende käitumist. Et mitmel välistehnoloogiaettevõttel on Euroopa turul oluline osa ja miljoneid ELi kliente, on ELi andmekaitse-eeskirjade kohaldamine nende organisatsioonide suhtes oluline, et tagada üksikisikute kaitse ja võrdsed võimalused.

Andmekaitse õiguskaitse valdkonnas – direktiiv (EL) 2016/680

Kehtetuks tunnistatud andmekaitsedirektiivis sätestati terviklik andmekaitsekord, mida on tõhustatud isikuandmete kaitse üldmääruse vastuvõtmisega. Kuigi kehtetuks tunnistatud andmekaitsedirektiiv oli terviklik, piirdus selle kohaldamisala tegevusega siseturul ning muude ametiasutuste kui õiguskaitseasutuste tegevusega. Seega oli vaja võtta vastu eraldi õigusakte, et saavutada andmekaitse ja muude

õigustatud huvide vajalik selgus ja tasakaal ning reageerida probleemidele, mis on teatud valdkondades eriti teravad. Üks näide on õiguskaitseasutustes isikuandmete töötlemist reguleerivad eeskirjad.

Esimene ELi õigusakt selle küsimuse reguleerimiseks oli nõukogu raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta. Selle eeskirju kohaldati ainult politsei- ja õigusvaldkonna andmete suhtes liikmesriikidevahelise andmevahetuse korral. Riigisisene isikuandmete töötlemine õiguskaitseasutustes jäeti selle kohaldamisalast välja.

Selle olukorra parandas direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist[32] (politsei- ja kriminaalõigusasutuste andmekaitse direktiiv). Direktiiv võeti vastu paralleelselt isikuandmete kaitse üldmäärusega ning sellega tunnistati kehtetuks raamotsus 2008/977/JSK ja kehtestati õiguskaitse kontekstis terviklik isikuandmete kaitse süsteem, tunnistades ühtlasi avaliku julgeolekuga seotud andmetöötluse eripära. Kuigi isikuandmete kaitse üldmääruses sätestatakse üldeeskirjad üksikisikute kaitseks nende isikuandmete töötlemisel ning selliste andmete vaba liikumise tagamiseks ELis, sätestatakse direktiivis andmekaitse erieeskirjad kriminaalasjades tehtava õiguskoostöö ja politseikoostöö valdkonnas. Kui pädev asutus töötleb isikuandmeid kuritegude ennetamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks, kohaldatakse direktiivi (EL) 2016/680. Kui pädevad asutused töötlevad isikuandmeid muudel kui eespool nimetatud eesmärkidel, kohaldatakse isikuandmete kaitse üldmääruse kohast üldist korda. Teisiti kui varasem õigusakt (nõukogu raamotsus 2008/977/JSK), laieneb direktiivi (EL) 2016/680 kohaldamisala isikuandmete riigisisesele töötlemisele õiguskaitseasutuste poolt ning see ei piirdu selliste andmete vahetamisega liikmesriikide vahel. Lisaks püütakse direktiiviga saavutada üksikisikute õiguste ja julgeolekuga seotud töötlemise õiguspäraste eesmärkide tasakaal.

Selleks kinnitatakse direktiivis õigust isikuandmete kaitsele ja keskseid põhimõtteid, mis peaksid hõlmama andmetöötlust, järgides hoolikalt isikuandmete kaitse

32 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist, ELT L 119, 4. mai 2016.

üldmääruses sätestatud eeskirju ja põhimõtteid. Üksikisikute õigused ja vastutavate töötlejate kohustused – näiteks seoses andmeturbe, lõimitud ja vaikimisi andmekaitse ning andmetega seotud rikkumisest teatamisega – sarnanevad isikuandmete kaitse üldmääruses sätestatud õiguste ja kohustustega. Direktiivis arvestatakse ja püütakse lahendada suuri tekkivaid tehnikaprobleeme, mis võivad eriti raskelt koormata üksikisikuid, näiteks profiilianalüüsi meetodite kasutamine õiguskaitseasutustes. Põhimõtteliselt tuleb keelata otsused, mis põhinevad üksnes isikuandmete automaattöötlemisel, sealhulgas profiilianalüüsil[33]. Lisaks sellele ei tohi otsused põhineda delikaatsetel andmetel. Selliste põhimõtete suhtes kohaldatakse direktiivis sätestatud teatud erandeid. Lisaks ei tohi selline töötlemine põhjustada ühegi inimese diskrimineerimist[34].

Direktiiv sisaldab ka eeskirju vastutavate töötlejate vastutuse tagamiseks. Nad peavad määrama andmekaitseametniku, kes jälgib andmekaitse-eeskirjade järgimist, teavitab ja nõustab oma kohustusi täitvat üksust ja töötajaid ning teeb koostööd järelevalveasutusega. Isikuandmete töötlemine politsei- ja kriminaalõigussektoris kuulub nüüd sõltumatute järelevalveasutuste järelevalve alla. Nii üldine andmekaitse õiguskord kui ka õiguskaitse- ja kriminaalasjade andmekaitse erikord peavad samuti vastama ELi põhiõiguste harta nõuetele.

Erikorda, mis kehtestati andmete töötlemiseks politsei- ja õigusalase koostöö raames politsei- ja kriminaalõigusasutuste andmekaitse direktiivis, kirjeldatakse üksikasjalikult 8. peatükis.

Eraelu puutumatuse ja elektroonilise side direktiiv

Konkreetsete andmekaitse-eeskirjade kehtestamist peeti vajalikuks ka elektroonilise side sektoris. Arvestades interneti, laua- ja mobiiltelefonside arengut, oli oluline tagada, et austatakse kasutajate õigust eraelu puutumatusele ja konfidentsiaalsusele. Direktiivis 2002/58/EÜ,[35] milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatuse ja elektroonilise side direktiiv ehk e-privaatsuse direktiiv), sätestatakse eeskirjad isikuandmete kaitse kohta nendes võrkudes ning eeskirjad isikuandmetega seotud rikkumistest teatamise ning side konfidentsiaalsuse kohta.

33 Politsei- ja kriminaalõigusasutuste andmekaitse direktiivi artikli 11 lõige 1.

34 *Ibid.*, artikli 11 lõiked 2 ja 3.

35 Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ELT 2002 L 201 (eraelu puutumatuse ja elektroonilise side direktiiv ehk e-privaatsuse direktiiv).

Seoses turvalisusega peavad elektrooniliste sideteenuste osutajad muu hulgas tagama, et juurdepääs isikuandmetele antakse ainult volitatud isikutele, ja võtma meetmeid, et vältida isikuandmete hävitamist, kadumist või kogemata kahjustamist[36]. Üldkasutatava sidevõrgu turvalisuse rikkumise erilise riski korral peavad operaatorid abonente sellest teavitama[37]. Kui vaatamata võetud turvameetmetele rikutakse turvalisust, peavad operaatorid teavitama isikuandmetega seotud rikkumisest riiklikku pädevat asutust, kellele on antud ülesandeks direktiivi rakendamine ja selle täitmise tagamine. Mõnikord peavad operaatorid teavitama isikuandmetega seotud rikkumisest ka üksikisikuid, nimelt kui rikkumine mõjutab tõenäoliselt nende isikuandmeid või eraelu puutumatust[38]. Side konfidentsiaalsus eeldab, et side ja metaandmete kuulamine, salaja pealt kuulamine, säilitamine või muu jälgimine või pealtkuulamine on põhimõtteliselt keelatud. Direktiiviga keelatakse ka pealesunnitud teave (rämpspost), v.a kui kasutajad on andnud nõusoleku, ning hõlmab arvutites ja seadmetes küpsiste säilitamise eeskirju. Need peamised negatiivsed kohustused näitavad selgelt, et side konfidentsiaalsus on olulisel määral seotud harta artiklis 7 sätestatud õigusega eraelu austamisele ja harta artiklis 8 sätestatud õigusega isikuandmete kaitsele.

2017. aasta jaanuaris avaldas komisjon ettepaneku võtta vastu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side valdkonnas, mis pidi kava kohaselt asendama e-privaatsuse direktiivi. Reformi eesmärk on viia elektroonilist sidet reguleerivad eeskirjad vastavusse isikuandmete kaitse üldmääruses kehtestatud uue andmekaitsekorraga. Uut määrust hakatakse vahetult kohaldama kogu ELis; kõik üksikisikud saavad oma elektroonilise side kaitse samal tasemel, samas kui sidevõrgu operaatorid ja ettevõtted saavad selguse, õiguskindluse ja kogu ELi hõlmava ühtse eeskirjade kogumi. Kavandatud eeskirjad elektroonilise side konfidentsiaalsuse kohta kehtivad ka uute osalejate suhtes, kes pakuvad e-privaatsuse direktiivis hõlmamata elektroonilisi sideteenuseid. E-privaatsuse direktiiv hõlmas ainult tavapäraste sideteenuste osutajaid. Arvestades selliste teenuste nagu Skype, WhatsApp, Facebook, Messenger ja Viber massilist kasutamist sõnumsides või helistamisel, kuuluvad need OTT- ehk voogedastusteenused nüüd määruse kohaldamisalasse ja peavad täitma selle andmekaitse-, privaatsus- ja turvalisuse nõudeid. Käesoleva käsiraamatu avaldamise ajal e-privaatsuse eeskirjade õigusloomeprotsess alles kestis.

36 Eraelu puutumatuse ja elektroonilise side direktiivi artikli 4 lõige 1.

37 *Ibid*., artikli 4 lõige 2.

38 *Ibid*., artikli 4 lõige 3.

Määrus (EÜ) nr 45/2001

Et andmekaitsedirektiivi sai kohaldada üksnes ELi liikmesriikide suhtes, tekkis vajadus täiendava õigusakti järele, et tagada andmekaitse isikuandmete töötlemisel ELi institutsioonides ja asutustes. Selle ülesande täidab määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (ELi institutsioonide andmekaitse määrus)[39].

Määruses (EÜ) nr 45/2001 järgitakse hoolikalt ELi üldise andmekaitsekorra põhimõtteid ning kohaldatakse neid andmetöötluse suhtes, mida ELi institutsioonid ja asutused teevad oma ülesannete täitmisel. Lisaks luuakse määrusega selle sätete kohaldamise jälgimiseks sõltumatu järelevalveasutus – Euroopa Andmekaitseinspektor. Euroopa andmekaitseinspektoril on järelevalvevolitused ja kohustus jälgida isikuandmete töötlemist ELi institutsioonides ja asutustes ning kuulata ja uurida kaebusi andmekaitse-eeskirjade väidetavate rikkumiste kohta. Ka annab Euroopa andmekaitseinspektor ELi institutsioonidele ja asutustele nõu kõigis isikuandmete kaitse küsimustes, alates uute õigusaktide ettepanekutest kuni andmetöötluse sise-eeskirjade koostamiseni.

2017. aasta jaanuaris esitas Euroopa Komisjon ettepaneku võtta vastu uus määrus, milles käsitletakse andmete töötlemist ELi institutsioonides ja millega tunnistatakse kehtetuks praegune määrus. Nii nagu e-privaatsuse direktiivi reformiga, ajakohastatakse ja ühtlustatakse ka määruse (EÜ) nr 45/2001 reformiga selle eeskirju isikuandmete kaitse üldmääruse kohase uue andmekaitsekorraga.

Euroopa Liidu Kohtu roll

Euroopa Liidu Kohus on pädev otsustama, kas liikmesriik on täitnud ELi andmekaitseõigusaktidest tulenevaid kohustusi, ja tõlgendama ELi õigusakte, et tagada nende mõjus ja ühtne kohaldamine kõigis liikmesriikides. Alates andmekaitsedirektiivi vastuvõtmisest 1995. aastal on kogunenud suur kogus kohtupraktikat, mis selgitab andmekaitsepõhimõtete ulatust ja tähendust ning põhiõigust isikuandmete kaitsele, nagu on harta artiklis 8 sätestatud. Kuigi direktiiv on kehtetuks tunnistatud ja jõustunud on uus õigusakt – isikuandmete kaitse üldmäärus–, on varasem kohtupraktika ELi andmekaitsepõhimõtete tõlgendamisel ja kohaldamisel endiselt kehtiv,

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

sest andmekaitsedirektiivi kesksed põhimõtted ja mõisted on säilitati isikuandmete kaitse üldmääruses.

1.2. Isikuandmete kaitse õiguse piirangud

Põhipunktid

- Õigus isikuandmete kaitsele ei ole absoluutne õigus; seda võidakse vajaduse korral piirata üldhuvi eesmärgil või teiste isikute õiguste ja vabaduste kaitsmiseks.
- Eraelu puutumatuse ja isikuandmete kaitse õiguste piiramise tingimused on loetletud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 ja harta artikli 52 lõikes 1. Need on välja töötatud ja tõlgendatud Euroopa Inimõiguste Kohtu ja Euroopa Liidu Kohtu praktikas.
- Euroopa Nõukogu andmekaitseõiguse kohaselt on isikuandmete töötlemine eraelu puutumatuse õiguse õiguspärane riive ja see võib toimuda üksnes juhul, kui
  - see on kooskõlas õigusaktidega;
  - see täidab õiguspärast eesmärki;
  - arvestatakse põhiõiguste ja -vabaduste põhiolemust;
  - see on demokraatlikus ühiskonnas õiguspärase eesmärgi saavutamiseks vajalik ja proportsionaalne.
- ELi õiguskorras seatakse hartaga kaitstud põhiõiguste teostamise piirangutele sarnased tingimused. Mis tahes põhiõiguse, sealhulgas isikuandmete kaitse piiramine võib olla seaduslik ainult siis, kui
  - see on kooskõlas õigusaktidega;
  - arvestatakse asjaomase õiguse olemust;
  - kohaldatakse proportsionaalsuse põhimõtet, see on vajalik ja
  - taotletakse ELi tunnustatud üldist huvi pakkuvaid eesmärke või on vajadus kaitsta teiste isikute õigusi ja vabadusi.

Harta artikli 8 kohane põhiõigus isikuandmete kaitsele ei ole absoluutne õigus, „vaid sellega tuleb arvestada vastavalt selle ülesandele ühiskonnas“[40]. Harta artikli 52 lõikes 1 tunnustatakse seega, et õiguste, näiteks harta artiklites 7 ja 8 sätestatud õiguste teostamist võib piirata, kui piirangud on ette nähtud õigusaktidega, need arvestavad nimetatud õiguste ja vabaduste olemust ning need on proportsionaalsuse põhimõtte kohaselt vajalikud ja vastavad tegelikult ELis tunnustatud üldist huvi pakkuvatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi[41]. Samamoodi on andmekaitse artikliga 8 tagatud ka Euroopa inimõiguste ja põhivabaduste kaitse süsteemis ja selle õiguse kasutamist võib vajaduse korral piirata, kui seda on vaja õiguspärase eesmärgi saavutamiseks. Siin jaotises käsitletakse sekkumise tingimusi Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni kohaselt, nagu on tõlgendatud Euroopa Inimõiguste Kohtu praktikas, ning harta artiklis 52 sätestatud seaduslike piirangute tingimusi.

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

Isikuandmete töötlemine võib olla sekkumine andmesubjekti õigusse eraelu puutumatuse kaitsele, mida kaitseb Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8[42]. Nagu selgitatud eespool (vt punkt 1.1.1 ja punkt 1.1.4), ei kinnitata Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis erinevalt ELi õiguskorrast isikuandmete kaitset kui eraldi põhiõigust. Pigem on isikuandmete kaitse osa õigustest, mida kaitseb õigus eraelu puutumatuse austamisele. Seega ei kuulu iga isikuandmete töötlemist hõlmav toiming Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaldamisalasse. Artikli 8 käivitamiseks tuleb kõigepealt leida, kas ohus on isiklik huvi või isiku eraelu. Euroopa Inimõiguste Kohus on käsitlenud oma praktikas mõistet „eraelu“ laia kontseptsioonina, mis hõlmab ka tööelu ja avaliku käitumise aspekte. Samuti on Euroopa Inimõiguste Kohus otsustanud, et isikuandmete kaitse on eraelu austamise õiguse oluline osa. Kuigi eraelu tõlgendus on lai, kõik andmetöötluse liigid ei ohustaks iseenesest artikli 8 alusel kaitstud õigusi.

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

41 *Ibid.*, punkt 50.

42 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 8. detsember 2008, punkt 67.

Kui Euroopa Inimõiguste Kohus leiab, et töötlemistoiming mõjutab üksikisikute õigust eraelu austamisele, uurib ta, kas sekkumine on õigustatud. Õigus eraelu austamisele ei ole absoluutne õigus, vaid seda tuleb tasakaalustada ja kooskõlastada muude õigustatud huvide ja õigustega, kas siis teiste inimeste huvidega (erahuvid) või kogu ühiskonna huvidega (avalikud huvid).

Kumulatiivsed tingimused, mille alusel võib sekkumine olla põhjendatud, on järgmised.

Kooskõla seadusega

Euroopa Inimõiguste Kohtu kohtupraktika järgi on sekkumine kooskõlas seadusega, kui see põhineb teatud tingimustele vastaval riigisisesel õigussättel. Õigusnorm peab olema „asjaomastele isikutele juurdepääsetav ja selle mõju peaks olema eeldatav“[43]. Eeskiri on eeldatav, „kui see on piisavalt täpselt sõnastatud ja võimaldab igal isikul – vajaduse korral asjakohase abiga – oma käitumist kohandada“[44]. Lisaks „oleneb õigusnormi nõutav täpsuse aste selles seoses konkreetsest reguleerimisesemest“[45].

Näited: kohtuasjas *Rotaru vs. Rumeenia*[46] väitis kaebuse esitaja, et tema õigust eraelu puutumatusele on rikutud, sest Rumeenia salateenistus hoidis ja kasutas tema isikuandmeid sisaldavat faili. EIK leidis, et kuigi riigi õigusaktid lubavad salajastesse failidesse koguda, neis talletada ja arhiivida andmeid, mis mõjutavad riigi julgeolekut, ei ole õigusaktides sätestatud nende volituste kasutamise piiranguid, mis jäid ametiasutuste otsustada. Riigi õigusaktides ei olnud näiteks määratletud, mis liiki teavet tohib töödelda, mis kategooriatesse kuuluvate isikute suhtes ja mis tingimustes tohib võtta

43 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 ja EIK, *Iordachi jt vs. Moldova*, nr 25198/02, 10. veebruar 2009, punkt 50.

44 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.

45 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.

46 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.

jälitusmeetmeid või mis menetlust tuleb järgida. Kohus järeldas seega, et riigi õigusaktid ei olnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 alusel kooskõlas eeldatavuse nõudega ning tegu oli selle artikli rikkumisega.

Kohtuasjas *Taylor-Sabori vs. Ühendkuningriik*[47] oli kaebuse esitaja suhtes toimunud politseijärelevalve. Kaebuse esitaja piiparisse paigaldatud klooni abil sai politsei jälgida talle saadetud sõnumeid. Seejärel kaebuse esitaja vahistati ja talle esitati süüdistus kontrollialuse uimastiga kaubitsemise vandenõus. Prokurör lähtus süüdistuse esitamisel muu hulgas jälgimise ajal tehtud kirjalikest märkmetest politsei transkribeeritud piiparisõnumite põhjal. Kaebuse esitaja kohtuprotsessi ajal puudus Briti õiguses siiski säte, mis oleks reguleerinud eraõigusliku sidesüsteemi kaudu edastatavate sõnumite pealtkuulamist. Seega ei olnud sekkumine kaebuse esitaja õigustesse kooskõlas seadusega. EIK järeldas, et sellega rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Kohtuasi *Vukota-Bojić vs. Šveits*[48] käsitles sotsiaalkindlustuse taotleja salajast jälgimist eradetektiividega, kelle oli tellinud taotleja kindlustusandja. EIK leidis, et kuigi kaebuses käsitletava järelevalvemeetme tellis eraõiguslik kindlustusandja, oli riik andnud kindlustusandjale õiguse pakkuda kohustuslikust ravikindlustusest tulenevaid hüvitisi ja koguda kindlustusmakseid. Konventsiooni kohaselt ei saa riik end ise vastutusest vabastada, delegeerides oma kohustused eraõiguslikele asutustele või isikutele. Riigi õigusaktid pidid tagama, et piisavad kaitsemeetmed Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õigustesse sekkumise kuritarvitamise vastu on „kooskõlas seadusega". Kohtuasjas järeldas EIK, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8 on rikutud, sest riigi õigusaktides ei olnud piisavalt selgelt määratletud kindlustusvaidlustes avaliku sektori asutustena tegutsevatele kindlustusandjatele antud kaalutlusõiguse ulatust ja teostamise viisi kindlustatud isiku salajase jälgimise läbiviimiseks. Eelkõige ei hõlmanud need piisavaid kaitsemeetmeid kuritarvitamise vastu.

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

48 EIK, *Vukota-Bojić vs. Šveits*, nr 61838/10, 18. oktoober 2016, punkt 77.

Õiguspärane eesmärk

Õiguspärane eesmärk võib olla kas mõni nimetatud avalikest huvidest või teiste isikute õiguste ja vabaduste kaitsmine. Õiguspärased eesmärgid, mis võivad sekkumist põhjendada, on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 järgi riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvid, korratuse või kuriteo ärahoidmine, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitse.

Näide: kohtuasi *Peck vs. Ühendkuningriik*[49] käsitles seda, kuidas kaebuse esitaja tegi tänaval veene läbi lõigates suitsiidikatse, teadmata, et teda jälgis valvekaamera. Valvekaameraid jälginud politsei päästis ta ja edastas seejärel videosalvestise meediale, kus see avaldati ilma kaebuse esitaja nägu varjamata. EIK leidis, et ametiasutustel ei olnud asjakohaseid või piisavaid põhjusi, mis oleksid õigustanud salvestise otsest avaldamist avalikkusele ilma kaebuse esitaja nõusolekuta või tema isikusamasust varjamata. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Vajalikkus demokraatlikus ühiskonnas

Euroopa Inimõiguste Kohtu järgi viitab vajalikkuse mõiste, et sekkumine vastab tungivale sotsiaalsele vajadusele ja on eelkõige proportsionaalne õiguspärase eesmärgiga[50]. Hinnates, kas meede on tungiva sotsiaalse vajaduse rahuldamiseks vajalik, uurib EIK selle asjakohasust ja sobivust taotletava eesmärgi suhtes. Selleks võib ta kaalutleda, kas sekkumisega üritatakse lahendada probleemi, mis võib lahendamata jätmise korral kahjustada ühiskonda, kas on tõendeid, et sekkumine võib sellist kahjulikku mõju leevendada, ja mis on laiemad ühiskondlikud hoiakud probleemi suhtes[51]. Kui julgeolekuteenistused näiteks koguksid ja säilitaksid selliste konkreetsete isikute isikuandmeid, kellel on tuvastatud seos terroristlike liikumistega, oleks see sekkumine isikute õigusesse eraelu austamisele, mis täidab siiski olulist ja tungivat sotsiaalset vajadust: riigi julgeolek ja võitlus terrorismi vastu. Vajalikkuse tõestamiseks peab sekkumine olema ka proportsionaalne. EIK praktikas hinnatakse

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

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

51 Artikli 29 töörühm (2014), *Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, Brüssel, 27. veebruar 2014, lk 7–8.

proportsionaalsust vajalikkuse mõiste raames. Proportsionaalsus eeldab, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga kaitstud õiguste riive ei ületa seda, mida on vaja õiguspärase eesmärgi saavutamiseks. Proportsionaalsuse hindamisel arvestatavad olulised tegurid on sekkumise ulatus, eelkõige mõjutatud isikute arv, ning selle ulatuse või üksikisikute õigustele avalduva kahjuliku mõju piiramiseks on kehtestatud kaitsemeetmed või tingimused[52].

Näide: kohtuasi *Khelili vs. Šveits*[53] käsitles juhtumit, kus politsei leidis kontrollimisel, et kaebuse esitajal olid kaasas järgmise tekstiga visiitkaardid: „Meeldiv ja kena kolmekümnendate eluaastate teises pooles olev naine soovib kohtuda mehega, et võtta koos klaasike või mõnikord välja minna. Telefon […].“ Kaebuse esitaja väitis, et pärast visiitkaartide leidmist sisestati ta andmebaasi prostituudina, kelleks olemist ta järjepidevalt eitas. Kaebuse esitaja nõudis, et tema kandest politsei andmebaasis kustutataks sõna „prostituut“. EIK tunnistas põhimõtteliselt, et üksikisiku isikuandmete säilitamine põhjusel, et ta võib sooritada uue kuriteo, võib teatud tingimustes olla proportsionaalne. Kaebuse esitaja juhtumis näis ebaseadusliku prostitutsiooni väide siiski liiga ebamäärane ja üldsõnaline ning selle tõendamiseks ei esitatud kindlaid fakte, sest teda ei olnud kunagi ebaseaduslikus prostitutsioonis süüdi mõistetud, seega ei saanud sekkumine vastata tungivale sotsiaalsele vajadusele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses. Kuivõrd ametiasutuste ülesanne oli tõendada kaebuse esitaja kohta talletatud andmete õigsust ja tema õigustesse sekkumise raskust, otsustas kohus, et demokraatlikus ühiskonnas ei olnud vaja 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: kohtuasi *S. ja Marper vs. Ühendkuningriik*[54] käsitles juhtumit, kus kaebuse mõlemad esitajad vahistati ja neile esitati kuriteosüüdistused. Politsei võttis nende sõrmejäljed ja DNA-proovid politsei- ja kriminaaltõendite seaduse kohaselt. Kaebuse esitajaid ei ole kuritegude eest kunagi süüdi mõistetud: üks mõisteti kohtus õigeks ja teise vastu algatatud kriminaalmenetlus lõpetati. Politsei hoidis siiski alles nende sõrmejäljed, DNA-profiilid ja rakuproovid ning säilitas neid andmeid politsei andmebaasis; riiklike

52 *Ibid.*, lk 9–11.

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

54 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 4. detsember 2008.

õigusaktide kohaselt võis neid säilitada alaliselt. Kuigi Ühendkuningriik väitis, et säilitamine aitas tuvastada tulevasi õigusrikkujaid ja seega järgiti kuritegude ennetamise ja avastamise õiguspärast eesmärki, leidis EIK, et taotlejate eraelu austamise õiguse riive oli põhjendamatu. Kohus tuletas meelde, et andmekaitse kesksed põhimõtted nõuavad, et isikuandmete säilitamine oleks kogumise eesmärgi suhtes proportsionaalne ja säilitamise aeg peab olema piiratud. Kohus oli nõus, et andmebaasi laiendamine nii, et see hõlmab nii süüdimõistetute kui ka kõigi kahtlustatavate, kuid süüdi mõistmata isikute DNA-profiile, võis aidata kaasa kuritegevuse avastamisele ja ennetamisele Ühendkuningriigis. Samas hämmastas kohut „säilitamisvolituste üldine ja valimatu olemus"[55].

Arvestades rakuproovides sisalduvat geneetilist ja terviseteavet, oli kaebuse esitajate eraelu õiguse riive eriti tugev. Sõrmejälgi ja proove võidakse võtta vahistatutelt ning neid hoitakse alaliselt politsei andmebaasis, olenemata süüteo olemusest ja raskusest, ning isegi väikeste süütegude korral, mis ei ole karistatavad vangistusega. Pealegi olid õigeks mõistetud isikute võimalused oma andmed andmebaasist eemaldada piiratud. EIK pööras erilist tähelepanu asjaolule, et üks kaebuse esitaja oli vahistamisel 11-aastane. Süüdi mõistmata alaealise isikuandmete säilitamine võib olla eriti kahjulik, arvestades tema haavatavust ja arengut ning ühiskonda lõimumise tähtsust[56]. Kohus otsustas ühehäälselt, et säilitamine oli ebaproportsionaalne sekkumine kaebuse esitajate õigusesse eraelu austamisele ning seda ei saa pidada demokraatlikus ühiskonnas vajalikuks.

Näide: kohtuasjas *Leander vs. Rootsi*[57] otsustas EIK, et riigi julgeoleku seisukohast olulistele ametikohtadele kandideerijate salajane jälgimine ei ole demokraatlikus ühiskonnas vajalikkuse nõudega iseenesest vastuolus. Lähtudes Rootsi õigusaktides andmesubjektide huvide kaitse erimeetmetest – näiteks kontroll parlamendi ja õiguskantsleri tasandil –, järeldas EIK, et Rootsi personalikontrolli süsteem vastas artikli 8 lõike 2 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.

55 *Ibid.*, punkt 119.

56 *Ibid.*, punkt 124.

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

1.2.2. ELi põhiõiguste harta kohaste õiguspäraste piirangute tingimused

Põhiõiguste harta on liigendatud ja sõnastatud teisiti kui Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Hartas ei kasutata tagatud õigustesse sekkumise mõistet, vaid selles on hartaga tunnustatud õiguste ja vabaduste teostamise piiramise säte.

Artikli 52 lõike 1 kohaselt tohib hartaga tunnustatud õiguste ja vabaduste teostamist ning sellest tulenevalt isikuandmete kaitse õiguse teostamist piirata üksnes siis, kui

- see on kooskõlas seadusega;
- selle korral arvestatakse isikuandmete kaitse õiguse olemust;
- kohaldatakse proportsionaalsuse põhimõtet, see on vajalik[58] ja
- see vastab liidu tasandil tunnustatud avalikku huvi pakkuvatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi.

Et isikuandmete kaitse on Euroopa Liidu õiguskorras eraldi ja iseseisev põhiõigus, mida kaitstakse harta artikli 8 alusel, on isikuandmete töötlemine iseenesest sellesse õigusesse sekkumine. Ei ole oluline, kas isikuandmed on seotud isiku eraeluga, on delikaatsed või kas andmesubjektele on tekitatud mis tahes ebamugavust. Et sekkumine oleks õiguspärane, peab see vastama kõigile harta artikli 52 lõikes 1 loetletud tingimustele.

Seaduses ette nähtud

Isikuandmete kaitse õiguse piirangud peavad olema sätestatud seaduses. See nõue tähendab, et piirangud peavad põhinema õiguslikul alusel, mis on piisavalt juurdepääsetav ja eeldatav ning sõnastatud piisavalt täpselt, et isikud mõistaksid oma kohustusi ja kohandaksid käitumist. Õiguslikus aluses tuleb selgelt määratleda ka pädevate asutuste volituste kasutamise ulatus ja viis, et kaitsta isikuid meelevaldse sekkumise eest. See tõlgendus sarnaneb EIK praktika kohase „õiguspärase

58 Isikuandmete kaitse põhiõigust piiravate meetmete vajalikkuse hindamine: vt Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11. aprill 2017.

sekkumise“ nõudega[59] ning on väidetud, et hartas kasutatud väljendi „seaduses ette nähtud“ tähendus peaks olema sama, mis on sellele antud seoses Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga[60]. EIK praktika ja eriti mõiste „seaduses ette nähtud“, mille ta on aastate jooksul välja töötanud, on oluline kaalutlus, mida Euroopa Liidu Kohus peab arvestama harta artikli 52 lõike 1 kohaldamisala tõlgendamisel[61].

Õiguse põhisisu arvestamine

ELi õiguskorras tuleb harta alusel kaitstud põhiõiguste piiramisel arvestada nende õiguste olemust. See tähendab, et piirangud, mis on nii ulatuslikud ja sekkuvad, et need kaotavad põhiõiguse põhisisu, ei ole põhjendatud. Kui kahjustatakse õiguse olemust, tuleb piirangut pidada ebaseaduslikuks, ilma et oleks vaja edasi hinnata, kas see teenib üldist huvi ning vastab vajalikkuse ja proportsionaalsuse kriteeriumidele.

Näide: kohtuasi *Schrems*[62] käsitles üksikisikute kaitset seoses nende isikuandmete edastamisega kolmandatele riikidele – sel konkreetsel juhul Ameerika Ühendriikidele. Austria kodanik Schrems, kes oli olnud mitu aastat Facebooki kasutaja, esitas Iirimaa andmekaitse järelevalveasutusele kaebuse, milles teatas oma isikuandmete edastamisest Facebooki Iiri tütarettevõtjalt Facebook Inc.-le ja USAs asuvatesse serveritesse, kus neid töödeldi. Ta väitis, et arvestades USAst pärit rikkumisest teataja Edward Snowdeni 2013. aasta paljastusi USA luureteenistuste jälgimistegevuse kohta, ei paku USA õigus ja tava USA territooriumile edastatud isikuandmetele piisavat kaitset. Snowden oli avalikustanud, et riiklikul julgeolekuagentuuril oli otseühendus ettevõtete, näiteks Facebooki serveritega, ning see sai lugeda vestluste ja erasõnumite sisu.

59 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11 aprill 2017, lk 4; vt ka ELK, *Euroopa Liidu Kohtu (suurkoda) arvamus 1/15*, 26. juuli 2017.

60 ELK, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen* ja *Secretary of State for the Home Department vs. Tom Watson, Peter Brice, Geoffrey Lewis*, *kohtujuristi ettepanek, Henrik Saugmandsgaard Øe,* esitatud 19 juulil 2016, punkt 140.

61 ELK, C-70/10, *Scarlet Extended SA vs. Société belge des auteurs compositeurs et éditeurs (SABAM)*, kohtujuristi ettepanek, Pedro Cruz Villalón, esitatud 14. aprillil 2011, punkt 100.

62 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

Andmete edastamine USA-le põhines 2000. aastal vastu võetud komisjoni otsusel piisava kaitse kohta, millega lubati edastada andmeid nendele USA ettevõtjatele, kes ise kinnitavad, et nad kaitsevad EList edastatud isikuandmeid ja järgivad programmi Safe Harbor põhimõtteid. Euroopa Liidu Kohus uuris komisjoni otsuse kehtivust harta seisukohalt. Kohus tuletas meelde, et põhiõiguste kaitse ELis eeldab, et nende õiguste erandeid ja piiranguid kohaldatakse üksnes rangelt vajalikus ulatuses. Kohus leidis, et õigusakt, mis võimaldab ametiasutustel elektroonilise side sisuga üldiselt tutvuda, on „harta artikliga 7 tagatud eraelu puutumatuse põhiõiguse põhisisu kahjustav". See õigus muutuks mõttetuks, kui USA ametiasutustel oleks volitus tutvuda teabevahetusega oma äranägemisel, ilma konkreetsete objektiivsete põhjendusteta, mis põhineksid riigi julgeoleku või kuriteo takistamise konkreetsetel kaalutlustel seoses asjaomase isikuga, ja ilma et nimetatud jälgimistavadega kaasneksid asjakohased kaitsemeetmed võimu kuritarvitamise vastu.

Peale selle märkis kohus, et „õigusakt, milles ei ole andmesubjektile ette nähtud mingit võimalust kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada", ei järgi põhiõigust tõhusale kohtulikule kaitsele (harta artikkel 47). Seega ei taganud programmi Safe Harbor käsitlev otsus USA poolt põhiõiguste kaitse taset, mis on põhimõtteliselt samaväärne ELis direktiivi kohaselt koostoimes põhiõiguste hartaga tagatud kaitsega. Seega tühistas Euroopa Liidu Kohus otsuse[63].

Näide: kohtuasjas *Digital Rights Ireland*[64] uuris Euroopa Liidu Kohus direktiivi 2006/24/EÜ (andmete säilitamise direktiiv) vastavust harta artiklitele 7 ja 8. Direktiiv kohustas elektroonilise side teenuste osutajaid säilitama andmeliiklus- ja asukohaandmeid vähemalt 6 ja kuni 24 kuud ning võimaldama riiklikel pädevatel asutustel nende andmetega tutvuda raskete kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele

63 Euroopa Liidu Kohtu otsus tühistada komisjoni otsus 520/2000/EÜ põhines ka muudel alustel, mida käsitletakse käsiraamatu teistes osades. Euroopa Kohus leidis eelkõige, et otsusega piirati ebaseaduslikult riiklike andmekaitseasutuste volitusi. Lisaks ei olnud andmesubjektidel programmi Safe Harbor korra alusel õiguskaitsevahendeid juhuks, kui nad soovivad oma isikuandmetega tutvuda ja/või lasta neid parandada või need kustutada. Seega kahjustati ka harta artiklis 47 sätestatud tõhusa kohtuliku kaitse põhiõiguse olemust.

64 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

võtmise eesmärgil. Direktiiv ei võimaldanud säilitada elektroonilise side sisu. Euroopa Liidu Kohus märkis, et andmed, mida teenuseosutajad pidid direktiivi kohaselt säilitama, hõlmasid andmeid, mis on vajalikud side allika ja sihtkoha, side kuupäeva, kellaaja ja kestuse, helistaja numbri, valitud numbrite ja IP-aadresside jälgimiseks ja tuvastamiseks. Need andmed „kokku võimaldavad nimelt teha väga täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse, näiteks nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad".

Seega oli direktiivi kohane isikuandmete säilitamine eriti raske sekkumine õigusesse eraelu puutumatusele ja isikuandmete kaitsele. Euroopa Liidu Kohus leidis siiski, et sekkumine ei kahjustanud nende õiguste olemust. Eraelu puutumatuse õiguse olemust ei kahjustatud, sest direktiiv ei võimaldanud saada teada elektroonilise side sisu. Samamoodi ei kahjustatud isikuandmete kaitse õiguse olemust, sest direktiiviga nõuti elektroonilise side teenuste osutajatelt, et nad järgiksid teatud andmekaitse ja andmeturbe põhimõtteid ning rakendaksid selleks asjakohaseid tehnilisi ja korralduslikke meetmeid.

Vajalikkus ja proportsionaalsus

Harta artikli 52 lõikes 1 sätestatakse, et proportsionaalsuse põhimõtte kohaselt võib hartas tunnustatud põhiõiguste ja -vabaduste teostamist piirata üksnes siis, kui see on vajalik.

Piirang võib olla **vajalik**, kui on vaja võtta meetmeid üldhuvi eesmärgi saavutamiseks – kuid vajadus, nagu Euroopa Liidu Kohus on tõlgendanud, tähendab ka, et võetud meetmed peavad olema teiste sama eesmärgi saavutamise võimalustega võrreldes vähem sekkuvad. Eraelu austamise ja isikuandmete kaitse õiguse piirangute korral hindab Euroopa Liidu Kohus ranget vajalikkust, märkides, et „erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga". Kui piirangut peetakse rangelt vajalikuks, on vaja hinnata ka selle proportsionaalsust.

Proportsionaalsus tähendab, et piirangu eelised peavad olema suuremad kui kahju asjaomaste põhiõiguste teostamisele[65]. Et vähendada eraelu puutumatuse ja andmekaitse õiguse teostamise kahju ja riske, on oluline, et piirangud hõlmaksid asjakohaseid kaitsemeetmeid.

65 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, lk 5.

Näide: kohtuasjas *Volker und Markus Schecke*[66] järeldas Euroopa Liidu Kohus, et kehtestades teatud põllumajandusfondidest toetust saanud füüsiliste isikute korral iga toetusesaaja isikuandmete avaldamise, eristamata neid asjaomaste kriteeriumide alusel, näiteks toetusperioodid, toetuse sagedus või liik ja summa, ületasid nõukogu ja komisjon piire, mida nõuab proportsionaalsuse põhimõtte järgimine.

Seepärast pidas Euroopa Liidu Kohus vajalikuks tunnistada kehtetuks nõukogu määruse (EÜ) nr 1290/2005 teatud sätted ja määrus (EÜ) nr 259/2008 tervikuna[67].

Näide: kohtuasjas *Digital Rights Ireland*[68] otsustas Euroopa Liidu Kohus, et andmete säilitamise direktiivi põhjustatud sekkumine õigusesse eraelu puutumatusele ei kahjustanud selle õiguse olemust, sest direktiiv keelas elektroonilise sisu säilitamise. Kohus järeldas siiski, et direktiiv on vastuolus harta artiklitega 7 ja 8, ning tunnistas direktiivi kehtetuks. Et koondatud andmeliiklus- ja asukohaandmeid tervikuna saab analüüsida ning saada isikute eraelust üksikasjaliku ülevaate, oli tegu raske sekkumisega nendesse õigustesse. Kohus arvestas, et direktiiviga nõuti laua- ja mobiiltelefonide, internetiühenduse, e-posti ja internetitelefonide metaandmete säilitamise kohaldamist kõigile elektroonilistele sidevahenditele, mille kasutamine on inimeste igapäevaelus väga tavaline. Tegelikkuses oli see sekkumine, mis mõjutas kogu Euroopa elanikkonda. Arvestades selle sekkumise ulatust ja raskust, on andmeliiklus- ja asukohaandmete säilitamine Euroopa Liidu Kohtu arvates põhjendatud ainult raske kuritegevuse vastu võitlemiseks. Lisaks ei sätestanud direktiiv objektiivseid kriteeriume, mis tagaksid, et riigi pädevate asutuste juurdepääs säilitatavatele andmetele piirdub rangelt vajalikuga. Samuti ei hõlmanud direktiiv sisulisi ega menetlustingimusi, mis reguleeriksid

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

67 Nõukogu 21. juuni 2005. aasta määrus (EÜ) nr 1290/2005 ühise põllumajanduspoliitika rahastamise kohta, ELT 2005 L 209; komisjoni 18. märtsi 2008. aasta määrus (EÜ) nr 259/2008, 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 2008 L 76.

68 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014, punkt 39.

riigi ametiasutuste juurdepääsu säilitatavatele andmetele ja nende kasutamist, mida ei olnud tehtud sõltuvaks kohtu või muu sõltumatu asutuse eelnevast läbivaatamisest.

ELK jõudis sarnasele järeldusele liidetud kohtuasjades *Tele2 Sverige AB vs. Post- och telestyrelsen* ja *Secretary of State for the Home Department vs. Tom Watson jt*[69]. Kohtuasjad käsitlesid andmeliiklus- ja asukohaandmete säilitamist, mis hõlmas „kõiki abonente ja registreeritud kasutajaid ning kõiki elektroonilise side vahendeid", sätestamata „mingeid taotletavast eesmärgist lähtuvaid eristamisi, piiranguid või erandeid"[70]. Selles kohtuasjas ei olnud isiku andmete säilitamise tingimus, kas isik oli otseselt või kaudselt seotud raskete kuritegudega või kas tema teabevahetus oli riigi julgeoleku seisukohast oluline. Et puudus säilitatavate andmete ja avalikule julgeolekule tekkiva ohu või ajavahemiku või geograafilise asukoha piirangute nõutav seos, järeldas ELK, et liikmesriigi õigusaktid väljusid raske kuritegevuse vastu võitlemise eesmärgi saavutamiseks rangelt vajaliku piiridest[71].

Sarnast lähenemist vajalikkusele väljendab Euroopa andmekaitseinspektor vajalikkuse töövahendis *Necessity Toolkit*[72]. Töövahendi eesmärk on aidata hinnata kavandatud meetmete vastavust ELi andmekaitseõigusele. See töötati välja selleks, et anda paremad vahendid ELi poliitikakujundajatele ja seadusandjatele, kes vastutavad isikuandmete töötlemist ning isikuandmete kaitse õiguse ja muude hartas sätestatud õiguste ja vabaduste piiramist hõlmavate meetmete väljatöötamise ja järelevalve eest.

Üldhuvi eesmärgid

Et hartas tunnustatud õiguste kasutamise mis tahes piirang oleks põhjendatud, peab see vastama sisuliselt ka liidu tunnustatud üldist huvi pakkuvatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi. Teiste isikute õiguste ja vabaduste kaitsmise vajaduse korral on õigus isikuandmete kaitsele sageli vastastikmõjus teiste põhiõigustega. Peatükis 1.3 on sellise vastastikmõju üksikasjalik analüüs. Üldhuvi eesmärgid hõlmavad ELi üldeesmärke, mis on kinnitatud Euroopa

69 ELK, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen ja Secretary of State for the Home Department vs. Tom Watson jt* [suurkoda], 21. detsember 2016, punktid 105–106.

70 *Ibid.*, punkt 105.

71 *Ibid.*, punkt 107.

72 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11. aprill 2017.

Liidu lepingu artiklis 3, näiteks rahu ja oma rahvaste hüvangu, sotsiaalse õigluse ja kaitse edendamine ning sellise vabadusel, turvalisusel ja õigusel rajaneva sisepiirideta ala moodustamine, kus isikute vaba liikumine on tagatud koos kuritegevuse ennetamise ja kuritegevuse vastu võitlemisega seotud asjakohaste meetmete rakendamisega, samuti muudes aluslepingute sätetega kaitstud eesmärkides ja huvides[73]. Isikuandmete kaitse üldmääruses täpsustatakse harta artikli 52 lõiget 2 sellega seoses veelgi: määruse artikli 23 lõikes 1 loetletakse mitu üldhuvi eesmärki, mille puhul peetakse üksikisikute õiguste piiramist õiguspäraseks, kui piirang arvestab isikuandmete kaitse õiguse olemust ning on vajalik ja proportsionaalne. Loetelus nimetatud üldhuvi eesmärgid on näiteks riigi julgeolek ja riigikaitse, kuritegevuse ennetamine, liidu või liikmesriigi olulised majandus- või finantshuvid, rahvatervis ja sotsiaalkindlustus.

Tähtis on määratleda ja selgitada piiranguga taotletavat üldhuvi eesmärki piisavalt üksikasjalikult, sest piirangu vajalikkust hinnatakse selle taustal. Piirangu eesmärgi ja kavandatud meetmete selget ja üksikasjalikku kirjeldust on vaja hindamiseks, kas piirang on vajalik[74]. Taotletav eesmärk ning piirangu vajalikkus ja proportsionaalsus on omavahel tihedalt seotud.

Näide: kohtuasi *Schwarz vs. Stadt Bochum*[75] käsitles eraelu austamise õiguse ja isikuandmete kaitse õiguse piiranguid, mis tulenevad sõrmejälgede võtmisest ja säilitamisest, kui liikmesriikide ametiasutused väljastavad passe[76]. Hageja esitas Bochumi linnale passitaotluse, kuid keeldus sõrmejälgede andmisest; pärast seda lükkas Bochumi linn passitaotluse tagasi. Seejärel esitas hageja hagi Saksamaa kohtusse, et pass väljastataks ilma sõrmejälgede võtmiseta. Saksamaa kohus saatis asja Euroopa Liidu Kohtule, küsides, kas määruse (EÜ) nr 2252/2004 (liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta) artikli 1 lõige 1 tuleb lugeda kehtivaks.

ELK märkis, et sõrmejäljed **on isikuandmed**, sest sisaldavad objektiivselt ainulaadset teavet isikute kohta, mis võimaldab neid täpselt tuvastada, ning sõrmejälgede võtmine ja säilitamine on töötlemine. Viimati nimetatud töötlemine, mida reguleeritakse määruse (EÜ) nr 2252/2004 artikli 1 lõikega 2, on

73 Selgitused põhiõiguste harta kohta (2007/C 303/02), ELT 2007 C 303, lk 17–35.

74 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11. aprill 2017, lk 4.

75 ELK, C-291/12, *Michael Schwarz vs. Stadt Bochum*, 17. oktoober 2013.

76 *Ibid.*, punktid 33–36.

oht õigusele eraelu austamisele ja isikuandmete kaitsele[77]. Samas võimaldab harta artikli 52 lõige 1 nende õiguste kasutamise piiranguid, kui piirangud on sätestatud seaduses, arvestavad nimetatud õiguste olemust ning on proportsionaalsuse põhimõtte kohaselt vajalikud ja vastavad tegelikult Euroopa Liidus tunnustatud üldhuvi eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi.

Kohtuasjas märkis Euroopa Liidu Kohus kõigepealt, et passi väljastamisel sõrmejälgede võtmisest ja säilitamisest tulenevat piirangut tuleb pidada **õigusaktides ette nähtuks**, sest need toimingud on sätestatud määruse (EÜ) nr 2252/2004 artikli 1 lõikes 2. Teiseks oli viimati nimetatud määruse eesmärk vältida passide võltsimist ja kasutamist pettuseks. Seega on artikli 1 lõige 2 kehtestatud selleks, et takistada muu hulgas ebaseaduslikku sisenemist Euroopa Liitu, ning seega taotleb see liidu tunnustatud üldhuvi eesmärki. Kolmandaks ei ilmnenud Euroopa Liidu Kohtule kättesaadavatest tõenditest ega väidetud, et nende õiguste kasutamise piirangud selles kohtuasjas ei arvestanud nende õiguste olemusega. Neljandaks nõuab sõrmejälgede säilitamine väga turvalisel andmekandjal, nagu sätestatakse sättes, keerukat tehnoloogiat. Selline säilitamine vähendab tõenäoliselt passi võltsimise ohtu ja soodustab passi autentsuse kontrollimise eest vastutavate asutuste tegevust ELi piiridel. Asjaolu, et meetod ei ole täiesti usaldusväärne, ei ole määrav. Kuigi meetod ei takista kõigi volitamata isikute vastuvõtmist, piisab sellest, et see vähendab oluliselt sellise vastuvõtmise tõenäosust. Arvestades eespool öeldut, leidis ELK, et määruse (EÜ) nr 2252/2004 artikli 1 lõikes 2 viidatud sõrmejälgede võtmine ja säilitamine on asjakohane, et saavutada määruse eesmärke ja selle laiendusena Euroopa Liitu ebaseadusliku sisenemise takistamise eesmärki[78].

Järgmiseks hindas ELK, kas selline töötlemine on **vajalik**, märkides, et toiming hõlmas sõrmejälje võtmist ainult kahelt sõrmelt, mida üldiselt võivad näha ka teised, nii et see ei ole intiimset laadi toiming. Ka ei põhjusta see asjaomasele isikule erilist füüsilist ega vaimset ebamugavust, mis oleks suurem kui inimese näokujutise jäädvustamine. Tuleb ka märkida, et sõrmejälgede võtmise ainus reaalne alternatiiv, mis ELK menetluses esile toodi, on silmaiirise kujutis. ELK-le esitatud toimikust ei nähtu, et viimati nimetatud menetlusega sekkutaks harta artiklites 7 ja 8 tunnustatud õigustesse vähem kui sõrmejälgede

77 *Ibid*., punktid 27–30.

78 *Ibid*., punktid 35–45.

võtmisega. Peale selle on mõlema meetodi tulemuslikkuse seisukohalt selge, et silmaiirise tuvastamise tehnika ei ole veel nii arenenud kui sõrmejälgede tuvastamise tehnika, see on praegu oluliselt kallim kui sõrmejälgede võrdlemise menetlus ning seetõttu on see üldiseks kasutamiseks vähem sobiv. Seega ei olnud ELK-le teada ükski meede, mis oleks ühtaegu piisavalt tõhus, et aidata saavutada passide pettuseks kasutamise eest kaitsmise eesmärki, ja ohustaks vähem harta artiklites 7 ja 8 tunnustatud õigusi kui sõrmejälgede kasutamisel põhinevast meetodist tulenevad meetmed[79].

ELK märkis, et määruse (EÜ) nr 2252/2004 artikli 4 lõikes 3 on selge sõnaga sätestatud, et sõrmejälgi võib kasutada ainult passi ehtsuse ja selle omaniku isiku tuvastamiseks, kuid määruse artikli 1 lõikes 2 ei sätestata sõrmejälgede säilitamist mujal kui passis endas, mis kuulub üksnes selle omanikule. Seega ei sätestatud määruses õiguslikku alust selle kohaselt kogutud andmete kestseks säilitamiseks ega selliste andmete kasutamiseks muul eesmärgil kui Euroopa Liitu ebaseadusliku sisenemise takistamine[80]. Arvestades kõiki eespool nimetatud kaalutlusi, järeldas ELK, et eelotsuse küsimuse uurimisel ei ilmnenud midagi, mis seaks kahtluse alla määruse (EÜ) nr 2252/2004 artikli 1 lõike 2 kehtivuse.

Harta ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni seos

Kuigi sõnastus erineb, meenutavad harta artikli 52 lõikes 1 sätestatud õiguste seaduslike piirangute tingimused Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõiget 2, mis käsitleb õigust eraelu austamisele. Euroopa Liidu Kohus ja Euroopa Inimõiguste Kohus viitavad oma praktikas sageli teineteise otsustele osana mõlema kohtu pidevast dialoogist, et tõlgendada andmekaitse-eeskirju ühtselt. Harta artikli 52 lõikes 3 märgitakse, et „[h]artas 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". Harta artikkel 8 ei vasta siiski täpselt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile[81]. Harta artikli 52 lõige 3 käsitleb iga õiguskorraga kaitstud õiguste sisu ja ulatust, mitte nende piirangute tingimusi. Arvestades mõlema kohtu vahelise dialoogi ja koostöö laiemat konteksti, võib ELK oma analüüsis arvestada

79 ELK, C-291/12, *Michael Schwarz vs. Stadt Bochum*, 17. oktoober 2013, punktid 46–53.

80 *Ibid.*, punktid 56–61.

81 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11. aprill 2017, lk 6.

Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud seadusliku piirangu kriteeriume, nagu neid on tõlgendanud EIK. Võimalik on ka vastupidine stsenaarium, kui EIK võib viidata hartas sätestatud seadusliku piirangu tingimustele. Igal juhul tuleb ka arvestada, et Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ei ole harta artikliga 8 täpselt samaväärset sätet, mis viitab isikuandmete kaitsele, eelkõige andmesubjekti õigustele, töötlemise õiguspärastele põhjustele ja sõltumatu asutuse järelevalvele. EIK praktikas võib leida mõningaid harta artikli 8 komponente, mida on arendatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 alusel ja mis on seotud konventsiooniga nr 108[82]. See seos tagab ELK ja EIK vastastikuse inspireerimise andmekaitse küsimustes.

1.3. Vastastikmõju teiste õiguste ja õigustatud huvidega

Põhipunktid

- Õigus andmekaitsele on sageli vastastikmõjus teiste õigustega, näiteks sõnavabadusega ning õigusega saada ja levitada teavet.
- See vastastikmõju on tihti kaksipidine: kuigi on olukordi, kus õigus isikuandmete kaitsele on vastuolus teatud õigusega, on ka olukordi, kus õigus isikuandmete kaitsele tagab tulemuslikult sama õiguse austamise. Nii on see näiteks sõnavabaduse korral, sest kutsesaladus on osa õigusest eraelu austamisele.
- Vajadus kaitsta teiste isikute õigusi ja vabadusi on üks kriteeriumeist, millega hinnatakse isikuandmete kaitse seaduslikku piiramist.
- Eri õiguste korral peavad kohtud need tasakaalustama.
- Isikuandmete kaitse üldmääruses nõutakse, et liikmesriigid ühitaksid õiguse isikuandmete kaitsele sõna- ja teabevabadusega.
- Liikmesriigid võivad riigisiseses õiguses vastu võtta ka erieeskirjad, et ühitada isikuandmete kaitse õigus üldsuse juurdepääsuga ametlikele dokumentidele ja kutsesaladuse hoidmise kohustustega.

Õigus isikuandmete kaitsele ei ole absoluutne õigus; selle õiguse seadusliku piiramise tingimusi on kirjeldatud eespool. Üks nii Euroopa Nõukogu kui ka ELi õiguse

82 Selgitused põhiõiguste harta kohta (2007/C 303/02), artikkel 8.

alusel tunnustatud õiguste seaduslike piirangute kriteeriumeist on, et andmekaitsesse sekkumine on vajalik teiste õiguste ja vabaduste kaitseks. Nii Euroopa Inimõiguste Kohus kui ka Euroopa Liidu Kohus on korduvalt öelnud, et kui andmekaitse on vastastikmõjus teiste õigustega, on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 ning harta artikli 8 kohaldamisel ja tõlgendamisel vaja tasakaalustamist teiste õigustega[83]. Sellise tasakaalu saavutamist illustreerivad mitu olulist näidet.

Lisaks tasakaalustamisele kohtute poolt võivad riigid vajaduse korral võtta vastu õigusakte, et ühitada õigus isikuandmete kaitsele teiste õigustega. Sel põhjusel on isikuandmete kaitse üldmääruses sätestatud mitu riigisisese erandi valdkonda.

Sõnavabaduse suhtes nõutakse isikuandmete kaitse üldmääruses, et liikmesriigid ühitaksid õigusaktiga „käesoleva määruse kohase õiguse isikuandmete kaitsele ning sõna- ja teabevabaduse õiguse, muu hulgas seoses isikuandmete töötlemisega ajakirjanduslikel eesmärkidel ning akadeemilise, kunstilise või kirjandusliku eneseväljenduse tarbeks"[84]. Liikmesriigid võivad vastu võtta ka õigusakte, millega ühitatakse andmekaitse üldsuse juurdepääsuga ametlikele dokumentidele ja kutsesaladuse hoidmise kohustusega, mida kaitstakse eraelu austamise õigusena[85].

1.3.1. Sõnavabadus

Üks õigusi, mis võib olla kõige olulisemas vastastikmõjus õigusega andmekaitsele, on 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." Nii põhiõiguste harta artiklis 11 kui ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 10 sätestatud teabevabadusega kaitstakse ühelt poolt õigust teavet edastada ja teisalt õigust teavet *saada*.

83 EIK, *Von Hannover vs. Saksamaa (nr 2)* [suurkoda], nr 40660/08 ja nr 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* [suurkoda], 29. jaanuar 2008, punkt 68.

84 Isikuandmete kaitse üldmääruse artikkel 85.

85 *Ibid.*, artiklid 86 ja 90.

Sõnavabaduse piirangud peavad vastama harta artikli 52 lõikes 1 sätestatud kriteeriumidele, mida on kirjeldatud eespool. Lisaks vastab artikkel 11 Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 10. Harta artikli 52 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 – need peavad olema ette nähtud seaduses ja olema „demokraatlikus ühiskonnas vajalikud [...] kaasinimeste maine või õiguste kaitseks". Sellised õigused hõlmavad eelkõige õigust eraelu austamisele ja õigust isikuandmete kaitsele.

Isikuandmete kaitse ja sõnavabaduse seost reguleerib isikuandmete kaitse üldmääruse artikkel 85 „Isikuandmete töötlemine ning sõna- ja teabevabadus". Artikli kohaselt peavad liikmesriigid ühitama õiguse isikuandmete kaitsele õigusega sõna- ja teabevabadusele. Eelkõige tehakse isikuandmete kaitse üldmääruse konkreetsetest peatükkidest erandeid ajakirjanduslikel eesmärkidel või teadusliku, kunstilise või kirjandusliku väljenduse eesmärgil, kui neid on vaja, et ühitada õigus isikuandmete kaitsele sõna- ja teabevabadusega.

Näide: kohtuasjas *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy*[86] paluti Euroopa Liidu Kohtul määratleda andmekaitse ja ajakirjandusvabaduse seos[87]. Kohus pidi analüüsima ligikaudu 1,2 miljoni füüsilise isiku maksuandmete levitamist SMS-teenuse kaudu äriühingu poolt, kes hankis andmed seaduslikult Soome maksuhaldurilt. Soome andmekaitse järelevalveasutus tegi otsuse, milles nõuti, et äriühing lõpetaks nende andmete levitamise. Äriühing vaidlustas otsuse riigisiseses kohtus, kes taotles ELK-lt selgitust andmekaitsedirektiivi tõlgendamise kohta. Eelkõige pidi ELK kontrollima, kas maksuhalduri avaldatud isikuandmete töötlemist, mis võimaldas mobiilikasutajatel tellida telefonile teiste füüsiliste isikute maksuandmeid, tuleb pidada isikuandmete töötlemiseks üksnes ajakirjanduslikul

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

87 Kohtuasi käsitles küsimust, kuidas tõlgendada andmekaitsedirektiivi artiklit 9 – praegu on see asendatud isikuandmete kaitse üldmääruse artikliga 85 –, mille tekst oli järgmine: „Kui isikuandmeid töödeldakse ainult ajakirjanduse jaoks või kirjandusliku või kunstilise eneseväljenduse huvides, sätestavad liikmesriigid erandid või kõrvalekalded käesoleva peatüki, IV peatüki ja VI peatüki sätetest ainult siis, kui see on vajalik selleks, et viia omavahel vastavusse eraelu puutumatuse õigus ja sõnavabadust reguleerivad eeskirjad."

eesmärgil. Olles järeldanud, et äriühingu tegevus oli „isikuandmete töötlemine“ andmekaitsedirektiivi artikli 3 lõike 1 tähenduses, analüüsis ELK direktiivi artiklit 9 (isikuandmete töötlemine ja sõnavabadus). Esimeseks märkis kohus, kui tähtis on sõnavabaduse õigus igas demokraatlikus ühiskonnas, ja leidis, et selle vabadusega seonduvaid mõisteid, näiteks ajakirjandust, tuleks tõlgendada laialt. Seejärel nentis kohus, et mõlema põhiõiguse tasakaalu tagamiseks tuleb seoses õigusega andmekaitsele tehtavate erandite ja piirangute korral piirduda rangelt vajalikuga. Selles kontekstis otsustas ELK, et asjaomaste äriühingute toiminguid riiklike õigusaktide kohaselt avalikest dokumentidest pärit andmetega võib käsitada ajakirjandusliku tegevusena, kui selle eesmärk on teabe, arvamuste ja mõtete avalikustamine, olenemata edastamise vahendist. Samuti otsustas kohus, et need toimingud ei piirdu üksnes meediaettevõtetega ja seda võidakse teha kasumi saamiseks. Samas jättis ELK liikmesriigi kohtu ülesandeks otsustada, kas see kehtib juhtumi konkreetsetel asjaoludel.

Sama juhtumit uuris ka EIK pärast riigisisese kohtu otsust ELK suuniste põhjal, et järelevalveasutuse korraldus lõpetada kogu maksuteabe avaldamine oli põhjendatud sekkumine äriühingu sõnavabadusse. EIK kinnitas seda käsitlusviisi[88]. Kohus leidis, et kuigi toimus sekkumine äriühingute õigusesse teabe levitamisele, oli sekkumine kooskõlas seadusega, täitis õiguspärast eesmärki ja oli demokraatlikus ühiskonnas vajalik.

Kohus tuletas meelde kohtupraktika kriteeriume, mis peaksid suunama riiklikke ametiasutusi ja ka EIKd ennast sõnavabaduse ja eraelu austamise õiguse tasakaalustamisel. Poliitiku kõne või üldhuvi küsimuse arutamise korral on teabe saamise ja levitamise õiguse piiramiseks vähe ruumi, sest üldsusel on õigus saada teavet „ja see on demokraatlikus ühiskonnas oluline õigus“[89]. Samas ei saa öelda, et ajakirjandusartiklid, mille ainus eesmärk on rahuldada teatud lugejaskonna uudishimu isiku eraelu vastu, aitaks kaasa üldhuvi pakkuvale arutelule. Andmekaitse-eeskirjadest ajakirjanduslikel eesmärkidel tehtava erandi eesmärk on, et ajakirjanikud saaksid ajakirjandustegevuse jaoks juurdepääsu andmetele ning neid koguda ja töödelda. Seega oli tõepoolest avalik huvi pakkuda juurdepääsu ja võimaldada kaebuse esitanud äriühingutel koguda ja töödelda asjaomaste maksuandmete suuri koguseid. Teisalt leidis kohus, et selliste toorandmete muutmata kujul ja ilma mis tahes analüüsita laialdaseks levitamiseks puudus avalik huvi. Maksuteave

88 EIK, *Satakunnan Markkinapörssi Oy ja Satamedia Oy vs. Soome* [suurkoda], nr 931/13, 27. juuni 2017.

89 *Ibid.*, punkt 169.

võimaldanuks üldsuse uudishimulikel liikmetel liigitada isikuid nende majandusliku seisundi järgi ja rahuldada üldsuse soovi saada teiste eraelulist teavet. Seda ei saa pidada avalikku huvi pakkuva arutelu toetamiseks.

Näide: kohtuasjas *Google Spain*[90] kaalutles Euroopa Liidu Kohus, kas Google'il oli kohustus kustutada oma otsingutulemuste loetelust vananenud teave kaebuse esitaja finantsraskuste kohta. Kui Google'i otsingumootoriga otsiti kaebuse esitaja nime, andis otsing tulemuseks linke vanadele ajaleheartiklitele, milles mainiti tema seost pankrotimenetlusega. Kaebuse esitaja pidas seda oma eraelu austamise ja isikuandmete kaitse õiguse rikkumiseks, sest menetlused olid lõppenud juba aastaid tagasi, mistõttu olid need viited muutunud asjakohatuks.

ELK selgitas kõigepealt, et interneti otsingumootorid ja isikuandmeid pakkuvad otsingutulemused võivad luua üksikisiku üksikasjaliku profiili. Kuivõrd ühiskond on üha digitaalsem, on nõue, et isikuandmed oleksid õiged ja neid ei avaldataks rohkem kui vaja (avaliku teabe korral) üksikisikute puhul isikuandmete kõrgetasemelise kaitse tagamise seisukohast ülioluline. „Vastutav töötleja peab oma ülesannete, pädevuse ja võimaluste piires tagama andmetöötluse vastavuse ELi õigusaktide nõuetele", et ette nähtud tagatised saaksid avaldada täielikku mõju. See tähendab, et õigus isikuandmete kustutamisele, kui töötlemist ei ole enam vaja või kui andmed on vananenud, hõlmab ka otsingumootoreid, mis leiti olevat vastutavad töötlejad, mitte üksnes volitatud töötlejad (vt punkt 2.3.1).

Uurides, kas Google peab kaebuse esitajaga seotud lingid eemaldama, leidis ELK, et teatud tingimustel on isikutel õigus lasta oma isikuandmed interneti otsingumootori otsingutulemustest kustutada. Seda õigust võib kasutada siis, kui isiku teave on andmetöötluse jaoks ebaõige, ebapiisav, ebaoluline või liigne. ELK tunnistas, et see õigus ei ole absoluutne; see peab olema tasakaalustatud teiste õigustega, eelkõige üldsuse huviga ja õigusega tutvuda teabega. Iga kustutamistaotlust tuleb hinnata eraldi, et tasakaalustada ühelt poolt andmesubjekti isikuandmete kaitse ja eraelu kaitse kui põhiõigused ning teisalt kõigi internetikasutajate õigustatud huvid. ELK esitas tasakaalustamisel arvestatavate tegurite suunised. Eriti tähtis tegur on asjaomase teabe olemus. Kui teave on isiku eraelu seisukohast delikaatne ja teabe

90 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punktid 81–83.

kättesaadavus ei ole üldsuse huvides, oleks andmekaitse ja eraelu puutumatus ülimuslik üldsuse õiguse suhtes teabega tutvuda. Teisalt kui ilmneb, et andmesubjekt on avaliku elu tegelane või et teave on selline, et see õigustab üldsuse juurdepääsu, on andmekaitse ja eraelu puutumatuse põhiõiguse riive põhjendatud.

Pärast otsuse langetamist võttis artikli 29 töörühm vastu ELK otsuse rakendamise suunised. Suunised sisaldavad selliste ühiskriteeriumide loetelu, mida järelevalveasutused peavad kasutama üksikisikute andmete kustutamise taotlustega seotud kaebuste käsitlemisel ja mis juhendavad neid õiguste tasakaalustamisel[91].

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

Näide: kohtuasjas *Axel Springer AG vs. Saksamaa*[92] otsustas EIK, et kohtumäärus, millega seatakse kaebuse esitanud äriühingule piirangud sellise artikli avaldamisel, mis käsitleb tuntud näitleja vahistamist ja süüdimõistmist, on vastuolus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 10. EIK kordas kriteeriume, mida tuleb arvestada sõnavabaduse ja eraelu austamise õiguse tasakaalustamisel, nagu on sätestatud tema kohtupraktikas:

- kas sündmus, mida avaldatud artiklis käsitleti, pakkus avalikku huvi;
- kas asjaomane isik oli avaliku elu tegelane ning
- kuidas teave saadi ja kas see oli usaldusväärne.

EIK leidis, et näitleja vahistamine ja süüdimõistmine oli avalik õigusfakt ja oli seega üldsuse huvides; et näitleja oli piisavalt tuntud kui avaliku elu tegelane; teabe oli esitanud prokuratuur ja pooled ei ole selle õigsust vaidlustanud. Seega ei olnud äriühingule määratud avaldamispiirangud mõistlikult

91 Artikli 29 töörühm (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González", C-131/12*, WP 225, Brüssel, 26. november 2014.

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

proportsionaalsed kaebuse esitaja eraelu kaitsmise õiguspärase eesmärgiga. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 10.

Näide: kohtuasi *Couderc ja Hachette Filipacchi Associés vs. Prantsusmaa*[93] käsitles juhtumit, kus Prantsuse nädalaajakiri avaldas intervjuu Nicole Coste'iga, kes väitis, et Monaco prints Albert on tema poja isa. Intervjuus kirjeldati ka Nicole Coste'i suhet vürstiga ja viisi, kuidas viimane lapse sünnile reageeris, lisati ka fotod printsist koos lapsega. Prints Albert esitas kirjastuse vastu kaebuse oma eraelu kaitse õiguse rikkumise kohta. Prantsuse kohtud leidsid, et artikli avaldamine on põhjustanud prints Albertile pöördumatu kahju, ja andsid kirjastajale korralduse kahju hüvitada ning avaldada ajakirja esikaanel kohtuotsuse üksikasjad.

Ajakirja kirjastajad andsid asja Euroopa Inimõiguste Kohtusse, väites, et Prantsuse kohtute otsusega sekkuti põhjendamatult nende sõnavabaduse õigusesse. EIK pidi tasakaalustama prints Alberti õigust eraelu austamisele ja kirjastaja õigust sõnavabadusele ning üldsuse õigust saada teavet. Olulised kaalutlused olid ka Nicole Coste'i õigus jagada oma lugu avalikkusega ja lapse huvi kehtestada ametlikult isa-lapse suhe.

EIK leidis, et intervjuu avaldamine oli sekkumine printsi eraellu, ja uuris seejärel, kas sekkumine oli vajalik. Kohus leidis, et avaldamine puudutas avaliku elu tegelast ja üldhuvi küsimust, sest Monaco kodanikel oli huvi teada vürsti lapse olemasolust, sest päriliku monarhia tulevik on „olemuslikult seotud järeltulijate olemasoluga" ning seega üldsuse jaoks murettekitav küsimus[94]. Kohus märkis ka, et artikkel võimaldas Nicole Coste'il ja tema lapsel kasutada õigust sõnavabadusele. Riigisisesed kohtud ei arvestanud nõuetekohaselt EIK kohtupraktikas välja töötatud põhimõtteid ja kriteeriume, kuidas tasakaalustada õigust eraelu austamisele ja õigust sõnavabadusele. Kohus järeldas, et Prantsusmaa rikkus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 10.

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

93 EIK, *Couderc ja Hachette Filipacchi Associés vs. Prantsusmaa* [suurkoda], nr 40454/07, 10. november 2015.

94 *Ibid.*, punktid 104–116.

Näide: kohtuasjas *Mosley vs. Ühendkuningriik*[95] avaldas riigisisene nädalaleht intiimseid fotosid kaebuse esitajast, kes oli tuntud isik ning kes esitas seejärel avaldaja vastu eduka tsiviilhagi ja sai kahjutasu. Antud rahalisele hüvitisele vaatamata kaebas ta, et jäi oma eraelu puutumatuse õiguse rikkumise ohvriks, sest tal ei olnud võimalust taotleda kohtumäärust enne fotode avaldamist, sest puudus õiguslik nõue, et ajaleht teataks avaldamisest ette.

EIK märkis, et kuigi materjali levitati üldiselt pigem meelelahutuse kui hariduse eesmärgil, loodeti selle puhul kahtlemata asjaomase konventsiooni artikliga 10 tagatavale kaitsele, mille võivad aga üles kaaluda artiklis 8 sätestatud nõuded, mille alusel ei tohi teavet levitada, kui see on eraelulise või intiimse sisuga ja selle levitamisel ei ole avalikku huvi pakkuvat mõõdet. Eriti üksikasjalikult tuli analüüsida piiranguid, mis võivad toimida teatud vormis eeltsensuurina. Kahju tõttu, mida võib tekitada materjali avaldamisest etteteatamise nõue, kahtluste tõttu selle tulemuslikkuse suhtes ja laia kaalutlusruumi tõttu valdkonnas leidis EIK, et artiklist 8 ei tulene õiguslikult siduvat eelteatamise kohustust. Seega otsustas kohus, et artiklit 8 ei rikutud.

Näide: kohtuasi *Bohlen vs. Saksamaa*[96] käsitles juhtumit, kus kaebuse esitaja, tuntud laulja ja produtsent, oli avaldanud autobiograafilise raamatu ja oli hiljem kohtuotsusega sunnitud sellest mõne lõigu eemaldama. Juhtumit kajastati riigi meediakanalites laialdaselt ja üks tubakafirma alustas humoorika reklaamikampaania sellele sündmusele viidates, kasutades kaebuse esitaja eesnime ilma tema nõusolekuta. Kaebuse esitaja nõudis reklaamiettevõtjalt kahju hüvitamist, kuid edutult, väites, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õigusi on rikutud. EIK kordas kriteeriume, millest juhindutakse eraelu austamise õiguse ja sõnavabaduse õiguse tasakaalustamisel, ning leidis, et tegu ei olnud artikli 8 rikkumisega. Kaebuse esitaja oli avaliku elu tegelane ja reklaamis ei viidatud tema eraelu üksikasjadele, vaid avalikule sündmusele, mida meedia oli juba kajastanud ja mis oli osa avalikust arutelust. Pealegi oli reklaam humoorikas ega sisaldanud kaebuse esitaja kohta midagi halvustavat ega negatiivset.

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

96 EIK, *Bohlen vs. Saksamaa*, nr 53495/09, 19. veebruar 2015, punktid 45–60.

Näide: kohtuasjas *Biriuk vs. Leedu*[97] väitis kaebuse esitaja Euroopa Inimõiguste Kohtule, et Leedu ei täitnud kohustust tagada tema eraelu õiguse austamine, sest kuigi suur ajaleht oli tema eraelu raskelt kahjustanud, määrasid juhtumit uurinud riigisisesed kohtud talle rahalise kahju hüvituseks naeruväärse summa. Mittevaralise kahju hüvitamisel kohaldasid riigisisesed kohtud avalikkuse teavitamist käsitlevate riiklike õigusaktide sätteid, millega kehtestati meedia poolt isiku eraelu kohta teabe avalikkusele ebaseadusliku levitamise tõttu tekitatud mittevaralise kahju hüvitamise madal ülemmäär. Juhtum tulenes artikli avaldamisest Leedu suurima päevalehe esilehel, kus teatati, et kaebuse esitaja on HIV-positiivne. Artiklis kritiseeriti ka kaebuse esitaja käitumist ja seati kahtluse alla tema moraalinormid.

EIK tuletas meelde, et isikuandmete, eelkõige meditsiiniliste andmete kaitse on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni kohase eraelu austamise põhiõiguse seisukohast keskse tähtsusega. Terviseandmete konfidentsiaalsus on eriti oluline, sest meditsiiniandmete avaldamine (käsitletaval juhul kaebuse esitaja HIV-staatus) võib oluliselt mõjutada inimese era- ja perekonnaelu, tema tööhõiveolukorda ja kaasatust ühiskonnas. Kohus pidas eriti tähtsaks asjaolu, et ajalehes esitatud teabe kohaselt olid kaebuse esitaja HIV-staatuse kohta andnud teavet haigla meditsiinitöötajad, mis on ilmselgelt vastuolus nende kohustusega hoida arstisaladust. Seega ei olnud tegu õiguspärase sekkumisega kaebuse esitaja õigusesse eraelule.

Artikli avaldas ajakirjandus ja sõnavabadus on ka Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud põhiõigus. Uurides, kas avaliku huvi olemasolu põhjendas kaebuse esitaja kohta sellise teabe avaldamist, leidis kohus, et avaldamise peamine eesmärk oli ajalehe müügi suurendamine, rahuldades lugejate uudishimu. Sellist eesmärki ei saa pidada ühiskonnale üldhuvi pakkuvat arutelu toetavaks. Et tegu oli „ajakirjandusvabaduse ennekuulmatu kuritarvitamisega", tähendasid kahju hüvitamise suured piirangud ja riigi õiguses mittevaralise kahju eest ette nähtud väike summa, et Leedu ei täitnud oma positiivset kohustust kaitsta kaebuse esitaja õigust eraelule. Kohus leidis, et tegu oli Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisega.

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

Õigus sõnavabadusele ja õigus isikuandmete kaitsele ei ole alati vastuolus. On juhtumeid, kus isikuandmete tõhus kaitse tagab sõnavabaduse.

Näide: kohtuasjas *Tele2 Sverige* märkis Euroopa Liidu Kohus, et direktiivist 2006/24/EÜ (andmete säilitamise direktiiv) ja harta artiklites 7 ja 8 sätestatud põhiõigustest tulenev sekkumine oli „ulatuslik riive, mida tuleb pidada eriti raskeks. Lisaks võib asjaolu, et andmete säilitamine ja hilisem kasutamine toimub abonenti või registreeritud kasutajat sellest teavitamata, tekitada asjassepuutuvates isikutes tunde, et nende eraelu pidevalt jälgitakse." Ka leidis ELK, et andmeliiklus- ja asukohaandmete üldine säilitamine võib mõjutada seda, kuidas kasutajad kasutavad sidevahendeid, ning „seeläbi ka harta artikliga 11 tagatud sõnavabaduse teostamist nende poolt"[98]. Selles mõttes aitavad andmekaitse-eeskirjad, mis nõuavad rangeid kaitsemeetmeid andmete üldise säilitamise vastu, lõppkokkuvõttes kaasa sõnavabaduse õiguse kasutamisele.

Seoses õigusega teavet saada, mis on samuti sõnavabaduse osa, mõistetakse üha enam, et demokraatliku ühiskonna toimimise seisukohalt on oluline tagada valitsussüsteemi läbipaistvus. Läbipaistvus on üldhuvi eesmärk, mis võib seega põhjendada sekkumist õigusesse andmekaitsele, kui see on vajalik ja proportsionaalne, nagu on selgitatud peatükis 1.2. Sel põhjusel on viimase 20 aasta jooksul leitud, et õigus tutvuda avaliku sektori asutuste valduses olevate dokumentidega peab olema kõigil Euroopa Liidu kodanikel ja igal füüsilisel või juriidilisel isikul, kes elab või kelle registrijärgne asukoht on liikmesriigis.

Euroopa Nõukogu õiguses saab viidata põhimõtetele, mis on sätestatud ametlikele dokumentidele juurdepääsu soovituses; soovituse eeskujul koostati ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon (konventsioon nr 205)[99].

98 ELK, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen* ja *Secretary of State for the Home Department vs. Tom Watson jt* [suurkoda], 21. detsember 2016, punktid 37 ja 101; ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014, punkt 28.

99 Euroopa Nõukogu ministrite komitee (2002), *Recommendation R (81) 19 and Recommendation Rec(2002)2 to member states on access to official documents*, 21. veebruar 2002; Euroopa Nõukogu, ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon, CETS nr 205, 18. juuni 2009. Konventsioon ei ole veel jõustunud.

ELi õiguses on dokumentidega tutvumise õigus tagatud määrusega (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (dokumentidele juurdepääsu määrus)[100]. Harta artikliga 42 ja ELi toimimise lepingu artikli 15 lõikega 3 laiendatakse dokumentidega tutvumise õigust liidu institutsioonide, organite ja asutuste dokumentidele mis tahes kandjal.

See õigus võib sattuda konflikti õigusega isikuandmete kaitsele, kui dokumendiga tutvumine avalikustaks muude inimeste isikuandmeid. Isikuandmete kaitse üldmääruse artiklis 86 sätestatakse selgelt, et avaliku sektori asutus või organ võib avaldada tema valduses olevates ametlikes dokumentides sisalduvaid isikuandmeid kooskõlas liidu[101] õigusega või kõnealuse avaliku sektori asutuse või organi suhtes kohaldatava liikmesriigi õigusega, et ühitada üldsuse juurdepääs sellistele ametlikele dokumentidele ja määruse kohane õigus isikuandmete kaitsele.

Seetõttu tuleb avaliku sektori asutuste valduses olevate dokumentide või teabega tutvumise taotluste korral arvestada nende inimeste õigust isikuandmete kaitsele, kelle andmeid need dokumendid sisaldavad.

Näide: kohtuasjas *Volker und Markus Schecke ja Hartmut Eifert vs. Land Hessen*[102] pidi Euroopa Liidu Kohus otsustama, kas ELi põllumajandustoetuste saajate nime ja saadud summade avaldamine, mida nõutakse ELi õigusaktidega, on proportsionaalne. Avaldamise eesmärk oli suurendada läbipaistvust ja soodustada üldsuse kontrolli avaliku sektori vahendite nõuetekohase kasutamise üle haldusasutustes. Mitu toetusesaajat vaidlustas avalikustamise proportsionaalsuse.

Märkides, et õigus isikuandmete kaitsele ei ole absoluutne, leidis ELK, et kahest ELi põllumajandusfondist toetuse saajaid ja neile makstud täpseid summasid nimetavate andmete avaldamisega veebilehel sekkutakse üldiselt toetusesaajate eraellu ning konkreetsemalt nende isikuandmete kaitsesse.

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

101 Harta artikkel 42, ELi toimimise lepingu artikli 15 lõige 3 ja määrus (EÜ) nr 1049/2001.

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

ELK leidis, et sellised põhiõiguste harta artiklite 7 ja 8 õiguste piirangud on sätestatud seaduses ning vastavad ELi tunnustatud avaliku huvi eesmärgile, nimelt eesmärgile suurendada läbipaistvust ühenduse vahendite kasutamisel. ELK pidas kahest ELi põllumajandusfondist toetust saavate füüsiliste isikute nimede ja neile makstud täpsete toetussummade avalikustamist siiski ebaproportsionaalseks ning harta artikli 52 lõike 1 alusel õigustamatuks. Kohus tunnistas demokraatlikus ühiskonnas maksumaksjate avaliku sektori vahendite kasutamisest teavitamise tähtsust. Samas kuna „[l]äbipaistvuse eesmärki ei saa isikuandmete kaitse õigusele automaatselt eelistada“,[103] on ELi institutsioonidel kohustus tasakaalustada liidu huvi läbipaistvuse tagamise vastu eraelu puutumatuse ja andmekaitseõiguse kasutamise piirangutega, mis avalikustamise tulemusena kahjustasid toetusesaajaid.

ELK leidis, et ELi institutsioonid ei olnud seda nõuetekohaselt tasakaalustanud, sest oli võimalik kavandada meetmeid, mis kahjustaksid isikute põhiõigusi vähem, ühtlasi tõhusalt toetades ka läbipaistvuse eesmärgi saavutamist, mida taotleti avalikustamisega. Näiteks võib kõiki toetusesaajaid mõjutava üldise, nende nimesid ja igaühele makstud täpse summa avalikustamise asemel mitte eristada neid asjakohaste kriteeriumide alusel, näiteks ajavahemike alusel, mil nad said toetust, toetuse saamise sageduse või suuruse ja olemuse alusel[104]. Seega tunnistas ELK osaliselt kehtetuks ELi õigusaktide sätted, milles käsitleti Euroopa põllumajandusfondidest toetuse saajatega seotud teabe avaldamist.

Näide: kohtuasjas *Rechnungshof vs. Österreichischer Rundfunk jt*[105] vaatas Euroopa Liidu Kohus läbi Austria teatud õigusakti kooskõla ELi andmekaitseõigusega. Õigusaktis nõuti, et riigiasutus koguks ja edastaks sissetulekuandmeid, et avaldada üldsusele kättesaadavaks tehtavas aastaaruandes eri avalik-õiguslike üksuste töötajate nimed ja sissetulekud. Mõni isik keeldus andmekaitse alusel oma andmete esitamisest.

ELK tugines oma arvamuses põhiõiguste kaitsele kui ELi õiguse üldpõhimõttele ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8, tuletades meelde, et harta ei olnud sel ajal siduv. Kohus leidis,

103 *Ibid.*, punkt 85.

104 *Ibid.*, punkt 89.

105 ELK, liidetud kohtuasjad C-465/00, C-138/01 ja C-139/09, *Rechnungshof vs. Österreichischer Rundfunk jt* ning *Christa Neukomm ja Jospeh Lauermann vs. Österreichischer Rundfunk*, 20. mai 2003.

et üksikisiku ametialase sissetuleku andmete kogumine ja eelkõige nende edastamine kolmandatele isikutele kuulub eraelu austamise õiguse kohaldamisalasse ja rikub seda õigust. Sekkumine võib olla õigustatud, kui see oleks olnud seadusega kooskõlas, taotlenud õiguspärast eesmärki ja olnud demokraatlikus ühiskonnas selle eesmärgi saavutamiseks vajalik. ELK märkis, et Austria õigusaktiga taotleti õiguspärast eesmärki, sest selle eesmärk oli hoida avaliku sektori töötajate palgad mõistlikes piirides – see kaalutlus on seotud ka riigi majandusliku heaoluga. Austria huvi avaliku sektori vahendite parima kasutamise tagamise vastu pidi siiski olema tasakaalus asjaomaste isikute eraelu austamise õigusesse sekkumise raskusega.

Jättes riigisisese kohtu ülesandeks kontrollida, kas isiku sissetuleku andmete avaldamine on vajalik ja proportsionaalne õigusaktiga taotletava eesmärgi suhtes, nõudis ELK, et siseriiklik kohus uuriks, kas sellist eesmärki saaks saavutada sama tulemuslikult vähem sekkuvate vahenditega, näiteks esitades isikuandmeid üksnes järelevalveasutustele, mitte üldsusele.

Järgmistes kohtuasjades selgus, et andmekaitse ja dokumentidele juurdepääsu tasakaalustamine nõuab iga juhtumi eraldi üksikasjalikku analüüsi. Kumbki õigus ei saa teist automaatselt tühistada. Euroopa Liidu Kohtul oli kahes kohtuasjas võimalus tõlgendada õigust saada juurdepääs isikuandmetega seotud dokumentidele.

Näide: kohtuasjas *Euroopa Komisjon vs. Bavarian Lager*[106] määratles Euroopa Liidu Kohus ELi institutsioonide dokumentidele juurdepääsu korral tagatava isikuandmete kaitse ulatuse ning määruse (EÜ) nr 1049/2001 (dokumentidele juurdepääsu käsitlev määrus) ja määruse (EÜ) nr 45/2001 (ELi institutsioonide andmekaitse määrus) vahelised seosed. 1992. aastal asutatud Bavarian Lager impordib Saksa pudeliõlut Ühendkuningriiki, peamiselt pubidele ja baaridele. Sellega tekkis aga probleeme, sest Briti õigusaktid soosisid *de facto* kodumaiseid tootjaid. Bavarian Lageri kaebuse peale algatas Euroopa Komisjon Ühendkuningriigi vastu liikmesriigi kohustuste rikkumise menetluse, mille järel muutis Ühendkuningriik asjaomaseid sätteid ja ühtlustas need 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 teatud

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

dokumendid koosoleku kohta, kuid kustutas koosoleku protokollist viis nime, sest kaks isikut olid selge sõnaga vastu oma isikuandmete avaldamisele ja kolmega ei saanud komisjon ühendust. 18. märtsi 2004 otsusega jättis komisjon rahuldamata Bavarian Lageri kordustaotluse tutvuda protokolli täisversiooniga, põhjendades seda eelkõige asjaomaste isikute eraelu kaitsega, mis on tagatud ELi institutsioonide andmekaitsemäärusega.

Et selline põhjendus ei olnud Bavarian Lagerile vastuvõetav, esitati hagi Esimese Astme Kohtusse. Nimetatud kohus tühistas komisjoni otsuse 8. novembri 2007. aasta otsusega (kohtuasi T-194/04, *Bavarian Lager Co. Ltd vs. Euroopa ühenduste komisjon*), arvestades, et üksnes asjaolu, et dokumendis oli asjaomaste asutuste esindajatena mainitud kõnealuste isikute nimesid, ei tähendanud tingimata eraelu austamise õiguse rikkumist ning see ei ohustanud nende eraelu.

Komisjoni apellatsioonkaebuse peale tühistas ELK Esimese Astme Kohtu otsuse. ELK leidis, et dokumentidele juurdepääsu määrus „kehtestab erikorra ja tugevdab niisuguse isiku kaitset, kelle isikuandmeid võidakse vajaduse korral üldsusele edastada". ELK järeldas, et kui dokumentidele juurdepääsu määruse alusel esitatud taotlusega soovitakse saada juurdepääsu isikuandmeid sisaldavatele dokumentidele, kohaldatakse kõiki ELi institutsioonide andmekaitsemääruse sätteid. Seejärel otsustas ELK, et komisjoni otsus jätta 1996. aasta oktoobris toimunud koosoleku protokolli täisversiooniga tutvumiseks esitatud taotlus rahuldamata oli õigustatud. Et komisjon ei saanud koosoleku viielt osalejalt nõusolekut nime avaldamiseks, täitis ta piisavalt selguse ja arusaadavuse kohustust, avaldades dokumendist versiooni, kust olid nende nimed eemaldatud.

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 [ELi institutsioonide andmekaitsemäärusele], kas on põhjust arvata, et andmete üleandmine kahjustaks andmesubjektide õigustatud huve."

Näide: kohtuasjas *Client Earth ja PAN Europe vs. EFSA*[107] uuris Euroopa Liidu Kohus, kas Euroopa Toiduohutusameti (EFSA) otsus keelduda lubamast taotlejatele täielikku juurdepääsu dokumentidele oli vajalik dokumentides viidatud isikute eraelu- ja andmekaitseõiguste kaitseks. Dokumendid käsitlesid taimekaitsevahendite turuleviimise suunisaruande kavandit, mille koostas EFSA töörühm koostöös välisekspertidega. Esialgu andis EFSA taotlejatele osalise juurdepääsu, keelates juurdepääsu mõnele suunisdokumendi kavandi variandile. Seejärel andis ta juurdepääsu kavandi versioonile, mis sisaldas väliseksperti märkusi. Ta kustutas ekspertide nimed, tuginedes määruse (EÜ) nr 45/2001 artikli 4 lõike 1 punktile b isikuandmete töötlemise kohta ELi institutsioonides ja asutustes ning vajadusele kaitsta välisekspertide eraelu puutumatust. Esimeses astmes kinnitas Euroopa Liidu Üldkohus EFSA otsust.

Kaebuse esitajate apellatsioonkaebuse peale tühistas ELK esimese astme otsuse. Kohus järeldas, et isikuandmete edastamine oli kõnealusel juhul vajalik, et tagada iga välieksperdi erapooletus ülesannete täitmisel teadlasena ja tagada, et EFSA otsustusprotsess oleks läbipaistev. ELK sõnul ei täpsustanud EFSA, kuidas suunisdokumendi kavandi kohta erimärkusi teinud väliseksperti nimede avaldamine kahjustaks ekspertide õigustatud huve. Üldine argument, et avalikustamine võib kahjustada eraelu puutumatust, ei ole piisav, kui seda ei toeta iga juhtumi korral konkreetsed tõendid.

Nende kohtuotsuste alusel tohib dokumentidele juurdepääsu korral sekkuda isikuandmete kaitse õigusesse üksnes konkreetsel ja õigustatud põhjusel. Dokumentidega tutvumise õigus ei tühista automaatselt õigust andmekaitsele[108].

See käsitlusviis sarnaneb Euroopa Inimõiguste Kohtu otsusega, mis käsitleb eraelu puutumatust ja juurdepääsu dokumentidele, nagu ilmneb järgmisest kohtuotsusest. Kohtuasjas *Magyar Helsinki* tehtud otsuses märkis Euroopa Inimõiguste Kohus, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 10 ei anna üksikisikule avaliku sektori asutuse valduses oleva teabega tutvumise õigust ega kohusta valitsust andma sellist teavet üksikisikule. Selline õigus või kohustus võib siiski tekkida: esiteks siis, kui teabe avalikustamise kohustus on pandud õigusliku jõu saanud kohtumäärusega; teiseks siis, kui juurdepääs teabele on oluline selleks,

107 ELK, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) vs. Euroopa Toiduohutusamet (EFSA), Euroopa Komisjon*, 16. juuli 2015.

108 Vt teisalt Euroopa andmekaitseinspektori (2011) üksikasjalikud kaalutlused dokumendis *„Public access to documents containing personal data after the Bavarian Lager ruling“*, Brüssel, 24. märts 2011.

et isik saaks kasutada õigust sõnavabadusele – eelkõige teabe saamise ja levitamise vabadusele –, ning kui selle keelamine riivab seda õigust[109]. Seda, kas ja mis ulatuses on teabele juurdepääsu keelamine sekkumine taotleja sõnavabadusse, tuleb hinnata igal kord eraldi ja arvestades konkreetseid asjaolusid, sealhulgas järgmist: i) teabenõude eesmärk; ii) taotletava teabe olemus; iii) taotleja roll ja iv) kas teave on valmis ja kättesaadav.

Näide: kohtuasjas *Magyar Helsinki Bizottság vs. Ungari*[110] taotles kaebuse esitaja, inimõiguste kaitse vabaühendus politseilt teavet *ex officio* kaitsja töö kohta, et saada valmis uuring riiklike kaitsjate määramise süsteemi toimimise kohta Ungaris. Politsei keeldus teabe esitamisest, väites, et tegu on isikuandmetega, mida ei avalikustata. Kohaldades eespool nimetatud kriteeriume, leidis EIK, et toimunud on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 alusel kaitstud õiguse riive. Täpsemalt öeldes soovis kaebuse esitaja kasutada õigust anda teavet üldist huvi pakkuvas küsimuses, taotles selleks juurdepääsu teabele ja teave oli vajalik kaebuse esitaja sõnavabaduse õiguse kasutamiseks. Riiklike kaitsjate määramine pakkus avalikkusele huvi. Ei olnud põhjust kahelda, et uuring sisaldas teavet, mida kaebuse esitaja kavatses avalikustada ja mida avalikkusel oli õigus saada. Seega oli kohus veendunud, et juurdepääs taotletud teabele oli kaebuse esitaja ülesande täitmiseks vajalik. Teave oli ka valmis ja kättesaadav.

EIK järeldas, et selles kohtuasjas kahjustas teabele juurdepääsu keelamine teabe saamise vabaduse sisu. Sellele järeldusele jõudmisel uuris kohus eelkõige taotletava teabe eesmärki ja panust olulisse avalikku arutellu, taotletava teabe olemust ja seda, kas see pakkus avalikku huvi, ning mis ühiskondlikku rolli täitis taotleja selles juhtumis.

Põhjendustes märkis kohus, et vabaühenduse korraldatud uuringus käsitleti kohtusüsteemi toimimist ja õigust õiglasele kohtumenetlusele, mis on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni kohaselt ülima tähtsusega õigus. Et taotletud teave ei hõlmanud üldkasutatava teabe valdkonnast väljapoole jäävaid andmeid, ei oleks see, kui politsei andnuks taotlejale teabele juurdepääsu, ohustanud asjaomaste andmesubjektide (*ex officio*

109 EIK, *Magyar Helsinki Bizottság vs. Ungari* [suurkoda], nr 18030/11, 8. november 2016, punkt 148.

110 *Ibid.*, punktid 181, 187–200.

riiklikud kaitsjad) õigust eraelu puutumatusele. Teave, mida kaebuse esitaja taotles, oli olemuselt statistiline ja käsitles seda, mitu korda oli *ex officio* kaitsja määratud esindama süüdistatavaid avalikus kriminaalmenetluses.

Kuivõrd uuringu eesmärk oli toetada olulist üldhuvi pakkuvat arutelu, oleks kohtu arvates pidanud vabaühenduse kavandatud avaldamisele mis tahes piiramist põhjalikult kontrollima. See teave pakkus avalikkusele huvi, sest avalik huvi hõlmab küsimusi, mis võivad tekitada märkimisväärseid vastuolusid, mis käsitlevad olulist sotsiaalset probleemi või mis on seotud probleemiga, mille kohta teabe saamisest oleks avalikkus huvitatud[111]. Seega hõlmaks see kindlasti arutelu õigusemõistmise ja õiglase kohtumenetluse üle, mis oli kaebuse esitaja uuringu teema. Tasakaalustades nimetatud eri õigusi ja kohaldades proportsionaalsuse põhimõtet, leidis Euroopa Inimõiguste Kohus, et kaebuse esitaja Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 kohaseid õigusi on põhjendamatult rikutud.

1.3.2. Kutsesaladus

Riigisisese õiguse kohaselt võib teatud teadete suhtes kohaldada kutsesaladuse hoidmise kohustust. Kutsesaladust võib pidada eriliseks eetikakohustuseks, mis tekitab teatud kutsealadele ja ülesannetele omase juriidilise kohustuse, mis põhineb usul ja usaldusel. Isikud ja asutused, kes täidavad selliseid ülesandeid, on kohustatud mitte avalikustama töökohustuste täitmisel saadud konfidentsiaalset teavet. Kutsesaladust kasutatakse eelkõige meditsiinitöötajate ja advokaadi-kliendi suhte korral, kusjuures paljudes jurisdiktsioonides kasutatakse kutsesaladuse hoidmise kohustust ka finantssektoris. Kutsesaladus ei ole põhiõigus, kuid seda kaitstakse eraelu austamise õiguse vormina. Näiteks on Euroopa Liidu Kohus otsustanud, et teatud juhtudel „võib tõepoolest osutuda vajalikuks keelata teatud konfidentsiaalse teabe avalikustamine, et kaitsta ettevõtja põhiõigust eraelu austamisele, mis on ette nähtud [...] inimõiguste ja põhivabaduste kaitse konventsiooni [...] artiklis 8 ja harta artiklis 7"[112]. Ka Euroopa Inimõiguste Kohtul on palutud otsustada, kas kutsesaladuse piiramine on konventsiooni artikli 8 rikkumine, nagu ilmneb esitatud näidetest.

111 *Ibid.*, punkt 156.

112 ELK, kohtuasi T-462/12, *Pilkington Group Ltd vs. Euroopa Komisjon*, Üldkohtu presidendi määrus, 11. märts 2013, punkt 44.

Näide: kohtuasjas *Pruteanu vs. Rumeenia*[113] esindas kaebuse esitaja juristina ärietteõõtet, kes oli saanud pettusesüüdistuse tõttu pangatehingute tegemise keelu. Juhtumi uurimise ajal andsid Rumeenia kohtud prokuratuurile teatud ajavahemikuks õiguse ettevõtte partneri telefonikõnesid pealt kuulata ja salvestada. Salvestused ja pealtkuulamised hõlmasid tema suhtlemist advokaadiga.

Alexandru Pruteanu väitis, et sellega sekkuti tema õigusesse eraelu ja sõnumisaladuse austamisele. Euroopa Inimõiguste Kohus rõhutas otsuses advokaadi-kliendi suhte staatust ja tähtsust. Advokaadi ja tema kliendi vestluste pealtkuulamisega rikuti kahtlemata kutsesaladuse hoidmise kohustust, mis oli nende suhte alus. Sellisel juhul võib advokaat esitada kaebuse ka enda eraelu ja sõnumisaladuse õiguse rikkumise kohta. ELK järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Näide: kohtuasi *Brito Ferrinho Bexiga Villa-Nova vs. Portugal*[114] käsitles juhtumit, kus kaebuse esitaja (advokaat) keeldus avalikustamast maksuhaldurile oma isiklikke pangaväljavõtteid, põhjendades seda ameti- ja pangasaladusega. Prokuratuur alustas maksupettuse uurimist ja taotles kutsesaladuse peatamist. Riigisisesed kohtud andsid korralduse kutse- ja pangasaladuse hoidmise eeskirjad peatada, leides, et avalikkuse huvi peaks olema taotleja erahuvide suhtes ülimuslik.

Kui asi jõudis Euroopa Inimõiguste Kohtusse, leidis kohus, et juurdepääsuga kaebuse esitaja pangaväljavõtetele sekkuti tema õigusesse kutsesaladuse austamisele, mis kuulub eraelu puutumatuse alla. Sekkumisel oli õiguslik alus, sest see põhines kriminaalmenetluse koodeksil ja selle eesmärk oli õigustpärane. Sekkumise vajalikkust ja proportsionaalsust uurides viitas Euroopa Inimõiguste Kohus siiski asjaolule, et konfidentsiaalsuse tühistamise menetlus toimus kaebuse esitaja osaluseta või teadmata. Hageja ei saanud seetõttu esitada oma argumente. Kuigi riigi õigus sätestas, et sellises menetluses tuleb konsulteerida juristide ühendusega, ei olnud ühendusega konsulteeritud. Kaebuse esitajal ei olnud võimalust konfidentsiaalsuse tühistamist vaidlustada ja selleks puudusid õiguskaitsevahendid. Menetlustagatiste ja

113 EIK, *Pruteanu vs. Rumeenia*, nr 30181/05, 3. veebruar 2015.

114 EIK, *Brito Ferrinho Bexiga Villa-Nova vs. Portugal*, nr 69436/10, 1. detsember 2015.

konfidentsiaalsuskohustuse peatamise meetme tõhusa kohtuliku kontrolli puudumise tõttu järeldas Euroopa Inimõiguste Kohus, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Kutsesaladuse ja andmekaitse vastastikmõju on sageli kaksipidine. Ühelt poolt aitavad õigusaktides kehtestatud andmekaitse-eeskirjad ja kaitsemeetmed tagada kutsesaladuse hoidmise. Näiteks eeskirjadega, mis nõuavad, et vastutavad ja volitatud töötlejad rakendaksid tugevaid andmekaitsemeetmeid, püütakse muu hulgas vältida seda, et kutsesaladusega kaitstud isikuandmed kaotaksid konfidentsiaalsuse. Lisaks võimaldab ELi isikuandmete kaitse üldmäärus töödelda terviseandmeid, mis on isikuandmete eriliik ja vajab tugevamat kaitset, kuid määrusega tehakse see sõltuvaks sellest, kas on olemas sobivad ja konkreetsed meetmed andmesubjektide õiguste, eelkõige kutsesaladuse kaitseks[115].

Teisalt võivad vastutavate ja volitatud töötlejate kutsesaladuse hoidmise kohustused teatud isikuandmete korral piirata andmesubjektide õigusi, eelkõige õigust saada teavet. Kuigi isikuandmete kaitse üldmäärus loetleb üksikasjalikult teabe, mis põhimõtteliselt tuleb esitada andmesubjektile, kui temalt ei ole saadud isikuandmeid, ei kohaldata seda avalikustamisnõuet, kui isikuandmed peavad jääma riigisisese või ELi õigusega nõutava kutsesaladuse hoidmise kohustuse tõttu salajaseks[116].

Isikuandmete kaitse üldmääruses sätestatakse, et liikmesriigid võivad oma õiguses võtta vastu erieeskirjad, et kaitsta kutse- või muu samaväärse saladuse hoidmise kohustusi ning ühitada õigus isikuandmete kaitsele kutsesaladuse hoidmise kohustusega[117].

Isikuandmete kaitse üldmääruses on sätestatud, et liikmesriigid võivad võtta vastu erieeskirjad järelevalveasutuste volituste kohta seoses vastutavate või volitatud töötlejatega, kelle suhtes kehtib kutsesaladuse hoidmise kohustus. Need erieeskirjad on seotud volitusega saada juurdepääs vastutava või volitatud töötleja ruumidele, nende andmetöötlusseadmetele ja nende valduses olevatele isikuandmetele, kui sellised isikuandmed on saadud saladuse hoidmise kohustusega hõlmatud tegevuse käigus. Seega peavad andmekaitse järelevalveasutused täitma vastutavatele ja volitatud töötlejatele kehtivaid kutsesaladuse hoidmise kohustusi. Lisaks on ka järelevalveasutuste liikmed kohustatud nii ametiaja jooksul kui ka hiljem hoidma

115 Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt h ja artikli 9 lõige 3.

116 *Ibid*., artikli 14 lõike 5 punkt d.

117 *Ibid*., põhjendus 164 ja artikkel 90.

kutsesaladust. Oma ülesannete täitmisel võivad järelevalveasutuste liikmed ja töötajad saada teada konfidentsiaalset teavet. Määruse artikli 54 lõikes 2 on selgelt sätestatud, et neil on sellise konfidentsiaalse teabe suhtes kutsesaladuse hoidmise kohustus.

Isikuandmete kaitse üldmääruses nõutakse, et liikmesriigid teavitaksid komisjoni eeskirjadest, mille nad võtavad vastu, et ühitada andmekaitse ja määruses sätestatud põhimõtted kutsesaladuse hoidmise kohustusega.

1.3.3. Usu- ja veendumusvabadus

Usu- ja veendumusvabadus on kaitstud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 9 (mõtte-, südametunnistuse- ja usuvabadus) ja ELi põhiõiguste harta artikli 10 alusel. Usulisi või filosoofilisi veendumusi paljastavaid isikuandmeid peetakse nii ELi kui ka Euroopa Nõukogu õiguse kohaselt eriliigiliseteks isikuandmeteks ning nende töötlemine ja kasutamine on tugevama kaitse all.

Näide: kaebuse esitaja kohtuasjas *Sinak Isik vs. Türgi*[118] oli aleviitide usukogukonna liige, kelle usul on sufismi ja muude islami-eelsete uskumuste mõjutusi ning mida osa teadlasi peab iseseisvaks religiooniks ja muud islami religiooni osaks. Hageja kaebas, et tema isikutunnistusel on tema tahte vastaselt märgitud, et tema religioon on islam ja mitte alevi. Riigisisesed kohtud lükkasid tagasi tema taotluse muuta isikutunnistuse märke tekstiks „alevi" põhjusel, et see sõna tähistab islami alarühma, mitte eraldi religiooni. Seejärel kaebas ta Euroopa Inimõiguste Kohtule, et oli kohustatud avaldama oma usu ilma nõusolekuta, sest isikutunnistusele oli kohustuslik märkida isiku religioon, ja et see rikub tema õigust usu- ja südametunnistusevabadusele, eriti arvestades, et määratlus „islam" tema isikutunnistusel on vale.

EIK kordas, et usuvabadus tähendab vabadust avaldada isiku usku kogukonnas koos teistega, avalikkuses ja sama usku jagavate isikute ringis, aga ka üksi ja eraviisiliselt. Tollal kehtinud riiklikud õigusaktid kohustasid isikuid kandma kaasas isikutunnistust ehk dokumenti, mida tuli näidata mis tahes riigiasutuse või eraettevõtja nõudel ja mis näitab isiku religiooni. Sellise kohustusega ei arvestatud, et õigus religiooni avaldada annab ka vastupidise õiguse, st õiguse mitte olla kohustatud avaldama oma usulisi veendumusi.

118 EIK, *Sinan Işık vs. Türgi*, nr 21924/05, 2. veebruar 2010.

Kuigi valitsus väitis, et riiklikke õigusakte on muudetud, nii et isikud võivad taotleda, et nende isikutunnistuse religiooni märge jäetaks tühjaks, võib kohtu arvates käsitada juba üksnes asjaolu, et religiooni märke kustutamist peab taotlema, sellena, et nii avalikustatakse teave nende suhtumise kohta religiooni. Lisaks sellele, kui isikutunnistustel on religiooni märge, on selle tühjaks jätmisel eriline tähendus, sest selliste isikutunnistuse omanikud, millel puudub religiooni teave, eristuvad nendest, kelle isikutunnistusel on nende veendumused märgitud. Kohus järeldas, et riigisisesed õigusaktid rikkusid Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 9.

Kirikute ja usuühenduste või kogukondade tegevuses võib siiski olla vaja liikmete isikuandmeid töödelda, et võimaldada suhtlust ja tegevuse korraldamist koguduses. Seega on kirikud ja usuühendused isikuandmete töötlemise eeskirju sageli rakendanud. Isikuandmete kaitse üldmääruse artikli 91 kohaselt võivad need eeskirjad jätkuvalt kehtida, kui need on põhjalikud ja kooskõlas määruse sätetega. Kirikuid ja usuühendusi, kellel on sellised eeskirjad, peab kontrollima sõltumatu järelevalveasutus, mis võib tegutseda üksnes nende suhtes, kui see täidab isikuandmete kaitse üldmääruses sellistele asutustele kehtestatud nõudeid[119].

Usuorganisatsioonid võivad isikuandmeid töödelda mitmel põhjusel: näiteks oma kogudusega ühenduse hoidmiseks või usu- või heategevusürituste ja pidustuste teabe edastamiseks. Teatud riikides peavad kirikud maksupõhjustel pidama liikmete registreid, sest usuorganisatsioonide liikmesus võib mõjutada isikute maksustamist. Igal juhul on Euroopa õiguse kohaselt usulisi veendumusi kajastavad andmed eriliigilised isikuandmed ning kirikud peavad vastutama nende andmete käitlemise ja töötlemise eest, eriti kuna usuorganisatsioonide töödeldav teave on sageli seotud laste, eakate või ühiskonna muude haavatavate liikmetega

1.3.4. Kunsti ja teaduse vabadus

Veel üks õigus, mida tuleb arvestada seoses õigusega eraelu austamisele ja isikuandmete kaitsele, on kunsti ja teaduse vabadus, mille kaitsmist nimetatakse otseselt ELi põhiõiguste harta artiklis 13. See õigus tuleneb peamiselt mõtte- ja sõnavabadusest ning selle kasutamisel arvestatakse harta artiklit 1 („Inimväärikus"). Euroopa Inimõiguste Kohtu järgi on kunstivabaduse kaitse tagatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 10[120]. Harta artikliga 13 tagatud õiguse

119 Isikuandmete kaitse üldmääruse artikli 91 lõige 2.

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

suhtes võidakse samal ajal kohaldada kooskõlas harta artikli 52 lõikega 1 piiranguid, mida võib tõlgendada ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 alusel[121].

Näide: kohtuasi *Vereinigung bildender Künstler vs. Austria*[122] käsitles juhtumit, kus Austria kohtud keelasid kaebuse esitanud ühendusel jätkata sellise maali eksponeerimist, millel olid avaliku elu tegelaste peade fotod, mis kujutasid neid suguühtes. Teosel kasutatud fotol olnud Austria parlamendiliige pöördus kaebuse esitanud ühenduse vastu kohtusse ning taotles tõkendit, et maali enam ei eksponeeritaks. Riigisisene kohus seadis tõkendi. EIK toonitas, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 10 laieneb selliste ideede edastamisele, mis solvavad, šokeerivad või häirivad riiki või elanikkonna mis tahes rühma. Kunstiteoseid loovad, esitavad, levitavad või eksponeerivad isikud toetavad ideede ja arvamuste vahetamist ning riik ei tohi nende väljendusvabadust liigselt piirata. Kuivõrd maal oli kollaažitehnikas, fotod olid üksnes asjaomaste isikute peadest ja kehad olid maalitud ebarealistlikult ja kunstilise liialdusega, millega ilmselgelt ei soovitud kajastada tegelikkust ega sellele vihjata, märkis EIK samuti, et on ebatõenäoline, et autori eesmärk oli jäljendada asjaomase isiku eraelu, vaid pigem soovis ta näidata tema avalikku staatust poliitikuna, ning et seda arvestades peaks asjaomane isik üles näitama suuremat sallivust kriitika suhtes. Olles analüüsinud asjaomaseid eri huve, leidis EIK, et maali edasise eksponeerimise tähtajatu keeld oli ebaproportsionaalne. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 10.

Euroopa andmekaitseõiguses tunnustatakse ka teaduse erilist väärtust ühiskonnas. Isikuandmete kaitse üldmäärus ja nüüdisajastatud konventsioon nr 108 lubavad säilitada andmeid pikema aja jooksul, kui isikuandmeid töödeldakse üksnes teadus- või ajaloouuringute eesmärkidel. Peale selle ja olenemata konkreetse töötlemise esialgsest eesmärgist ei peeta isikuandmete edasist kasutamist teadusuuringutes nõuetega kokkusobimatuks eesmärgiks[123]. Samal ajal tuleb sellisel töötlemisel rakendada andmesubjektide õiguste ja vabaduste kaitseks asjakohaseid kaitsemeetmeid. ELi või liikmesriikide õigusaktides võidakse sätestada andmesubjekti õiguste erandeid,

121 Selgitused põhiõiguste harta kohta, ELT 2007 C 303.

122 EIK, *Vereinigung bildender Künstler vs. Austria*, nr 68354/01, 25. jaanuar 2007, punktid 26 ja 34.

123 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt b ja nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b.

näiteks õigusest andmetega tutvuda, neid parandada ja nende töötlemist piirata ning vaidlustada isikuandmete töötlemine teadus- ja ajaloouuringute või statistilisel eesmärgil (vt ka peatükk 6.1 ja peatükk 9.4).

1.3.5. Intellektuaalomandi kaitse

Õigus omandi kaitsele on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni esimese protokolli artiklis 1 ja ELi põhiõiguste harta artikli 17 lõikes 1. Seoses õigusega omandile on isikuandmete kaitse seisukohast eriti oluline intellektuaalomandi kaitse, mida on selge sõnaga nimetatud harta artikli 17 lõikes 2. ELi õiguskorras on mitu direktiivi, mille eesmärk on tagada intellektuaalomandi, eelkõige autoriõiguse tõhus kaitse. Intellektuaalomand hõlmab peale kirjandus- ja kunstiteoste ka patente, kaubamärke ja nendega seonduvaid õigusi.

Nagu on selgitanud Euroopa Liidu Kohtu praktika, tuleb omandiõiguse kui põhiõiguse kaitse tasakaalustada teiste põhiõiguste kaitsega, eelkõige õigusega isikuandmete kaitsele[124]. On olnud juhtumeid, kus autoriõiguste kaitse asutused on nõudnud, et internetiühenduse pakkujad avalikustaksid failijagamise internetiplatvormide kasutajate isikud. Selliste platvormide kaudu saavad internetikasutajad sageli tasuta alla laadida ka autoriõigusega kaitstud lugusid.

Näide: kohtuasi *Promusicae vs. Telefónica de España*[125] käsitles juhtumit, kus Hispaania internetiühenduse pakkuja Telefónica keeldus avaldamast muusikaprodutsente ning heli- ja audiovisuaalsete salvestiste väljaandjaid koondavale vabaühendusele Promusicae isikuandmeid konkreetsete isikute kohta, kellele osutati internetiühenduse teenuseid. Promusicae taotles teabe avaldamist, et asjaomaste isikute vastu saaks algatada tsiviilkohtumenetluse, sest vabaühenduse väitel kasutasid nad failivahetusprogrammi, mis võimaldas juurdepääsu salvestistele, mille varalised kasutusõigused kuulusid Promusicae liikmetele.

Hispaania kohus edastas asja ELK-le, küsides, kas selliste isikuandmete edastamist tsiviilkohtumenetluse raames nõutakse ühenduse õiguse alusel autoriõiguse tõhusa kaitse tagamiseks. Kohus viitas direktiividele 2000/31/EÜ, 2001/29/EÜ ja 2004/48/EÜ koostoimes harta artiklitega 17 ja 47. ELK järeldas,

124 ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU* [suurkoda], 29. jaanuar 2008, punktid 62–68.

125 *Ibid.*, punktid 54 ja 60.

et need kolm direktiivi, samuti eraelu puutumatuse ja elektroonilise side direktiiv (direktiiv 2002/58/EÜ) ei välista liikmesriikide võimalust sätestada autoriõiguse tõhusa kaitse eesmärgil kohustust edastada tsiviilkohtumenetluse raames isikuandmeid.

ELK rõhutas, et kohtuasi tõstatas seega küsimuse, kuidas ühitada selliste erinevate põhiõiguste kaitse nõudeid nagu õigus eraelu puutumatusele, õigus omandiõiguse kaitsele ja 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.“[126]

Näide: kohtuasi *Bonnier Audio AB jt vs. Perfect Communication Sweden AB*[127] käsitles intellektuaalomandiõiguste ja isikuandmete kaitse tasakaalu. Kaebuse esitajad – viis kirjastusettevõtet, kes on 27 audioraamatu autoriõiguse omanikud – esitasid Rootsi kohtusse hagi, väites, et nende autoriõigust on rikutud FTP-serveri abil (failiedastusprotokoll, mis võimaldab failide jagamist ja andmeedastust interneti kaudu). Taotlejad nõudsid internetiteenuse osutajalt failid saatnud IP-aadressi kasutanud isiku nime ja aadressi avaldamist. Internetiteenuse osutaja ePhone vaidlustas hagiavalduse, väites, et sellega rikuti direktiivi 2006/24/EÜ (andmete säilitamise direktiiv – tunnistati kehtetuks 2014. aastal).

Rootsi kohus edastas asja Euroopa Liidu Kohtule, küsides, kas direktiiv 2006/24/EÜ välistab direktiivi 2004/48/EÜ (intellektuaalomandiõiguste jõustamise direktiiv) artiklil 8 põhineva liikmesriigi õigusnormi kohaldamise, mis võimaldab teha ettekirjutuse, millega nõutakse internetiteenuse osutajatelt teabe edastamist autoriõiguste omajatele abonentide kohta, kelle

126 *Ibid.*, punktid 65 ja 68; vt ka ELK, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vs. Netlog NV*, 16. veebruar 2012.

127 ELK, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB vs. Perfect Communication Sweden AB*, 19. aprill 2012.

IP-aadresse väidetavalt rikkumiste toimepanemisel kasutati. Küsimus põhines eeldusel, et kaebuse esitaja esitas selgeid tõendeid konkreetse autoriõiguse rikkumise kohta ja meede on proportsionaalne.

ELK märkis, et direktiivis 2006/24/EÜ käsitleti ainult elektroonilise side teenuste osutajate loodud andmete töötlemist ja säilitamist raskete kuritegude uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks ning nende andmete edastamist riigi pädevatele asutustele. Seega jääb intellektuaalomandiõiguste jõustamise direktiivi ülevõttev riiklik säte direktiivi 2006/24/EÜ kohaldamisalast välja ja seepärast see direktiiv seda ei välista[128].

Taotluse esitajate taotletud nime ja aadressi teatamise kohta leidis ELK, et see on isikuandmete töötlemine ja kuulub direktiivi 2002/58/EÜ (e-privaatsuse direktiiv) kohaldamisalasse. Kohus märkis ka, et nende andmete edastamine oli tsiviilkohtumenetluses nõutav autoriõiguse omaniku kasuks, et tagada autoriõiguse tõhus kaitse, ja seega kuulub see ka direktiivi 2004/48/EÜ kohaldamisalasse[129].

ELK järeldas, et direktiive 2002/58/EÜ ja 2004/48/EÜ tuleb tõlgendada nii, et need ei välistaks sellist riigisisest õigusakti, nagu käsitletakse põhikohtuasjas, sest need õigusaktid võimaldavad isikuandmete avalikustamise taotlust menetleval riiklikul kohtul kaalutleda vastandlikke huve, lähtudes iga juhtumi asjaoludest ja nõuetekohaselt arvestades proportsionaalsuse põhimõtte nõudeid.

1.3.6. Andmekaitse ja majanduslikud huvid

Digiajastul ehk suurandmete ajastul on andmete kohta öeldud, et need on majanduses innovatsiooni ja loovuse edendamise „uus nafta“[130]. Paljud ettevõtted on loonud andmetöötluse ümber tugevad ärimudelid ja see töötlemine hõlmab sageli isikuandmeid. Osa äriühinguid võib arvata, et isikuandmete kaitse erieeskirjad võivad tegelikkuses tekitada liiga koormavaid kohustusi, mis võivad kahjustada nende majandushuve. Seega tekib küsimus, kas vastutavate ja volitatud töötlejate või üldsuse majandushuvid võivad õigustada andmekaitseõiguse piiramist.

128 *Ibid.*, punktid 40–41.

129 *Ibid.*, punktid 52–54. Vt ka ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU* [suurkoda], 29. jaanuar 2008, punkt 58.

130 Vt näiteks Financial Times (2016), *Data is the new oil... who's going to own it?*, 16. november 2016.

Näide: kohtuasjas *Google Spain*[131] leidis ELK, et teatud tingimustel on isikutel õigus nõuda otsingutulemuste eemaldamist oma otsinguregistrist. ELK märkis põhjendustes, et otsingumootorite ja loetletud otsingutulemuste kasutamine võib luua isiku üksikasjaliku profiili. See teave võib käsitleda üksikisiku eraelu ulatuslikku osa ja ilma otsingumootorita ei oleks seda olnud lihtne leida ega seostada. Seega oli tegu võimaliku raske sekkumisega andmesubjektide põhiõigustesse eraelu puutumatusele ja isikuandmete kaitsele.

Euroopa Kohus uuris seejärel, kas sekkumine võib olla õigustatud. Otsingumootorit käitava äriühingu majandushuvi kohta töötlemisel märkis ELK, et „tuleb tõdeda, et riivet ei saa õigustada pelgalt otsingumootori haldaja majandushuviga sellise töötlemise suhtes", ja et põhiõiguste harta artiklites 7 ja 8 sätestatud põhiõigused on üldjuhul ülimuslikud selliste majandushuvide ja üldsuse huvi suhtes vastava isiku nime põhjal tehtud otsinguga seda teavet leida[132].

Euroopa andmekaitseõiguse üks peamisi kaalutlusi on anda üksikisikutele suurem voli oma isikuandmete üle. Eriti digiajastul on palju suurem nende äriühingute mõjuvõim, kellel on juurdepääs tohutule kogusele isikuandmetele ja kes neid töötlevad, kui nende isikuandmete omanike mõjuvõim hallata oma teavet. Euroopa Liidu Kohus käsitleb andmekaitse ja majandushuvide – näiteks kolmandate isikute huve piiratud vastutusega äriühingute korral – tasakaalustamisel igat juhtumit eraldi, nagu näitab ilmekalt kohtuasjas *Manni* tehtud otsus.

Näide: kohtuasi *Manni*[133] käsitles isiku andmete lisamist avalikku äriregistrisse. Salvatore Manni palus Lecce kaubanduskojal kustutada registrist tema isikuandmed, kui ta avastas, et võimalikud kliendid nägid registrist, et ta on hallanud ettevõtet, mis läks rohkem kui kümmekond aastat tagasi pankrotti. See teave tekitas tema potentsiaalsetes klientides eelarvamust ja võis kahjustada tema ärihuve.

131 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014.

132 *Ibid.*, punktid 81 ja 97.

133 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 9. märts 2017.

ELK-l paluti määrata, kas ELi õiguses tunnustatakse sellisel juhul õigust andmete kustutamisele. Sellele järeldusele jõudmisel tasakaalustas kohus ELi andmekaitse-eeskirju ja Salvatore Manni ärihuvi kõrvaldada teave tema endise äriühingu pankroti kohta avalikkuse huviga teabele juurdepääsu suhtes. Kohus võttis teadmiseks asjaolu, et äriühingute avalikule registrile avalikustamine oli sätestatud seaduses ja eelkõige ELi direktiivis, mille eesmärk on lihtsustada äriühingute teabe kättesaadavust kolmandatele isikutele. Avalikustamine oli oluline, et kaitsta kolmandate isikute huve, kes võivad soovida teha äri teatud äriühinguga, sest piiratud vastutusega äriühingud vastutavad kolmandate isikute ees ainult oma varadega. Seega „peab avalikustamine võimaldama kolmandatel isikutel tutvuda äriühingu põhidokumentide sisuga ja muu äriühingut puudutava teabega, eelkõige andmetega isikute kohta, kellel on õigus äriühingut esindada“[134].

Arvestades registri õiguspärase eesmärgi tähtsust, leidis Euroopa Liidu Kohus, et Salvatore Mannil ei olnud õigust oma isikuandmete kustutamisele, sest vajadus kaitsta kolmandate isikute huve seoses piiratud vastutusega äriühingutega ning tagada õiguskindlus, õiglane kaubandus ja seega siseturu nõuetekohane toimimine kaalus üles tema andmekaitse õigusaktidest tulenevad õigused. Seda eriti seetõttu, et üksikisikud, kes otsustavad osaleda kaubanduses piiratud vastutusega äriühingu kaudu, on teadlikud, et nad peavad avalikustama oma identiteedi ja ametikohtade teabe.

Kuigi ELK leidis, et sellisel juhul ei ole põhjust andmeid kustutada, tõdes ta, et on olemas õigus esitada vastuväiteid töötlemise kohta, märkides: „ei saa [...] välistada, et võivad esineda eriolukorrad, kus õigustatud ja veenvad põhjused, mis on seotud andmesubjekti konkreetse juhtumiga, õigustavad erandkorras seda, et pärast piisavalt pika aja möödumist [...] on äriühingute registrisse kantud seda isikut puudutavate isikuandmetega tutvumine piiratud kolmandate isikutega, kellel on erihuvi nendega tutvuda“[135].

ELK märkis, et riigisiseste kohtute ülesanne on hinnata iga kord eraldi ja isiku kõiki asjakohaseid asjaolusid arvestades hinnata selliste õiguspäraste ja ülekaalukate põhjuste olemasolu või puudumist, mis võib erandkorras õigustada kolmandate isikute juurdepääsu piiramist äriühingute registrites sisalduvatele isikuandmetele. Kohus selgitas siiski, et Salvatore Manni korral

134 *Ibid*., punkt 49.

135 *Ibid*., punkt 60.

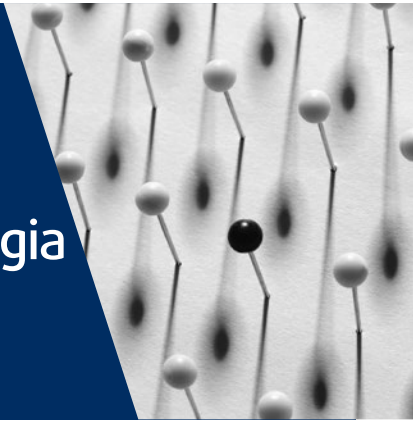
ei saa ainuüksi asjaolu, et tema isikuandmete avaldamine registris väidetavalt mõjutas tema kliente, lugeda selliseks õigustatud ja ülekaalukaks põhjuseks. Salvatore Manni võimalikel klientidel on õigustatud huvi saada teavet tema eelmise ettevõtte pankroti kohta.

Salvatore Manni ja teiste registrisse kantud isikute põhiõiguste riive eraelu austamise ja isikuandmete kaitse suhtes, mis on tagatud harta artiklitega 7 ja 8, täitis üldhuvi eesmärki ning oli vajalik ja proportsionaalne.

Kohtuasjas *Manni* leidis Euroopa Liidu Kohus seega, et õigus andmekaitsele ja eraelu puutumatusele ei kaalunud üles kolmandate isikute huvi saada juurdepääs äriühingute registris olevale teabele piiratud vastutusega äriühingute kohta.

2

Andmekaitse terminoloogia



EL	Teemad	EN
Isikuandmed		
Isikuandmete kaitse üldmääruse artikli 4 punkt 1 Isikuandmete kaitse üldmääruse artikli 4 punkt 5 ja artikli 5 lõike 1 punkt e Isikuandmete kaitse üldmääruse artikkel 9 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen* [suurkoda], 2010 ELK, C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU* [suurkoda], 2008 ELK, C-70/10, *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 ELK, C-582/14, *Patrick Breyer vs. Bundesrepublik Deutschland*, 2016 ELK, liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 2014	**Andmekaitse õiguslik määratlus**	Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt a EIK, *Bernh Larsen Holding AS and Others vs. Norra*, nr 24117/08, 2013 EIK, *Uzun vs. Saksamaa*, nr 35623/05, 2010 EIK, *Amann vs. Šveits* [suurkoda], nr 27798/95, 2000
ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 2003	**Eriliigilised isikuandmed (delikaatsed isikuandmed)**	Nüüdisajastatud konventsiooni nr 108 artikli 6 lõige 1

EL	Teemad	EN
ELK, C-434/16, *Peter Nowak vs. Data Protection Commissioner*, 2017	**Isikuandmete anonüümimine ja pseudo-nüümimine**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt e Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 50
Andmetöötlus		
Isikuandmete kaitse üldmääruse artikli 4 lõige 2 ELK, C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 2014 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 2017 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 2003 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 2014	**Mõisted**	Nüüdisajastatud konventsiooni nr 108 artikli 2 punktid b ja c
Andmete kasutajad		
Isikuandmete kaitse üldmääruse artikli 4 lõige 7 ELK, C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 2014 ELK, C-1318/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 2014	**Vastutav töötleja**	Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt d Profiilianalüüsi soovituse artikli 1 punkt g*
Isikuandmete kaitse üldmääruse artikli 4 lõige 8	**Volitatud töötleja**	Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt f Profiilianalüüsi soovituse artikli 1 punkt h
Isikuandmete kaitse üldmääruse artikli 4 lõige 9	**Vastuvõtja**	Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt e
Isikuandmete kaitse üldmääruse artikli 4 lõige 10	**Kolmas isik**	

EL	Teemad	EN
Nõusolek		
Isikuandmete kaitse üldmääruse artikli 4 punkt 11 ja artikkel 7 ELK, C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 2011 ELK, C-536/15, *Tele2 (Netehrlands) BV jt vs. Autoriteit Consument en Markt (AMC)*, 2017	**Kehtiva nõusoleku mõiste ja nõuded**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2 Meditsiiniandmete kaitse soovituse artikkel 6 ja muud hilisemad soovitused EIK, *Elberte vs. Läti*, nr 61243/08, 2015

*Märkus: * Euroopa Nõukogu ministrite komitee (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (profiilianalüüsi soovitus), 23. november 2010.*

2.1. Isikuandmed

Põhipunktid

- Andmed on isikuandmed, kui andmed on seotud tuvastatud või tuvastatava isikuga (andmesubjektiga).
- Kontrollimisel, kas füüsiline isik on tuvastatav, peab vastutav töötleja või muu isik arvestama kõiki mõistlikke vahendeid, mida tõenäoliselt kasutatakse füüsilise isiku otseseks või kaudseks tuvastamiseks, näiteks teiste hulgast esiletoomist.
- Autentimisega tõendatakse isiku isikusamasus ja/või see, et ta tohib teha teatud toiminguid.
- Osa andmeid on andmete eriliigid – eriliigilised isikuandmed, mis on loetletud nüüdisajastatud konventsioonis nr 108 ja andmekaitse õigusaktides –, mille jaoks on nõutav tugevdatud kaitse ning seega kehtib nende suhtes eri õiguskord.
- Andmed on anonüümitud, kui need ei seostu enam tuvastatud ega tuvastatava isikuga.
- Andmete pseudonüümimisega välistatakse isikuandmete seostamine andmesubjektiga ilma täiendava teabeta, mida hoitakse eraldi. Võti, mis võimaldab andmesubjekte uuesti tuvastada, tuleb hoida eraldi ja turvaliselt. Pseudonüümitud andmed jäävad isikuandmeteks. ELi õiguses puudub pseudonüümitud andmete mõiste.
- Anonüümitud andmete suhtes andmekaitse põhimõtteid ja eeskirju ei kohaldata, kuid neid kohaldatakse pseudonüümitud andmete suhtes.

2.1.1. Isikuandmete mõiste põhiaspektid

ELi ja **Euroopa Nõukogu õiguses** on isikuandmed määratletud kui teave tuvastatud või tuvastatava füüsilise isiku kohta[136]. See tähendab teavet isiku kohta, kelle isik on kas iseenesest selge või selle saab tuvastada täiendava teabe põhjal. Kontrollimisel, kas isik on tuvastatav, peab vastutav töötleja või muu isik arvestama kõiki mõistlikke vahendeid, mida tõenäoliselt kasutatakse füüsilise isiku otseseks või kaudseks tuvastamiseks, näiteks teiste hulgast esiletoomist, mis võimaldab käsitleda üht isikut teisiti kui muid[137].

Kui sellise isiku andmeid töödeldakse, on ta andmesubjekt.

Andmesubjekt

ELi õiguse kohaselt on andmekaitse-eeskirjad suunatud ainult füüsilistele isikutele[138] ja Euroopa andmekaitseõiguses on kaitse tagatud üksnes elus olevatele isikutele[139]. Isikuandmete kaitse üldmääruses määratletakse isikuandmed kui igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta.

Euroopa Nõukogu õiguses, eelkõige nüüdisajastatud konventsioonis nr 108, viidatakse ka üksikisikute kaitsele seoses nende isikuandmete töötlemisega. Ka seal tähendavad isikuandmed teavet tuvastatud või tuvastatava isiku kohta. Füüsilist isikut (nagu on isikuandmete kaitse üldmääruses) ja üksikisikut (nüüdisajastatud konventsioonis nr 108) nimetatakse andmekaitseõiguses andmesubjektiks.

Mõningast kaitset saavad ka juriidilised isikud. Euroopa Inimõiguste Kohtu kohtupraktikas on otsuseid hagiavalduste kohta, milles juriidilised isikud väitsid, et on rikutud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 neile antud õigust kaitsele andmete kasutamise vastu. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 hõlmab nii õigust era- ja perekonnaelu kui ka kodu ja sõnumite saladuse austamisele. Seega võib kohus pigem uurida juhtumeid viimasena nimetatu kui eraelu raames.

136 Isikuandmete kaitse üldmääruse artikli 4 punkt 1 ja nüüdisajastatud konventsiooni nr 108 artikli 2 punkt a.

137 Isikuandmete kaitse üldmääruse põhjendus 26.

138 *Ibid.*, artikkel 1.

139 *Ibid.*, põhjendus 27. Vt ka artikli 29 töörühm (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20. juuni 2007, lk 22.

Näide: kohtuasi *Bernh Larsen Holding AS jt vs. Norra*[140] käsitles kolme Norra äriühingu kaebust maksuhalduri otsuse suhtes, millega nõuti, et nad esitaksid maksuaudiitoritele koopia kõigist nende ühiskasutuses olnud arvutiserveris olnud andmetest.

EIK leidis, et kaebuse esitanud äriühingutele sellise kohustuse määramisega riivati nende õigusi seoses kodu ja sõnumite saladuse austamisega Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaselt. Kohus leidis siiski, et maksuhaldur oli väärkasutamise takistamiseks kehtestanud tõhusad ja piisavad kaitsemeetmed: kaebuse esitajaid teavitati aegsasti ette; nad viibisid kohapealse kontrolli juures ja neil oli võimalus ametnikega suhelda; materjal kavatseti pärast maksuauditi lõpetamist hävitada. Seda silmas pidades oli olemas õiglane tasakaal seoses ühelt poolt kaebuse esitanud ettevõtjate õigusega kodu ja sõnumite saladuse austamisele ning nende heaks töötavate inimeste eraelu puutumatuse kaitsmise huviga ja teisalt avaliku huviga tagada tõhus kontroll maksuseisundi hindamiseks. Kohus järeldas, et seega artiklit 8 ei rikutud.

Nüüdisajastatud konventsiooni nr 108 kohaselt hõlmab andmekaitse peamiselt füüsiliste isikute andmete kaitset, kuid konventsiooniosalised võivad seda oma riigisisestes õigusaktides laiendada juriidilistele isikutele, näiteks äriühingutele ja ühendustele. Nüüdisajastatud konventsiooni seletuskirjas on märgitud, et riigisisene õigus võib kaitsta juriidiliste isikute õigustatud huve, laiendades konventsiooni kohaldamisala sellistele osalejatele[141]. **ELi andmekaitseõigus** ei hõlma juriidilisi isikuid käsitlevat andmetöötlust, eelkõige ei puuduta see juriidilise isikuna asutatud ettevõtjaid, sealhulgas juriidilise isiku nime ja vormi ning kontaktandmeid[142]. Samas kaitseb side konfidentsiaalsust ja juriidiliste isikute õigustatud huve abonentide ja kasutajate andmete automaatse salvestamise ja töötlemise suureneva mahu korral e-privaatsuse direktiiv[143]. Juriidilistele isikutele laiendatakse kaitset ka e-privaatsuse määruse eelnõus.

140 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.

141 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 30.

142 Isikuandmete kaitse üldmääruse põhjendus 14.

143 E-privaatsuse direktiivi põhjendus 7 ja artikli 1 lõige 2.

Näide: kohtuasjas *Volker und Markus Schecke ja Hartmut Eifert vs. Land Hessen*[144] 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 [...].“[145]

Tasakaalustades ühelt poolt ELi huvi tagada läbipaistvus ning teisalt toetust saanud üksikisikute põhiõigused eraelu puutumatusele ja andmekaitsele, leidis ELK, et nende põhiõiguste riive oli ebaproportsionaalne. Kohus leidis, et läbipaistvuse eesmärgi oleks saanud tulemuslikult saavutada meetmetega, mis sekkuvad vähem asjaomaste üksikisikute õigustesse. Toetust saanud juriidiliste isikute teabe avaldamise proportsionaalsuse uurimisel jõudis ELK siiski teistsugusele järeldusele ja otsustas, et selline avaldamine ei ületanud proportsionaalsuse põhimõtte piire. Kohus märkis, et „[i]sikuandmete kaitse õiguse riive raskus on juriidiliste ja füüsiliste isikute puhul erinev“[146]. Juriidilistel isikutel on suurem kohustus avaldada enda kohta andmeid. ELK järeldas, et riigi ametiasutuste kohustus uurida enne selliste andmete avaldamist iga toetust saanud juriidilise isiku kohta, kas tema nime alusel on tuvastatavad füüsilised isikud, paneks neile ametiasutustele ebamõistlikult suure halduskoormuse. Seepärast on õigusaktid, millega nõutakse juriidiliste isikute andmete üldist avaldamist, saavutanud kõnealuste konkureerivate huvide õiglase tasakaalu.

Andmete olemus

Mis tahes liiki andmed võivad olla isikuandmed, kui need seonduvad tuvastatud või tuvastatava isikuga.

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

145 *Ibid.*, punktid 52–53.

146 *Ibid.*, punkt 87.

Näide: töötaja töötulemuste hinnang juhilt, mida säilitatakse töötaja isikutoimikus, on isikuandmed töötaja kohta. See on nii isegi siis, kui hinnangu sisu on osaliselt või täielikult üksnes juhi isiklik arvamus, näiteks „töötaja ei ole tööle pühendunud", mitte faktid, näiteks „töötaja puudus viimase kuue kuu jooksul töölt viis nädalat".

Isikuandmed on ka teave isiku eraelu kohta, sealhulgas kutsetegevuse kohta, ja ühiskondliku elu kohta.

Kohtuasjas *Amann*[147] tõlgendas EIK terminit „isikuandmed" nii, et see ei piirdu üksnes isiku eraeluga. Termini „isikuandmed" selline määratlus on asjakohane ka isikuandmete kaitse üldmääruse seisukohast.

Näide: kohtuasjas *Volker und Markus Schecke ja Hartmut Eifert vs. Land Hessen*[148] märkis ELK: „Selles suhtes ei ole tähtsust asjaolul, et avaldatud andmed seonduvad kutsealase tegevusega [...]. Euroopa Inimõiguste Kohus on Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni 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"[...]."

Näide: liidetud kohtuasjades *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*[149] märkis Euroopa Liidu Kohus, et sisserände- ja kodakondsusameti otsuse eelnõus sisalduv õiguslik analüüs, mis käsitleb elamisloa taotlusi, ei ole iseenesest isikuandmed, isegi kui need võivad sisaldada mõningaid isikuandmeid.

EIK kohtupraktika seoses Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 näitab, et eraelu ja kutsetegevuse küsimuste eristamine võib olla keerukas[150].

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

148 ELK, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen* [suurkoda], 9. november 2010, punkt 59.

149 ELK, liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 17. juuli 2014, punkt 39.

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

Näide: kohtuasi *Bărbulescu vs. Rumeenia*[151] käsitles juhtumit, kus kaebuse esitaja vallandati tööandja internetiühenduse töö ajal kasutamise tõttu, mis oli töökorra rikkumine. Kaebuse esitaja tööandja oli jälginud tema teabevahetust ja riigisiseses kohtumenetluses esitati üksnes erasõnumeid näitavad logiandmed. EIK leidis, et artikkel 8 on kohaldatav, kuid jättis lahtiseks küsimuse, kas tööandja piiravad eeskirjad jätavad taotlejale õigustatud ootuse eraelu puutumatusele, kuid oli igal juhul seisukohal, et tööandja juhised ei saa likvideerida era- ja ühiskondlikku elu töökohas. Sisulisest küljest tuli konventsioonis osalevatele riikidele anda ulatuslik kaalutlusõigus, kui nad hindavad vajadust luua õigusraamistik, mis hõlmab tingimusi, mille alusel tööandja võib reguleerida oma töötajate töövälist – elektroonilist või muud – teabevahetust töökohal. Riigisisesed ametiasutused peavad siiski tagama, et tööandjate poolt sõnumite ja muu teabevahetuse jälgimise meetmete kehtestamisega, olenemata meetmete ulatusest ja kestusest, kaasnevad asjakohased ja piisavad kaitsemeetmed kuritarvitamise vastu. Proportsionaalsus ja omavolivastased menetlustagatised on hädavajalikud ning Euroopa Inimõiguste Kohus tuvastas mitu nende asjaolude seisukohast olulist tegurit, näiteks mis ulatuses tööandjad töötajaid jälgivad, töötajate eraelu puutumatusse sekkumise ulatus, tagajärjed töötajale ning see, kas tagatud on piisavad kaitsemeetmed. Peale selle peavad riigisisesed ametiasutused tagama, et töötajale, kelle teabevahetust on jälgitud, on juurdepääs õiguskaitsevahendile kohtus, kelle pädevuses on vähemalt sisuliselt määrata, kuidas neid kriteeriume järgiti ja kas vaidlustatud meetmed olid seaduslikud. Kohtuasjas tuvastas Euroopa Inimõiguste Kohus konventsiooni artikli 8 rikkumise, sest riigisisesed ametiasutused ei pakkunud piisavat kaitset kaebuse esitaja õigusele eraelu ja sõnumisaladuse austamisele ning ei suutnud seega õiglaselt tasakaalustada asjaomaseid huve.

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

- selles teabega tuvastatakse isik või isik on tuvastatav või
- tuvastamata isikut saab selle teabe abil teiste hulgast nii esile tuua, et selle alusel saab lisauurimise abil välja selgitada andmesubjekti.

151 EIK, *Bărbulescu vs. Rumeenia* [suurkoda], nr 61496/08, 5. september 2017, punkt 121.

Mõlemat liiki teavet kaitstakse Euroopa andmekaitseõiguses samamoodi. Üksikisikute otsene või kaudne tuvastatavus eeldab pidevat hindamist, „võttes arvesse nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid“[152]. Euroopa Inimõiguste Kohus on korduvalt märkinud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis kasutatav mõiste „isikuandmed“ on sama kui konventsioonis nr 108, eriti seoses tuvastatud või tuvastatavate isikutega seotuse tingimusega[153].

Isikuandmete kaitse üldmääruses on sätestatud, et „tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal“[154]. Tuvastamine nõuab seega elemente, mis kirjeldavad isikut nii, et ta on eristatav kõigist muudest inimestest ja on isikuna äratuntav. Sellised kirjeldavad tunnused on eelkõige isiku nimi, millega võidakse isik otseselt tuvastada. Mõnikord võib sama mõju olla peale nime ka muudel tunnustel, mis muudavad isiku otseselt tuvastatavaks. Isiku võivad tuvastatavaks muuta näiteks telefoninumber, isikukood ja sõiduki registreerimisnumber. Samuti on võimalik kasutada seoseid, näiteks arvutifaile, küpsiseid ja veebiliikluse jälgimise vahendeid, et selgitada üksikisikud välja nende käitumist ja harjumusi tuvastades. Nagu on selgitatud artikli 29 töörühma arvamuses, on võimalik isikut isegi tema nime ja aadressi küsimata liigitada sotsiaal-majanduslike, psühholoogiliste, filosoofiliste või muude kriteeriumide alusel ning omistada talle teatud otsuseid, sest isiku kontaktpunkt (arvuti) ei eelda enam tema identiteedi avalikustamist kitsas tähenduses[155]. Isikuandmete määratlus on nii Euroopa Nõukogu kui ka ELi õiguses piisavalt lai, et hõlmata kõiki tuvastamisvõimalusi (ja seega kõiki tuvastatavuse astmeid).

Näide: kohtuasjas *Promusicae vs. Telefónica de España*[156] 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

152 Isikuandmete kaitse üldmääruse põhjendus 26.

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

154 Isikuandmete kaitse üldmääruse artikli 4 lõige 1.

155 Artikli 29 töörühm (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20. juuni 2007, lk 15.

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

isikuandmed, st teave tuvastatud või tuvastatava füüsilise isiku kohta vastavalt direktiivi 95/46/EÜ artikli 2 punktis a olevale määratlusele [praeguse isikuandmete kaitse üldmääruse artikli 4 punkt 1] [...]. Sellise teabe edastamine, mida Telefónica Promusicae sõnul salvestab – mida Telefónica ei vaidlusta –, kujutab endast isikuandmete töötlemist"[157].

Näide: kohtuasi *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] käsitles internetiteenuse osutaja Scarlet keeldumist paigaldada süsteem, millega filtreeritakse failijagamistarkvara kasutatavat elektroonilist sidet, et takistada sellist failide jagamist, millega rikutakse autoriõigust, mida kaitseb SABAM (haldusettevõte, mis esindab autoreid, heliloojaid ja toimetajaid). Euroopa Liidu Kohus leidis, et kasutajate IP-aadressid „on kaitstud isikuandmed, sest nende identifitseerimine võimaldab selliste kasutajate täpse tuvastamise".

Et paljud nimed ei ole kordumatud, võib isiku identiteedi kinnitamiseks olla vaja lisatunnuseid, et teda ei peetaks ekslikult kellekski teiseks. Mõnikord võib olla vaja otseseid ja kaudseid tunnuseid kombineerida, et tuvastada teabe subjektiks olev isik. Sageli kasutatakse sünnikuupäeva ja -kohta. Peale selle on kodanike tõhusamaks eristamiseks kehtestatud mitmes riigis isikukoodide süsteem. Isikuandmed võivad olla edastatud maksuandmed[159], haldusdokumendis sisalduvad andmed elamisloa taotleja kohta[160] ning pangandus- ja usaldussuhteid käsitlevad dokumendid[161]. Tänapäeva tehnoloogiaajastul kasutatakse isikute tuvastamiseks üha rohkem biomeetrilisi andmeid, näiteks sõrmejäljekujutisi, digifotosid ja silmaiirisekujutisi.

Euroopa andmekaitseõiguse kohaldatavuse suhtes ei ole andmesubjekti tegelikuks tuvastamiseks tunnuseid siiski vaja; piisab sellest, kui asjaomane isik on tuvastatav. Isik on tuvastatav siis, kui on olemas piisavalt elemente, mille alusel saab ta otseselt või kaudselt tuvastada[162]. Isikuandmete kaitse üldmääruse põhjenduse 26 kohaselt tuleb arvestada, kas teabe eeldatavate kasutajate jaoks on tõenäoliselt kättesaa-

157 Endise direktiivi 95/46/EÜ artikli 2 punkt b, nüüd isikuandmete kaitse üldmääruse artikli 4 punkt 2.

158 ELK, C-70/10, *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011, punkt 51.

159 ELK, C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 1. oktoober 2015.

160 ELK, *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 17. juuli 2014.

161 EIK, *M.N. jt vs. San Marino*, nr 28005/12, 7. juuli 2015.

162 Isikuandmete kaitse üldmääruse artikli 4 lõige 1.

davad mõistlikud vahendid isiku tuvastamiseks ning kas nad neid kasutavad; see hõlmab kolmandatest isikutest vastuvõtjate valduses olevat teavet (vt punkt 2.3.2).

Näide: kohalik ametiasutus otsustab hakata koguma kohalikel tänavatel kiirust ületavate autode andmeid. Autod pildistatakse, registreerides automaatselt aja ja koha, et anda need andmed üle pädevale asutusele kiirust ületanud juhtide trahvimiseks. Üks andmesubjekt esitab kaebuse, väites, et kohalikul ametiasutusel ei ole andmekaitseõiguse kohaselt õiguslikku alust selliseid andmeid koguda. Kohalik ametiasutus on seisukohal, et ta ei kogu isikuandmeid. Sõidukite registreerimismärgid on tema väitel anonüümsed. Kohalikul ametiasutusel ei ole seaduslikku juurdepääsu üldisele sõidukiregistrile, et tuvastada selle järgi auto omanik või juht.

Selline mõttekäik ei ole kooskõlas isikuandmete kaitse üldmääruse põhjendusega 26. Et andmete kogumise eesmärk on ilmselgelt kiiruseületajate tuvastamine ja trahvimine, võib eeldada, et selle jaoks üritatakse tuvastada isikuid. Kuigi kohalikel ametiasutustel ei ole võimalust isikuid otseselt tuvastada, edastavad nad andmed pädevale asutusele – politseile –, kellel on see võimalus olemas. Põhjendus 26 hõlmab selge sõnaga ka stsenaariumi, kus on eeldatav, et üksikisikut võivad peale andmete esmase kasutaja üritada tuvastada teised andmete vastuvõtjad. Põhjenduse 26 kontekstis on kohaliku ametiasutuse tegevus andmete kogumine tuvastatavate isikute kohta ning nõuab seega andmekaitseõigusega kooskõlas olevat õiguslikku alust.

Et „teha kindlaks, kas füüsilise isiku tuvastamiseks võetakse mõistliku tõenäosusega meetmeid, tuleks arvestada kõiki objektiivseid tegureid, näiteks tuvastamise maksumus ja selleks vajalik aeg, võttes arvesse nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid“[163].

Näide: kohtuasjas *Breyer vs. Bundesrepublik Deutschland*[164] käsitles Euroopa Liidu Kohus andmesubjektide kaudset tuvastatavust. Juhtum oli seotud dünaamiliste IP-aadressidega, mis muutuvad igal uuel ühenduskorral internetiga. Saksamaa föderaalasutuste hallatavad veebikohad registreerisid ja

163 *Ibid*., põhjendus 26.

164 ELK, C-582/14, *Patrick Breyer vs. Bundesrepublik Deutschland*, 19. oktoober 2016, punktd 47–48.

säilitasid dünaamilisi IP-aadresse küberrünnakute tõkestamiseks ja vajaduse korral kriminaalmenetluse algatamiseks. Ainult internetiteenuse pakkujal, keda Patrick Breyer kasutas, oli tema isiku tuvastamiseks vajalik lisateave.

Euroopa Liidu Kohus leidis, et dünaamiline IP-aadress, mille elektroonilise meedia teenuse pakkuja salvestab hetkel, kui isik külastab veebilehte, mille see teenusepakkuja teeb üldsusele kättesaadavaks, on isikuandmed, kui ainult kolmandal isikul – praegusel juhul internetiteenuse pakkujal – on isiku tuvastamiseks vajalik täiendav teave[165]. Kohus leidis, et selleks, et teavet saaks käsitleda isikuandmetena, „ei ole nõutud, et kõik isikut tuvastada võimaldavad andmed oleksid ühe isiku valduses". Internetiteenuse pakkuja registreeritud dünaamilise IP-aadressi kasutajad võidakse teatud olukordades, näiteks kriminaalmenetluse raames küberrünnakute korral, tuvastada muude isikute abiga[166]. ELK märgib, et kui teenusepakkujal „on seaduslikud vahendid, mis võimaldavad kõnealuse isiku tuvastada tänu täiendavale teabele, mis on selle isiku internetiühenduse pakkuja valduses", saab seda käsitada kui „meedet, mida võidakse tõenäoliselt kasutada kõnealuse isiku tuvastamiseks". Seepärast peetakse sellist teavet isikuandmeteks.

Euroopa Nõukogu õiguses mõistetakse tuvastatavust sarnaselt. Nüüdisajastatud konventsiooni nr 108 seletuskirjas on sarnane kirjeldus: mõiste „tuvastatav" tähendab peale isiku tsiviilõigusliku või juriidilise isikusamasuse ka seda, mis võib võimaldada isikut n-ö individualiseerida või teiste hulgast esile tuua, mille tulemusena võidakse teda kohelda erinevalt. Selline „individualiseerimine" võib toimuda näiteks konkreetselt viidates isikule või seadmele või seadmete kombinatsioonile (arvuti, mobiiltelefon, kaamera, mängimisseadmed jt), mis on seotud registreerimisnumbri, pseudonüümi, biomeetriliste või geneetiliste andmete, asukohaandmete, IP-aadressi või muu identifikaatoriga[167]. Isikut ei peeta tuvastatavaks, kui tema tuvastamine nõuab ebamõistlikult palju aega, vaeva või ressursse. See on nii näiteks juhul, kui andmesubjekti tuvastamiseks oleks vaja liiga keerulisi, pikki ja kulukaid toiminguid. Aja, vaeva või ressursside ebamõistlikkust tuleb hinnata iga kord eraldi, arvestades

165 Endine Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, artikli 2 punkt a.

166 ELK, C-70/10, *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011, punktid 47–48.

167 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 18.

selliseid tegureid nagu töötlemise eesmärk, tuvastamise kulu ja kasulikkus, vastutava töötleja liik ja kasutatav tehnoloogia[168].

Seoses andmekaitseõiguse kohaldatavusega on tähtis märkida, et isikuandmete talletamise või kasutamise vorm ei ole oluline. Kirjalikud või häälteated võivad sisaldada isikuandmeid ja kujutisi[169], sealhulgas videovalve salvestis[170] või heli[171]. Ka elektrooniliselt salvestatud ja paberkandjal olev teave võib olla isikuandmed. Isegi inimkudede rakuproovid – milles on tema DNA – võivad olla allikad, millest saab eraldada biomeetrilisi andmeid[172], kui andmed on seotud inimese pärilike või omandatud geneetiliste omadustega, annavad ainulaadset teavet inimese tervise või füsioloogia kohta ja need saadakse tema bioloogilise proovi analüüsi tulemusena[173].

Anonüümimine

Nii isikuandmete kaitse üldmääruses kui ka nüüdisajastatud konventsioonis nr 108 sisalduva andmete säilitamise piiramise põhimõtte kohaselt (üksikasjalikum teave: vt 3. peatükk) tuleb andmeid säilitada „kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse“[174]. Järelikult tuleb andmed kustutada või anonüümida, kui vastutav töötleja soovib neid säilitada pärast seda, kui neid ei ole enam vaja ja need ei teeni enam algset eesmärki.

Andmete anonüümimine tähendab, et isikuandmete kogumist kõrvaldatakse kõik tuvastamist võimaldavad elemendid, nii et andmesubjekt ei ole enam tuvastatav[175]. Arvamuses 05/2014 analüüsib artikli 29 töörühm anonüümimistehnikate

168 *Ibid*., punkt 17.

169 EIK, *Von Hannover vs. Saksamaa*, nr 59320/00, 24. juuni 2004; EIK, *Sciacca vs. Itaalia*, nr 50774/99, 11. jaanuar 2005; ELK, C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 11. detsember 2014.

170 EIK, *Peck vs. Ühendkuningriik*, nr 44647/98, 28. jaanuar 2003; EIK, *Köpke vs. Saksamaa* (detsember), nr 420/07, 5. oktoober 2010; Euroopa Andmekaitseinspektor (2010), *The EDPS video-surveillance guidelines*, 17. märts 2010.

171 EIK, *P.G. ja J.H. vs. Ühendkuningriik*, nr 44787/98, 25. september 2001, punktid 59–60; EIK, *Wisse vs. Prantsusmaa*, nr 71611/01, 20. detsember 2005 (prantsuskeelne variant).

172 Vt artikli 29 töörühm (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20. juuni 2007, lk 9; Euroopa Nõukogu (2006), *Recommendation No. Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin*, 15. märts 2006.

173 Isikuandmete kaitse üldmääruse artikli 4 lõige 13.

174 *Ibid*., artikli 5 lõike 1 punkt e; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt e.

175 Isikuandmete kaitse üldmääruse põhjendus 26.

tulemuslikkust ja piiranguid[176]. Töörühm tunnistab selliste tehnikate võimalikku väärtust, kuid rõhutab, et teatud meetodid ei pruugi alati toimida. Konkreetses olukorras optimaalse lahenduse leidmiseks tuleb asjakohane anonüümimisprotsess otsustada iga kord eraldi. Olenemata kasutatavast tehnikast tuleb tuvastamine pöördumatult välistada. See tähendab, et andmete anonüümimisel ei tohi teabe hulka jääda elemente, mille abil saaks asjaomase(d) isiku(d) tuvastada mõistliku vaevaga[177]. Taastuvastamise riski saab hinnata aja, vaeva või ressursside järgi, mida on vaja, arvestades andmete olemust, nende kasutamise konteksti, olemasolevaid taastuvastamise tehnoloogiaid ja seonduvaid kulusid[178].

Kui andmed on edukalt anonüümitud, ei ole need enam isikuandmed ning andmekaitse õigusakte enam ei kohaldata.

Isikuandmete kaitse üldmääruses sätestatakse, et isikuandmete töötlemist kontrollival isikul või organisatsioonil ei saa olla kohustust säilitada, omandada või töödelda täiendavat teavet, et tuvastada andmesubjekt üksnes selleks, et täita määruse nõudeid. Sellel reeglil on siiski oluline erand: kui andmesubjekt annab juurdepääsuõiguse, andmete parandamise, kustutamise, töötlemise ja andmete ülekandmise piiramise õiguse teostamiseks vastutavale töötlejale täiendavat teavet, mis võimaldab tema isiku tuvastada, muutuvad varem anonüümitud andmed taas isikuandmeteks[179].

Pseudonüümimine

Isikuandmed sisaldavad isiku tuvastamist võimaldavaid tunnuseid või muid elemente, näiteks nime, sünnikuupäeva, sugu, aadressi. Isikuandmete pseudonüümimisel asendatakse need tunnused pseudonüümiga.

ELi õiguses määratletakse pseudonüümimine kui „isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid“[180]. Teisiti kui anonüümitud

176 Artikli 29 töörühm (2014), *Opinion 05/2014 on Anonymization Techniques*, WP 216, 10. aprill 2014.

177 Isikuandmete kaitse üldmääruse põhjendus 26.

178 Euroopa Nõukogu, konventsiooni nr 108 komitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, punkt 6.2.

179 Isikuandmete kaitse üldmääruse artikkel 11.

180 *Ibid.*, artikli 4 lõige 5.

andmed, on pseudonüümitud andmed endiselt isikuandmed ja seepärast kehtivad nende suhtes andmekaitse õigusaktid. Kuigi pseudonüümimine võib vähendada andmesubjektide turvariske, ei ole see väljaspool isikuandmete kaitse üldmääruse kohaldamisala.

Isikuandmete kaitse üldmääruses tunnustatakse pseudonüümimise eri kasutusviise kui asjakohast tehnilist meedet andmekaitse tõhustamiseks ning seda on konkreetselt nimetatud andmete töötlemise kavandamise ja turbe vahendina[181]. See on ka asjakohane kaitsemeede, mida võib kasutada isikuandmete töötlemisel muudel eesmärkidel kui need, mille jaoks need algselt koguti[182].

Euroopa Nõukogu nüüdisajastatud konventsiooni nr 108 õiguslikus määratluses ei ole pseudonüümimist eraldi nimetatud. Samas öeldakse nüüdisajastatud konventsiooni nr 108 seletuskirjas selgesti, et pseudonüümi või digitaalse identifikaatori / digitaalse identiteedi kasutamisega ei anonüümita andmeid, sest andmesubjekt on endiselt tuvastatav või individualiseeritud[183]. Üks andmete pseudonüümimise meetod on andmete krüptimine. Kui andmed on pseudonüümitud, on seos identiteediga olemas pseudonüümi ja krüptovõtme kujul. Ilma sellise võtmeta on pseudonüümitud andmeid raske tuvastada. Samas on neil, kellel on õigus krüptovõtit kasutada, lihtne isik uuesti tuvastada. Seepärast tuleb eriti hoolikalt jälgida, et krüptovõtmeid ei saaks kasutada volitamata isikud. Seetõttu tuleb pseudonüümitud andmeid pidada isikuandmeteks, mis on hõlmatud nüüdisajastatud konventsiooniga nr 108[184].

Autentimine

Autentimisega kinnitab isik väidetavat identiteeti ja/või seda, et tal on õigus teha teatud toiminguid, näiteks siseneda turvaalale või võtta pangakontolt raha. Autentimine võib toimuda järgmiselt: biomeetriliste andmete võrdlus, näiteks passifoto või sõrmejälgede võrdlemine selle isiku andmetega, kelleks inimene väidab end olevat, näiteks sisserändekontrollis;[185] sellise teabe küsimine, mida tohib teada üksnes teatud isikusamasuse või volitusega isik, näiteks isikukood või salasõna; teatud pääsmiku esitamise nõudmine, mis tohib olla üksnes teatud isikusamasuse või volitusega isiku valduses, näiteks kiipkaart või pangaseifi võti. Peale salasõna või kiipkaardi on

181 *Ibid.*, artikli 25 lõige 1.

182 *Ibid.*, artikli 6 lõige 4.

183 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 18.

184 *Ibid.*

185 *Ibid.*, punktid 56–57.

elektroonilises suhtluses eriti tõhus isikutuvastus- ja autentimisvahend elektrooniline allkiri, mõnikord koos PIN-koodidega.

2.1.2. Isikuandmete eriliigid

Nii **ELi** kui ka **Euroopa Nõukogu õiguses** on isikuandmete eriliigid, mille olemuse tõttu võib nende töötlemine ohustada andmesubjekti ja mis seega vajavad tugevdatud kaitset. Selliste andmete suhtes kohaldatakse keelupõhimõtet ja on ainult mõni tingimus, mille korral on selline töötlemine seaduslik.

Nüüdisajastatud konventsiooni nr 108 (artikkel 6) ja isikuandmete kaitse üldmääruse (artikkel 9) raames peetakse delikaatseteks andmeteks järgmisi andmeliike:

- isikuandmed, millest ilmneb rassiline või etniline päritolu;
- isikuandmed, millest ilmnevad poliitilised vaated, usulised või muud, sealhulgas filosoofilised veendumused;
- isikuandmed, millest ilmneb ametiühingusse kuulumine;
- isiku tuvastamiseks töödeldavad geneetilised andmed ja biomeetrilised andmed;
- isikuandmed, mis käsitlevad terviseseisundit, seksuaalelu või seksuaalset sättumust.

Näide: kohtuasi *Bodil Lindqvist*[186] käsitles veebilehel isikutele viitamist nimega või teisiti, näiteks telefoninumbriga või harrastuste teabega. ELK märkis, et „osutamine asjaolule, et isik vigastas oma jalga ja töötab haiguspuhkusel olles osalise tööajaga, sisaldab tervislikku seisundit käsitlevaid isikuandmeid“[187].

186 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003, punkt 51.

187 Endise direktiivi 95/46/EÜ artikli 8 lõige 1, nüüd isikuandmete kaitse üldmääruse artikli 9 lõige 2.

Süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmed

Nüüdisajastatud konventsioonis nr 108 käsitletakse isikuandmeid, mis on seotud süütegude, kriminaalmenetluse ja süüdimõistvate kohtuotsuste ning nendega seotud turvameetmetega isikuandmete eriliikide loetelus[188]. Isikuandmete kaitse üldmääruse raames ei nimetata süüdimõistvate kohtuotsuste ja süütegude või asjakohaste turvameetmetega seotud isikuandmeid andmete eriliikide loetelus, vaid neid käsitletakse eraldi artiklis. Isikuandmete kaitse üldmääruse artiklis 10 on sätestatud, et selliseid andmeid töödeldakse „ainult ametiasutuse järelevalve all või siis, kui töötlemine on lubatud liidu või liikmesriigi õigusega, milles on sätestatud asjakohased kaitsemeetmed andmesubjektide õiguste ja vabaduste kaitseks". Teisalt peetakse süüteoasjades süüdimõistvate kohtuotsuste terviklikku registrit ainult eriliste ametiasutuse järelevalve all[189]. ELis reguleeritakse isikuandmete töötlemist õiguskaitse kontekstis eriõigusaktiga – direktiiviga (EL) 2016/680[190]. Direktiivis sätestatakse andmekaitse erieeskirjad, mis on pädevatele asutustele siduvad, kui nad töötlevad isikuandmeid konkreetselt kuritegude ennetamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks (vt punkt 8.2.1).

2.2. Andmetöötlus

Põhipunktid

- Termin „andmetöötlus" hõlmab kõiki isikuandmetega tehtavaid toiminguid.
- Termin „töötlemine" hõlmab automaatset ja mitteautomaatset töötlemist.
- ELi õiguses hõlmab termini „töötlemine" mõiste ka käsitsi töötlemist korrastatud andmekogumis.
- Euroopa Nõukogu õiguses võivad riigid termini „töötlemine" mõistet oma õigusaktides laiendada käsitsi töötlemisele.

188 Nüüdisajastatud konventsiooni nr 108 artikli 6 lõige 1.

189 Isikuandmete kaitse üldmääruse artikkel 10.

190 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, ELT 2016 L 119.

2.2.1. Andmetöötluse mõiste

Isikuandmete töötlemise mõiste on terviklik **nii ELi kui ka Euroopa Nõukogu õiguses**: „„isikuandmete töötlemine“ – [isikuandmetega] [...] tehtav toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine“[191]. Nüüdisajastatud konventsioonis nr 108 on määratlusele lisatud isikuandmete talletamine[192].

Näide: kohtuasi *František Ryneš*[193] käsitles juhtumit, kuidas František Ryneš jäädvustas oma kinnisvara kaitseks paigaldatud koduse videovalvesüsteemiga kaks isikut, kes lõhkusid tema elamu aknaid. Euroopa Liidu Kohus leidis, et isikuandmete salvestamist ja säilitamist hõlmav videovalve on automatiseeritud andmetöötlus, mis kuulub ELi andmekaitseõiguse kohaldamisalasse.

Näide: kohtuasjas *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*[194] taotles Salvatore Manni oma isikuandmete eemaldamist reitinguagentuuri registrist, milles teda seostati kinnisvaraettevõtte likvideerimisega, mis kahjustas tema mainet. ELK seisukoha järgi „teostab registrit pidav ametiasutus, kui ta kannab nimetatud teabe registrisse, säilitab seda seal ja annab selle vastavalt olukorrale taotluse alusel kolmandale isikule üle, „isikuandmete töötlemist“, mille eest ta „vastutab““.

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

Tööandjad peavad töötajate palgaandmed edastama maksuhaldurile. Ka selline andmete edastamine kuulub nüüdisajastatud konventsiooni nr 108 ja isikuandmete kaitse üldmääruse tähenduses andmetöötluse alla. Sellise avaldamise õiguslik alus ei tulene siiski töölepingust. Töötlemistoiminguteks, mille tulemusena saadab tööandja maksuhaldurile palgaandmed, peab

191 Isikuandmete kaitse üldmääruse artikli 4 lõige 2. Vt ka nüüdisajastatud konventsiooni nr 108 artikli 2 punkt b.

192 Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt b.

193 ELK, C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 11. detsember 2014, punkt 25.

194 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 9. märts 2017, punkt 35.

olema täiendav õiguslik alus. Tavaliselt on see sätestatud riigi maksuseaduse sätetega. Kui neid sätteid ei oleks – ja kui töötlemiseks ei oleks muid õigus-päraseid põhjusi –, loetaks selline andmete edastamine ebaseaduslikuks töötlemiseks.

2.2.2. Isikuandmete automaatne töötlemine

Automaatse andmetöötluse suhtes kohaldatakse täielikult nüüdisajastatud konventsiooni nr 108 ja isikuandmete kaitse üldmääruse kohast andmekaitset.

ELi õiguses tähendab automatiseeritud andmetöötlus toiminguid, mida kohaldatakse „isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes“[195]. Nüüdisajastatud konventsioonis nr 108 on sarnane määratlus[196]. Praktikas tähendab see, et isikuandmete täielikult või osaliselt automaatne töötlemine, näiteks personaalarvuti, mobiilseadme või ruuteriga, on hõlmatud nii ELi kui ka Euroopa Nõukogu andmekaitse-eeskirjadega.

Näide: kohtuasi *Bodil Lindqvist*[197] käsitles veebilehel isikutele viitamist nimega või teisiti, näiteks telefoninumbriga või harrastuste teabega. Euroopa Liidu Kohus leidis, 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/EÜ artikli 3 lõike 1 tähenduses“[198].

Näide: kohtuasjas *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] nõudis Mario Costeja González, et kustutataks tema nime otsingu järel Google'i otsingumootoris kuvatavast tulemuste loetelust link kahe ajalehe veebilehele, kus teatatakse kinnisvaraoksjonist sotsiaalkindlustusmaksete võlgnevuse sissenõudmiseks, või et seda linki muudetaks. ELK märkis, et „internetis avaldatud teabe

195 Isikuandmete kaitse üldmääruse artikli 2 lõige 1 ja artikli 4 punkt 2.

196 Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt b; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 21.

197 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003, punkt 27.

198 Isikuandmete kaitse üldmääruse artikli 2 lõige 1.

199 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014.

otsimise eesmärgil automatiseeritult, pidevalt ja süstemaatiliselt internetti läbi kammides „kogub“ otsingumootori haldaja andmeid, millest ta seejärel teeb oma indekseerimisprogrammide raames „väljavõtteid“ ning mida ta „salvestab“ ja „korrastab“, oma serverites „säilitab“ ning vajaduse korral „annab üle“ või „teeb kättesaadavaks“ kasutajatele otsingutulemuste loetelu kujul“[200]. ELK järeldas, et selline tegevus on töötlemine ning „seejuures ei ole oluline, et otsingumootori haldaja teeb samasuguseid toiminguid ka muud liiki teabe puhul ega tee isikuandmetel ja muudel andmetel vahet“.

2.2.3. Isikuandmete mitteautomaatne töötlemine

Andmeid tuleb kaitsta ka andmete käsitsi töötlemisel.

ELi õiguses ei piirdu andmekaitse üksnes automaatse andmetöötlusega. ELi õiguses kohaldatakse andmekaitset seega isikuandmete töötlemisel automatiseerimata andmete kogumis, st spetsiaalselt struktureeritud paberdokumentide kogumis[201]. Korrastatud andmekogum on selline, kus isikuandmete kogum liigitatakse, muutes need teatud kriteeriumide alusel kättesaadavaks. Kui tööandja näiteks peab pabertoimikut „Töötajate puhkus“, mis sisaldab kõiki üksikasju kõigi puhkuste kohta, mida töötajad on võtnud eelmisel aastal ja kus andmed on tähestiku järjekorras, on see automatiseerimata andmete kogum, mille suhtes kohaldatakse ELi andmekaitse-eeskirju. Andmekaitse laiendamise põhjus on järgmine:

- paberkandjal teavet on võimalik korrastada nii, et teavet saab leida kiiresti ja lihtsalt;

- isikuandmete säilitamisel korrastatud paberkandjatel on lihtne vältida õigusaktides sätestatud automaatse andmetöötluse piiranguid[202].

Euroopa Nõukogu õiguses selgub automaatse töötlemise määratlusest, et automaattoimingute teatud etappides võidakse nõuda ka isikuandmete mitteautomaatset käsitlemist[203]. Nüüdisajastatud konventsiooni nr 108 artikli 2 punktis c on märgitud, et automaattöötlemise mittekasutamisel tähendab andmetöötlus toimingut või

200 *Ibid.*, punkt 28.

201 Isikuandmete kaitse üldmääruse artikli 2 lõige 1.

202 Isikuandmete kaitse üldmääruse põhjendus 15.

203 Nüüdisajastatud konventsiooni nr 108 artikli 2 punktid b ja c.

toiminguid, mida isikuandmetega tehakse sellistes korrastatud andmekogudes, mis on juurdepääsetavad või kättesaadavad konkreetsete kriteeriumide kohaselt.

2.3. Isikuandmete kasutajad

Põhipunktid

- Isik või üksus, kes määrab teiste inimeste isikuandmete töötlemise vahendid ja eesmärgid, on andmekaitseõiguse seisukohalt vastutav töötleja; kui see otsus tehakse kollektiivselt, võidakse neid nimetada kaasvastutavateks töötlejateks.
- Volitatud töötleja on füüsiline või juriidiline isik, kes töötleb isikuandmeid vastutava töötleja nimel.
- Kui volitatud töötleja määrab andmetöötluse vahendid ja eesmärgid ise, saab temast vastutav töötleja.
- Isik, kellele vastutav töötleja andmeid avaldab, on vastuvõtja.
- Kolmas isik on füüsiline või juriidiline isik, kes ei ole andmesubjekt, vastutav ega volitatud töötleja, ega isik, keda on volitatud isikuandmeid töötlema vastutava töötleja või volitatud töötleja otseses alluvuses.
- Nõusolek kui isikuandmete töötlemise õiguslik alus peab olema vabatahtlik, teadlik, konkreetne ja ühemõtteline sooviavaldus selge kinnitusena, millega antakse töötlemise nõusolek.
- Nõusoleku alusel eriliiki isikuandmete töötlemiseks on vaja selgesõnalist nõusolekut.

2.3.1. Vastutavad töötlejad ja volitatud töötlejad

Olulisim aspekt, mis kaasneb vastutava või volitatud töötleja rolliga, on õiguslik vastutus andmekaitseõigusega kehtestatud asjaomaste kohustuste täitmise eest. Erasektoris on selles rollis tavaliselt füüsiline või juriidiline isik ja avalikus sektoris ametiasutus. Isikuandmete vastutaval ja volitatud töötlejal on oluline erinevus: esimene on füüsiline või juriidiline isik, kes määrab töötlemise eesmärgid ja vahendid, kuid teine on füüsiline või juriidiline isik, kes töötleb andmeid vastutava töötleja nimel, järgides rangeid juhiseid. Põhimõtteliselt on vastutav andmetöötleja see, kes peab töötlemist kontrollima ja kes selle eest vastutab, sealhulgas õiguslikult. Samas on andmekaitse-eeskirjade reformi tulemusel volitatud töötlejal kohustus järgida paljusid vastutava töötleja suhtes kohaldatavaid nõudeid. Isikuandmete kaitse

üldmääruse kohaselt peavad vastutavad töötlejad näiteks pidama kõigi töötlemistoimingute kategooriate registrit, et tõendada, et täidavad määrusest tulenevaid kohustusi[204]. Ka peavad volitatud töötlejad rakendama töötlemise turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid[205], määrama teatud olukordades andmekaitseametniku[206] ja teatama isikuandmetega seotud rikkumised vastutavale töötlejale[207].

See, kas isikul on pädevus otsustada ja määrata töötlemise eesmärk ja vahendid, oleneb juhtumi faktilistest elementidest või asjaoludest. Isikuandmete kaitse üldmääruses sätestatud vastutava töötleja määratluse kohaselt võivad vastutavad töötlejad olla füüsilised isikud, juriidilised isikud või muud asutused. Samas on artikli 29 töörühm rõhutanud, et selleks, et andmesubjektidel oleks stabiilsem alus kasutada oma õigusi, „tuleb vastutava töötlejana eelkõige käsitada pigem äriühingut või asutust kui konkreetset isikut selles"[208]. Näide: ettevõte müüb tervishoiutooteid meditsiinitöötajatele. Tooteid saavate meditsiinitöötajate nimekirja koostamisel ja haldamisel on vastutav töötleja ettevõte, mitte müügijuht, kes nimekirja tegelikult kasutab ja haldab.

> Näide: kui ettevõtte Päikesekiir turundusosakond kavatseb hakata töötlema andmeid turu-uuringu jaoks, on andmete töötlemisel vastutav töötleja ettevõte Päikesekiir, mitte selle turundusosakonna töötajad. Turundusosakond ei saa olla vastutav töötleja, sest see ei ole eraldi isik.

Füüsilised isikud võivad olla vastutavad töötlejad nii ELi kui ka Euroopa Nõukogu õiguse alusel. Samas ei kuulu isikuandmete kaitse üldmääruse ja nüüdisajastatud konventsiooni nr 108 eeskirjade kohaldamisalasse üksikisikud, kui nad töötlevad teiste isikuandmeid eranditult isiklike või koduste tegevuste käigus, ning neid ei loeta vastutavaks töötlejaks[209]. Isik, kes peab kirjavahetust, sõprade ja töökaaslastega juhtunut kirjeldavat isiklikku päevikut ning pereliikmete terviseandmeid, võib olla andmekaitse-eeskirjade nõuetest vabastatud, sest selline tegevus võib olla

204 Isikuandmete kaitse üldmääruse artikli 30 lõige 2.

205 *Ibid.*, artikkel 32.

206 *Ibid.*, artikkel 37.

207 *Ibid.*, artikli 33 lõige 2.

208 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brüssel, 16. veebruar 2010.

209 Isikuandmete kaitse üldmääruse põhjendus 18 ja artikli 2 lõike 2 punkt c; nüüdisajastatud konventsiooni nr 108 artikli 3 lõige 2.

eranditult isiklik või seotud koduse tegevusega. Isikuandmete kaitse üldmääruses on samuti märgitud, et isiklik ja kodune tegevus võib hõlmata ka kirjavahetust ja aadresside loetelu või tegevust suhtlusvõrgustikes ja internetis, mis toimub sellise isikliku või koduse tegevuse raames[210]. Seevastu kohaldatakse andmekaitse-eeskirju täies mahus vastutavate ja volitatud töötlejate suhtes, kes pakuvad isikuandmete isiklikel või kodustel eesmärkidel töötlemise vahendeid (nt suhtlusvõrgustike platvorme)[211].

Kodanike juurdepääs internetile ja võimalus kasutada e-kaubanduse platvorme, suhtlusvõrgustikke ja blogiplatvorme, et jagada isiklikku teavet enda ja teiste isikute kohta, raskendab isiklikel ja mitteisiklikel eesmärkidel töötlemise eristamist[212]. See, kas tegevus on eranditult isiklik või kodune, oleneb asjaoludest[213]. Tegevus, millel on kutselise või äritegevuse aspekte, ei saa kuuluda koduse tegevuse erandi alla[214]. Seega, kui andmetöötluse ulatus ja sagedus viitavad kutselisele või täisajaga tegevusele, võib eraisikut pidada vastutavaks töötlejaks. Lisaks töötlemistoimingu kutselisele või ärilisele iseloomule tuleb arvestada veel üht tegurit: kas isikuandmed tehakse kättesaadavaks paljudele isikutele, kes on ilmselgelt väljaspool üksikisiku erasfääri. Andmekaitsedirektiivi käsitlevas kohtupraktikas on leitud, et andmekaitseõigus kohaldub, kui eraisik avaldab andmeid teiste inimeste kohta internetis avalikus veebikohas. Euroopa Liidu Kohus ei ole veel sarnaste asjaolude kohta otsuseid teinud isikuandmete kaitse üldmääruse raames, milles on rohkem juhiseid teemade kohta, mida saab käsitleda väljaspool andmekaitse õigusaktide kohaldamisala koduse tegevuse erandi raames, näiteks sotsiaalmeedia kasutamisel isiklikul eesmärgil.

Näide: kohtuasi *Bodil Lindqvist*[215] käsitles veebilehel isikutele viitamist nimega või teisiti, näiteks telefoninumbriga või harrastuste teabega. Euroopa Liidu Kohus leidis, et „toiming, mis seisneb veebilehel erinevatele isikutele

210 Isikuandmete kaitse üldmääruse põhjendus 18.

211 *Ibid*., põhjendus 18; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 29.

212 Vt artikli 29 töörühma avaldus andmekaitsereformi paketi arutelude kohta (2013), *Annex 2: Proposals and Amendments regarding exemption for personal or household activities*, 27. veebruar 2013.

213 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 28.

214 Vt isikuandmete kaitse üldmääruse põhjendus 18 ja nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 27.

215 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003.

osutamises ja nende individualiseerimises kas nime või muude vahendite [...] alusel, on „isikuandmete täielikult või osaliselt automatiseeritud töötlemine“ andmekaitse direktiivi artikli 3 lõike 1 tähenduses[216].

Sellisel juhul ei ole isikuandmete töötlemisel tegu üksnes isiklikel või kodustel eesmärkidel tehtavate toimingutega, mis ei kuulu ELi andmekaitse-eeskirjade kohaldamisalasse, sest 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“[217].

ELK arvates võib eraviisiliselt paigaldatud turvakaamerate visuaalsalvestisi reguleerida teatud tingimustel ka ELi andmekaitse õigusaktidega.

Näide: kohtuasi *František Ryneš*[218] käsitles juhtumit, kuidas František Ryneš jäädvustas oma kinnisvara kaitseks paigaldatud koduse videovalvesüsteemiga kaht isikut, kes lõhkusid tema elamu aknaid. Salvestis anti politseile ja sellele tugineti kriminaalmenetluses.

ELK märkis, et „[k]ui niisugune videovalve [...] kasvõi osaliselt ulatub avalikku ruumi ja on seetõttu suunatud selle vahendi abil andmete töötleja isiklikust sfäärist väljapoole, ei saa seda pidada tegevuseks, millega tegeldakse üksnes „isiklikel või kodustel“ eesmärkidel [...]“[219].

Vastutav töötleja

ELi õiguses on vastutav töötleja isik või üksus, kes „määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid“[220]. Vastutava töötleja otsus määrab, miks ja kuidas andmeid töödeldakse.

216 *Ibid.*, punkt 27; endise direktiivi 95/46/EÜ artikli 3 lõige 1, nüüd isikuandmete kaitse üldmääruse artikli 2 lõige 1.

217 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003, punkt 47.

218 ELK, C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 11. detsember 2014, punkt 33.

219 Endise direktiivi 95/46/EÜ artikli 3 lõike 2 teine taane, nüüd isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkt c.

220 Isikuandmete kaitse üldmääruse artikli 4 lõige 7.

Euroopa Nõukogu õiguses määratletakse vastutav töötleja nüüdisajastatud konventsioonis nr 108 kui füüsiline või juriidiline isik, riigiasutus, talitus, esindus või muu asutus, kellel on üksi või koos teistega pädevus teha otsuseid andmetöötluse kohta[221]. Selline otsustusõigus puudutab töötlemise eesmärke ja vahendeid, samuti töödeldavaid andmekategooriaid ja juurdepääsu andmetele[222]. Küsimus, kas see õigus tuleneb õiguslikust määratlusest või faktilistest asjaoludest, tuleb otsustada iga kord eraldi[223].

Näide: kohtuasja *Google Spain*[224] algatas Hispaania kodanik, kes soovis, et Google'ist eemaldataks tema finantsminevikku käsitlev vana ajaleheartikkel.

Euroopa Liidu Kohtult küsiti, kas Google kui otsingumootori haldaja on andmete vastutav töötleja andmekaitsedirektiivi artikli 2 punkti d tähenduses[225]. Et tagada „andmesubjektide tõhus ja täielik kaitse"[226], kaalutles ELK vastutava töötleja laia määratlust. ELK leidis, et otsingumootori haldaja määras tegevuse eesmärgid ja vahendid ning muutis veebikohtade avaldajate poolt internetilehekülgedele laaditud andmed kättesaadavaks igale internetikasutajale, kes teeb otsingu andmesubjekti nime põhjal[227]. Seepärast otsustas ELK, et Google'it võib pidada vastutavaks töötlejaks[228].

Kui vastutav või volitatud töötleja on asutatud väljaspool ELi, määrab vastutav või volitatud töötleja kirjalikult oma esindaja ELis[229]. Isikuandmete kaitse üldmääruses rõhutatakse, et esindaja peab olema asutatud „ühes liikmesriikidest, kus asuvad andmesubjektid, kelle isikuandmeid töödeldakse neile kaupade või teenuste

221 Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt d.

222 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 22.

223 *Ibid.*

224 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014.

225 Isikuandmete kaitse üldmääruse artikli 4 punkt 7; ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punkt 21.

226 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punkt 34.

227 *Ibid.*, punktid 35–40.

228 *Ibid.*, punkt 41.

229 Isikuandmete kaitse üldmääruse artikli 27 lõige 1.

pakkumise korral või kelle käitumist jälgitakse“[230]. Kui esindajat ei ole määratud, saab ikkagi võtta õiguslikke meetmeid vastutava või volitatud töötleja enda suhtes[231].

Kaasvastutavad töötlejad

Isikuandmete kaitse üldmääruses sätestatakse, et kui kaks või enam vastutavat töötlejat määravad ühiselt isikuandmete töötlemise eesmärgid ja vahendid, on nad kaasvastutavad töötlejad. See tähendab, et nad otsustavad koos töödelda andmeid ühisel eesmärgil[232]. Nüüdisajastatud konventsiooni nr 108 seletuskirjas märgitakse, et mitu vastutavat töötlejat või kaasvastutus on võimalik ka **Euroopa Nõukogu raamistikus**[233].

Artikli 29 töörühm juhib tähelepanu, et kaasvastutus võib olla eri vormis ja mitme vastutava töötleja osalus kontrollitegevuses võib olla ebavõrdne[234]. Selline paindlikkus võimaldab käsitleda üha keerukamaid andmetöötluse olukordi[235]. Kaasvastutavad töötlejad peavad seepärast määrama erilepingus oma vastutusvaldkonnad määrusest tulenevate kohustuste täitmisel[236].

Kaasvastutavate töötlejatega kaasneb kaasvastutus töötlemise eest[237]. **ELi õiguse** raamistikus tähendab see, et iga vastutav või volitatud töötleja võidakse võtta täielikult vastutusele kogu kaasvastutuse ajal toimunud töötlemisega tekitatud kahju eest, et tagada tõhus hüvitamine andmesubjektile[238].

Näide: kaasvastutuse tüüpiline näide on mitme krediidiasutuse hallatav ebausaldusväärsete klientide andmebaas. Kui kaasvastutavate töötlejate hulka kuuluv pank saab krediidiliini saamise taotluse, kontrollitakse andmebaasi, et teha taotleja krediidivõimelisuse suhtes teadlik otsus.

230 *Ibid.*, artikli 27 lõige 3.

231 *Ibid.*, artikli 27 lõige 5.

232 *Ibid.*, artikli 4 punkt 7 ja artikkel 26.

233 Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt d; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 22.

234 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concepts of “controller” and “processor”*, WP 169, Brüssel, 16. veebruar 2010, lk 19.

235 *Ibid.*

236 Isikuandmete kaitse üldmääruse põhjendus 79.

237 *Ibid.*, punkt 21.

238 *Ibid.*, artikli 82 lõige 4.

Õigussätted ei ütle selge sõnaga, kas kaasvastutus tähendab, et vastutavatel töötlejatel peab olema sama ühine eesmärk, või piisab, kui nende eesmärgid kattuvad ainult osaliselt. Euroopa tasandi asjakohane kohtupraktika seni veel puudub. 2010. aasta arvamuses vastutavate ja volitatud töötlejate kohta märgib artikli 29 töörühm, et kaasvastutavate töötlejate kõik töötlemise eesmärgid ja vahendid on ühised või ühised on ainult mõni eesmärk või vahend või osa neist[239]. Esimene võimalus tähendab poolte väga tihedaid suhteid ja teine nõrgemaid.

Artikli 29 töörühm pooldab kaasvastutuse mõiste laiemat tõlgendamist, et võimaldada teatud paindlikkust andmetöötluse üha keerukama olukorra käsitlemisel[240]. Töörühma seisukohta näitlikustab juhtum, mis on seotud Ülemaailmse Pankadevahelise Finantstelekommunikatsiooni Ühinguga (SWIFT).

Näide: nn SWIFTi juhtumis palkasid Euroopa pangad SWIFTi haldama andmete edastamist pangatehingutes, esialgu volitatud töötlejana. SWIFT avaldas USAs asuvas andmetöötluskeskuses talletatud asjaomased andmed pangatehingute kohta USA rahandusministeeriumile, kuigi ühingu palganud Euroopa pangad ei olnud sellist korraldust otseselt andnud. Artikli 29 töörühm järeldas olukorra seaduslikkuse hindamisel, et SWIFTi kasutavaid Euroopa pangandusasutusi ja SWIFTi ennast tuleb pidada kaasvastutavateks töötlejateks, kelle vastutusel avalikustatakse Euroopa klientide andmed USA ametiasutustele[241].

Volitatud töötleja

ELi õiguses on volitatud töötleja keegi, kes töötleb isikuandmeid vastutava töötleja nimel[242]. Volitatud töötlejale usaldatud toimingud võivad olla piiratud väga spetsiifilise ülesande või valdkonnaga või olla üsna üldised ja laiahaardelised.

Euroopa Nõukogu õiguses on volitatud töötleja mõiste sama kui ELi õiguses[243].

239 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brüssel, 16. veebruar 2010, lk 19.

240 *Ibid*.

241 Artikli 29 töörühm (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brüssel, 22. november 2006.

242 Isikuandmete kaitse üldmääruse artikli 4 lõige 8.

243 Nüüdisajastatud konventsiooni nr 108 artikli 2 punkt f.

Lisaks andmete töötlemisele teiste nimel on volitatud töötlejad nende enda eesmärkidel toimuva andmetöötluse kontekstis ka ise vastutava töötleja rollis, näiteks 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 seose andmetöötlustoimingutega, mida ta teeb talle kui tööandjale kehtivate kohustuste täitmiseks.

Vastutava ja volitatud töötleja seos

Nagu öeldud, on vastutav töötleja isik või üksus, kes määrab töötlemise eesmärgid ja vahendid. Isikuandmete kaitse üldmääruses on selgelt öeldud, et volitatud töötleja tohib isikuandmeid töödelda ainult vastutava töötleja juhiste alusel[244]. Vastutava töötleja ja volitatud töötleja suhte oluline element on nendevaheline leping, mis on ka õiguslik nõue[245].

Näide: ettevõtte Päikesekiir direktor otsustab, et Päikesekiire kliendiandmeid hakkab haldama ettevõte Pilveke, kes on pilvepõhise andmesäilituse spetsialist. Ettevõte Päikesekiir jääb vastutavaks töötlejaks ja ettevõte Pilveke on üksnes volitatud töötleja, sest lepingu kohaselt võib Pilveke kasutada Päikesekiire kliendiandmeid üksnes Päikesekiire määratud eesmärkidel.

Kui volitatud töötlejale antakse õigus määrata töötlemise vahendid, peab vastutaval töötlejal olema siiski võimalus volitatud töötleja otsuseid vahendite kohta asjakohasel määral kontrollida. Üldvastutus on siiski vastutaval töötlejal, kes peab jälgima, et volitatud töötlejate otsused oleksid kooskõlas andmekaitseõigusega ja tema juhistega.

Kui volitatud töötleja ei järgi andmete kasutamisel vastutava töötleja määratud andmetöötlustingimusi, saab ka volitatud töötlejast vastutav töötleja, vähemalt seoses nende andmetega, mille korral eiratakse vastutava töötleja juhiseid. Tõenäoliselt saab sellest volitatud töötlejast ebaseaduslikult tegutsev vastutav töötleja. Algne

244 Isikuandmete kaitse üldmääruse artikkel 29.

245 *Ibid.*, artikli 28 lõige 3.

vastutav töötleja peab seevastu selgitama, kuidas oli võimalik, et volitatud töötleja rikkus volitusi[246]. Artikli 29 töörühm eeldab sellistel juhtudel, et töötlejad on kaasvastutavad, sest see tagab andmesubjektide huvide parima kaitse[247].

Samuti võib tekkida küsimusi seoses vastutuse jagunemisega olukorras, kus vastutav töötleja on väikeettevõtja ja volitatud töötleja suurettevõtja, kes määrab oma teenuse tingimused kindlaks ise. Selle olukorra kohta märgib artikli 29 töörühm siiski, et vastutuse nõudeid ei tohiks leevendada majandusliku tasakaalustamatuse alusel ja vastutava töötleja mõiste käsitlus tuleb säilitada[248].

Selguse ja läbipaistvuse huvides tuleb vastutava ja volitatud töötleja suhete üksikasjad sätestada kirjalikus lepingus[249]. Leping peab hõlmama eelkõige töötlemise sisu, olemust, eesmärki ja kestust, isikuandmete liiki ja andmesubjektide kategooriaid. Samuti tuleb selles sätestada vastutava ja volitatud töötleja kohustused ja õigused, näiteks konfidentsiaalsuse ja turvalisuse nõuded. Sellise lepingu puudumise korral rikutakse vastutava töötleja kohustust esitada kirjalikud dokumendid vastastikuse vastutuse kohta ja sellega võivad kaasneda karistused. Kui kahju on tekkinud vastutava töötleja seaduslike juhiste järgimata jätmisest või eiramisest, võidakse lisaks vastutavale töötlejale vastutusele võtta ka volitatud töötleja[250]. Töötleja peab pidama vastutava töötleja nimel tehtavate kõigi töötlemistoimingute kategooriate registrit[251]. See register tuleb järelevalveasutuse nõudmisel teha talle kättesaadavaks, sest vastutav ja volitatud töötleja peavad mõlemad oma ülesannete täitmisel tegema selle asutusega koostööd[252]. Vastutavatel ja volitatud töötlejatel on isikuandmete kaitse üldmääruse nõuete täitmise tõendamiseks võimalus järgida ka heakskiidetud toimimisjuhendit või sertifitseerimismehhanismi[253].

Mõnikord määravad volitatud töötlejad teatud ülesandeid allhanke korras täitma muid volitatud töötlejaid. See on õigusaktide alusel lubatud, kui vastutava ja

246 *Ibid.*, artikli 82 lõige 2.

247 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brüssel, 16. veebruar 2010, lk 25; artikli 29 töörühm (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brüssel, 22. november 2006.

248 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brüssel, 16. veebruar 2010, lk 26.

249 Isikuandmete kaitse üldmääruse artikli 28 lõiked 3 ja 9.

250 *Ibid.*, artikli 82 lõige 2.

251 *Ibid.*, artikli 30 lõige 2.

252 *Ibid.*, artikli 30 lõige 4 ja artikkel 31.

253 *Ibid.*, artikli 28 lõige 5 ja artikli 42 lõige 4.

volitatud töötleja vahel on kehtestatud lepingutingimused, sealhulgas see, kas vastutav töötleja peab andma selleks loa iga kord eraldi või piisab tema teavitamisest. Isikuandmete kaitse üldmääruses on sätestatud, et algne volitatud töötleja jääb vastutava töötleja ees täielikult vastutavaks, kui teine volitatud töötleja ei täida oma andmekaitsekohustusi[254].

Euroopa Nõukogu õiguses on eespool selgitatud vastutava ja volitatud töötleja tõlgendus täielikult kohaldatav[255].

2.3.2. Vastuvõtjad ja kolmandad isikud

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

Kolmas isik on isik, kes ei ole vastutav töötleja ega volitatud töötleja. Isikuandmete kaitse üldmääruse artikli 4 punkti 10 kohaselt on kolmas isik „füüsiline või juriidiline isik, avaliku sektori asutus, amet või organ, välja arvatud andmesubjekt, vastutav töötleja, volitatud töötleja ja isikud, kes võivad isikuandmeid töödelda vastutava töötleja või volitatud töötleja otseses alluvuses". See tähendab, et vastutavast töötlejast eraldi organisatsioonis töötavad isikud on kolmandad isikud (või kuuluvad kolmanda isiku juurde), isegi kui organisatsioon kuulub samasse kontserni või valdusettevõttesse. Teisalt peakontori otseses alluvuses kliendikontosid töötlevad panga harukontorid ei ole kolmandad isikud[256].

Vastuvõtja mõiste on laiem kui kolmanda isiku mõiste. Isikuandmete kaitse üldmääruse artikli 4 punkti 9 tähenduses on vastuvõtja „füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kellele isikuandmed avaldatakse, olenemata sellest, kas tegemist on kolmanda isikuga või mitte". Vastuvõtja võib olla kas muu isik kui vastutav või volitatud töötleja, – st kolmas isik – või vastutava või volitatud töötlejaga seotud isik, näiteks töötaja või sama ettevõtte või asutuse muu osakond.

Vastuvõtjaid ja kolmandaid isikuid on vaja eristada üksnes andmete õiguspärase avaldamise tingimuste tõttu. Vastutava või volitatud töötleja töötajad võivad olla

254 *Ibid.*, artikli 28 lõige 4.

255 Vt näiteks nüüdisajastatud konventsiooni nr 108 artikli 2 punktid b ja f; profiilianalüüsi soovituse artikkel 1.

256 Artikli 29 töörühm (2010), *Opinion 1/2010 on the concept of "controller" and "processor"*, WP 169, Brüssel, 16. veebruar 2010, lk 31.

isikuandmete vastuvõtjad ilma täiendava õigusliku aluseta, kui nad on kaasatud vastutava või volitatud töötleja andmetöötlustoimingutesse. Arvestades, et kolmandal isikul, kes on vastutavast töötlejast või volitatud töötlejast eraldi isik, ei ole õigust kasutada vastutava töötleja töödeldavaid isikuandmeid, v.a teatud erijuhtudel, kus selleks on konkreetne õiguslik alus.

Näide: vastutava töötleja töötaja, kes kasutab tööandja antud volituste alusel teatud isikuandmeid, on andmete vastuvõtja, kuid mitte kolmas isik, sest ta kasutab andmeid vastutava töötleja nimel ja tema juhiste järgi. Kui tööandja näiteks avalikustab töötajate isikuandmed personaliosakonnale peagi toimuvate arenguvestluste jaoks, on personaliosakond isikuandmete vastuvõtja, sest andmed on neile avalikustatud vastutava töötleja jaoks tehtava töötlemise käigus.

Samas kui organisatsioon annab oma töötajate andmed koolitusettevõttele, kes kohandab nende alusel töötajate koolitusprogrammi, on koolitusettevõte kolmas isik, sest tal ei ole töötajate isikuandmete töötlemiseks konkreetset seaduslikku alust või luba (nagu on personaliosakonnal töösuhte tõttu vastutava töötlejaga). Teisisõnu ei ole nad saanud seda teavet töösuhte raames isikuandmete vastutava töötlejaga.

2.4. Nõusolek

Põhipunktid

- Nõusolek kui isikuandmete töötlemise õiguslik alus peab olema vabatahtlik, teadlik, konkreetne ja ühemõtteline sooviavaldus selge kinnitusena, millega antakse töötlemise nõusolek.
- Eriliiki andmete töötlemiseks on vaja selgesõnalist nõusolekut.

Nagu põhjalikult käsitletakse 4. peatükis, on nõusolek üks isikuandmete töötlemise kuuest õiguspärasest alusest. Nõusolek on „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus“[257].

257 Isikuandmete kaitse üldmääruse artikli 4 lõige 11. Vt ka nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2.

ELi õiguses peab kehtiva nõusoleku jaoks olema täidetud mitu tingimust, mille eesmärk on tagada, et andmesubjektid tõeliselt nõustuvad oma andmete konkreetse kasutamisega.[258]

- Nõusolek peab olema antud kinnitusena, millega andmesubjekt annab vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt nõusoleku oma isikuandmete töötlemiseks. Selline kinnitus võib olla kas tegevus või avaldus.

- Andmesubjektil peab olema õigus võtta nõusolek millal tahes tagasi.

- Sellises kirjalikus kinnituses, mis hõlmab ka muid teemasid, näiteks teenuse tingimusi, peavad nõusoleku taotlused olema selges ja lihtsas keeles ning arusaadavas ja lihtsas vormis, milles nõusolek on teistest teemadest selgelt eristatud; kui osa kinnitusest on isikuandmete kaitse üldmäärusega vastuolus, ei ole see siduv.

Nõusolek kehtib andmekaitseõiguse kontekstis ainult siis, kui kõik need nõuded on täidetud. Vastutava töötleja ülesanne on tõendada, et andmesubjekt andis oma andmete töötlemiseks nõusoleku[259]. Kehtiva nõusoleku tingimusi käsitletakse põhjalikumalt punktis 4.1.1 (andmetöötluse seaduslikud alused).

Konventsioonis nr 108 nõusoleku määratlust sätestatud ei ole; see on jäetud riikide otsustada. **Euroopa Nõukogu õiguses** vastavad kehtiva nõusoleku tingimused siiski varem selgitatud tingimustele[260].

Kehtiva nõusoleku suhtes tsiviilõiguses kohaldatavad lisanõuded, näiteks õigus- ja teovõime, kehtivad loomulikult ka andmekaitse kontekstis, sest need nõuded on õiguslikus mõttes iseenesest mõistetavad eeltingimused. Õigus- ja teovõimeta isikute kehtetu nõusoleku korral ei ole nende andmete töötlemiseks õiguslikku alust. Alaealiste õigus- ja teovõime kohta sõlmida lepinguid on isikuandmete kaitse üldmääruses sätestatud, et kehtiva nõusoleku saamiseks vajalik vanuse alampiir ei mõjuta liikmesriikide üldist lepinguõigust[261].

258 Isikuandmete kaitse üldmääruse artikkel 7.

259 *Ibid.*, artikli 7 lõige 1.

260 Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2 ja konventsiooni seletuskirja punktid 42–45.

261 Isikuandmete kaitse üldmääruse artikli 8 lõige 3.

Nõusolek tuleb anda selgel viisil, et andmesubjekti kavatsuse kohta ei jääks mingit kahtlust[262]. Delikaatseete isikuandmete töötlemisel peab nõusolek olema selgesõnaline ja selle võib anda kas suuliselt või kirjalikult[263]. Viimane võib toimuda ka elektrooniliste vahendite abil[264]. **ELi** ja **Euroopa Nõukogu õiguse** raamistikus tuleb nõusolek oma isikuandmete töötlemiseks anda avaldusega või selget nõusolekut väljendava tegevusega[265]. Seega ei saa nõusolekut välja lugeda vaikimisest, valmis tähistusega märkeruutudest, eeltäidetud vormidest või tegevusetusest[266].

262 *Ibid*., artikli 6 lõike 1 punkt a ja artikli 9 lõike 2 punkt a.

263 *Ibid*., põhjendus 32.

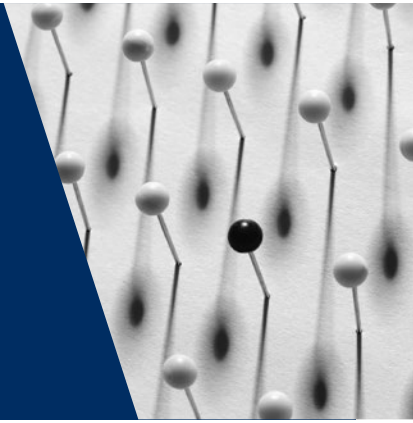
264 *Ibid*.

265 *Ibid*., artikli 4 punkt 11; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

266 Isikuandmete kaitse üldmääruse põhjendus 32; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

3

Euroopa andmekaitseõiguse üldpõhimõtted



EL	Teemad	EN
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a	**Seaduslikkuse põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 3
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a	**Õigluse põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt a EIK, *K.H. jt vs. Slovakkia*, nr 32881/04, 2009
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a ELK, C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 2015	**Läbipaistvuse põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt a ja artikkel 8 EIK, *Haralambie vs. Rumeenia*, nr 21737/03, 2009
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt b	**Eesmärgi piirangu põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland* ja *Kärntner Landesregierung jt* [suurkoda], 2014	**Võimalikult väheste andmete kogumise põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt c
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt d ELK, C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M. E. E. Rijkeboer*, 2009	**Andmete õigsuse põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt d

EL	Teemad	EN
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt e ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland* ja *Kärntner Landesregierung jt* [suurkoda], 2014	**Säilitamise piirangu põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt e EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 2008
Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt f ja artikkel 32	**Andmete turvalisuse (tervikluse ja konfidentsiaalsuse) põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikkel 7
Isikuandmete kaitse üldmääruse artikli 5 lõige 2	**Vastutuse põhimõte**	Nüüdisajastatud konventsiooni nr 108 artikkel 10

Isikuandmete kaitse üldmääruse artiklis 5 on sätestatud isikuandmete töötlemise põhimõtted. Need põhimõtted hõlmavad järgmist:

- seaduslikkus, õiglus ja läbipaistvus;
- eesmärgi piirang;
- võimalikult väheste andmete kogumine;
- andmete õigsus;
- säilitamise piirang;
- terviklus ja konfidentsiaalsus.

Nendest põhimõtetest lähtuvad määruse järgmistes artiklites esitatud üksikasjalikumad sätted. Neid põhimõtteid käsitletakse ka nüüdisajastatud konventsiooni nr 108 artiklites 5, 7, 8 ja 10. Kõik Euroopa Nõukogu või ELi tasandi hilisemad andmekaitse õigusaktid peavad järgima neid põhimõtteid ja neid tuleb arvestada nimetatud õigusaktide tõlgendamisel. ELi õiguse kohaselt on töötlemispõhimõtete piirangud lubatud ainult ulatuses, milles need vastavad artiklites 12–22 sätestatud õigustele ja kohustustele, ning need peavad olema kooskõlas põhiõiguste ja -vabaduste olemusega. ELi või riikide tasandil võidakse sätestada nende üldpõhimõtete erandid ja piirangud[267]; need peavad olema kooskõlas õigusaktidega, neil peab olema õigus-

267 Nüüdisajastatud konventsiooni nr 108 artikli 11 lõige 1; isikuandmete kaitse üldmääruse artikli 23 lõige 1.

pärane eesmärk ning need peavad olema demokraatlikus ühiskonnas vajalikud ja proportsionaalsed meetmed[268]. Kõik kolm tingimust peavad olema täidetud.

3.1. Töötlemispõhimõtete seaduslikkus, õiglus ja läbipaistvus

Põhipunktid

- Seaduslikkuse, õigluse ja läbipaistvuse põhimõtteid kohaldatakse isikuandmete mis tahes töötlemise suhtes.
- Isikuandmete kaitse üldmääruse kohaselt eeldab seaduslikkus kas
  - andmesubjekti nõusolekut;
  - vajadust sõlmida leping;
  - juriidilist kohustust;
  - vajadust kaitsta andmesubjekti või muu isiku elulisi huve;
  - vajadust täita avalikes huvides olev ülesanne;
  - vastutava töötleja või kolmanda isiku õigustatud huvide vajadust, kui andmesubjekti huvid ja õigused ei ole nende suhtes ülimuslikud.
- Isikuandmete töötlemine peab toimuma õiglaselt.
  - Andmesubjekti tuleb teavitada riskist, et töötlemisel puuduks ettenägematu negatiivne mõju.
- Isikuandmete töötlemine peab olema läbipaistev.
  - Vastutavad töötlejad peavad andmesubjekte teavitama nende andmete töötlemisest, esitades muu hulgas töötlemise eesmärgi ning vastutava töötleja isiku ja aadressi.
  - Teave töötlemistoimingute kohta peab olema selges ja lihtsas keeles, et andmesubjektidel oleks lihtne mõista asjaomaseid eeskirju, riske, kaitsemeetmeid ja õigusi.
  - Andmesubjektidel on õigus tutvuda oma andmetega olenemata nende töötlemise kohast.

268 Isikuandmete kaitse üldmääruse artikli 23 lõige 1.

3.1.1. Andmetöötluse seaduslikkus

ELi ja Euroopa Nõukogu andmekaitseõiguses nõutakse, et isikuandmeid töödeldaks seaduslikult[269]. Seaduslikuks töötlemiseks on nõutav andmesubjekti nõusolek või muu andmekaitse õigusaktides sätestatud õiguspärane põhjus[270]. Isikuandmete kaitse üldmääruse artikli 6 lõige 1 sisaldab lisaks nõusolekule viit töötlemise seaduslikku alust: töötlemine on seaduslik, kui isikuandmete töötlemine on vajalik lepingu täitmiseks, ülesande täitmiseks vastutava töötleja avaliku võimu teostamisel, juriidilise kohustuse täitmiseks, vastutava töötleja või kolmandate isikute õigustatud huvide täitmiseks või andmesubjekti eluliste huvide kaitsmiseks. Seda käsitletakse üksikasjalikult peatükis 4.1.

3.1.2. Töötlemise õiglus

Lisaks töötlemise seaduslikkusele nõutakse ELi ja Euroopa Nõukogu andmekaitseõiguses, et isikuandmeid töödeldaks õiglaselt[271]. Õiglase töötlemise põhimõte mõjutab peamiselt vastutava töötleja ja andmesubjekti suhet.

Vastutavad töötlejad peavad andmesubjekte ja üldsust teavitama, et töötlevad andmeid seaduslikult ja läbipaistvalt, ning peavad suutma tõendada töötlemistoimingute vastavust isikuandmete kaitse üldmäärusele. Andmetöötlustoimingud ei tohi olla salajased ning andmesubjektid peavad teadma võimalikke riske. Lisaks sellele peavad vastutavad töötlejad võimaluse piires püüdma ilma viivituseta täita andmesubjekti soove, eelkõige kui andmetöötluse õiguslik alus on andmesubjekti nõusolek.

> Näide: kohtuasjas *K.H. jt vs. Slovakkia*[272] viibisid kaebuse esitajaid (roma päritolu naised) raseduse ja sünnituse ajal ravil kahes Ida-Slovakkia haiglas. Hiljem ei rasestunud neist enam keegi, kuigi proovisid korduvalt. Riigisisesed kohtud otsustasid, et haiglad peavad lubama kaebuse esitajatel ja nende esindajatel tutvuda tervisekaartidega ning teha neist käsitsi väljakirjutisi,

269 Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 3; isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a.

270 Euroopa Liidu põhiõiguste harta artikli 8 lõige 2; isikuandmete kaitse üldmääruse põhjendus 40 ja artiklid 6–9; nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 41.

271 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt a.

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

kuid ei rahuldanud taotlust teha dokumentidest koopiaid, väidetavalt selleks, et takistada nende väärkasutamist. Riikide kohustused Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 alusel hõlmavad ilmtingimata ka kohustust anda andmesubjektidele koopiad nende andmetest. Riik otsustab, kuidas isikuandmeid sisaldavaid toimikuid kopeeritakse, ning (kui asjakohane) põhjendab koopiate tegemisest keeldumist. Kaebuse esitajate juhtumis põhjendasid riigisisesed kohtud kaebuse esitajatele tervisekaartidest koopiate tegemise keelamist peamiselt sellega, et seda teavet tuleb kaitsta väärkasutamise eest. EIK siiski ei mõistnud, kuidas oleksid kaebuse esitajad, kellel lubati igal juhul tutvuda oma täielike tervisekaartidega, saanud väärkasutada teavet enda kohta. Peale selle ei olnud nimetatud väärkasutamise riski ennetamiseks vaja tingimata jätta kaebuse esitajad ilma andmete koopiatest, vaid seda oleks saanud teha ka teisiti, näiteks piirates andmetele juurdepääsuga isikute hulka. Riik ei esitanud piisavalt mõjuvaid põhjuseid, miks kaebuse esitajatele ei võimaldatud tõhusat juurdepääsu nende tervise andmetele. Kohus järeldas, et rikuti artiklit 8.

Internetiteenuste korral peavad andmetöötlussüsteemide funktsioonid olema sellised, et andmesubjektid mõistaksid täielikult, mis nende andmetega tehakse. Igal juhul ei piirdu õigluse põhimõte läbipaistvuskohustustega ja võib olla seotud ka isikuandmete eetilise töötlemisega.

Näide: ülikooli teaduskond tegi uuringu, milles analüüsiti meeleolu muutusi 50 isikul. Isikud pidid registreerima oma mõtted iga tunni tagant kindlal ajal elektroonilises failis. Selles projektis osalemiseks ja andmete konkreetseks kasutuseks ülikooli poolt andis nõusoleku 50 inimest. Teaduskond avastas peagi, et elektroonilisse päevikusse kantud mõtted oleksid väga kasulikud teises vaimse tervise projektis, mida koordineeris teine uurimisrühm. Kuigi ülikool saanuks vastutava töötlejana kasutada samu andmeid teise uurimisrühma töös ilma andmetöötluse seaduslikkust tagavate täiendavate meetmeteta, sest eesmärgid olid kokkusobivad, teavitas ülikool andmesubjekte ja küsis oma eetikakoodeksit ja õiglase töötlemise põhimõtet järgides uut nõusolekut.

3.1.3. Töötlemise läbipaistvus

ELi ja Euroopa Nõukogu andmekaitseõiguses nõutakse, et isikuandmete töötlemine oleks „andmesubjektile läbipaistev“[273].

Selle põhimõttega sätestatakse vastutava töötleja kohustus võtta asjakohaseid meetmeid, et hoida andmesubjekte – kes võivad olla kasutajad või kliendid – kursis nende andmete kasutamise viisiga[274]. Läbipaistvus võib tähendada teavet, mida antakse isikule enne töötlemise alustamist[275], teavet, mis peaks olema andmesubjekti jaoks töötlemise ajal kergesti kättesaadav[276], ning ka teavet, mida antakse andmesubjektidele, kui nad on taotlenud juurdepääsu oma andmetele[277].

> Näide: kohtuasi *Haralambie vs. Rumeenia*[278] käsitles juhtumit, kus kaebuse esitajale anti juurdepääs salateenistusasutuses tema kohta hoitavatele andmetele viis aastat pärast taotluse esitamist. EIK kinnitas, et inimestele, kelle kohta säilitatakse avaliku sektori asutustes isikutoimikuid, on väga oluline, et nad saaksid nende andmetega tutvuda. Ametiasutustel on kohustus tagada tõhus menetlus, mis võimaldaks andmesubjektil teabega tutvuda. EIK arvates ei saanud viieaastast viivitust kaebuse esitaja juurdepääsutaotluse rahuldamisel põhjendada edastatud toimikute arvu 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 rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Andmetöötlustoiminguid tuleb andmesubjektidele selgitada lihtsalt mõistetaval viisil, et nad saaks aru, mida nende andmetega tegema hakatakse. See tähendab, et andmesubjekt peab isikuandmete kogumise ajal teadma isikuandmete töötlemise konkreetset põhjust[279]. Töötlemise läbipaistvus eeldab, et kasutatakse selget ja

273 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt a; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt a ja artikkel 8.

274 Isikuandmete kaitse üldmääruse artikkel 12.

275 *Ibid.*, artiklid 13 ja 14.

276 Artikli 29 töörühm (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brüssel, 8. juuni 2017, lk 23.

277 Isikuandmete kaitse üldmääruse artikkel 15.

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

279 Isikuandmete kaitse üldmäärus, põhjendus 39.

lihtsat keelt[280]. Asjaomastele isikutele peab olema selge, mis on nende isikuandmete töötlemisega seotud riskid, eeskirjad, kaitsemeetmed ja õigused[281].

Ka märgitakse **Euroopa Nõukogu õiguses**, et vastutav töötleja on kohustatud andma andmesubjektidele teatud olulise teabe ennetavalt. Teavet vastutava töötleja (või kaasvastutavate töötlejate) nime ja aadressi, andmetöötluse õigusliku aluse ja eesmärkide, töödeldavate andmete liikide ja vastuvõtjate ning õiguste teostamise vahendite kohta võib esitada mis tahes asjakohases vormingus (veebilehe, isiklikes seadmetes olevate tehnoloogiliste vahendite jne abil), kui teave esitatakse andmesubjektile õiglaselt ja tõhusalt. Esitatud teave peab olema lihtne, loetav, arusaadav ja asjaomaste andmesubjektide jaoks kohandatud (näiteks vajaduse korral lapsesõbralikus keeles). Esitada tuleb ka täiendav teave, mida on vaja õiglase andmetöötluse tagamiseks või mis on sellise eesmärgi jaoks kasulik, näiteks säilitamisperiood, andmetöötlemise aluseks olevate põhjenduste tundmine või teave andmete teise lepingupoole vastuvõtjale või kolmandast isikust vastuvõtjale edastamise kohta (samuti teave, kas see konkreetne kolmas isik tagab asjakohasel tasemel kaitse, või vastutava töötleja poolt andmekaitse asjakohase taseme tagamiseks võetud meetmete teave)[282].

Vastavalt oma andmetega tutvumise õigusele[283] on andmesubjektil õigus saada vastutavalt töötlejalt teavet, kas tema isikuandmeid töödeldakse, ning kui jah, siis mis andmeid töödeldakse[284]. Lisaks peavad vastutavad või volitatud töötlejad teabe saamise õiguse[285] kohaselt teavitama isikuid, kelle andmeid töödeldakse, töötlemise eesmärkidest, kestusest ja vahenditest ennetavalt, põhimõtteliselt enne töötlemise alustamist.

Näide: kohtuasi *Smaranda Bara jt vs. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] käsitles füüsilisest isikust ettevõtjate sissetuleku maksustamisandmete edastamist Rumeenias riiklikult maksuametilt riiklikule ravikindlustusele, mille alusel

280 *Ibid*.

281 *Ibid*.

282 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 68.

283 Isikuandmete kaitse üldmääruse artikkel 15.

284 Nüüdisajastatud konventsiooni nr 108 artikkel 8 ja artikli 9 lõike 1 punkt b.

285 Isikuandmete kaitse üldmääruse artiklid 13 ja 14.

286 ELK, C-201/14, *Smaranda Bara jt vs. Casa Naţională de Asigurări de Sănătate jt*, 1. oktoober 2015, punktid 28–46.

nõuti tervisekindlustusmaksete tasumist. Euroopa Liidu Kohtul paluti leida, kas andmesubjektile oleks pidanud andma enne nende andmete töötlemist riiklikus ravikindlustuses teavet vastutava töötleja isiku ja andmete edastamise eesmärgi kohta. ELK leidis, et kui liikmesriigi avaliku halduse asutus edastab isikuandmeid teisele avaliku halduse asutusele, kes neid andmeid edasi töötleb, tuleb andmesubjekte sellisest edastamisest või töötlemisest teavitada.

Teatud olukordades tohib teha andmesubjektide andmetöötlusest teavitamise kohustuses erandeid, mida käsitletakse üksikasjalikumalt peatükis 6.1 (andmesubjekti õigused).

3.2. Eesmärgi piirangu põhimõte

Põhipunktid

- Enne andmete töötlemist peab olema määratletud töötlemise eesmärk.
- Andmeid ei tohi edasi töödelda viisil, mis on algse eesmärgiga kokkusobimatu, kuigi isikuandmete kaitse üldmääruses on ette nähtud selle eeskirja erandid seoses avalikes huvides toimuva arhiivimise, teadus- või ajaloouuringute või statistilisel eesmärgil töötlemisega.
- Sisuliselt tähendab eesmärgi piirangu põhimõte, et isikuandmete töötlemine peab toimuma kindlal piiritletud eesmärgil ja ainult algse eesmärgiga kokkusobivatel täiendavatel, täpselt määratletud eesmärkidel.

Eesmärgi piirangu põhimõte on üks Euroopa andmekaitseõiguse põhimõtteid. See on tihedalt seotud läbipaistvuse, prognoositavuse ja kasutajate kontrolliga: kui töötlemise eesmärk on piisavalt konkreetne ja selge, teavad inimesed, mida oodata, ning läbipaistvus ja õiguskindlus on suuremad. Samal ajal on oluline eesmärgi selge piiritlemine, et andmesubjektid saaksid tõhusalt kasutada oma õigusi, näiteks vastuväidete esitamise õigust[287].

See põhimõte eeldab, et isikuandmete töötlemine peab toimuma kindlal eesmärgil ja ainult algse eesmärgiga kokkusobivatel täiendavatel, täpselt määratletud eesmärkidel[288]. Isikuandmete töötlemine ilma konkreetset ja/või piiritletud eesmärki

287 Artikli 29 töörühm (2013), *Opinion 3/2013 on purpose limitation*, WP 203, 2. aprill 2013.

288 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt b.

määratlemata on seega ebaseaduslik. Samuti ei ole seaduslik isikuandmete töötlemine ilma kindla eesmärgita, tuginedes üksnes kaalutlusele, et sellest võib olla kunagi kasu. Isikuandmete töötlemise õiguspärasus sõltub töötlemise eesmärgist, mis peab olema selge, kindlaksmääratud ja õiguspärane.

Iga uue eesmärgi puhul, mis on algse eesmärgiga kokkusobimatu, on andmete töötlemiseks vaja eraldi õiguslikku alust ning 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. Näiteks tuleb hoolikalt kaaluda isikuandmete avalikustamist kolmandatele isikutele uuel eesmärgil, sest selline avalikustamine vajab tõenäoliselt täiendavat õiguslikku alust, mis erineb andmete kogumise õiguslikust alusest.

Näide: lennuettevõtja kogub reisijatelt broneerimisel teatud andmeid, et tagada nõuetekohane lennuteenus. Lennuettevõtja vajab järgmisi andmeid: reisijate istekoha numbrid; füüsilised eripiirangud, nt ratastooli vajadus; toitlustamise erisoovid, nt koššer- või halal-toit. Kui lennuettevõtjal palutakse edastada need broneeringuinfos sisalduvad andmed sihtriigi sisserändeasutusele, kasutatakse neid seejärel sisserände kontrolli eesmärgil, mis erineb algsest andmete kogumise eesmärgist. Nende andmete edastamiseks sisserändeasutusele on seepärast vaja eraldi uut õiguslikku alust.

Konkreetse eesmärgi ulatuse ja piirangute suhtes rakendatakse nüüdisajastatud konventsioonis nr 108 ja isikuandmete kaitse üldmääruses kooskõla põhimõtet – andmete kasutamise eesmärgid peavad olema kooskõlas esialgse õigusliku alusega. Seega ei tohi andmeid edasi töödelda andmesubjektile ootamatult, sobimatult või vastumeelselt[289]. Et hinnata, kas edasist töötlemist saab pidada olevaks kooskõlas, peab vastutav töötleja arvestama (muu hulgas)

- „mis tahes seoseid sellise eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel,

- isikuandmete kogumise konteksti, eelkõige andmesubjekti ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes,

289 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 49.

- isikuandmete laadi,
- kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning
- asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes"[290]. Seda saab teha näiteks krüptimise või pseudonüümimisega.

Näide: ettevõte Päikesekiir saab kliendisuhete haldamisel kliendiandmeid. Seejärel edastab ta need andmed otseturundusettevõttele Kuukiir, kes kavatseb neid kasutada kolmandate ettevõtete turunduskampaaniate toetamisel. Päikesekiire poolt andmete edastamine muude ettevõtete turunduse eesmärgil on andmete edasine kasutamine uuel eesmärgil, mis ei ole kooskõlas ettevõtte Päikesekiir esialgse kliendiandmete kogumise eesmärgiga, mis oli kliendisuhete haldamine. Seega on andmete edastamiseks ettevõttele Kuukiir vaja eraldi õiguslikku alust.

Kui ettevõte Päikesekiir sooviks asjaomaseid kliendisuhete haldusega seotud andmeid kasutada enda turunduseesmärgil, st enda toodete turundusteabe saatmiseks klientidele, oleks see üldiselt kooskõlas esialgse eesmärgiga.

Isikuandmete kaitse üldmääruses ja nüüdisajastatud konventsioonis nr 108 märgitakse, et algse eesmärgiga *a priori* kooskõlas olevaks loetakse „isikuandmete edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil"[291]. Isikuandmete edasisel töötlemisel tuleb siiski võtta asjakohased kaitsemeetmed, näiteks andmed anonüümida, krüptida või pseudonüümida ning piirata andmetele juurdepääsu[292]. Isikuandmete kaitse üldmääruses lisatakse: „Kui andmesubjekt on andnud nõusoleku või kui töötlemine põhineb liidu või liikmesriigi õigusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, millega kaitsta eelkõige üldist avalikku huvi pakkuvaid olulisi eesmärke, peaks vastutaval töötlejal olema lubatud isikuandmeid edasi töödelda, olenemata

290 Isikuandmete kaitse üldmääruse põhjendus 50 ja artikli 6 lõige 4; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 49.

291 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt b; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b. Selliste riigisiseste sätete näide on Austria andmekaitseseadus (Datenschutzgesetz), Bundesgesetzblatt I Nr. 165/1999, punkt 46.

292 Isikuandmete kaitse üldmääruse artikli 6 lõige 4; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 50.

eesmärkidele vastavusest."[293] Edasisel töötlemisel tuleb andmesubjekti teavitada nii eesmärkidest kui ka tema õigustest, näiteks vastuväidete esitamise õigusest[294].

Näide: ettevõte Päikesekiir on kogunud oma klientidelt kliendisuhete haldusega seotud andmeid ja säilitab neid. Kui Päikesekiir soovib neid andmeid hiljem kasutada klientide ostuharjumuste statistikaanalüüsiks, on see lubatud, sest statistika eesmärk on kooskõlas olev eesmärk. Selle jaoks ei ole vaja täiendavat õiguslikku alust, näiteks andmesubjektide nõusolekut. Samas peab isikuandmete edasiseks töötlemiseks statistilisel eesmärgil ettevõte Päikesekiir võtma asjakohased andmesubjekti õiguste ja vabaduste kaitsemeetmed. Tehnilised ja korralduslikud meetmed, mida Päikesekiir peab rakendama, võivad hõlmata pseudonüümimist.

3.3. Võimalikult väheste andmete kogumise põhimõte

Põhipunktid

- Andmetöötlus peab piirduma õiguspärase eesmärgi täitmiseks vajalikuga.
- Isikuandmete töötlemine tohib toimuda ainult siis, kui töötlemise eesmärki ei saa mõistlikult täita muul viisil.
- Andmetöötlus ei tohi ebaproportsionaalselt riivata asjaomaseid huve, õigusi ega vabadusi.

Töödelda tohib ainult andmeid, mis on piisavad, asjakohased ja piirduvad eesmärgiga, mille jaoks neid kogutakse ja/või edasi töödeldakse[295]. Töötlemiseks valitud andmete liigid peavad olema vajalikud töötlemistoimingute teatatud üldeesmärgi saavutamiseks ja vastutav töötleja peab rangelt piirama andmete kogumise sellise teabe kogumiseks, sest see on otseselt seotud töötlemise konkreetse eesmärgiga.

293 Isikuandmete kaitse üldmääruse põhjendus 50.

294 *Ibid*.

295 Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt c; isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

Näide: kohtuasjas *Digital Rights Ireland*[296] analüüsis ELK, kas andmete säilitamise direktiiv, mille eesmärk on ühtlustada riigisiseseid sätteid, mis käsitlevad üldkasutatavate elektroonilise side teenuste või -võrkude loodud või töödeldud isikuandmete säilitamist nende võimalikuks edastamiseks pädevatele asutustele, et võidelda raskete kuritegude, näiteks organiseeritud kuritegevuse ja terrorismi vastu, on kehtiv. Kuigi seda peeti eesmärgiks, mis tõeliselt rahuldab üldhuvi eesmärki, peeti probleemiks üldsõnalisust, millega direktiiv hõlmas „kõiki isikuid ning kõiki elektroonilise side vahendeid ja andmeliiklusandmeid, ilma et raskete kuritegude vastu võitlemise eesmärki arvestades oleks ette nähtud mingit eristamist, piirangut või erandit“[297].

Peale selle on eraelu puutumatust soodustava eritehnoloogia kasutamisega mõnikord võimalik isikuandmete kasutamist täielikult vältida või kasutada meetmeid, millega vähendatakse andmete andmesubjektiga seostamise võimalust (nt pseudonüümimine), mille tulemuseks on eraelu puutumatust kaitsev lahendus. See on eriti asjakohane ulatuslike andmetöötlussüsteemide korral.

Näide: linnavolikogu pakub linna ühistranspordi pidevatele kasutajatele teatud tasu eest kiipkaarti. Kasutaja nimi on prinditud kaardile ja on elektrooniliselt kiibil. Bussi või trammi sisenedes tuleb kiipkaarti viibata sõidukis oleva kaardilugeri ees. Lugeri loetud andmeid kontrollitakse elektrooniliselt sõidukaardi kõigi ostjate nimedega andmebaasist.

See süsteem ei järgi võimalikult väheste andmete kogumise põhimõtet kuigi optimaalselt – kontrollimiseks, kas isikul on õigus kasutada ühissõidukit, ei ole tingimata vaja võrrelda kaardi kiibil olevaid isikuandmeid andmebaasiga. Piisaks näiteks spetsiaalsest elektroonilisest kujutisest, näiteks vöötkoodist kaardi kiibil, millega saaks kaarti kaardilugeri ees viibates kinnitada kaardi kehtivust. Selline süsteem ei salvestaks andmeid, et kes kasutas mis sõidukit millal. See oleks võimalikult väheste andmete kogumise põhimõtte järgi ka kõige optimaalsem lahendus, sest selle põhimõtte järgi peab andmete kogumine piirduma eesmärgi saavutamiseks minimaalselt vajalikuga.

296 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

297 *Ibid.*, punktid 44 ja 57.

Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 1 sisaldab nõuet, et isikuandmete töötlemine oleks proportsionaalne selle õiguspärase eesmärgi suhtes. Töötlemise kõigis etappides peavad kõik asjaomased huvid olema õiglases tasakaalus. See tähendab, et isikuandmeid, mis on piisavad ja asjakohased, kuid mis tähendaks ebaproportsionaalset sekkumist asjaomastesse põhiõigustesse ja vabadustesse, tuleks pidada liigseks[298].

3.4. Andmete õigsuse põhimõte

Põhipunktid

- Vastutav töötleja peab kõigis andmetöötlustoimingutes järgima andmete õigsuse põhimõtet.
- Ebaõiged andmed tuleb viivitamata kustutada või parandada.
- Õigsuse tagamiseks võib olla vaja andmeid korrapäraselt kontrollida ja ajakohastada.

Vastutav töötleja võib tema käsutuses olevaid isikuandmeid kasutada üksnes siis, kui ta saab olla mõistlikkuse piires kindel, et andmed on õiged ja ajakohased.[299]

Andmete õigsuse tagamise kohustust tuleb käsitleda andmetöötluse eesmärki arvestades.

Näide: kohtuasjas *Rijkeboer*[300] arutas ELK Madalmaade kodaniku taotlust saada Amsterdami linnavalitsuselt teavet, kes on isikud, kellele kohalik omavalitsus edastas kahe viimase aasta jooksul tema valduses olevaid andmeid, mis käsitlesid kaebuse esitajat, ja ka avaldatud andmete sisu kohta. ELK märkis: „Õigus eraelu puutumatusele eeldab, et andmesubjekt saab veenduda, et tema isikuandmeid töödeldakse õigesti ja seaduslikult, see tähendab eelkõige, et teda puudutavad põhiandmed on õiged ja et need saadetakse

298 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 52; isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

299 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt d; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt d.

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

heakskiidetud vastuvõtjatele.“ Seejärel viitas ELK andmekaitsedirektiivi preambulale, milles sätestatakse, et andmesubjektidel peab olema õigus tutvuda oma isikuandmetega, et kontrollida andmete õigsust[301].

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

Näide: meditsiinilise operatsiooni protokolli ei tohi muuta ehk ajakohastada isegi siis, kui hiljem selgub, et protokolli tähelepanekud olid ekslikud. Sellistel juhtudel võib protokolli tähelepanekuid üksnes täiendada, märkides selgelt, et need on hilisemad täiendused.

Teisalt on olukordi, kus andmeid on vaja ilmtingimata ajakohastada ja nende õigsust korrapäraselt kontrollida, sest andmete püsimine ebaõigena võib kahjustada andmesubjekti.

Näide: kui isik soovib sõlmida pangaga laenulepingu, kontrollib pank tavaliselt võimaliku kliendi krediidivõimet. Selleks on olemas eriandmebaasid, kus on eraisikute varasemate laenude andmed. Kui sellises andmebaasis on isiku kohta ebaõiged või aegunud andmed, võib see isikut kahjustada. Selliste andmebaaside vastutavad töötlejad peavad seega võtma erimeetmeid, et tagada andmete õigsuse põhimõtte järgimine.

3.5. Säilitamise piirangu põhimõte

Põhipunktid

- Andmete säilitamise piirangu põhimõte tähendab, et isikuandmed tuleb kustutada või anonüümida kohe, kui neid ei ole enam kogumise esialgsete eesmärkide jaoks vaja.

301 Endise direktiivi 95/46/EÜ preambul, põhjendus 41.

Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktis e ja ka nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punktis e on nõue, et „isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse". Kui eesmärgid on täidetud, tuleb andmed seega kustutada või anonüümida. Selleks „peaks vastutav töötleja kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks", tagamaks, et andmeid ei säilitata kauem kui vaja[302].

Kohtuasjas *S. ja Marper* järeldas Euroopa Inimõiguste Kohus, et Euroopa Nõukogu asjakohaste õigusaktide põhimõtete ning muude konventsiooniosaliste õiguse ja tavade kohaselt peab andmete säilitamine vastama kogumise eesmärgile ning sellel peab olema kindel tähtaeg, eelkõige politseivaldkonnas[303].

> Näide: kohtuasjas *S. ja Marper*[304] otsustas Euroopa Inimõiguste Kohus, et kaebuse mõlema esitaja sõrmejälgede, rakuproovide ja DNA-profiilide alaline säilitamine oli demokraatlikus ühiskonnas ebaproportsionaalne ja tarbetu, arvestades, et mõlema taotleja vastu algatatud kriminaalmenetlus oli lõppenud – ühe taotleja menetlus õigeksmõistva kohtuotsusega ja teise menetlus lõpetati.

Isikuandmete säilitamise tähtaeg kehtib üksnes andmesubjektide tuvastamist võimaldavate andmete suhtes. Andmeid, mida enam ei vajata, saab seega seaduslikult säilitada neid anonüümides.

Andmete arhiivimisel üldhuvides, teadus- või ajaloouuringute või statistilisel eesmärgil võib andmeid säilitada kauem, kui andmeid kasutatakse ainult nendel eesmärkidel[305]. Isikuandmete jätkuvaks säilitamiseks ja kasutamiseks tuleb andmesubjekti õiguste ja vabaduste kaitseks rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid.

Nüüdisajastatud konventsioon nr 108 lubab säilitamise piirangu põhimõttest ka erandeid, kui need on seaduses sätestatud, austavad põhiõiguste ja -vabaduste

302 Isikuandmete kaitse üldmääruse põhjendus 39.

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

304 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 4. detsember 2008.

305 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt e; nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b ja artikli 11 lõige 2.

olemust ning on piiratud arvu õiguspäraste eesmärkide saavutamiseks vajalikud ja proportsionaalsed[306]. Sellised erandid on näiteks riigi julgeoleku kaitse, kuritegude uurimine ja nende eest vastutusele võtmine, kriminaalkaristuste täideviimine, andmesubjekti kaitse ning teiste isikute õiguste ja põhivabaduste kaitse.

Näide: kohtuasjas *Digital Rights Ireland*[307] kaalutles Euroopa Liidu Kohus, kas andmete säilitamise direktiiv, mille eesmärk on ühtlustada riigisiseseid sätteid üldkasutatavate elektroonilise side teenuste või -võrkude loodud või töödeldud isikuandmete säilitamise kohta, et võidelda raskete kuritegude, näiteks organiseeritud kuritegevuse ja terrorismi vastu, on kehtiv. Andmete säilitamise direktiiviga kehtestati kohustus, et „andmeid säilitatakse mitte vähem kui kuue kuu jooksul, ilma et direktiivi artiklis 5 ette nähtud andmeliikidel tehtaks mingit vahet selle järgi, kui kasulikud võivad andmed taotletava eesmärgi seisukohalt olla või milliseid isikuid need puudutavad"[308]. ELK juhtis tähelepanu ka sellele, et andmete säilitamise direktiivis puuduvad objektiivsed kriteeriumid, mille põhjal määrata andmete säilitamise täpne kestus, mis võib olla vähemalt 6 kuud kuni 24 kuud, tagamaks, et kestus piirduks rangelt vajalikuga[309].

3.6. Andmete turvalisuse põhimõte

Põhipunktid

- Isikuandmete turvalisus ja konfidentsiaalsus on andmesubjektile tekkiva kahjuliku mõju takistamisel äärmiselt olulised.
- Turvameetmed võivad olla tehnilised ja/või korralduslikud.
- Pseudonüümimine on protsess, millega saab isikuandmeid kaitsta.
- Turvameetmete asjakohasus tuleb määrata iga kord eraldi ja korrapäraselt läbi vaadata.

306 Nüüdisajastatud konventsiooni nr 108 artikli 11 lõige 1; nüüdisajastatud konventsiooni nr 108 seletuskirja punktid 91–98.

307 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

308 *Ibid.*, punkt 63.

309 *Ibid.*, punkt 64.

Andmete turvalisuse põhimõte eeldab, et isikuandmete töötlemisel rakendatakse asjakohaseid tehnilisi või korralduslikke meetmeid, et kaitsta andmeid juhusliku, volitamata või ebaseadusliku juurdepääsu, kasutamise, muutmise, avalikustamise, kadumise, hävitamise või kahjustamise eest[310]. Isikuandmete kaitse üldmääruses märgitakse, et vastutav töötleja ja volitatud töötleja peaksid selliste meetmete rakendamisel arvestama „teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele“[311]. Olenevalt iga juhtumi konkreetsetest asjaoludest võivad asjakohased tehnilised ja korralduslikud meetmed hõlmata näiteks isikuandmete pseudonüümimist ja krüptimist ja/või meetmete tõhususe korrapärast katsetamist ja hindamist, et tagada andmete töötlemise turvalisus[312].

Nagu on selgitatud punktis 2.1.1, tähendab andmete pseudonüümimine isikuandmetes sisalduvate tunnuste – mis võimaldavad andmesubjekti tuvastada – asendamist pseudonüümiga ja nende tunnuste eraldi hoidmist tehniliste või korralduslike meetmetega. Pseudonüümimist ei tohi segi ajada anonüümimisega, kus katkestatakse kõik isiku tuvastamist võimaldavad seosed.

Näide: lause „Charles Spencer, sündinud 3. aprillil 1967, on nelja lapse (kahe poisi ja kahe tüdruku) isa“ saab pseudonüümida näiteks nii:

„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“.

Kasutajad, kellel on juurdepääs pseudonüümitud andmetele, ei saa tunnustest „324“ ega „YESz3201“ tavaliselt tuletada tunnust „Charles Spencer, sündinud 3. aprillil 1967“. Seega on sellised andmed väärkasutamise eest tõenäoliselt paremini kaitstud.

310 Isikuandmete kaitse üldmääruse põhjendus 39 ja artikli 5 lõike 1 punkt f; nüüdisajastatud konventsiooni nr 108 artikkel 7.

311 Isikuandmete kaitse üldmääruse artikli 32 lõige 1.

312 *Ibid.*

Esimese näite korral on kaitse siiski nõrgem. Kui lauset „C. S. 1967 on nelja lapse (kahe poisi ja kahe tüdruku) isa" kasutatakse Charles Spenceri kodukülas, on lihtne teda ära tunda. Pseudonüümimise meetod võib mõjutada andmekaitse tõhusust.

Sageli varjatakse isikusamasust nii, et isikuandmete atribuudid on krüptitud või neid hoitakse eraldi. Eriti kasulik on see olukorras, kus vastutavad töötlejad peavad tagama, et nad käsitlevad samade andmesubjektide andmeid, kuid nad ei pea teadma või ei tohi teada andmesubjektide tegelikku isikut. Näide: teadlane analüüsib patsientide haiguslugusid ja patsientide isikuid teab ainult nende ravihaigla, millelt teadlane sai pseudonüümitud haiguslood. Pseudonüümimine on seega oluline lüli eraelu puutumatuse tugevdamise tehnoloogias. Samuti võib see olla oluline lõimitud eraelukaitse rakendamisel. Lõimitud eraelukaitse tähendab, et andmekaitse lõimitakse andmetöötlussüsteemidesse juba nende kavandamisel.

Isikuandmete kaitse üldmääruse artiklis 25 (lõimitud andmekaitse) nimetatakse otseselt pseudonüümimist kui asjakohast tehnilist ja korralduslikku meedet, mida vastutavad töötlejad peavad rakendama andmekaitsepõhimõtete järgimiseks ja vajalike kaitsemeetmete lõimimiseks. Seda tehes täidavad vastutavad töötlejad määruse nõudeid ja kaitsevad andmesubjektide õigusi isikuandmete töötlemisel.

Heakskiidetud toimimisjuhendi või heakskiidetud sertifitseerimismehhanismi järgimine võib aidata tõendada töötlemise turvalisuse nõude täitmist[313]. Euroopa Nõukogu arvamuses isikuandmete kaitse mõju kohta broneeringuinfo töötlemisel leidub veel näiteid asjakohastest turvameetmetest isikuandmete kaitsmiseks broneeringuinfo süsteemides. Need on näiteks andmete säilitamine turvalises füüsilises keskkonnas, juurdepääsu piiramine kihiliste sisselogimistega ja tugev krüptograafia andmete edastamisel[314].

Näide: suhtlusvõrgustikud ja e-posti teenuse pakkujad võimaldavad kasutajatel lisada oma pakutavatele teenustele kahekihilise autentimise kaudu täiendava andmeturbekihi. Lisaks isikliku salasõna sisestamisele peab kasutaja isiklikule kontole sisenemiseks läbima teise sisselogimise, näiteks sisestades turvakoodi, mis saadeti tema kontoga seotud mobiiltelefoni numbrile. Nii tagab kaheetapiline kontrollimine isikuandmete parema kaitse häkkimise kaudu volitamata juurdepääsu eest.

313 *Ibid.*, artikli 32 lõige 3.

314 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD (2016)18rev, 19. august 2016, lk 9.

Nüüdisajastatud konventsiooni nr 108 seletuskirjas on täiendavad näited asjakohaste kaitsemeetmete kohta, näiteks kutsesaladuse hoidmise kohustuse rakendamine või kvalifitseeritud tehniliste turvameetmete (nt andmete krüptimine) kehtestamine[315]. Konkreetsete turvameetmete kehtestamisel peab vastutav töötleja (või volitatud töötleja, kui asjakohane) arvestama mitut tegurit, näiteks töödeldavate isikuandmete olemust ja mahtu, võimalikke kahjulikke tagajärgi andmesubjektidele ja andmetele juurdepääsu piiramise vajadust[316]. Asjakohaste turvameetmete rakendamisel tuleb arvestada andmeturbe meetodite ja andmetöötlusvahendite viimast arengut. Selliste meetmete hind peab olema proportsionaalne võimalike riskide raskuse ja tõenäosusega. Turvameetmed tuleb korrapäraselt läbi vaadata, et neid vajaduse korral ajakohastada[317].

Isikuandmetega seotud rikkumise korral nõutakse nii nüüdisajastatud konventsioonis nr 108 kui ka isikuandmete kaitse üldmääruses, et vastutav töötleja teataks põhjendamatu viivituseta pädevale järelevalveasutusele rikkumisest, mis ohustab üksikisikute õigusi ja vabadusi[318]. Sarnane andmesubjekti teavitamise kohustus kehtib ka juhul, kui isikuandmetega seotud rikkumine tekitab tõenäoliselt suure riski tema õigustele ja vabadustele[319]. Andmesubjektile asjaomaste rikkumiste kohta esitatud teade peab olema selges ja lihtsas keeles[320]. Pärast isikuandmetega seotud rikkumisest teada saamist peab volitatud töötleja sellest viivitamata teatama vastutavale töötlejale[321]. Teatud olukordades kehtib teatamiskohustuse suhtes erand – näiteks ei ole vastutav töötleja kohustatud teatama järelevalveasutusele, kui isikuandmetega seotud „rikkumise tulemusena ei teki tõenäoliselt ohtu füüsilise isiku õigustele ja vabadustele“[322]. Samuti ei ole vaja teavitada andmesubjekti, kui kasutatud rakendusmeetmed muudavad isikuandmed juurdepääsuõiguseta isikutele loetamatuks või kui hilisemad meetmed tagavad, et suure riski teke ei ole enam tõenäoline[323]. Kui andmesubjektide teavitamine isikuandmetega seotud rikkumisest nõuaks vastutavalt töötlejalt ebaproportsionaalset jõupingutust, saab teha avaliku teadaande või võtta muu sarnase meetme, „millega teavitatakse kõiki andmesubjekte võrdselt tulemuslikul viisil“[324].

315 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 56.

316 *Ibid*., punkt 62.

317 *Ibid*., punkt 63.

318 Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 2; isikuandmete kaitse üldmääruse artikli 33 lõige 1.

319 Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 2; isikuandmete kaitse üldmääruse artikli 34 lõige 1.

320 Isikuandmete kaitse üldmääruse artikli 34 lõige 2.

321 *Ibid*., artikli 33 lõige 1.

322 *Ibid*.

323 *Ibid*., artikli 34 lõike 3 punktid a ja b.

324 *Ibid*., artikli 34 lõike 3 punkt c.

3.7. Vastutuse põhimõte

Põhipunktid

- Vastutuse põhimõte tähendab, et vastutavad ja volitatud töötlejad peavad võtma aktiivselt ja järjepidevalt andmekaitse andmetöötlustoimingutes tagamise ja edendamise meetmeid.
- Vastutavad ja volitatud töötlejad vastutavad selle eest, et nende andmetöötlustoimingud oleksid kooskõlas andmekaitseõigusega ja nende vastavate kohustustega.
- Vastutav töötleja peab suutma millal tahes andmesubjektile, üldsusele ja järelevalveasutustele tõendada, et tema andmetöötlustoimingud on kooskõlas andmekaitsesätetega. Volitatud töötlejad peavad täitma ka teatud kohustusi, mis on rangelt seotud vastutusega (nt töötlemistoimingute registreerimine ja andmekaitseametniku ametisse nimetamine).

Isikuandmete kaitse üldmääruses ja nüüdisajastatud konventsioonis nr 108 sätestatakse, et vastutav töötleja vastutab käesolevas peatükis kirjeldatud isikuandmete töötlemise põhimõtete järgimise eest ning peab suutma seda tõendada[325]. Selleks peab vastutav töötleja võtma asjakohaseid tehnilisi ja korralduslikke meetmeid[326]. Kuigi isikuandmete kaitse üldmääruse artikli 5 lõikes 2 sätestatud vastutuse põhimõte on suunatud üksnes vastutavatele töötlejatele, eeldatakse, et vastutavad ka volitatud töötlejad, sest nad peavad täitma mitut kohustust ja on vastutusega tihedalt seotud.

ELi ja Euroopa Nõukogu andmekaitse õigusaktides sätestatakse samuti, et vastutav töötleja vastutab vastavuse eest peatükkides 3.1–3.6 käsitletud andmekaitsepõhimõtetele ja peab suutma seda tagada[327]. Artikli 29 töörühm märgib, et „menetluste liigid ja mehhanismid oleneksid töötlusest ja andmeliikidest tulenevatest riskidest“[328].

325 *Ibid.*, artikli 5 lõige 2; nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 1.

326 Isikuandmete kaitse üldmääruse artikkel 24.

327 *Ibid.*, artikli 5 lõige 2; nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 1.

328 Artikli 29 töörühm (2010), *Opinion 3/2010 on the principle of accountability*, WP 173, Brüssel, 13. juuli 2010, punkt 12.

Vastutavad töötlejad võivad soodustada selle nõude täitmist mitmeti, näiteks järgmisega:

- andmetöötlustoimingute registreerimine ja taotluse korral registri kättesaadavaks tegemine järelevalveasutusele[329];
- teatud olukordades andmekaitseametniku määramine, kes osaleb kõigis isikuandmete kaitsega seotud küsimustes[330];
- andmekaitse mõju hindamine selliste töötlemisviiside korral, millega tõenäoliselt kaasneb suur risk füüsiliste isikute õigustele ja vabadustele[331];
- lõimitud andmekaitse ja vaikimisi andmekaitse tagamine[332];
- andmesubjektide õiguste kasutamise korra ja menetluste rakendamine[333];
- heakskiidetud toimimisjuhendite või sertifitseerimismehhanismide järgimine[334].

Kuigi isikuandmete kaitse üldmääruse artikli 5 lõikes 2 sätestatud vastutuse põhimõte ei ole konkreetselt suunatud volitatud töötlejatele, on selles vastutuse sätted, mis sisaldavad ka volitatud töötlejate kohustusi, näiteks isikuandmete töötlemise toimingute registreerimine ja andmekaitseametniku määramine isikuandmete töötlemise mis tahes toimingu korral, mis seda nõuab[335]. Volitatud töötlejad peavad ka tagama, et kõik andmete turvalisuse tagamiseks vajalikud meetmed on rakendatud[336]. Vastutava ja volitatud töötleja vahelises õiguslikult siduvas lepingus peab olema sätestatud, et volitatud töötleja aitab vastutaval töötlejal täita teatud järgimisnõudeid, näiteks andmekaitse mõju hindamisel või vastutava töötleja teavitamisel mis tahes isikuandmetega seotud rikkumisest kohe, kui ta saab sellest teada[337].

329 Isikuandmete kaitse üldmääruse artikkel 30.

330 *Ibid.*, artiklid 37–39.

331 *Ibid.*, artikkel 35; nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 2.

332 Isikuandmete kaitse üldmääruse artikkel 25; nüüdisajastatud konventsiooni nr 108 artikli 10 lõiked 2 ja 3.

333 *Ibid.*, artiklid 12 ja 24.

334 *Ibid.*, artiklid 40 ja 42.

335 *Ibid.*, artikli 5 lõige 2, artiklid 30 ja 37.

336 *Ibid.*, artikli 28 lõike 3 punkt c.

337 *Ibid.*, artikli 28 lõike 3 punkt d.

Majanduskoostöö ja Arengu Organisatsioon (OECD) võttis 2013. aastal vastu eraelu puutumatuse suunised, milles rõhutati, et vastutavatel töötlejatel on oluline roll andmekaitse toimimise tagamisel. Suunised sisaldavad vastutuse põhimõtet, sätestades, et vastutav töötleja vastutab suunistes kehtestatud põhimõtete jõustamise meetmete võtmise eest[338].

Näide: õigusaktidest võib vastutuse põhimõtte rõhutamisega seoses esile tõsta e-privaatsuse direktiivi 2002/58/EÜ 2009. aasta muutmisdirektiivi[339]. Muudetud artiklis 4 sätestatakse direktiivis kohustus („tagatakse isikuandmete töötlemise turvapoliitika rakendamine"). Seega otsustas seadusandja, et direktiivis käsitletavatesse turbesätetesse on vaja sisse tuua sõnaselge turbepoliitika kehtestamise ja rakendamise nõue.

Artikli 29 töörühma arvamuse[340] kohaselt on vastutuse põhiolemus, et vastutav töötleja peab

- kehtestama meetmed, mis tagaksid tavapärastes tingimustes andmekaitse-eeskirjade täitmise andmetöötlustoimingute ajal;
- koostama dokumendid, millega tõendatakse andmesubjektidele ja järelevalveasutustele, mis meetmed on andmekaitse-eeskirjade täitmiseks võetud.

Vastutuse põhimõtte alusel peavad vastutavad töötlejad seega aktiivselt tõendama, et nende tegevus on nõuetekohane, ning mitte üksnes ootama, et andmesubjektid või järelevalveasutused osutaksid puudustele.

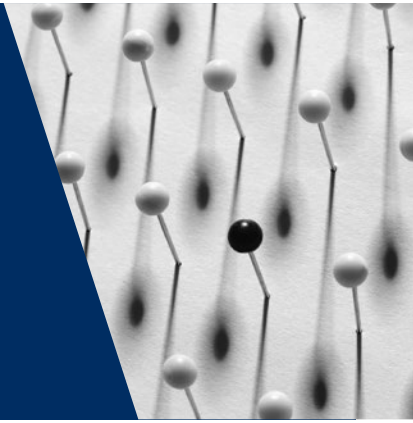
338 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, artikkel 14.

339 Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiv 2009/136/EÜ, 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 2009 L 337, lk 11.

340 Artikli 29 töörühm (2010), *Opinion 3/2010 on the principle of accountability*, WP 173, Brüssel, 13. juuli 2010.

4

Euroopa andmekaitseõiguse eeskirjad



EL	Teemad	EN
Andmete seadusliku töötlemise eeskirjad		
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt a ELK, C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 2011 ELK, C-536/15, *Tele2 (Netherlands) BV jt vs. Autoriteit Consument en Markt (AMC)*, 2017	**Nõusolek**	Profiilianalüüsi soovituse punkti 3.4 alapunkt b ja punkt 3.6 Nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt b	**Lepinguline (lepingueelne) suhe**	Profiilianalüüsi soovituse punkti 3.4 alapunkt b
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt c	**Vastutava töötleja seadusejärgsed kohustused**	Profiilianalüüsi soovituse punkti 3.4 alapunkt a
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt d	**Andmesubjekti elulised huvid**	Profiilianalüüsi soovituse punkti 3.4 alapunkt b
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e ELK, C-524/06, *Huber vs. Bundesrepublik Deutschland* [suurkoda], 2008	**Avalikud huvid ja avaliku võimu teostamine**	Profiilianalüüsi soovituse punkti 3.4 alapunkt b

EL	Teemad	EN
Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f ELK, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*, 2017 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*, 2011	**Teiste isikute õigustatud huvid**	Profiilianalüüsi soovituse punkti 3.4 alapunkt b EIK, *Y vs. Türgi*, nr 648/10, 2015
Isikuandmete kaitse üldmääruse artikli 6 lõige 4	**Eesmärgi piirangu erand: täiendav töötlemine muudel eesmärkidel**	Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b
Delikaatsete andmete seadusliku töötlemise eeskirjad		
Isikuandmete kaitse üldmääruse artikli 9 lõige 1	**Üldine töötlemiskeeld**	Nüüdisajastatud konventsiooni nr 108 artikkel 6
Isikuandmete kaitse üldmääruse artikli 9 lõige 2	**Üldise keelu erandid**	Nüüdisajastatud konventsiooni nr 108 artikkel 6
Turvalise töötlemise eeskirjad		
Isikuandmete kaitse üldmääruse artikkel 32	**Kohustus tagada töötlemise turvalisus**	Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 1 EIK, *I vs. Soome*, nr 20511/03, 2008
Isikuandmete kaitse üldmääruse artikkel 28 ja artikli 32 lõike 1 punkt b	**Kohustus tagada konfidentsiaalsus**	Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 1
Isikuandmete kaitse üldmääruse artikkel 34 Eraelu puutumatuse ja elektroonilise side direktiivi artikli 4 lõige 2	**Isikuandmetega seotud rikkumistest teatamine**	Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 2
Vastutuse ja nõuetele vastavuse edendamise eeskirjad		
Isikuandmete kaitse üldmääruse artiklid 12, 13 ja 14	**Läbipaistvus üldiselt**	Nüüdisajastatud konventsiooni nr 108 artikkel 8
Isikuandmete kaitse üldmääruse artiklid 37, 38 ja 39	**Andmekaitse-ametnikud**	Nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 1

EL	Teemad	EN
Isikuandmete kaitse üldmääruse artikkel 30	**Isikuandmete töötlemise toimingute registreerimine**	
Isikuandmete kaitse üldmääruse artiklid 35 ja 36	**Mõjuhinnang ja eelkonsulteerimine**	Nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 2
Isikuandmete kaitse üldmääruse artiklid 33 ja 34	**Isikuandmetega seotud rikkumistest teatamine**	Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 2
Isikuandmete kaitse üldmääruse artiklid 40 ja 41	**Toimimisjuhendid**	
Isikuandmete kaitse üldmääruse artiklid 42 ja 43	**Sertifitseerimine**	
Lõimitud ja vaikimisi andmekaitse		
Isikuandmete kaitse üldmääruse artikli 25 lõige 1	**Lõimitud andmekaitse**	Nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 2
Isikuandmete kaitse üldmääruse artikli 25 lõige 2	**Vaikimisi andmekaitse**	Nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 3

Põhimõtete olemus on alati üldine. Nende rakendamine konkreetsetes olukordades jätab teatud tõlgendamisruumi ja valikuvabaduse. **Euroopa Nõukogu õiguses** saavad nüüdisajastatud konventsiooni nr 108 osalised määrata tõlgendusruumi suuruse riigisiseste õigusaktidega. **Euroopa Liidu õigus** on teistsugune – siseturu andmekaitse kehtestamisel otsustati, et ELi tasandil tuleb rakendada üksikasjalikumaid eeskirju, et liikmesriikide õigusaktidega tagatud andmekaitse tase oleks ühtlane. Andmekaitse üldmääruse artikli 5 põhimõtetes kehtestatakse mitu üksikasjalikku eeskirja, mis on riigisiseses õiguskorras vahetult kohaldatavad. Sel põhjusel käsitlevad järgmised tähelepanekud Euroopa tasandi üksikasjalike andmekaitse-eeskirjade kohta peamiselt ELi õigust.

4.1. Andmete seadusliku töötlemise eeskirjad

Põhipunktid

- Isikuandmete töötlemine on seaduslik, kui see vastab ühele järgmistest kriteeriumidest:
  - töötlemine põhineb andmesubjekti nõusolekul;
  - lepinguline suhe nõuab isikuandmete töötlemist;
  - töötlemist on vaja vastutava töötleja seadusjärgse kohustuse täitmiseks;
  - töötlemist on vaja andmesubjekti või muu isiku eluliste huvide kaitsmiseks;
  - töötlemist on vaja avalike huvidega seotud ülesande täitmiseks;
  - töötlemist on vaja vastutavate töötlejate või kolmandate isikute õigustatud huvide tõttu, kui nimetatud huvide suhtes ei ole ülimuslikud andmesubjektide huvid või põhiõigused.
- Delikaatsete isikuandmete töötlemise seaduslikkuse tagamiseks peab töötlemine vastama rangematele erinõuetele.

4.1.1. Andmete töötlemise õiguspärased põhjused

Isikuandmete kaitse üldmääruse II peatükis „Põhimõtted“ on sätestatud, et isikuandmete töötlemine peab esiteks vastama andmekvaliteedi põhimõtetele, mis on sätestatud määruse artiklis 5. Üks põhimõtteid on, et isikuandmete töötlemisel tagatakse, et „töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev“. Teiseks, et andmeid saaks töödelda seaduslikult, peab töötlemine vastama seaduslikule alusele, mis muudab andmete töötlemise õiguspäraseks. Need on loetletud määruse artiklis 6[341] (tavaliste isikuandmete korral) ja artiklis 9 (eriliiki isikuandmete või delikaatsete andmete korral). Ka nüüdisajastatud konventsiooni nr 108 II peatükis, millega kehtestatakse isikuandmete kaitse aluspõhimõtted, sätestatakse, et andmete töötlemise seaduslikkuseks peab see olema „proportsionaalne taotletava õiguspärase eesmärgi suhtes“.

341 ELK, liidetud kohtuasjad C-465/00, C-138/01 ja C-139/01, *Rechnungshof vs. Österreichischer Rundfunk jt* ja *Christa Neukomm ja Jospeh Lauermann vs. Österreichischer Rundfunk*, 20. mai 2003, punkt 65; ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008, punkt 48; 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 26.

Olenemata töötlemise õiguslikust alusest, millele vastutav töötleja tugineb, et algatada isikuandmete töötlemise toiming, peab ta kohaldama ka isikuandmete kaitse üldõiguses sätestatud kaitsemeetmeid.

Nõusolek

Euroopa Nõukogu õiguses on nõusolekut käsitletud nüüdisajastatud konventsiooni nr 108 artikli 5 lõikes 2. Sellele on osutatud ka Euroopa Inimõiguste Kohtu kohtupraktikas ja mitmes Euroopa Nõukogu soovituses[342]. **ELi õiguses** on nõusolek seadusliku andmetöötluse alusena kehtestatud isikuandmete kaitse üldmääruse artiklis 6 ning sellele on selge sõnaga viidatud ka põhiõiguste harta artiklis 8. Kehtiva nõusoleku omadusi selgitatakse nõusoleku määratluses isikuandmete kaitse üldmääruse artiklis 4, kehtiva nõusoleku saamise tingimused on üksikasjalikult sätestatud artiklis 7 ning erieeskirjad, mida kohaldatakse lapse nõusolekule seoses infoühiskonna teenustega, on kehtestatud artiklis 8.

Nagu on selgitatud peatükis 2.4, peab nõusolek olema vabatahtlik, teadlik, konkreetne ja üheselt mõistetav. Nõusolek peab olema avaldus või selget nõusolekut väljendav tegevus, mis kinnitab nõusolekut isikuandmete töötlemiseks, ning isikul on õigus oma nõusolek millal tahes tagasi võtta. Vastutavatel töötlejatel on kohustus kontrollitavalt dokumenteerida nõusolekut.

Vabatahtlik nõusolek

Euroopa Nõukogu nüüdisajastatud konventsiooni nr 108 raamistikus peab andmesubjekti nõusolek olema tahtliku valiku vaba tahteavaldus[343]. Vabatahtlik nõusolek kehtib üksnes juhul, „kui andmesubjektil on võimalik teha tegelik valik ning puudub pettuse, heidutamise, sunni või märkimisväärsete negatiivsete tagajärgede oht nõusolekust keeldumise korral“[344]. Seetõttu on **ELi õiguses** sätestatud, et nõusolekut ei loeta vabatahtlikult antuks, „kui andmesubjektil pole tõelist või vaba valikuvõimalust või ta ei saa kahjulike tagajärgedeta nõusoleku andmisest keelduda või seda tagasi võtta“[345]. Isikuandmete kaitse üldmääruses rõhutatakse: „Selle hindamisel,

342 Vt näiteks Euroopa Nõukogu ministrite komitee (2010), *Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23. november 2010, artikli 3.4 punkt b.

343 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

344 Vt ka artikli 29 töörühm (2011), *Opinion 15/2011 on the notion of consent*, WP 187, Brüssel, 13. juuli 2011, lk 12.

345 Isikuandmete kaitse üldmääruse põhjendus 42.

kas nõusolek anti vabatahtlikult, tuleb võimalikult suurel määral võtta arvesse asjaolu, kas lepingu täitmise, sealhulgas teenuse osutamise tingimuseks on muu hulgas seatud nõusoleku isikuandmine andmete töötlemiseks, mis ei ole vajalik kõnealuse lepingu täitmiseks."[346] Nüüdisajastatud konventsiooni nr 108 seletuskirjas on öeldud, et „andmesubjekti puhul ei või kasutada lubamatut mõjutamist või survet (mis võib olla majanduslikku või muud laadi), olgu tegemist otsese või kaudse mõjutamise või survega, ning nõusolekut ei tuleks pidada vabatahtlikult antuks, kui andmesubjektil puudub tegelik valik või kui ta ei saa nõusoleku andmisest ilma piiranguteta keelduda või seda tagasi võtta"[347].

Näide: mõned riigi A kohalikud omavalitsused otsustasid välja töötada sisseehitatud kiibiga elamiskaardid. Elanikud ei ole kohustatud neid elektroonilisi kaarte hankima. Samas puudub kaardita elanikel juurdepääs mitmele olulisele haldusteenusele, näiteks ei saa nad tasuda veebis kohalikke makse, esitada kaebusi elektrooniliselt (et asutuse kohustus vastata kolme päeva jooksul toimiks nende kasuks) ning isegi vältida järjekordi, osta kohaliku omavalitsuse hallatavatesse kontserdisaalidesse soodushinnaga pileteid ega kasutada sissepääsul skannerit.

Selles näites ei saa isikuandmete töötlemine kohalikus omavalitsuses põhineda nõusolekul. Et elektroonilise kaardi saamiseks ja isikuandmete töötlemiseks nõusoleku saamiseks avaldatakse elanikele vähemalt kaudset survet, ei ole nõusolek vabatahtlik. Omavalitsused peavad elektrooniliste kaartide süsteemi väljatöötamisel kasutama isikuandmete töötlemise õigustamiseks muud õiguslikku alust. Nad võivad näiteks põhjendada, et isikuandmete töötlemine on vaja avalikes huvides oleva ülesande täitmiseks, mis on isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e kohaselt isikuandmete töötlemise üks seaduslikke aluseid[348].

Nõusolek ei pruugi olla vabatahtlik ka alluvusega seotud juhtudel, kui nõusolekut taotlev vastutav töötleja ja nõusolekut andev andmesubjekt on majanduslikult või

346 *Ibid.*, artikli 7 lõige 4.

347 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

348 Artikli 29 töörühm (2011), *Opinion 15/2011 on the definition of consent*, WP 187, Brüssel, 13. juuli 2011, lk 16. Täiendavad näited juhtumitest, kus andmete töötlemine ei saa põhineda nõusolekul, kuid mis eeldab muud õiguslikku alust, et isikuandmete töötlemine oleks õiguspärane, on arvamuses lk 14 ja 17.

muul põhjusel oluliselt ebavõrdsed[349]. Sellise ebavõrdsuse ja alluvuse tüüpiline näide on see, et tööandja töötleb isikuandmeid töösuhte kontekstis. Artikli 29 töörühma järgi ei saa töötajad tööandja-töötaja suhtest tuleneva sõltuvuse tõttu peaaegu kunagi nõusolekut vabalt anda, mitte anda või tühistada. Arvestades võimutasakaalu puudumist, võivad töötajad anda erandkorras vaba nõusoleku ainult siis, kui tagajärjed ei ole seotud pakkumise vastuvõtmise ega tagasilükkamisega[350].

Näide: suurettevõte kavatseb koostada kataloogi kõigi töötajate nimede, ametiülesannete ja tööaadressidega üksnes selleks, et parandada ettevõttesisest suhtlust. Personalijuht teeb ettepaneku lisada kataloogi ka iga töötaja foto, et kolleege oleks näiteks koosolekutel lihtsam ära tunda. Töötajate esindajad nõuavad, et kataloogi lisataks fotod üksnes töötajatest, kes annavad selleks eraldi nõusoleku.

Sellises olukorras tuleb töötaja nõusolekut käsitada õigusliku alusena fotode töötlemiseks kataloogis, sest võib arvata, et sellel puuduvad töötajale mis tahes tagajärjed, olenemata sellest, kas ta nõustub või ei nõustu foto avaldamisega kataloogis.

Näide: äriühing A kavandab koosolekut, kus osalevad selle kolm töötajat ja äriühingu B juhatajad, et arutada võimalikku projektikoostööd tulevikus. Koosolek toimub äriühingu B ruumides. Äriühing B küsib äriühingult A koosolekul osalejate nimed, CVd ja fotod. Äriühing B väidab, et tal on vaja osalejate nimesid ja fotosid, et turvatöötajad saaksid hoone sissepääsu juures kontrollida, kas tegu on õigete isikutega, ning CVd võimaldavad juhatajatel paremini koosolekuks valmistuda. Sellisel juhul ei saa äriühing A edastada oma töötajate isikuandmeid nõusoleku alusel. Nõusolekut ei saa pidada „vabatahtlikult antuks", sest on võimalik, et pakkumise tagasilükkamisel on töötajatele negatiivsed tagajärjed (näiteks võidakse töötaja asendada muu töötajaga, kes peale koosolekul osalemise tema asemel suhtleb edaspidi ka äriühinguga B ning aitab üldiselt projektile kaasa). Isikuandmete töötlemine peab seega põhinema muul isikuandmete töötlemise seaduslikul alusel.

349 Vt ka artikli 29 töörühm (2001), *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, Brüssel, 13 september 2001; artikli 29 töörühm (2005), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brüssel, 25 november 2005; artikli 29 töörühm (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brüssel, 8. juuni 2017.

350 Artikli 29 töörühm (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brüssel, 8. juuni 2017.

See ei tähenda siiski, et nõusolek ei saa kunagi olla kehtiv tingimustel, kui mittenõustumisel võib olla mõningaid negatiivseid tagajärgi. Näiteks kui kaupluse kliendikaardi väljastamisega mittenõustumise tagajärg on üksnes see, et klient ei saa teatud kaupadelt väikest allahindlust, võib nõusolek siiski olla kehtiv õiguslik alus, et töödelda kliendikaardi väljastamiseks nõusoleku andnud klientide isikuandmeid. Ettevõtte ja kliendi vahel alluvussuhe puudub ja mittenõustumise tagajärjed ei ole andmesubjekti jaoks vaba valiku välistamiseks piisavalt rasked (kui hinnaalandus on piisavalt väike, et mitte mõjutada nende vaba valikut).

Samas kui kaupu või teenuseid saab osta ainult siis, kui teatud isikuandmeid avaldatakse vastutavale töötlejale või antakse edasi kolmandatele isikutele, ei ole andmesubjekti nõusolek oma andmete (mis ei ole lepingu jaoks vajalikud) avaldamiseks vabatahtlik ning seega ei ole see andmekaitseõiguse seisukohalt ka kehtiv[351]. Isikuandmete kaitse üldmääruses on nõusoleku sidumine kaupade ja teenuste pakkumisega üsna rangelt keelatud[352].

Näide: kui reisijad lubavad lennuettevõtjal edastada broneeringuinfot (isikusamasuse, söömisharjumiste või terviseprobleemide andmeid) konkreetse välisriigi sisserändeasutustele, ei ole andmekaitseõiguse alusel tegu kehtiva nõusolekuga, sest sinna riiki reisida soovijatel ei ole valikuvõimalust. Et broneeringuinfo edastamine oleks seaduslik, on nõusoleku asemel vaja muud õiguslikku alust, tõenäoliselt eriotstarbelist õigusakti.

Teadlik nõusolek

Andmesubjektil peab enne valiku tegemist olema piisavalt teavet. Tavaliselt on teadlikuks nõusolekuks vaja nõusoleku eseme täpset ja lihtsalt arusaadavat kirjeldust. Artikli 29 töörühma selgituse kohaselt peab nõusolek rajanema andmesubjekti andmete töötlemiseks nõusoleku andmisega seotud tegevust kajastavate faktide ja tagajärgede teadmisel ja mõistmisel. „Isikule tuleb anda selgelt ning arusaadavalt täpne ja täielik teave seonduvates [...] küsimustes, nagu töödeldavate andmete laad, töötlemise eesmärk, isikud, kellele andmed võidakse edastada, ja andmesubjekti õigused.“[353] Et nõusolek oleks teadlik, peavad üksikisikud ka teadvustama isikuandmete töötlemisega mittenõustumise tagajärgi.

351 Isikuandmete kaitse üldmääruse artikli 7 lõige 4.

352 *Ibid*.

353 Artikli 29 töörühm (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Brüssel, 15. veebruar 2007.

Teadliku nõusoleku olulisust arvestades püüti mõistet selgitada isikuandmete kaitse üldmääruses ja nüüdisajastatud konventsiooni nr 108 seletuskirjas. Isikuandmete kaitse üldmääruse põhjenduspunktides on sätestatud, et teadlik nõusolek tähendab, et selle „andmiseks peaks andmesubjekt olema teadlik vähemalt sellest, kes on vastutav töötleja ja milleks kavatsetakse isikuandmeid töödelda“[354].

Erandolukorras, kui nõusolekut kasutatakse erandina, et tagada rahvusvahelise andmeedastuse seaduslik alus, peab vastutav töötleja teavitama andmesubjekti edastamise sellistest võimalikest riskidest, mis tulenevad andmekaitse piisavuse otsuse ja asjakohaste kaitsemeetmete puudumisest, et tema nõusolekut saaks pidada kehtivaks[355].

Nüüdisajastatud konventsiooni nr 108 seletuskirjas märgitakse, et teavet tuleb anda andmesubjekti otsuse mõju kohta, nimelt nõusoleku andmise tähenduse ja ulatuse kohta[356].

Oluline on teabe kvaliteet. Teabe kvaliteet tähendab, et teave peab olema selle eeldatavatele vastuvõtjatele arusaadavas keeles. Teabe esitamisel tuleb vältida kantseliiti, see peab olema lihtsas ja selges keeles, et see oleks tavalisele kasutajale mõistetav[357]. Teave peab olema andmesubjektile ka kergesti kättesaadav ning seda võib esitada suuliselt või kirjalikult. Olulised tegurid on teabe kättesaadavus ja nähtavus: teave peab olema selgelt nähtav ja märgatav. Internetikeskkonnas võib hea lahendus olla kihilised teated, kus andmesubjekt saab valida, kas lugeda teabe lühiülevaadet või üksikasjalikumat varianti.

Konkreetne nõusolek

Et nõusolek oleks kehtiv, peab see täpsustama ka töötlemise eesmärki, mida tuleb kirjeldada selgelt ja ühemõtteliselt. Lisaks peab nõusoleku eesmärgi teave olema kvaliteetne. Selles kontekstis on asjakohased keskmise andmesubjekti mõistlikud eeldused. Kui andmetöötlustoiminguid kavatsetakse lisada või muuta nii, mida ei oleks mõistlikult saanud algse nõusoleku andmise ajal eeldada ning mille tõttu töötlemise eesmärk muutub, tuleb küsida andmesubjektilt uuesti nõusolekut. Kui töötlemisel on mitu eesmärki, tuleb nõusolek anda kõigi eesmärkide kohta[358].

354 Isikuandmete kaitse üldmääruse põhjendus 42.

355 *Ibid*., artikli 49 lõike 1 punkt a.

356 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

357 Artikli 29 töörühm (2011), *Opinion 15/2011 on the definition of consent*, WP 187, Brüssel, 13. juuli 2011, lk 19.

358 Isikuandmete kaitse üldmääruse põhjendus 32.

Näited: ELK käsitles kohtuasjas *Deutsche Telekom AG*[359] küsimust, kas sideettevõtja, kellel oli vaja edastada abonentide isikuandmeid, pidi küsima andmesubjektidelt nõusoleku taaskinnitamist[360], sest andmete vastuvõtjad ei olnud nõusoleku andmise ajal nimetatud.

ELK leidis, et eraelu puutumatuse ja elektroonilise side direktiivi artikli 12 alusel ei ole enne andmete edastamist vaja uut nõusolekut. Andmesubjektid said nõustuda üksnes töötlemise eesmärgiga, st nende andmete avaldamisega, ning ei saanud valida, mis kataloogides lubada neid andmeid avaldada.

ELK 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“[361]. Lisaks võib „juba isikuandmete avaldamine teatava otstarbega kataloogis [...] osutuda abonenti kahjustavaks“[362] ega ole andmete avaldaja isikusamasuse küsimus.

Kohtuasi *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV vs. Autoriteit Consument en Markt (AMC)*[363] käsitles Belgia äriühingu nõuet, et numbriinfo- ja kataloogiteenuste äriühingud, kes annavad telefoninumbreid Madalmaades, peavad võimaldama äriühingutel tutvuda abonentide andmetega. Belgia äriühing tugines universaalteenuste direktiivis[364] sätestatud kohustusele. Selle kohaselt nõutakse telefoninumbreid andvatelt äriühingutelt, et nad teeksid numbrid kättesaadavaks kataloogiteenuste ettevõtjatele, kes neid taotlevad, kui abonendid on andnud nõusoleku oma numbrite avaldamiseks. Madalmaade äriühingud keeldusid seda tegemast, väites, et nad ei ole kohustatud esitama asjaomaseid andmeid teises liikmesriigis asutatud

359 ELK, C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 5. mai 2011. Vt eelkõige punktid 53 ja 54.

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

361 ELK, C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 5. mai 2011; punkt 61.

362 *Ibid.*, punkt 62.

363 ELK, C-536/15, *Tele2 (Netherlands) BV jt vs. Autoriteit Consument en Markt (AMC)*, 15. märts 2017.

364 Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul (universaalteenuse direktiiv), EÜT L 108, 2002, lk 51, mida on muudetud Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiviga 2009/136/EÜ (universaalteenuste direktiiv), ELT 2009 L 337, lk 11.

ettevõtjale. Nad väitsid, et kasutajad andsid nõusoleku oma numbrite avaldamiseks tingimusel, et need avaldatakse Madalmaade kataloogis. ELK leidis, et universaalteenuste direktiiv hõlmab kõiki kataloogiteenuste ettevõtjate taotlusi, olenemata sellest, mis liikmesriigis nad on asutatud. Samuti leidis ELK, et samade andmete edastamine muule ettevõtjale nende andmete avaldamiseks üldkasutatavas kataloogis, ilma et asjaomaselt abonendilt oleks saadud uut nõusolekut, ei saa kahjustada õigust isikuandmete kaitsele[365]. Nendel kaalutlustel ei tule abonentidele telefoninumbreid andval ettevõtjal küsida abonendilt eraldi nõusolekut iga liikmesriigi kohta, kuhu andmeid tema kohta võib edastada[366].

Ühemõtteline nõusolek

Kogu nõusolek tuleb anda ühemõtteliselt[367]. See tähendab, et ei saa olla põhjendatud kahtlust, et andmesubjekt tahtis väljendada enda nõusolekut oma andmete töötlemiseks. Näiteks ei näita andmesubjekti tegevusetus ühemõttelist nõusolekut.

Nii oleks see vastutavate töötlejate korral, kui nad saavad nõusoleku privaatsusteadete kaudu, näiteks teatega „meie teenuse kasutamisel nõustute oma isikuandmete töötlemisega". Sellisel juhul võib olla vaja, et vastutavad töötlejad peavad tagama, et kasutajad annavad sellistele põhimõtetele käsitsi ja ükshaaval nõusoleku.

Kui nõusolek on antud lepingu osaks olevas kirjalikus vormis, peab nõusolek isikuandmete töötlemiseks olema individuaalne ja igal juhul „tuleks kaitsemeetmetega tagada, et andmesubjekt on teadlik nõusoleku andmisest ja nõusoleku andmise ulatusest"[368].

Nõuded laste nõusolekule

Isikuandmete kaitse üldmäärusega pakutakse lastele infoühiskonna teenuste osutamise raames erilist kaitset, sest „lapsed ei pruugi olla piisavalt teadlikud asjaomastest ohtudest, tagajärgedest ja kaitsemeetmetest ning oma õigustest seoses

365 ELK, C-536/15, *Tele2 (Netherlands) BV jt vs. Autoriteit Consument en Markt (AMC)*, 15. märts 2017, punkt 36.

366 *Ibid*., punktid 40–41.

367 Isikuandmete kaitse üldmääruse artikli 4 lõige 11.

368 *Ibid*., põhjendus 42.

isikuandmete töötlemisega“[369]. Seega, vastavalt **ELi õigusele**, kui infoühiskonna teenuste osutajad töötlevad alla 16-aastaste laste isikuandmeid nõusoleku alusel, on selline andmete töötlemine seaduslik „üksnes sellisel juhul ja sellises ulatuses, kui selleks on sellise nõusoleku või loa andnud isik, kellel on lapse suhtes vanemlik vastutus“[370]. Liikmesriigid võivad riigisisestes õigusaktides sätestada väiksema vanuse, kui see ei ole alla 13 aasta[371]. Vanemliku vastutuse kandja nõusolekut ei ole vaja „seoses lapsele otse pakutavate ennetavate või nõustamisteenustega“[372]. Laste isikuandmete töötlemisel peab teave olema ja suhtlemine toimuma selges ja lihtsas keeles, mis on lapsele kergesti arusaadav[373].

Õigus võtta nõusolek millal tahes tagasi

Isikuandmete kaitse üldmäärus sisaldab üldist õigust võtta nõusolek millal tahes tagasi[374]. Andmesubjekti tuleb enne nõusolekut sellest õigusest teavitada ja tal peab olema võimalik kasutada seda õigust omal äranägemisel. Nõusoleku tagasivõtmisel ei saa andmesubjekti kohustada seda põhjendada ja sellega ei tohi kaasneda muid negatiivseid tagajärgi kui andmete varem kokku lepitud kasutamisest tulenevatest eelistest ilmajäämine. Nõusoleku tagasivõtmine peab olema sama lihtne kui andmine[375]. Nõusolekut ei saa lugeda vabatahtlikult antuks, kui andmesubjekt ei saa nõusolekut tagasi võtta kahjulike tagajärgedeta või kui tagasivõtmine ei ole sama lihtne kui oli andmine[376].

Näide: klient nõustub, et talle saadetakse reklaamposti aadressile, mille ta annab vastutavale töötlejale. Kui klient võtab nõusoleku tagasi, ei tohi vastutav töötleja talle enam reklaamposti saata. Nõusoleku tagasivõtmisega ei tohi kaasneda karistavaid tagajärgi, näiteks tasusid. Tagasivõtmine rakendub siiski tulevikus ja sellel puudub tagasiulatuv mõju. Ajavahemik, mil kliendi

369 *Ibid.*, põhjendus 38.

370 *Ibid.*, artikli 8 lõike 1 esimene taane. Infoühiskonna teenuste mõiste on määratletud isikuandmete kaitse üldmääruse artikli 4 punktis 25.

371 Isikuandmete kaitse üldmääruse artikli 8 lõike 1 teine taane.

372 *Ibid.*, põhjendus 38.

373 *Ibid.*, põhjendus 58. Vt ka nüüdisajastatud konventsiooni nr 108 artikli 15 lõike 2 punkt e. Nüüdisajastatud konventsiooni nr 108 seletuskirja punktid 68 ja 125.

374 Isikuandmete kaitse üldmääruse artikli 7 lõige 3; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 45.

375 Isikuandmete kaitse üldmääruse artikli 7 lõige 3.

376 Isikuandmete kaitse üldmääruse põhjendus 42; nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 42.

isikuandmeid töödeldi kliendi nõusoleku alusel seaduslikult, oli õiguspärane. Tagasivõtmine välistab andmete edasise töötlemise, v.a kui töötlemine on kooskõlas õigusega andmete kustutamisele[377].

Lepingu täitmise vajalikkus

ELi õiguses on isikuandmete seadusliku töötlemise alus ka see, kui „isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks" (isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt b). See säte hõlmab ka lepingueelseid suhteid. Kui näiteks üks pool kavatseb sõlmida lepingu, kuid ei ole seda veel teinud, võib isikuandmete töötlemist olla vaja seepärast, et teatud kontrollid ei ole veel valmis. Kui ühel lepingupoolel on vaja lepingu sõlmimiseks töödelda andmeid, on selline töötlemine õiguspärane, kui see on vajalik „lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele"[378].

Andmete töötlemise mõiste kui „õiguspärane alus, mis on sätestatud seadusega" (nüüdisajastatud konventsiooni nr 108 artikli 5 lõige 2) hõlmab ka „andmete töötlemist lepingu (lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele) täitmiseks andmesubjekti osalusel"[379].

Vastutava töötleja seadusejärgsed kohustused

ELi õiguses sätestatakse andmetöötluse õiguspärasuse alusena ka see, kui „töötlemine on vajalik vastutava töötleja seadusejärgse kohustuse täitmiseks" (isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt c). See säte hõlmab avalikus ja erasektoris tegutsevaid vastutavaid töötlejaid; avaliku sektori vastutavate töötlejate seadusejärgsed kohustused võivad kuuluda ka isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e kohaldamisalasse. On palju näiteid olukordadest, kus seadus kohustab erasektori vastutavaid töötlejaid töötlema konkreetsete andmesubjektide andmeid. Näiteks peavad tööandjad oma töötajate andmeid töötlema sotsiaalkindlustuse ja maksustamise eesmärgil ning ettevõtjad peavad töötlema oma klientide andmeid maksustamise eesmärgil.

377 Isikuandmete kaitse üldmääruse artikli 17 lõike 1 punkt b.

378 *Ibid*., artikli 6 lõike 1 punkt b.

379 Nüüdisajastatud konventsiooni nr 108 seletuskiri, punkt 46; Euroopa Nõukogu ministrite komitee (2010), *Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23. november 2010, artikli 3.4 punkt b.

Seadusejärgne kohustus võib tuleneda liidu või liikmesriigi õigusest, mis võib olla alus ühele või mitmele andmetöötlemistoimingule. Õigusaktis peab olema määratud isikuandmete töötlemise eesmärk, vastutava töötleja määramise tingimused, töötlemisele kuuluvate isikuandmete liik, asjaomased andmesubjektid, üksused, kellele tohib andmeid avaldada, eesmärgi piirangud, säilitamise aeg ning muud seadusliku ja õiglase töötlemise tagamise meetmed[380]. Mis tahes selline isikuandmete töötlemise alus peab vastama nii põhiõiguste harta artiklitele 7 ja 8 kui ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8.

Ka **Euroopa Nõukogu õiguses** käsitletakse vastutava töötleja seadusejärgseid kohustusi andmetöötluse õigusliku alusena[381]. Nagu märgitud eespool, on erasektori vastutavate töötlejate juriidilised kohustused ainult üks kaasinimeste õigustatud huvide alla kuuluv erijuhtum Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõike 2 tähenduses. Seepärast kehtib esitatud näide (tööandjad töötlevad töötajate andmeid) ka Euroopa Nõukogu õiguse korral.

Andmesubjekti või muu füüsilise isiku elulised huvid

ELi õiguses on isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktis d sätestatud, et isikuandmeid tohib töödelda, kui „töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks". Sellele õiguslikule alusele võib tugineda üksnes isikuandmete töötlemiseks muu füüsilise isiku eluliste huvide alusel, kui seda töötlemist „ei saa ilmselgelt teostada muul õiguslikul alusel"[382]. Mõnikord võib teatud liiki andmetöötlus toimuda korraga avalikes huvides ja andmesubjekti või muu isiku elulistes huvides. Näiteks epideemiate ja nende leviku seires või humanitaarhädaolukordades.

Euroopa Nõukogu õiguses ei ole andmesubjekti elulisi huve Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 nimetatud. Samas kuuluvad andmesubjekti elulised huvid nüüdisajastatud konventsiooni nr 108 artikli 5 lõikes 2 (isikuandmete töötlemise õiguspärasus) sätestatud „õiguspärase aluse" mõiste alla[383].

380 Isikuandmete kaitse üldmääruse põhjendus 45.

381 Euroopa Nõukogu ministrite komitee (2010), *Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23. november 2010, artikli 3.4 punkt a.

382 Isikuandmete kaitse üldmääruse põhjendus 46.

383 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 46.

Avalikud huvid ja avaliku võimu teostamine

Avalikku võimu saab teostada paljudel viisidel, mistõttu sätestatakse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktis e, et isikuandmeid võib seaduslikult töödelda, kui see „on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks [...]“[384].

Näide: kohtuasi *Huber vs. Bundesrepublik Deutschland*[385] käsitles juhtumit, kus Saksamaal elanud Austria kodanik (Heinz Huber) esitas föderaalsele migratsiooni- ja pagulasametile taotluse kustutada välismaalaste keskregistrist tema andmed. Selles registris on isikuandmed teistest ELi riikidest pärit inimeste kohta, kes ei ole Saksamaa kodanikud, kuid elavad Saksamaal kauem kui kolm kuud; seda kasutatakse statistilisel 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, sest selline register puudub Saksamaa kodanike kohta.

ELK leidis, et direktiivi 95/46/EÜ artikli 7 punkti e[386] alusel on isikuandmete töötlemine õiguspärane, kui töötlemine on vajalik avalike huvidega või avaliku võimu teostamisega seotud ülesande täitmiseks.

ELK märkis, et „arvestades eesmärki tagada kõigis liikmesriikides võrdne kaitse, ei või direktiivi 95/46/EÜ artikli 7 punktis e[387] 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.“[388]

384 Vt isikuandmete kaitse üldmääruse põhjendus 45.

385 ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008.

386 Endise andmekaitsedirektiivi artikli 7 punkt e, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e.

387 *Ibid*.

388 ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008, punkt 52.

ELK märkis, et liidu kodaniku õigus elada liikmesriigis, mille kodanik ta ei ole, ei ole tingimusteta, vaid võib olla allutatud Euroopa Ühenduse 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 on põhimõtteliselt õiguspärane, ei tohi selline register sisaldada muud teavet peale selle, mis on vajalik asjaomasel eesmärgil. ELK 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 asjaomases kohtuasjas on need tingimused täidetud. Kui tingimused ei ole täidetud, ei saa sellises registris nagu välismaalaste keskregister isikuandmete säilitamist ja töötlemist statistilisel eesmärgil mingil juhul pidada vajalikuks direktiivi 95/46/EÜ[389] artikli 7 punkti e[390] tähenduses.

Seoses registris sisalduvate andmete kasutamisega kuritegevusevastase võitluse eesmärgil leidis ELK, et see 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. Sellest tulenevalt leidis ELK, et sätet tuleb tõlgendada nii, et „sellega on vastuolus liikmesriigi poolt kuritegevuse vastase võitluse eesmärgil spetsiaalse välismaalastest liidu kodanike isikuandmete töötlemise süsteemi rajamine"[391].

Isikuandmete kasutamise suhtes avalikkuses tegutsevate ametiasutuste poolt kohaldatakse ka **Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni** artiklit 8 ja (kui asjakohane) on see hõlmatud ka nüüdisajastatud konventsiooni nr 108 artikli 5 lõikega 2[392].

389 ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008, punktid 54, 58–59 ja 66–68.

390 Endise andmekaitsedirektiivi artikli 7 punkt e, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e.

391 ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008, punktid 78 ja 81.

392 Nüüdisajastatud konventsiooni nr 108 seletuskirja punktid 46 ja 47.

Vastutava töötleja või kolmanda isiku õigustatud huvid

ELi õiguse kohaselt võib õigustatud huve olla ka muudel isikutel kui ainult andmesubjektidel. Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti f kohaselt võib isikuandmeid töödelda, kui „töötlemine on vajalik vastutava töötleja või kolmanda isiku [või kolmandate isikute, v.a avaliku sektori asutused oma ülesannete täitmisel] õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused [...]"[393].

Õigustatud huvi olemasolu tuleb iga kord hoolikalt hinnata[394]. Kui tuvastatakse vastutava töötleja õigustatud huvi, tuleb need huvid ning andmesubjekti huvid või põhiõigused ja -vabadused tasakaalustada[395]. Sellisel hindamisel tuleb arvestada andmesubjekti mõistlikke ootusi, et leida, kas vastutava töötleja huvid on andmesubjekti huvide või põhiõiguste suhtes ülimuslikud[396]. Kui andmesubjekti õigused on vastutava töötleja õigustatud huvide suhtes ülimuslikud, võib vastutav töötleja võtta meetmeid ja rakendada kaitsemeetmeid, et tagada, et mõju andmesubjekti õigustele oleks minimaalne (nt andmeid pseudonüümides) ning muuta õiguste tasakaal vastupidiseks, enne kui saab seaduslikult tugineda sellele töötlemise õiguspärasele alusele. Arvamuses andmete vastutava töötleja õigustatud huvide mõiste kohta rõhutas artikli 29 töörühm, et vastutava töötleja õigustatud huvide ja andmesubjekti põhiõiguste tasakaalustamisel on keskne roll vastutusel ja läbipaistvusel ning andmesubjekti õigusel vaidlustada oma andmete töötlemine või andmetele juurdepääs, andmete muutmine, kustutamine või edastamine[397].

Isikuandmete kaitse üldmääruse põhjenduspunktides on näiteid, mida tähendab asjaomase vastutava töötleja õigustatud huvi. Näiteks võib isikuandmeid töödelda ilma andmesubjekti nõusolekuta, kui isikuandmeid töödeldakse otseturunduse eesmärgil või kui selline töötlemine on „pettuste vältimiseks rangelt vajalik"[398].

ELK on kohtupraktikas käsitlenud küsimust laiemalt, et määrata, mis on õigustatud huvi.

393 Võrreldes direktiiviga 95/46/EÜ on isikuandmete kaitse üldmääruses rohkem näiteid selle kohta, mida peetakse õigustatud huviks.

394 Isikuandmete kaitse üldmääruse preambul, põhjendus 47.

395 Artikli 29 töörühm (2014), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, 4. aprill 2014.

396 *Ibid*.

397 *Ibid*.

398 Isikuandmete kaitse üldmääruse preambul, põhjendus 47.

Näide: kohtuasi *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*[399] käsitles Riia trollibussiteenust osutava äriühingu trollibussile tekitatud kahju, mille põhjustas reisija, kes avas ootamatult takso ukse. Rīgas satiksme soovis kaevata reisija kahju hüvitamiseks kohtusse. Samas andis politsei üksnes reisija nime ja keeldus andmast reisija isikut tõendava dokumendi numbrit ja aadressi, väites, et avalikustamine on riigisiseste andmekaitse õigusaktide kohaselt ebaseaduslik.

Läti eelotsusetaotluse esitanud kohus palus Euroopa Liidu Kohtul teha eelotsus, kas ELi andmekaitse õigusaktides on kehtestatud kohustus avalikustada kõik isikuandmed, mis võimaldavad esitada tsiviilkohtusse nõude andmekaitsesubjekti vastu, kes on väidetavalt sooritanud haldusõigusrikkumise[400].

ELK selgitas, et ELi andmekaitsedirektiiv ei näe ette kohustust, vaid väljendab võimalust töödelda isikuandmeid, avalikustades vajalikke andmeid kolmandale isikule, kellel on õigustatud huvi[401]. ELK kehtestas kolm kumulatiivset tingimust, mille täitmisel on isikuandmete töötlemine õigustatud huvi alusel seaduslik[402]. Esiteks peab andmete avaldamine olema vajalik kolmanda isiku õigustatud huvide teostamiseks. Selles kohtuasjas tähendab isikuandmete taotlemine isiku kohtusse kaebamiseks varalise kahju tekitamise eest kolmanda isiku õigustatud huvi. Teiseks on vaja, et isikuandmete töötlemine toimuks õigustatud huvide teostamiseks. Selles kohtuasjas oli isikuandmete (nt aadress ja/või isikukood) saamine isiku tuvastamise eesmärgil rangelt vajalik. Kolmandaks ei tohi andmesubjekti põhiõigused ja -vabadused olla vastutava töötleja või kolmandate isikute õigustatud huvide suhtes ülimuslikud. Huvide tasakaal tuleb määrata iga kord eraldi, arvestades selliseid asjaolusid nagu andmesubjekti õiguste rikkumise raskus või teatud asjaoludel ka tema vanus. Selles kohtuasjas ei leidnud ELK siiski, et teabe avaldamisest keeldumine oleks olnud põhjendatud üksnes seetõttu, et andmesubjekt oli alaealine.

399 ELK, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*, 4. mai 2017.

400 *Ibid.*, punkt 23.

401 *Ibid.*, punkt 26.

402 *Ibid.*, punktid 28–34.

Kohtuasja *ASNEF ja FECEMD* kohtuotsuses käsitles ELK otseselt andmetöötlust õigustatud huvide seaduslikul alusel, mis sel ajal oli sätestatud andmekaitsedirektiivi artikli 7 punktis f[403].

Näide: kohtuasjas *ASNEF ja FECEMD*[404] selgitas ELK, et liikmesriigid ei tohi oma õigusaktidega lisada andmekaitsedirektiivi artikli 7 punktis f esitatud kriteeriumidele uusi andmetöötluse seaduslikkuse kriteeriume[405]. See oli ajendatud juhtumist, kus Hispaania andmekaitseõiguses oli säte, millega said teised eraõiguslikud isikud seoses isikuandmete töötlemisega tugineda õigustatud huvile, kui see teave oli juba avaldatud avalikes allikates.

Esiteks märkis ELK, et direktiivi 95/46/EÜ[406] eesmärk on viia isikuandmete töötlemisega seonduv üksikisikute õiguste ja vabaduste kaitse kõigis liikmesriikides samale tasemele. Samuti lisati, et valdkonna õigusaktide ühtlustamise tulemusel ei tohi nendega pakutav kaitse väheneda. Selle asemel peab liidus tagatava kaitstuse tase olema kõrgem[407]. ELK järeldas: „Seega tuleneb eesmärgist tagada kõigis liikmesriikides võrdväärne kaitstuse tase, et direktiivi 95/46/EÜ artikkel 7[408] näeb ette ammendava ja piirava loetelu juhtudest, millal isikuandmete töötlemist võib pidada seaduslikuks." Samuti järeldub, „et liikmesriigid ei saa lisada direktiivi 95/46/EÜ artiklile 7[409] uusi isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume ega kehtestada täiendavaid nõudeid, mis muudavad selles artiklis[410] sätestatud kuuest kriteeriumist mõne kriteeriumi ulatust". ELK tunnistas, et seoses direktiivi 95/46/EÜ artikli 7 punkti f kohase tasakaalustamisega on võimalik

403 Endise andmekaitsedirektiivi artikli 7 punkt f, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f.

404 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.

405 Endise andmekaitsedirektiivi artikli 7 punkt f, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f.

406 Endine andmekaitsedirektiiv, praegune isikuandmete kaitse üldmäärus.

407 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 28. Vt andmekaitsedirektiivi põhjendused 8 ja 10.

408 Endise andmekaitsedirektiivi artikkel 7, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f.

409 Endise andmekaitsedirektiivi artikkel 7, praeguse isikuandmete kaitse üldmääruse artikkel 6.

410 *Ibid.*

kaalutleda asjaolu, et nimetatud töötlemisega andmesubjekti põhiõigustele kaasneva riive raskus võib sõltuda sellest, kas asjaomased andmed on juba esitatud avalikkusele kättesaadavates allikates või mitte.

Kohus märkis siiski, et selle direktiivi artikli 7 punkt f välistab liikmesriigil „kategooriliselt ja üldiselt teatud isikuandmete kategooriate töötlemise, ilma et lubatud oleks kaaluda konkreetsel juhtumil vastanduvaid õigusi ja huve".

Neid tähelepanekuid arvestades järeldas ELK, et direktiivi 95/46/EÜ artikli 7 punkti f[411] tuleb tõlgendada „nii, et sellega on vastuolus siseriiklikud õigusnormid, mis nõuavad selleks, et ilma andmesubjekti nõusolekut küsimata võiks 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"[412].

Kui isikuandmeid töödeldakse õigustatud huvide alusel, on isikul isikuandmete kaitse üldmääruse artikli 21 lõike 1 kohaselt õigus oma konkreetsest olukorrast lähtudes esitada igal ajal vastuväiteid. Vastutav töötleja ei tohi isikuandmeid edasi töödelda, v.a kui ta tõendab, et töödeldakse mõjuval õiguspärasel põhjusel.

Euroopa Nõukogu õiguses on sarnaseid lõike ka nüüdisajastatud konventsioonis nr 108[413] ja Euroopa Nõukogu soovitustes. Profiilianalüüsi soovituse järgi on isikuandmete töötlemine profiilianalüüsi eesmärgil õiguspärane, kui see on vajalik kaasinimeste õigustatud huvides, v.a kui selline huvi on andmesubjektide põhiõiguste ja -vabaduste suhtes ülimuslik[414]. Lisaks on kaasinimeste õiguste ja vabaduste kaitset nimetatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 kui andmekaitseõiguse piiramise üht õiguspärast põhjust.

411 Endise andmekaitsedirektiivi artikli 7 punkt f, praeguse isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f.

412 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, punktid 40, 44 ja 48–49.

413 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 46.

414 Euroopa Nõukogu ministrite komitee (2010), *Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23. november 2010, artikli 3.4 punkt b (profiilianalüüsi soovitus).

Näide: kohtuasjas *Y vs. Türgi*[415] oli kaebuse esitaja HIV-positiivne. Et ta oli haiglasse saabumisel teadvusetu, teatas kiirabibrigaad haiglatöötajatele, et patsient on HIV-positiivne. Kaebuse esitaja väitis Euroopa Inimõiguste Kohtus, et selle teabe avaldamisega rikuti tema õigust eraelu austamisele. Haiglatöötajate ohutuse tagamise vajadust arvestades ei peetud selle teabe jagamist siiski tema õiguste rikkumiseks.

4.1.2. Eriliiki isikuandmete (delikaatsete andmete) töötlemine

Euroopa Nõukogu õiguses võivad riigid seoses delikaatsete andmete kasutamisega ise otsustada asjakohased kaitsemeetmed eeldusel, et nüüdisajastatud konventsiooni nr 108 artikli 6 tingimused on täidetud – õigusaktides peavad olema kehtestatud konventsiooni sätteid täiendavad asjakohased kaitsemeetmed. **ELi õiguses** sisaldub isikuandmete kaitse üldmääruse artiklis 9 eriliiki isikuandmete (delikaatsete andmete) töötlemise üksikasjalik kord. Eriliigilised isikuandmed on need, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused ja ametiühingusse kuulumine, samuti hõlmavad need geneetiliste ja biomeetriliste andmete töötlemisel saadavaid andmeid füüsilise isiku kordumatuks tuvastamiseks ning terviseandmeid, seksuaalelu või seksuaalse sättumuse andmeid. Delikaatsete andmete töötlemine on põhimõtteliselt keelatud[416].

Samas on olemas ammendav loetelu selle keelu eranditest, mis on esitatud määruse artikli 9 lõikes 2 ja mis on delikaatsete isikuandmete töötlemise õiguslikud alused. Need erandid hõlmavad olukordi, kus

- andmesubjekt annab selgesõnalise nõusoleku andmete töötlemiseks;
- töödeldakse isikuandmeid poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega mittetulundusühingu õiguspärase tegevuse raames ning tingimusel, et töötlemine käsitleb ainult ühingu liikmeid või endisi liikmeid või isikuid, kes on ühinguga püsivalt seotud selle tegevuse eesmärkide tõttu;
- töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud;

415 EIK, *Y vs. Türgi*, nr 648/10, 17. veebruar 2015.

416 Endise andmekaitsedirektiivi artikli 7 punkt f, praeguse isikuandmete kaitse üldmääruse artikli 9 lõige 1.

- töötlemine on vajalik:
  - seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega;
  - et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve (kui andmesubjekt on võimetu nõusolekut andma);
  - õigusnõude koostamiseks, esitamiseks või kaitsmiseks või juhul, kui kohtud täidavad oma õigust mõistvat funktsiooni;
  - ennetava meditsiini või töömeditsiiniga seotud põhjustel: „töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks, tuginedes liidu või liikmesriigi õigusele või tervishoiutöötajaga sõlmitud lepingule“;
  - avalikes huvides toimuva arhiivimise, teadus- või ajaloouuringute või statistilisel eesmärgil;
  - rahvatervise valdkonna avalikes huvides või
  - olulise avaliku huviga seotud põhjustel.

Seega ei käsitata eriliiki andmete töötlemisel lepingusuhet andmesubjektiga delikaatsete andmete õigusliku töötlemise õiguspärase alusena, v.a kui leping on sõlmitud tervishoiutöötajaga, kellel on kutsesaladuse hoidmise kohustus[417].

Andmesubjekti selgesõnaline nõusolek

ELi õiguse alusel on andmetöötluse seaduslikkuse peamine tingimus – hoolimata andmete mittedelikaatsusest – andmesubjekti nõusolek. Delikaatsete isikuandmete korral peab andmesubjekti nõusolek olema selgesõnaline. Liidu või liikmesriigi õiguses võib siiski olla sätestatud, et andmesubjekt ei saa eriliiki andmete töötlemise

417 Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktid h ja i.

keeldu tühistada[418], näiteks kui töötlemisega kaasnevad andmesubjektile ebatavalised riskid.

Tööõigus või sotsiaalkindlustus- ja sotsiaalkaitseõigus

ELi õiguse kohaselt võib artikli 9 lõikes 1 sätestatud keelu tühistada, kui töötlemine on vajalik vastutava töötleja või andmesubjekti kohustuste täitmiseks või õiguste teostamiseks tööhõive või sotsiaalkindlustuse valdkonnas. Samas peab töötlemine olema lubatud ELi õiguse, riigisisese õiguse või liikmesriigi õiguse kohase kollektiivlepinguga, millega kehtestatakse asjakohased kaitsemeetmed andmesubjekti põhiõiguste ja huvide kaitseks[419]. Organisatsiooni valduses olevad tööhõiveandmed võivad sisaldada delikaatseid isikuandmeid teatud tingimustel, mis on kehtestatud isikuandmete kaitse üldmääruses ja asjaomastes riigisisestes õigusaktides. Näiteks võivad delikaatsed isikuandmed olla ametiühingusse kuulumise või terviseseisundi teave.

Andmesubjekti või muu isiku elulised huvid

ELi õiguses on sätestatud, et nagu tavalisi andmeid, tohib ka delikaatseid isikuandmeid töödelda, kui see on andmesubjekti või teise füüsilise isiku elulistes huvides[420]. Muu isiku eluliste huvide alusel saaks isikuandmeid põhimõtteliselt töödelda üksnes siis, kui töötlemist „ei saa ilmselgelt teostada muul õiguslikul alusel"[421]. Mõnel juhul võib isikuandmete töötlemine kaitsta nii isiklikke kui ka avalikke huve, näiteks kui töötlemine on vajalik humanitaareesmärgil[422].

Delikaatsete isikuandmete töötlemine andmesubjekti elulistes huvides on õiguspärane, kui andmesubjektilt ei ole võimalik küsida nõusolekut, sest ta oli näiteks teadvusetu, teda ei olnud kohal või teda ei õnnestunud kätte saada. Teisisõnu oli isik füüsiliselt või õiguslikult võimetu nõusolekut andma.

418 *Ibid.*, artikli 9 lõike 2 punkt a

419 Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt b.

420 *Ibid.*, artikli 9 lõike 2 punkt c.

421 *Ibid.*, põhjendus 46.

422 *Ibid.*

Heategevusorganisatsioonid ja mittetulundusühingud

Isikuandmete töötlemine on lubatud ka poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega sihtasutuse, ühenduse või muu mittetulundusühingu õiguspärase tegevuse raames. See töötlemine peab siiski käsitlema ainult sama ühingu liikmeid või endisi liikmeid või isikuid, kes on ühinguga püsivalt seotud[423]. Isikuandmeid ei saa avalikustada väljaspool neid ühinguid ilma andmesubjekti nõusolekuta.

Andmed, mille andmesubjekt on ilmselgelt avalikustanud

Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkti e kohaselt ei ole töötlemine keelatud, kui töödeldakse andmeid, mille andmesubjekt on ilmselgelt avalikustanud. Kuigi mõiste „andmesubjekt on ilmselgelt avalikustanud" tähendus ei ole määruses määratletud, sest see on delikaatsete isikuandmete töötlemise keelu erand, tuleb seda tõlgendada rangelt ja nii, et andmesubjekt peab avalikustama oma isikuandmed tahtlikult. Seega kui televisioonis näidatakse videovalvekaamerast saadud videot, milles muu hulgas näidatakse, kuidas tuletõrjuja saab hoonest inimesi päästes vigastada, ei saa seda tõlgendada nii, et tuletõrjuja on andmed ilmselgelt avalikustanud. Teisalt, kui tuletõrjuja otsustab juhtunut kirjeldada ning video ja fotod avaldada avalikus veebikohas, oleks see tahtlik ja kinnitust väljendav isikuandmete avalikustamise toiming. On oluline märkida, et andmete üldsusele kättesaadavaks tegemine ei ole nõusolek, vaid teist liiki luba andmete eriliikide töötlemiseks.

Asjaolu, et andmesubjekt oli töödeldud isikuandmed avalikustanud, ei vabasta vastutavaid töötlejaid nende andmekaitseõigusest tulenevatest kohustustest. Isikuandmete suhtes kehtib näiteks jätkuvalt eesmärgi piirangu põhimõte, isegi kui andmed on tehtud üldsusele kättesaadavaks[424].

Õigusnõuded

Andmete eriliikide töötlemine, mis on „vajalik õigusnõude koostamiseks, esitamiseks või kaitsmiseks" kohtumenetluse, haldusmenetluse või kohtuvälise menetluse raames,[425] on isikuandmete kaitse üldmääruse[426] alusel samuti lubatud. Sellisel juhul

423 *Ibid.*, artikli 9 lõike 2 punkt d.

424 Artikli 29 töörühm (2013), *Opinion 3/13 on purpose limitation*, WP 203, Brüssel, 2. aprill 2013, lk 14.

425 Isikuandmete kaitse üldmääruse preambul, põhjendus 52.

426 *Ibid.*, artikli 9 lõike 2 punkt f.

peab töötlemine olema seotud konkreetse õigusnõudega ja vastavalt selle esitamiseks või kaitsmiseks ning seda võib nõuda ükskõik kumb vaidluse osapool.

Kohtud võivad oma õigusmõistmisfunktsiooni täites töödelda eriliiki isikuandmeid õigusvaidluste lahendamise raames[427]. Selles kontekstis töödeldavate andmete eriliikide näited on põlvnemise tõestamise geneetilised andmed ja terviseseisund, kui osa tõenditest on seotud kuriteos kannatanu vigastuste üksikasjadega.

Olulise avaliku huviga seotud põhjused

Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkti g kohaselt võivad liikmesriigid kehtestada täiendavaid asjaolusid, mille korral võib töödelda delikaatseid isikuandmeid, juhul kui

- töötlemine on seotud olulise avaliku huviga;
- see toimub Euroopa Liidu või liikmesriigi õiguse alusel;
- Euroopa Liidu või liikmesriigi õigus on proportsionaalne, austab isikuandmete kaitse õiguse olemust ning tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks[428].

Hea näide on elektroonilised terviseregistrid. Selliste süsteemide kaudu saavad tervishoiuteenuste osutajad teha patsiendi ravi ajal kogutud terviseandmed kättesaadavaks sama patsiendiga tegelevatele teistele tervishoiuteenuste osutajatele, ulatuslikult ja tavaliselt kogu riigis.

Artikli 29 töörühm järeldas, et olemasolevad patsiendiandmete töötlemise õiguseeskirjad selliste süsteemide loomist ei võimalda[429]. Elektroonilised terviseregistrid võivad siiski eksisteerida, kui need rajanevad „olulise avaliku huviga seotud

427 *Ibid.*

428 *Ibid.*, artikli 9 lõike 2 punkt g.

429 Artikli 29 töörühm (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Brüssel, 15. veebruar 2007. Vt ka isikuandmete kaitse üldmääruse artikli 9 lõige 3.

põhjustel"[430]. See nõuaks nende loomiseks selget õiguslikku alust, mis sisaldaks ka vajalikke kaitsemeetmeid, et tagada süsteemi turvaline toimimine[431].

Delikaatsete andmete töötlemise muud alused

Isikuandmete kaitse üldmääruses on sätestatud, et delikaatseid andmeid võib töödelda, kui töötlemine on vajalik[432]

- ennetava meditsiini või töömeditsiiniga seotud põhjustel, töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks, tuginedes ELi või liikmesriigi õigusele või tervishoiutöötajaga sõlmitud lepingule;

- rahvatervise valdkonna avalikes huvides, nagu kaitse suure piiriülese terviseohu korral või kõrgete kvaliteedi- ja ohutusnõuete tagamine tervishoiu ning ravimite või meditsiiniseadmete puhul, tuginedes liidu või liikmesriigi õigusele; õigusaktides tuleb sätestada sobivad ja konkreetsed meetmed andmesubjekti õiguste ja vabaduste kaitseks;

- arhiivimise, teadus- või ajaloouuringute või statistilisel eesmärgil, tuginedes liidu või liikmesriigi õigusele. See õigus peab olema proportsionaalne saavutatava eesmärgiga, austama isikuandmete kaitse õiguse olemust ning tagatud peavad olema sobivad ja konkreetsed meetmed andmesubjekti õiguste ja huvide kaitseks.

Täiendavad tingimused riigisiseses õiguses

Isikuandmete kaitse üldmääruse kohaselt võivad liikmesriigid säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega[433].

430 Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt g.

431 Artikli 29 töörühm (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Brüssel, 15. veebruar 2007.

432 Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktid h, i ja j.

433 *Ibid.*, artikli 9 lõike 2 punkt h ja artikli 9 lõige 4.

4.2. Turvalise töötlemise eeskirjad

Põhipunktid

- Andmetöötluse turvalisuse eeskirjad kohustavad vastutavat ja volitatud töötlejat võtma sobivaid tehnilisi ja korralduslikke meetmeid, et ennetada mis tahes ebaseaduslikke sekkumisi andmetöötlustoimingutesse.
- Andmete turvalisuse vajaliku taseme määravad
  - konkreetse andmetöötlusliigi korral turul saadaolevad turvafunktsioonid;
  - kulud;
  - andmetöötluse riskid seoses andmesubjekti põhiõiguste ja -vabadustega.
- Isikuandmete konfidentsiaalsuse tagamine on osa isikuandmete kaitse üldmääruses tunnustatud üldpõhimõttest.

Nii **ELi kui ka Euroopa Nõukogu õiguse** kohaselt on vastutavatel töötlejatel üldine kohustus olla isikuandmete töötlemisel läbipaistev ja vastutustundlik ning eelkõige isikuandmetega seotud rikkumise korral, kui selliseid rikkumisi esineb. Isikuandmetega seotud rikkumiste korral peavad vastutavad töötlejad teavitama järelevalveasutusi, v.a kui rikkumise tulemusena ei teki tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele. Andmesubjekte tuleks teavitada isikuandmetega seotud rikkumisest ka siis, kui on tõenäoline, et sellega kaasneb suur oht füüsiliste isikute õigustele ja vabadustele.

4.2.1. Andmeturbe elemendid

ELi õiguse asjakohastes sätetes on sätestatud järgmist:

> *„Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele, rakendavad vastutav töötleja ja volitatud töötleja ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid […].“*[434]

434 *Ibid.*, artikli 32 lõige 1.

Need meetmed hõlmavad muu hulgas järgmist:

- isikuandmete pseudonüümimine ja krüpteerimine[435];
- isikuandmeid töötlevate süsteemide ja teenuste kestva konfidentsiaalsuse, tervikluse, kättesaadavuse ja vastupidavuse tagamine[436];
- isikuandmete kättesaadavuse ja füüsilise või tehnilise vahejuhtumi korral andmetele juurdepääsu õigeaegne taastamine[437];
- tehniliste ja korralduslike meetmete tõhususe testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks[438].

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

> *„Iga lepinguosaline näeb ette, et vastutav töötleja ja vajaduse korral volitatud töötleja võtab asjakohaseid turvameetmeid selliste riskide vastu nagu andmetele juhuslik või volitamata juurdepääs, andmete hävitamine, kaotsiminek, kasutamine, muutmine või avalikustamine.“*[439]

ELi ja Euroopa Nõukogu õiguse alusel on vastutaval töötlejal kohustus teatada järelevalveasutusele isikuandmetega seotud rikkumisest, mis võib mõjutada üksikisikute õigusi ja vabadusi (vt punkt 4.2.3).

Sageli on andmete turvalise töötlemise tagamiseks kehtestatud ka valdkondlikke-, riiklikke ja rahvusvahelisi standardeid. Näiteks uuritakse ELi üleeuroopaliste telekommunikatsioonivõrkude (eTEN) projektide hulka kuuluva Euroopa eraelu puutumatuse märgiste süsteemi (EuroPriSe) raamistikus toodete, eelkõige tarkvara Euroopa andmekaitseõiguse nõuete alusel sertifitseerimise võimalusi. Et suurendada ELi, selle liikmesriikide ja ettevõtjaskonna suutlikkust võrgu- ja infoturbe probleemide ennetamisel, käsitlemisel ja lahendamisel, asutati Euroopa Liidu Võrgu- ja

435 *Ibid.*, artikli 32 lõike 1 punkt a.

436 *Ibid.*, artikli 32 lõike 1 punkt b.

437 *Ibid.*, artikli 32 lõike 1 punkt c.

438 *Ibid.*, artikli 32 lõike 1 punkt d.

439 Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 1.

Infoturbeamet (ENISA)[440]. ENISA avaldab regulaarselt praeguste turvaohtude analüüse ning annab nõu, kuidas neid käsitleda[441].

Peale õigete vahendite – riist- ja tarkvara – on andmeturbe jaoks vaja ka asjakohaseid organisatsioonilisi sisekorraeeskirju. Need võiksid ideaaljuhul hõlmata järgmist:

- kõigi töötajate regulaarne teavitamine andmeturbe eeskirjadest ja nende kohustustest andmekaitseõiguse alusel, eelkõige konfidentsiaalsuskohustustest;
- selge vastutuse jaotus ja pädevuste kirjeldus andmekaitseküsimustes, eelkõige seoses otsustega isikuandmete töötlemise ja nende kolmandatele isikutele või andmesubjektidele edastamise kohta;
- isikuandmete kasutamine üksnes kooskõlas pädeva isiku juhistega või üldeeskirjadega;
- meetmed, millega kaitstakse juurdepääsu vastutava või volitatud töötleja asukohtadele ning riist- ja tarkvarale, sealhulgas juurdepääsuloa olemasolu kontrollimine;
- tagamine, et volituse isikuandmetele juurdepääsuks on andnud pädev isik ja esitatud on vajalikud dokumendid;
- automaattoimingud seoses elektroonilise juurdepääsuga isikuandmetele ja selliste toimingute regulaarne kontroll organisatsioonisisese järelevalveisiku vastutusel (mistõttu tuleb kõik andmetöötlustoimingud registreerida);
- põhjalikud dokumendid andmete muu avaldamise kohta kui automaatse juurdepääsu korral, et tõendada, et andmeid ei ole edastatud ebaseaduslikult.

Tõhusate turvalisuse ettevaatusmeetmete tagamisel on oluline roll ka töötajatele andmeturbe küsimustes asjakohase koolituse ja õppe pakkumine. Samuti tuleb kehtestada kontrollimenetlused, et tagada, et asjakohased meetmed on olemas mitte

440 Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta määrus (EÜ) nr 526/2013, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004, ELT 2013 L 165.

441 Näiteks ENISA (2016), *Cyber Security and Resilience of smart cars. Good practices and recommendations*; ENISA (2016), *Security of Mobile Payments and Digital Wallets*.

ainult paberil, vaid neid rakendatakse ja need toimivad ka tegelikkuses (nt sise- või välisauditid).

Vastutav või volitatud töötleja saab turvalisust täiustada ka järgmiste meetmetega: andmekaitseametnike määramine, töötajate turbealane koolitamine, korrapärased auditid, läbistustestimine ja kvaliteedimärgised.

Näide: kohtuasi *I vs. Soome*[442] käsitles juhtumit, kus kaebuse esitaja ei suutnud tõestada, et tema terviseandmeid olid ebaseaduslikult vaadanud tema töökohaks oleva haigla muud töötajad. Seepärast ei rahuldanud riigisisesed kohtud tema kaebust, et tema õigust isikuandmete kaitsele oli rikutud. EIK järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8, sest haigla terviseandmete registreerimise süsteem oli selline, et tagantjärele ei olnud võimalik patsiendi andmete kasutamist tuvastada, sest süsteem näitas üksnes viit viimast kasutuskorda, ning pealegi kustutati see teave kohe, kui toimik tagastati arhiivi. Kohtu arvates oli otsustav tegur, et haigla registreerimissüsteem ei olnud ilmselgelt kooskõlas riigisiseses õiguses nõutuga, kusjuures riigisisesed kohtud ei olnud pööranud sellele nüansile piisavalt tähelepanu.

Euroopa Liit on kehtestanud võrgu- ja infosüsteemide turvalisuse direktiivi (edaspidi „võrgu- ja infoturbe direktiiv"),[443] mis on esimene kogu ELi hõlmav küberjulgeoleku õigusakt. Direktiivi eesmärk on ühelt poolt parandada küberturvet riigi tasandil ja teisalt suurendada ELi-sisest koostööd. Samuti kehtestatakse sellega kohustused oluliste teenuste operaatoritele (sealhulgas energia-, tervishoiu-, pangandus-, transpordi-, digitaristu jne sektori ettevõtjatele) ja digitaalteenuste osutajatele, et hallata riske, tagada oma võrgu- ja infosüsteemide turvalisus ning teatada turvaintsidentidest.

Väljavaated

2017. aasta septembris tegi Euroopa Komisjon ettepaneku määruse eelnõu kohta, mille eesmärk oli reformida ENISA volitusi, et arvestada ameti uusi pädevusi ja kohustusi seoses võrgu- ja infoturbe direktiiviga. Kavandatud määruse eesmärk on

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

443 Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, ELT 2016 L 194.

arendada ENISA ülesandeid ja tugevdada tema rolli ELi küberturvalisuse ökosüsteemi võrdlusalusena[444]. Kavandatav määrus ei tohiks piirata isikuandmete kaitse üldmääruse põhimõtteid ja Euroopa küberturvalisuse sertifitseerimiskavade vajalikke elemente selgitades peaks see samuti tugevdama isikuandmete turvalisust. Samaaegselt 2017. aasta septembris tegi Euroopa Komisjon ettepaneku rakendusmääruse eelnõu kohta, milles täpsustatakse elemendid, mida digitaalse teenuse osutajad peavad arvestama, et tagada võrgu- ja infosüsteemide turvalisus, nagu on nõutud võrgu- ja infoturbe direktiivi artikli 16 lõikes 8. Käsiraamatu koostamise ajal mõlema ettepaneku arutelud alles kestsid.

4.2.2. Konfidentsiaalsus

ELi õiguse kohaselt tunnustab isikuandmete kaitse üldmäärus isikuandmete konfidentsiaalsust kui osa üldpõhimõttest[445]. Üldkasutatavate elektroonilise side teenuste osutajad peavad tagama konfidentsiaalsuse. Samuti on neil kohustus kaitsta oma teenuste turvalisust[446].

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

Et töötaja peab hoidma klientide andmeid konfidentsiaalsena, peab ta enne isikuandmete avaldamist võtma vähemalt minimaalseid turvameetmeid. Ta võib helistajale näiteks pakkuda, et helistab tagasi kliendi toimikus olevale telefoninumbrile.

Vastavalt artikli 5 lõike 1 punktile f töödeldakse isikuandmeid viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid (usaldusväärsus ja konfidentsiaalsus).

Artikli 32 kohaselt peavad vastutav ja volitatud töötleja rakendama kõrge turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. Need

444 *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act)*, COM(2017)477, 13. september 2017, lk 6.

445 Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt f.

446 Eraelu puutumatuse ja elektroonilise side direktiivi artikli 5 lõige 1.

on näiteks isikuandmete pseudonüümimine ja krüpteerimine, suutlikkus tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, käideldavus ja vastupidavus, meetmete tõhususe hindamine ja katsetamine ning võime taastada töötlemine füüsilise või tehnilise vahejuhtumi korral. Lisaks võib tervikluse ja konfidentsiaalsuse põhimõtte järgimise tõendamise elemendina kasutada heakskiidetud toimimisjuhendite või heakskiidetud sertifitseerimismehhanismi järgimist. Samuti tuleb isikuandmete kaitse üldmääruse artikli 28 kohaselt vastutavat töötlejat volitatud töötlejaga siduvas lepingus sätestada, et volitatud töötleja tagab, et isikuandmeid töötlema volitatud isikud on kohustunud järgima konfidentsiaalsusnõuet või nende suhtes kehtib asjakohane seadusest tulenev konfidentsiaalsuskohustus.

Konfidentsiaalsuskohustus ei kehti olukordades, kus isik tutvub andmetega eraisikuna ning mitte vastutava töötleja või volitatud töötleja töötajana. Sel juhul isikuandmete kaitse üldmääruse artiklid 32 ja 28 ei kehti, sest olukord, kus isikuandmeid kasutab eraisik, ei kuulu andmekaitsedirektiivi kohaldamisalasse, vaid kuulub koduse tegevuse erandi alla[447]. See erand kehtib juhul, kui isikuandmeid kasutab „füüsiline isik eranditult isiklike või koduste tegevuste käigus"[448]. Alates ELK otsusest kohtuasjas *Bodil Lindqvist*[449] tuleb seda erandit tõlgendada siiski kitsendavalt, eelkõige seoses andmete avaldamisega. Eelkõige ei laiene koduse tegevuse erand isikuandmete avaldamisele internetis piiramatule arvule vastuvõtjatele või andmetöötlusele, millel on ametialaseid või ärilisi aspekte (seda kohtuasja on täpsemalt käsitletud punktides 2.1.2, 2.2.2 ja 2.3.1).

Konfidentsiaalsuse aspekt on ka side konfidentsiaalsus, mille suhtes kohaldatakse erinorme. E-privaatsuse direktiivi elektroonilise side konfidentsiaalsuse tagamise erieeskirjade kohaselt peavad liikmesriigid keelama isikutel, kes ei ole kasutajad, ilma kasutajate loata kuulata, salaja pealt kuulata, säilitada või muul viisil pealt kuulata või jälgida sidet ja sellega seotud metaandmeid[450]. Riigisiseses õiguses võidakse lubada selle põhimõtte erandeid üksnes riigi julgeoleku, riigikaitse, kuritegude ennetamise või avastamise eesmärgil ning ainult siis, kui need meetmed on taotletavate eesmärkide saavutamiseks vajalikud ja proportsionaalsed[451]. Samu eeskirju kohaldatakse ka tulevases e-privaatsuse määruses, kuid e-privaatsuse õigusakti

447 Isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkt c.

448 *Ibid.*

449 ELK, C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003.

450 Eraelu puutumatuse ja elektroonilise side direktiivi artikli 5 lõige 1.

451 *Ibid.*, artikli 15 lõige 1.

reguleerimisala laiendatakse üldkasutatavate elektrooniliste sideteenuste osas, et need hõlmaksid ka OTT-teenuste (nt mobiilirakendused) kaudu toimuvat sidet.

Euroopa Nõukogu õiguses vihjatakse konfidentsiaalsuskohustusele nüüdisajastatud konventsiooni nr 108 artikli 7 lõikes 1 andmeturbe käsitlemisel.

Volitatud töötlejate korral tähendab konfidentsiaalsuskohustus, et nad ei tohi avalikustada andmeid kolmandatele isikutele ega teistele vastuvõtjatele ilma loata. Ka vastutava või volitatud töötleja töötajad võivad isikuandmeid konfidentsiaalsusnõuete alusel kasutada üksnes oma pädeva juhi juhiseid järgides.

Konfidentsiaalsuskohustus peab sisalduma kõigis vastutavate töötlejate ja nende volitatud töötlejate vahel sõlmitavates lepingutes. Lisaks peavad vastutavad ja volitatud töötlejad võtma konkreetseid meetmeid oma töötajatele konfidentsiaalsuskohustuse määramiseks õiguslikul tasandil, lisades tavaliselt töötaja töölepingusse konfidentsiaalsustingimused.

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

4.2.3. Isikuandmetega seotud rikkumisest teatamine

Isikuandmetega seotud rikkumine tähendab turvanõuete rikkumist, mis põhjustab töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu[452]. Kuigi uued tehnoloogiad (nt krüpteerimine) pakuvad nüüd rohkem võimalusi andmetöötluse turvalisuse tagamiseks, on isikuandmetega seotud rikkumine ikka veel tavaline nähtus. Isikuandmetega seotud rikkumiste põhjused võivad varieeruda alates organisatsiooni töötajate juhuslikest vigadest kuni välisohtudeni (nt häkkerid ja küberkuritegevuse rühmitused).

Isikuandmetega seotud rikkumised võivad olla väga kahjulikud nende isikute eraelu puutumatusele ja andmekaitsele, kes rikkumise tagajärjel kaotavad kontrolli oma isikuandmete üle. Rikkumistega võib kaasneda identiteedivargus või -pettus, rahaline või varaline kahju, kutsesaladusega kaitstud isikuandmete konfidentsiaalsuse kaotus ja kahju andmesubjekti mainele. Suunistes, mis käsitlevad isikuandmetega

452 Isikuandmete kaitse üldmääruse artikli 4 punkt 12; vt ka artikli 29 töörühm (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3. oktoober 2017, lk 8.

seotud rikkumisest teatamist määruse (EL) 2016/679 alusel, selgitab artikli 29 töörühm, et rikkumistel võib olla kolme liiki kahjulik mõju isikuandmetele: avalikustamine, hävimine ja/või muutmine[453]. Lisaks kohustusele võtta meetmeid töötlemise turvalisuse tagamiseks, nagu on selgitatud peatükis 4.2, on sama oluline tagada, et vastutavad töötlejad käsitleksid rikkumisi nende ilmnemisel nõuetekohaselt ja õigeaegselt.

Järelevalveasutused ja üksikisikud ei ole sageli isikuandmetega seotud rikkumisest teadlikud ning see takistab üksikisikutel võtmast meetmeid, et kaitsta end rikkumise negatiivsete tagajärgede eest. Üksikisikute õiguste kinnitamiseks ja isikuandmetega seotud rikkumise mõju piiramiseks kehtestavad **EL ja Euroopa Nõukogu** teatud asjaoludel vastutavatele töötlejatele teatamisnõude.

Euroopa Nõukogu nüüdisajastatud konventsiooni nr 108 alusel peavad konventsiooniosalised vähemalt nõudma, et vastutavad töötlejad teavitaksid pädevat järelevalveasutust isikuandmetega seotud rikkumistest, mis võivad oluliselt mõjutada andmesubjektide õigusi. Selline teade tuleb esitada viivitamata[454].

ELi õigusega on kehtestatud üksikasjalik kord, mis reguleerib teadete ajastust ja sisu[455]. Sellest tulenevalt peavad vastutavad töötlejad teatama teatud isikuandmetega seotud rikkumisest järelevalveasutustele põhjendamatu viivituseta ning võimaluse korral 72 tunni jooksul pärast rikkumisest teada saamist. Kui järelevalveasutust teavitatakse hiljem kui 72 tunni jooksul, tuleb seda teates põhjendada. Vastutavad töötlejad on teatamiskohustusest vabastatud ainult siis, kui nad suudavad tõendada, et isikuandmetega seotud rikkumine ei põhjusta tõenäoliselt ohtu asjaomaste isikute õigustele ja vabadustele.

Määruses täpsustatakse miinimumteave, mida teade peab sisaldama, et järelevalveasutus saaks võtta vajalikud meetmed[456].Teade peab sisaldama vähemalt isikuandmetega seotud rikkumise olemuse kirjeldust ning asjaomaste andmesubjektide liike ja ligikaudset arvu, isikuandmetega seotud rikkumise võimalike tagajärgede kirjeldust ning vastutava töötleja poolt isikuandmetega seotud rikkumise lahendamiseks ja võimaliku kahjuliku mõju leevendamiseks võetud meetmete kirjeldust.

453 Artikli 29 töörühm (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3. oktoober 2017, lk 6.

454 Nüüdisajastatud konventsiooni nr 108 artikli 7 lõige 2 ja konventsiooni seletuskirja punktid 64–66.

455 Isikuandmete kaitse üldmääruse artiklid 33 ja 34.

456 *Ibid.*, artikli 33 lõige 3.

Lisaks sellele tuleb esitada andmekaitseametniku või muu kontaktpunkti nimi ja kontaktandmed, et pädev järelevalveasutus saaks vajaduse korral lisateavet.

Kui isikuandmetega seotud rikkumine võib tõenäoliselt põhjustada suurt ohtu üksikisikute õigustele ja vabadustele, teavitab vastutav töötleja neid isikuid (andmesubjekte) põhjendamatu viivituseta isikuandmetega seotud rikkumisest[457]. Andmesubjektidele esitatav teave, sealhulgas andmete rikkumise kirjeldus, peab olema koostatud selges ja lihtsas keeles ning sisaldama teavet, mis sarnaneb teabega, mis tuleb esitada järelevalveasutustele. Teatud asjaoludel võib vastutavad töötlejad vabastada kohustusest teavitada andmesubjekti sellistest rikkumistest. Erandeid kohaldatakse, kui vastutav töötleja on kehtestanud asjakohased tehnilised ja korralduslikud kaitsemeetmed ning neid kohaldati isikuandmetega seotud rikkumisest mõjutatud isikuandmete suhtes, kasutades eelkõige selliseid meetmeid, mis muudavad isikuandmed juurdepääsuõiguseta isikutele loetamatuks (nt krüpteerimine). Ka meetmed, mida võtab vastutav töötleja pärast rikkumise toimumist ja mis tagavad, et kahju andmesubjektide õigustele ja vabadustele ei ole enam tõenäoline, võivad ta vabastada kohustusest teavitada andmesubjekte. Kui teavitamine nõuab vastutavalt töötlejalt ebaproportsionaalset jõupingutust, on andmesubjekte võimalik teavitada rikkumisest muude vahendite, näiteks avaliku teadaande või muude sarnaste meetmete abil[458].

Isikuandmetega seotud rikkumisest järelevalveasutusele ja asjaomastele andmesubjektidele teatamise kohustus on vastutaval töötlejal. Isikuandmetega seotud rikkumised võivad siiski tekkida olenemata sellest, kas andmeid töötleb vastutav või volitatud töötleja. Seetõttu on oluline tagada, et ka volitatud töötleja oleks kohustatud teatama isikuandmetega seotud rikkumisest. Sellisel juhul peab volitatud töötleja teatama vastutavale töötlejale isikuandmetega seotud rikkumisest põhjendamatu viivituseta[459]. Vastutav töötleja on seejärel kohustatud teavitama järelevalveasutust ja mõjutatud andmesubjekte vastavalt eespool nimetatud eeskirjadele ja tähtajale.

457 *Ibid.*, artikkel 34.

458 *Ibid.*, artikli 34 lõike 3 punkt c.

459 *Ibid.*, artikli 33 lõige 2.

4.3. Vastutuse ja nõuetele vastavuse edendamise eeskirjad

Põhipunktid

- Vastutuse tagamiseks isikuandmete töötlemisel peavad vastutavad ja volitatud töötlejad pidama registrit nende vastutusel tehtud töötlemistoimingute kohta ning esitama selle nõudmisel järelevalveasutustele.
- Isikuandmete kaitse üldmääruses on sätestatud nõuetele vastavuse edendamiseks mitu vahendit:
  - andmekaitseametnike määramine teatud olukordades;
  - mõju hindamine enne isikuandmete töötlemise selliste toimingute alustamist, mis võivad tõenäoliselt tugevalt ohustada üksikisikute õigusi ja vabadusi;
  - eelkonsulteerimine asjaomase järelevalveasutusega, kui mõjuhinnang näitab, et töötlemisega kaasneb risk, mida ei saa leevendada;
  - vastutavate ja volitatud töötlejate toimimisjuhendid, kus on täpsustatud määruse kohaldamine eri töötlusvaldkondades;
  - sertifitseerimise mehhanismid, pitserid ja märgised.
- Euroopa Nõukogu õiguses pakutakse nüüdisajastatud konventsioonis nr 108 nõuetele vastavuse edendamiseks välja sarnased vahendid.

Vastutuse põhimõte on eriti oluline, et tagada andmekaitse-eeskirjade jõustamine Euroopas. Vastutav töötleja vastutab andmekaitse-eeskirjade täitmise eest ja peab suutma seda tõendada. Vastutus ei peaks tekkima alles pärast rikkumise toimumist. Pigem on vastutavatel töötlejatel ennetav kohustus järgida andmetöötluse kõigis etappides nõuetekohast andmehalduspoliitikat. Euroopa andmekaitse õigusaktide kohaselt peavad vastutavad töötlejad rakendama tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada, et töötlemine toimub kooskõlas õigusega. Nende meetmete hulgas on andmekaitseametnike määramine, töötlemist käsitlevate registrite pidamine ja dokumentide säilitamine ning eraelu puutumatuse mõjuhinnangu tegemine.

4.3.1. Andmekaitseametnikud

Andmekaitseametnikud on isikud, kes annavad nõu andmekaitse-eeskirjade täitmise kohta andmeid töötlevates organisatsioonides. Nad on olulised isikud vastutuse tagamisel, sest nad toetavad nõuete täitmist, tegutsedes ühtlasi järelevalveasutuste, andmesubjektide ja neid ametisse nimetatud organisatsiooni vahendajatena.

Euroopa Nõukogu õiguse alusel pannakse nüüdisajastatud konventsiooni nr 108 artikli 10 lõikega 1 vastutavatele töötlejatele ja volitatud töötlejatele üldine vastutus. Selleks peavad vastutavad ja volitatud töötlejad võtma kõik asjakohased meetmed, et järgida konventsioonis sätestatud andmekaitse-eeskirju, ning suutma tõendada, et nende kontrolli all toimuv andmetöötlus on kooskõlas konventsiooni sätetega. Kuigi konventsioonis ei täpsustata konkreetseid meetmeid, mida vastutavad ja volitatud töötlejad peavad võtma, nähtub nüüdisajastatud konventsiooni nr 108 seletuskirjast, et andmekaitseametniku määramine on üks võimalik meede, mis aitab kooskõla tõendada. Andmekaitseametnikele tuleb anda kõik nende ülesannete täitmiseks vajalikud vahendid[460].

Teisiti kui Euroopa Nõukogu õiguses ei ole **ELis** andmekaitseametniku määramine alati vastutavate ja volitatud töötlejate pädevuses, vaid teatud tingimustel kohustuslik. Isikuandmete kaitse üldmääruses tunnistatakse, et andmekaitseametnikul on keskne roll uues juhtimissüsteemis, ning määrus sisaldab üksikasjalikke sätteid, mis käsitlevad ametniku määramist, ametiseisundit, kohustusi ja ülesandeid[461].

Isikuandmete kaitse üldmääruse alusel on andmekaitseametniku määramine kohustuslik kolmel erijuhul: kui isikuandmeid töötleb avaliku sektori asutus või organ; kui vastutava töötleja või volitatud töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud, mis nõuavad ulatuslikku andmesubjektide korrapärast ja süstemaatilist jälgimist, või kui vastutava töötleja või volitatud töötleja põhitegevuse moodustab andmete eriliikide ja süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine[462]. Kuigi määruses ei ole määratletud selliseid mõisteid nagu „ulatuslik süstemaatiline jälgimine“ ja „põhitegevus“, on artikli 29 töörühm avaldanud suunised, kuidas neid tõlgendada[463].

460 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 87.

461 Isikuandmete kaitse üldmääruse artiklid 37–39.

462 *Ibid.*, artikli 37 lõige 1.

463 Artikli 29 töörühm (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, viimati muudetud ja vastu võetud 5. aprillil 2017.

Näide: tõenäoliselt käsitatakse sotsiaalmeedia ettevõtteid ja otsingumootoreid vastutavate töötlejatena, kelle töötlemistoimingud nõuavad andmesubjektide ulatuslikku, korrapärast ja süstemaatilist jälgimist. Selliste ettevõtete ärimudel põhineb suure koguse isikuandmete töötlemisel ning nad saavad olulist tulu, pakkudes suunatud reklaamiteenuseid ja võimaldades äriühingutel reklaamida veebikohtades. Sihtreklaam on reklaamimisviis, mis põhineb demograafial ja tarbijate varasematel ostudel või ostukäitumisel. Seetõttu on vaja süstemaatiliselt jälgida andmesubjektide veebiharjumusi ja -käitumist.

Näide: haigla ja ravikindlustuse pakkuja on tüüpilised näited sellistest vastutavatest töötlejatest, kelle tegevus seisneb isikuandmete eriliikide suuremahulises töötlemises. Üksikisiku terviseseisundi teave on nii Euroopa Nõukogu kui ka ELi õiguses sätestatud isikuandmete eriliikidena, mis tähendab tõhusamat kaitset. ELi õiguses tunnistatakse täiendavalt eriliikidena geneetilisi ja biomeetrilisi andmeid. Kui meditsiiniasutused ja kindlustusandjad töötlevad selliseid andmeid suures koguses, peavad nad isikuandmete kaitse üldmääruse kohaselt määrama andmekaitseametniku.

Lisaks on isikuandmete kaitse üldmääruse artikli 37 lõikes 4 sätestatud, et muudel kui artikli 37 lõikes 1 osutatud juhtudel võivad vastutav töötleja või volitatud töötleja või nende kategooriaid esindavad ühendused ja muud organid määrata andmekaitseametniku või nad peavad seda tegema, kui see on nõutav liidu või liikmesriigi õigusega.

Kõigil teistel organisatsioonidel puudub juriidiline kohustus andmekaitseametniku määramiseks. Samas on isikuandmete kaitse üldmääruses sätestatud, et vastutavad ja volitatud töötlejad võivad otsustada määrata andmekaitseametniku vabatahtlikult, ühtlasi võimaldades liikmesriikidel teha selline määramine kohustuslikuks enamatele organisatsioonidele kui need, kellele kohaldatakse seda määruse alusel[464].

Kui vastutav töötleja on määranud andmekaitseametniku, peab vastutav töötleja ja volitatud töötleja tagama „andmekaitseametniku nõuetekohase ja õigeaegse kaasamise kõikidesse isikuandmete kaitsega seotud küsimustesse“[465]. Näiteks peavad andmekaitseametnikud osalema andmekaitse mõju hindamise nõustamisel ning organisatsiooni töötlemistoimingute registrite koostamisel ja säilitamisel. Et andmekaitseametnikud saaksid oma ülesandeid tulemuslikult täita, peavad vastutavad

464 Isikuandmete kaitse üldmääruse artikli 37 lõiked 3 ja 4.

465 *Ibid.*, artikli 38 lõige 1.

töötlejad ja volitatud töötlejad neile tagama vajalikud ressursid, sealhulgas rahalised vahendid, taristu ja seadmed. Täiendavad nõuded hõlmavad andmekaitseametnikele ülesannete täitmiseks piisava aja tagamist ja pideva koolituse tagamist, et nad saaksid arendada oma asjatundlikkust ja püsida kursis andmekaitseõiguse kõigi arengusuundumustega[466].

Isikuandmete kaitse üldmäärusega kehtestatakse põhitagatised, millega tagatakse, et andmekaitseametnikud tegutsevad sõltumatult. Vastutavad ja volitatud töötlejad peavad tagama, et andmekaitseametnikud ei saaks nende ülesannete täitmise suhtes juhiseid äriühingult, sh tippjuhtkonnalt. Andmekaitseametnikke ei tohi nende ülesannete täitmise eest ametist vabastada ega karistada[467]. Näide: andmekaitseametnik soovitab vastutaval või volitatud töötlejal hinnata andmekaitse mõju, sest ta leiab, et töötlemisega kaasneb andmesubjektidele tõenäoliselt suur oht. Äriühing ei nõustu andmekaitseametniku nõuannetega, ei pea seda põhjendatuks ja otsustab seetõttu mõjuhinnangut mitte teha. Äriühing võib nõuannet eirata, kuid ta ei saa andmekaitseametnikku nõuande eest ametist vabastada ega karistada.

Andmekaitseametniku ülesanded ja kohustused on üksikasjalikult sätestatud isikuandmete kaitse üldmääruse artiklis 39. Nende hulka kuuluvad nõuded teavitada ja nõustada äriühingut ning andmeid töötlevaid töötajaid seoses nende kohustustega, mis tulenevad õigusaktidest, ning jälgida kooskõla ELi ja liikmesriikide andmekaitse-eeskirjadega, tehes kontrolle ja koolitades töötlemistoimingutes osalevaid töötajaid. Andmekaitseametnikud peavad tegema koostööd ka järelevalveasutusega ja tegutsema järelevalveasutuse kontaktpunktina andmetöötluse küsimustes, näiteks andmetega seotud rikkumise korral.

Seoses isikuandmetega, mida käsitlevad ELi institutsioonid ja asutused, on määruses (EÜ) nr 45/2001 sätestatud, et iga liidu institutsioon ja asutus peab määrama andmekaitseametniku. Andmekaitseametniku ülesanne on tagada, et määruse sätteid kohaldatakse ELi institutsioonides ja asutustes nõuetekohaselt ning et nii andmesubjekte kui ka vastutavaid töötlejaid teavitatakse nende õigustest ja kohustustest[468]. Samuti on ta kohustatud vastama Euroopa andmekaitseinspektori nõuetele ja tegema temaga vajaduse korral koostööd. Sarnaselt isikuandmete kaitse üldmäärusele sisaldab määrus (EÜ) nr 45/2001 sätteid andmekaitseametnike sõltumatuse

466 Artikli 29 töörühm (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, viimati muudetud ja vastu võetud 5. aprillil 2017, punkt 3.1.

467 Isikuandmete kaitse üldmääruse artikli 38 lõiked 2 ja 3.

468 Andmekaitseametnike ülesannete täielik loetelu: vt määruse (EÜ) nr 45/2001 artikli 24 lõige 1.

kohta nende ülesannete täitmisel ning vajadust tagada neile vajalik personal ja vahendid[469]. Töötlemistoiminguid teostavatest andmekaitseametnikest tuleb teatada ELi institutsioonile või asutusele (või nende organisatsioonide osakondadele) ning andmekaitseametnikud peavad pidama teatavaks tehtud töötlemistoimingute registrit[470].

4.3.2. Isikuandmete töötlemise toimingute registreerimine

Nõuetele vastavuse tõendamiseks ja aruandmiseks on äriühingud sageli õiguslikult kohustatud oma tegevust dokumenteerima ja registreerima. Oluline näide on maksuõigus ja auditeerimine, mille alusel peavad kõik ettevõtted säilitama ulatusliku dokumentatsiooni ja pidama registrit. Oluline on sarnaste nõuete kehtestamine muudes õigusvaldkondades, eelkõige andmekaitseõiguses, sest registri pidamine aitab oluliselt järgida andmekaitse-eeskirju. **ELi õiguses** sätestatakse seega, et vastutavad töötlejad või nende esindajad peavad registreerima enda vastutusel tehtavad isikuandmete töötlemise toimingud[471]. Selle kohustuse eesmärk on tagada, et vajaduse korral oleks järelevalveasutustel vajalikud dokumendid, mis võimaldavad neil kinnitada töötlemise seaduslikkust.

Dokumenteeritav teave hõlmab järgmist:

- vastutava töötleja ning (kui asjakohane) kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed;
- töötlemise eesmärgid;
- andmesubjektide kategooriate ja töötlemisega seotud isikuandmete liikide kirjeldus;
- teave vastuvõtjate kategooriate kohta, kellele isikuandmeid on avalikustatud või avalikustatakse;
- teave, kas isikuandmeid on edastatud või kavatsetakse edastada kolmandatele riikidele või rahvusvahelistele organisatsioonidele;

469 Määruse (EÜ) nr 45/2001 artikli 24 lõiked 6 ja 7.

470 *Ibid.*, artiklid 25 ja 26.

471 Isikuandmete kaitse üldmääruse artikkel 30.

- võimaluse korral eri liiki isikuandmete kustutamise tähtajad, samuti ülevaade andmetöötluse turvalisuse tagamiseks võetud tehnilistest meetmetest[472].

Kohustus pidada isikuandmete kaitse üldmääruse alusel töötlemistoimingute registrit kehtib peale vastutavate töötlejate ka volitatud töötlejatele. See on oluline edasiminek, sest enne määruse vastuvõtmist hõlmas vastutava ja volitatud töötleja vahel sõlmitud leping peamiselt volitatud töötleja kohustusi. Nende registripidamise kohustus on nüüd seadusega alusel otseselt ette nähtud.

Isikuandmete kaitse üldmääruses on sätestatud ka selle kohustuse erand. Registri pidamise nõuet ei kohaldata alla 250 töötajaga ettevõtja või organisatsiooni (vastutav töötleja või volitatud töötleja) suhtes. Samas tuleb erandi korral järgida nõuet, et töötlemine asjaomase organisatsiooni poolt ei tekita tõenäoliselt ohtu andmesubjekti õigustele ja vabadustele, töötlemine on juhtumipõhine ning ei töödelda artikli 9 lõikes 1 osutatud andmete eriliike või artiklis 10 osutatud süüdimõistvate kohtuotsuste ja süütegudega seotud andmeid.

Andmetöötlustoimingute dokumenteerimine peab võimaldama vastutavatel ja volitatud töötlejatel tõendada vastavust määrusele. Samuti peab see võimaldama järelevalveasutustel jälgida töötlemise seaduslikkust. Kui järelevalveasutus taotleb juurdepääsu nimetatud registritele, on vastutavad ja volitatud töötlejad kohustatud tegema koostööd ja tegema need kättesaadavaks.

4.3.3. Andmekaitsealane mõjuhinnang ja eelkonsulteerimine

Töötlemistoimingud kujutavad üksikisiku õigustele teatud olemuslikke riske. Isikuandmed võidakse kaotada, avaldada volitamata isikutele või töödelda ebaseaduslikult. Loomulikult sõltuvad riskid töötlemise olemusest ja ulatusest. Suuremahuliste toimingute korral, mis hõlmavad näiteks delikaatsete andmete töötlemist, on risk andmesubjektidele palju suurem võimalikest riskidest siis, kui väike äriühing töötleb oma töötajate aadresse ja eratelefoninumbreid.

Et tekib uusi tehnoloogiaid ja töötlemine muutub üha keerukamaks, peavad vastutavad töötlejad selliste riskide käsitlemiseks uurima enne töötlemistoimingu alustamist kavandatava töötlemise tõenäolist mõju. See võimaldab organisatsioonidel

472 *Ibid.*, artikli 30 lõige 1.

eelnevalt nõuetekohaselt riske tuvastada, käsitleda ja leevendada, piirates oluliselt töötlemise kahju üksikisikutele.

Andmekaitse mõjuhinnang on ette nähtud nii **Euroopa Nõukogu kui ka ELi õigusega**. Euroopa Nõukogu õigusraamistikus nõutakse nüüdisajastatud konventsiooni nr 108 artikli 10 lõikes 2, et lepinguosalised tagaksid, et vastutavad ja volitatud töötlejad „uurivad kavandatud andmete töötlemise tõenäolist mõju andmesubjektide õigustele ja põhivabadustele enne asjaomase töötlemise alustamist" ning pärast hindamist kavandataks töötlemine viisil, millega ennetatakse või minimeeritakse töötlemisega seotud riske.

ELi õigusega on kehtestatud sarnane ja üksikasjalikum kohustus vastutavatele töötlejatele, kes kuuluvad isikuandmete kaitse üldmääruse kohaldamisalasse. Määruse artiklis 35 on sätestatud, et mõju tuleb hinnata siis, kui töötlemisel tekib üksikisikute õigustele ja vabadustele tõenäoliselt suur risk. Määruses ei ole sätestatud, kuidas riski tõenäosust hinnata, vaid pigem on näidatud, mis riskid need võivad olla[473]. See loetleb töötlemistoimingud, millega kaasneb suur risk ja mille korral on eelnev mõju hindamine eriti vajalik, nimelt juhtudel, kui

- isikuandmeid töödeldakse selleks, et teha otsuseid füüsiliste isikute kohta pärast isikutega seotud isiklike aspektide profiilianalüüsil põhinevat mis tahes süstemaatilist ja põhjalikku hindamist;

- eriligiiliste andmete või süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete töötlemine toimub suures ulatuses;

- töötlemine hõlmab avaliku ala ulatuslikku ja süstemaatilist jälgimist.

Järelevalveasutused peavad vastu võtma ja avalikustama selliste isikuandmete töötlemise toimingute liikide loetelu, mille suhtes kohaldatakse nõuet teha andmekaitsealane mõjuhinnang. Järelevalveasutused võivad samuti koostada selliste töötlemistoimingute loetelu, mille korral andmekaitse mõjuhinnangut ei nõuta[474].

Kui on vaja teha mõjuhinnang, peavad vastutavad töötlejad hindama töötlemise vajalikkust ja proportsionaalsust ning võimalikke riske üksikisikute õigustele. Mõju hindamine peab sisaldama ka kavandatavaid turvameetmeid tuvastatud riskide

473 Isikuandmete kaitse üldmääruse preambul, põhjendus 75.

474 *Ibid.*, artikli 35 lõiked 4 ja 5.

käsitlemiseks. Loetelude koostamiseks peavad liikmesriikide järelevalveasutused tegema koostööd nii omavahel kui ka Euroopa Andmekaitsenõukoguga. See tagab kogu ELis järjepideva lähenemisviisi nendele toimingutele, mis nõuavad mõju hindamist, ning vastutavad töötlejad peavad järgima samu nõudeid sõltumata asukohast.

Kui pärast mõju hindamist selgub, et töötlemise tulemusel tekib suur risk üksikisikute õigustele ja riskileevendusmeetmeid ei võetud, peab vastutav töötleja enne töötlemistoimingu alustamist konsulteerima asjaomase järelevalveasutusega[475].

Artikli 29 töörühm on avaldanud suunised andmekaitse mõjuhinnangu kohta ning selle kohta, kuidas määrata, kas isikuandmete töötlemise tulemusena tekib tõenäoliselt suur risk[476]. Töörühm töötas välja 9 kriteeriumi, et aidata määrata, kas andmekaitse mõjuhinnang on nõutav konkreetse juhtumi korral:[477] 1) hindamine; 2) õiguslike või samaväärsete oluliste tagajärgedega automaatotsuste tegemine; 3) süstemaatiline jälgimine; 4) delikaatsed andmed; 5) isikuandmete ulatuslik töötlemine; 6) andmekogumite sobitamine või kombineerimine; 7) haavatavate andmesubjektide andmed; 8) uuenduslik kasutamine või uute tehnoloogiliste või korralduslike lahenduste rakendamine; 9) kui isikuandmete töötlemise toimingud ise „takistavad andmesubjektidel õiguse või teenuse või lepingu kasutamist". Artikli 29 töörühm kehtestas üldreegli, et vähem kui kahele kriteeriumile vastavate töötlemistoimingute korral on ohutase madalam ja puudub vajadus teha andmekaitsehinnang, kuid vähemalt kahele kriteeriumile vastavate toimingute korral on hindamine nõutav. Kui ei ole selge, kas andmekaitse mõjuhinnangut on vaja, soovitab artikli 29 töörühm mõju siiski hinnata, sest see on „kasulik vahend, mis aitab vastutavatel töötlejatel järgida andmekaitse õigusakte"[478]. Uue andmetöötlustehnoloogia kasutuselevõtu korral on oluline, et koostatakse andmekaitse mõjuhinnang[479].

475 *Ibid.*, artikli 3 lõige 1; artikli 29 töörühm (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Brüssel, 4. oktoober 2017.

476 Artikli 29 töörühm (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Brüssel, 4. oktoober 2017.

477 *Ibid.*, lk 9–11.

478 *Ibid.*, lk 9.

479 *Ibid.*

4.3.4. Toimimisjuhendid

Toimimisjuhendeid kasutatakse mitmes tööstusvaldkonnas, et kirjeldada ja täpsustada isikuandmete kaitse üldmääruse kohaldamist valdkonnas. Isikuandmete vastutavate ja volitatud töötlejate jaoks võib selliste juhendite koostamine oluliselt parandada ELi andmekaitse-eeskirjade järgimist ja tõhustada nende rakendamist. Valdkonnaliikmete oskusteabe abil leitakse lahendused, mis on praktilised ja mida seepärast tõenäoliselt ka järgitaks. Tunnistades asjaomaste juhendite olulisust andmekaitseõiguse tõhusal kohaldamisel, kutsutakse isikuandmete kaitse üldmääruses liikmesriike, järelevalveasutusi, komisjoni ja Euroopa Andmekaitsenõukogu üles toetama toimimisjuhendite koostamist, mille eesmärk on aidata kaasa määruse nõuetekohasele kohaldamisele kogu ELis[480]. Juhendites võib täpsustada määruse kohaldamist konkreetsetes valdkondades, sealhulgas sellistes küsimustes nagu isikuandmete kogumine, andmesubjektidele ja üldsusele antav teave ning andmesubjektide õiguste kasutamine.

Et tagada toimimisjuhendite vastavus isikuandmete kaitse üldmääruse alusel kehtestatud eeskirjadele, tuleb need enne vastuvõtmist esitada pädevale järelevalveasutusele. Järelevalveasutus esitab seejärel arvamuse, kas juhendi kavand vastab määrusele, ning kui ta leiab, et see tagab piisavad asjakohased kaitsemeetmed, kiidab ta kavandi heaks[481]. Järelevalveasutused peavad avaldama heakskiidetud toimimisjuhendid ja nende heakskiitmise kriteeriumid. Kui toimimisjuhendi kavand on seotud töötlemistoimingutega mitmes liikmesriigis, esitab pädev järelevalveasutus enne juhendi kavandi, muudetud või laiendatud juhendi heakskiitmist juhendi Euroopa Andmekaitsenõukogule, kes esitab arvamuse, kas juhend vastab isikuandmete kaitse üldmäärusele. Komisjon võib rakendusaktidega otsustada, et talle esitatud heakskiidetud toimimisjuhend kehtib kogu liidus.

Toimimisjuhendi järgimine annab olulisi eeliseid nii andmesubjektidele kui ka vastutavatele ja volitatud töötlejatele. Need juhendid sisaldavad üksikasjalikke juhiseid, millega kohandatakse õigusnõudeid konkreetsetele sektoritele ja edendatakse töötlemistoimingute läbipaistvust. Ka vastutavad ja volitatud töötlejad võivad kasutada juhendi järgimist tõendina, et nad toimivad kooskõlas ELi õigusega, ning selleks, et parandada enda avalikku kuvandit organisatsioonidena, kes peavad oma tegevuses andmekaitset esmatähtsaks ning on sellele pühendunud. Heakskiidetud toimimisjuhendeid koos siduvate ja jõustatavate kohustustega võib kasutada asjakohaste kaitsemeetmetena andmete edastamisel kolmandatele riikidele. Et tagada,

480 Isikuandmete kaitse üldmääruse artikli 40 lõige 1.

481 *Ibid.*, artikli 40 lõige 5.

et toimimisjuhendeid järgivad organisatsioonid järgivad juhendeid ka tegelikult, võib nõuete täitmise seireks ja tagamiseks määrata eraldi (asjaomase järelevalveasutuse akrediteeritud) asutuse. Oma ülesannete tulemuslikuks täitmiseks peab asutus olema sõltumatu, tal peavad olema tõendatud eksperditeadmised toimimisjuhendis reguleeritud küsimustes ning tal peavad olema kehtestatud läbipaistvad menetlused ja struktuurid, mis võimaldavad tal käsitleda toimimisjuhendi rikkumise kohta esitatud kaebusi[482].

Euroopa Nõukogu õiguses on nüüdisajastatud konventsioonis nr 108 sätestatud, et riigisisese õigusega tagatud andmekaitse taset saab edukalt tugevdada vabatahtlike reguleerimismeetmetega, näiteks hea toimimistava juhendite või kutseliste toimimisjuhenditega. Samas on need nüüdisajastatud konventsioonis nr 108 üksnes vabatahtlikud meetmed: sellise meetme võtmise juriidilist kohustust ei ole võimalik kehtestada, kuigi see on soovitatav, ja sellised meetmed ei ole iseenesest piisavad, et tagada konventsiooni täielik järgimine[483].

4.3.5. Sertifitseerimine

Lisaks toimimisjuhenditele saavad vastutavad ja volitatud töötlejad isikuandmete kaitse üldmääruse järgimist tõendada sertifitseerimismehhanismide ning andmekaitsepitserite ja -märgiste abil. Selleks sätestatakse määruses vabatahtlik sertifitseerimissüsteem, mille kohaselt teatud asutused või järelevalveasutused võivad väljastada sertifikaate. Vastutavad ja volitatud töötlejad, kes otsustavad sertifitseerimismehhanismi järgida, võivad suurendada nähtavust ja usaldusväärsust sertifikaatide, pitserite ja märgiste abil, sest nende abil saavad andmesubjektid kiiresti hinnata organisatsioonide andmekaitse taset. Oluline on märkida, et sertifikaadi omamine ei vähenda vastutava või volitatud töötleja kohustusi ja vastutust täita määruse kõiki nõudeid.

4.4. Lõimitud ja vaikimisi andmekaitse

Lõimitud andmekaitse

ELi õiguses nõutakse, et vastutavad töötlejad kehtestavad meetmed andmekaitsepõhimõtete tõhusaks rakendamiseks ja vajalike kaitsemeetmete integreerimiseks,

482 *Ibid.*, artikli 41 lõiked 1 ja 2.

483 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 33.

et täita määruse nõudeid ja kaitsta andmesubjektide õigusi[484]. Neid meetmeid tuleb rakendada nii töötlemise ajal kui ka töötlemisvahendite määramisel. Meetmete rakendamisel peab vastutav töötleja arvestama viimaseid arenguid, rakendamiskulusid, isikuandmete töötlemise olemust, ulatust ja eesmärke ning riske andmesubjekti õigustele ja vabadustele ning riskide raskust[485].

Euroopa Nõukogu õiguses nõutakse, et vastutavad ja volitatud töötlejad hindavad enne töötlemise algust isikuandmete töötlemise tõenäolist mõju andmesubjektide õigustele ja vabadustele. Lisaks on vastutavad ja volitatud töötlejad kohustatud kavandama andmetöötluse nii, et ennetada või minimeerida õiguste ja vabaduste kahjustamise riski, ning rakendama tehnilisi ja korralduslikke meetmeid, mis arvestavad isikuandmete kaitse õiguse mõju isikuandmete töötlemise kõigis etappides[486].

Vaikimisi andmekaitse

ELi õigusaktidega nõutakse, et vastutav töötleja rakendaks asjakohaseid meetmeid tagamaks, et vaikimisi töödeldakse üksnes isikuandmeid, mis on vajalikud konkreetse eesmärgi saavutamiseks. See kehtib kogutud isikuandmete koguse, töötlemise ulatuse, säilitamisaja ja kättesaadavuse suhtes[487]. See meede peab näiteks tagama, et mitte kõigil vastutavate töötlejate töötajatel ei ole juurdepääsu andmesubjektide isikuandmetele. Euroopa Andmekaitseinspektor töötas vajalikkuse töövahendis[488] välja täiendavad suunised.

Euroopa Nõukogu õiguses nõutakse, et vastutavad ja volitatud töötlejad rakendavad tehnilisi ja korralduslikke meetmeid, et arvestada isikuandmete kaitse õiguse mõju andmetöötluse kõigis etappides[489].

484 Isikuandmete kaitse üldmääruse artikli 25 lõige 1.

485 Vt artikli 29 töörühm (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 4. oktoober 2017. Vt ka ENISA (2015), *Privacy and Data Protection by Design-from policy to engineering*, 12. jaanuar 2015.

486 Nüüdisajastatud konventsiooni nr 108 artikli 10 lõiked 2 ja 3; nüüdisajastatud konventsiooni seletuskirja punkt 89.

487 Isikuandmete kaitse üldmääruse artikli 25 lõige 2.

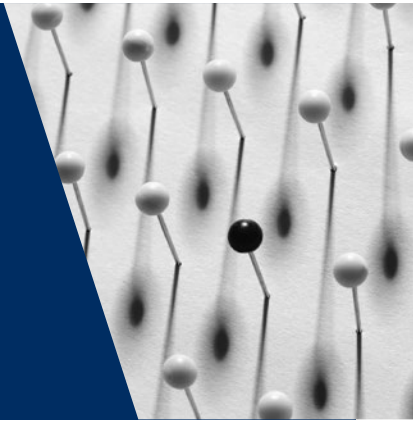
488 Euroopa Andmekaitseinspektor (2017), *Necessity Toolkit*, Brüssel, 11. aprill 2017.

489 Nüüdisajastatud konventsiooni nr 108 artikli 10 lõige 3; nüüdisajastatud konventsiooni seletuskirja punkt 89.

2016. aastal avaldas ENISA aruande eraelu puutumatust tagavate vahendite ja teenuste kohta[490]. Muu hulgas esitatakse selles hinnangus kriteeriumid ja parameetrid, mis näitavad eraelu puutumatuse häid või halbu tavasid. Kuigi osa kriteeriume – näiteks pseudonüümimine ja heakskiidetud sertifitseerimismehhanismid – on otseselt seotud isikuandmete kaitse üldmääruse sätetega, pakuvad teised kriteeriumid uuenduslikke algatusi, et tagada lõimitud ja vaikimisi eraelukaitse. Näiteks kuigi kasutatavuse kriteerium ei ole otseselt seotud eraelu puutumatusega, võib see tugevdada eraelu puutumatust, sest võimaldab eraelu puutumatust tagava vahendi või teenuse laiemat kasutuselevõttu. Tegelikkuses võib üldsus vähe kasutada neid eraelu puutumatust tagavaid vahendeid, mida on raske rakendada, isegi kui need pakuvad väga tugevaid eraelu puutumatuse tagatisi. Lisaks on otsustava tähtsusega kriteerium eraelu puutumatust tagava vahendi valmidus ja stabiilsus, mis tähendab, et vahend areneb aja jooksul ja vastab eraelu puutumatusega seotud olemasolevatele või uutele ülesannetele. Muud eraelu puutumatust soodustavad tehnoloogiad, näiteks turvalise side kontekstis, on otspunktkrüpteerimine (sideviis, kus ainsad inimesed, kes saavad sõnumeid lugeda, on omavahel suhtlevad inimesed); kliendi ja serveri vahelise side krüpteerimine (krüpteeritakse kliendi ja serveri vaheline sidekanal); autentimine (suhtlevate poolte isikusamasuse kontrollimine) ning anonüümne side (kolmas isik ei saa tuvastada suhtlevate poolte isikuid).

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools*, 20. detsember 2016.

5 Sõltumatu järelevalveasutus



EL	Teemad	EN
Põhiõiguste harta artikli 8 lõige 3 Euroopa Liidu toimimise lepingu artikli 16 lõige 2 Isikuandmete kaitse üldmääruse artiklid 51–59 ELK, C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik* [suurkoda], 2010 ELK, C-614/10, *Euroopa Komisjon vs. Austria Vabariik* [suurkoda], 2012 ELK, C-288/12, *Euroopa Komisjon vs. Ungari* [suurkoda], 2014 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 2015	**Järelevalve-asutused**	Nüüdisajastatud konventsiooni nr 108 artikkel 15
Isikuandmete kaitse üldmääruse artiklid 60–67	**Järelevalve-asutuste koostöö**	Nüüdisajastatud konventsiooni nr 108 artiklid 16–21
Isikuandmete kaitse üldmääruse artiklid 68–76	**Euroopa Andmekaitse-nõukogu**	

Põhipunktid

- Sõltumatu järelevalve on Euroopa andmekaitseõiguse oluline osa ja on sätestatud põhiõiguste harta artikli 8 lõikes 3.
- Et andmekaitse oleks tõhus, tuleb riikide õigusaktide alusel moodustada sõltumatud järelevalveasutused.
- Järelevalveasutustel peab tegutsemisel olema tagatud täielik sõltumatus, mis peab olema tunnustatud nende asutamise õigusaktides ja kajastuma iga järelevalveasutuse organisatsioonistruktuuris.
- Järelevalveasutustel on erivolitused ja -ülesanded, näiteks järgmised:
  - andmekaitse järelevalve ja edendamine riigi tasandil;
  - andmesubjektidele, vastutavatele töötlejatele ning samuti valitsusele ja kogu avalikkusele nõu andmine;
  - kaebuste läbivaatamine ning andmesubjektide abistamine juhtumites, kus väidetavalt on rikutud andmekaitseõigusi;
  - vastutavate ja volitatud töötlejate juhendamine.
- Järelevalveasutusel on ka õigus vajaduse korral sekkuda
  - hoiatades, noomides või isegi trahvides vastutavaid või volitatud töötlejaid;
  - nõudes andmete parandamist, sulgemist või kustutamist;
  - keelates andmete töötlemise või määrates haldustrahvi;
  - andes asja kohtusse.
- Et sageli osalevad isikuandmete töötlemisel eri riikides asuvad vastutavad ja volitatud töötlejad ning andmesubjektid, peavad järelevalveasutused tegema üksteisega piiriülestes küsimustes koostööd, et tagada üksikisikute tõhus kaitse Euroopas.
- ELis luuakse isikuandmete kaitse üldmäärusega piiriülese töötlemise juhtumite jaoks ühtne kontaktpunkt. Osa äriühinguid teeb piiriülese töötlemise toiminguid seoses isikuandmete töötlemisega mitmes liikmesriigis asutatud äriühingu tegevuse raames või seoses äriühinguga, mis on asutatud liidus ainult ühes kohas, kuid mis mõjutab oluliselt andmesubjekte mitmes liikmesriigis. Selliste äriühingute järelevalvet teeb ainult üks riiklik andmekaitse järelevalveasutus.
- Koostöö- ja järjepidevusmehhanism võimaldab rakendada koordineeritud lähenemisviisi kõigi juhtumiga seotud järelevalveasutuste vahel. Peamise või ühe tegevuskoha juhtiv järelevalveasutus konsulteerib teiste asjaomaste järelevalveasutustega ja esitab oma otsuse kavandi.

- Sarnaselt praeguse artikli 29 töörühmaga osaleb Euroopa Andmekaitsenõukogus iga liikmesriigi järelevalveasutus ja Euroopa Andmekaitseinspektor.
- Euroopa Andmekaitsenõukogu ülesannete hulka kuulub näiteks määruse nõuetekohase kohaldamise seire, komisjoni nõustamine asjakohastes küsimustes ning mitmesuguste teemade kohta arvamuste, suuniste või parimate tavade avaldamine.
- Peamine erinevus on, et Euroopa Andmekaitsenõukogu ei esita mitte ainult arvamusi, nagu on sätestatud direktiivis 95/46/EÜ. Andmekaitsenõukogu esitab ka siduvad otsused juhtumite korral, kus järelevalveasutus on esitanud ühtsete kontaktpunktide kohta asjakohase ja põhjendatud vastuväite, kui esinevad vastuolulised arvamused, mis järelevalveasutus on juhtiv, ning kui pädev järelevalveasutus ei taotle Euroopa Andmekaitsenõukogu arvamust või ei järgi seda. Eesmärk on tagada määruse järjepidev kohaldamine kõigis liikmesriikides.

Sõltumatu järelevalve on Euroopa andmekaitseõiguse oluline osa. Nii ELi kui ka Euroopa Nõukogu õiguses peetakse sõltumatute järelevalveasutuste olemasolu hädavajalikuks, et tagada üksikisikute õiguste ja vabaduste tõhus kaitse nende isikuandmete töötlemisel. Et andmeid töödeldakse pidevalt ja selle mõistmine on üksikisikutele üha keerukam mõista, tegutsevad need asutused digiajastu järelevalvajatena. ELis peetakse sõltumatute järelevalveasutuste olemasolu üheks tähtsaimaks isikuandmete kaitse õiguse elemendiks, mis on sätestatud ELi esmastes õigusaktides. ELi põhiõiguste harta artikli 8 lõikes 3 ja Euroopa Liidu toimimise lepingu artikli 16 lõikes 2 tunnistatakse isikuandmete kaitset põhiõigusena ning kinnitatakse, et andmekaitse-eeskirjade täitmist peab kontrollima sõltumatu asutus.

Andmekaitseõiguse sõltumatu järelevalve tähtsust on tunnistatud ka kohtupraktikas.

Näide: kohtuasjas *Schrems*[491] küsis Euroopa Liidu Kohus, kas isikuandmete edastamine USA-le esimese ELi-USA programmi Safe Harbor lepingu alusel oli kooskõlas ELi andmekaitseõigusega, arvestades Edward Snowdeni paljastusi USA riikliku julgeolekuagentuuri ulatusliku järelevalve kohta. Isikuandmete edastamine USAsse põhines Euroopa Komisjoni 2000. aasta otsusel, mis võimaldas edastada isikuandmeid EList USA organisatsioonidele, kes kinnitavad ise programmi Safe Harbor raames, et süsteem tagab isikuandmete kaitse piisava taseme. Kui Iiri järelevalveasutusel paluti uurida kaebuse esitaja kaebust andmete edastamise seaduslikkuse kohta pärast Snowdeni paljastusi, lükkas Iiri järelevalveasutus kaebuse tagasi põhjendusega, et komisjoni

491 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

otsuse olemasolu USA andmekaitsekorra piisavuse kohta, mis kajastub programmi Safe Harbor põhimõtetes (programmi Safe Harbor käsitlev otsus), ei võimaldanud tal kaebust edasi uurida.

Euroopa Liidu Kohus leidis siiski, et komisjoni sellise otsuse olemasolu, mis võimaldab andmete edastamist kolmandatele riikidele, kes tagavad piisava kaitsetaseme, ei kaota riiklike järelevalveasutuste volitusi ega vähenda neid. Euroopa Liidu Kohus märkis, et nende asutuste volitused teha järelevalvet ELi andmekaitse-eeskirjade üle ja tagada nende täitmine tulenevad ELi esmasest õigusest, eelkõige põhiõiguste harta artikli 8 lõikest 3 ja Euroopa Liidu toimimise lepingu artikli 16 lõikest 2. „Sõltumatute järelevalveasutuste asutamine […] on seega oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega.“[492]

Seetõttu otsustas Euroopa Liidu Kohus, et isegi kui isikuandmete edastamise suhtes on Euroopa Komisjon teinud kaitse piisavuse otsuse ja avaldus esitatakse riiklikule järelevalveasutusele, on asutus kohustatud avalduse nõuetekohase hoolsusega läbi vaatama. Järelevalveasutus võib avalduse tagasi lükata, kui leiab, et see on alusetu. Sellisel juhul rõhutas Euroopa Liidu Kohus, et õigus tõhusale õiguskaitsevahendile eeldab, et üksikisikutel peab olema võimalik vaidlustada selline otsus liikmesriigi kohtus, kes võib esitada Euroopa Liidu Kohtule komisjoni otsuse kehtivuse kohta eelotsusetaotluse. Kui järelevalveasutus leiab, et kaebus on põhjendatud, peab tal olema võimalik osaleda kohtumenetluses ja pöörduda liikmesriigi kohtusse. Liikmesriigi kohtud võivad pöörduda Euroopa Liidu Kohtusse, sest see on ainus organ, kellel on õigus otsustada, kas komisjoni tehtud kaitse piisavuse otsus kehtib[493].

Seejärel uuris Euroopa Liidu Kohus programmi Safe Harbor käsitleva otsuse kehtivust, et leida, kas andmete edastamise süsteem on kooskõlas ELi andmekaitse-eeskirjadega või mitte. Kohus leidis, et programmi Safe Harbor käsitleva otsuse artikliga 3 piirati riiklike järelevalveasutuste volitusi (mis olid antud andmekaitsedirektiivi alusel), et võtta meetmeid andmete edastamise tõkestamiseks juhul, kui USAs ei ole isikuandmete kaitse tagatud piisaval tasemel. Arvestades, kui olulised on sõltumatud järelevalveasutused

492 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015, punkt 41.

493 *Ibid.*, punktid 53–66.

andmekaitse õigusaktide järgimise tagamiseks, leidis Euroopa Liidu Kohus, et andmekaitsedirektiivi alusel ja põhiõiguste hartat arvestades ei olnud komisjonil pädevust piirata sel viisil sõltumatute järelevalveasutuste volitusi. Järelevalveasutuste volituste piiramine oli üks põhjustest, miks Euroopa Liidu Kohus kuulutas programmi Safe Harbor käsitleva otsuse kehtetuks.

Seega on Euroopa õiguse kohaselt sõltumatu järelevalve oluline mehhanism andmekaitse tõhususe tagamisel. Sõltumatud järelevalveasutused on eraelu puutumatuse rikkumise korral andmesubjektide jaoks esimene kontaktpunkt[494]. ELi ja Euroopa Nõukogu õiguse kohaselt on järelevalveasutuste loomine kohustuslik. Mõlemas õigusraamistikus on kirjeldatud nende asutuste ülesandeid ja volitusi sarnaselt isikuandmete kaitse üldmääruses sisalduvatele ülesannetele ja volitustele. Põhimõtteliselt peavad järelevalveasutused seega tegutsema nii Euroopa Nõukogu kui ka ELi õiguskorras ühtmoodi[495].

5.1. Sõltumatus

ELi õiguse ja **Euroopa Nõukogu õiguse** kohaselt peab iga järelevalveasutus tegutsema talle antud ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult[496]. Järelevalveasutuse ja selle liikmete ning töötajate sõltumatus otsestest või kaudsetest välismõjutustest on andmekaitse otsuste tegemisel ülioluline, et tagada täielik objektiivsus. Järelevalveasutuse loomise õigusakt peab sisaldama sätteid, millega tagatakse asutuse sõltumatus, kuid seejuures peab sõltumatus kajastuma ka asutuse organisatsioonistruktuuris. 2010. aastal uuris Euroopa Liidu Kohus esimest korda, mis ulatuses on andmekaitse järelevalveasutused kohustatud olema sõltumatud[497]. Näited illustreerivad, kuidas Euroopa Liidu Kohus määratleb „täieliku sõltumatuse“ tähendust.

494 Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt d.

495 *Ibid*., artikkel 51; nüüdisajastatud konventsiooni nr 108 artikkel 15.

496 Isikuandmete kaitse üldmääruse artikli 52 lõige 1; nüüdisajastatud konventsiooni nr 108 artikli 15 lõige 5.

497 FRA (2010), „Põhiõigused: peamised õiguslikud ja poliitilise arengusuunad 2010. aastal“, aastaaruanne 2010, lk 59; FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities*, mai 2010.

Näide: kohtuasjas *Euroopa Komisjon vs. Saksamaa Liitvabariik*[498] palus Euroopa Komisjon Euroopa Liidu Kohtul tuvastada, et Saksamaa oli ebaõigesti üle võtnud andmekaitse tagamise eest vastutavate asutuste täieliku sõltumatuse nõude ning seega rikkunud andmekaitsedirektiivi artikli 28 lõikest 1 tulenevaid kohustusi. Komisjoni arvamuse kohaselt rikkus sõltumatuse nõuet asjaolu, et Saksamaa allutas riiklikule järelevalvele asutused, kes olid eri liidumaades (*Länder*) pädevad tegema isikuandmete töötlemise järelevalvet, et tagada vastavus andmekaitseõigusele.

Euroopa Liidu Kohus rõhutas, et väljendit „täiesti sõltumatult" tuleb tõlgendada selle sätte tavapärasest tähendusest ning ELi andmekaitseõiguse eesmärkidest ja ülesehitusest lähtudes[499]. ELK märkis, et järelevalveasutused on isikuandmete töötlemisega seotud õiguste kaitsjad. Järelevalveasutuste asutamine liikmesriikides on seega „oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega"[500]. ELK järeldas, et „oma ülesannete täitmisel peavad järelevalveasutused tegutsema objektiivselt ja erapooletult. Selleks peavad nad olema kaitstud igasuguse välise mõju eest, kaasa arvatud riigi või liidumaade otsene või kaudne mõju."[501]

Samuti leidis ELK, et väljendit „täiesti sõltumatult" tuleb tõlgendada Euroopa Andmekaitseinspektori sõltumatust arvestades, nagu on kirjeldatud ELi institutsioonide andmekaitse määruses. Selles määruses nõuab sõltumatuse mõiste, et Euroopa Andmekaitseinspektor ei tohi taotleda ega võtta vastu juhiseid teistelt isikutelt.

Seega leidis ELK, et Saksamaa andmekaitseasutused ei olnud ELi andmekaitseõiguse tähenduses täiesti sõltumatud, sest nad olid allutatud riigiasutuste järelevalvele.

Näide: kohtuasjas *Euroopa Komisjon vs. Austria Vabariik*[502] tõstis ELK esile sarnaseid probleeme seoses Austria andmekaitseasutuse (andmekaitsekomisjoni) liikmete ja töötajate ametikohtadega. ELK järeldas, et asjaolu, et föderaalkantselei vastutas järelevalveasutuse personaliküsimuste eest,

498 ELK, C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik* [suurkoda], 9. märts 2010, punkt 27.

499 *Ibid.*, punktid 17 ja 29.

500 *Ibid.*, punkt 23.

501 *Ibid.*, punkt 25.

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

kahjustas ELi andmekaitseõiguses sätestatud sõltumatuse nõuet. ELK leidis ka, et nõue, et andmekaitseasutus pidi kantseleid mis tahes ajal oma tööst teavitama, muudab järelevalveasutuse täieliku sõltumatuse olematuks.

Näide: kohtuasjas *Euroopa Komisjon vs. Ungari*[503] keelustati sarnased riiklikud tavad, mis mõjutavad tööjõu sõltumatust. ELK juhtis tähelepanu, et „nõue tagada, et iga järelevalveasutus tegutseb talle usaldatud ülesannete täitmisel täiesti sõltumatult, hõlmab asjaomase liikmesriigi kohustust pidada kinni selle asutuse ametiaja kestusest kuni algselt ette nähtud tähtaja lõpuni". ELK leidis ka, et „kuna Ungari lõpetas ennetähtaegselt isikuandmete kaitse järelevalveasutuse ametiaja, on ta rikkunud kohustusi, mis tulenevad [...] direktiivist 95/46/EÜ [...]."

„Täieliku sõltumatuse" mõiste ja kriteeriumid on nüüd selge sõnaga sätestatud isikuandmete kaitse üldmääruses, mis sisaldab Euroopa Liidu Kohtu kirjeldatud otsustega kehtestatud põhimõtteid. Määruse kohaselt tähendab täielik sõltumatus järelevalveasutustele antud ülesannete täitmisel ja volituste kasutamisel järgmist:[504]

- iga järelevalveasutuse liikmed peavad olema vabad nii otsestest kui ka kaudsetest välismõjutustest ning ei tohi kelleltki küsida ega vastu võtta juhiseid;
- iga järelevalveasutuse liikmed peavad hoiduma oma kohustustega kokkusobimatust tegevusest, et vältida huvide konflikte;
- liikmesriigid peavad tagama, et igal järelevalveasutusel oleks inim-, tehnilised ja rahalised ressursid ning taristu oma ülesannete tõhusaks täitmiseks;
- liikmesriigid peavad tagama, et iga järelevalveasutus valib oma töötajad ise;
- järelevalveasutuse üle tehakse riigisisese õiguse alusel finantskontrolli, mis ei tohi mõjutada asutuse sõltumatust. Järelevalveasutustel peavad olema eraldi ja avalikud aastaeelarved, mis võimaldavad neil nõuetekohaselt tegutseda.

Järelevalveasutuste sõltumatust peetakse oluliseks nõudeks ka Euroopa Nõukogu õiguses. Nüüdisajastatud konventsiooni nr 108 kohaselt peavad järelevalveasutused „tegutsema oma ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult ja

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

504 Isikuandmete kaitse üldmääruse artikkel 52.

erapooletult", küsimata või vastu võtmata juhiseid[505]. Sel viisil tunnistatakse konventsioonis, et need asutused ei saa tõhusalt kaitsta andmetöötlusega seotud üksikisikute õigusi ja vabadusi, v.a kui nad täidavad oma ülesandeid täiesti sõltumatult. Nüüdisajastatud konventsiooni nr 108 seletuskirjas on sätestatud mitu elementi, mis aitavad tagada selle sõltumatuse. Need elemendid hõlmavad järelevalveasutuste võimalust palgata oma töötajaid ja võtta vastu otsuseid ilma välise sekkumiseta, samuti tegureid, mis on seotud nende ülesannete täitmise kestusega ja tingimustega, mille alusel nad võivad oma ülesannete täitmise lõpetada[506].

5.2. Pädevus ja volitused

ELi õiguse alusel on isikuandmete kaitse üldmääruses sätestatud järelevalveasutuste pädevus ja organisatsioonistruktuur ning asutusi kohustatakse olema pädevad ja omama volitusi määrusega nõutud ülesannete täitmiseks.

Järelevalveasutus on riigisiseses õiguses peamine asutus, kes tagab ELi andmekaitseõiguse järgimise. Järelevalveasutuste kohustuste hulka kuuluvad lisaks jälgimisele arvukad ülesanded ja volitused, sealhulgas proaktiivsed ja ennetavad järelevalvetoimingud. Nimetatud ülesannete täitmiseks peavad järelevalveasutustel olema asjakohased isikuandmete kaitse üldmääruse artiklites 57 ja 58 loetletud uurimis-, parandus- ja nõuandvad volitused, näiteks järgmised:[507]

- vastutavate töötlejate ja andmesubjektide nõustamine kõikides andmekaitseküsimustes;
- lepingu tüüptingimuste, siduvate sise-eeskirjade või halduskorra kinnitamine;
- töötlemistoimingute uurimine ja vastav sekkumine;
- vastutava töötleja tegevuse järelevalveks vajaliku mis tahes teabe esitamise nõudmine;
- vastutavatele töötlejatele hoiatuste või noomituste esitamine ja korralduste andmine teadete esitamiseks isikuandmetega seotud rikkumiste kohta, mis tuleb saata andmesubjektidele;

505 Nüüdisajastatud konventsiooni nr 108 artikli 15 lõige 5.

506 Nüüdisajastatud konventsiooni nr 108 seletuskiri.

507 Isikuandmete kaitse üldmääruse artiklid 57 ja 58. Vt ka konventsiooni nr 108 lisaprotokolli artikkel 1.

- andmete parandamiseks, sulgemiseks, kustutamiseks või hävitamiseks korralduse andmine;
- ajutiselt või lõplikult töötlemise keelamine või trahvide määramine;
- asja esitamine kohtule.

Ülesannete täitmiseks peab järelevalveasutusel olema võimalus tutvuda järelepärimise jaoks vajalike kõigi isikuandmete ja teabega, samuti peab tal olema juurdepääs ruumidele, kus vastutav töötleja hoiab asjakohast teavet. Euroopa Liidu Kohtu sõnul tuleb järelevalveasutuse volitusi tõlgendada laialt, et tagada andmesubjektide isikuandmete kaitse täielik tõhusus ELis.

Näide: kohtuasjas *Schrems* küsis ELK, kas isikuandmete edastamine USA-le esimese ELi-USA programmi Safe Harbor lepingu alusel oli kooskõlas ELi andmekaitseõigusega, arvestades Edward Snowdeni paljastusi. ELK põhjendas, et riiklikud järelevalveasutused, kes tegutsevad oma ülesandeid täites vastutavate töötlejate poolse andmetöötluse sõltumatute järelevalvajatena, võivad takistada isikuandmete edastamist kolmandale riigile vaatamata kaitse piisavuse otsuse olemasolule, kui on olemas piisavad tõendid, et kolmandas riigis ei ole piisav kaitse enam tagatud[508].

Iga järelevalveasutus on pädev teostama uurimis- ja sekkumisvolitusi oma territooriumil. Et vastutavate ja volitatud töötlejate tegevus on siiski sageli piiriülene ja andmetöötlus mõjutab mitmes liikmesriigis asuvaid andmesubjekte, tekib küsimus seoses pädevuse jagunemisega eri järelevalveasutuste vahel. Euroopa Liidu Kohtul oli võimalik uurida seda küsimust kohtuasjas *Weltimmo*.

Näide: kohtuasjas *Weltimmo*[509] kaalutles ELK riiklike järelevalveasutuste pädevust käsitleda küsimusi, mis hõlmavad nende jurisdiktsioonis asutamata organisatsioone. Weltimmo on Slovakkias registreeritud äriühing, kes haldab veebikohta, kus avaldab Ungaris asuva kinnisvara kuulutusi. Reklaamijad esitasid Ungari andmekaitseasutusele Ungari andmekaitseseaduse

508 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015, punktid 26–36 ja 40–41.

509 ELK, C-230/14, *Weltimmo s.r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktoober 2015.

rikkumise kohta kaebuse ja amet trahvis Weltimmot. Äriühing vaidlustas trahvi riigisisestes kohtutes ja kohtuasi edastati ELK-le, et leida, kas ELi andmekaitsedirektiiv võimaldas liikmesriigi järelevalveasutustel kohaldada oma riigi andmekaitseseadust teises liikmesriigis registreeritud äriühingu suhtes.

ELK tõlgendas andmekaitsedirektiivi artikli 4 lõike 1 punkti a nii, et on lubatud kohaldada selle liikmesriigi andmekaitse õigusnorme, mis ei ole liikmesriik, kus nende andmete töötlemise eest vastutav isik on registreeritud, „tingimusel et kõnealusel isikul on selle liikmesriigi territooriumil stabiilne asukoht, mille kaudu ta tegutseb tegelikult ja tulemuslikult, kas või minimaalselt ning see töötlemine toimub selle tegevuse raames". ELK märkis, et tema käsutuses oleva teabe põhjal on Weltimmo tegutsenud Ungaris tegelikult ja tulemuslikult, sest äriühingul on Ungaris esindaja, kes on kantud Slovakkia äriregistrisse Ungaris asuva aadressiga, samuti on äriühingul Ungari pangakonto ja nimekast ning ka tema tegevus toimub Ungaris ja kirjalikult ungari keeles. See teave viitas tegevuskoha olemasolule, mistõttu kuulunuks Weltimmo tegevus Ungari andmekaitseõiguse ja Ungari järelevalveasutuse jurisdiktsiooni alla. Samas jättis ELK riigisisese kohtu ülesandeks kontrollida teavet ja otsustada, kas Weltimmol on Ungaris tegevuskoht.

Kui eelotsusetaotluse esitanud kohus oleks leidnud, et Weltimmol on Ungaris tegevuskoht, olnuks Ungari järelevalveasutusel õigus määrata trahv. Kui liikmesriigi kohus otsustanuks vastupidist (et Weltimmol ei ole Ungaris tegevuskohta), olnuks kohaldatav õigus sellest tulenevalt selle liikmesriigi/liikmesriikide õigus, kus äriühing oli registreeritud. Et sellel juhul tuleb järelevalveasutuste volitusi teostada kooskõlas teiste liikmesriikide territoriaalse suveräänsusega, ei saanuks Ungari ametiasutus määrata karistusi. Et andmekaitsedirektiiv sisaldas ka järelevalveasutuste koostöö kohustust, saab Ungari ametiasutus siiski paluda Slovakkia asutusel seda küsimust uurida, tuvastada Slovakkia õiguse rikkumine ning määrata Slovakkia õigusaktides sätestatud karistused.

Isikuandmete kaitse üldmääruse vastuvõtmisega on nüüd kehtestatud üksikasjalikud eeskirjad seoses järelevalveasutuste pädevusega piiriüleste juhtumite korral. Määrusega luuakse ühtse kontaktpunkti mehhanism ja ühtlasi on määruses sätted, millega antakse järelevalveasutustele koostöövolitused. Tõhusa koostöö tagamiseks piiriüleste juhtumite korral nõutakse isikuandmete kaitse üldmääruses, et moodustatakse juhtiv järelevalveasutus, kes tegutseb vastutava või volitatud töötleja

peamise või ainsa tegevuskoha järelevalveasutusena[510]. Juhtiv järelevalveasutus vastutab piiriüleste juhtumite eest, ta on vastutava või volitatud töötleja ainus partner ning ta koordineerib koostööd teiste järelevalveasutustega, püüdes saavutada konsensust. Koostöö hõlmab teabevahetust, vastastikust abistamist jälgimisel ja uurimisel ning siduvate otsuste vastuvõtmist[511].

Euroopa Nõukogu õiguses on järelevalveasutuste pädevus ja volitused sätestatud nüüdisajastatud konventsiooni nr 108 artiklis 15. Need volitused vastavad järelevalveasutustele ELi õiguse alusel antud volitustele, hõlmates uurimis- ja sekkumisvolitusi, volitusi otsuste tegemiseks ja halduskaristuste kehtestamiseks konventsiooni sätete rikkumise korral ning kohtumenetluses osalemise volitusi. Samuti on sõltumatutel järelevalveasutustel pädevus käsitleda andmesubjektide esitatud taotlusi ja kaebusi, teadvustada andmekaitseõigust üldsusele ning anda riiklikele otsustajatele nõu mis tahes õigus- või haldusmeetmete kohta, millega nähakse ette isikuandmete töötlemine.

5.3. Koostöö

Isikuandmete kaitse üldmäärusega kehtestatakse järelevalveasutuste koostöö üldraamistik ning sätestatakse täpsemad eeskirjad järelevalveasutuste koostöö kohta piiriülesel andmetöötlusel.

Isikuandmete kaitse üldmääruse alusel osutavad järelevalveasutused üksteisele vastastikust abi ja jagavad asjakohast teavet, et tagada määruse ühetaoline rakendamine ja kohaldamine[512]. See hõlmab järelevalveasutusi, kellele esitati taotlus konsultatsioonide, kontrollide ja uurimiste tegemiseks. Järelevalveasutused võivad teha ühisoperatsioone, sealhulgas ühiseid uurimisi ja ühiseid järelevalvemeetmeid, milles osalevad kõigi järelevalveasutuste töötajad[513].

Vastutavad ja volitatud töötlejad tegutsevad ELis üha enam riikidevahelisel tasandil. Selleks on vaja liikmesriikide pädevate järelevalveasutuste tihedat koostööd, et tagada isikuandmete töötlemise vastavus isikuandmete kaitse üldmääruse nõuetele. Määruse kohaselt toimib ühtse kontaktpunkti mehhanism nii: kui vastutaval või volitatud töötlejal on tegevuskoht mitmes liikmesriigis või kui tal on üks

510 Isikuandmete kaitse üldmääruse artikli 56 lõige 1.

511 *Ibid*., artikkel 60.

512 *Ibid*., artikli 61 lõiked 1–3 ja artikli 62 lõige 1.

513 *Ibid*., artikli 62 lõige 1.

tegevuskoht, kuid töötlemistoimingud mõjutavad oluliselt andmesubjekte mitmes liikmesriigis, on peamise (või ühtse) tegevuskoha järelevalveasutus vastutava või volitatud töötleja piiriülese tegevuse eest vastutav juhtiv järelevalveasutus. Juhtivatel järelevalveasutustel on õigus võtta vastutava või volitatud töötleja suhtes jõustamismeetmeid. Ühtse kontaktpunkti mehhanismi eesmärk on parandada ELi andmekaitse õigusaktide ühtlustamist ja ühetaolist kohaldamist eri liikmesriikides. See on kasulik ka ettevõtjatele, sest nad peavad suhtlema üksnes juhtiva järelevalveasutuse, mitte mitme järelevalveasutusega. See suurendab ettevõtjate jaoks õiguskindlust ja tähendab kiiremat otsustamist ning seda, et eri järelevalveasutused ei esita ettevõtjatele vastuolulisi nõudeid.

Juhtiva järelevalveasutuse tuvastamiseks tuleb määrata ettevõtte peamine tegevuskoht ELis. Mõiste „peamine tegevuskoht" on määratletud isikuandmete kaitse üldmääruses. Lisaks on artikli 29 töörühm välja andnud vastutava või volitatud töötleja juhtiva järelevalveasutuse tuvastamise suunised, milles on peamise tegevuskoha tuvastamise kriteeriumid[514].

Kõrgetasemelise andmekaitse tagamiseks kogu ELis ei tegutse juhtiv järelevalveasutus üksi. Ta peab tegema koostööd teiste asjaomaste järelevalveasutustega, et teha otsuseid seoses vastutavate ja volitatud töötlejate poolse isikuandmete töötlemisega, püüdes saavutada konsensust ja tagada järjepidevus. Asjaomaste järelevalveasutuste koostöö hõlmab teabevahetust, vastastikust abistamist, ühiseid uurimisi ja jälgimistegevusi[515]. Vastastikuse abi osutamisel peavad järelevalveasutused hoolikalt käsitlema teiste järelevalveasutuste esitatud teabenõudeid ja võtma järelevalvemeetmeid, näiteks käsitlema eelneva loa menetluste ja konsultatsioonide, kontrollide ja uurimiste taotlusi. Vastastikust abi tuleb teiste liikmesriikide järelevalveasutustele anda taotluse korral põhjendamatu viivituseta ja mitte hiljem kui ühe kuu jooksul pärast taotluse saamist[516].

Kui vastutaval töötlejal on tegevuskoht mitmes liikmesriigis, võivad järelevalveasutused teha ühisoperatsioone, sealhulgas uurimisi ja järelevalvemeetmeid, milles osalevad teiste liikmesriikide järelevalveasutuste töötajad[517].

514 Artikli 29 töörühm (2016), *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244, Brüssel, 13. detsember 2016, muudetud 5. aprillil 2017.

515 Isikuandmete kaitse üldmääruse artikli 60 lõiked 1–3.

516 *Ibid.*, artikli 61 lõiked 1 ja 2.

517 *Ibid.*, artikli 62 lõige 1.

Järelevalveasutuste koostöö on oluline nõue ka Euroopa Nõukogu õiguses. Nüüdisajastatud konventsioonis nr 108 on sätestatud, et järelevalveasutused peavad oma ülesannete täitmiseks tegema vajalikul määral koostööd[518]. Selleks tuleb näiteks anda üksteisele mis tahes asjakohast ja kasulikku teavet ning koordineerida uurimisi ja võtta ühismeetmeid[519].

5.4. Euroopa Andmekaitsenõukogu

Selles peatükis on eespool juba kirjeldatud sõltumatute järelevalveasutuste tähtsust ja nende Euroopa andmekaitseõigusaktide kohaseid peamisi pädevusi. Euroopa Andmekaitsenõukogu on oluline tegutseja, kes tagab andmekaitse-eeskirjade tulemusliku ja järjekindla kohaldamise kogu ELis.

Isikuandmete kaitse üldmäärusega loodi Euroopa Andmekaitsenõukogu Euroopa Liidu asutusena, kellel on juriidilise isiku staatus[520]. Andmekaitsenõukogu on artikli 29 töörühma[521] õigusjärglane. Töörühm loodi andmekaitsedirektiiviga selleks, et nõustada komisjoni ELi meetmete osas, mis mõjutavad üksikisikute õigusi isikuandmete töötlemisel ja eraelu puutumatust, edendada direktiivi ühetaolist kohaldamist ning esitada komisjonile eksperdiarvamusi andmekaitsega seotud küsimustes. Artikli 29 töörühm koosnes ELi liikmesriikide järelevalveasutuste esindajatest ning komisjoni ja Euroopa Andmekaitseinspektori esindajatest.

Nagu andmekaitse töörühma, kuuluvad ka Euroopa Andmekaitsenõukokku iga liikmesriigi järelevalveasutuste juhid või nende esindajad ja Euroopa Andmekaitseinspektor või tema esindajad[522]. Euroopa Andmekaitseinspektoril on võrdne hääleõigus, v.a vaidluste lahendamisega seotud juhtudel, kui ta võib hääletada ainult ELi institutsioonide suhtes kohaldatavate selliste põhimõtete ja eeskirjadega seotud otsuste üle, mis on sisuliselt kooskõlas isikuandmete kaitse üldmääruse põhimõtetega. Komisjonil on õigus osaleda andmekaitsenõukogu tegevuses ja kohtumistel

518 Nüüdisajastatud konventsiooni nr 108 artiklid 16 ja 17.

519 *Ibid*., artikkel 17.

520 Isikuandmete kaitse üldmääruse artikkel 68.

521 Direktiivi 95/46/EÜ kohaselt oli artikli 29 töörühma ülesanne nõustada komisjoni ELi meetmete osas, mis mõjutavad üksikisikute õigusi seoses isikuandmete töötlemise ja eraelu puutumatusega, edendada direktiivi ühetaolist kohaldamist ning esitada komisjonile eksperdiarvamusi andmekaitsega seotud küsimustes. Artikli 29 töörühm koosnes ELi liikmesriikide järelevalveasutuste esindajatest koos komisjoni ja Euroopa Andmekaitseinspektori esindajatega.

522 Isikuandmete kaitse üldmääruse artikli 68 lõige 3.

ilma hääleõiguseta[523]. Andmekaitsenõukogu valib oma liikmete hulgast viieks aastaks lihthäälteenamusega eesistuja (kes vastutab andmekaitsenõukogu esindamise eest) ja kaks eesistuja asetäitjat. Peale selle on Euroopa Andmekaitsenõukogu käsutuses ka Euroopa Andmekaitseinspektori pakutav sekretariaat, mis annab andmekaitsenõukogule analüütilist, halduslikku ja logistilist tuge[524].

Euroopa Andmekaitsenõukogu ülesandeid on üksikasjalikult kirjeldatud isikuandmete kaitse üldmääruse artiklites 64, 65 ja 70 ning need sisaldavad põhjalikke kohustusi, mis jagunevad kolmeks põhitegevuseks.

- **Järjepidevus.** Andmekaitsenõukogu võib teha õiguslikult siduvaid otsuseid kolmel juhul: kui järelevalveasutus on esitanud ühtsete kontaktpunktide kohta asjakohase ja põhjendatud vastuväite; kui tekivad vastuolulised arvamused, mis järelevalveasutus on juhtiv, ning kui pädev järelevalveasutus ei taotle Euroopa Andmekaitsenõukogu arvamust või ei järgi seda[525]. Euroopa Andmekaitsenõukogu peamine ülesanne on tagada, et isikuandmete kaitse üldmäärust kohaldatakse järjepidevalt kogu ELis ja sellel oleks oluline roll järjepidevuse mehhanismis, nagu on kirjeldatud peatükis 5.5.

- **Konsulteerimine.** Euroopa Andmekaitsenõukogu ülesanne on anda komisjonile nõu kõigis küsimustes, mis on seotud isikuandmete kaitsega liidus, näiteks isikuandmete kaitse üldmääruse muudatused, andmete töötlemist käsitlevate ELi õigusaktide muudatused, mis võivad olla vastuolus ELi andmekaitse-eeskirjadega, või komisjoni otsustega kaitse piisavuse kohta, mis võimaldavad edastada isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile.

- **Suunised.** Samuti annab nõukogu määruse järjepideva kohaldamise ergutamiseks välja suuniseid, soovitusi ja parimaid tavasid ning edendab järelevalveasutuste koostööd ja teadmiste vahetamist. Lisaks peab nõukogu julgustama vastutavate või volitatud töötlejate ühendusi koostama toimimisjuhendid ning võtma kasutusele andmekaitse sertifitseerimise mehhanisme ja andmekaitsepitsereid.

Euroopa Andmekaitsenõukogu otsuseid võib vaidlustada Euroopa Liidu Kohtus.

523 *Ibid.*, artikli 68 lõiked 4 ja 5.

524 *Ibid.*, artiklid 73 ja 75.

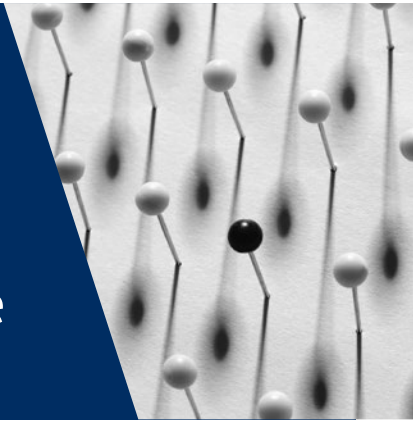
525 *Ibid.*, artikkel 65.

5.5. Isikuandmete kaitse üldmääruse järjepidevuse mehhanism

Isikuandmete kaitse üldmäärusega kehtestatakse järjepidevuse mehhanism, et tagada määruse järjepidev kohaldamine kõigis liikmesriikides, mille alusel järelevalveasutused teevad koostööd omavahel ja (kui asjakohane) komisjoniga. Järjepidevuse mehhanismi kasutatakse kahes olukorras. Esimene on seotud Euroopa Andmekaitsenõukogu arvamustega, kui pädev järelevalveasutus kavatseb võtta meetmeid, näiteks isikuandmete töötlemise selliste toimingute loetelu, mis nõuavad andmekaitse mõjuhinnangut, või määrata lepingu tüüptingimused. Teine on seotud Euroopa Andmekaitsenõukogu siduvate otsustega järelevalveasutuste kohta ühtse kontaktpunkti juhtumite korral ning kui järelevalveasutus ei järgi või ei taotle Euroopa Andmekaitsenõukogu arvamust.

6

Andmesubjektide õigused ja nende õiguste jõustamine



EL	Teemad	EN
Õigus saada teavet		
Isikuandmete kaitse üldmääruse artikkel 12 ELK, C-473/12, *Institut professionnel des agents immobiliers (IPI) vs. Englebert*, 2013 ELK, C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 2015	**Teabe läbipaistvus**	Nüüdisajastatud konventsiooni nr 108 artikkel 8
Isikuandmete kaitse üldmääruse artikli 13 lõiked 1 ja 2 ning artikli 14 lõiked 1 ja 2	**Teabe sisu**	Nüüdisajastatud konventsiooni nr 108 artikli 8 lõige 1
Isikuandmete kaitse üldmääruse artikli 13 lõige 1 ja artikli 14 lõige 3	**Teabe andmise aeg**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt b
Isikuandmete kaitse üldmääruse artikli 12 lõiked 1, 5 ja 7	**Teabe esitamise vahendid**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt b
Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt d ja artikli 14 lõike 2 punkt e, artiklid 77, 78 ja 79	**Õigus esitada kaebus**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt f

EL	Teemad	EN
Õigus tutvuda andmetega		
Isikuandmete kaitse üldmääruse artikli 15 lõige 1 ELK, C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M. E. E. Rijkeboer*, 2009 ELK, liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 2014 ELK, C-434/16, *Peter Nowak vs. Data Protection Commissioner*, 2017	**Õigus tutvuda oma isikuandmetega**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt b EIK, *Leander vs. Rootsi*, nr 9248/81, 1987
Õigus andmete parandamisele		
Isikuandmete kaitse üldmääruse artikkel 16	**Ebaõigete isikuandmete parandamine**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt e EIK, *Cemalettin Canli vs. Türgi*, nr 22427/04, 2008 EIK, *Ciubotaru vs. Moldova*, nr 27138/04, 2010
Õigus andmete kustutamisele		
Isikuandmete kaitse üldmääruse artikli 17 lõige 1	**Isikuandmete kustutamine**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt e EIK, *Segerstedt-Wiberg jt vs. Rootsi*, nr 62332/00, 2006
ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 2014 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 2017	**Õigus olla unustatud**	
Õigus isikuandmete töötlemise piiramisele		
Isikuandmete kaitse üldmääruse artikli 18 lõige 1	**Õigus piirata isikuandmete kasutamist**	
Isikuandmete kaitse üldmääruse artikkel 19	**Teatamiskohustus**	
Andmete ülekandmise õigus		
Isikuandmete kaitse üldmääruse artikkel 20	**Andmete ülekandmise õigus**	

EL	Teemad	EN
Õigus esitada vastuväiteid		
Isikuandmete kaitse üldmääruse artikli 21 lõige 1 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 2017	**Õigus esitada vastuväiteid seoses andmesubjekti konkreetse olukorraga**	Profiilianalüüsi soovituse punkt 5.3 Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt d
Isikuandmete kaitse üldmääruse artikli 21 lõige 2	**Õigus esitada vastuväiteid andmete turunduseesmärgil kasutamise kohta**	Otseturundust käsitleva soovituse artikkel 4.1
Isikuandmete kaitse üldmääruse artikli 21 lõige 5	**Õigus esitada vastuväiteid automaat-vahenditega**	
Automaatotsuste tegemise ja profiilianalüüsiga seotud õigused		
Isikuandmete kaitse üldmääruse artikkel 22	**Automaatotsuste tegemise ja profiilianalüüsiga seotud õigused**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt a
Isikuandmete kaitse üldmääruse artikkel 21	**Õigus vaidlustada automaatotsuste tegemine**	
Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt f	**Õigus sisulisele selgitusele**	Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt c
Õiguskaitsevahendid, vastutus, karistused ja hüvitamine		
Põhiõiguste harta artikkel 47 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 2015 Isikuandmete kaitse üldmääruse artiklid 77–84	**Riigisisese andmekaitseõiguse rikkumised**	Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 13 (ainult Euroopa Nõukogu liikmesriigid) Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt f ning artiklid 12, 15 ja 16–21 EIK, *K.U. vs. Soome*, nr 2872/02, 2008 EIK, *Biriuk vs. Leedu*, nr 23373/03, 2008
ELi institutsioonide andmekaitse määruse artiklid 34 ja 49 ELK, C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd* [suurkoda], 2010	**ELi õiguse rikkumised ELi institutsioonides ja asutustes**	

Laiemalt õiguslike eeskirjade ja kitsamalt andmesubjektide õiguste rakendamise tõhusus sõltub oluliselt sellest, kas nende jõustamiseks on olemas asjakohased mehhanismid. Digiajastul on andmete töötlemine muutunud üldlevinuks ja üksikisikute jaoks üha raskemini mõistetavaks. Andmesubjektide ja vastutavate töötlejate vahelise võimutasakaalutuse leevendamiseks on üksikisikutele antud teatud õigused, et saada suurem mõju oma isikuandmete töötlemise üle. Õigus tutvuda oma isikuandmetega ja õigus lasta neid parandada on sätestatud ELi põhiõiguste harta artikli 8 lõikes 2, mis on ELi esmast õigust sisaldav dokument ning millel on ELi õiguskorras oluline väärtus. ELi teisene õigus – eelkõige isikuandmete kaitse üldmäärus – on loonud sidusa õigusraamistiku, mis võimestab andmesubjekte, andes neile õigusi seoses vastutavate töötlejatega. Lisaks isikuandmetega tutvumise ja nende parandamise õigusele tunnustatakse isikuandmete kaitse üldmääruses mitut muud õigust, näiteks õigust andmete kustutamisele (õigus olla unustatud), õigust esitada vastuväiteid või piirata andmete töötlemist ning automaatotsuste tegemise ja profiilianalüüsiga seotud õigusi. Sarnased kaitsemeetmed, mis võimaldavad andmesubjektidel teostada tõhusat kontrolli oma andmete üle, sisalduvad ka nüüdisajastatud konventsioonis nr 108. Artiklis 9 on loetletud õigused, mida üksikisikud peavad saama kasutada oma isikuandmete töötlemisel. Lepinguosalised peavad tagama, et need õigused oleksid kättesaadavad kõigile nende jurisdiktsioonis olevatele andmesubjektidele, ning neile on lisatud tõhusad õiguslikud ja praktilised vahendid, mis võimaldavad andmesubjektidel neid õigusi kasutada.

Lisaks üksikisiku õiguste tagamisele on sama tähtis luua mehhanismid, mis võimaldavad andmesubjektidel oma õiguste rikkumisi vaidlustada, võtta vastutavaid töötlejaid vastutusele ja nõuda hüvitist. Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ning põhiõiguste hartas sätestatud õigus tõhusale õiguskaitsevahendile tähendab, et igal inimesel peab olema võimalus pöörduda kohtusse.

6.1. Andmesubjektide õigused

Põhipunktid

- Igal andmesubjektil on õigus saada vastutavalt töötlejalt teavet teda käsitlevate andmete mis tahes töötluse kohta, mõningate eranditega.
- Andmesubjektidel on õigus
  - tutvuda oma isikuandmetega ja saada töötlemise kohta teatud teavet;

  - lasta oma andmeid töötleval vastutaval töötlejal andmeid parandada, kui andmed on ebaõiged;
  - lasta vastutaval töötlejal oma andmed kustutada (kui asjakohane), kui ta töötleb andmesubjekti andmeid ebaseaduslikult;
  - õigus töötlemist ajutiselt piirata;
  - lasta teatud tingimustel oma andmeid üle kanda teisele vastutavale töötlejale.
- Peale selle on andmesubjektidel õigus esitada töötlemise korral vastuväiteid järgmise kohta:
  - nende konkreetse olukorraga seotud põhjustel;
  - nende andmete otseturunduse eesmärgil kasutamise korral.
- Andmesubjektidel on õigus, et nende suhtes ei kohaldata otsuseid, mis põhinevad üksnes automaattöötlusel, sealhulgas profiilianalüüsil, millel on õiguslikud tagajärjed või mis mõjutavad andmesubjekti oluliselt. Lisaks on andmesubjektidel õigus
  - nõuda et vastutava töötleja poolelt toimub inimsekkumine;
  - väljendada oma seisukohta ja vaidlustada automaattöötlusel põhinevat otsust.

6.1.1. Õigus saada teavet

Euroopa Nõukogu õiguse ja **ELi õiguse** kohaselt on töötlemistoimingute vastutavatel töötlejatel kohustus teavitada andmesubjekti isikuandmete kogumise ajal nende kavandatud töötlemise kohta. See kohustus ei sõltu andmesubjekti taotlusest, vaid vastutav töötleja peab täitma kohustust ennetavalt, olenemata sellest, kas andmesubjekt osutab teabe vastu huvi või mitte.

Euroopa Nõukogu õiguse kohaselt peavad konventsiooniosalised vastavalt nüüdisajastatud konventsiooni nr 108 artiklile 8 tagama, et vastutavad töötlejad teatavad andmesubjektile enda nime ja alalise elu- või tegevuskoha, töötlemise õiguslikkuse aluse ja eesmärgi, töödeldavate isikuandmete liigid, nende isikuandmete vastuvõtjad (kui on) ja selle, kuidas nad saavad kasutada oma õigusi vastavalt artiklile 9, mis hõlmab õigust andmetega tutvuda, neid parandada ja kasutada õiguskaitsevahendeid. Andmesubjektile tuleb edastada ka muud täiendavat teavet, mida peetakse vajalikuks, et tagada isikuandmete õiglane ja läbipaistev töötlemine. Nüüdisajastatud konventsiooni nr 108 seletuskirjas selgitatakse, et andmesubjektidele esitatav

teave peab olema kergesti kättesaadav, loetav, arusaadav ja asjaomaste andmesubjektide jaoks kohandatud[526].

ELi õiguse kohaselt eeldab läbipaistvuse põhimõte, et isikuandmete töötlemine peab olema üksikisikutele üldiselt läbipaistev. Üksikisikutel on õigus teada, kuidas ja mis isikuandmeid kogutakse, kasutatakse või muul viisil töödeldakse, samuti on neil õigus teada, mis on töötlemisega seotud ohud, kaitsemeetmed ja nende õigused[527]. Seega kehtestatakse isikuandmete kaitse üldmääruse artikliga 12 vastutavatele töötlejatele laiaulatuslik kohustus esitada läbipaistvat teavet ja/või teavitada, kuidas andmesubjektid saavad oma õigusi kasutada[528]. Teave peab olema kokkuvõtlik, läbipaistev, arusaadav ja lihtsalt kättesaadav ning selges ja lihtsas keeles. Teave tuleb esitada kirjalikult, asjakohasel juhul ka elektrooniliselt, ning seda võib esitada ka suuliselt andmesubjekti taotlusel ja tingimusel, et andmesubjekti isikusamasus on kindlalt tuvastatud. Teave esitatakse liigsete viivituste või kulutusteta[529].

Isikuandmete kaitse üldmääruse artiklites 13 ja 14 käsitletakse andmesubjektide õigust saada teavet olukordades, kus isikuandmeid koguti andmesubjektidelt otse, või olukordades, kus andmeid ei saadud otse andmesubjektidelt.

Teabe saamise õiguse ulatust ja selle ELi õiguse kohaseid piiranguid on selgitatud Euroopa Liidu Kohtu praktikas.

Näide: kohtuasjas *Institut professionnel des agents immobiliers (IPI) vs. Englebert*[530] paluti Euroopa Liidu Kohtul tõlgendada direktiivi 95/46/EÜ artikli 13 lõiget 1. See artikkel andis liikmesriikidele võimaluse valida, kas võtta õigusmeetmeid, et piirata andmesubjekti õigust saada teavet, kui seda on vaja, et kaitsta muu hulgas teiste isikute õigusi ja vabadusi ning ennetada ja uurida reguleeritud kutsealadel sooritatud kuritegusid või eetikarikkumisi. IPI on Belgia kinnisvaramaaklerite kutseühing, kelle ülesanne on tagada, et kinnisvaramaakleri kutsealal tegutsetaks nõuetekohaselt. Kutseühing palus

526 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 68.

527 Isikuandmete kaitse üldmääruse põhjendus 39.

528 *Ibid.*, artiklid 13 ja 14; nüüdisajastatud konventsiooni nr 108 artikli 8 lõike 1 punkt b.

529 Isikuandmete kaitse üldmääruse artikli 12 lõige 5; nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt b.

530 ELK, C-473/12, *Institut professionnel des agents immobiliers (IPI) vs. Geoffrey Englebert jt*, 7. november 2013.

riigisisesel kohtul avaldada, et kostjad olid rikkunud kutse-eeskirju, ja keelata mitme kinnisvarabüroo tegevus. Hagi aluseks olid eradetektiivide esitatud tõendid, mida IPI oli kasutanud.

Liikmesriigi kohus kahtles detektiivide tõendite usaldusväärsuses, arvestades võimalust, et nende saamisel ei järgitud Belgia õigusaktide andmekaitsenõudeid, eelkõige kohustust teavitada andmesubjekte nende isikuandmete töötlemisest enne selle teabe kogumist. ELK märkis, et artikli 13 lõikes 1 on sätestatud, et liikmesriigid „võivad", kuid ei ole kohustatud sätestama oma riigisiseses õiguses erandeid kohustusest teavitada andmesubjekte nende andmete töötlemisest. Et artikli 13 lõige 1 hõlmab kuritegude või kutse-eetikaga seotud rikkumiste ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist, mille tõttu liikmesriigid võivad üksikisikute õigusi piirata, võib selline moodustis nagu IPI ja tema nimel tegutsevad eradetektiivid oma tegevuses tugineda sellele sättele. Kui liikmesriik ei ole sellist erandit sätestanud, tuleb andmesubjekte sellest teavitada.

Näide: kohtuasjas *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*[531] selgitas Euroopa Liidu Kohus, kas ELi õigus välistab riigi haldusasutuse võimaluse edastada isikuandmeid teisele avalikule haldusasutusele edasiseks töötlemiseks, ilma et andmesubjekte teavitataks sellisest edastamisest ja töötlemisest. Käsitletaval juhul ei olnud riiklik haldusasutus taotlejatele enne edastamist teatanud, et nad olid taotlejate andmed edastanud riiklikule haigekassale.

ELK leidis, et ELi õigusest tulenev nõue teavitada andmesubjekti tema isikuandmete töötlemisest on „seda tähtsam, et see on vajalik tingimus, et asjassepuutuvad isikud saaksid kasutada oma õigust töödeldud andmetega tutvuda" ja neid parandada „ja oma õigust nende andmete töötlemisele vastuväiteid esitada". Õiglase töötlemise põhimõte kohustab ametiasutusi teavitama andmesubjekte sellest, et nad edastavad andmed töötlemiseks teisele ametiasutusele. Direktiivi 95/46/EÜ artikli 13 lõike 1 kohaselt võivad liikmesriigid piirata õigust saada teavet, kui selliseid piiranguid on vaja riigi oluliste majandushuvide, sealhulgas maksuküsimuste kaitsmiseks. Samas tuleb sellised piirangud kehtestada õigusaktidega. Et edastatavate andmete määratlus ega edastamise üksikasjalik kord ei olnud sätestatud õigusaktis, vaid üksnes kahe avaliku sektori asutuse vahelises protokollis, ei olnud ELi

531 ELK, C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 1. oktoober 2015.

õiguses sätestatud erandi tingimused täidetud. Taotlejaid oleks pidanud eelnevalt teavitama nende andmete edastamisest riiklikule haigekassale ja sellest, kuidas asutus andmeid edasi töötleb.

Teabe sisu

Vastavalt nüüdisajastatud konventsiooni nr 108 artikli 8 lõikele 1 peab vastutav töötleja esitama andmesubjektile kogu teabe, mis tagab isikuandmete õiglase ja läbipaistva töötlemise, sealhulgas järgmise:

- vastutava töötleja isikuandmed ja alaline elu- või asukoht;
- kavandatava andmetöötluse õiguslik alus ja eesmärgid;
- töödeldavate isikuandmete liigid;
- teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta, kui asjakohane;
- viisid, kuidas andmesubjektid saavad oma õigusi kasutada.

Isikuandmete kaitse üldmääruses on sätestatud, et kui andmesubjekti isikuandmeid kogutakse andmesubjektilt, esitab vastutav töötleja isikuandmete saamise ajal andmesubjektile kogu järgmise teabe:[532]

- vastutava töötleja nimi ja kontaktandmed, sealhulgas asjakohasel juhul andmekaitseametniku kontaktandmed;
- töötlemise eesmärk ja õiguslik alus (nt leping või seadusejärgne kohustus);
- teave vastutava töötleja õigustatud huvi kohta, kui see on töötlemise alus;
- isikuandmete võimalikud vastuvõtjad või vastuvõtjate kategooriad;
- teave, kas andmed edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile ja kas see põhineb kaitse piisavuse otsusel või sõltub asjakohastest kaitsemeetmetest;

532 Isikuandmete kaitse üldmääruse artikli 13 lõige 1.

- isikuandmete säilitamise tähtaeg või (kui see ei ole võimalik) tähtaja määramise kriteeriumid;
- andmesubjektide isikuandmete töötlemise õigused, näiteks õigus andmetega tutvuda, neid parandada või kustutada ning piirata isikuandmete töötlemist või esitada vastuväide nende töötlemise kohta;
- kas isikuandmete esitamist nõutakse õigusakti või lepingu alusel, kas andmesubjekt on kohustatud esitama oma isikuandmed ning mis on isikuandmete esitamata jätmise tagajärjed;
- teave automaatotsuste, sealhulgas profiilianalüüsi olemasolu kohta;
- teave õiguse kohta esitada kaebus järelevalveasutusele;
- teave nõusoleku tagasivõtmise õiguse olemasolu kohta.

Automaatotsuste, sealhulgas profiilianalüüsi tegemisel peavad andmesubjektid saama asjakohast teavet profiilianalüüsi loogika, tähtsuse ja talle prognoositavate tagajärgede kohta.

Kui isikuandmed ei ole saadud andmesubjektilt otse, peab vastutav töötleja teavitama üksikisikut isikuandmete päritolu kohta. Igal juhul peab vastutav töötleja muu hulgas teavitama andmesubjekte automaatotsuste, sealhulgas profiilianalüüsi tegemisest[533]. Kui vastutav töötleja kavatseb isikuandmeid edasi töödelda muul eesmärgil kui see, mis toodi algselt andmesubjektile põhjenduseks, esitab vastutav töötleja vastavalt eesmärgi piirangu ja läbipaistvuse põhimõtetele andmesubjektile teabe nimetatud muu eesmärgi kohta. Vastutavad töötlejad peavad esitama teabe enne mis tahes täiendavat töötlemist. Ehk teisisõnu: kui andmesubjekt on andnud isikuandmete töötlemise nõusoleku, peab vastutav töötleja saama andmesubjekti uue nõusoleku, kui andmete töötlemise eesmärk muutub või kui sellele lisatakse täiendavaid eesmärke.

Teabe andmise aeg

Isikuandmete kaitse üldmääruses eristatakse kaht stsenaariumi ja kaht hetke, kui vastutav töötleja peab esitama andmesubjektile teavet.

533 Isikuandmete kaitse üldmääruse artikli 13 lõige 2 ja artikli 14 lõike 2 punkt f.

- Kui isikuandmeid kogutakse otse andmesubjektilt, peab vastutav töötleja teatama isikuandmete saamise ajal andmesubjektile kõik temaga seotud andmed ja isikuandmete kaitse üldmääruse kohased õigused andmete kogumise ajal[534]. Kui vastutav töötleja kavatseb isikuandmeid muul eesmärgil edasi töödelda, esitab ta kogu asjakohase teabe enne töötlemist.

- Kui isikuandmeid ei ole saadud otse andmesubjektilt, on vastutav töötleja kohustatud esitama andmesubjektile teabe töötlemise kohta „mõistliku aja jooksul pärast isikuandmete saamist, kuid hiljemalt ühe kuu jooksul" või enne andmete avalikustamist kolmandale isikule[535].

Nüüdisajastatud konventsiooni nr 108 seletuskirjas on sätestatud, et kui andmesubjekte ei ole võimalik teavitada töötlemise alustamisel, võib seda teha hiljem, näiteks kui vastutav töötleja võtab mis tahes põhjusel andmesubjektiga ühendust[536].

Teabe andmise eri viisid

Nii Euroopa Nõukogu kui ka ELi õiguse kohaselt peab vastutav töötleja esitama andmesubjektidele kokkuvõtliku, läbipaistva, arusaadava ja lihtsasti kättesaadava teabe. See peab olema koostatud kirjalikult või muul viisil, sealhulgas elektrooniliselt, kasutades selget, lihtsat ja kergesti mõistetavat keelt. Teabe esitamisel võib vastutav töötleja kasutada standardikoone, et esitada teavet kergesti nähtaval ja mõistetaval viisil[537]. Näiteks võib kasutada tabalukuikooni, mis näitab, et andmeid kogutakse turvaliselt ja/või krüptitakse. Andmesubjektidel on võimalik taotleda teabe esitamist suuliselt. Teave peab olema tasuta, v.a kui andmesubjekti taotlused on selgelt põhjendamatud või liigsed (nt korduvad)[538]. Lihtne juurdepääs esitatud teabele on ülioluline, et andmesubjektil oleks võimalik kasutada oma õigusi, mis on sätestatud ELi andmekaitseõiguses.

534 *Ibid.*, artikli 13 lõiked 1 ja 2, sissejuhatav osa, kus isikuandmete kaitse üldmääruses viidatakse teabele, mis käsitleb kohustuse kohaldamist „isikuandmete saamise ajal".

535 *Ibid.*, artikli 13 lõige 3 ja artikli 14 lõige 3; vt ka viide mõistliku ajavahemiku ja põhjendamatu viivituseta kohta nüüdisajastatud konventsiooni nr 108 artikli 8 lõike 1 punktis b.

536 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 70.

537 Euroopa Komisjon arendab edasi ikoonide kaudu esitletavat teavet ning standardikoonide esitamise korda delegeeritud õigusaktide abil; vt isikuandmete kaitse üldmääruse artikli 12 lõige 8.

538 Isikuandmete kaitse üldmääruse artikli 12 lõiked 1, 5 ja 7; nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt b.

Õiglase andmetöötluse põhimõtte kohaselt peab teave olema andmesubjektidele lihtsalt mõistetav. Keelekasutus peab sobima sihtrühmaga. Keelekasutuse tase ja liik sõltub näiteks sellest, kas sihtrühmaks on laps või täiskasvanu, üldsus või teadlane. Küsimust, kuidas seda mõistetava teabe aspekti tasakaalustada, on käsitletud artikli 29 töörühma arvamuses teabesätete suurema ühtlustatuse kohta. See edendab nn kihiliste teadete[539] ideed, mis võimaldab andmesubjektil otsustada, mis üksikasjalikkuse taset ta eelistab. Selline teabe esitamise viis ei vabasta vastutavat töötlejat siiski tema kohustusest, mis tuleneb isikuandmete kaitse üldmääruse artiklitest 13 ja 14. Vastutav töötleja peab esitama andmesubjektile kogu teabe.

Üks tõhusamaid teabe andmise viise on, kui asjakohane teave esitatakse vastutava töötleja veebilehel, näiteks veebilehe privaatsuspoliitika. Paljud inimesed ei kasuta siiski internetti, mida tuleb arvestada ettevõtte või avaliku sektori asutuse teavitamispoliitikas.

Privaatsusteade isikuandmete töötlemise kohta veebilehel võib olla näiteks järgmine.

Kes me oleme?

Andmete vastutav töötleja on Bed and Breakfast C&U, [aadress: xxx], telefon xxx, faks xxx, e-post info@c&u.com; andmekaitseametniku kontaktandmed: [xxx].

Isikuandmete kaitse teade kuulub meie hotelliteenuseid reguleerivate tingimuste juurde.

Mis andmeid teilt kogume?

Me kogume teilt järgmist teavet: nimi, postiaadress, telefoninumber, e-posti aadress, kohalviibimise andmed, krediit- ja deebetkaardi number ning meie veebikohta külastanud arvutite IP-aadressid või domeeninimed.

539 Artikli 29 töörühm (2004), *Opinion 10/2004 on More Harmonised Information Provisions*, WP 100, Brüssel, 25. november 2004.

Miks me teie andmeid kogume?

Töötleme teie andmeid teie nõusolekul ja broneerimiseks, teile pakutavate teenustega seotud lepingute sõlmimiseks ja täitmiseks ning seadusega (nt kohalike maksude seadus) kehtestatud nõuete täitmiseks, mille kohaselt peame koguma isikuandmeid, et saaksime tasuda majutuse kohalikku maksu.

Kuidas teie andmeid töödeldakse?

Teie isikuandmeid säilitatakse kolm kuud. Teie andmete põhjal ei tehta automaatotsuseid.

Bed and Breakfast C&U järgib rangeid turbekordasid, millega tagatakse, et teie isikuandmeid ei kahjustata, hävitata ega avalikustata kolmandatele isikutele ilma teie loata, ning takistatakse volitamata juurdepääsu. Teavet säilitatakse arvutites, mis asuvad piiratud füüsilise juurdepääsuga turvalises keskkonnas. Kasutame elektroonilise juurdepääsu piiramiseks turvalisi tulemüüre ja muid meetmeid. Kui andmed tuleb edastada kolmandale isikule, nõuame neilt teie isikuandmete kaitsmiseks sarnaste meetmete olemasolu.

Kogu teavet, mida kogume või talletame, kasutatakse ainult meie kontorites. Isikuandmetele on juurdepääs ainult isikutel, kes vajavad teavet käesoleva lepingu kohaste ülesannete täitmiseks. Küsime teilt selge sõnaga, kui vajame teie isiku tuvastamise teavet. Enne teile teabe avaldamist võime paluda teil läbida meie turvakontrollid. Te saate meile esitatud isikuandmeid millal tahes uuendada, võttes meiega otse ühendust.

Mis on teie õigused?

Teil on õigus saada oma andmetele juurdepääs, saada oma andmetest koopia, nõuda andmete kustutamist või parandamist või taotleda oma andmete ülekandmist teisele vastutavale töötlejale.

Saate taotlusi esitada e-posti aadressil info@c&u.com. Peame vastama teie taotlusele ühe kuu jooksul, kuid kui päring on liiga keerukas või saame liiga palju muid päringuid, teatame teile, et tähtaega võidakse pikendada veel kahe kuu võrra.

Juurdepääs oma isikuandmetele

Teil on õigus saada oma andmetele juurdepääs, mis antakse teile taotluse korral koos andmetöötluse põhjendustega, taotleda andmete kustutamist või parandamist, ning õigus, et teie kohta ei tehta täielikult automaatseid otsuseid ilma teie seisukohti arvestamata. Saate taotlusi esitada e-posti aadressil info@c&u.com. Teil on samuti õigus vaidlustada isikuandmete töötlemine, võtta nõusolek tagasi ja esitada kaebus riiklikule järelevalveasutusele, kui leiate, et andmete töötlemine rikub seadust, ning nõuda ebaseadusliku töötlemise tagajärjel tekkinud kahju hüvitamist.

Kaebuse esitamise õigus

Isikuandmete kaitse üldmääruses nõutakse, et vastutav töötleja teavitaks andmesubjekti riikliku ja ELi õiguse kohastest täitmise tagamise mehhanismidest isikuandmetega seotud rikkumiste korral. Vastutav töötleja peab teavitama andmesubjekte nende õigusest esitada kaebus isikuandmetega seotud rikkumise kohta järelevalveasutusele ja vajaduse korral liikmesriigi kohtule[540]. Samuti nähakse Euroopa Nõukogu õigusega ette andmesubjektide õigus saada teavet oma õiguste kasutamise võimaluste kohta, sealhulgas õiguse kohta kasutada artikli 9 lõike 1 punktis f sätestatud õiguskaitsevahendit.

Teatamiskohustuse erandid

Isikuandmete kaitse üldmääruses on sätestatud teatamiskohustuse erand. Isikuandmete kaitse üldmääruse artikli 13 lõike 4 ja artikli 14 lõike 5 kohaselt ei kohaldata andmesubjektide teavitamise kohustust, kui andmesubjektil on juba kogu asjakohane teave olemas[541]. Samuti kui isikuandmed ei ole saadud andmesubjektilt, ei kohaldata teatamiskohustust, kui teabe esitamine on võimatu või nõuaks ebaproportsionaalseid jõupingutusi, eelkõige kui isikuandmeid töödeldakse avalikes huvides toimuva arhiivimise, teadus- või ajaloouuringute või statistilisel eesmärgil[542].

540 Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt d ning artikli 14 lõike 2 punkt e; nüüdisajastatud konventsiooni nr 108 artikli 8 lõike 1 punkt f.

541 *Ibid*., artikli 13 lõige 4 ja artikli 14 lõike 5 punkt a.

542 *Ibid*., artikli 14 lõike 5 punktid b–e.

Peale selle on liikmesriikidel isikuandmete kaitse üldmääruse alusel jäetud kaalutlusruum, et piirata isikutele määruse alusel antud kohustusi ja õigusi, kui see on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, näiteks selleks, et tagada riigi ja avalik julgeolek, riigikaitse, kohtuliku uurimise ja kohtumenetluste kaitse või majandus- ja finantshuvide kaitse, samuti erahuvid, mis kaaluvad üles andmekaitsehuvid[543].

Kõik erandid ja piirangud peavad olema demokraatlikus ühiskonnas vajalikud ning vastama taotletavale eesmärgile. Väga erandlikel juhtudel, näiteks meditsiinilisel näidustusel, tuleb andmesubjekti enda kaitsmiseks piirata läbipaistvuse ja arusaadavuse kohustuse täitmist; see on eelkõige seotud kõigil andmesubjektidel oleva isikuandmetega tutvumise õiguse piiramisega[544]. Kaitse miinimumtasemena tuleb riigisiseses õiguses siiski järgida ELi õigusega kaitstud põhiõiguste ja -vabaduste olemust[545]. See eeldab, et riigi õiguses on erisätted töötlemise eesmärgi, töödeldavate isikuandmete liikide, kaitsemeetmete ja muude menetlusnõuete kohta[546].

Kui isikuandmeid töödeldakse teadus- ja ajaloouuringute või statistilisel eesmärgil või avalikes huvides toimuva arhiivimise eesmärgil, võidakse liidu või liikmesriigi õiguses sätestada teatamiskohustuse erandid, kui see võib tõenäoliselt muuta võimatuks konkreetsete eesmärkide saavutamise või seda oluliselt takistada[547].

Sarnased piirangud on kehtestatud Euroopa Nõukogu õiguses, kus andmesubjektile nüüdisajastatud konventsiooni nr 108 artikli 9 alusel antud õiguste suhtes võidakse rangetel tingimustel kohaldada nüüdisajastatud konventsiooni nr 108 artikli 11 kohaseid võimalikke piiranguid. Lisaks ei kohaldata vastavalt nüüdisajastatud konventsiooni nr 108 artikli 8 lõikele 2 vastutavate töötlejate isikuandmete töötlemise läbipaistvuse kohustust, kui andmesubjektil on see teave juba olemas.

Isiku õigus tutvuda oma isikuandmetega

Euroopa Nõukogu õiguses on isiku õigus tutvuda oma isikuandmetega selge sõnaga sätestatud nüüdisajastatud konventsiooni nr 108 artiklis 9. Selle kohaselt on igal isikul on õigus saada taotluse korral teavet oma isikuandmete töötlemise kohta, mis

543 Isikuandmete kaitse üldmääruse artikli 23 lõige 1.

544 Isikuandmete kaitse üldmääruse artikkel 15.

545 Isikuandmete kaitse üldmääruse artikli 23 lõige 1.

546 *Ibid.*, artikli 23 lõige 2.

547 *Ibid.*, artikli 89 lõiked 2 ja 3.

edastatakse talle arusaadaval viisil. Andmetega tutvumise õigust on tunnustatud peale nüüdisajastatud konventsiooni nr 108 sätete ka Euroopa Inimõiguste Kohtu praktikas. Euroopa Inimõiguste Kohus on korduvalt kinnitanud, et üksikisikutel on õigus tutvuda teabega nende isikuandmete kohta ja see õigus tuleneb vajadusest austada eraelu puutumatust[548]. Teatud tingimustel võib siiski piirata õigust saada juurdepääs avalikes või eraorganisatsioonides säilitatavatele isikuandmetele[549].

ELi õiguse kohaselt on isikuandmete kaitse üldmääruse artiklis 15 selge sõnaga tunnistatud õigust tutvuda enda andmetega ning see on sätestatud ka ELi põhiõiguste harta artikli 8 lõikes 2 kui isikuandmete kaitse põhiõiguse element[550]. Üksikisiku õigus tutvuda oma isikuandmetega on üks Euroopa andmekaitseõiguse põhielemente[551].

Isikuandmete kaitse üldmääruses on sätestatud, et igal andmesubjektil on õigus tutvuda oma isikuandmetega ja saada teatavat teavet töötlemise kohta, mida peavad esitama vastutavad töötlejad[552]. Eelkõige on igal andmesubjektil õigus saada vastutavalt töötlejalt kinnitus, kas teda käsitlevaid andmeid töödeldakse või mitte, ning teavet vähemalt järgmise kohta:

- töötlemise eesmärk;
- asjaomased andmeliigid;
- vastuvõtjad või vastuvõtjate kategooriad, kellele andmed avalikustatakse;
- kavandatav isikuandmete säilitamise tähtaeg või (kui see ei ole võimalik) tähtaja määramise kriteeriumid;

548 EIK, *Gaskin vs. Ühendkuningriik*, nr 10454/83, 7. juuli 1989; EIK, *Odièvre vs. Prantsusmaa* [suurkoda], 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.

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

550 Vt ka ELK, liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel ja Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 17. juuli 2014; ELK, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) vs. Euroopa Toiduohutusamet (EFSA), Euroopa Komisjon*, 16. juuli 2015.

551 ELK, liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel ja Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 17. juuli 2014.

552 Isikuandmete kaitse üldmääruse artikli 15 lõige 1.

- teave õiguse kohta taotleda isikuandmete parandamist, kustutamist või töötlemise piiramist;
- teave õiguse kohta esitada kaebus järelevalveasutusele;
- kui isikuandmeid ei koguta andmesubjektilt, siis olemasolev teave töödeldavate andmete allika kohta;
- automaatotsuste korral andmete automaattöötlemise loogika kohta.

Vastutav töötleja peab esitama andmesubjektile töödeldavate isikuandmete koopia. Mis tahes teave tuleb edastada andmesubjektile arusaadaval kujul, mis tähendab, et vastutav töötleja peab tagama, et andmesubjekt mõistaks esitatud teavet. Näiteks tavaliselt ei piisa tehniliste lühendite ja kodeeritud terminite või akronüümide lisamisest andmetega tutvumise taotlusele, v.a kui nende tähendust on selgitatud. Automaatotsuste, sealhulgas profiilianalüüsi tegemisel tuleb selgitada automaatotsuste üldloogikat, sealhulgas kriteeriume, mille alusel andmesubjekti hinnati. Sarnased nõuded on sätestatud ka **Euroopa Nõukogu õiguses**[553].

Näide: isikuandmetega tutvumine aitab andmesubjektil kontrollida, kas andmed on õiged või mitte. Seetõttu on oluline, et andmesubjekti teavitatakse arusaadaval kujul peale töödeldavate tegelike andmete ka andmeliikidest, mille alusel isikuandmeid töödeldakse, näiteks nimi, IP-aadress, asukoha koordinaadid, krediitkaardi number jt.

Andmetega tutvumise taotlusele vastates tuleb siis, kui andmed ei ole saadud andmesubjektilt, esitada teave andmete allika kohta, kui see on olemas. Seda sätet tuleb käsitada õigluse, läbipaistvuse ja vastutuse põhimõtte kontekstis. Vastutav töötleja ei või andmeallika teavet selle varjamiseks hävitada – v.a kui kustutamine oleks toimunud vaatamata saadud juurdepääsutaotlusele – ning see peab siiski vastama tema üldistele vastutusnõuetele.

Nagu on sätestatud Euroopa Liidu Kohtu praktikas, ei või isikuandmetega tutvumise õigust tähtaegadega põhjendamatult piirata. Samuti peab andmesubjektidele tagama mõistliku võimaluse saada teavet varasemate andmetöötlustoimingute kohta.

553 Vt nüüdisajastatud konventsiooni nr 108 artikli 8 lõike 1 punkt c.

Näide: kohtuasjas *Rijkeboer*[554] paluti Euroopa Liidu Kohtul määrata, kas üksikisiku õigus saada teavet isikuandmete vastuvõtjate või vastuvõtjate kategooriate ja andmete sisu kohta võib piirduda ühe aastaga enne andmetega tutvumise taotluse esitamist.

Et leida, kas ELi õiguse alusel on selline ajapiirang lubatud, otsustas ELK tõlgendada artiklit 12 direktiivi eesmärke arvestades. Esiteks märkis ELK, et andmetega tutvumise õigust on vaja, et andmesubjekt saaks kasutada õigust nõuda, et vastutav töötleja parandab, kustutab või sulgeb andmed, või teavitab parandustest, kustutamistest või sulgemistest kolmandaid isikuid, kellele need andmed avalikustati. Tõhusat andmetega tutvumise õigust on vaja ka selleks, et andmesubjekt saaks kasutada õigust vaidlustada oma isikuandmete töötlemine või esitada kaebus ja nõuda kahju hüvitamist[555].

Kohus leidis, et andmesubjektidele antud õiguste 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."

6.1.2. Õigus andmete parandamisele

ELi õiguse ja **Euroopa Nõukogu õiguse** kohaselt on andmesubjektidel õigus nõuda oma isikuandmete parandamist. Isikuandmete õigsus on oluline, et tagada andmesubjektide andmekaitse kõrge tase[556].

Näide: kohtuasjas *Ciubotaru vs. Moldova*[557] ei saanud kaebuse esitaja muuta oma etnilist päritolu ametlikes registrikannetes moldovlasest rumeenlaseks väidetavalt põhjusel, et ta ei põhjendanud taotlust. EIK leidis, et riikidel on õigus nõuda üksikisiku etnilise identiteedi registreerimisel objektiivseid tõendeid. Kui selline taotlus põhineb ainult subjektiivsetel ja põhjendamata alustel, on ametiasutustel õigus jätta see rahuldamata. Kaebuse esitaja taotlus

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

555 Isikuandmete kaitse üldmääruse artikli 15 lõike 1 punktid c ja f, artikkel 16, artikli 17 lõige 2 ja artikkel 21 ning VIII peatükk.

556 *Ibid*., artikkel 16 ja põhjendus 65; nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt e.

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

ei põhinenud siiski ainult sellel, kuidas ta ise oma etnilist päritolu tajus; ta viitas objektiivselt kontrollitavatele seostele rumeenlaste etnilise rühmaga, näiteks keel, nimi, samastumine rühmaga jt. Samas pidi ta riigi õigusaktide alusel tõendama, et tema vanemad kuulusid rumeenlaste etnilisse rühma. Moldova ajaloo tõttu tekitas see nõue ületamatuid takistusi olukorras, kus isik soovis registreerida muud etnilist identiteeti kui see, mida olid tema vanemate kohta registreerinud Nõukogude ametiasutused. Et 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 rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Mõnel juhul piisab sellest, kui andmesubjekt lihtsalt esitab taotluse näiteks nime kirjapildi parandamiseks või aadressi või telefoninumbri muutmiseks. **ELi õiguse** ja **Euroopa Nõukogu õiguse** kohaselt tuleb ebaõiged isikuandmed parandada põhjendamatu või liigse viivituseta[558]. Kui sellised taotlused on seotud õiguslikult oluliste küsimustega, näiteks andmesubjekti õigusliku staatusega või kehtiva elukoha aadressiga, kuhu saata õigusdokumente, ei pruugi parandamistaotlus olla piisav ning vastutaval töötlejal on õigus nõuda väidetava ebaõigsuse põhjendamise tõendeid. Selliste nõudmistega ei tohi andmesubjektile määrata liigset tõendamiskoormist ning jätta nad selle kaudu ilma andmete parandamise võimalusest. Euroopa Inimõiguste Kohus on leidnud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumisi mitmel juhul, kui hageja ei saanud vaidlustada salajastes registrites hoitava teabe õigsust[559].

Näide: kohtuasjas *Cemalettin Canli vs. Türgi*[560] tuvastas Euroopa Inimõiguste Kohus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise seoses ebaõigete politseiaruannetega kriminaalmenetluses.

Kaebuse esitaja oli kahel korral kaasatud kriminaalmenetlustesse kahtlustatuna ebaseaduslikesse rühmitustesse kuulumises, ent teda ei olnud süüdi mõistetud. Kui kaebuse esitaja uuesti vahistati ja teda süüdistati veel ühes kuriteos, esitas politsei kriminaalkohtule aruande pealkirjaga „Muude

558 Isikuandmete kaitse üldmääruse artikkel 16; nüüdisajastatud konventsiooni nr 108 artikli 9 lõige 1.

559 EIK, *Rotaru vs. Rumeenia* [suurkoda], nr 28341/95, 4. mai 2000.

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

kuritegude teave", milles väideti, et kaebuse esitaja on kahe ebaseadusliku rühmituse liige. Kaebuse esitaja palus aruannet ja politsei registrikirjeid muuta, kuid tema taotlust ei rahuldatud. EIK leidis, et politseiaruandes olev teave kuulus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaldamisalasse, sest ka süstemaatiliselt kogutud ja ametiasutuste registrites säilitatav avalik teave võib kuuluda eraelu alla. Peale selle ei olnud politseiaruandes sisalduv teave koostatud õigesti ja selle esitamine kriminaalkohtule ei olnud kooskõlas riigisisese õigusega. Kohus järeldas, et rikuti artiklit 8.

Tsiviilkohtumenetlustes või riigiasutuse menetlustes saab andmesubjekt oma andmete õigsuse kontrollimiseks taotleda, et tema andmetele lisataks kirje või märge, et andmete õigsus on vaidlustatud ning ametlikku otsust ei ole veel tehtud[561]. Selle aja jooksul ei tohi vastutav töötleja jätta eriti kolmandatele isikutele muljet, et andmed on täielikud või ei kuulu muutmisele.

6.1.3. Õigus andmete kustutamisele (õigus olla unustatud)

Andmesubjektide õigus lasta oma andmed kustutada on eriti oluline andmekaitsepõhimõtete tõhusa kohaldamise, eelkõige võimalikult väheste andmete kogumise põhimõtte seisukohast (isikuandmed peavad piirduma sellega, mis on nende töötlemise otstarbe seisukohalt vajalik). Seega on õigus andmete kustutamisele sätestatud nii Euroopa Nõukogu kui ka ELi õigusaktides[562].

Näide: kohtuasjas *Segerstedt-Wiberg jt vs. Rootsi*[563] arutati juhtumit, kus kaebuse esitajaid seostati teatud liberaalsete ja kommunistlike erakondadega. Kaebuse esitajad kahtlustasid, et nende teave oli kantud kaitsepolitsei registritesse, ning taotlesid selle kustutamist. EIK leidis, et andmete säilitamisel oli õiguslik alus ja õiguspärane eesmärk. Kaebuse mõne esitaja kohta märkis EIK siiski, et andmete jätkuva säilitamisega sekkuti liiga palju nende eraellu. Näiteks ühe kaebuse esitaja puhul säilitasid ametiasutused teavet, et 1969. aastal oli ta väidetavalt õhutanud meeleavaldustel vägivaldset

561 Isikuandmete kaitse üldmääruse artikkel 18 ja põhjendus 67.

562 *Ibid.*, artikkel 17.

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

vastuhakku politseile. EIK leidis, et selle teabega seoses ei saanud olla asjakohast riigi julgeolekuga seotud huvi, eelkõige seepärast, et teave käsitles aastatetaguseid kahtlustusi. EIK järeldas, et kaebuse esitajate suhtes oli nelja isiku korral viiest rikutud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8, sest nende andmete jätkuv säilitamine ei olnud asjakohane, sest väidetavad kaebuse esitajate teod olid toimunud ammu.

Näide: kohtuasjas *Brunet vs. Prantsusmaa*[564] esitas hageja kaebuse oma isikuandmete säilitamise kohta politsei andmebaasis, mis sisaldas teavet nii süüdimõistetute, süüdistatavate kui ka kannatanute kohta. Kuigi kriminaalmenetlus taotluse esitaja vastu lõpetati, olid tema andmed andmebaasis alles. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8. Järelduse tegemisel leidis kohus, et taotlejal ei olnud võimalik lasta oma isikuandmeid andmebaasist kustutada. EIK arutas ka andmebaasi lisatud teabe olemust ja leidis, et sellega sekkuti taotleja eraelu puutumatusse, sest andmebaas sisaldas andmeid tema isikusamasuse ja isiksuse kohta. Lisaks leidis kohus, et andmete andmebaasis säilitamise tähtaeg (20 aastat) oli liiga pikk, eelkõige seetõttu, et ükski kohus ei olnud taotlejat kunagi süüdi mõistnud.

Nüüdisajastatud konventsioonis nr 108 tunnistatakse selge sõnaga, et igaühel on õigus ebaõigete, valede või ebaseaduslikult töödeldud andmete kustutamisele[565].

ELi õiguse kohaselt jõustatakse isikuandmete kaitse üldmääruse artikliga 17 andmesubjektide taotlused andmete kustutamise kohta. Õigust lasta oma isikuandmed kustutada põhjendamatu viivituseta kohaldatakse, kui

- isikuandmeid ei ole enam vaja eesmärgil, millega seoses need on kogutud või muul viisil töödeldud;
- andmesubjekt võtab töötlemiseks antud nõusoleku tagasi ja puudub muu õiguslik alus isikuandmete töötlemiseks;
- andmesubjekt vaidlustab isikuandmete töötlemise ja töötlemiseks puuduvad ülekaalukad õiguspärased põhjused;

564 EIK, *Brunet vs. Prantsusmaa*, nr 21010/10, 18. september 2014.

565 Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt e.

- isikuandmeid on töödeldud ebaseaduslikult;
- isikuandmed tuleb kustutada, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust;
- isikuandmeid koguti seoses isikuandmete kaitse üldmääruse artikli 8 kohaselt infoühiskonna teenuste pakkumisega lapsele[566].

Andmetöötluse õiguspärasuse tõendamise kohustus on vastutavatel töötlejatel, sest nad vastutavad töötlemise seaduslikkuse eest[567]. Vastutuse põhimõttest lähtudes peab vastutav töötleja suutma millal tahes tõendada, et tema andmetöötlustoimingutel on nõuetekohane õiguslik alus, ning vastasel korral tuleb töötlemine peatada[568]. Isikuandmete kaitse üldmääruses sätestatakse erandid õigusest olla unustatud, sealhulgas juhul, kui isikuandmete töötlemine on vajalik

- sõna- ja teabevabaduse õiguse kasutamiseks;
- et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õiguses sätestatud juriidilist kohustust, mis näeb ette isikuandmete töötlemise, või täita avalikes huvides olevat ülesannet või teostada vastutava töötleja avalikku võimu;
- rahvatervise valdkonnas avaliku huviga seotud põhjustel;
- avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil;
- õigusnõuete koostamiseks, esitamiseks või kaitsmiseks[569].

Euroopa Liidu Kohus on kinnitanud andmete kustutamise õiguse tähtsust andmekaitse kõrge taseme tagamisel.

566 Isikuandmete kaitse üldmääruse artikli 17 lõige 1.

567 *Ibid*.

568 *Ibid*., artikli 5 lõige 2.

569 *Ibid*., artikli 17 lõige 3.

Näide: kohtuasjas *Google Spain*[570] arutas Euroopa Liidu Kohus, kas Google pidi kustutama aegunud teabe taotleja finantsraskuste kohta oma otsingutulemuste loetelust. Muu hulgas vaidlustas Google selle, et teda peeti vastutavaks, väites, et ta ainult annab hüperlingi avaldaja veebilehele, mis majutab teavet, käsitletaval juhul ajalehe veebilehele, kus kirjutati taotleja maksejõuetusest[571]. Google väitis, et taotlus aegunud teabe veebileheküljelt kustutamiseks tuleb esitada veebilehekülje majutajale ja mitte Google'ile, mis esitab ainult lingi algsele leheküljele. Euroopa Liidu Kohus järeldas, et kui Google otsib teavet ja veebilehekülgi ning indekseerib otsingutulemuste esitamiseks sisu, muutub ta vastutavaks töötlejaks, kelle suhtes kohaldatakse ELi õigusest tulenevaid kohustusi.

ELK selgitas, et interneti otsingumootorid ja isikuandmeid sisaldavad otsingutulemused võivad koostada andmesubjekti kohta üksikasjaliku profiili[572]. Otsingumootorid teevad niisuguses tulemuste loetelus sisalduva teabe kõikjal kättesaadavaks. Selle riive potentsiaalset raskust silmas pidades tuleb tõdeda, et riivet ei saa õigustada üksnes otsingumootori haldaja majandushuviga sellise töötlemise suhtes. Tuleb püüda saavutada õiglane tasakaal eelkõige internetikasutajate teabele juurdepääsu õiguspäraste huvide ja andmesubjektide ELi põhiõiguste harta artiklitest 7 ja 8 tulenevate põhiõiguste vahel. Üha digitaalsemas ühiskonnas on nõue, et isikuandmed peavad olema õiged ja ei lähe kaugemale sellest, mis on vajalik (nt avaliku informatsiooni jaoks), väga oluline, et tagada isikute kõrgetasemeline andmekaitse. „Vastutav töötleja [peab] oma ülesannete, pädevuse ja võimaluste piires tagama andmetöötluse vastavuse [ELi õiguse] nõuetele", et kehtestatud õiguslikel

570 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punktid 55–58.

571 Google vaidlustas ELi andmekaitse-eeskirjade kohaldamise ka seetõttu, et Google Inc. on asutatud USAs ja kohtuasjas käsitletav isikuandmete töötlemine toimus samuti USAs. Teine väide ELi andmekaitse õigusaktide mittekohaldatavuse kohta oli seotud väitega, et otsingumootoreid ei saa pidada vastutavateks töötlejateks otsingutulemustes esitatud andmete suhtes, sest nad ei tea andmete sisu ja neil ei ole selle üle kontrolli. Euroopa Liidu Kohus lükkas mõlemad väited tagasi, leides, et direktiiv 95/46/EÜ oli juhtumis kohaldatav, ning jätkas tagatud õiguste ulatuse uurimist, eelkõige seoses õigusega isikuandmete kustutamisele.

572 *Ibid.*, punktid 36, 38, 80–81 ja 97.

tagatistel oleks täielik mõju[573]. See tähendab, et õigus oma isikuandmete kustutamisele, kui töötlemine on aegunud või ei ole enam vajalik, hõlmab ka seda teavet kordavaid vastutavaid töötlejaid[574].

Kaalutledes, kas Google pidi eemaldama taotlejaga seotud lingid, leidis Euroopa Liidu Kohus, et teatud tingimustel on üksikisikutel õigus nõuda isikuandmete kustutamist. Seda õigust võib kasutada, kui üksikisikuga seotud teave ei ole õige, piisav, asjakohane või on töötlemise eesmärke arvestades liigne. ELK tunnistas, et see õigus ei ole absoluutne, seda tuleb tasakaalustada teiste isikute õiguste ja huvidega, eelkõige üldsuse huviga saada teatud teavet. Iga andmete kustutamise taotlust tuleb hinnata eraldi, et tasakaalustada ühelt poolt andmesubjekti isikuandmete ja eraelu puutumatuse põhiõigusi ning teisalt kõigi internetikasutajate, sealhulgas avalikustajate õigustatud huvid. ELK esitas juhised tegurite kohta, mida tuleb sellel tasakaalustamisel arvestada. Eriti tähtis tegur on asjaomase teabe olemus. Kui teave on seotud üksikisiku eraeluga ning teabe kättesaadavuse suhtes puudub avalik huvi, on isikuandmete kaitse ja eraelu puutumatus ülimuslikud üldsuse õiguse suhtes saada teabele juurdepääs. Samas kui ilmneb, et andmesubjekt on avaliku elu tegelane või teave on selline, et selle kättesaadavus üldsusele on põhjendatud, võib üldsuse ülekaalukas huvi saada teavet õigustada sekkumist andmesubjekti põhiõigustesse seoses andmekaitse ja eraelu puutumatusega.

Pärast kohtuotsust võttis artikli 29 töörühm vastu Euroopa Liidu Kohtu otsuse rakendamise suunised[575]. Suunistes on loetelu ühistest kriteeriumidest, mida järelevalveasutused saavad kasutada üksikisikute esitatud andmete kustutamise taotlustega seotud kaebuste käsitlemisel, samuti selgitatakse järelevalveasutustele, mida õigus andmete kustutamisele hõlmab, ning juhendatakse neid õiguste tasakaalustamisel. Suunistes rõhutatakse, et iga juhtumit tuleb hinnata eraldi. Et õigus olla unustatud ei ole absoluutne, võib taotluse tulemus oleneda juhtumist. Seda illustreerib ka Euroopa Liidu Kohtu kohtupraktika pärast Google'i kohtuasja.

573 *Ibid*., punktid 81–83.

574 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punkt 88. Vt ka artikli 29 töörühm (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brüssel, 26. november 2014, ja Euroopa Nõukogu ministrite komitee (2012), *Recommendation CM/Rec 2012(3) of the Committee of Ministers to member states on the protection of human rights with regard to search engines*, 4. aprill 2012.

575 Artikli 29 töörühm (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brüssel, 26. november 2014.

Näide: kohtuasjas *Camera di Commercio di Lecce vs. Manni*[576] pidi Euroopa Liidu Kohus uurima, kas üksikisikul on õigus lasta kustutada oma isikuandmed, mis on avaldatud avalikus äriühingute registris, kui tema äriühing on lõpetanud tegevuse. Hr Manni palus Lecce kaubanduskojal kustutada registrist tema isikuandmed, sest oli avastanud, et võimalikud kliendid võivad registrit vaadata ja näha, et ta on olnud varem sellise ettevõtte juhataja, mis oli läinud rohkem kui kümme aastat tagasi pankrotti. Kaebuse esitaja leidis, et see teave peletaks võimalikke kliente.

Tasakaalustades hr Manni õigust isikuandmete kaitsele üldsuse huviga saada teavet, uuris Euroopa Liidu Kohus kõigepealt avaliku registri otstarvet. Kohus osutas, et avalikustamine oli sätestatud seaduses ja eelkõige ELi direktiivis, mille eesmärk on lihtsustada äriühinguid käsitleva teabe kättesaadavust kolmandatele isikutele. Seega peaks kolmandatel isikutel olema juurdepääs ja võimalus tutvuda äriühingu põhidokumentide sisuga ja muu äriühingut käsitleva teabega, „eelkõige andmetega isikute kohta, kellel on õigus äriühingut esindada". Ka oli avalikustamise eesmärk tagada õiguskindlus, arvestades liikmesriikidevahelise kaubanduse intensiivistumist, tagades, et kolmandatel isikutel on juurdepääs kogu asjakohasele teabele äriühingute kohta kogu ELis.

ELK märkis ka, et ka pärast aja möödumist ja äriühingu tegevuse lõpetamist kehtivad äriühinguga seotud õigused ja juriidilised kohustused sageli edasi. Lõpetamisega seotud vaidlused võivad olla pikad ning äriühingu, selle juhtide ja likvideerijatega seotud küsimused võivad tekkida veel aastaid pärast seda, kui äriühing on tegevuse lõpetanud. ELK leidis, et kõiki võimalikke stsenaariume ning igas liikmesriigis sätestatud aegumistähtaegade erinevusi arvestades „näib praeguses olukorras võimatu määrata kindlaks äriühingu lõpetamisest alates ühtset tähtaega, mille möödumisel ei ole nende olemasolu registris ja nende avalikustamine enam vajalik". Avalikustamise õiguspärase eesmärgi ja raskuste tõttu tähtaja määramisel, mille möödumise järel võib isikuandmed registrist kustutada, ilma et see kahjustaks kolmandate isikute huve, leidis Euroopa Liidu Kohus, et ELi andmekaitse-eeskirjad ei taga õigust isikuandmete kustutamisele isikutele, kes on samasuguses olukorras nagu hr Manni.

576 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 9. märts 2017.

Kui vastutav töötleja on teinud isikuandmed avalikuks ja temalt nõutakse teabe kustutamist, on vastutav töötleja kohustatud võtma „mõistlikke“ meetmeid, et teatada andmesubjekti taotlus andmed kustutada teistele vastutavatele töötlejatele, kes töötlevad samu andmeid. Vastutava töötleja tegevuses tuleb arvestada olemasolevaid tehnoloogiaid ja rakenduskulusid[577].

6.1.4. Õigus isikuandmete töötlemise piiramisele

Isikuandmete kaitse üldmääruse artikliga 18 antakse andmesubjektidele õigus panna vastutavale töötlejale nende isikuandmete töötlemisel ajutine piirang. Andmesubjektid võivad nõuda, et vastutav töötleja piiraks töötlemist, kui

- vaidlustatakse isikuandmete õigsus;
- isikuandmete töötlemine on ebaseaduslik ja andmesubjekt taotleb isikuandmete kustutamise asemel nende kasutamise piiramist;
- andmeid tuleb säilitada õigusnõuete esitamiseks või kaitsmiseks;
- oodatakse otsust, kas vastutava töötleja õigustatud huvid on andmesubjekti huvide suhtes ülimuslikud[578].

Meetodid, millega vastutav töötleja saab isikuandmete töötlemist piirata, võivad olla näiteks valitud andmete ajutine kandmine teise töötlemissüsteemi, mis muudab andmed kasutajatele kättesaamatuks, või isikuandmete ajutine eemaldamine[579]. Vastutav töötleja peab andmesubjekti enne töötlemispiirangu tühistamist sellest teavitama[580].

Kohustus teatada isikuandmete parandamisest, kustutamisest või töötlemise piiramisest

Vastutav töötleja peab edastama teabe isikuandmete parandamise või kustutamise või töötlemise piiramise kohta igale vastuvõtjale, kellele vastutav töötleja on isikuandmed avaldanud, v.a kui see on võimatu või nõuab ebaproportsionaalseid

577 Isikuandmete kaitse üldmääruse artikli 17 lõige 2 ja põhjendus 66.

578 *Ibid*., artikli 18 lõige 1.

579 *Ibid*., põhjendus 67.

580 *Ibid*., artikli 18 lõige 3.

jõupingutusi[581]. Vastutav töötleja teavitab andmesubjekti nendest vastuvõtjatest andmesubjekti taotluse korral[582].

6.1.5. Andmete ülekandmise õigus

Isikuandmete kaitse üldmääruse kohaselt on andmesubjektidel õigus andmete ülekandmisele olukordades, kus isikuandmeid, mille nad on edastanud vastutavale töötlejale, töödeldakse automaatvahenditega nõusoleku alusel või kus isikuandmete töötlemine on vajalik lepingu täitmiseks ja toimub automaatvahenditega. See tähendab, et andmete ülekandmise õigus ei kehti olukordades, kus isikuandmete töötlemine põhineb muul õiguslikul alusel kui nõusolek või leping[583].

Kui andmete ülekandmise õigus on kohaldatav ja tehniliselt teostatav, on andmesubjektidel õigus nõuda, et nende andmed edastatakse otse ühelt vastutavalt töötlejalt teisele[584]. Selle võimaldamiseks tuleb vastutaval töötlejal välja töötada koostalitlevad vormingud, mis võimaldavad andmesubjektidele andmete ülekandmist[585]. Isikuandmete kaitse üldmääruses täpsustatakse, et koostalitlusvõime toetamiseks peavad need vormingud olema struktureeritud, üldkasutatavad ja masinloetavad[586]. Laias tähenduses võib koostalitlusvõimet määratleda kui infosüsteemide suutlikkust andmeid vahetada ja võimaldada teabe jagamist[587]. Kuigi kasutatavate vormingute eesmärk on koostalitlusvõime saavutamine, puuduvad isikuandmete kaitse üldmääruses täpsed soovitused kasutatavate erivormingute kohta: vormingud võivad oleneda valdkonnast[588].

Artikli 29 töörühma suuniste kohaselt toetab andmete ülekandmine „kasutajate valikuvõimalusi, kasutajate kontrolli ja kasutajate mõjuvõimu suurendamist“, mille eesmärk on anda andmesubjektidele kontroll nende isikuandmete üle[589]. Suunistes selgitatakse andmete ülekandmise põhielemente, näiteks järgmisi:

581 *Ibid.*, artikkel 19.

582 *Ibid.*

583 *Ibid.*, põhjendus 68 ja artikli 20 lõige 1.

584 *Ibid.*, artikli 20 lõige 2.

585 *Ibid.*, põhjendus 68 ja artikli 20 lõige 1.

586 *Ibid.*, põhjendus 68.

587 Euroopa Komisjon, teatis „Piirivalve ja julgeoleku tugevamad ja arukamad infosüsteemid“, COM(2016) 205 final, 2. aprill 2016.

588 Artikli 29 töörühm (2016), *Guidelines on the right to data portability*, WP 242, 13. detsember 2016, läbi vaadatud 5. aprillil 2017, lk 13.

589 *Ibid.*

- andmesubjektide õigus saada oma isikuandmeid, mida vastutav töötleja on töödelnud, struktureeritud, üldkasutatavas ning masinloetavas ja koostalitlevas vormingus;

- õigus edastada need andmed takistusteta ühelt vastutavalt töötlejalt teisele, kui see on tehniliselt teostatav;

- vastutuse kord – kui vastutav töötleja vastab andmete ülekandmise taotlusele, tegutseb ta andmesubjekti juhiste kohaselt, mis tähendab, et ta ei vastuta selle eest, kas vastuvõtja järgib andmekaitseõigust, arvestades, et andmesubjekt otsustab, kellele andmed üle kantakse;

- andmete ülekandmise õiguse kasutamine ei piira muid õigusi, nagu ka kõigi muude isikuandmete kaitse üldmääruse kohaste õiguste korral.

6.1.6. Õigus esitada vastuväiteid

Andmesubjektid võivad tugineda oma õigusele esitada vastuväiteid otseturunduse eesmärgil töödeldavate andmete töötlemisele ja isikuandmete töötlemisele enda eriolukorrast lähtudes. Õigust esitada vastuväiteid saab kasutada automatiseeritud vahendite teel.

Õigus esitada vastuväiteid andmesubjektide eriolukorrast lähtudes

Andmesubjektidel ei ole üldist õigust esitada vastuväiteid oma andmete töötlemise vastu[590]. Isikuandmete kaitse üldmääruse artikli 21 lõikes 1 antakse andmesubjektile õigus oma eriolukorrast lähtudes esitada vastuväiteid, kui töötlemise õiguslik alus on avalikes huvides oleva ülesande täitmine vastutava töötleja poolt või kui töötlemine põhineb vastutava töötleja õigustatud huvidel[591]. Õigus esitada vastuväiteid kehtib profiilianalüüsi kohta. Sarnast õigust tunnustatakse nüüdisajastatud konventsioonis nr 108[592].

Õiguse puhul esitada vastuväiteid andmesubjekti eriolukorrast lähtudes püütakse tasakaalustada andmesubjekti andmekaitseõigused ja teiste isikute seaduslikud

590 Vt ka EIK, *M.S. vs. Rootsi*, nr 20837/92, 27. august 1997 (juhtum, kus meditsiiniandmeid edastati nõusolekuta või vastuväite esitamise võimaluseta); EIK, *Leander vs. Rootsi*, nr 9248/81, 26. märts 1987; EIK, *Mosley vs. Ühendkuningriik*, nr 48009/08, 10. mai 2011.

591 Isikuandmete kaitse üldmääruse põhjendus 69; artikli 6 lõike 1 punktid e ja f.

592 Nüüdisajastatud konventsiooni nr 108 artikli 9 artikli 1 punkt d; profiilianalüüsi soovituse punkt 5.3.

õigused töödelda andmesubjekti isikuandmeid. Euroopa Liidu Kohus on siiski selgitanud, et andmesubjekti õigused on vastutava töötleja majandushuvide suhtes „üldjuhul" ülimuslikud, olenevalt „teabe laadist ja delikaatsusest andmesubjektide eraelu suhtes ning üldsuse huvist seda teavet saada"[593]. Isikuandmete kaitse üldmääruse kohaselt on tõendamiskohustus vastutavatel töötlejatel, kes peavad kaalukalt põhjendama, miks töötlemist jätkatakse[594]. Sarnaselt selgitatakse nüüdisajastatud konventsiooni nr 108 seletuskirjas, et andmete töötlemise õiguspäraseid aluseid (mis võivad olla ülimuslikud andmesubjektide õiguse suhtes esitada vastuväiteid) tuleb tõendada iga kord eraldi[595].

Näide: kohtuasjas *Manni*[596] leidis Euroopa Liidu Kohus, et isikuandmete äriühinguregistris avalikustamise õiguspärase eesmärgi, eelkõige kolmandate isikute huvide kaitse ja õiguskindluse tagamise vajaduse tõttu ei olnud hr Mannil põhimõtteliselt õigust nõuda oma isikuandmete kustutamist äriühingute registrist. Samas tunnistas kohus töötlemise vaidlustamise õiguse olemasolu, märkides, et „ei saa [...] välistada, et võivad esineda eriolukorrad, kus õigustatud ja veenvad põhjused, mis on seotud andmesubjekti konkreetse juhtumiga, õigustavad erandkorras seda, et pärast piisavalt pika aja möödumist [...] on äriühingute registrisse kantud seda isikut puudutavate isikuandmetega tutvumine piiratud kolmandate isikutega, kellel on erihuvi nendega tutvuda".

ELK leidis, et iga juhtumi hindamine on riigisiseste kohtute ülesanne, arvestades isiku kõiki asjakohaseid asjaolusid ja seda, kas on olemas õiguspärased ja ülekaalukad põhjused, mis võivad erandkorras õigustada kolmandate isikute piiratud juurdepääsu äriühingute registris olevatele isikuandmetele. Kohus selgitas siiski, et hr Manni juhtumi korral ei saa ainuüksi asjaolu, et tema isikuandmete avaldamine registris väidetavalt mõjutas tema kliente, lugeda selliseks õigustatud ja ülekaalukaks põhjuseks. Hr Manni võimalikel klientidel on õigustatud huvi saada teavet tema endise ettevõtte pankroti kohta.

593 ELK, C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014, punkt 81.

594 Vt ka nüüdisajastatud konventsiooni nr 108 artikli 98 lõike 1 punkt d, kus märgitakse, et andmesubjekt võib esitada vastuväite oma andmete töötlemisele, v.a kui vastutav töötleja tõendab, et andmeid töödeldakse õiguspärasel põhjusel, mis on andmesubjekti huvide või õiguste ja põhivabaduste suhtes ülimuslik.

595 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 78.

596 ELK, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 9. märts 2017, punktid 47 ja 60.

Vastuväite rahuldamise tulemusel ei tohi vastutav töötleja asjaomaseid andmeid enam töödelda. Andmesubjekti andmetega enne vaidlustamist tehtud töötlemistoimingud jäävad siiski õiguspäraseks.

Õigus esitada vastuväiteid andmete otseturunduse eesmärgil töötlemise kohta

Isikuandmete kaitse üldmääruse artikli 21 lõige 2 sätestab eriõiguse esitada vastuväiteid isikuandmete kasutamisele otseturunduse eesmärgil, täpsustades e-privaatsuse direktiivi artiklit 13. See õigus on sätestatud ka nüüdisajastatud konventsioonis nr 108 ja Euroopa Nõukogu soovituses otseturunduse kohta[597]. Nüüdisajastatud konventsiooni nr 108 seletuskirjas selgitatakse, et otseturunduse eesmärgil andmete töötlemisele vastuväidete esitamine peab lõppema kõnealuste isikuandmete tingimusteta kustutamise või eemaldamisega[598].

Andmesubjektil on õigus esitada millal tahes ja tasuta vastuväiteid oma isikuandmete otseturunduse eesmärgil kasutamise kohta. Andmesubjekte tuleb sellest õigusest selgelt teavitada, tehes seda mis tahes muust teabest eraldi.

Õigus esitada vastuväiteid automatiseeritud vahendite teel

Kui isikuandmeid kasutatakse ja töödeldakse infoühiskonna teenuste jaoks, võib andmesubjekt kasutada õigust esitada vastuväiteid enda isikuandmete töötlemisele automatiseeritud vahendite teel.

Infoühiskonna teenused on määratletud kui teenused, mida tavaliselt osutatakse tasu eest, eemalt elektrooniliselt ja teenusesaaja isikliku taotluse alusel[599].

Infoühiskonna teenuseid pakkuvate vastutavate töötlejate käsutuses peavad olema asjakohased tehnilised korraldused ja menetlused tagamaks, et õigust esitada vastuväiteid automaatvahenditega saab tõhusalt kasutada[600]. Näiteks võib see hõlmata

597 Euroopa Nõukogu ministrite komitee (1985), *Recommendation Rec(85)20 to member states on the protection of personal data used for the purposes of direct marketing*, 25. oktoober 1985, artikli 4 lõige 1.

598 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 79.

599 Direktiiv 98/34/EÜ (millega nähakse ette tehnilistest standarditest ja eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord), mida on muudetud direktiiviga 98/48/EÜ, artikli 1 punkt 2.

600 Isikuandmete kaitse üldmääruse artikli 21 lõige 5.

küpsiste blokeerimist veebilehtedel või internetilehekülgede sirvimise jälgimise väljalülitamist.

Õigus esitada vastuväiteid töötlemise kohta teadus- või ajaloouuringute või statistilistel eesmärgil

ELi õiguse kohaselt tuleb teadusuuringuid tõlgendada laialt, sealhulgas näiteks tehnoloogia arendamine ja tutvustamine, alusuuringud, rakendusuuringud ja erasektori rahastatavad teadusuuringud[601]. Ajaloouuringud hõlmavad ka genealoogiauuringuid, kusjuures määrust ei kohaldata surnute suhtes[602]. Statistiline eesmärk tähendab kõiki isikuandmete kogumise ja töötlemise toiminguid, mida on vaja statistikauuringuteks või statistika koostamiseks[603]. Ka isikuandmete teadusuuringute eesmärgil töötlemise vaidlustamisel on õiguslikuks aluseks andmesubjekti eriolukord[604]. Ainus erand on vajadus töödelda andmeid avalikes huvides olevate ülesannete täitmiseks. Samas ei kohaldata õigust andmete kustutamisele siis, kui töötlemine on vajalik (avaliku huvi põhjustel või mitte) teadus- või ajaloouuringute või statistika eesmärgil[605].

Isikuandmete kaitse üldmäärus tasakaalustab teadus-, statistiliste või ajaloouuringute nõudeid ning andmesubjektide õigusi artiklis 89 sätestatud konkreetsete kaitsemeetmete ja eranditega. Seega võidakse liidu või liikmesriigi õigusaktides sätestada erandid õigusest esitada vastuväiteid, kui see õigus muudab teadusuuringu eesmärkide saavutamise tõenäoliselt võimatuks või kahjustab neid tugevalt ning kui sellised erandid on nende eesmärkide saavutamiseks vajalikud.

Euroopa Nõukogu õiguses on nüüdisajastatud konventsiooni nr 108 artikli 9 lõikes 2 sätestatud, et andmesubjektide õiguste, sealhulgas vaidlustamise õiguse piirangud võidakse seaduses sätestada andmete töötlemisel arhiveerimise eesmärgil avalikes huvides, teadus- või ajaloouuringute või statistilistel eesmärgil, kui puudub andmesubjektide õiguste ja põhivabaduste rikkumise äratuntav risk.

Samas tunnistatakse seletuskirjas (punkt 41) ka, et andmesubjektidel peab olema võimalus anda nõusolek ainult teatud uurimisvaldkondadele või uurimisprojektide

601 *Ibid.*, põhjendus 159.

602 *Ibid.*, põhjendus 160.

603 *Ibid.*, põhjendus 162.

604 *Ibid.*, artikli 21 lõige 6.

605 *Ibid.*, artikli 17 lõike 3 punkt d.

osadele ulatuses, mida võimaldab kavandatud eesmärk, ja esitada vastuväiteid, kui nad leiavad, et töötlemine mõjutab liiga nende õigusi ja vabadusi, ilma et selleks oleks õiguspärast põhjust.

Teisisõnu peetakse sellist töötlemist juba eelnevalt sobivaks, kui on olemas muud kaitsemeetmed ja toimingud välistavad põhimõtteliselt igasuguse sellise teabe kasutamise, mis on saadud konkreetset isikut puudutavate otsuste või meetmete jaoks.

6.1.7. Automatiseeritud töötlusel põhinevate üksikotsuste tegemine, sealhulgas profiilianalüüs

Automaatotsused tehakse töödeldud isikuandmete alusel täiesti automaatselt ja ilma inimese sekkumiseta. **ELi õiguses** ei tohi andmesubjektide suhtes kohaldada automaatotsuseid, millel on õiguslik mõju või sarnane märkimisväärne mõju. Olukorras, kus sellised otsused võivad oluliselt mõjutada isikute elu, sest on seotud näiteks krediidivõimelisuse, e-värbamise, töötulemuste, käitumise või usaldusväärsuse analüüsiga, on negatiivsete tagajärgede vältimiseks vaja konkreetseid kaitsemeetmeid. Automaatotsuste tegemine hõlmab isikuandmete mis tahes automaattöötlemises seisnevat profiilianalüüsi, millega hinnatakse „füüsilise isikuga seotud isiklikke aspekte, mille eesmärk on eelkõige selliste aspektide analüüsimine ja prognoosimine, mis on seotud töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega“[606].

> Näide: tulevase kliendi krediidivõimelisuse kiireks hindamiseks koguvad krediidiinfoagentuurid teatud andmeid, näiteks andmeid, kuidas klient on hallanud oma laenu- ja teenuse-/tarbimiskontosid, kliendi eelmisi aadresse ning avalikest allikatest saadud teavet, näiteks valijate nimekirja, avalikke dokumente (sh kohtulahendeid) või pankroti- ja maksejõuetuse andmeid. Need isikuandmed sisestatakse seejärel hindamisalgoritmi, millega arvutatakse üldväärtus, mis näitab võimaliku kliendi krediidivõimelisust.

Artikli 29 töörühma väitel on õigus, et isiku suhtes ei tehta otsuseid, mis võivad põhjustada andmesubjektile õiguslikke tagajärgi või mis teda oluliselt mõjutavad,

606 *Ibid.*, põhjendus 71, artikli 4 lõige 4 ja artikkel 22.

üksnes andmete automaattöötlemise põhjal, samaväärne üldise keeluga ega eelda, et andmesubjekt peaks sellist otsust ise eelnevalt vaidlustama[607].

Isikuandmete kaitse üldmääruse kohaselt võib õiguslike tagajärgedega automaatotsuste või üksikisikuid oluliselt mõjutavate otsuste tegemine olla siiski vastuvõetav, kui see on vajalik lepingu sõlmimiseks või vastutava töötleja ja andmesubjekti vahelise lepingu täitmiseks või kui andmesubjekt on andnud selgesõnalise nõusoleku. Automaatotsuste tegemine on vastuvõetav ka siis, kui see on seadusega lubatud ja kui andmesubjekti õigused, vabadused ja õigustatud huvid on nõuetekohaselt kaitstud[608].

Samuti sätestatakse isikuandmete kaitse üldmääruses, et vastutava töötleja kohustuste hulka seoses teabega, mis tuleb isikuandmete kogumisel esitada, kuulub kohustus teavitada andmesubjekte automaatotsuste tegemisest, sealhulgas profiilianalüüsist[609]. Õigus tutvuda andmetöötleja töödeldavate isikuandmetega ei muutu[610]. Teave peab peale profiilianalüüsi tegemise mainimise sisaldama ka sisulist teavet, mis loogikat profiilianalüüsis kasutatakse ja mis on töötlemise prognoositavad tagajärjed isikutele[611]. Näiteks peab tervisekindlustusettevõtja, kes teeb taotluste kohta automaatotsuseid, andma andmesubjektidele üldteavet, kuidas algoritm toimib ja mis tegurite järgi algoritm arvutab kindlustusmakseid. Samamoodi võivad andmesubjektid andmetega tutvumise õiguse kasutamisel taotleda vastutavalt töötlejalt teavet automaatotsuste tegemise kohta, samuti sisulist teavet kasutatava loogika kohta[612].

Andmesubjektidele antava teabe eesmärk on tagada läbipaistvus ja võimaldada neil anda teavitatud nõusolek, kui see on asjakohane, või nõuda inimese sekkumist. Vastutav töötleja on kohustatud võtma sobivaid meetmeid andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitseks. See hõlmab vähemalt õigust nõuda vastutavalt töötlejalt inimsekkumist ja andmesubjekti võimalust väljendada oma seisukohta ning vaidlustada otsus, mis põhineb tema isikuandmete automaattöötlemisel[613].

607 Artikli 29 töörühm (2017), *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3. oktoober 2017, lk 15.

608 Isikuandmete kaitse üldmääruse artikli 22 lõige 2.

609 *Ibid.*, artikkel 12.

610 *Ibid.*, artikkel 15.

611 *Ibid.*, artikli 13 lõike 2 punkt f.

612 *Ibid.*, artikli 15 lõike 1 punkt h.

613 *Ibid.*, artikli 22 lõige 3.

Artikli 29 töörühm on esitanud täiendavad suunised automaatotsuste tegemise kohta isikuandmete kaitse üldmääruse raames[614].

Euroopa Nõukogu õiguse kohaselt on isikutel õigus, et nende kohta ei tehta otsust, mis mõjutab neid oluliselt ja mis põhineb üksnes andmete automatiseeritud töötlemisel, ilma nende seisukohti arvestamata[615]. Nõue arvestada andmesubjekti seisukohtadega, kui otsused põhinevad üksnes andmete automaattöötlemisel, tähendab, et andmesubjektil on õigus selliseid otsuseid vaidlustada ning tal peab olema võimalus vaidlustada vastutava töötleja kasutatavate isikuandmete mis tahes ebaõigsusi, ning vaidlustada küsimus, kas tema suhtes kohaldatud profiilianalüüs on asjakohane[616]. Üksikisik ei saa seda õigust siiski kasutada, kui automaatotsus on lubatud seadusega, mida kohaldatakse vastutava töötleja suhtes ja milles on sätestatud ka andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitse asjakohased meetmed. Lisaks on andmesubjektidel õigus saada taotluse korral teavet andmetöötluse aluseks olevate põhjenduste kohta[617]. Nüüdisajastatud konventsiooni nr 108 seletuskirjas on krediidihindamise näide. Üksikisikutel peab olema õigus saada teavet peale positiivse või negatiivse hindamisotsuse kohta ka nende isikuandmete töötlemise aluseks olnud *loogika* kohta, mille tulemusel otsus tehti. Nende elementide mõistmine aitab tõhusalt kasutada muid olulisi kaitsemeetmeid, näiteks õigust esitada vastuväiteid ja õigust esitada kaebus pädevale asutusele[618].

Profiilianalüüsi soovitus ei ole õiguslikult siduv, kuid selles täpsustatakse isikuandmete kogumise ja töötlemise tingimusi profiilianalüüsi kontekstis[619]. Soovituses on sätted vajaduse kohta tagada, et töötlemine profiilianalüüsi kontekstis peab olema õiglane, seaduslik ja proportsionaalne ning toimuma kindlaksmääratud ja õiguspärastel eesmärkidel. Selles on ka sätted teabe kohta, mida vastutavad töötlejad peavad andma andmesubjektidele. Soovituses käsitletakse samuti andmekvaliteedi põhimõtet, mille kohaselt peavad vastutavad töötlejad võtma meetmeid andmete ebaõigsust põhjustavate tegurite parandamiseks, profiilianalüüsi riskide või vigade

614 Artikli 29 töörühm (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3. oktoober 2017.

615 Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt a.

616 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 75.

617 Nüüdisajastatud konventsiooni nr 108 artikli 9 lõike 1 punkt c.

618 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 77.

619 Euroopa Nõukogu ministrite komitee (2010), *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23. november 2010, artikli 5 lõige 5.

piiramiseks ning kasutatavate andmete ja algoritmide kvaliteedi regulaarseks hindamiseks.

6.2. Õiguskaitsevahendid, vastutus, karistused ja hüvitamine

Põhipunktid

- Nüüdisajastatud konventsiooni nr 108 kohaselt tuleb konventsiooniosaliste õigusaktidega ette näha asjakohased õiguskaitsevahendid ja karistused juhtudeks, kui rikutakse õigust isikuandmete kaitsele.
- ELis on isikuandmete kaitse üldmääruses sätestatud õiguskaitsevahendid andmesubjektidele nende õiguste rikkumise korral ning karistused vastutavatele töötlejatele ja volitatud töötlejatele, kes ei täida määruse sätteid. Määruses on sätestatud ka õigus hüvitisele ja vastutus.
    - Andmesubjektidel on õigus esitada järelevalveasutusele kaebus määruse väidetavate rikkumiste kohta ning õigus tõhusale õiguskaitsevahendile ja hüvitisele.
    - Tõhusa õiguskaitsevahendi õiguse kasutamisel võivad üksikisikuid esindada andmekaitse valdkonnas tegutsevad mittetulundusühingud.
    - Vastutav või volitatud töötleja vastutab rikkumise tagajärjel tekkinud materiaalse ja immateriaalse kahju eest.
    - Järelevalveasutustel on õigus määrata määruse rikkumise eest haldustrahve summas kuni 20 000 000 eurot või ettevõtja korral 4% kogu tema ülemaailmsest aastakäibest – olenevalt sellest, kumb on suurem.
- Andmesubjektid võivad andmekaitseõiguse rikkumiste korral viimase abinõuna ja teatud tingimustel pöörduda Euroopa Inimõiguste Kohtu poole.
- Igal füüsilisel või juriidilisel isikul on aluslepingutes sätestatud tingimustel õigus esitada Euroopa Liidu Kohtule kaebus Euroopa Andmekaitsenõukogu mis tahes otsuse tühistamise kohta.

Euroopas ei piisa isikuandmete tagamiseks õigusaktide vastuvõtmisest. Euroopa andmekaitse-eeskirjade toimimiseks on vaja luua mehhanismid, mis võimaldavad üksikisikutel võtta meetmeid oma õiguste rikkumiste vastu ja taotleda kahju hüvitamist. Oluline on ka, et järelevalveasutustel oleks õigus määrata tõhusaid, hoiatavaid ja rikkumisega proportsionaalseid karistusi.

Andmekaitseõigusest tulenevaid õigusi saab kasutada isik, kelle õigused on ohus (andmesubjekt). Samas võivad andmesubjekte nende õiguste kasutamisel esindada ka teised isikud, kes vastavad riigi õigusaktide alusel teatud nõuetele. Mitme riigisisese õigusakti kohaselt peavad lapsi ja vaimupuudega isikuid esindama nende eestkostjad[620]. ELi andmekaitseõiguse kohaselt võivad järelevalveasutuse või kohtu poole pöördumisel esindada andmesubjekti ka ühendused, kelle õiguspärane eesmärk on edendada andmekaitseõigusi[621].

6.2.1. Õigus esitada järelevalveasutusele kaebus

Nii **Euroopa Nõukogu** kui ka **ELi õiguse** kohaselt on üksikisikutel õigus esitada taotlusi ja kaebusi pädevale järelevalveasutusele, kui nad leiavad, et nende isikuandmeid ei ole töödeldud kooskõlas õigusaktidega.

Nüüdisajastatud konventsioonis nr 108 tunnustatakse andmesubjektide õigust saada järelevalveasutuselt abi konventsiooniga antud õiguste teostamisel, olenemata kodakondsusest või elukohast[622]. Abitaotluse võib tagasi lükata ainult erandlikel asjaoludel ning andmesubjektid ei pea kandma abistamiskulusid ega maksma sellega seotud tasusid[623].

Sarnased sätted leiduvad ka ELi õigussüsteemis. Isikuandmete kaitse üldmääruses nõutakse, et järelevalveasutused võtaksid meetmeid kaebuste esitamise lihtsustamiseks, koostades näiteks elektroonilise kaebusvormi[624]. Andmesubjekt võib esitada kaebuse järelevalveasutusele liikmesriigis, kus on tema alaline elukoht, töökoht või väidetava rikkumise toimumiskoht[625]. Kaebusi tuleb uurida ja järelevalveasutus peab teavitama asjaomast isikut kaebuse menetlemise tulemusest[626].

620 FRA (2015), *Lapse õigusi käsitleva Euroopa õiguse käsiraamat*, Luxembourg, Euroopa Liidu Väljaannete Talitus; FRA (2013), *Legal capacity of persons with intellectual disabilities and persons with mental health problems*, Luxembourg, Euroopa Liidu Väljaannete Talitus.

621 Isikuandmete kaitse üldmääruse artikkel 80.

622 Nüüdisajastatud konventsiooni nr 108 artikkel 18.

623 *Ibid*., artiklid 16–17.

624 Isikuandmete kaitse üldmääruse artikli 57 lõige 2.

625 *Ibid*., artikli 77 lõige 1

626 *Ibid*., artikli 77 lõige 2.

ELi institutsioonide või asutuste tehtud võimalikest rikkumistest võib teatada Euroopa Andmekaitseinspektorile[627]. Kui ta ei ole kuue kuu jooksul vastanud, tähendab see, et kaebus on tagasi lükatud. Euroopa Andmekaitseinspektori otsuste peale saab esitada kaebusi Euroopa Liidu Kohtule määruse (EÜ) nr 45/2001 raames, millega pannakse ELi institutsioonidele ja asutustele andmekaitse-eeskirjade järgimise kohustus.

Tagatud peab olema võimalus kaevata riikliku järelevalveasutuse otsus kohtusse. See võimalus peab olema nii andmesubjektidel kui ka vastutavatel ja volitatud töötlejatel, kes on osalenud järelevalveasutuse algatatud menetluses.

Näide: 2017. aasta septembris trahvis Hispaania andmekaitseamet Facebooki mitme andmekaitse-eeskirja rikkumise eest. Järelevalveasutus kritiseeris suhtlusvõrgustikku isikuandmete, sealhulgas eriliiki isikuandmete kogumise, säilitamise ja töötlemise pärast reklaami eesmärgil ja ilma andmesubjekti nõusolekuta. Otsus põhines järelevalveasutuse omal algatusel tehtud uurimisel.

6.2.2. Õigus tõhusale õiguskaitsevahendile

Lisaks õigusele esitada järelevalveasutusele kaebus peab isikutel olema õigus tõhusale õiguskaitsevahendile ja hagi esitamisele kohtusse. Õigus õiguskaitsevahendile on Euroopa õigustraditsioonis hästi sätestatud ning seda tunnustatakse põhiõigusena nii ELi põhiõiguste harta artikli 47 kui ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 13 alusel[628].

ELi õiguse kohaselt on oluline, et andmesubjektidele oleks tagatud tõhusad õiguskaitsevahendid nende õiguste rikkumise korral, mis ilmneb selgesti nii isikuandmete kaitse üldmääruse sätetest (kus kehtestatakse õigus tõhusale õiguskaitsevahendile järelevalveasutuste, vastutavate töötlejate või volitatud töötlejate vastu) kui ka Euroopa Liidu Kohtu kohtupraktikast.

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

628 Vt näiteks EIK, *Karabeyoğlu vs. Türgi*, nr 30083/10, 7. juuni 2016; EIK, *Mustafa Sezgin Tanrıkulu vs. Türgi*, nr 27473/06, 18. juuli 2017.

Näide: kohtuasjas *Schrems*[629] tunnistas Euroopa Liidu Kohus kehtetuks programmi Safe Harbor kaitse piisavuse otsuse. Nimetatud otsusega lubati andmete rahvusvahelist edastamist EList USA organisatsioonidele, kes on end ise sertifitseerinud programmi Safe Harbor raames. ELK leidis, et programmil Safe Harbor on mitu puudust, mis ohustavad ELi kodanike põhiõigusi eraelu puutumatuse kaitsele, isikuandmete kaitsele ja õigust tõhusale õiguskaitsevahendile.

Seoses eraelu puutumatuse ja andmekaitseõiguste rikkumisega rõhutas Euroopa Liidu Kohus, et USA õigusaktidega antakse teatud ametiasutustele juurdepääs liikmesriikidelt USA-le edastatud isikuandmetele ja lubatakse neil neid töödelda viisil, mis on vastuolus andmete edastamise esialgse eesmärgiga ja ületab riigi julgeoleku kaitseks rangelt vajalikku ja proportsionaalset. Tõhusa õiguskaitsevahendi õiguse kohta märkis kohus, et andmesubjektidel ei olnud haldus- ega kohtulikke õiguskaitsevahendeid, et võimaldada neil asjakohasel juhul tutvuda enda isikuandmetega, neid parandada ega kustutada. ELK leidis, et õigusakt, milles ei ole andmesubjektile ette nähtud ühtki võimalust kasutada õiguskaitsevahendeid, et oma isikuandmetega tutvuda või lasta neid parandada või kustutada, „ei järgi [...] harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu". Kohus toonitas, et õiguseeskirjade järgimist tagava õiguskaitsevahendi olemasolu tuleneb õigusriigi põhimõttest.

Üksikisikud, vastutavad või volitatud töötlejad, kes soovivad vaidlustada järelevalveasutuse õiguslikult siduva otsuse, võivad esitada kohtule hagi[630]. Mõistet „otsus" tuleb tõlgendada laialt, hõlmates järelevalveasutuste uurimis-, karistus- ja loaandmise volitusi, samuti kaebuste rahuldamata jätmise või tagasilükkamise otsuseid. Kohtule esitatava hagi esemeks ei saa siiski olla õiguslikult mittesiduvad meetmed, näiteks järelevalveasutuse arvamused või nõuanded[631]. Hagi tuleb esitada selle liikmesriigi kohtutele, kus asjaomane järelevalveasutus on asutatud[632].

Kui vastutav või volitatud töötleja rikub andmesubjekti õigusi, on andmesubjektidel õigus esitada kohtule kaebus[633]. Vastutava või volitatud töötleja vastu algatatud

629 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

630 Isikuandmete kaitse üldmääruse artikkel 78.

631 *Ibid*., põhjendus 143.

632 *Ibid*., artikli 78 lõige 3.

633 *Ibid*., artikkel 79.

menetluste korral on eriti oluline, et üksikisikutel oleks võimalus valida, kuhu hagi esitada. Nad võivad seda teha kas liikmesriigis, kus vastutav või volitatud töötleja on asutatud, või liikmesriigis, kus on andmesubjekti alaline elukoht[634]. Teine võimalus lihtsustab üksikisikute õiguste kasutamist, sest võimaldab esitada hagisid elukohariigis ja tuttavas õiguskorras. Vastutavate ja volitatud töötlejate vastu algatatud menetluse koha piiramine liikmesriigiga, kus need on asutatud, võib takistada muudes liikmesriikides elavaid andmesubjekte kohtumenetluse algatamisel, sest sellega kaasneks reisi- ja lisakulud ning menetlus võib toimuda võõrkeeles ja välisriigi õiguskorras. Ainus erand on juhtumid, kus vastutav või volitatud töötleja on avaliku sektori asutus ja töötlemine toimub avaliku võimu teostamisel. Sellisel juhul on hagi menetlemise pädevus ainult asjaomase avaliku sektori asutuse riigisisestel kohtutel[635].

Kuigi enamasti teevad andmekaitse-eeskirjadega seotud juhtumite kohtuotsuseid liikmesriikide kohtud, võidakse mõnikord juhtumeid esitada Euroopa Liidu Kohtule. Esimene võimalus on, kui andmesubjekt, vastutav või volitatud töötleja või järelevalveasutus esitab Euroopa Andmekaitsenõukogu otsuse kohta tühistushagi. Hagi suhtes kohaldatakse siiski Euroopa Liidu toimimise lepingu artikli 263 tingimusi, mis tähendab, et hagi on vastuvõetav, kui füüsilised ja juriidilised isikud tõendavad, et andmekaitsenõukogu otsus puudutab neid otseselt ja isiklikult.

Teine stsenaarium on seotud Euroopa Liidu institutsioonide või asutustega, kes töötlevad isikuandmeid ebaseaduslikult. Kui ELi institutsioonid rikuvad andmekaitse õigusakte, võivad andmesubjektid esitada hagi otse Euroopa Liidu Kohtu osaks olevale Üldkohtule. Üldkohus vastutab esimeses astmes kaebuste eest, mis käsitlevad ELi õiguse rikkumisi ELi institutsioonides. Seega võib Üldkohtule esitada ka kaebusi Euroopa Andmekaitseinspektori kui ELi institutsiooni vastu[636].

Näide: kohtuasi *Bavarian Lager*[637] käsitles juhtumit, kus ettevõte esitas Euroopa Komisjonile taotluse, et tutvuda komisjoni korraldatud ja väidetavalt ettevõttega seotud juriidiliste küsimustega seotud koosoleku protokolli täisversiooniga. Komisjon lükkas ettevõtte juurdepääsutaotluse tagasi

634 *Ibid.*, artikli 79 lõige 2.

635 *Ibid.*

636 Määruse (EÜ) nr 45/2001 artikli 32 lõige 3.

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

ülekaalukate andmekaitsehuvide tõttu[638]. Bavarian Lager esitas ELi institutsioonide andmekaitse määruse artikli 32 alusel otsuse kohta kaebuse Esimese Astme Kohtule (Üldkohtu eelkäija). Oma otsusega (kohtuasjas T-194/04, *The Bavarian Lager Co. Ltd vs. Euroopa Ühenduste Komisjon*) tühistas Esimese Astme Kohus komisjoni otsuse, millega jäeti rahuldamata kaebuse esitaja juurdepääsu taotlus. Euroopa Komisjon kaebas otsuse edasi Euroopa Liidu Kohtusse.

Euroopa Liidu Kohus otsustas (suurkojas) tühistada Esimese Astme Kohtu otsuse ja kinnitas, et Euroopa Komisjon lükkas tagasi taotluse tutvuda koosoleku protokolli täisversiooniga põhjusel, et kaitsta koosolekul osalenute isikuandmeid. ELK leidis, et komisjon toimis õigesti, keeldudes selle teabe avalikustamisest, sest osalejad ei olnud andnud nõusolekut isikuandmete avalikustamiseks. Lisaks ei tõendanud Bavarian Lager selle teabega tutvumise vajalikkust.

Andmesubjektid, järelevalveasutused, vastutavad või volitatud töötlejad võivad paluda riigisisestes kohtumenetlustes riigisisesel kohtul esitada Euroopa Liidu Kohtule taotlus selgituste saamiseks ELi institutsioonide, organite või asutuste õigusaktide tõlgendamise ja kehtivuse kohta. Selliseid selgitusi nimetatakse eelotsusteks. Need ei ole otsesed õiguskaitsevahendid kaebuse esitajale, ent eelotsuste abil saavad liikmesriikide kohtud tagada, et tõlgendavad ELi õigusakte õigesti. Eelotsusemehhanismi kaudu jõudsid Euroopa Liidu Kohtusse olulised kohtuasjad – näiteks *Digital Rights Ireland* ja *Kärntner Landesregierung jt*[639] ning *Schrems*[640] –, mis on ELi andmekaitseõigust tugevalt mõjutanud.

Näide: *Digital Rights Ireland* ja *Kärntner Landesregierung jt*[641] olid liidetud kohtuasjad, mille esitasid Iirimaa kõrgema astme kohus (High Court) ja Austria konstitutsioonikohus seoses direktiivi 2006/24/EÜ (andmete säilitamise direktiiv) vastavusega ELi andmekaitseõigusele. Austria konstitutsioonikohus

638 Argumendi analüüs: vt Euroopa Andmekaitseinspektor (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Brüssel, Euroopa Andmekaitseinspektor.

639 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

640 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

641 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

esitas Euroopa Liidu Kohtule küsimusi direktiivi 2006/24/EÜ artiklite 3–9 kehtivuse kohta ELi põhiõiguste harta artiklite 7, 9 ja 11 kontekstis. Nende hulgas oli küsimus, kas Austria föderaalse sideseaduse teatud sätted, mis käsitlevad andmete säilitamise direktiivi ülevõtmist, on vastuolus endise andmekaitsedirektiivi ja ELi institutsioonide andmekaitse määruse teatud aspektidega.

Kohtuasjas *Kärntner Landesregierung jt* märkis üks konstitutsioonikohtu menetluses osalenud kaebuse esitajaid, hr Seitlinger, et kasutab telefoni, internetti ja e-posti nii tööeesmärgil kui ka eraviisiliselt. Sellest tulenevalt liigub tema saadetav ja vastu võetav teave avalikes sidevõrkudes. Austria 2003. aasta sideseaduse kohaselt on tema teenuseosutajal õiguslik kohustus koguda ja säilitada andmeid tema võrgukasutuse kohta. Hr Seitlinger leidis, et tema isikuandmete selline kogumine ja säilitamine oli teabe võrgu kaudu saatmise ja vastuvõtmise tehnilise eesmärgi täitmiseks ebavajalik. Samuti ei olnud nende andmete kogumist ja säilitamist vaja arveldamiseks. Hr Seitlinger märkis, et ta ei olnud andnud nõusolekut oma isikuandmete kasutamiseks, mida koguti ja säilitati Austria 2003. aasta sideseaduse tõttu.

Hr Seitlinger esitas sel põhjusel hagiavalduse Austria konstitutsioonikohtule, väites, et tema sideteenuse osutajale määratud kohustuste täitmisega rikutakse talle ELi põhiõiguste harta artikliga 8 tagatud põhiõigusi. Arvestades, et Austria õigusaktidega rakendati ELi õigust (sel ajal andmete säilitamise direktiivi), edastas Austria konstitutsioonikohus asja Euroopa Liidu Kohtule, et see otsustaks, kas direktiiv on kooskõlas ELi põhiõiguste hartas sätestatud õigusega eraelu puutumatusele ja andmekaitsele.

Euroopa Liidu Kohtu suurkoda tegi kohtuasjas otsuse, mille tulemusena tühistati ELi andmete säilitamise direktiiv. ELK leidis, et direktiiviga kaasnes eraelu puutumatuse ja andmekaitse põhiõiguse eriti raske riive, mis ei piirdunud rangelt vajalikuga. Direktiiviga taotleti õiguspärast eesmärki, sest see võimaldas riigi ametiasutustele lisavõimalusi raskete kuritegude uurimiseks ja nende eest vastutusele võtmiseks ning oli seega väärtuslik vahend kriminaaluurimises. Euroopa Liidu Kohus märkis siiski, et põhiõiguste piiranguid tuleks kohaldada ainult siis, kui need on hädavajalikud, ning nendega peaksid kaasnema selged ja täpsed eeskirjad nende kohaldamisala kohta ning üksikisikute kaitsemeetmed.

> ELK seisukoht oli, et direktiiv ei täitnud vajalikkuse hindamise eesmärki. Esiteks ei kehtestatud direktiiviga selgeid ja täpseid eeskirju, mis piiraksid sekkumise ulatust. Säilitatavate andmete ja raskete kuritegude seose nõudmise asemel kohaldati direktiivi kõigi elektrooniliste sidevahendite kõigi kasutajate metaandmete suhtes. Seega oli tegu sekkumisega peaaegu kogu ELi elanikkonna eraelu puutumatuse ja andmekaitse õigustesse, mida võib pidada ebaproportsionaalseks. See ei hõlmanud tingimusi, mis piiraksid isikuandmetega tutvumist volitatud isikutele, samuti ei kohaldatud sellise juurdepääsu suhtes menetlustingimusi, näiteks nõuet saada enne juurdepääsu haldusasutuse või kohtu heakskiit. Direktiivis ei olnud sätestatud selgeid kaitsemeetmeid säilitatavate andmete kaitseks. Direktiiv ei taganud seega andmete tõhusat kaitset kuritarvitamise riski ning andmetele ebaseadusliku juurdepääsu ja nende ebaseadusliku kasutamise eest[642].

Põhimõtteliselt peab Euroopa Liidu Kohus eelotsuse küsimustele vastama ega saa eelotsuse tegemisest keelduda põhjusel, et vastus ei oleks algset kohtuasja arvestades asjakohane ega õigeaegne. Keelduda saab siiski juhul, kui küsimus ei kuulu ELK pädevusvaldkonda[643]. ELK teeb otsuse ainult eelotsusetaotluse põhielementide kohta, kuid riigisisene kohus säilitab pädevuse esialgse kohtuasja lahendamisel[644].

Euroopa Nõukogu õiguse kohaselt peavad konventsiooniosalised kehtestama nüüdisajastatud konventsiooni nr 108 sätete rikkumise korral kasutatavad asjakohased kohtu- ja kohtuvälised õiguskaitsevahendid[645]. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 väidetavaid andmekaitseõiguste rikkumisi Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni osalisriigi poolt võib lisaks esitada Euroopa Inimõiguste Kohtule, kui kõik kättesaadavad riigisisesed õiguskaitsevahendid on ammendatud. Euroopa Inimõiguste Kohtule esitatud hagi Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 rikkumise kohta peab vastama ka muudele vastuvõetavuse kriteeriumidele (Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklid 34–35)[646].

642 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014, punkt 69.

643 ELK, C-244/80, *Pasquale Foglia vs. Mariella Novello (nr 2)*, 16. detsember 1981; ELK, C-467/04, *Kriminaalasi vs. Gasparini jt*, 28. september 2006.

644 ELK, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union vs. Viking Line ABP, OÜ Viking Line Eesti* [suurkoda], C-438/05, 11. detsember 2007, punkt 85.

645 Nüüdisajastatud konventsiooni nr 108 artikkel 12.

646 Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklid 34–37.

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

Näide: kohtuasjas *K.U. vs. Soome*[647] väitis kaebuse esitaja (alaealine), et tema kohta oli interneti tutvumiskohas avaldatud seksuaalse alatooniga kuulutus. Teenuseosutaja keeldus Soome õiguses sätestatud konfidentsiaalsuskohustuse tõttu avaldamast teabe avaldaja nime. Kaebuse esitaja väitis, et olukorras, kus eraisik avaldas tema kohta internetis süüstavaid andmeid, ei olnud talle Soome õigusaktidega tagatud piisavat kaitset. EIK leidis, et peale kohustuse hoiduda meelevaldsest sekkumisest üksikisikute eraellu on riikidel ka positiivsed kohustused, mis hõlmavad selliste meetmete vastuvõtmist, mille eesmärk on tagada eraelu austamine ka üksikisikute omavaheliste suhete valdkonnas. Selle juhtumi korral tulnuks selleks, et kaebuse esitajat reaalselt ja tulemuslikult kaitsta, võtta tõhusaid meetmeid rikkuja isiku tuvastamiseks ja talle süüdistuse esitamiseks. Riik sellist kaitset siiski ei pakkunud ning kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Näide: kohtuasi *Köpke vs. Saksamaa*[648] käsitles juhtumit, kus kaebuse esitajat kahtlustati varguses töökohal ja teda hakati seepärast jälgima varjatud videovalve abil. EIK järeldas, et kohtuasjas ei olnud märke, et riigi ametiasutused ei olnud suutnud kaalutlusruumi piires tagada kaebuse esitajale tema õigust eraelu austamisele artikli 8 tähenduses ning seejuures samaväärselt arvestada nii tööandja huvi kaitsta oma õigust omandile kui ka avalikku huvi tagada nõuetekohane õigusemõistmine. Seepärast tunnistati avaldus vastuvõetamatuks.

Kui EIK leiab, et konventsiooniosaline on rikkunud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga kaitstavat mis tahes õigust, peab konventsiooniosaline EIK otsust täitma (Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 46). Täitemeetmete rakendamisel tuleb kõigepealt peatada rikkumine ja võimalikult palju hüvitada kaebuse esitajale tekkinud kahju. Kohtuotsuste täitmiseks

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

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

võib olla vaja ka üldmeetmeid, et tulevikus ennetada selliseid kohtu avastatud juhtumitega sarnanevaid rikkumisi kas õigusaktide muutmise, kohtupraktika või muude meetmete abil.

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

Õigus volitada mittetulunduslikku asutust, organisatsiooni või ühendust

Isikuandmete kaitse üldmäärus võimaldab üksikisikutel, kes esitavad järelevalveasutusele kaebuse või kohtule hagi, volitada ennast esitama mittetulundusühingut, organisatsiooni või ühingut[649]. Nende mittetulundusühingutel põhikirjalised eesmärgid peavad olema üldhuvides ja nad peavad tegutsema andmekaitse valdkonnas. Nad võivad esitada kaebuse või kasutada õigust õiguskaitsevahendile andmesubjekti(de) nimel. Määrus võimaldab liikmesriikidel otsustada – riigisisese õiguse kohaselt –, kas asutus võib esitada andmesubjektide nimel kaebusi ilma nimetatud andmesubjektide volituseta.

See esindusõigus võimaldab üksikisikutel saada kasu selliste mittetulunduslike üksuste teadmistest ning organisatsiooni- ja finantssuutlikkusest, mis oluliselt lihtsustab üksikisikutele õiguste kasutamist. Isikuandmete kaitse üldmäärus võimaldab neil üksustel esitada kollektiivhagisid mitme andmesubjekti nimel. See on kasulik ka kohtusüsteemi toimimisele ja tõhususele, sest sarnased hagid rühmitatakse ja neid käsitletakse koos.

6.2.3. Vastutus ja õigus hüvitisele

Õigus tõhusale õiguskaitsevahendile peab andma üksikisikutele õiguse nõuda sellise kahju hüvitamist, mis on tekkinud nende isikuandmete töötlemisel vastuolus kohaldatavate õigusaktidega. Vastutava ja volitatud töötleja vastutus ebaseadusliku töötlemise korral on isikuandmete kaitse üldmääruses selgelt sätestatud[650]. Määrusega antakse üksikisikutele õigus saada vastutavalt või volitatud töötlejalt hüvitist nii materiaalse kui ka immateriaalse kahju eest ning määruse põhjenduses sätestatakse, et „[k]ahju mõistet tuleks Euroopa Kohtu praktikat arvestades

649 Isikuandmete kaitse üldmääruse artikkel 80.

650 *Ibid*., artikkel 82.

tõlgendada laialt ja sellisel viisil, mis kajastab täielikult käesoleva määruse eesmärke“[651]. Vastutavad töötlejad vastutavad ja võivad saada hüvitisnõudeid, kui nad ei täida määrusest tulenevaid kohustusi. Isikuandmete volitatud töötleja vastutab töötlemisel tekitatud kahju eest ainult siis, kui ta ei ole täitnud määruse nõudeid, mis on suunatud konkreetselt volitatud töötlejatele, või kui ta ei ole järginud vastutava töötleja seaduslikke juhiseid või on tegutsenud nende vastaselt. Kui vastutav või volitatud töötleja on maksnud täieliku hüvitise, sätestatakse isikuandmete kaitse üldmääruses, et vastutav või volitatud töötleja võib nõuda teistelt sama töötlemisega seotud vastutavatelt või volitatud töötlejatelt tagasi hüvitise see osa, mis vastab kahjuvastutuse määrale[652]. Vastutusest vabastamise nõuded on siiski väga ranged ja tuleb tõendada, et vastutav või volitatud töötleja ei vastutanud kahju põhjustanud sündmuse eest.

Hüvitamine peab olema tekkinud kahju suhtes „täielik ja tõhus“. Kui kahju on põhjustanud mitme vastutava ja volitatud töötleja tehtud töötlemine, peab iga vastutav või volitatud töötleja vastutama kogu kahju eest. Selle reegli eesmärk on tagada andmesubjektidele tõhus hüvitamine ja kooskõlastatud lähenemisviis nõuete täitmisele töötlemistoimingutes osalevate vastutavate ja volitatud töötlejate poolt.

Näide: andmesubjektid ei pea esitama hagi ja nõudma hüvitist kõigilt kahju korral vastutavatelt isikutelt, sest see võib kaasa tuua kulukaid ja pikaajalisi menetlusi. Piisab, kui esitatakse hagi ühe kaasvastutava töötleja vastu, kes võib seejärel vastutada kogu kahju korral. Sellistel juhtudel on kahjutasu maksval vastutaval või volitatud töötlejal hiljem õigus nõuda teistelt töötlemises osalenud ja rikkumise eest vastutavatelt isikutelt makstud summa sisse nende kahjuvastutuse osa ulatuses. Need menetlused eri kaasvastutavate töötlejate ja volitatud töötlejate vahel toimuvad pärast seda, kui andmesubjekt on saanud hüvitise ja andmesubjekt ei ole nende osa.

Euroopa Nõukogu õigusraamistikus nõutakse nüüdisajastatud konventsiooni nr 108 artiklis 12, et konventsiooniosalised kehtestaksid konventsiooni nõuete rikkumise suhtes asjakohased õiguskaitsevahendid. Nüüdisajastatud konventsiooni nr 108 seletuskirjas märgitakse, et õiguskaitsevahendid peavad sisaldama võimalust otsuse või praktika kohtulikuks vaidlustamiseks, kuid ühtlasi tuleb kättesaadavaks teha ka

651 *Ibid.*, põhjendus 146.

652 *Ibid.*, artikli 82 lõiked 2 ja 5.

kohtuvälised õiguskaitsevahendid[653]. Nende õiguskaitsevahendite kättesaadavuse korra, eeskirjad ja järgitava menetluse otsustab iga konventsiooniosaline ise. Konventsiooniosalised ja riigisisesed kohtud peavad kaalutlema ka töötlemisest põhjustatud materiaalse ja immateriaalse kahju rahalise hüvitamise sätteid ning kollektiivhagide esitamise võimaldamist[654].

6.2.4. Karistused

Euroopa Nõukogu õiguses sätestatakse nüüdisajastatud konventsiooni nr 108 artiklis 12, et iga konventsiooniosaline peab kehtestama asjakohased karistused ja õiguskaitsevahendid juhuks, kui rikutakse neid riigisisese õiguse sätteid, mille alusel rakendatakse konventsioonis sätestatud peamisi andmekaitsepõhimõtteid. Konventsiooniga ei kehtestata ega määrata konkreetseid karistusi. Vastupidi, konventsioonis osutatakse selgelt, et igal konventsiooniosalisel on õigus otsustada kriminaal-, haldus- või tsiviilõiguslike karistuste olemus. Nüüdisajastatud konventsiooni nr 108 seletuskirjas sätestatakse, et karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad[655]. Konventsiooniosalised peavad seda põhimõtet järgima, kui nad määravad oma riigisiseses õiguskorras olemasolevate karistuste olemuse ja ranguse.

ELi õiguses antakse isikuandmete kaitse üldmääruse artikliga 83 liikmesriikide järelevalveasutustele õigus määrata määruse rikkumise korral haldustrahve. Artiklis 83 on sätestatud trahvide suurus ja asjaolud, mida riiklikud ametiasutused trahvi määramisel arvestavad, samuti trahvide ülemmäärad. Seega on karistuskord ELis ühtlustatud.

Isikuandmete kaitse üldmääruses kasutatakse trahvide astmelist süsteemi. Järelevalveasutustel on õigus määrata määruse rikkumise eest haldustrahve summas kuni 20 000 000 eurot või ettevõtja korral 4% tema kogu ülemaailmsest aastakäibest – olenevalt sellest, kumb on suurem. Sellise suurusega trahvi võib põhjustada näiteks töötlemise aluspõhimõtete ja nõusoleku tingimuste rikkumine, andmesubjektide õiguste ja määruse nende sätete rikkumine, mis reguleerivad isikuandmete edastamist kolmandates riikides asuvatele vastuvõtjatele. Muude rikkumiste korral võivad järelevalveasutused määrata trahve kuni 10 000 000 euro ulatuses või

653 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 100.

654 *Ibid*.

655 *Ibid.*

ettevõtja korral 2% tema kogu ülemaailmsest aastakäibest – olenevalt sellest, kumb on suurem.

Määratava trahvi liigi ja suuruse määramisel peavad järelevalveasutused arvestama mitut tegurit[656]. Nad peavad nõuetekohaselt kaalutlema näiteks rikkumise olemust, raskust ja kestust, mõjutatud isikuandmete liike ja seda, kas rikkumine oli tahtlik või tingitud hooletusest. Kui vastutav või volitatud töötleja on võtnud meetmeid andmesubjektide tekitatud kahju leevendamiseks, tuleb seda arvestada. Teised tähtsad tegurid, millest järelevalveasutused juhinduvad otsustamisel, on ka järelevalveasutusega pärast rikkumist tehtud koostöö ulatus ja viis, kuidas järelevalveasutus sai rikkumisest teada (näiteks kas sellest teatas töötlemise eest vastutav üksus või andmesubjekt, kelle õigusi rikuti)[657].

Lisaks trahvide määramise võimalusele on järelevalveasutustel palju muid parandusvolitusi. Järelevalveasutuste parandusvolitused on sätestatud isikuandmete kaitse üldmääruse artiklis 58. Need ulatuvad vastutavatele ja volitatud töötlejatele korralduste, hoiatuste ja noomituse tegemisest töötlemistoimingute ajutise või isegi alalise keelamiseni.

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

656 Isikuandmete kaitse üldmääruse artikli 83 lõige 2.

657 Artikli 29 töörühm (2017), *Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679*, WP 253, 3. oktoober 2017.

7

Isikuandmete rahvusvaheline edastamine ja piiriülene liikumine

EL	Teemad	EN
Isikuandmete edastamine		
Isikuandmete kaitse üldmääruse artikkel 44	Mõiste	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõiked 1 ja 2
Isikuandmete vaba liikumine		
Isikuandmete kaitse üldmääruse artikli 1 lõige 3 ja põhjendus 170	ELi liikmesriikide vahel	
	Konventsiooni nr 108 osalisriikide vahel	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 1
Isikuandmete edastamine kolmandatele riikidele või rahvusvahelistele organisatsioonidele		
Isikuandmete kaitse üldmääruse artikkel 45 C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 2015	Kaitse piisavuse otsus / kolmandad riigid või rahvusvahelised organisatsioonid, kes tagavad asjakohasel tasemel kaitse	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 2
Isikuandmete kaitse üldmääruse artikli 46 lõiked 1 ja 2	Asjakohased kaitsemeetmed, sealhulgas andmesubjektide kohtulikult kaitstavad õigused ja õiguskaitsevahendid, mis on tagatud lepingu tüüptingimuste, siduvate kontsernisiseste eeskirjade, toimimisjuhendite ja sertifitseerimismehhanismide kaudu	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõiked 2, 3, 5 ja 6

EL	Teemad	EN
Isikuandmete kaitse üldmääruse artikli 46 lõige 3	Pädeva järelevalveasutuse volitusel: lepingutingimused ja avaliku sektori asutuste halduskokkulepetesse lisatud sätted	
Isikuandmete kaitse üldmääruse artikli 46 lõige 5	Olemasolevad volitused direktiivi 95/46/EÜ alusel	
Isikuandmete kaitse üldmääruse artikkel 47	Siduvad kontsernisisesed eeskirjad	
Isikuandmete kaitse üldmääruse artikkel 49	Erandid konkreetsetes olukordades	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 4
Näited: ELi ja USA broneeringuinfo leping ELi ja USA SWIFT-leping	Rahvusvahelised kokkulepped	Nüüdisajastatud konventsiooni nr 108 artikli 14 lõike 3 punkt a

ELi õiguse kohaselt sätestatakse isikuandmete kaitse üldmääruses andmete vaba liikumine Euroopa Liidus. Samas on määruses erinõuded isikuandmete edastamise kohta kolmandatesse riikidesse väljaspool ELi ja rahvusvahelistele organisatsioonidele. Määruses tunnistatakse selliste edastuste tähtsust, eriti rahvusvahelise kaubanduse ja koostöö seisukohast, kuid tunnistatakse ka suurenenud riski isikuandmetele. Seepärast on määruse eesmärk pakkuda kolmandatesse riikidesse edastatavatele isikuandmetele samasugust kaitset kui ELis[658]. Euroopa Nõukogu õiguses tunnistatakse ka rakenduseeskirjade tähtsust andmete piiriülesel liikumisel, mis põhineb vabal liikumisel poolte vahel, ja kolmandatele isikutele edastamise erinõuete tähtsust.

7.1. Isikuandmete edastamise olemus

Põhipunktid

- Euroopa Liidul ja Euroopa Nõukogul on eeskirjad, mis käsitlevad isikuandmete edastamist vastuvõtjatele kolmandates riikides või rahvusvahelistele organisatsioonidele.
- Andmesubjekti õiguste kaitse tagamine andmete edastamise korral väljapoole ELi võimaldab, et ELi õigusaktidega tagatud kaitse kehtib EList pärit isikuandmetele.

658 Isikuandmete kaitse üldmääruse põhjendused 101 ja 116.

Euroopa Nõukogu õiguses kirjeldatakse andmete piiriülest liikumist isikuandmete edastamisena vastuvõtjatele, kes kuuluvad välisriigi jurisdiktsiooni[659]. Andmete piiriülene liikumine vastuvõtjale, kes ei kuulu ühe lepinguosalise jurisdiktsiooni alla, on lubatud ainult siis, kui on olemas kaitse piisav tase[660].

ELi õiguses reguleeritakse „[t]öödeldavate või pärast kolmandale riigile või rahvusvahelisele organisatsioonile edastamist töötlemiseks ette nähtud isikuandmete" edastamist[661]. Sellised andmevood on lubatud ainult siis, kui need vastavad isikuandmete kaitse üldmääruse V peatükis sätestatud eeskirjadele.

Isikuandmete piiriülene liikumine on lubatud vastuvõtjale, kes kuulub vastavalt Euroopa Nõukogu õigusele või ELi õigusele konventsiooniosalise või liikmesriigi jurisdiktsiooni alla. Mõlemad õigussüsteemid võimaldavad ka andmete edastamist riiki, mis ei ole konventsiooniosaline või liikmesriik, kui teatud tingimused on täidetud.

7.2. Isikuandmete vaba liikumine liikmesriikide või konventsiooniosaliste vahel

Põhipunktid

- Isikuandmete liikumine kogu ELis ning isikuandmete edastamine nüüdisajastatud konventsiooni nr 108 osalisriikide vahel peab toimuma piiranguteta. Samas ei ole kõik nüüdisajastatud konventsiooni nr 108 osalisriigid ELi liikmesriigid ja seega ei ole võimalik edastada andmeid ELi liikmesriigist kolmandasse riiki (isegi kui see on konventsiooni nr 108 osalisriik), kui riik ei täida isikuandmete kaitse üldmääruses sätestatud tingimusi.

Euroopa Nõukogu õiguses peab nüüdisajastatud konventsiooni nr 108 osaliste vahel toimuma isikuandmete vaba liikumine. Andmete edastamine võib siiski olla keelatud, kui on olemas tegelik ja tõsine oht, et edastamisega teisele konventsiooniosalisele kaasneks konventsiooni sätete eiramine, või kui konventsiooniosaline on

659 Nüüdisajastatud konventsiooni nr 108 seletuskirja punkt 102.

660 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 2.

661 Isikuandmete kaitse üldmääruse artikkel 44.

selleks kohustatud piirkondlikku rahvusvahelisse organisatsiooni kuuluvate riikide ühiste kaitse-eeskirjade alusel[662].

ELi õiguses on keelatud ELi liikmesriikide vahel isikuandmete vaba liikumise piirangud või keelud, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel[663]. Isikuandmete vaba liikumise piirkonda on laiendatud Euroopa Majanduspiirkonna (EMP) lepinguga,[664] millega tuuakse siseturule Island, Liechtenstein ja Norra.

Näide: kui mitmes liikmesriigis, sealhulgas Sloveenias ja Prantsusmaal asutatud rahvusvahelise ettevõtjate kontserni sidusettevõtja saadab isikuandmeid Sloveeniast Prantsusmaale, ei tohi sellist andmete liikumist Sloveenia õigusaktidega isikuandmete kaitsega seotud kaalutlustel piirata ega keelata.

Samas kui sama Sloveenia ettevõtja soovib edastada samu isikuandmeid Malaisia emaettevõtjale, peab Sloveenia andmeeksportija arvestama isikuandmete kaitse üldmääruse V peatüki eeskirjadega. Nende sätete eesmärk on kaitsta ELi jurisdiktsiooni alla kuuluvate andmesubjektide isikuandmeid.

ELi õiguses kohaldatakse isikuandmete kuritegude ennetamise, uurimise, avastamise või nende eest süüdistuse esitamise või kriminaalkaristuste täideviimise eesmärgil EMP liikmesriikidesse liikumise suhtes direktiivi (EL) 2016/680[665]. Ühtlasi tagab see, et isikuandmete vahetamine liidu pädevate asutuste vahel ei ole andmekaitse tõttu piiratud ega keelatud. Euroopa Nõukogu õiguse kohaselt kuulub isikuandmete mis tahes töötlemine (sh nende piiriülene liikumine konventsiooni nr 108 teiste osaliste vahel) konventsiooni nr 108 kohaldamisalasse, ilma eesmärkidel või tegevusvaldkondadel põhinevate eranditeta, kuigi konventsiooniosalised võivad teha erandeid. Kõik EMP liikmed on ühinenud ka konventsiooniga nr 108.

662 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 1.

663 Isikuandmete kaitse üldmääruse artikli 1 lõige 3.

664 Nõukogu ja komisjoni 13. detsembri 1993. aasta otsus 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 1994 L 1.

665 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, ELT 2016 L 119.

7.3. Isikuandmete edastamine kolmandatele riikidele / muudele kui osalisriikidele või rahvusvahelistele organisatsioonidele

Põhipunktid

- Mõlemad, **Euroopa Nõukogu** ja **EL** lubavad edastada isikuandmeid kolmandatele riikidele või rahvusvahelistele organisatsioonidele, kui teatud andmekaitsetingimused on täidetud.
  - **Euroopa Nõukogu õiguse** kohaselt on võimalik saavutada asjakohane kaitse tase riigi või rahvusvahelise organisatsiooni õigusega või asjakohaste standardite kehtestamisega.
  - **ELi õiguse** kohaselt tohib andmeid edastada, kui kolmas riik tagab kaitse piisava taseme või kui andmete vastutav või volitatud töötleja tagab asjakohased kaitsemeetmed (sh jõustatavad andmesubjektide õigused ja tõhusad õiguskaitsevahendid) selliste vahendite kaudu nagu isikuandmete kaitse tüüptingimused või siduvad kontsernisisesed eeskirjad.
- **Mõlemas, Euroopa Nõukogu ja ELi õiguses** sätestatakse erandtingimused, mis võimaldavad isikuandmete edastamist erilistel asjaoludel, isegi kui puuduvad kaitse piisav tase ja asjakohaseid kaitsemeetmed.

Kuigi nii Euroopa Nõukogu kui ka ELi õiguses lubatakse andmete liikumist kolmandatesse riikidesse või rahvusvahelistesse organisatsioonidesse, on kummaski õiguses sätestatud eri tingimused. Mõlemas tingimuste kogumis arvestatakse organisatsiooni eri struktuuri ja eesmärke.

ELi õiguse kohaselt on põhimõtteliselt kaks võimalust lubada isikuandmete edastamist kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Andmete edastamine võib toimuda Euroopa Komisjoni tehtud kaitse piisavuse otsuse alusel[666] või – kui sellist kaitse piisavuse otsust ei ole – tingimusel, et vastutav või volitatud töötleja tagab asjakohased kaitsemeetmed, sealhulgas andmesubjektide kohtulikult kaitstavad õigused ja õiguskaitsevahendid[667]. Kui puuduvad kaitse piisavuse otsus ja asjakohased kaitsemeetmed, on olemas mitu erandit.

666 Isikuandmete kaitse üldmääruse artikkel 45.

667 *Ibid*., artikkel 46.

Euroopa Nõukogu õiguse kohaselt on andmete vaba edastamine muudele kui konventsiooniosalistele lubatud siiski üksnes järgmisel alusel:

- asjaomase riigi või rahvusvahelise organisatsiooni õigus, sealhulgas kohaldatavad rahvusvahelised lepingud või kokkulepped, mis tagavad asjakohased kaitsemeetmed;

- erakorralised või heakskiidetud standardsed kaitsemeetmed, mis on tagatud õiguslikult siduvate ja täitmisele pööratavate õigusvahenditega, mille on vastu võtnud ja mida rakendavad andmete edastamises ja edasises töötlemises osalevad isikud[668].

Sarnaselt ELi õigusega on asjakohase andmekaitse taseme puudumise korral olemas mitu erandit.

7.3.1. Edastamine kaitse piisavuse otsuse alusel

ELi õiguses on isikuandmete vaba liikumine kolmandatesse riikidesse, kui tagatakse andmekaitse piisav tase, sätestatud isikuandmete kaitse üldmääruse artiklis 45. Euroopa Liidu Kohus on selgitanud, et termin „kaitse piisav tase" eeldab, et kolmas riik tagab põhiõiguste ja -vabaduste kaitse taseme, mis on „sisuliselt samaväärne"[669] ELis õigusaktidega tagatud kaitsega. Vahendid, mida kolmas riik sellega seoses niisuguse kaitsetaseme saavutamiseks kasutab, võivad erineda nendest, mida rakendatakse liidus, sest kaitse piisavuse nõue ei tähenda, et ELi eeskirju tuleb punkt-punktilt kopeerida[670].

Euroopa Komisjon hindab andmekaitse taset välisriikides, uurides nende riigisisest õigust ja kohaldatavaid rahvusvahelisi kohustusi. Arvestada tuleb ka riigi osalemist mitmepoolsetes või piirkondlikes süsteemides, eelkõige isikuandmete kaitse valdkonnas. Kui Euroopa Komisjon leiab, et kolmas riik või rahvusvaheline organisatsioon tagab kaitse piisava taseme, võib ta teha kaitse piisavuse otsuse, millel on siduv

668 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõike 3 punktid a ja b.

669 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015, punkt 96.

670 *Ibid.*, punkt 74. Vt ka Euroopa Komisjon (2017), komisjoni teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas", COM(2017)7 final, 10. jaanuar 2017, lk 6.

mõju[671]. Euroopa Liidu Kohus on siiski märkinud, et riiklikel järelevalveasutustel on endiselt pädevus uurida isiku avaldust tema isikuandmete kaitse kohta, mis on edastatud kolmandale riigile, kelle puhul komisjon on seisukohal, et riik tagab kaitse piisava taseme, kui see isik väidab, et kolmandas riigis kehtivad õigusaktid ja tavad ei taga kaitse piisavat taset[672].

Euroopa Komisjon võib hinnata ka kolmanda riigi territooriumi osa või konkreetset sektorit, nagu tehti näiteks Kanada erasektori kaubandusõiguse õigusaktide korral[673]. Samuti tehakse järeldused kaitse piisavuse kohta andmete edastamiseks ELi ja kolmandate riikide vahel sõlmitud lepingute alusel. Nendes otsustes käsitletakse üksnes üht liiki andmeedastust, näiteks broneeringuinfo edastamist lennuettevõtjatelt välisriikide piirikontrolliasutustele EList teatud välisriikidesse suunduvatel lendudel (vt punkt 7.3.4).

Kaitse piisavuse otsuseid kontrollitakse pidevalt. Euroopa Komisjon vaatab sellised otsused korrapäraselt läbi, et jälgida nende staatust mõjutavaid arengusuundumusi. Seega, kui Euroopa Komisjon leiab, et kolmas riik või rahvusvaheline organisatsioon ei vasta enam nõuetele, mis õigustavad kaitse piisavuse otsust, võib ta otsust muuta, selle peatada või tühistada. Ka võib komisjon alustada läbirääkimisi asjaomase kolmanda riigi või rahvusvahelise organisatsiooniga, et lahendada otsusega seotud küsimus.

Kaitse piisavuse otsused, mille Euroopa Komisjon on teinud direktiivi 95/46/EÜ alusel, jäävad kehtima, kuni neid isikuandmete kaitse üldmääruse artikli 45 kohaselt tehtud komisjoni otsusega muudetakse, asendatakse või tunnistatakse kehtetuks.

Praeguseks on Euroopa Komisjon kinnitanud, et piisavat kaitset pakuvad Andorra, Argentina, Fääri saared, Guernsey, Iisrael, Jersey, Kanada (kaubandusorganisatsioonid, mis kuuluvad isikuandmete kaitse ja elektrooniliste dokumentide seaduse (PIPEDA) kohaldamisalasse), Mani saar, Šveits, Uruguay ja Uus-Meremaa. Seoses andmete edastamisega USA-le tegi Euroopa Komisjon 2000. aastal kaitse piisavuse otsuse, millega lubati edastada andmeid ettevõtjatele, kes on ise kinnitanud EList

671 Korrapäraselt ajakohastatav loetelu riikidest, mille andmekaitse tase on tunnistatud piisavaks, on avaldatud Euroopa Komisjoni õigusküsimuste peadirektoraadi veebilehel.

672 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015, punktid 63 ja 65–66.

673 Euroopa Komisjon (2002), komisjoni 20. detsembri 2001. aasta otsus 2002/2/EÜ 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 2002 L 2.

edastatavate isikuandmete kaitsmist ja vastavust programmi Safe Harbor põhimõtetele[674]. Euroopa Liidu Kohus tühistas otsuse 2015. aastal ja 2016. aasta juulis võeti vastu uus kaitse piisavuse otsus, mis võimaldab ettevõtetel ühineda alates 1. augustist 2016.

Näide: kohtuasi *Schrems*[675] käsitles juhtumit, kus Austria kodanik Maximillian Schrems oli olnud mitu aastat Facebooki kasutaja. Osa andmeid või kõik andmed, mille ta Facebookile esitas, edastas Facebooki Iiri tütarettevõtja USAs asuvatesse serveritesse, kus neid töödeldi. Maximillian Schrems esitas Iirimaa andmekaitseasutusele kaebuse, olles seisukohal, et arvestades USA kodanikust rikkumisest teataja Edward Snowdeni paljastusi USA luureteenistuste järelevalvetegevuse kohta, ei paku USA õigus ja tavad sellesse riiki edastatud andmetele piisavat kaitset. Iirimaa ametiasutus lükkas kaebuse tagasi põhjendusel, et komisjon leidis 26. juuli 2000. aasta otsuses, et USA tagab programmi Safe Harbor raames USAsse edastatavate isikuandmete kaitse piisava taseme. Juhtum edastati Iirimaa kõrgema astme kohtule (High Court), kes tegi selle kohta eelotsuse taotluse Euroopa Liidu Kohtule.

ELK leidis, et komisjoni otsus programmi Safe Harbor raamistiku piisavuse kohta on kehtetu. Esimeseks märkis ELK, et otsusega lubati programmi Safe Harbor andmekaitsepõhimõtete kohaldatavust piirata riigi julgeoleku, avaliku huvi või õiguskaitse nõuete alusel või USA riigisiseste õigusaktide alusel. Seega võimaldas otsus sekkuda nende isikute põhiõigustesse, kelle isikuandmed on edastatud või võidakse edastada USAsse[676]. Lisaks märkis kohus, et otsus ei sisaldanud järeldusi selliste eeskirjade olemasolu kohta USAs, mille eesmärk on niisugust sekkumist piirata, ega tõhusa õiguskaitse olemasolu kohta sellise sekkumise vastu[677]. ELK rõhutas, et ELis tagatud põhiõiguste ja -vabaduste kaitse eeldab, et õigusaktides, millega sekkutakse artiklitesse 7 ja 8, kehtestataks selged ja täpsed eeskirjad, millega määratletakse meetme ulatus ja kohaldamine ning kehtestatakse minimaalsed kaitsemeetmed,

674 Komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ 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 2000 L 215. Euroopa Liidu Kohus tunnistas otsuse kehtetuks kohtuasjas C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda].

675 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

676 *Ibid.*, punkt 84.

677 *Ibid.*, punktid 88–89.

erandid ja piirangud seoses isikuandmete kaitsega[678]. Arvestades, et komisjoni otsuses ei märgitud, et USA tõepoolest tagab riigisisese õigusega või endale võetud rahvusvaheliste kohustustega kaitse taseme, järeldas ELK, et otsusega ei ole täidetud andmekaitsedirektiivi asjakohase andmete edastamise sätte nõudeid ning seetõttu on otsus kehtetu[679].

USA kaitse tase ei ole seega „sisuliselt samaväärne" ELi tagatud põhiõiguste ja -vabadustega[680]. ELK väitis, et rikuti ELi põhiõiguste harta mitut artiklit. Esiteks rikuti artiklit 7, sest USA õigusakt „võimaldab ametiasutustel elektroonilise side sisuga üldiselt tutvuda". Teiseks rikuti ka artiklit 47, sest õigusakt ei sätestanud üksikisikutele õiguskaitsevahendeid seoses isikuandmetega tutvumise, nende parandamise või kustutamisega. Arvestades, et programmiga Safe Harbor rikuti eespool nimetatud artikleid, ei töödeldud isikuandmeid enam seaduslikult, mis põhjustas artikli 8 rikkumise.

Kui Euroopa Liidu Kohus oli tunnistanud programmi Safe Harbor kehtetuks, leppisid komisjon ja USA kokku ELi-USA uue andmekaitseraamistiku Privacy Shield. 12. juulil 2016 tegi komisjon otsuse, milles kinnitatakse, et USA tagab kaitse piisava taseme isikuandmetele, mida Euroopa Liit edastab USA organisatsioonidele ELi-USA andmekaitseraamistiku Privacy Shield raames[681].

Sarnaselt programmiga Safe Harbor on ELi-USA andmekaitseraamistiku Privacy Shield eesmärk kaitsta isikuandmeid, mida edastatakse EList USAsse kaubanduslikul eesmärgil[682]. USA ettevõtjad võivad ise kinnitada oma andmekaitseraamistiku Privacy Shield loetelu järgimist, kohustudes järgima raamistiku andmekaitsestandardeid. USA pädevad asutused jälgivad ja kontrollivad sertifitseeritud ettevõtjate vastavust nendele standarditele.

678 *Ibid*., punktid 91–92.

679 *Ibid*., punktid 96–97.

680 *Ibid*., punktid 73–74 ja 96.

681 Komisjoni 12. juuli 2016. aasta rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ, ELT 2016 L 207. Artikli 29 töörühm avaldas heameelt edasiminekute üle, mis kaasnesid programmi Safe Harbor käsitleva otsusega, ning kiitis komisjoni ja USA ametiasutusi, et nad arvestasid andmekaitseraamistiku Privacy Shield lõplikus versioonis probleeme, mille töörühm tõstatas arvamuses WP 238 ELi-USA andmekaitseraamistiku Privacy Shield kaitse piisavuse otsuse eelnõu kohta. Töörühm märkis siiski, et mitu probleemi on lahendamata. Üksikasjalikum teave: vt artikli 29 töörühm (2016), *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 13. aprill 2016, 16/EN WP 238.

682 Lisateave: vt EU-U.S. Privacy Shield factsheet.

Eelkõige sätestatakse raamistikuga Privacy Shield

- andmekaitsekohustused ettevõtjatele, kes saavad EList isikuandmeid;
- kaitse ja hüvitusmehhanism üksikisikutele, eelkõige ombudsmani mehhanismi loomine, mis on USA luureteenistustest sõltumatu ja käsitleb nende isikute kaebusi, kes leiavad, et USA ametiasutused on nende isikuandmeid kasutanud riigi julgeoleku valdkonnas ebaseaduslikult;
- iga-aastane ühine läbivaatamine raamistiku rakendamise jälgimiseks;[683] esimene läbivaatamine toimus 2017. aasta septembris[684].

USA valitsuse kirjalikud kohustused ja kinnitused on lisatud andmekaitseraamistikku Privacy Shield käsitlevale otsusele. Nendega sätestatakse piirangud ja kaitsemeetmed USA valitsuse juurdepääsu kohta isikuandmetele õiguskaitse ja riigi julgeoleku eesmärgil.

7.3.2. Edastamine asjakohaste kaitsemeetmete kohaldamisel

Mõlemas, **Euroopa Nõukogu** ja **ELi õiguses** tunnustatakse asjakohaseid kaitsemeetmeid andmeid eksportiva vastutava töötleja ja kolmanda riigi või rahvusvahelise organisatsiooni vastuvõtja vahel kui vastuvõtja jaoks andmekaitse piisava taseme tagamise võimalikku vahendit.

ELi õiguse kohaselt on isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile lubatud, kui vastutav või volitatud töötleja sätestab asjakohased kaitsemeetmed ja kohtulikult kaitstavad õigused ning kui andmesubjektidele on kättesaadavad tõhusad õiguskaitsevahendid[685]. Vastuvõetavate asjakohaste kaitsemeetmete loetelu on sätestatud üksnes ELi andmekaitseõiguses. Asjakohased kaitsemeetmed võivad olla kehtestatud

683 Lisateave: vt Euroopa Komisjoni veebileht EU-U.S. Privacy Shield.

684 Euroopa Komisjon, *Komisjoni aruanne Euroopa Parlamendile ja nõukogule ELi-USA andmekaitseraamistiku Privacy Shield toimimise esimese iga-aastase läbivaatamise kohta*, COM(2017) 611 final, 18. oktoober 2017.Vt ka artikli 29 töörühm, *EU – U.S. Privacy Shield – First annual Joint Review*, vastu võetud 28. novembril 2017, 17/EN WP 255.

685 Isikuandmete kaitse üldmääruse artikkel 46.

- õiguslikult siduva ja täitmisele pööratava dokumendiga avaliku sektori asutuste või organite vahel;
- siduvates kontsernisisestes eeskirjades;
- isikuandmete kaitse tüüptingimustes, mille on vastu võtnud kas Euroopa Komisjon või järelevalveasutus;
- toimimisjuhendites;
- sertifitseerimismehhanismides[686].

ELis asuva vastutava või volitatud töötleja ja kolmandas riigis asuva andmete vastuvõtja vahelised kohandatud lepingu tüüptingimused on samuti vahend, millega kehtestada asjakohased kaitsemeetmed. Enne kui selliseid lepingu tüüptingimusi saab kasutada isikuandmete edastamise vahendina, peab pädev järelevalveasutus need heaks kiitma. Sarnaselt võivad avaliku sektori asutused kasutada oma halduskokkulepetes sisalduvaid andmekaitsesätteid, kui järelevalveasutus on selleks loa andnud[687].

Euroopa Nõukogu õiguses on andmete liikumine riiki või rahvusvahelisse organisatsiooni, mis ei ole nüüdisajastatud konventsiooni nr 108 osaline, lubatud tingimusel, et on tagatud piisav kaitse. Selle võib saavutada järgmiste meetmetega:

- riigi või rahvusvahelise organisatsiooni õigus või
- õiguslikult siduvas dokumendis sisalduvad erakorralised või standardsed kaitsemeetmed[688].

686 Isikuandmete kaitse üldmääruse artikli 46 lõike 1 punktid c ja d, lõike 2 punktid a, b, e, ja f ning artikkel 47.

687 *Ibid*., artikli 46 lõige 3.

688 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõike 3 punkt b.

Edastamine lepingutingimuste kohaldamisel

Nii **Euroopa Nõukogu** kui ka **ELi õiguses** tunnustatakse vastuvõtja piisava andmekaitse taseme tagamise võimaliku meetmena andmeid eksportiva vastutava töötleja ja kolmandas riigis asuva vastuvõtja vahelise lepingu tingimusi[689].

ELi tasandil töötas Euroopa Komisjon artikli 29 töörühma kaasabil välja isikuandmete kaitse tüüptingimused, mis sertifitseeriti komisjoni otsusega ametlikult kui piisava andmekaitse tõend[690]. Et komisjoni otsused on liikmesriikides tervikuna siduvad, peavad andmeid edastavad riiklikud asutused oma menetlustes tunnustama lepingu tüüptingimusi[691]. Seega kui andmeid eksportiv vastutav töötleja ja kolmanda riigi vastuvõtja lepivad kokku ja allkirjastavad tingimused, peab see järelevalveasutusele piisavalt tõendama, et piisavad kaitsemeetmed on kehtestatud. Samas leidis Euroopa Liidu Kohus kohtuasjas *Schrems*, et Euroopa Komisjonil ei ole pädevust piirata riiklike järelevalveasutuste volitusi teha järelevalvet isikuandmete edastamise üle kolmandasse riiki, mille suhtes komisjon on teinud kaitse piisavuse otsuse[692]. Seega ei takistata riiklikel järelevalveasutustel kasutada oma volitusi, sealhulgas õigust peatada või keelata isikuandmete edastamine, kui edastamine toimub vastuolus ELi või riigisisese andmekaitseõigusega, näiteks kui andmete importija ei täida lepingu tüüptingimusi[693].

Isikuandmete kaitse tüüptingimuste olemasolu ELi õigusraamistikus ei takista vastutavat töötlejat koostamast muid erakorralisi individuaalseid lepingutingimusi, kui järelevalveasutus on need heaks kiitnud[694]. Nendega tuleb lõppkokkuvõttes tagada siiski sama kaitsetase kui isikuandmete kaitse tüüptingimustega. Erakorraliste tingimuste heakskiitmisel peavad järelevalveasutused kohaldama järjepidevuse mehhanismi, et tagada kogu ELis ühtne õiguslik lähenemisviis[695]. See tähendab, et pädev

689 Isikuandmete kaitse üldmääruse artikli 46 lõige 3; nüüdisajastatud konventsiooni nr 108 artikli 14 lõike 3 punkt b.

690 *Ibid.*, artikli 46 lõike 2 punkt b ja artikli 46 lõige 5.

691 *Ibid.*, artikli 46 lõike 2 punkt c; Euroopa Liidu toimimise lepingu artikkel 288.

692 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015, punktid 96–98 ja 102–105.

693 Et arvestada Euroopa Liidu Kohtu seisukohta kohtuasjas *Schrems*, muutis komisjon oma otsust lepingu tüüptingimuste kohta. Komisjoni 16. detsembri 2016. aasta rakendusotsus (EL) 2016/2297, millega muudetakse otsuseid 2001/497/EÜ ja 2010/87/EL kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste ja nende riikide volitatud töötajate kohta, kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 95/46/EÜ, ELT 2016 L 344.

694 Isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt a.

695 *Ibid.*, artikkel 63 ja artikli 64 lõike 1 punkt e.

järelevalveasutus peab edastama oma otsuse kavandi Euroopa Andmekaitsenõukogule. Euroopa Andmekaitsenõukogu avaldab selle kohta arvamuse ja järelevalveasutus peab lõpliku otsuse tegemisel seda arvamust täielikult arvestama. Kui ta ei kavatse Euroopa Andmekaitsenõukogu arvamust järgida, käivitatakse Euroopa Andmekaitsenõukogus vaidluste lahendamise mehhanism ja nõukogu teeb siduva otsuse[696].

Lepingu tüüptingimuse kõige olulisemad osad on järgmised:

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

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

Praegu on olemas kaks tüüptingimuste kogumit, mida saab kasutada vastutavate töötlejate vahelisel andmeedastusel ja mille hulgast andmeid eksportiv vastutav töötleja saab valida[697]. Kui vastutav töötleja edastab andmeid volitatud töötlejale, on selleks olemas ainult üks lepingu tüüptingimuste kogum,[698] kuid nende suhtes toimub praegu kohtumenetlus.

Näide: pärast seda, kui Euroopa Liidu Kohus tunnistas programmi Safe Harbor käsitleva otsuse kehtetuks,[699] ei saa isikuandmete edastamine USA-le enam põhineda sellel kaitse piisavuse otsusel. USA ametiasutustega peetud läbirääkimiste ajal ja kuni uue kaitse piisavuse otsuse vastuvõtmiseni (võeti vastu

696 *Ibid*., artiklid 64 ja 65.

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

698 Euroopa Komisjon (2010), komisjoni 5. veebruari 2010. aasta otsus 2010/87/EL kolmandates riikides asuvatele volitatud töötlejatele isikuandmete edastamise lepingu tüüptingimuste kohta nõukogu ja Euroopa Parlamendi direktiivi 95/46/EÜ alusel, ELT 2010 L 39. Käsiraamatu koostamise ajal on menetlemisel lepingu tüüptingimuste kasutamise suhtes isikuandmete USA-le edastamise alusena kohtuasi Iirimaa kõrgema astme kohtus High Court.

699 ELK, C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015.

12. juulil 2016)[700] sai andmeid edastada ainult muudel õiguslikel alustel, näiteks lepingu tüüptingimuste või siduvate kontsernisiseste eeskirjade alusel. Paljud äriühingud, sealhulgas Facebook Ireland (kelle vastu algatati kohtuasi, mis viis programmi Safe Harbor käsitleva otsuse tühistamiseni), läksid ELi ja USA vahel andmete edastamise jätkamiseks üle lepingu tüüptingimustele.

Maximillian Schrems esitas Iirimaa järelevalveasutusele kaebuse, paludes tal peatada USA-le andmete edastamine lepingu tüüptingimuste alusel. Sisuliselt väitis ta, et kui Facebooki Iiri tütarettevõtja edastab tema isikuandmeid äriühingule Facebook Inc. ja USAs asuvatesse serveritesse, ei ole mingit tagatist, et andmed on kaitstud. Äriühingule Facebook Inc. on siduvad USA õigusaktid, millega teda võidakse kohustada avalikustada isikuandmeid USA õiguskaitseasutustele, ning Euroopa kodanikel puuduvad kättesaadavad õiguskaitsevahendid see tegevus vaidlustada[701]. Neil põhjustel leidis Euroopa Liidu Kohus, et programmi Safe Harbor käsitlev otsus on kehtetu, ja kuigi kohtu otsus piirdus selle otsuse läbivaatamisega, pidas kaebuse esitaja tõstatatud küsimusi asjakohaseks, kui andmete edastamine põhineb lepingutingimustel. Käsiraamatu koostamise ajal uuris juhtumit Iirimaa kõrgema astme kohus (High Court). Kaebuse esitaja kavatseb ilmselt esitada asja Euroopa Liidu Kohtusse, kus soovib vaidlustada Euroopa Komisjoni lepingu tüüptingimusi käsitleva otsuse kehtivuse. Nagu on kirjeldatud 5. peatükis, on ainult Euroopa Liidu Kohtul pädevus tunnistada ELi õigusakt kehtetuks.

Edastamine siduvate kontsernisiseste eeskirjade kohaldamisel

ELi õigusega lubatakse ka isikuandmete edastamist siduvate kontsernisiseste eeskirjade alusel, kui andmeid edastatakse rahvusvaheliselt sama kontserni või ettevõtjate rühma piires, mis on osa ühisest majandustegevusest[702]. Enne kui siduvaid kontsernisiseseid eeskirju saab kasutada isikuandmete edastamise vahendina, peab pädev järelevalveasutus need kooskõlas siduvate kontsernisiseste eeskirjadega heaks kiitma, kasutades järjepidevuse mehhanismi.

700 Komisjoni 12. juuli 2016. aasta rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ, ELT L 207.

701 Lisateave: vt läbivaadatud kaebus Facebook Ireland Ltd vastu, mille Maximillian Schrems esitas Iiri andmekaitsevolinikule 1. detsembril 2015.

702 Isikuandmete kaitse üldmääruse artikkel 47.

Heakskiidu saamiseks peavad siduvad kontsernisisesed eeskirjad olema õiguslikult siduvad, hõlmama kõiki olulisi andmekaitsepõhimõtteid ja olema kohaldatavad kontserni iga liikme suhtes ja poolt. Need peavad selge sõnaga andma andmesubjektidele kohtulikult kaitstavad õigused, hõlmama kõiki olulisi andmekaitsepõhimõtteid ja järgima teatud vorminõudeid, näiteks märkides ettevõtja struktuuri ning kirjeldades andmete edastamist ja andmekaitsepõhimõtete kohaldamist. See hõlmab sellise teabe esitamist andmesubjektidele. Siduvates kontsernisisestes eeskirjades tuleb muu hulgas täpsustada andmesubjektide õigused ja sätted vastutuse kohta eeskirjade rikkumise korral[703]. Siduvate kontsernisiseste eeskirjade heakskiitmisel käivitatakse järelevalveasutuste koostöö järjepidevuse mehhanism (vt kirjeldus 5. peatükis).

Järjepidevuse mehhanismi raames kontrollib juhtiv järelevalveasutus kavandatavaid siduvaid kontsernisiseseid eeskirju, võtab vastu otsuse kavandi ja edastab selle Euroopa Andmekaitsenõukogule. Andmekaitsenõukogu esitab selle kohta arvamuse ja juhtiv järelevalveasutus võib siduvad kontsernisisesed eeskirjad ametlikult heaks kiita, arvestades seejuures andmekaitsenõukogu arvamust. See arvamus ei ole õiguslikult siduv, kuid kui järelevalveasutus kavatseb arvamust eirata, käivitatakse vaidluste lahendamise mehhanism ja Euroopa Andmekaitsenõukogu kutsutakse üles võtma vastu õiguslikult siduv otsus kahe kolmandiku liikmete häälteenamusega[704].

Euroopa Nõukogu õiguses kuuluvad õiguslikult siduvas dokumendis sisalduvate erakorraliste või standardsete kaitsemeetmete[705] hulka ka siduvad kontsernisisesed eeskirjad.

7.3.3. Erandid konkreetsetes olukordades

ELi õiguse kohaselt võib isikuandmete edastamine kolmandasse riiki olla õigustatud isegi siis, kui puudub asjakohane otsus või puuduvad kaitsemeetmed, näiteks lepingu tüüptingimused või siduvad kontsernisisesed eeskirjad, ja mis tahes järgmise asjaolu korral:

- andmesubjekt annab selgesõnalise nõusoleku andmete edastamiseks;

703 Üksikasjalik kirjeldus: vt isikuandmete kaitse üldmääruse artikkel 47.

704 *Ibid*., artikli 57 lõike 1 punkt s, artikli 58 lõike 1 punkt j, artikli 64 lõike 1 punkt f, artikli 65 lõiked 1 ja 2.

705 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõike 3 punkt b.

- andmesubjekt astub või kavatseb astuda sellisesse lepingulisse suhtesse, kus andmete piiriülene edastamine on vajalik;
- lepingu sõlmimine vastutava töötleja ja kolmanda isiku vahel andmesubjekti huvides;
- avaliku huvi olulised põhjused;
- õigusnõuete koostamine, esitamine või kaitsmine;
- andmesubjekti eluliste huvide kaitsmine;
- andmeid edastatakse avalikest registritest; sellisel juhul on tegu ülekaaluka huviga tagada laiema avalikkuse juurdepääs avalikes registrites säilitatavale teabele[706].

Kui ükski nendest tingimustest ei kohaldu ja kui edastamine ei saa põhineda kaitse piisavuse otsusel või asjakohastel kaitsemeetmetel, võib edastamine toimuda üksnes siis, kui see ei ole korduv, käsitleb piiratud arvu andmesubjekte ja on vajalik vastutava töötleja mõjuvate õigustatud huvide tagamise eesmärgil, kui andmesubjekti õigused ei ole nende suhtes ülimuslikud[707]. Sellistel juhtudel peab vastutav töötleja hindama edastamise asjaolusid ja tagama kaitsemeetmed. Samuti peab ta teatama järelevalveasutusele ja asjaomastele andmesubjektidele nii andmete edastamisest kui ka seda põhjendavast õigustatud huvist.

Asjaolu, et erandid on andmete seaduslikul edastamisel viimane abinõu[708] (mida tohib kasutada ainult kaitse piisavuse otsuse puudumise korral ja kui muid kaitsemeetmeid ei ole kehtestatud), rõhutab nende erandlikku olemust ja seda toonitatakse isikuandmete kaitse üldmääruse põhjendustes eraldi[709]. Seega on erandid vastuvõetavad võimalusena edastada andmeid „teatavatel asjaoludel" nõusoleku alusel ja kui edastamine on „juhtumipõhine ja vajalik"[710] seoses lepingu või õigusliku nõudega.

706 Isikuandmete kaitse üldmääruse artikkel 49.

707 *Ibid.*

708 *Ibid.*, artikli 49 lõige 1.

709 Vt isikuandmete kaitse üldmääruse artikli 49 lõike 1 punktid a, b ja e ning põhjendus 113.

710 *Ibid.*, artikli 49 lõige 1.

Lisaks peavad eriolukordade erandid olema artikli 29 töörühma suuniste kohaselt erandlikud, põhinema konkreetsetel juhtumitel ja neid ei saa kasutada andmete suuremahulise või korduva edastamise korral[711]. Ka Euroopa Andmekaitseinspektor rõhutas määruse (EÜ) nr 45/2001 kohase edastamise õigusliku alusena kasutatavate erandite erakorralist iseloomu, märkides, et seda lahendust tuleks kasutada „piiratud juhtudel" ja „juhusliku edastamise" korral[712].

Näide: globaalse piletite levitamise süsteemi (GDS) teenust pakkuv ettevõte, mille peakorter asub USAs, pakub kogu maailmas paljudele lennuettevõtjatele, hotellidele ja ristluslaevadele veebipõhist broneerimissüsteemi, töödeldes seejuures kümnete miljonite isikute andmeid ELis. Andmete esialgsel edastamisel USAs asuvatesse serveritesse tugineb GDS-teenust pakkuv ettevõte andmete edastamise (mida on vaja lepingu sõlmimiseks) õigusliku alusena erandile. Seega ei taga ettevõte Euroopast pärit, USAsse saadetavate ja seejärel üle kogu maailma asuvatele hotellidele edastatavatele isikuandmetele muid kaitsemeetmeid (mis tähendab, et kaitsemeetmed puuduvad ka hilisemal edastamisel). GDS-teenust pakkuv ettevõte ei täida isikuandmete kaitse üldmääruses andmete rahvusvahelise seadusliku edastamise nõudeid, sest tugineb andmete suuremahulise edastamise õigusliku alusena erandile.

Kui puudub kaitse piisavuse otsus, on ELil või selle liikmesriikidel õigus piirata avaliku huvi olulistel põhjustel isikuandmete eriliikide edastamist kolmandasse riiki, kuigi on olemas muud edastamise tingimused. Neid piiranguid tuleb pidada erandlikeks ja liikmesriigid peavad teatama asjakohased sätted komisjonile[713].

Euroopa Nõukogu õigus lubab andmete liikumist territooriumidele, kus puudub asjakohane andmekaitse, kui

- andmesubjekt on andnud nõusoleku;
- andmete edastamine on vajalik andmesubjekti huvides;

711 Artikli 29 töörühm (2005), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brüssel, 25. november 2005.

712 Euroopa Andmekaitseinspektor (2014), *Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies*, seisukoht, Brüssel, 14. juuli 2014, lk 15.

713 Vt isikuandmete kaitse üldmääruse artikli 49 lõige 5.

- tegu on seaduses sätestatud ülekaalukate õigustatud huvidega, eelkõige oluliste avalike huvidega;

- tegu on vajaliku ja proportsionaalse meetmega demokraatlikus ühiskonnas[714].

7.3.4. Rahvusvahelistel lepingutel põhinev edastamine

EL võib sõlmida kolmandate riikidega rahvusvahelisi lepinguid, millega reguleeritakse isikuandmete edastamist konkreetsel eesmärgil. Need lepingud peavad sisaldama asjakohaseid kaitsemeetmeid, et tagada asjaomaste isikute isikuandmete kaitse. Isikuandmete kaitse üldmääruse olemasolu ei piira nende rahvusvaheliste lepingute täitmist[715].

Liikmesriigid võivad sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega ka rahvusvahelisi lepinguid, mis tagavad üksikisikute põhiõiguste ja -vabaduste asjakohase kaitse, kui need lepingud ei mõjuta isikuandmete kaitse üldmääruse kohaldamist.

Sarnane eeskiri on sätestatud nüüdisajastatud konventsiooni nr 108 artikli 12 lõike 3 punktis a.

Isikuandmete edastamist hõlmavad rahvusvahelised lepingud on näiteks broneeringuinfo kokkulepped.

Broneeringuinfo

Broneeringuinfot koguvad lennuettevõtjad lennupiletite broneerimisel ning see sisaldab muu hulgas lennureisija nime, aadressi, krediitkaardiandmeid ja istekoha numbrit. Lennuettevõtjad koguvad seda teavet ka oma ärilisel eesmärgil. EL on sõlminud mõne kolmanda riigiga (Austraalia, Kanada ja USA) lepingud broneeringuinfo edastamise kohta terroriaktide või raskete rahvusvaheliste kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks. Lisaks

714 Nüüdisajastatud konventsiooni nr 108 artikli 14 lõige 4.

715 Isikuandmete kaitse üldmääruse põhjendus 102.

võttis liit 2016. aastal vastu direktiivi (EL) 2016/861 (ELi broneeringuinfo direktiiv)[716]. Direktiiv annab ELi liikmesriikidele broneeringuinfo muude kolmandate riikide pädevatele asutustele edastamise õigusraamistiku, et samuti ennetada, avastada ja uurida terroriakte ja raskeid kuritegusid või võtta nende eest vastutusele. Broneeringuinfo edastamine kolmandate riikide ametiasutustele toimub iga kord eraldi, hinnates, kas edastamist on vaja direktiivis määratletud eesmärkidel, ning tingimusel, et järgitakse põhiõigusi.

ELi ja kolmandate riikide vaheliste broneeringuinfo lepingutega seoses on vaidlustatud nende vastavust ELi põhiõiguste hartas sätestatud eraelu puutumatuse ja andmekaitse põhiõigusele. Kui EL allkirjastas pärast Kanadaga peetud läbirääkimisi 2014. aastal broneeringuinfo edastamise ja töötlemise lepingu, otsustas Euroopa Parlament saata asja Euroopa Liidu Kohtusse, et hinnata lepingu õiguspärasust ELi õiguse, eriti põhiõiguste harta artiklite 7 ja 8 seisukohast.

Näide: arvamuses ELi ja Kanada vahelise broneeringuinfo lepingu kohta[717] märkis Euroopa Liidu Kohus, et kavandatav leping ei ole praeguses vormis kooskõlas hartas tunnustatud põhiõigustega, ning seetõttu ei tohiks lepingut sõlmida. Et leping hõlmas isikuandmete töötlemist, oli see sekkumine isikuandmete kaitse õigusesse, mida kaitseb harta. Leping piirab ühtlasi artiklis 7 sätestatud eraelu puutumatuse õigust, sest broneeringuinfot võib tervikuna koondada ja analüüsida viisil, mis toob selgelt esile reisimisharjumused, isikute suhted ning nende finantsolukorra, toitumisharjumuste ja terviseseisundi teabe, mõjutades seega nende eraelu.

Põhiõiguste riive, mille tekitas kavandatav leping, taotles üldhuvi eesmärki, nimelt avaliku julgeoleku ning terrorismi ja raskete rahvusvaheliste kuritegude vastu võitlemise eesmärki. Euroopa Liidu Kohus tuletas siiski meelde, et selleks, et riive oleks põhjendatud, peab see piirduma taotletava eesmärgi saavutamiseks rangelt vajalikuga. Pärast lepingu sätete analüüsimist leidis ELK, et kavandatav leping ei vastanud „rangelt vajaliku" kriteeriumile. Tegurid, mida ELK sellele järeldusele jõudmisel kaalus, olid järgmised.

716 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/681, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks, ELT 2016 L 119.

717 ELK, *Euroopa Kohtu (suurkoda) arvamus 1/15*, 26. juuli 2017.

- Asjaolu, et kavandatav leping hõlmas delikaatsete isikuandmete edastamist. Kavandatava lepingu kohaselt kogutud broneeringuinfo võib sisaldada delikaatseid andmeid, näiteks teavet, mis avalikustab rassilise või etnilise päritolu, usulised veendumused või reisija terviseseisundi. Delikaatsete isikuandmete edastamine ja töötlemine Kanada ametiasutuste poolt võib ohustada diskrimineerimiskeelu põhimõtet ning eeldab seega täpset ja kindlat põhjendust, mis põhineb muudel põhjustel kui avalik julgeolek ja võitlus raskete kuritegude vastu. Kavandatavas lepingus selliseid põhjendusi ei ole[718].

- Ka kõigi reisijate broneeringuinfo andmete jätkuvat säilitamist viie aasta jooksul, isegi pärast seda, kui reisijad on Kanadast lahkunud, peeti range vajalikkuse piire ületavaks. Euroopa Liidu Kohus leidis, et Kanada ametiasutustel võiks olla lubatud säilitada nende reisijate andmeid, kelle kohta objektiivsed tõendid viitavad, et nad võivad ohustada avalikku julgeolekut, isegi pärast Kanadast lahkumist. Seevastu ei ole põhjendatud kõigi nende reisijate isikuandmete säilitamine, kelle kohta ei ole isegi kaudseid tõendeid, et nad ohustavad avalikku julgeolekut[719].

Konventsiooni nr 108 nõuandekomitee on avaldanud arvamuse broneeringuinfot käsitlevate Euroopa Nõukogu õiguse kohaste lepingute andmekaitsemõju kohta[720].

Sõnumiandmed

Belgias asuv Ülemaailmne Pankadevahelise Finantsinfo Ühing (SWIFT), kes töötleb enamikku Euroopa pankadest lähtuvaid ülemaailmseid rahaülekandeid, käitas USAs peegelkeskust ja talle esitati nõue avalikustada andmeid USA rahandusministeeriumile terrorismi uurimise eesmärgil terrorismi rahastamise jälgimise programmi raames[721].

718 *Ibid.*, punkt 165.

719 *Ibid.*, punktid 204–207.

720 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19. august 2016.

721 Vt sellega seoses: artikli 29 töörühm (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, WP 186, Brüssel, 13. juuni 2011; artikli 29 töörühm (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, 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*, otsus, 9. detsember 2008.

ELi seisukohalt ei olnud SWIFTil piisavat õiguslikku alust avaldada neid andmeid (peamiselt ELi kodanike kohta) USA-le ainult põhjusel, et seal asus üks SWIFTi andmetöötluskeskusi.

2010. aastal sõlmiti ELi ja USA erikokkulepe (SWIFT-leping), et tagada vajalik õiguslik alus ja piisavad andmekaitsestandardid[722].

Selle lepingu alusel edastatakse SWIFTi säilitatavaid finantsandmeid jätkuvalt USA rahandusministeeriumile terrorismi või selle rahastamise tõkestamise, uurimise või avastamise või nende eest kohtulikule vastutusele võtmise eesmärgil. USA rahandusministeerium võib SWIFTilt finantsandmeid küsida, kui taotluses

- tuvastatakse võimalikult selgelt, mis finantsandmeid on vaja;
- põhjendatakse selgelt, miks neid andmeid on vaja;
- täpsustatakse võimalikult üksikasjalikult taotluse eesmärk, et nõutavate andmete kogus oleks minimaalne;
- ei nõuta ühtse euromaksete piirkonnaga (SEPA) seotud andmeid[723].

USA rahandusministeerium saadab igast esitatud taotlusest koopia Europolile, kes kontrollib, kas taotlus on kooskõlas SWIFT-lepingu põhimõtetega[724]. Kui Europol kinnitab, et on, peab SWIFT finantsandmed edastama otse USA rahandusministeeriumile. Ministeerium peab neid finantsandmeid säilitama turvalises füüsilises keskkonnas, kus neile on juurdepääs üksnes terrorismi või selle rahastamist uurivatel analüütikutel, ning neid andmeid ei tohi siduda ühegi muu andmebaasiga. Üldiselt tuleb SWIFTilt saadud finantsandmed kustutada hiljemalt viie aasta möödudes andmete vastuvõtmisest. Konkreetse uurimise või kohtulikule vastutusele võtmise jaoks vajalikke finantsandmeid võib säilitada ainult seni, kuni see on uurimise või kohtulikule vastutusele võtmise jaoks vajalik.

722 Nõukogu 13. juuli 2010. aasta otsus 2010/412/EL 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 2010 L 195, lk 3–4. Lepingu tekst on otsusele lisatud, ELT 2010 L 195, lk 5–14.

723 *Ibid*., artikli 4 lõige 2.

724 Europoli tegevust selles valdkonnas on auditeerinud Europoli ühine järelevalveasutus.

USA rahandusministeerium tohib SWIFTilt saadud andmetest pärit teavet edastada USAs või mujal asuvatele teatud õiguskaitse-, avaliku julgeoleku või terrorismivastase võitluse ametiasutustele üksnes terrorismi või selle rahastamise tõkestamise, uurimise või avastamise või nende eest kohtulikule vastutusele võtmise eesmärgil. Kui kavatsetakse edastada 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, kui andmete jagamine on äärmiselt vajalik avalikku julgeolekut ähvardava vahetu ja raske ohu ennetamiseks.

SWIFT-lepingu põhimõtete järgimise järelevalvet teevad sõltumatud järelevaatajad, sealhulgas Euroopa Komisjoni määratud isik. Neil on võimalus reaalajas ja tagasiulatuvalt läbi vaadata kõik esitatud andmetega tehtud otsingud, nõuda lisateavet, mis põhjendab nende otsingute seost terrorismiga, ja volitus blokeerida kõik otsingud, mis näivad olevat vastuolus lepingus sätestatud kaitsemeetmetega.

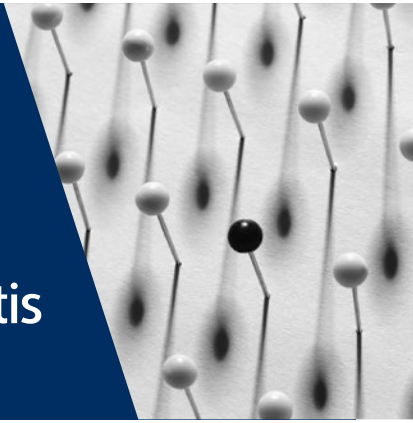
Andmesubjektidel on õigus saada pädevalt ELi järelevalveasutuselt kinnitus, kas andmete kasutamisel on austatud nende isikuandmete kaitsega seotud õigusi. Samuti on andmesubjektidel õigus lasta parandada, kustutada või sulgeda andmed, mida USA rahandusministeerium nende kohta SWIFT-lepingu alusel on kogunud ja säilitab. Andmesubjektide õiguse suhtes andmetega tutvuda võidakse teatud 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, esimene kehtivusperiood kestis 2015. aasta augustini. Leping pikeneb edasi automaatselt ühe aasta kaupa, kui üks lepinguosalistest ei teata teisele lepinguosalisele kirjalikult vähemalt kuus kuud ette, et ta ei kavatse lepingut enam pikendada. Automaatset pikendamist kohaldati augustis 2015, 2016 ja 2017 ning sellega tagatakse SWIFT-lepingu kehtivus vähemalt 2018. aasta augustini[725].

725 *Ibid.*, artikli 23 lõige 2.

8

Andmekaitse politsei ja kriminaalõiguse kontekstis



EL	Teemad	EN
Politsei- ja kriminaalõigusasutuste andmekaitse direktiiv	Üldine	Nüüdisajastatud konventsioon nr 108
	Politsei	Politseisoovitus Praktiline juhend isikuandmete kasutamise kohta politseivaldkonnas
	Järelevalve	EIK, *B.B. vs. Prantsusmaa*, nr 5335/06, 2009 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 2008 EIK, *Allan vs. Ühendkuningriik*, nr 48539/99, 2002 EIK, *Malone vs. Ühendkuningriik*, nr 8691/79, 1984 EIK, *Klass jt vs. Saksamaa*, nr 5029/71, 1978 EIK, *Szabó ja Vissy vs. Ungari*, nr 37138/14, 2016 EIK, *Vetter vs. Prantsusmaa*, nr 59842/00, 2005
	Küberkuritegevus	Küberkuritegevuse konventsioon

EL	Teemad	EN
Muud eriõigusaktid		
Prümi otsus	**Eriliiki andmed: sõrmejäljed, DNA, huligaansus, lennureisijate andmed, sideandmed jt.**	Nüüdisajastatud konventsiooni nr 108 artikkel 6 Politseisoovitus, praktiline juhend isikuandmete kasutamise kohta politseivaldkonnas
Rootsi algatus (nõukogu raamotsus 2006/960/JSK)	**Õiguskaitseasutuste vahel teabe ja jälitusteabe vahetamise lihtsustamine**	EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 2008
Direktiiv (EL) 2016/681, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland* ja *Kärntner Landesregierung jt* [suurkoda], 2014 ELK, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige* ja *Home Department vs. Tom Watson jt* [suurkoda], 2016	**Isikuandmete säilitamine**	EIK, *B.B. vs. Prantsusmaa*, nr 5335/06, 2009
Europoli määrus Eurojusti otsus	**Eriasutustes**	Politseisoovitus
Teise põlvkonna Schengeni infosüsteemi otsus Viisainfosüsteemi määrus Eurodaci määrus Tolliinfosüsteemi otsus	**Eriotstarbelistes ühistes infosüsteemides**	Politseisoovitus EIK, *Dalea vs. Prantsusmaa*, nr 964/07, 2010

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 Euroopa Liit kehtestanud eriõigusaktid. Siin peatükis on ülevaade Euroopa Nõukogu õigusest (peatükk 8.1) ja ELi õigusest (peatükk 8.2) seoses andmekaitsega politsei- ja kriminaalõiguse valdkonnas.

8.1. Euroopa Nõukogu õigusaktid andmekaitse ja riigi julgeoleku, politsei- ja kriminaalõiguse kohta

Põhipunktid

- Politseitegevuse kõigi valdkondade andmekaitse suhtes kohaldatakse nüüdisajastatud konventsiooni nr 108 ja Euroopa Nõukogu politseisoovitust.
- Küberkuritegevuse konventsioon (Budapesti konventsioon) on siduv rahvusvaheline õigusakt, milles käsitletakse elektrooniliste võrkude vastu või nende abil sooritatud kuritegusid. See on oluline ka selliste muude kui küberkuritegude uurimisel, mille kohta on elektroonilisi tõendeid.

Üks Euroopa Nõukogu ja ELi õiguse olulisi erinevusi on, et teisiti kui ELi õiguses, kohaldatakse **Euroopa Nõukogu õigust** ka riigi julgeoleku valdkonnas. See tähendab, et konventsiooniosalised peavad järgima Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8 ka riigi julgeolekuga seotud tegevuses. Mitmes Euroopa Inimõiguste Kohtu (EIK) otsuses käsitletakse riigi tegevust riigi julgeoleku õigusaktide ja -tava tundlikes valdkondades[726].

Politsei- ja kriminaalõigusega seoses hõlmab Euroopa tasandil nüüdisajastatud konventsioon nr 108 kõiki isikuandmete töötlemise valdkondi ning konventsiooni sätete eesmärk on reguleerida isikuandmete üldist töötlemist. Seega kohaldatakse nüüdisajastatud konventsiooni nr 108 andmekaitse suhtes politsei- ja kriminaalõiguse valdkonnas. Geneetiliste andmete, süütegude, kriminaalmenetluste ja süüdimõistvate kohtuotsuste ning nendega kaasnevate turvameetmetega seotud isikuandmete, isiku kordumatuks tuvastamiseks kasutatavate biomeetriliste andmete ja mis tahes eriliiki isikuandmete töötlemine on lubatud ainult siis, kui on olemas asjakohased kaitsemeetmed riskide vastu, mida selliste andmete töötlemine võib tekitada andmesubjekti huvidele, õigustele ja põhivabadustele; eelkõige diskrimineerimise riski vastu[727].

726 Vt näiteks EIK, *Klass jt vs. Saksamaa*, nr 5029/71, 6. september 1978; EIK, *Rotaru vs. Rumeenia* [suurkoda], nr 28341/95, 4. mai 2000; EIK, *Szabó ja Vissy vs. Ungari*, nr 37138/14, 12. jaanuar 2016.

727 Nüüdisajastatud konventsiooni nr 108 artikkel 6.

Politsei- ja kriminaalõigusasutustel on oma juriidilisi ülesandeid täites sageli vaja töödelda isikuandmeid, millega võivad asjaomastele isikutele kaasneda rasked tagajärjed. Politseisoovituses, mille Euroopa Nõukogu võttis vastu 1987. aastal, antakse Euroopa Nõukogu liikmesriikidele juhised, kuidas rakendada konventsiooni nr 108 põhimõtteid politseiasutustes isikuandmete töötlemise kontekstis[728]. Soovitust täiendati praktilise juhendiga isikuandmete kasutamise kohta politseivaldkonnas, mille võttis vastu konventsiooni nr 108 nõuandekomitee[729].

Näide: kohtuasi *D.L. vs. Bulgaaria*[730] käsitles juhtumit, kus sotsiaalteenuste ametiasutus paigutas kaebuse esitaja kohtumääruse alusel kinnisesse kasvatusasutusse. Asutus jälgis üldiselt ja valimatult kogu kirjavahetust ja kõiki telefonivestlusi. Euroopa Inimõiguste Kohus leidis, et artiklit 8 rikuti, sest see meede ei olnud demokraatlikus ühiskonnas vajalik. Kohus märkis, et tuleb teha kõik, et võimaldada asutuses viibivatele alaealistele piisavat kontakti välismaailmaga, sest see on lahutamatu osa nende õigusest väärikale kohtlemisele ja hädavajalik nende ühiskonda taasintegreerimise ettevalmistamisel. See kehtib nii külastuste kui ka kirjavahetuse või telefonivestluste kohta. Lisaks ei eristatud järelevalves suhtlemist pereliikmete ja laste õigusi esindavate vabaühenduste või juristidega. Peale selle ei põhinenud suhtluse pealtkuulamise otsus iga konkreetse juhtumi riskide individuaalsel analüüsil.

Näide: kohtuasi *Dragojević vs. Horvaatia*[731] käsitles juhtumit, kus kaebuse esitajat kahtlustati seotuses ebaseadusliku uimastikaubandusega. Ta tunnistati süüdi pärast seda, kui eeluurimiskohtunik andis loa kasutada salajase jälgimise meetmeid kaebuse esitaja telefonikõnede pealtkuulamiseks. Euroopa Inimõiguste Kohus leidis, et meede, mille vastu kaebus esitati, oli sekkumine õigusesse eraelu ja sõnumisaladuse austamisele. Eeluurimiskohtuniku antud luba põhines üksnes prokuratuuri kinnitusel, et „uurimist ei saa läbi viia muude vahenditega". EIK märkis ka, et kriminaalkohtud olid piiranud oma hinnangut jälgimismeetmete kasutamise kohta ja valitsus ei pakkunud kättesaadavaid õiguskaitsevahendeid. Seega rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

728 Euroopa Nõukogu ministrite komitee (1987), *Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector*, 17. september 1987.

729 Euroopa Nõukogu (2018), Konventsiooni nr 108 nõuandekomitee, *Practical Guide on the use of personal data in the police sector*, T-PD(2018)1.

730 EIK, *D.L. vs. Bulgaaria*, nr 7472/14, 19. mai 2016.

731 EIK, *Dragojević vs. Horvaatia*, nr 68955/11, 15. jaanuar 2015.

8.1.1. Politseisoovitus

EIK on mitmes kohtuasjas järeldanud, et isikuandmete salvestamise ja säilitamisega politseiasutustes ja riigi julgeoleku asutustes sekkuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikega 1 tagatud õiguste kasutamisse. Sellise sekkumise põhjendatust käsitletakse paljudes Euroopa Inimõiguste Kohtu otsustes[732].

Näide: kohtuasi *B.B. vs. Prantsusmaa*[733] käsitles juhtumit, kus kaebuse esitaja mõisteti süüdi seksuaalkuritegudes 15-aastaste alaealiste vastu isikuna, kellel on lapsega usaldussuhe. Tema vanglakaristus lõppes 2000. aastal. Aasta hiljem esitas ta taotluse karistuse kustutamiseks karistusregistrist, kuid taotlus lükati tagasi. 2004. aastal loodi Prantsusmaal seadusega seksuaalkurjategijate riiklik kohtute hallatav andmebaas ja taotlejale teatati, et ta on sinna kantud. Euroopa Inimõiguste Kohus leidis, et süüdimõistetud seksuaalkurjategija andmete sisestamine riiklikku kohtute hallatavasse andmebaasi kuulub Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 kohaldamisalasse. Samas kui rakendati piisavaid andmekaitsetagatisi, näiteks andmesubjekti õigust taotleda andmete kustutamist, andmete säilitamise tähtaja piiramist ning piiratud juurdepääsu asjaomastele andmetele, saavutati asjaomaste konkureerivate isiklike huvide ja avalike huvide õiglane tasakaal. Kohus järeldas, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8 ei rikutud.

Näide: kohtuasi *S. ja Marper vs. Ühendkuningriik*[734] käsitles juhtumit, kus mõlemat kaebuse esitajat süüdistati kuritegudes, kuid ei mõistetud süüdi. Politsei hoidis siiski alles ja säilitas nende sõrmejäljed, rakuproovid ja DNA-profiilid. Nimetatud 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 eristamatu säilitamisega, millel puudub selge tähtaeg ja süüdistustest vabastatud isikutel oli keeruline taotleda andmete kustutamist, sekkuti ebaproportsionaalselt kaebuse esitajate õigusesse eraelu austamisele. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

732 Vt näiteks 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, või EIK, *Aycaguer vs. Prantsusmaa*, nr 8806/12, 22. juuni 2017.

733 EIK, *B.B. vs. Prantsusmaa*, nr 5335/06, 17. detsember 2009.

734 EIK, *S. ja Marper vs. Ühendkuningriik* [suurkoda], nr 30562/04 ja nr 30566/04, 4. detsember 2008, punktid 119 ja 125.

Elektroonilise side kontekstis on otsustava tähtsusega riigiasutuste sekkumine õigusesse eraelu puutumatusele ja andmekaitsele. Sidevahendite jälgimise või pealtkuulamise vahendid (nt pealtkuulamisseadmed) on lubatud ainult siis, kui need on sätestatud seaduses ja kui need on demokraatlikus ühiskonnas vajalik meede, mis teenib järgmisi huve:

- riigi julgeoleku kaitse;
- avalik julgeolek;
- riigi rahalised huvid;
- kuritegude tõkestamine või
- andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse.

Paljud muud EIK otsused käsitlevad varjatud jälgimise kaudu isikuandmete kaitse õigusesse sekkumise põhjendusi.

Näide: kohtuasi *Allan vs. Ühendkuningriik*[735] käsitles juhtumit, kus ametiasutused salvestasid salaja kinnipeetava isiklikke vestlusi sõbraga vangla külastusalal ja kaassüüdistatavaga vanglakambris. EIK leidis, et heli- ja videosalvestusseadmete kasutamist kaebuse esitaja kambris ja vangla külastusalal ning kaasvangi abiga võib käsitada sekkumisena kaebuse esitaja õigusesse eraelu austamisele. Et sel ajal puudus varjatud salvestusseadmete politseis kasutamise õigusraamistik, ei olnud sekkumine kooskõlas õigusaktidega. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Näide: kohtuasi *Roman Zakharov vs. Venemaa*[736] käsitles juhtumit, kus taotluse esitaja kaebas kohtusse kolm mobiilsideoperaatorit. Ta väitis, et on rikutud tema õigust telefonivestluste privaatsusele, sest operaatorid olid paigaldanud seadmeid, mis võimaldasid föderaalsel turvateenistusel tema telefonivestlusi kuulata pealt ilma kohtu eelneva loata. Euroopa Inimõiguste Kohus leidis, et side pealtkuulamist reguleerivad riigisisesed õigussätted ei taga piisavaid ja tõhusaid tagatisi meelevaldsuse ja kuritarvitamise riski

735 EIK, *Allan vs. Ühendkuningriik*, nr 48539/99, 5. november 2002.

736 EIK, *Roman Zakharov vs. Venemaa* [suurkoda], nr 47143/06, 4. detsember 2015.

vastu. Eelkõige ei nõutud riigisiseses õiguses, et säilitatavad andmed kustutataks pärast säilitamise eesmärgi täitmist. Kuigi kohtu luba oli nõutav, oli kohtulik kontroll vähene.

Näide: kohtuasjas *Szabó ja Vissy vs. Ungari*[737] väitsid hagejad, et Ungari õigusaktid on vastuolus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8. Peale selle väideti, et õigusaktid ei paku kuritarvitamise ja omavoli vastu piisavaid tagatisi. Euroopa Inimõiguste Kohus leidis, et Ungari õiguses ei nõuta jälgimiseks kohtu luba. Kohus märkis siiski, et kuigi jälgimise pidi heaks kiitma justiitsminister, oli see järelevalve äärmiselt poliitiline ega suutnud tagada „range vajalikkuse" põhimõttega nõutavat hindamist. Lisaks ei sätestanud riigisisene õigus kohtulikku kontrolli, arvestades, et asjaomastele isikutele ei saadetud teateid. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Et andmete töötlemine politseiasutustes võib asjaomaseid isikuid oluliselt mõjutada, on isikuandmete töötlemise üksikasjalikud andmekaitse-eeskirjad eriti vajalikud. Euroopa Nõukogu politseisoovituses käsitleti seda teemat järgmiste soovitustega: kuidas koguda isikuandmeid politsei töö jaoks; kuidas säilitada andmefaile; kellel peaks olema juurdepääs andmetele, sealhulgas isikuandmete välisriikide politseiasutustele edastamise tingimused; kuidas peaksid andmesubjektid saama kasutada andmekaitseõigusi; kuidas rakendada sõltumatute ametiasutuste tehtavat kontrolli. Samuti käsitleti soovituses kohustust tagada piisav andmeturve.

Soovitusega ei sätestata, et politseiasutused võivad isikuandmeid koguda piiramatult ja valimatult. Soovituse kohaselt peavad politseiasutuste kogutavad isikuandmed piirduma andmetega, mida on vaja reaalse ohu vältimiseks või konkreetse kuriteo eest vastutusele võtmiseks. Täiendav andmete kogumine peab põhinema riigisisestel eriõigusaktidel. Delikaatsete andmete töötlemine peab piirduma konkreetse uurimise kontekstis absoluutselt vajalikuga.

Kui isikuandmeid kogutakse andmesubjekti teadmata, tuleb andmesubjekti sellest teavitada kohe, kui andmete avaldamine ei kahjusta enam uurimist. Andmete kogumine tehniliste seiresüsteemide või muude automaatvahendite abil peab põhinema konkreetsele õigsulikule alusele.

737 EIK, *Szabó ja Vissy vs. Ungari*, nr 37138/14, 12. jaanuar 2016.

Näide: kohtuasi *Versini-Campinchi ja Crasnianski vs. Prantsusmaa*[738] käsitles juhtumit, kus kaebuse esitaja (advokaat) vestles telefoni teel kliendiga, kelle telefoni kuulati eeluurimiskohtuniku taotlusel pealt. Vestluse üleskirjutusest nähtus, et advokaat avalikustas kutsesaladusega kaitstud teavet. Prokurör saatis selle teabe advokatuurile, kes määras kaebuse esitajale karistuse. Euroopa Inimõiguste Kohus tõdes eraelu ja sõnumisaladuse austamise õiguse riivet mitte ainult seoses isikuga, kelle telefoni pealt kuulati, vaid ka seoses kaebuse esitajaga, kelle suhtlust pealt kuulati ja üles kirjutati. Sekkumine toimus kooskõlas seadusega ja järgiti korrakaitse õiguspärast eesmärki. Kaebuse esitaja suhtes algatatud distsiplinaarmenetluse raames saavutas kaebuse esitaja, et kontrolliti telefonikõnede pealtkuulamise salvestiste üleskirjutiste seaduslikkust. Kuigi ta ei saanud taotleda telefonivestluse üleskirjutise tühistamist, leidis Euroopa Inimõiguste Kohus, et kontroll oli tõhus ja sellega sai piirata kaebuses käsitletud sekkumist demokraatliku ühiskonna jaoks vajalikuga. EIK leidis, et väide, et võimalus algatada advokaadi vastu üleskirjutuse alusel kriminaalmenetlus võib halvata juristi ja tema kliendi teabevahetusvabadust ning seega ka viimase kaitseõigust, ei ole usutav, kui advokaadi avaldatud teave võib tuleneda advokaadi ebaseaduslikust käitumisest. Seega artikli 8 rikkumist ei tuvastatud.

Euroopa Nõukogu politseisoovituses sätestatakse, et isikuandmete säilitamisel tuleb selgelt eristada haldus- ja politseiandmeid, andmesubjektide eri kategooriate (nt kahtlustatavad, süüdimõistetud, kannatanud ja tunnistajad) isikuandmeid ning faktideks peetavaid andmeid ja kahtlustel või oletustel põhinevaid andmeid.

Politseiandmete kasutamise eesmärk peab olema rangelt piiratud. See mõjutab politseiandmete avalikustamist kolmandatele isikutele: selliste andmete avalikustamine või nendest teatamine väljaspool politseisektorit peaks olema lubatud üksnes siis, kui selleks on selgesõnaline õiguslik kohustus või luba. Selliste andmete edastamine või avalikustamine väljaspool politseisektorit võib olla lubatud ainult siis, kui selleks on selge juriidiline kohustus või luba.

Näide: kohtuasi *Karabeyoğlu vs. Türgi*[739] käsitles juhtumit, kus kaebuse esitaja (kohtunik) telefoniliine jälgiti kriminaaluurimises ebaseadusliku organisatsiooni suhtes, millesse kuulumises teda kahtlustati või mille abistajaks ja toetajaks teda peeti. Pärast otsust süüdistust mitte esitada hävitas

738 EIK, *Versini-Campinchi ja Crasnianski vs. Prantsusmaa*, nr 49176/11, 16. juuni 2016.

739 EIK, *Karabeyoğlu vs. Türgi*, nr 30083/10, 7. juuni 2016.

kriminaaluurimise eest vastutav prokurör salvestised. Üks koopia jäi siiski uurijate valdusse, kes kasutasid seda hiljem tõendusmaterjalina kaebuse esitaja suhtes algatatud distsiplinaarmenetluses. Euroopa Inimõiguste Kohus leidis, et asjakohaseid õigusakte on rikutud, sest teavet kasutati muul eesmärgil kui see, milleks see oli kogutud, ning seda ei hävitatud ettenähtud tähtaja jooksul. Sekkumine kaebuse esitaja õigusesse eraelu austamisele ei olnud tema suhtes algatatud distsiplinaarmenetluse korral kooskõlas seadusega.

Andmete rahvusvaheline edastamine või avalikustamine peaks piirduma üksnes välisriikide politseiasutustega ning põhinema erisätetel ja ka rahvusvahelistel lepingutel, v.a kui seda on vaja raske ja vahetu ohu takistamiseks.

Andmete töötlemist politseis peab riigisisese andmekaitseõiguse järgimise tagamiseks kontrollima sõltumatu järelevalveasutus. Andmesubjektidel peavad olema kõik nüüdisajastatud konventsioonis nr 108 sätestatud õigused andmetega tutvuda. Kui andmesubjektide õigust andmetega tutvuda on piiratud konventsiooni nr 108 artikli 9 alusel tõhusa politseiuurimise ja kriminaalkaristuste täideviimise huvides, peab andmesubjektil kooskõlas riigi õigusaktidega olema õigus esitada kaebus riigi andmekaitse järelevalveasutusele või muule sõltumatule asutusele.

8.1.2. Küberkuritegevuse Budapesti konventsioon

Ajal, kui kuritegevuses kasutatakse või kahjustatakse üha rohkem elektroonilisi andmetöötlussüsteeme, on selle vastu vaja uusi kriminaalõiguse sätteid. Euroopa Nõukogu võttis sel põhjusel vastu rahvusvahelise õigusakti – küberkuritegevuse konventsiooni (Budapesti konventsiooni) –, et käsitleda elektrooniliste võrkude vastu ja nende kaudu sooritatud kuritegude probleemi[740]. Konventsiooniga võivad ühineda ka muud riigid kui Euroopa Nõukogu liikmesriigid. 2018. aasta alguseks oli konventsiooniga ühinenud 14 Euroopa Nõukogu välist riiki[741] ja ühinema oli kutsutud veel 7 mitteliikmesriiki.

Küberkuritegevuse konventsioon on siiani kõige olulisem rahvusvaheline leping, milles käsitletakse internetis või muudes rahvusvahelistes võrkudes sooritatud õigusrikkumisi. Selle alusel peavad konventsiooniosalised ajakohastama ja ühtlustama

740 Euroopa Nõukogu ministrite komitee (2001), arvutikuritegevusvastane konventsioon, CETS nr 185, Budapest, 23. november 2001, jõustus 1. juulil 2004.

741 Ameerika Ühendriigid, Austraalia, Colombia, Dominikaani Vabariik, Iisrael, Jaapan, Kanada, Mauritius, Panama, Senegal, Sri Lanka, Tonga, Tšiili ja Tuneesia. Vt lepingu nr 185 allkirjastamise ja ratifitseerimise tabel (seisuga juuli 2017).

oma kriminaalseadustikku, mis käsitleb häkkimist ja muid turvarikkumisi, sealhulgas autoriõiguse rikkumist, arvuti abil sooritatud pettusi, lapspornot ja muud ebaseaduslikku kübertegevust. Samuti sätestatakse konventsioonis menetluspädevused, kuidas teha läbiotsimisi arvutivõrkudes ja kuulata pealt sidevahendeid küberkuritegevuse vastu võitlemisel. Konventsioon võimaldab ka tõhusat rahvusvahelist koostööd. Konventsiooni lisaprotokollis tunnistatakse kuritegelikuks rassistlik ja ksenofoobne propaganda arvutivõrkudes.

Kuigi konventsiooni otsene eesmärk ei ole edendada andmekaitset, tunnistatakse sellega kuritegelikuks tegevus, millega võidakse rikkuda andmesubjekti õigust isikuandmete kaitsele. Lisaks sellele nõutakse konventsioonis, et konventsiooniosalised võtaksid õiguslikke meetmeid, et võimaldada riigisisestel ametiasutustel jälgida andmeliiklust ja sisuandmeid[742]. Samuti on konventsiooniga osalisriikidele ette nähtud kohustus, et konventsiooni rakendamisel tuleb tagada inimõiguste ja vabaduste, sealhulgas Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist tulenevate õiguste piisav kaitse, näiteks õigus andmekaitsele[743]. Budapesti konventsiooniga ühinemisel ei kaasne konventsiooniosalistele kohustust ühineda ka konventsiooniga nr 108.

8.2. Politsei- ja kriminaalõiguse valdkonna andmekaitsega seotud ELi õigusaktid

Põhipunktid

- ELis reguleeritakse politsei- ja kriminaalõiguse valdkonna andmekaitset nii liikmesriikide politsei- ja kriminaalõiguse asutuste kui ka ELi osalejate riigisisese ja piiriülese koostöö kontekstis.
- Liikmesriikide tasandil tuleb riigisisesesse õigusesse üle võtta politsei- ja kriminaalõigusasutuste andmekaitse direktiiv.
- Andmekaitset politsei- ja õiguskaitse valdkonna piiriüleses koostöös, eelkõige terrorismi ja piiriülese kuritegevuse vastases võitluses reguleeritakse eriõigusaktidega.

742 Euroopa Nõukogu ministrite komitee (2001), Küberkuritegevuse konventsioon, CETS nr 185, Budapest, 23. november 2001, artiklid 20 ja 21.

743 *Ibid.*, artikli 15 lõige 1.

- Eraldi andmekaitse-eeskirjad on piiriülest õiguskaitset toetavatel ja edendavatel ELi asutusel – Euroopa Politseiametil (Europol), Euroopa Õigusalase Koostöö Üksusel (Eurojust) ja hiljuti asutatud Euroopa Prokuratuuril.
- Olemas on andmekaitse erieeskirjad ka ELi tasandi pädevate politsei- ja õigusasutuste vahelise piiriülese teabevahetuse ühiste teabesüsteemide jaoks. Need on eelkõige teise põlvkonna Schengeni infosüsteem (SIS II), viisainfosüsteem (VIS) ning Eurodac (kesksüsteem, milles säilitatakse ELi liikmesriikides varjupaika taotlevate kolmandate riikide kodanike ja kodakondsuseta isikute sõrmejäljeandmeid).
- EL ajakohastab eespool nimetatud andmekaitsesätteid, et need oleksid kooskõlas politsei- ja kriminaalõigusasutuste andmekaitse direktiivi sätetega.

8.2.1. Politsei- ja kriminaalõigusasutuste andmekaitse direktiiv

Direktiiviga (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist (politsei- ja kriminaalõigusasutuste andmekaitse direktiiv),[744] taotletakse eesmärki kaitsta isikuandmeid, mida kogutakse ja töödeldakse kriminaalõiguse eesmärkidel, muu hulgas järgmiseks:

- süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine;
- kriminaalkaristuste täideviimine ning
- juhud, kui politsei- või muud õiguskaitseasutused tegutsevad eesmärgiga järgida seadust ning kaitsta avalikku julgeolekut ja ühiskonna põhiõigusi ähvardavate ohtude eest, mis võivad olla kuritegu, ja neid ennetada.

Politsei- ja kriminaalõigusasutuste andmekaitse direktiiv kaitseb kriminaalmenetluses osalevate isikute eri kategooriate, nt tunnistajate, teabe esitajate, kannatanute,

744 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, ELT 2016 L 119, lk 89 (politsei- ja kriminaalõigusasutuste andmekaitse direktiiv).

kahtlustatavate ja kaasosaliste isikuandmeid. Politsei- ja kriminaalõiguse valdkonna asutused on kohustatud järgima direktiivi sätteid, kui nad töötlevad selliseid isikuandmeid õiguskaitse eesmärgil nii direktiivi isikulise kui ka materiaalse kohaldamisala raames[745].

Teatud tingimustel on lubatud kasutada andmeid ka muul eesmärgil. Andmete töötlemine teistsugusel õiguskaitse eesmärgil kui see, milleks andmed koguti, on lubatud ainult siis, kui see on seaduslik, vajalik ja riigisisese või ELi õiguse kohaselt proportsionaalne[746]. Muude eesmärkide suhtes kohaldatakse isikuandmete kaitse üldmääruse eeskirju. Andmete jagamise registreerimine ja dokumenteerimine on üks pädevate asutuste konkreetseid kohustusi, et aidata selgitada, mis kohustused kaasnevad kaebustega.

Politsei- ja kriminaalõiguse valdkonna pädevad asutused on avaliku sektori asutused, samuti asutused, kellele on riigisisese õiguse ja avaliku võimu poolt antud volitused täita avaliku võimu ülesandeid,[747] nt eravanglad[748]. Direktiivi kohaldatavus hõlmab nii andmete töötlemist riigisisesel tasandil kui ka piiriülest töötlemist liikmesriikide politsei- ja õigusasutuste vahel, samuti pädevate asutuste tehtud rahvusvahelisi andmeedastusi kolmandatele riikidele ja rahvusvahelistele organisatsioonidele[749]. See ei hõlma riigi julgeolekut ega isikuandmete töötlemist ELi institutsioonides, organites ja asutustes[750].

Direktiiv tugineb suures ulatuses isikuandmete kaitse üldmääruses sisalduvatele põhimõtetele ja määratlustele, arvestades politsei- ja kriminaalõiguse valdkondade eripära. Järelevalvet võivad teha samad liikmesriikide ametiasutused, kes teevad seda ka isikuandmete kaitse üldmääruse alusel. Politsei- ja kriminaalõigusasutuste uute kohustustena on direktiivi lisatud andmekaitseametnike määramine ja

745 Politsei- ja kriminaalõigusasutuste andmekaitse direktiivi artikli 2 lõige 1.

746 *Ibid.*, artikli 4 lõige 2.

747 *Ibid.*, artikli 3 lõige 7.

748 Euroopa Komisjon (2016), komisjoni teatis Euroopa Parlamendile, mis on esitatud Euroopa Liidu toimimise lepingu artikli 294 lõike 6 alusel ning milles käsitletakse nõukogu seisukohta seoses Euroopa Parlamendi ja nõukogu direktiivi (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) vastuvõtmisega ja nõukogu raamotsuse 2008/977/JSK kehtetuks tunnistamisega, COM(2016) 213 final, Brüssel, 11. aprill 2016.

749 Politsei- ja kriminaalõigusasutuste andmekaitse direktiivi V peatükk.

750 *Ibid.*, artikli 2 lõige 3.

andmekaitse mõju hindamine[751]. Kuigi need mõisted lähtuvad isikuandmete kaitse üldmäärusest, käsitletakse direktiivis politsei- ja kriminaalõigusasutuste eripära. Võrreldes töötlemisega kaubanduslikul eesmärgil, mida reguleerib määrus, võib turvalisusega seotud töötlemine nõuda teatud paindlikkust. Näiteks võib andmesubjektidele samaväärse kaitse taseme tagamine seoses õigusega saada teavet, oma andmetega tutvuda või need kustutada, nagu on sätestatud isikuandmete kaitse üldmääruses, tähendada, et õiguskaitse eesmärgil tehtav mis tahes järelevalvetoiming muutub õiguskaitse kontekstis ebatõhusaks. Sel põhjusel puudub direktiivis läbipaistvuse põhimõte. Samamoodi tuleb turvalisusega seotud töötlemisel paindlikult kohaldada ka võimalikult väheste andmete kogumise ja eesmärgi piirangu põhimõtet, millega nõutakse, et isikuandmete töötlemine piirduks üksnes sellega, mida on vaja töötlemise eesmärkide saavutamiseks, ning neid töödeldaks täpselt ja selgelt kindlaksmääratud eesmärkidel. Pädevate asutuste konkreetsel juhul kogutud ja säilitatud teavet võidakse pidada tulevaste juhtumite lahendamisel väga kasulikuks.

Töötlemise põhimõtted

Politsei- ja kriminaalõigusasutuste andmekaitse direktiivis on sätestatud mõni peamine isikuandmete kasutamise kaitsemeede. Selles sõnastatakse ka nende andmete töötlemise põhimõtted. Liikmesriigid peavad tagama, et

- isikuandmeid töödeldakse seaduslikult ja õiglaselt;
- isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda viisil, mis on nende eesmärkidega vastuolus;
- isikuandmed on piisavad, asjakohased ja täpsed ning ei ületa selle otstarbe piire, milleks neid töödeldakse;
- isikuandmed on õiged, vajaduse korral ajakohastatud; võetakse kõik mõistlikud meetmed, et viivitamata kustutada või parandada andmete töötlemise eesmärgi seisukohast ebaõiged isikuandmed;
- isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada, ainult seni, kuni seda on vaja andmete töötlemise eesmärgi jaoks;

751 *Ibid.*, vastavalt artiklis 32 ja artiklis 27.

- isikuandmeid töödeldakse viisil, mis tagab nende nõuetekohase turvalisuse, sealhulgas kaitse volitamata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid[752].

Direktiivi kohaselt on töötlemine õiguspärane ainult siis, kui seda tehakse asjaomase ülesande täitmiseks vajalikus ulatuses. Lisaks peab isikuandmeid töötlema pädev asutus, et saavutada direktiivis määratletud eesmärgid, ning see peab põhinema ELi või riigisisesel õigusel[753]. Andmeid ei tohi säilitada kauem kui vaja ja need tuleb teatud tähtaja möödumisel kustutada või regulaarselt läbi vaadata. Andmeid tohib kasutada üksnes pädev asutus ning ainult eesmärgil, mille jaoks need koguti, edastati või kättesaadavaks tehti.

Andmesubjekti õigused

Direktiivis kehtestatakse ka andmesubjekti õigused, muu hulgas järgmised.

- Õigus saada teavet. Liikmesriigid peavad kohustama vastutavat töötlejat teha andmesubjektile kättesaadavaks 1) vastutava töötleja nimi ja kontaktandmed, 2) andmekaitseametniku kontaktandmed, 3) kavandatud töötlemise eesmärgid, 4) õigus esitada järelevalveasutusele kaebus ja selle kontaktandmed ning 5) õigus isikuandmetega tutvuda, neid parandada või kustutada ning andmete töötlemist piirata[754]. Lisaks nendele üldistele teabenõuetele on direktiivis sätestatud, et teatud juhtudel ja selleks, et võimaldada nende õiguste kasutamist, peavad vastutavad töötlejad andma andmesubjektidele teavet töötlemise õigusliku aluse ja andmete säilitamise aja kohta. Kui isikuandmeid edastatakse teistele vastuvõtjatele, sealhulgas kolmandates riikides või rahvusvahelistes organisatsioonidele, tuleb andmesubjekte selliste vastuvõtjate kategooriatest teavitada. Vastutavad töötlejad peavad ka esitama täiendavat teavet, arvestades andmete töötlemise konkreetseid asjaolusid, näiteks kui isikuandmeid koguti varjatud jälgimisel, st andmesubjekti teadmata. See tagab andmesubjekti suhtes õiglase töötlemise[755].

752 *Ibid.*, artikli 4 lõige 1.

753 *Ibid.*, artikkel 8.

754 *Ibid.*, artikli 13 lõige 1.

755 *Ibid.*, artikli 13 lõige 2.

- Õigus isikuandmetega tutvuda. Liikmesriigid peavad tagama, et andmesubjektil on õigus teada, kas tema isikuandmeid töödeldakse või mitte. Kui töödeldakse, peab andmesubjektil olema juurdepääs teatud teabele, näiteks töödeldavate andmete liikidele[756]. Seda õigust võidakse siiski piirata, näiteks selleks, et hoida ära uurimise või kuriteo eest vastutusele võtmise takistamist või kaitsta avalikku julgeolekut ning teiste isikute õigusi ja vabadusi[757].

- Õigus oma isikuandmeid parandada. Liikmesriigid on kohustatud tagama, et andmesubjekt saab lasta oma isikuandmeid parandada põhjendamatu viivituseta. Lisaks on andmesubjektil õigus lasta ebatäielikke andmeid täiendada[758].

- Õigus isikuandmeid kustutada ja töötlemist piirata. Teatud juhtudel peab vastutav töötleja isikuandmed kustutama. Lisaks sellele võib andmesubjekt tagada oma isikuandmete kustutamise, kuid ainult siis, kui neid töödeldakse ebaseaduslikult[759]. Teatud olukordades võib isikuandmete töötlemist pigem piirata kui isikuandmed kustutada: 1) kui isikuandmete õigsus on vaidlustatud, kuid seda ei saa tõestada, või 2) kui isikuandmeid on vaja tõendite esitamiseks[760].

Kui vastutav töötleja keeldub isikuandmeid parandamast või kustutamast või andmete töötlemist piiramast, tuleb andmesubjekti sellest kirjalikult teavitada. Liikmesriigid võivad teabe saamise õigust piirata muu hulgas avaliku julgeoleku või teiste isikute õiguste ja vabaduste kaitsmiseks samadel põhjustel nagu juurdepääsuõiguse piiramisel[761].

Andmesubjektil on tavaliselt õigus saada teavet oma isikuandmete töötlemise kohta ja nende andmetega tutvuda ning õigus lasta andmeid parandada või töötlemispiirang tühistada, mida ta võib teha, pöördudes otse vastutava töötleja poole. Abinõuna on võimalik ka andmesubjektide õiguste kaudne teostamine andmekaitse järelevalveasutuse kaudu politsei- ja kriminaalõiguse valdkonna asutuste andmekaitse direktiivi alusel ning seda kohaldatakse siis, kui vastutav töötleja piirab andmesubjekti õigust[762]. Direktiivi artiklis 17 on nõutud, et liikmesriigid võtaksid

756 *Ibid.*, artikkel 14.
757 *Ibid.*, artikkel 15.
758 *Ibid.*, artikli 16 lõige 1.
759 *Ibid.*, artikli 16 lõige 2.
760 *Ibid.*, artikli 16 lõige 3.
761 *Ibid.*, artikli 16 lõige 4.
762 *Ibid.*, artikkel 17.

meetmeid, millega tagatakse, et andmesubjektide õigusi võib teostada ka nende järelevalveasutuse kaudu. See ongi põhjus, miks peab vastutav töötleja teavitama andmesubjekti võimalikust kaudsest juurdepääsust andmetele.

Vastutavate ja volitatud töötlejate kohustused

Politsei- ja kriminaalõigusasutuste andmekaitse direktiivi kontekstis on andmete vastutavad töötlejad pädevad riiklikud asutused või muud asutused, kellel on asjakohased avalikud volitused ja kes teostavad avalikku võimu ning määravad isikuandmete töötlemise eesmärgid ja vahendid. Direktiiviga on andmete vastutavatele töötlejatele kehtestatud mitu kohustust tagada õiguskaitse eesmärgil töödeldavate isikuandmete kõrgetasemeline kaitse.

Pädevad asutused peavad pidama automaattöötlemissüsteemides tehtavate töötlemistoimingute logisid. Logisid tuleb pidada vähemalt isikuandmete kogumise, muutmise, nendega tutvumise, avalikustamise, sealhulgas edastamise, ühendamise ja kustutamise kohta[763]. Direktiivis on sätestatud, et andmetega tutvumise ja andmete avalikustamise logid peavad võimaldama määrata toimingute kuupäeva ja kellaaja, põhjuse ja võimaluse korral süsteemi kasutanud või isikuandmeid avalikustanud isiku ning asjaomaste isikuandmete vastuvõtjad. Logisid tuleb kasutada üksnes töötlemise seaduslikkuse kontrollimiseks, siseseireks, isikuandmete tervikluse ja turvalisuse tagamiseks ning kriminaalmenetluses[764]. Järelevalveasutuse nõudmisel peavad vastutav ja volitatud töötleja tegema logid kättesaadavaks.

Eelkõige on vastutavatel töötlejatel üldine kohustus rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada töötlemine kooskõlas direktiiviga, ja tõendada sellise töötlemise seaduslikkust[765]. Nende meetmete kavandamisel peavad vastutavad töötlejad arvestama töötlemise olemust, ulatust, konteksti ja eelkõige võimalikke riske üksikisikute õigustele ja vabadustele. Vastutavad töötlejad peavad võtma vastu sisepoliitika ja rakendama meetmeid, mis soodustavad andmekaitse põhimõtete, eelkõige lõimitud ja vaikimisi andmekaitse põhimõtete järgimist[766]. Kui töötlemisega tekib isikute õigustele tõenäoliselt suur risk – näiteks uute tehnoloogiate kasutamise tõttu –, peavad vastutavad töötlejad tegema enne töötlemise

763 *Ibid.*, artikli 25 lõige 1.

764 *Ibid.*, artikli 25 lõige 2.

765 *Ibid.*, artikkel 19.

766 *Ibid.*, artikkel 20.

alustamist andmekaitse mõjuhinnangu[767]. Direktiivis on loetletud ka meetmed, mida vastutavad töötlejad peavad võtma töötlemise turvalisuse tagamiseks, sealhulgas meetmed, millega ennetatakse volitamata juurdepääs vastutavate töötlejate töödeldavatele isikuandmetele, tagamaks, et volitatud isikutel on juurdepääs ainult isikuandmetele, mis on hõlmatud nende juurdepääsuõigusega, et töötlemissüsteemi funktsioonid toimivad nõuetekohaselt ja säilitatavaid isikuandmeid ei saa süsteemi rikke tõttu kahjustada[768]. Isikuandmetega seotud rikkumise korral peavad vastutavad töötlejad teavitama järelevalveasutust kolme päeva jooksul, kirjeldades rikkumise olemust, selle võimalikke tagajärgi, asjaomaste isikuandmete liike ja andmesubjektide ligikaudset arvu. Isikuandmetega seotud rikkumisest tuleb teatada „põhjendamatu viivituseta" ka andmesubjektile, kui rikkumine võib tõenäoliselt põhjustada suurt ohtu tema õigustele ja vabadustele[769].

Direktiiv sisaldab vastutuse põhimõtet, millega kohustatakse vastutavaid töötlejaid võtma meetmeid selle põhimõtte järgimise tagamiseks. Vastutavad töötlejad peavad dokumenteerima kõigi nende vastutusalasse kuuluvate töötlemistoimingute kategooriad: selliste dokumentide üksikasjalik sisu on kirjeldatud direktiivi artiklis 24. Dokumendid tuleb järelevalveasutusele nõudmise korral kättesaadavaks teha, et nad saaksid jälgida vastutava töötleja töötlemistoiminguid. Vastutuse suurendamise teine oluline meede on andmekaitseametniku määramine. Vastutavad töötlejad peavad määrama andmekaitseametniku, kuigi direktiiv võimaldab liikmesriikidel sellest kohustusest vabastada kohtud ja muud sõltumatud õigusasutused[770]. Andmekaitseametniku kohustused sarnanevad isikuandmete kaitse üldmääruses sätestatud kohustustega. Andmekaitseametnik jälgib direktiivis määratletud tingimuste täitmist, annab teavet ja nõustab töötajaid, kes töötlevad andmeid andmekaitse õigusaktidest tulenevate kohustuste täitmisel. Andmekaitseametnik annab nõu ka andmekaitse mõjuhinnangu vajaduse kohta ja tegutseb järelevalveasutuse kontaktpunktina.

Edastamine kolmandatele riikidele või rahvusvahelistele organisatsioonidele

Sarnaselt isikuandmete kaitse üldmäärusega on ka direktiivis kehtestatud isikuandmete kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele

767 *Ibid.*, artikkel 27.

768 *Ibid.*, artikkel 29.

769 *Ibid.*, artiklid 30 ja 31.

770 *Ibid.*, artikkel 32.

edastamise tingimused. Isikuandmete piiranguteta edastamine väljapoole ELi jurisdiktsiooni võiks kahjustada ELi õiguses sätestatud kaitsemeetmeid ja tugevat kaitset. Samas erinevad need tingimused isikuandmete kaitse üldmääruse tingimustest. Isikuandmete edastamine kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele on lubatud, kui[771]

- edastamine on vajalik direktiivi eesmärkide täitmiseks;
- isikuandmeid edastatakse kolmanda riigi või rahvusvahelise organisatsiooni pädevale asutusele direktiivi tähenduses, kuigi üksik- ja erijuhtudel on sellest reeglist olemas erand[772];
- piiriüleses koostöös saadud isikuandmeid võib kolmandatele riikidele või rahvusvahelistele organisatsioonidele edastada üksnes selle liikmesriigi loal, kellelt andmed saadi, kuigi pakilistel juhtudel võidakse teha erandeid;
- Euroopa Komisjon on teinud kaitse piisavuse otsuse, kehtestatud on asjakohased kaitsemeetmed ja konkreetsetes olukordades kohaldatakse andmete edastamise erandeid;
- isikuandmete edasiseks edastamiseks muule kolmandale riigile või rahvusvahelisele organisatsioonile on vaja eelnevat luba andmete päritoluliikmesriigi pädevalt asutuselt, kes muu hulgas arvestab kuriteo raskust ja andmekaitse taset teise rahvusvahelise edastuse sihtriigis[773].

Direktiivi kohaselt võib isikuandmeid edastada, kui täidetud on üks kolmest tingimusest. Esimene tingimus on täidetud, kui Euroopa Komisjon on direktiivi alusel teinud kaitse piisavuse otsuse. Otsus võib kehtida kogu kolmanda riigi territooriumi või selle teatud valdkondade või rahvusvahelise organisatsiooni suhtes. Seda saab teha siiski ainult siis, kui on tagatud piisav kaitse ja direktiivis määratletud tingimused on täidetud[774]. Sellisel juhul ei ole isikuandmete edastamiseks liikmesriigi luba vaja[775]. Euroopa Komisjon peab jälgima arenguid, mis võivad mõjutada kaitse piisavuse otsuse toimimist. Lisaks peab otsus sisaldama korrapärase läbivaatamise

771 *Ibid.*, artikkel 35.

772 *Ibid*, artikkel 39.

773 *Ibid.*, artikli 35 lõige 1.

774 *Ibid.*, artikkel 36.

775 *Ibid.*, artikli 36 lõige 1.

mehhanismi. Komisjon võib otsuse ka kehtetuks tunnistada, muuta või peatada, kui kättesaadavast teabest ilmneb, et tingimused kolmandas riigis või rahvusvahelises organisatsioonis ei taga enam piisavat kaitset. Sellisel juhul peab komisjon alustama konsultatsioone kolmanda riigi või rahvusvahelise organisatsiooniga, et püüda olukorda parandada.

Kaitse piisavuse otsuse puudumisel võib edastamine põhineda asjakohastel kaitsemeetmetel. Need võib sätestada õiguslikult siduvas dokumendis või vastutav töötleja võib ise hinnata isikuandmete edastamisega seotud asjaolusid ja võib järeldada, et asjakohased kaitsemeetmed on olemas. Ise hindamisel tuleb arvestada Europoli või Eurojusti ja kolmanda riigi või rahvusvahelise organisatsiooni vahel sõlmitud võimalikke koostöölepinguid, konfidentsiaalsuskohustuste olemasolu ja eesmärgi piiramist ning tagatisi, et andmeid ei kasutata julma ja ebainimliku kohtlemise mis tahes vormi, sealhulgas surmanuhtluse eesmärgil[776]. Viimati nimetatud juhul peab vastutav töötleja teavitama pädevat järelevalveasutust selle kategooria all edastatavatest kategooriatest[777].

Kui kaitse piisavuse otsust ei ole tehtud või asjakohaseid kaitsemeetmeid ei ole kehtestatud, võib edastamist siiski lubada direktiivis kirjeldatud eriolukordades. Need on näiteks andmesubjekti või muu isiku eluliste huvide kaitse ning sellise vahetu ja suure ohu vältimine, mis ähvardab liikmesriigi või kolmanda riigi avalikku julgeolekut[778].

Üksik- ja erijuhtudel võivad pädevad asutused edastada isikuandmeid kolmandates riikides asuvatele vastuvõtjatele, kes ei ole pädevad asutused, kui on täidetud üks eespool kirjeldatud kolmest tingimusest ning täidetud on ka direktiivi artiklis 39 sätestatud lisatingimused. Eelkõige peab edastamine olema rangelt vajalik edastava pädeva asutuse ülesande täitmiseks, kes vastutab ka selle määramise eest, et üksikisikute põhiõigused ja -vabadused ei ole edastamist õigustava üldise huvi suhtes ülimuslikud. Sellised edastamised tuleb dokumenteerida ja edastav pädev asutus peab pädevat järelevalveasutust teavitama[779].

Samuti nõutakse direktiivis kolmandate riikide ja rahvusvaheliste organisatsioonide korral ka rahvusvahelise koostöö mehhanismide väljatöötamist, et soodustada

776 *Ibid.*, põhjendus 71.

777 *Ibid.*, artikli 37 lõige 1.

778 *Ibid.*, artikli 38 lõige 1.

779 *Ibid.*, artikli 37 lõige 3.

õigusaktide tõhusat täitmist, ning sellega aidatakse andmekaitse järelevalveasutustel teha koostööd teiste riikide asjaomaste asutustega[780].

Sõltumatu järelevalveasutus ja andmesubjektide õiguskaitsevahendid

Iga liikmesriik peab tagama, et direktiivi kohaselt vastu võetud sätete kohaldamise üle teeks järelevalvet ning pakuks asjakohast nõustamist üks või mitu riigi tasandi sõltumatut järelevalveasutust[781]. Direktiivi kohaldamiseks loodud järelevalveasutus võib olla sama mis isikuandmete kaitse üldmääruse alusel loodud järelevalveasutus, kuid liikmesriikidel on õigus määrata muu asutus, kui sõltumatuse kriteeriumid on täidetud. Järelevalveasutused vaatavad samuti läbi kõigi isikute esitatud kaebused oma õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega pädevates asutustes.

Kui andmesubjektide õiguste kasutamist on vaja tungivatel põhjustel piirata, peab andmesubjektil olema õigus esitada kaebus pädevale riiklikule järelevalveasutusele ja/või kohtule. Kui isik kannab kahju direktiivi rakendava riigisisese õigusakti rikkumise tõttu, on tal õigus saada hüvitist vastutavalt töötlejalt või muult liikmesriigi õiguse kohaselt pädevalt asutuselt[782]. Üldiselt peab andmesubjektidel olema võimalik kasutada õiguskaitsevahendit, kui on rikutud nende õigusi, mis on tagatud direktiivi rakendavate riiklike õigusaktidega[783].

8.3. Muud eriõigusaktid seoses andmekaitsega õiguskaitses

Lisaks politsei- ja kriminaalõigusasutuste andmekaitse direktiivile reguleeritakse liikmesriikide valduses oleva teabe vahetamist teatud valdkondades mitme õigusaktiga, näiteks nõukogu raamotsusega 2009/315/JSK, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu, nõukogu otsusega 2000/642/JSK liikmesriikide rahapesu andmebüroode vahelise koostöö korra kohta teabe vahetamisel ja nõukogu 18. detsembri 2006. aasta

780 *Ibid.*, artikkel 40.

781 *Ibid.*, artikkel 41.

782 *Ibid.*, artikkel 56.

783 *Ibid.*, artikkel 54.

raamotsusega 2006/960/JSK Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta[784].

On oluline, et pädevate asutuste piiriülene koostöö[785] hõlmab üha enam sisserändeandmete vahetamist. Seda õigusvaldkonda ei peeta politsei- ja kriminaalõigusküsimuste osaks, ent see on politsei- ja õigusasutuste tegevuse mitmes aspektis asjakohane. Sama kehtib ELi imporditavaid või EList teistesse riikidesse eksporditavaid kaupu käsitlevate andmete kohta. Piirikontrolli kaotamine Schengeni alal on suurendanud pettuste riski, mis tähendab, et liikmesriigid peavad tugevdama koostööd, edendades eelkõige piiriülest teabevahetust, et tagada riikide ja ELi tasandi tollieeskirjade rikkumiste kiire avastamine ja nende eest vastutusele võtmine. Lisaks on viimastel aastatel suurenenud raske ja organiseeritud kuritegevus ning terrorism, millega võib kaasneda rahvusvaheline reisimine ning millega seoses on paljudel juhtudel ilmnenud vajadus suurendada piiriülest koostööd politsei ja õiguskaitse valdkonnas[786].

Prümi otsus

Oluline näide piiriülesest institutsioonilisest koostööst liikmesriikide valduses oleva teabe vahetamise kaudu on nõukogu otsus 2008/615/JSK koos selle rakendussätetega otsuses 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega (Prümi otsus), millega lisati 2008. aastal ELi õigusesse Prümi leping[787]. Prümi leping on rahvusvahelise

784 Euroopa Liidu Nõukogu (2009), nõukogu 26. veebruari 2009. aasta raamotsus 2009/315/JSK, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu, ELT 2009 L 93; Euroopa Liidu Nõukogu (2009), nõukogu 17. oktoobri 2000. aasta otsus 2000/642/JSK liikmesriikide rahapesu andmebüroode vahelise koostöö korra kohta teabe vahetamisel, EÜT 2000 L 271; nõukogu 18. detsembri 2006. aasta raamotsus 2006/960/JSK Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta, ELT 2006 L 386.

785 Euroopa Komisjon (2012), komisjoni teatis Euroopa Parlamendile ja nõukogule: „Õiguskaitsekoostöö tugevdamine ELis: Euroopa teabevahetusmudel (EIXM)“, COM(2012) 735 final, Brüssel, 7. detsember 2012.

786 Vt Euroopa Komisjon (2011), ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks, COM(2011) 32 final, Brüssel, 2. veebruar 2011, lk 1.

787 Euroopa Liidu Nõukogu (2008), nõukogu 23. juuni 2008. aasta otsus 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega, ELT 2008 L 210.

politseikoostöö leping, mille sõlmisid 2005. aastal Austria, Belgia, Hispaania, Luksemburg, Madalmaad, Prantsusmaa ja Saksamaa[788].

Prümi otsuse eesmärk on aidata allakirjutanud 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:

- automaatne juurdepääs DNA-profiilidele, sõrmejäljeandmetele ja teatud riiklikele sõidukite registreerimisandmetele;
- andmete esitamine seoses suursündmustega, millel on piiriülene mõõde;
- teabe edastamine terroriaktide ennetamiseks;
- muud piiriülese politseikoostöö tõhustamise meetmed.

Prümi otsuse alusel kättesaadavaks tehtavaid andmebaase hallatakse üksnes riikide õigusaktide alusel, ent andmete vahetamist reguleeritakse täiendavalt ka otsusega, mille kooskõla politsei- ja kriminaalõigusasutuste andmekaitse direktiiviga hakatakse hindama. Selliste andmevoogude järelevalve eest vastutavad pädevad asutused on riikide andmekaitse järelevalveasutused.

Raamotsus 2006/960/JSK – Rootsi algatus

Ka raamotsus 2006/960/JSK (Rootsi algatus)[789] on näide piiriülesest koostööst, mida tehakse riigi tasandi õiguskaitseasutuste valduses olevate andmete vahetamisel. Rootsi algatuses käsitletakse konkreetselt teabe ja jälitusteabe vahetamist ning artiklis 8 sätestatakse andmekaitse erieeskirjad.

Selle õigusakti kohaselt peab vahetatud teabe ja jälitusteabe kasutamine toimuma teavet saava liikmesriigi andmekaitsesätete kohaselt samade eeskirjade alusel, nagu oleksid need kogutud selles liikmesriigis. Artiklis 8 sätestatakse ka, et teabe

788 Austria Vabariigi, Belgia Kuningriigi, Hispaania Kuningriigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi, Prantsuse Vabariigi ja Saksamaa Liitvabariigi eelkõige terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastases võitluses piiriülese koostöö tõhustamise leping.

789 Euroopa Liidu Nõukogu (2006), nõukogu 18. detsembri 2006. aasta raamotsus 2006/960/JSK Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta, ELT L 386/89, 29. detsember 2006.

ja jälitusteabe esitamisel võib pädev õiguskaitseasutus kehtestada tingimusi, mis on kooskõlas riigisiseste õigusaktidega nende andmete kasutamise kohta vastuvõtva pädeva õiguskaitseasutuse poolt. Neid tingimusi võib kohaldada ka nende kriminaaluurimise või kriminaaljälitustoimingute tulemustest teavitamise suhtes, mille puhul teabe ja jälitusteabe vahetamist taotleti. Kui riigisisestes õigusaktides on sätestatud kasutuspiirangute erandid (nt kohtuasutustele, seadusandlikele organitele), võib teavet ja jälitusteavet kasutada alles pärast teavet edastava liikmesriigiga eelkonsulteerimist.

Esitatud teavet ja jälitusteavet võib kasutada

- eesmärgil, milleks teave on edastatud, või
- avalikku julgeolekut ähvardava vahetu ja raske ohu ennetamiseks.

Töötlemine muudel eesmärkidel võib olla lubatud, kuid ainult teabe edastanud liikmesriigi eelneval loal.

Rootsi algatuses on märgitud ka, et töödeldavaid isikuandmeid tuleb kaitsta vastavalt rahvusvahelistele õigusaktidele, näiteks järgmistele:

- Euroopa Nõukogu konventsioon üksikisikute kaitse kohta isikuandmete automaattöötlusel[790];
- konventsiooni 8. novembri 2001. aasta lisaprotokoll, mis käsitleb järelevalveasutusi ja andmete piiriülest liikumist[791];
- Euroopa Nõukogu soovitus nr R (87) 15, millega reguleeritakse isikuandmete kasutamist politseivaldkonnas[792].

790 Euroopa Nõukogu (1981), isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, CETS nr 108.

791 Euroopa Nõukogu (2001), isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni lisaprotokoll, mis käsitleb järelevalveasutusi ja andmete piiriülest liikumist, CETS nr 108.

792 Euroopa Nõukogu ministrite komitee (1987), *Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)*.

ELi broneeringuinfo direktiiv

Broneeringuinfo andmed on seotud lennureisijate teabega, mida lennuettevõtjad koguvad ja säilitavad broneerimissüsteemides ja väljumiste kontrollisüsteemides oma ärilistel eesmärkidel. Need andmed sisaldavad mitmesugust teavet, näiteks sõidukuupäevi, marsruuti, piletiteavet, kontaktandmeid, broneerinud reisifirmat, maksevahendi teavet, istekoha numbrit ja pagasiteavet[793]. Broneeringuinfo töötlemine võib aidata õiguskaitseasutustel tuvastada teadaolevaid või võimalikke kahtlustatavaid ja teha hindamisi, mis põhinevad reisiharjumustel ja muudel, tavaliselt kuritegevusega seostatavatel näitajatel. Ka võimaldab broneeringuinfo analüüs kuritegelikus tegevuses osalemises kahtlustatavate reisimarsruutide ja kontaktide jälgimist tagantjärele, mis võimaldab õiguskaitseasutustel tuvastada kuritegelikke võrgustikke[794]. EL on sõlminud broneeringuinfo vahetamiseks kolmandate riikidega mõne lepingu, nagu on selgitatud jaotises 7. Lisaks on EL kehtestanud broneeringuinfo ELis töötlemise korra direktiiviga (EL) 2016/681, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks (ELi broneeringuinfo direktiiv)[795]. Selle direktiiviga sätestatakse lennuettevõtjate kohustused edastada broneeringuinfot pädevatele asutustele ning kehtestatakse ranged andmekaitsemeetmed selliste andmete töötlemisel ja kogumisel. ELi broneeringuinfo direktiivi kohaldatakse Euroopa Liitu suunduvate ja sellest väljuvate rahvusvaheliste lendude suhtes, samuti ELi-siseste lendude suhtes, kui liikmesriik nii otsustab[796].

Kogutud broneeringuinfo tohib sisaldada üksnes ELi broneeringuinfo direktiiviga lubatud teavet. Teavet tuleb säilitada ühe teabeüksusena turvalises kohas igas liikmesriigis. Broneeringuinfo tuleb anonüümida kuus kuud pärast selle saamist lennuettevõtjalt ja infot säilitatakse kuni viis aastat[797]. Broneeringuinfo andmeid vahetatakse liikmesriikide vahel, liikmesriikide ja Europoli vahel või kolmandate riikidega, kuid ainult üksikjuhtudel.

793 Euroopa Komisjon (2011), ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks, COM(2011) 32 final, Brüssel, 2. veebruar 2011, lk 1.

794 Euroopa Komisjon (2015), *Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives*, Brüssel, 11. jaanuar 2015.

795 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/681, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks (ELT 2016 L 119, lk 132).

796 Broneeringuinfo direktiiv, L 119, lk 132, artikli 1 lõige 1 ja artikli 2 lõige 1.

797 *Ibid.*, artikli 12 lõiked 1 ja 2.

Broneeringuinfo edastamine ja töötlemine ning andmesubjektidele tagatud õigused peavad olema kooskõlas politsei- ja kriminaalõigusasutuste andmekaitse direktiiviga ning tagama eraelu ja isikuandmete kõrgel tasemel kaitse, mida nõutakse hartas, nüüdisajastatud konventsioonis nr 108 ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis.

Politsei- ja kriminaalõigusasutuste andmekaitse direktiivi kohaselt vastutavad pädevad riiklikud järelevalveasutused ka liikmesriikide poolt broneeringuinfo direktiivi alusel vastu võetud sätete kohaldamise küsimustes nõustamise ja kohaldamise järelevalve eest.

Sideandmete säilitamine

Andmete säilitamise direktiiviga[798] – mis tunnistati kehtetuks 8. aprillil 2014 kohtuasjas *Digital Rights Ireland* – kohustati sideteenuse osutajaid hoidma metaandmeid raskete kuritegude vastu võitlemise erieesmärgil kättesaadavana vähemalt 6 kuud, kuid mitte kauem kui 24 kuud, olenemata sellest, kas teenuseosutaja veel vajab neid andmeid arveldamiseks või tehniliselt teenuse osutamiseks või mitte.

Sideandmete säilitamine riivab selgelt õigust andmekaitsele[799]. Sellise riive põhjendatus on vaidlustatud ELi liikmesriikides mitmes kohtumenetluses[800].

Näide: kohtuasjades *Digital Rights Ireland* ja *Kärntner Landesregierung jt*[801] esitas kontsern Digital Rights Iirimaa kõrgema astme kohtule (High Court) ja Michael Seitlinger Austria konstitutsioonikohtule kaebuse, vaidlustades elektroonilise side andmete säilitamist võimaldavate riigisiseste meetmete seaduslikkuse. Digital Rights palus, et Iirimaa kohus kuulutaks kehtetuks

798 Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, ELT 2006 L 105.

799 Euroopa Andmekaitseinspektor (2011), 31. mai 2011. aasta arvamus komisjoni hindamisaruande kohta nõukogule ja Euroopa Parlamendile seoses andmete säilitamise direktiiviga (direktiiv 2006/24/EÜ), 31. mai 2011.

800 Saksamaa föderaalne konstitutsioonikohus (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. märts 2010; Rumeenia föderaalne konstitutsioonikohus (*Curtea Constituțională a României*), nr 1258, 8. oktoober 2009; Tšehhi Vabariigi konstitutsioonikohus (*Ústavní soud České republiky*), 94/2011 Coll., 22. märts 2011.

801 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014, punkt 65.

direktiivi 2006/24/EÜ ja riigisisese kriminaalõiguse osa, mis käsitleb terroriakte. Sarnase vaide esitasid Michael Seitlinger ja üle 11 000 muu hageja, kes taotlesid, et tühistataks Austria sideseaduse säte, millega võeti üle direktiiv 2006/24/EÜ.

Nende eelotsusetaotluste käsitlemisel tunnistas Euroopa Liidu Kohus andmete säilitamise direktiivi kehtetuks. ELK sõnul annavad andmed, mida direktiivi kohaselt tohib säilitada, ühtekokku täpset teavet isikute kohta. Lisaks uuris ELK eraelu austamise ja isikuandmete kaitse põhiõigustesse sekkumise raskust. Kohus leidis, et säilitamine vastab avaliku huvi eesmärgile, nimelt võitlusele raskete kuritegude vastu ja seega avaliku julgeoleku eest. ELK märkis siiski, et ELi seadusandja on direktiivi vastuvõtmisega rikkunud proportsionaalsuse põhimõtet. Kuigi direktiiv võib olla asjakohane taotletava eesmärgi saavutamiseks, toob see kaasa eraelu puutumatuse ja isikuandmete kaitse põhiõiguste ulatusliku ja väga raske riive, ilma et riive oleks täpselt piiritletud sätetega, mis võimaldaks tagada, et riive piirduks üksnes vältimatult vajalikuga.

Andmete säilitamise eriõigusakti puudumisel on andmete säilitamine lubatud erandina direktiivi 2002/58/EÜ (eraelu puutumatuse ja elektroonilise side direktiiv)[802] kohasest sideandmete konfidentsiaalsusest, et võidelda raskete kuritegude vastu. Selline säilitamine peab piirduma säilitatavate andmete liikide, asjaomaste sidevahendite, isikute ja säilitamise valitud kestuse seisukohalt rangelt vajalikuga. Riigisisestel ametiasutustel võib olla juurdepääs säilitatavatele andmetele rangete tingimuste alusel, sealhulgas sõltumatu asutuse tehtava eelneva läbivaatamise alusel. Andmeid tuleb säilitada Euroopa Liidus.

Näide: pärast kohtuasjade *Digital Rights Ireland* ja *Kärntner Landesregierung jt*[803] kohtuotsuse tegemist esitati Euroopa Liidu Kohtule veel kaks juhtumit seoses Rootsis ja Ühendkuningriigis kehtiva üldkohustusega elektroonilise side teenuste osutajatele säilitada sideandmeid, nagu nõuti kehtetuks tunnistatud andmete säilitamise direktiivis. Kohtuasjades *Tele2 Sverige* ja *Home*

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

803 ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014.

Department vs. Tom Watson jt[804] otsustas Euroopa Liidu Kohus, et riigisisesed õigusaktid, millega nähakse ette andmete üldine ja valimatu säilitamine, nõudmata mis tahes seost säilitada tulevate andmete ja avalikku julgeolekut ähvardava ohu vahel ning täpsustamata tingimusi – nt säilitamise aega, geograafilist piirkonda, raske kuriteoga tõenäoliselt seotud isikute rühma –, ületavad rangelt vajaliku piire ning neid ei saa pidada demokraatlikus ühiskonnas põhjendatuks, nagu on nõutud direktiivis 2002/58/EÜ koostoimes ELi põhiõiguste hartaga.

Väljavaated

2017. aasta jaanuaris avaldas Euroopa Komisjon ettepaneku võtta vastu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side valdkonnas, mille eesmärk oli kehtetuks tunnistada ja asendada direktiiv 2002/58/EÜ[805]. Ettepanekus ei ole ühtki erisätet andmete säilitamise kohta. Samas sätestatakse selles, et liikmesriigid võivad seadusega piirata määrusest tulenevaid teatud kohustusi ja õigusi, kui selline piirang on vajalik ja proportsionaalne meede konkreetsete avalike huvide, sealhulgas riigi julgeoleku, riigikaitse, avaliku julgeoleku kaitsmiseks ning kuritegude tõkestamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks[806]. Seega oleks liikmesriikidel võimalik säilitada või luua riigisiseseid andmete säilitamise õigusraamistikke, millega sätestatakse suunatud säilitamismeetmed, kuivõrd need raamistikud on kooskõlas liidu õigusega, arvestades Euroopa Liidu Kohtu tava e-privaatsuse direktiivi ja Euroopa Liidu põhiõiguste harta tõlgendamisel[807]. Käsiraamatu koostamise ajal arutelud määruse vastuvõtmise üle alles kestsid.

804 ELK, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen ja Secretary of State for the Home Department vs. Tom Watson jt* [suurkoda], 21. detsember 2016.

805 Euroopa Komisjon (2017), ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus), COM(2017) 10 final, Brüssel, 10. jaanuar 2017.

806 *Ibid.*, põhjendus 26.

807 Vt ettepanek: määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul, COM(2017) 10 final, seletuskirja punkt 1.3.

ELi–USA õiguskaitse eesmärgil vahetatavate isikuandmete kaitse raamkokkulepe

1. veebruaril 2017 jõustus ELi–USA süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmisega seotud isikuandmete töötlemise raamkokkulepe[808]. ELi–USA raamkokkuleppe eesmärk on tagada ELi kodanikele kõrgel tasemel andmekaitse, suurendades samal ajal ELi ja USA õiguskaitseasutuste koostööd. Raamkokkulepe täiendab ELi ja USA vahelisi ning liikmesriikide ja USA õiguskaitseasutuste vahelisi kokkuleppeid, aidates kehtestada selged ja ühtlustatud andmekaitse-eeskirjad valdkonna tulevaste lepingute jaoks. Selles mõttes on kokkuleppe eesmärk luua püsiv õigusraamistik, et toetada teabevahetust.

Iseenesest ei ole kokkulepe isikuandmete vahetamise sobiv õiguslik alus, kuid pakub asjaomastele isikutele sobivaid andmekaitsemeetmeid. See hõlmab kõigi nende isikuandmete töötlemist, mis on vajalikud kuritegude, sealhulgas terrorismi ennetamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks[809].

Kokkuleppes sätestatakse mitu kaitsemeedet, et tagada isikuandmete kasutamine ainult kokkuleppes sätestatud eesmärkidel. Eelkõige tagatakse kokkuleppega ELi kodanikele järgmine kaitse:

- isikuandmete kasutamise piirangud: isikuandmeid võib kasutada ainult süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eesmärgil;
- kaitse meelevaldse ja põhjendamatu diskrimineerimise eest;
- andmete hilisem edastamine: mis tahes edasisaatmine muudele riikidele kui USA, ELi-välistele riikidele või rahvusvahelisele organisatsioonile peab toimuma selle riigi pädeva asutuse eelneval nõusolekul, kes andmed algselt edastas;
- andmekvaliteet: isikuandmeid tuleb säilitada nende õigsust, asjakohasust, ajakohasust ja terviklikkust arvestades;

808 Vt Euroopa Liidu Nõukogu (2016), *Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'*, pressiteade 305/16, 2. juuni 2016.

809 Ameerika Ühendriikide ja Euroopa Liidu vaheline 18. mai 2016. aasta kokkulepe süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmisega seotud isikuandmete kaitse kohta, (OR. en) 8557/16, artikli 3 lõige 1. Vt ka Euroopa Komisjoni 26. mai 2010. aasta teade ELi ja USA vahelise andmekaitsekokkuleppe läbirääkimiste kohta, MEMO/10/216, ja Euroopa Komisjoni 26. mai 2010. aasta pressiteade ELi ja USA vahelise andmekaitsekokkuleppe rangete privaatsusstandardite kohta, IP/10/609.

- töötlemise turvalisus, sealhulgas isikuandmetega seotud rikkumistest teatamine;
- delikaatsete isikuandmete töötlemine on lubatud ainult asjakohaste kaitsemeetmete alusel seaduse kohaselt;
- säilitamise tähtajad: isikuandmeid ei tohi säilitada kauem, kui see on vajalik või asjakohane;
- juurdepääsu- ja andmete parandamise õigus: igal isikul on õigus tutvuda oma isikuandmetega teatud tingimustel ja ta võib nõuda andmete parandamist, kui need on ebaõiged;
- automaatotsused eeldavad asjakohaseid kaitsemeetmeid, sealhulgas inimsekkumise võimalust;
- tõhus järelevalve, sealhulgas ELi ja USA järelevalveasutuste koostöö, ning
- õiguskaitsevahendid ja jõustamine: ELi kodanikel on õigus[810] pöörduda õiguskaitse saamiseks USA kohtutesse, kui USA ametiasutused keelduvad juurdepääsu lubamisest nende isikuandmetele või andmete parandamisest või avalikustavad nende isikuandmed ebaseaduslikult.

Raamkokkuleppe lepingu alusel on loodud ka süsteem, kuidas vajaduse korral teavitada asjaomaste isikute liikmesriigi pädevat järelevalveasutust kõigist andmekaitsega seotud rikkumistest. Raamkokkuleppes sätestatud õiguslikud tagatised kindlustavad ELi kodanike võrdse kohtlemise USAs, kui on rikutud eraelu puutumatust[811].

810 President Obama allkirjastas USA õiguskaitsevahendite seaduse US Judicial Redress Act 24. veebruaril 2016.

811 Euroopa Andmekaitseinspektor esitas ELi ja USA lepingu kohta arvamuse, milles soovitab muu hulgas järgmisi kohandusi: 1) lisada artiklile, mis käsitleb andmete säilitamist mitte kauem, kui vajalik ja asjakohane, sõnad „konkreetsetel eesmärkidel, milleks andmed edastati", ning 2) välistada võimalik delikaatsete andmete massiline edastamine. Vt Euroopa Andmekaitseinspektori arvamus 1/2016: esialgne arvamus Ameerika Ühendriikide ja Euroopa Liidu vahelise kuritegude ennetamise, uurimise, avastamise ning nende eest vastutusele võtmisega seotud isikuandmete kaitse lepingu kohta, punkt 35.

8.3.1. Andmekaitse ELi õigus- ja õiguskaitseasutustes

Europol

ELi õiguskaitseasutuse Europoli peakorter asub Haagis ja Europoli riiklik üksus on igas liikmesriigis. Europol asutati 1998. aastal; selle praegune õiguslik staatus ELi institutsioonina põhineb Euroopa Liidu Õiguskaitsekoostöö Ameti määrusel (Europoli määrus)[812]. Europoli eesmärk on aidata ennetada ja uurida organiseeritud kuritegevust, terrorismi ja muid vähemalt kaht liikmesriiki mõjutavaid rasket kuritegevust, mis on loetletud Europoli määruse I lisas. Europol teeb seda teabe vahetamise ja ELi teabekeskuse kaudu, pakkudes jälitusandmete analüüse ja ohuhinnanguid.

Eesmärkide saavutamiseks on Europolis loodud Europoli infosüsteem, mis pakub liikmesriikidele andmebaasi kriminaalteabe ja muu teabe vahetamiseks riiklike üksuste kaudu. Europoli infosüsteemi võib kasutada selliste andmete avaldamiseks, mis on seotud isikutega, keda kahtlustatakse või kes on süüdi mõistetud Europoli pädevusse kuuluva kuriteo sooritamises, või isikutega, kelle kohta on faktilisi tõendeid, et nad sooritavad Europoli pädevusse kuuluvaid kuritegusid. Europol ja riiklikud üksused võivad sisestada andmeid vahetult Europoli infosüsteemi ja saada sealt teavet. Andmeid tohib muuta, parandada või kustutada üksnes andmed sisestanud pool. Europolile võivad anda teavet ka ELi asutused, kolmandad riigid ja rahvusvahelised organisatsioonid.

Europol võib saada teavet, sealhulgas isikuandmeid, ka avalikult kättesaadavatest allikatest, näiteks internetist. Isikuandmete edastamine ELi asutustele on lubatud ainult siis, kui see on vajalik Europoli või vastuvõtva ELi asutuse ülesannete täitmiseks. Isikuandmete edastamine kolmandatele riikidele või rahvusvahelistele organisatsioonidele on lubatud ainult siis, kui Euroopa Komisjon otsustab, et riik või rahvusvaheline organisatsioon tagab piisava andmekaitse taseme (kaitse piisavuse otsus), või kui on olemas rahvusvaheline või koostööleping. Europol võib vastu võtta ja töödelda eraõiguslike isikute ja eraisikute isikuandmeid rangel tingimusel, et andmed edastab Europoli riiklik üksus oma riigisisese õiguse kohaselt, kolmanda riigi kontaktpunkt või rahvusvaheline organisatsioon, kellega toimub koostöö koostöölepingu või kolmanda riigi asutuse või rahvusvahelise organisatsiooni kaudu, kelle

812 Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta määrus (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK (ELT 2016 L 135, lk 53).

suhtes kohaldatakse kaitse piisavuse otsust või kellega EL on sõlminud rahvusvahelise lepingu. Kogu teabevahetus toimub turvalise teabevahetusvõrgu (SIENA) kaudu.

Uutele suundumustele reageerimiseks on moodustatud Europolis erikeskused. Küberkuritegevuse vastase võitluse Euroopa keskus moodustati Europolis 2013. aastal[813]. Keskus toimib ELi teabepunktina küberkuritegevuse valdkonnas, aidates kiiremini reageerida internetikuritegude korral, arendades ja rakendades digitaalkriminalistika suutlikkust ning luues parimat tava küberkuritegude uurimisel. Keskus keskendub järgmisele küberkuritegevusele:

- kuriteod, mille on sooritanud organiseeritud rühmitused suure kriminaaltulu saamise eesmärgil, näiteks internetipettused;
- kuriteod, mis põhjustavad ohvritele rasket kahju, näiteks laste seksuaalne ärakasutamine internetikeskkonnas;
- kuriteod, mis häirivad elutähtsaid taristuid või infosüsteeme Euroopa Liidus.

2016. aasta jaanuaris moodustati Euroopa terrorismivastase võitluse keskus eesmärgiga pakkuda liikmesriikidele operatiivtuge terroriaktide uurimisel. Keskus võrdleb reaalajas edastatavaid operatiivandmeid Europoli juba olemasolevate andmetega, leides kiiresti finantsseosed, ja analüüsib kõiki kättesaadavaid juurdlusandmeid, et aidata koostada terroristlikust võrgustikust struktureeritud ülevaade[814].

Nõukogu 2015. aasta novembri kohtumise tulemusena moodustati 2016. aasta veebruaris rändajate smugeldamise vastane Euroopa keskus, et toetada liikmesriike rändajate salakaubaveos osalevate kuritegelike võrgustike tuvastamisel ja likvideerimisel. See on teabekeskus, mis toetab ELi piirkondlike töörühmade büroosid Catanias (Itaalia) ja Pireuses (Kreeka), kes abistavad riikide ametiasutusi mitmes valdkonnas, näiteks luureandmete jagamisel, kriminaaljuurdlustes ja inimeste smugeldamise võrgustike vastutusele võtmisel[815].

813 Vt ka Euroopa andmekaitseinspektor (2012), Euroopa andmekaitseinspektori arvamus – komisjoni teatis nõukogule ja Euroopa Parlamendile: küberkuritegevuse vastase võitluse Euroopa keskuse loomine, Brüssel, 29. juuni 2012.

814 Vt Europoli veebileht Euroopa terrorismivastase võitluse keskuse kohta.

815 Vt Europoli rändajate smugeldamise vastase Euroopa keskuse veebileht.

Europoli tegevust reguleerivat andmekaitsekorda on tõhustatud ja see tugineb ELi institutsioonide andmekaitse määruse[816] põhimõtetele ning on kooskõlas ka politsei- ja kriminaalõigusasutuste andmekaitse direktiiviga, nüüdisajastatud konventsiooniga nr 108 ja politseisoovitusega.

Isikuandmete töötlemine seoses kuriteoohvrite, tunnistajate või muude isikutega, kes võivad anda teavet kuritegude kohta, või alla 18-aastaste isikute korral on lubatud, kui see on rangelt vajalik ja proportsionaalne võitluseks kuritegevuse vastu, mis kuulub Europoli eesmärkide hulka[817]. Delikaatsete isikuandmete töötlemine on keelatud, v.a kui see on rangelt vajalik ja proportsionaalne Europoli eesmärkide alla kuuluva kuritegevuse ennetamiseks või selle vastu võitlemiseks ja kui need andmed täiendavad Europolis töödeldavaid isikuandmeid[818]. Mõlemal juhul on asjaomastele andmetele juurdepääs üksnes Europolil[819].

Andmeid tohib säilitada ainult vajaliku ja proportsionaalse aja jooksul ning säilitamise jätkamine vaadatakse läbi iga kolme aasta järel, vastasel korral kustutatakse andmed automaatselt[820].

Teatud tingimustel võib Europol edastada isikuandmeid ELi asutusele või kolmanda riigi asutusele või rahvusvahelisele organisatsioonile otse[821]. Kui andmetega seotud rikkumised võivad raskelt kahjustada asjaomaste andmesubjektide õigusi ja vabadusi, tuleb rikkumistest teatada neile põhjendamatu viivituseta[822]. Europoli tegevuse järelevalveks isikuandmete töötlemisel määratakse liikmesriigi tasandil riiklik järelevalveasutus[823].

Euroopa Andmekaitseinspektor vastutab füüsiliste isikute põhiõiguste ja -vabaduste kaitse tagamise eest isikuandmete töötlemisel Europolis ning Europoli ja andmesubjektide nõustamise eest kõikides isikuandmete töötlemisega seotud küsimustes. Selleks tegutseb Euroopa Andmekaitseinspektor uurimis- ja kaebuste menetlemise

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

817 Europoli määruse artikli 30 lõige 1.

818 *Ibid.*, artikli 30 lõige 2.

819 *Ibid.*, artikli 30 lõige 3.

820 *Ibid.*, artikkel 31.

821 *Ibid.*, vastavalt artiklid 24 ja 25.

822 *Ibid.*, artikkel 35.

823 Europoli määruse artikkel 42.

organina ning teeb tihedat koostööd riiklike järelevalveasutustega[824]. Euroopa Andmekaitseinspektor ja riiklikud järelevalveasutused kohtuvad vähemalt kaks korda aastas koostöönõukogus, millel on nõuandepädevus[825]. Liikmesriigid on kohustatud seadusega asutama järelevalveasutuse, kes on pädev jälgima isikuandmete edastamise lubatavust riigi tasandilt Europolile ja Europolist liikmesriigile ning liikmesriigi suhtlemist Europoliga isikuandmete teemal[826]. Ka on liikmesriigid kohustatud tagama, et riiklik järelevalveasutus saab täita oma Europoli määruse kohaseid ülesandeid ja kohustusi täiesti sõltumatult[827]. Andmete töötlemise seaduslikkuse kontrollimiseks, oma tegevuse jälgimiseks ning andmetervikluse ja turvalisuse tagamiseks peab Europol oma andmetöötlustoimingute kohta logisid või dokumenteerib need. Need logid sisaldavad teavet töötlemistoimingute kohta automaattöötlussüsteemides, mis on seotud andmete kogumise, muutmise, andmetega tutvumise, andmete avalikustamise, kombineerimise ja kustutamisega[828].

Euroopa Andmekaitseinspektori otsuse võib edasi kaevata Euroopa Liidu Kohtusse[829]. Igal isikul, kes on kandnud kahju ebaseadusliku andmetöötlustoimingu tagajärjel, on õigus saada hüvitist tekitatud kahju eest kas Europolilt või vastutavalt liikmesriigilt, esitades esimesel juhul kaebuse Euroopa Kohtule või teisel juhul pädevale riigisisesele kohtule[830]. Lisaks võib Europoli tegevust kontrollida liikmesriikide parlamentide ja Euroopa Parlamendi parlamentaarse ühiskontrolli töörühm[831]. Lisaks õigusele nõuda isikuandmete kontrollimist, parandamist või kustutamist on igal isikul õigus tutvuda isikuandmetega, mida Europol võib tema kohta säilitada. Nende õiguste suhtes võidakse kohaldada erandeid ja piiranguid.

824 *Ibid.*, artiklid 43 ja 44.
825 *Ibid.*, artikkel 45.
826 *Ibid.*, artikli 42 lõige 1.
827 *Ibid.*, artikli 42 lõige 1.
828 *Ibid.*, artikkel 40.
829 *Ibid.*, artikkel 48.
830 *Ibid.*, artikkel 50.
831 *Ibid.*, artikkel 51.

Eurojust

2002. aastal asutatud Eurojust on ELi asutus peakorteriga Haagis. Eurojust edendab õiguskoostööd vähemalt kaht liikmesriiki mõjutavate raskete kuritegude uurimisel ja kohtu alla andmisel[832]. 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 staatust reguleerivad riigi õigusaktid ja kellele on antud pädevus täita ülesandeid eesmärgiga edendada ja parandada õiguskoostööd. Peale selle tegutsevad liikmesriiki esindavad liikmed Eurojusti teatud eriülesannete täitmiseks üheskoos kolleegiumina.

Eurojust võib töödelda isikuandmeid üksnes oma eesmärkide saavutamiseks. See piirdub konkreetse teabega inimeste kohta, keda kahtlustatakse Eurojusti pädevusse kuuluva kuriteo sooritamises või selles osalemises või kes on sellise kuriteo eest süüdi mõistetud. Samuti võib Eurojust töödelda teavet Eurojusti pädevusse kuuluvate kuritegude tunnistajate või ohvrite kohta[833]. Erandjuhtudel võib Eurojust piiratud aja jooksul töödelda täiendavaid isikuandmeid, mis on seotud süüteo asjaoludega, kui need andmed on otseselt asjakohased ja seotud toimuva uurimisega. Oma pädevuse piires võib Eurojust teha koostööd teiste ELi institutsioonide, asutuste ja organitega ning vahetada nendega isikuandmeid. Samuti võib Eurojust teha koostööd ja vahetada isikuandmeid kolmandate riikide ja organisatsioonidega.

Seoses andmekaitsega peab Eurojust tagama sellise kaitsetaseme, mis on vähemalt samaväärne tasemega, mis on ette nähtud nüüdisajastatud konventsiooni nr 108 ja selle hilisemate muudatuste põhimõtetega. Andmete

832 Euroopa Liidu Nõukogu (2002), nõukogu 28. veebruari 2002. aasta otsus 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, EÜT 2002 L 63; Euroopa Liidu Nõukogu (2003), nõukogu 18. juuni 2003. aasta otsus 2003/659/JSK, millega muudetakse nõukogu otsust 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, ELT 2003 L 44; Euroopa Liidu Nõukogu (2009), nõukogu 16. detsembri 2008. aasta otsus 2009/426/JSK, millega tugevdatakse Eurojusti ja muudetakse otsust 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu, ELT 2009 L 138 (Eurojusti otsused).

833 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[834].

Eurojustis on moodustatud 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 taotluse kohta tehtud otsusega. Kui Eurojust töötleb isikuandmeid ebaseaduslikult, vastutab ta kõigi andmesubjektile tekitatud kahjude korral kooskõlas selle liikmesriigi õigusega, kus asub Eurojusti peakontor asub (Madalmaad).

Väljavaated

2013. aasta juulis tegi Euroopa Komisjon ettepaneku võtta vastu määrus, millega reformitakse Eurojusti. Ettepanekule lisati ettepanek asutada Euroopa Prokuratuur (vt allpool). Määruse eesmärk on viia funktsioonid ja struktuur kooskõlla Lissaboni lepinguga. Lisaks on reformi eesmärk eristada selgelt Eurojusti operatiivülesanded, mida täidab Eurojusti kolleegium, ja haldusülesanded. Sellega võimaldatakse liikmesriikidel rohkem keskenduda operatiivülesannetele. Asutatakse uus juhatus, mis abistab kolleegiumi haldusülesannete täitmisel[835].

Euroopa Prokuratuur

Liikmesriikidel on ainupädevus esitada süüdistusi pettuse ja ELi eelarve ebaõige kohaldamise kuritegudes, millel on ka võimalik piiriülene mõju. Selliste kuritegude sooritajate uurimise, neile süüdistuse esitamise ja kohtu alla andmise tähtsus on suurenenud, arvestades eriti praegust majanduskriisi[836]. Euroopa Komisjon on teinud ettepaneku määruse kohta, mis käsitleb sõltumatu Euroopa Prokuratuuri loomist[837] eesmärgiga võidelda ELi finantshuve kahjustavate kuritegude vastu. Euroopa Prokuratuur luuakse tõhustatud koostöömenetluse kaudu, mis võimaldab vähemalt üheksal liikmesriigil seada sisse tihedam valdkondlik koostöö ELi struktuurides, ilma muid

834 Eurojusti isikuandmete töötlemist ja kaitset käsitleva töökorra sätted, ELT 2005 C 68/01, 19. märts 2005, lk 1.

835 Vt Euroopa Komisjoni veebileht Eurojusti kohta.

836 Vt Euroopa Komisjon (2013), ettepanek: nõukogu määrus Euroopa Prokuratuuri asutamise kohta, COM(2013) 534 final, Brüssel, 17. juuli 2013, lk 1, ja komisjoni veebileht Euroopa Prokuratuuri kohta.

837 Euroopa Komisjon (2013), ettepanek: nõukogu määrus Euroopa Prokuratuuri asutamise kohta, COM(2013) 534 final, Brüssel, 17. juuli 2013.

ELi riike kaasamata[838]. Tõhustatud koostööga on liitunud Belgia, Bulgaaria, Eesti, Hispaania, Horvaatia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Portugal, Prantsusmaa, Rumeenia, Saksamaa, Slovakkia, Sloveenia, Soome ja Tšehhi Vabariik; ühinemise kavatsust on väljendanud Austria ja Itaalia[839].

Euroopa Prokuratuuri pädevuses on uurida ELi pettusi ja muid ELi finantshuve kahjustavaid kuritegusid ja nende eest süüdistusi esitada, eesmärgiga uurimisi ja süüdistuste esitamist eri riikide õiguskordades tõhusalt koordineerida ning parandada ressursside kasutamist ja teabevahetust Euroopa tasandil[840].

Euroopa Prokuratuuri juhib Euroopa prokurör ja igas liikmesriigis on vähemalt üks delegeeritud Euroopa prokurör, kes vastutab uurimise ja süüdistuste esitamise eest liikmesriigis.

Ettepanekus sätestatakse tugevad kaitsemeetmed, millega tagatakse Euroopa Prokuratuuri juurdlustega seotud isikute õigused, mis on sätestatud riigisiseses õiguses, ELi õiguses ja ELi põhiõiguste hartas. Peamiselt põhiõigusi puudutavate uurimistoimingute jaoks on vaja eelnevat luba liikmesriigi kohtult[841]. Euroopa Prokuratuuri uurimiste üle teevad kohtulikku kontrolli riigisisesed kohtud[842].

Isikuandmete töötlemise suhtes Euroopa Prokuratuuris kohaldatakse ELi institutsioonide andmekaitse määrust[843]. Operatiivküsimustega, näiteks Europoliga seotud isikuandmete töötlemiseks on Euroopa Prokuratuuril eraldi andmekaitsekord, mis sarnaneb Europoli ja Eurojusti tegevust reguleeriva korraga, sest Euroopa Prokuratuuri ülesannete täitmine hõlmab isikuandmete töötlemist õiguskaitseasutuste ja prokuratuuridega liikmesriikide tasandil. Euroopa Prokuratuuri andmekaitse-eeskirjad on seega peaaegu samad kui politsei- ja kriminaalõigusasutuste andmekaitse direktiivi eeskirjad. Euroopa Prokuratuuri asutamise ettepaneku kohaselt peab isikuandmete

838 ELi toimimise lepingu artikli 86 lõige 1 ja artikli 329 lõige 1.

839 Vt Euroopa Liidu Nõukogu (2017), 20 liikmesriiki lepivad kokku Euroopa Prokuratuuri asutamise üksikasjades, pressiteade, 8. juuni 2017.

840 Euroopa Komisjon (2013), ettepanek: nõukogu määrus Euroopa Prokuratuuri asutamise kohta, COM(2013) 534 final, Brüssel, 17. juuli 2013, lk 1 ja 51–51. Vt ka Euroopa Komisjoni veebileht Euroopa Prokuratuuri kohta.

841 Euroopa Komisjon (2013), 17. juuli 2013. aasta ettepanek: nõukogu määrus Euroopa Prokuratuuri asutamise kohta, COM(2013) 534 final, Brüssel, artikli 26 lõige 4.

842 *Ibid.*, artikkel 36.

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

töötlemine vastama seaduslikkuse ja õigluse, eesmärgi piirangu, võimalikult väheste andmete kogumise, andmete õigsuse, tervikluse ja konfidentsiaalsuse põhimõttele. Euroopa Prokuratuur peab nii palju kui võimalik eristama eri liiki andmesubjektide isikuandmeid, näiteks kuriteos süüdi mõistetute, kahtlustatavate, kannatanute ja tunnistajate isikuandmeid. Samuti peab ta püüdma kontrollida töödeldavate isikuandmete kvaliteeti ja nii palju kui võimalik eristama faktidel põhinevaid isikuandmeid isiklikel hinnangutel põhinevatest isikuandmetest.

Ettepanek sisaldab sätteid, mis käsitlevad andmesubjektide õigusi, eelkõige teabe saamise õigust, oma isikuandmetega tutvumise õigust, andmete parandamise, kustutamise ja töötlemise piiramise õigust, ning selles sätestatakse, et neid õigusi saab kaudselt kasutada Euroopa Andmekaitseinspektori kaudu. Ettepanek hõlmab ka töötlemise turvalisuse ja vastutuse põhimõtet, millega nõutakse, et Euroopa Prokuratuur rakendaks asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada töötlemise riskidele vastav turvalisuse tase, dokumenteerida kõik töötlemistoimingud ja hinnata enne töötlemist andmekaitse mõju, kui töötlemisviis (nt uute tehnoloogiate kasutamine) tõenäoliselt tekitab suure riski isikute õigustele. Ettepanekus on ka säte, et kolleegium määrab andmekaitseametniku, kes tuleb nõuetekohaselt kaasata kõikidesse isikuandmete kaitsega seotud küsimustesse ja kes peab tagama, et Euroopa Prokuratuur järgib kohaldatavaid andmekaitse õigusakte.

8.3.2. Andmekaitse ELi tasandi ühistes infosüsteemides

Lisaks andmevahetusele liikmesriikide vahel ja piiriülese kuritegevuse vastu võitlemise ELi eriasutuste, näiteks Europoli, Eurojusti ja Euroopa Prokuratuuri loomisele on ELi tasandil kasutusele võetud mitu ühist infosüsteemi, mis võimaldavad ja toetavad koostööd ja andmete vahetamist liikmesriikide pädevate asutuste ja ELi ametiasutuste vahel konkreetsetel õiguskaitsega, sealhulgas piirivalve, sisserände ning varjupaiga- ja tollivaldkonnaga seotud eesmärkidel. Algselt loodi Schengeni ala ELi õigusest sõltumatult toimiva rahvusvahelise lepingu alusel, mille tulemusena arendati Schengeni infosüsteem (SIS) välja mitmepoolsete lepingute alusel ja see võeti hiljem üle ELi õigusesse. Viisainfosüsteem (VIS), Eurodac, Eurosur ja tolliinfosüsteem (TIS) loodi vahenditena, mida reguleerib ELi õigus.

Nende süsteemide järelevalvet teevad ühiselt riiklikud järelevalveasutused ja Euroopa Andmekaitseinspektor. Kõrgetasemelise kaitse tagamiseks teevad need ametiasutused koostööd järelevalve koordineerimisrühmades, kus käsitletakse

järgmisi suuremahulisi IT-süsteeme: 1) Eurodac; 2) viisainfosüsteem; 3) Schengeni infosüsteem; 4) tolliinfosüsteem ja 5) siseturu infosüsteem[844]. Järelevalve koordineerimisrühmad kohtuvad tavaliselt kaks korda aastas valitud esimehe juhatusel ja võtavad vastu suuniseid, arutavad piiriüleseid juhtumeid või võtavad vastu kontrollide ühisraamistikke.

Teise põlvkonna Schengeni infosüsteemi (SIS II), viisainfosüsteemi (VIS) ja Eurodaci operatiivjuhtimise eest vastutab 2012. aastal asutatud Euroopa suuremahuliste IT-süsteemide amet (eu-LISA)[845]. eu-LISA põhiülesanne on tagada nimetatud 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 selleaegse Euroopa Ühenduse liikmesriiki lepingu Beneluxi Majandusliidu riikide, Prantsusmaa ja Saksamaaga kokkuleppe kontrolli järkjärgulise kaotamise kohta nende ühispiiridel (Schengeni leping), et tagada isikute vaba liikumine ja kaotada piirikontroll Schengeni alal[846]. Et tasakaalustada avalikku julgeolekut ohustavat mõju, mis võib tekkida avatud piiride tõttu, tugevdati piirikontrolli Schengeni ala välispiiridel ning tugevdati riikide politsei- ja õigusasutuste koostööd.

Schengeni lepinguga liitus veel mitu riiki ja seejärel lõimiti Schengeni süsteem Amsterdami lepinguga lõplikult ELi õigusraamistikku[847]. Seda otsust hakati rakendama 1999. aastal. Schengeni infosüsteemi uusim versioon, teise põlvkonna Schengeni infosüsteem (SIS II) võeti kasutusele 9. aprillil 2013. Nüüd kasutavad seda kõik ELi liikmesriigid[848] ning Island, Liechtenstein, Norra ja Šveits[849]. Juurdepääs SIS II-le on ka Europolil ja Eurojustil.

844 Vt Euroopa Andmekaitseinspektori veebileht järelevalve kooskõlastamise kohta.

845 Euroopa Parlamendi ja nõukogu 25. oktoobri 2011. aasta määrus (EL) nr 1077/2011, millega asutatakse Euroopa amet vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimiseks, ELT 2011 L 286.

846 Beneluxi Majandusliidu riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vaheline leping kontrolli järkjärgulise kaotamise kohta nende ühispiiridel, EÜT 2000 L 239.

847 Euroopa ühendused (1997), Amsterdami leping, millega muudetakse Euroopa Liidu lepingut, Euroopa ühenduste aluslepinguid ja teatavaid nendega seotud akte, EÜT 1997 C 340.

848 Horvaatia, Iirimaa ja Küpros teevad ettevalmistusi SIS II-ga lõimumiseks, kuid ei ole veel selle osa. Vt Schengeni infosüsteemi teave Euroopa Komisjoni rände- ja siseasjade peadirektoraadi veebilehel.

849 Euroopa Parlamendi ja nõukogu 20. detsembri 2006. aasta määrus (EÜ) nr 1987/2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT 2006 L 381; Euroopa Liidu Nõukogu (2007), nõukogu 12. juuni 2007. aasta otsus 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT 2007 L 205.

SIS II koosneb keskinfosüsteemist (C-SIS), iga liikmesriigi riigisisesest süsteemist (N-SIS) ning keskinfosüsteemi ja liikmesriikide süsteemide vahelisest sidetaristust. Keskinfosüsteemis on liikmesriikide sisestatud teatud andmed isikute ja esemete kohta. Schengeni infosüsteemi kasutavad kogu Schengeni ala riikide piirivalve-, politsei-, tolli-, viisa- ja kohtuasutused. Igal liikmesriigil on oma riigisisene eksemplar keskinfosüsteemist (C-SIS) ehk riiklik Schengeni infosüsteem (N-SIS); seda ajakohastatakse pidevalt ja selle kaudu ajakohastatakse seega ka keskinfosüsteemi. Schengeni infosüsteemis on nelja liiki hoiatusteateid:

- isikul ei ole õigust Schengeni alale siseneda või seal viibida;
- kohtu- või õiguskaitseasutused on isiku või eseme kuulutanud tagaotsitavaks (nt Euroopa vahistamismäärused, diskreetse kontrolli taotlused);
- isik on kuulutatud kadunuks;
- esemed (nt paberraha, autod, kaubikud, tulirelvad ja isikut tõendavad dokumendid) on registreeritud kui varastatud või kadunud.

Hoiatusteate korral tuleb SIRENE büroode kaudu algatada järelmeetmed. SIS II-l on uued funktsioonid, näiteks võimalus sisestada järgmisi andmeid: biomeetrilised andmed (nt sõrmejäljed ja fotod); uut tüüpi hoiatusteated (nt varastatud vee- ja õhusõidukite, konteinerite või maksevahendite kohta); täiendatud hoiatusteated isikute ja esemete kohta; vahistamise, üleandmise või väljasaatmise eesmärgil tagaotsitavate isikutega seotud Euroopa vahistamismääruste koopiad.

SIS II põhineb kahel teineteist täiendaval õigusaktil: SIS II otsusel[850] ja SIS II määrusel[851]. ELi seadusandja kasutas otsuse ja määruse vastuvõtmiseks eri õiguslikke aluseid. Otsusega reguleeritakse SIS II kasutamist eesmärkidel, mis on hõlmatud politsei- ja õigusalase koostööga kriminaalasjades (endine ELi kolmas sammas). Määrust kohaldatakse viisade, varjupaiga, sisserände ja isikute vaba liikumisega seotud muu poliitika (endine esimene sammas) alla kuuluvate hoiatusmenetluste suhtes. Iga samba hoiatusmenetlusi tuli reguleerida eraldi õigusaktidega, sest mõlemad õigusaktid võeti vastu enne Lissaboni lepingut ja sammaste struktuuri kaotamist.

850 Nõukogu 12. juuni 2007. aasta otsus 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT L 205, 7. august 2007.

851 Euroopa Parlamendi ja nõukogu 20. detsembri 2006. aasta määrus (EÜ) nr 1987/2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, ELT L 381, 28. detsember 2006.

Mõlemas õigusaktis on andmekaitse-eeskirjad. SIS II otsusega keelatakse delikaatsete isikuandmete töötlemine[852]. Isikuandmete töötlemine kuulub nüüdisajastatud konventsiooni nr 108 kohaldamisalasse[853]. Lisaks on isikutel õigus tutvuda neid käsitlevate isikuandmetega, mis sisestatakse SIS II-te[854].

SIS II määrus reguleerib kolmandate riikide kodanike riiki sisenemise või riigis viibimise keelamiseks tehtud hoiatusteadete tingimusi ning sisestamise ja töötlemise menetlusi. Selles sätestatakse ka liikmesriiki sisenemise või seal viibimise eesmärgil lisa- ja täiendava teabe vahetamise eeskirjad[855]. Ka määruses on andmekaitse-eeskirjad. Isikuandmete kaitse üldmääruse artikli 9 lõikes 1 viidatud delikaatseid andmeliike ei tohi töödelda[856]. SIS II määrus hõlmab ka järgmisi andmesubjekti õigusi:

- andmesubjektiga seotud isikuandmete juurdepääsu õigus[857];
- faktiliselt ebaõigete andmete parandamise õigus[858];
- ebaseaduslikult säilitatavate andmete kustutamise õigus[859] ning
- õigus teavitamisele, kui andmesubjekti suhtes on sisestatud hoiatusteade. Teave esitatakse kirjalikult koos hoiatusteate aluseks olnud riigisisese otsuse koopiaga või viitega otsusele[860].

Teabe saamise õigust ei anta, kui 1) isikuandmeid ei ole saadud andmesubjektilt ja teabe esitamine osutub võimatuks või eeldaks ebaproportsionaalset jõupingutust; 2) andmesubjektil on see teave juba olemas või 3) riigisiseste õigusaktide kohaselt on võimalik piirang, muu hulgas riigi julgeoleku, riigikaitse ja avaliku korra kaitseks või kuritegude ennetamiseks[861].

852 SIS II otsuse artikkel 56; SIS II määruse artikkel 40.
853 SIS II otsuse artikkel 57.
854 SIS II otsuse artikkel 58; SIS II määruse artikkel 41.
855 SIS II määruse artikkel 2.
856 *Ibid.*, artikkel 40.
857 *Ibid.*, artikli 41 lõige 1.
858 *Ibid.*, artikli 41 lõige 5.
859 *Ibid.*, artikli 41 lõige 5.
860 *Ibid.*, artikli 42 lõige 1.
861 *Ibid.*, artikli 42 lõige 2.

Mõlema, SIS II otsuse ja SIS II määruse korral võib üksikisikute juurdepääsuõigusi SIS II suhtes kasutada mis tahes liikmesriigis ja neid käsitletakse kooskõlas selle liikmesriigi riigisisese õigusega[862].

> Näide: kohtuasi *Dalea vs. Prantsusmaa*[863] käsitles juhtumit, kus kaebuse esitajale ei antud Prantsusmaa viisat, sest Prantsusmaa ametiasutused olid Schengeni infosüsteemi teatanud, et teda ei tohi riiki lubada. Kaebuse esitaja püüdis Prantsusmaa andmekaitsekomisjoni ja lõpuks riiginõukogu kaudu taotleda andmetega tutvumist ja andmete parandamist või kustutamist, kuid asjata. EIK leidis, et kaebuse esitajast Schengeni infosüsteemi teatamine oli seaduslik ja sellel oli õiguspärane eesmärk kaitsta riigi julgeolekut. Et kaebuse esitaja ei tõendanud, et ta oli Schengeni alale pääsemisest keeldumise tõttu saanud reaalset kahju, ja et ametiasutused võtsid piisavaid meetmeid, et teda kaitsta meelevaldsete otsuste eest, oli sekkumine kaebuse esitaja õigusesse eraelu austamisele proportsionaalne. Kaebuse esitaja artikli 8 alusel esitatud kaebus tunnistati seega vastuvõetamatuks.

Riikliku Schengeni infosüsteemi (N-SIS) järelevalve eest vastutab iga liikmesriigi pädev järelevalveasutus. See asutus peab tagama, et vähemalt kord iga nelja aasta tagant korraldataks riikliku Schengeni infosüsteemi andmetöötlustoimingute audit[864]. Riikide järelevalveasutused teevad koostööd Euroopa Andmekaitseinspektoriga ja tagavad riikliku Schengeni infosüsteemi (N-SIS) koordineeritud järelevalve; keskinfosüsteemi (C-SIS) järelevalve eest vastutab Euroopa Andmekaitseinspektor. Läbipaistvuse huvides saadetakse Euroopa Parlamendile, nõukogule ja eu-LISA-le iga kahe aasta tagant ühine tegevusaruanne. Schengeni infosüsteemi järelevalve kooskõlastamise tagamiseks on loodud SIS II järelevalve koordineerimisrühm, kes kohtub kuni kaks korda aastas. Kooskõlastusrühm koosneb Euroopa Andmekaitseinspektorist ja nende liikmesriikide järelevalveasutuste esindajatest, kes on SIS II rakendanud, samuti Islandi, Liechtensteini, Norra ja Šveitsi esindajatest, sest Schengeni liikmeks olemise tõttu kohaldatakse SISi ka nende suhtes[865]. Küpros, Horvaatia ja Iirimaa ei ole veel SIS II-ga liitunud ning osalevad seepärast järelevalve koordineerimisrühmas üksnes vaatlejana. Järelevalve koordineerimisrühmas teevad Euroopa Andmekaitseinspektor ja riikide järelevalveasutused aktiivselt koostööd, vahetades

862 SIS II määruse artikli 41 lõige 1; SIS II otsuse artikkel 58.

863 EIK, *Dalea vs. Prantsusmaa*, nr 964/07, 2. veebruar 2010.

864 SIS II määruse artikli 60 lõige 2.

865 Vt Euroopa Andmekaitseinspektori veebileht Schengeni infosüsteemi kohta.

teavet, abistades üksteist auditite ja kontrollide tegemisel, kavandades ühtlustatud ettepanekuid võimalike probleemide ühiste lahenduste kohta ja teadvustades üldsusele andmekaitseõigusi[866]. SIS II järelevalve kooskõlastusrühm võtab andmesubjektide abistamiseks vastu ka suuniseid. Üks näide on juhend, mis abistab andmesubjekte nende juurdepääsuõiguste kasutamisel[867].

Väljavaated

2016. aastal hindas Euroopa Komisjon Schengeni infosüsteemi, milles selgus, et on loodud riiklikud mehhanismid, mis võimaldavad andmesubjektidel tutvuda SIS II-s oma isikuandmetega, neid parandada ja kustutada või saada ebaõigete andmete eest hüvitist[868]. SIS II tõhususe ja tulemuslikkuse täiustamiseks tegi Euroopa Komisjon kolm määruse ettepanekut:

- määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist, millega tunnistatakse kehtetuks SIS II määrus;

- määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist politseikoostöös ja kriminaalasjades tehtavas õigusalases koostöös, millega tunnistatakse muu hulgas kehtetuks SIS II otsus, ning

- määrus Schengeni infosüsteemi kasutamise kohta ebaseaduslikult riigis viibivate kolmandate riikide kodanike tagasisaatmiseks.

On oluline, et ettepanekud võimaldavad töödelda biomeetriliste andmete muid liike peale fotode ja sõrmejälgede, mis juba kuuluvad praegusesse SIS II süsteemi. Näokujutisi ja sõrmejälgi, peopesajälgi ja DNA-profiile säilitatakse ka SISi andmebaasis. SIS II määruses ja SIS II otsuses sätestati võimalus teha isiku tuvastamiseks päring sõrmejälgede järgi, kuid ettepanekutes tehakse see päring kohustuslikuks olukorras, kus isikut ei ole võimalik tuvastada teisiti. Kui see saab tehniliselt võimalikuks, hakatakse päringuid tegema ja isikuid tuvastama näokujutiste, fotode ja peopesajälgede järgi. Biomeetrilisi tunnuseid käsitlevad uued eeskirjad on eriline risk üksikisikute õigustele. Euroopa andmekaitseinspektor märkis oma arvamuses

866 SIS II määruse artikkel 46; SIS II otsuse artikkel 62.

867 Vt SIS II järelevalve koordineerimisrühm, Schengeni infosüsteem. Juurdepääsuõiguse kasutamise juhend, avaldatud Euroopa Andmekaitseinspektori veebilehel.

868 Euroopa Komisjon (2016), Komisjoni aruanne Euroopa Parlamendile ja nõukogule „Teise põlvkonna Schengeni infosüsteemi (SIS II) hindamine vastavalt määruse (EÜ) nr 1987/2006 artikli 24 lõikele 5, artikli 43 lõikele 3 ja artikli 50 lõikele 5 ning otsuse 2007/533/JSK artikli 59 lõikele 3 ja artikli 66 lõikele 5“, COM(2016) 880 final, Brüssel, 21. detsember 2016.

komisjoni ettepanekute[869] kohta, et biomeetrilised andmed on väga delikaatsed ja nende lisamine sellistesse ulatuslikesse andmebaasidesse peaks põhinema nende SISi kandmise vajalikkuse tõenduspõhisel hinnangul. Teisisõnu tuleb uute tunnuste töötlemise vajadust tõendada. Euroopa andmekaitseinspektor leidis ka, et rohkem tuleb selgitada, mis teavet saab DNA-profiili lisada. Et DNA-profiil võib sisaldada delikaatset teavet (eriti näiteks terviseprobleemide teavet), peavad SISis säilitatavad DNA-profiilid sisaldama ainult minimaalset teavet, mida on tingimata vaja kadunud isikute tuvastamiseks ning mille hulgast välistatakse selgelt tervise-, rassilise päritolu ja muu delikaatne teave[870]. Ettepanekutes kehtestatakse siiski täiendavad kaitsemeetmed andmete kogumise ja edasise töötlemise piiramiseks rangelt vajaliku ja operatiivselt nõutavaga ning juurdepääs piirdub isikutega, kellel on isikuandmete töötlemiseks operatiivvajadus[871]. Ettepanekud võimaldavad eu-LISA-l esitada liikmesriikidele korrapäraseid andmekvaliteedi aruandeid, et hoiatusteated andmekvaliteedi tagamiseks korrapäraselt läbi vaadata[872].

Viisainfosüsteem

Viisainfosüsteem (VIS), mida haldab samuti eu-LISA, töötati välja ELi ühise viisapoliitika rakendamise toetamiseks[873]. Viisainfosüsteem võimaldab Schengeni riikidel vahetada viisataotlejate andmeid täielikult tsentraliseeritud süsteemi kaudu, mis ühendab Schengeni riikide ELi-välistes riikides asuvaid konsulaate ja saatkondi kõigi Schengeni riikide välispiiridel asuvate piiripunktidega. Viisainfosüsteemiga töödeldakse Schengeni ala lühiajalisi ja transiitviisasid. Tänu viisainfosüsteemile saab piirikontroll biomeetriliste tunnuste, eelkõige sõrmejälgede abil kontrollida, kas viisa esitaja on selle seaduslik omanik, ning tuvastada dokumentideta või võltsdokumentidega isikud.

869 Euroopa Andmekaitseinspektor (2017), Euroopa andmekaitseinspektori arvamus, mis käsitleb Schengeni infosüsteemi uut õiguslikku alust, arvamus 7/2017, 2. mai 2017.

870 *Ibid*., punkt 22.

871 Euroopa Komisjon (2016), ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist politseikoostöös ja kriminaalasjades tehtavas õigusalases koostöös ning millega muudetakse määrust (EL) nr 515/2014 ja tunnistatakse kehtetuks määrus (EÜ) nr 1986/2006, nõukogu otsus 2007/533/JSK ja komisjoni otsus 2010/261/EL, COM(2016) 883 final, Brüssel, 21. detsember 2016.

872 *Ibid*., lk 15.

873 Euroopa Liidu Nõukogu (2004), nõukogu 8. juuni 2004. aasta otsus 2004/512/EÜ viisainfosüsteemi (VIS) kehtestamise kohta, ELT 2004 L 213; Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 767/2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), ELT 2008 L 218; Euroopa Liidu Nõukogu (2008), nõukogu 23. juuni 2008. aasta otsus 2008/633/JSK, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel, ELT 2008 L 218.

Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrusega (EÜ) nr 767/2008 (mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus)) reguleeritakse lühiajaliste viisade taotlustega seotud isikuandmete edastamise tingimusi ja menetlusi. Viisasüsteemi abil jälgitakse ka taotluste kohta tehtud otsuseid, sealhulgas viisa tühistamise, kehtetuks tunnistamise või pikendamise otsuseid[874]. Viisainfosüsteemi määrus käsitleb peamiselt taotleja, tema viisa, fotode ja sõrmejälgede andmeid, seoseid varasemate taotlustega ja taotlejaga kaasas olevate isikute taotlustoimikute või kutsujate andmeid[875]. Juurdepääs viisainfosüsteemi andmete sisestamiseks, andmete muutmiseks või kustutamiseks piirdub ainult viisasid väljastavate asutustega; juurdepääs andmetega tutvumiseks antakse viisasid väljastavatele asutustele ja asutustele, kellel on välispiiripunktides toimuva kontrollimise ning sisserände- ja varjupaigakontrollide pädevus.

Teatud tingimustel võivad riikide pädevad politseiasutused ja Europol taotleda viisainfosüsteemi sisestatud andmetega tutvumist terroriaktide ja kuritegude ennetamise, avastamise ja uurimise eesmärgil[876]. Viisainfosüsteem on loodud ühise viisapoliitika rakendamise toetamiseks ja seega rikutaks selle muutmisel õiguskaitsevahendiks eesmärgi piirangu põhimõtet; nagu on selgitatud peatükis 3.2, nõuab see põhimõte, et isikuandmeid töödeldakse ainult kindlal, selgel ja õiguspärasel eesmärgil ning töötlemine peab olema andmetöötluse eesmärgi suhtes piisav, asjakohane ja mitte liigne. Sel põhjusel ei anta riiklikele õiguskaitseasutustele ja Europolile viisainfosüsteemi andmebaasi pidevat juurdepääsu. Juurdepääs võidakse anda ainult iga kord eraldi ja sellega kaasnevad ranged kaitsemeetmed. Nende asutuste juurdepääsu viisainfosüsteemile ja sellega tutvumise tingimusi ning tagatisi reguleeritakse nõukogu otsusega 2008/633/JSK[877].

Viisainfosüsteemi määruses sätestatakse ka järgmised andmesubjekti õigused.

- Õigus saada vastutavalt liikmesriigilt teada selles liikmesriigis isikuandmete töötlemise eest vastutava töötleja nimi ja kontaktandmed, andmete viisainfosüsteemis töötlemise eesmärk, isikute kategooriad, kellele andmeid võidakse edastada

874 Viisainfosüsteemi määruse artikkel 1.

875 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 767/2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), ELT 2008 L 218, artikkel 5.

876 Euroopa Liidu Nõukogu (2008), nõukogu 23. juuni 2008. aasta otsus 2008/633/JSK, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel, ELT 2008 L 218.

877 *Ibid.*

(vastuvõtjad), ja andmete säilitamise kestus. Lisaks tuleb viisataotlejaid teavitada asjaolust, et nende isikuandmete kogumine viisainfosüsteemis on nende taotluse läbivaatamiseks kohustuslik, ning liikmesriigid peavad neile teatama ka, et neil on õigus oma andmetega tutvuda, taotleda nende parandamist või kustutamist, ning nende õiguste kasutamise korra[878].

- Õigus tutvuda viisainfosüsteemis säilitatavate neid käsitlevate isikuandmetega[879].

- Õigus lasta ebaõiged andmed parandada[880].

- Õigus ebaseaduslikult säilitatud andmed kustutada[881].

Viisainfosüsteemi järelevalve tagamiseks moodustati viisainfosüsteemi järelevalve koordineerimisrühm. See koosneb Euroopa Andmekaitseinspektori ja riiklike järelevalveasutuste esindajatest, kes kohtuvad kuni kaks korda aastas. Rühm koosneb ELi 28 liikmesriigi ning Islandi, Liechtensteini, Norra ja Šveitsi esindajatest.

Eurodac

Lühend Eurodac tähendab Euroopa sõrmejälgede võrdlemise süsteemi[882]. See on kesksüsteem, mis sisaldab ELi liikmesriigis varjupaika taotlevate kolmandate riikide kodanike sõrmejäljeandmeid[883]. Süsteem on olnud kasutusel alates jaanuarist 2003, millal võeti vastu nõukogu määrus (EÜ) nr 343/2003; uuesti sõnastatud

878 Viisainfosüsteemi määruse artikkel 37.

879 *Ibid*., artikli 38 lõige 1.

880 *Ibid*., artikli 38 lõige 2.

881 *Ibid*., artikli 38 lõige 2.

882 Vt Euroopa Andmekaitseinspektori veebileht Eurodaci kohta.

883 Nõukogu 11. detsembri 2000. aasta määrus (EÜ) nr 2725/2000, mis käsitleb sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist Dublini konventsiooni tõhusa kohaldamise eesmärgil, ELT 2000 L 316; nõukogu 28. veebruari 2002. aasta määrus (EÜ) nr 407/2002, millega nähakse ette sõrmejälgede võrdlemise Eurodac-süsteemi kehtestamist Dublini konventsiooni tõhusa kohaldamise eesmärgil käsitleva määruse (EÜ) nr 2725/2000 teatavad rakenduseeskirjad, ELT 2002 L 62 (Eurodaci määrus); Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 603/2013, millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest) tõhusaks kohaldamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil ning millega muudetakse määrust (EL) nr 1077/2011, millega asutatakse Euroopa amet vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimiseks, ELT 2013 L 180, lk 1 (uuesti sõnastatud Eurodaci määrus).

määrust hakati kohaldama 2015. aastal. Selle põhieesmärk on aidata määrata, mis liikmesriik vastutab konkreetse varjupaigataotluse läbivaatamise eest kooskõlas määrusega (EÜ) nr 343/2003. Määruses kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest (Dublini III määrus)[884]. Eurodacis säilitatavate isikuandmete põhieesmärk on toetada Dublini III määruse kohaldamist[885].

Riikide õiguskaitseasutustel ja Europolil on lubatud võrrelda kriminaaluurimistega seotud sõrmejälgi Eurodacis sisalduvate sõrmejälgedega, kuid ainult terrori- või muude raskete kuritegude ennetamise, avastamise või uurimise eesmärgil. Eurodac on loodud ELi varjupaigapoliitika rakendamise toetamise vahendina, mitte õiguskaitsevahendina, ja seepärast saavad õiguskaitseasutused juurdepääsu andmebaasile ainult erijuhtudel, eriasjaoludel ja rangete tingimuste alusel[886]. Andmete edasiseks kasutamiseks õiguskaitse eesmärgil kohaldatakse politsei- ja kriminaalõigusasutuste andmekaitse direktiivi; andmed, mille peamine eesmärk on hõlbustada Dublini III määruse kohaldamist, on kaitstud isikuandmete kaitse üldmääruse alusel. Liikmesriigi või Europoli uuesti sõnastatud Eurodaci määruse alusel saadud isikuandmete edasisaatmine mis tahes kolmandale riigile, rahvusvahelisele organisatsioonile või eraõiguslikule juriidilisele isikule, mis on asutatud ELis või väljaspool seda, on keelatud[887].

Eurodac koosneb eu-LISA hallatavast keskküsusest (kus säilitatakse ja võrreldakse sõrmejälgi) ning liikmesriikide ja keskandmebaasi vahelise elektroonilise andmeedastuse süsteemist. Liikmesriigid võtavad sõrmejäljed kõigilt vähemalt 14-aastastelt isikutelt, kes taotlevad nende territooriumil varjupaika, ja igalt vähemalt 14-aastaselt välismaalaselt või kodakondsuseta isikult, kes on kinni peetud välispiiri ebaseaduslikku ületamise tõttu, ning edastavad need keskküsusele. Samuti võivad liikmesriigid võtta ja edastada nende välismaalaste või kodakondsuseta isikute sõrmejäljed, kelle suhtes avastatakse, et nad viibivad riigi territooriumil ebaseaduslikult.

884 Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 604/2013, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest, ELT 2013 L 180 (Dublini III määrus).

885 Uuesti sõnastatud Eurodaci määrus, ELT 2013 L 180, lk 1, artikli 1 lõige 1.

886 *Ibid.*, artikli 1 lõige 2.

887 *Ibid.*, artikkel 35.

Kuigi kõik liikmesriigid võivad tutvuda Eurodaciga ja taotleda võrdlemist sõrmejäljeandmetega, on andmete muutmise, parandamise, täiendamise või kustutamise õigus ainult liikmesriigil, kes on sõrmejäljed kogunud ja edastanud need keskküksusele[888]. Andmekaitse jälgimiseks ja andmeturbe tagamiseks dokumenteerib eu-LISA kogu andmetöötluse[889]. Riiklikud järelevalveasutused abistavad andmesubjekte ja annavad nõuandeid, kuidas nad saavad kasutada oma õigusi[890]. Sõrmejäljeandmete kogumise ja edastamise kohtulikku kontrolli teevad riigisisesed kohtud[891]. Kesksüsteemi töötlemistoimingute suhtes kohaldatakse ELi institutsioonide andmekaitsemäärust[892] ja selle järelevalvet teeb Euroopa Andmekaitseinspektor; kesksüsteemi haldab Eurodaciga seoses eu-LISA[893]. Kui isik kannab kahju ebaseadusliku töötlemistoimingu või Eurodaci määrusega vastuolus oleva tegevuse tagajärjel, on tal õigus saada kahju eest vastutavalt liikmesriigilt hüvitist[894]. Tuleb siiski rõhutada, et varjupaigataotlejad on eriti haavatav inimrühm, kes on sageli läbinud pika ja ohtliku teekonna. Nad on haavatavad ja sageli on nad varjupaigataotluse läbivaatamise ajal ebakindlas olukorras, mis võib neil takistada õiguste, sealhulgas hüvitise saamise õiguse kasutamist.

Et kasutada Eurodaci õiguskaitse eesmärgil, peavad liikmesriigid määrama ametiasutused, kellel on õigus taotleda juurdepääsu, ning ametiasutused, kes kontrollivad, kas võrdlemise taotlused on õiguspärased[895]. Riigisisestel ametiasutustel ja Europolil on Eurodaci sõrmejäljeandmetele juurdepääs väga rangetel tingimustel. Taotlev asutus peab esitama põhjendatud elektroonilise taotluse alles pärast andmete võrdlemist muude kättesaadavate infosüsteemide, näiteks riiklike sõrmejäljeandmebaaside ja viisainfosüsteemi andmetega. Et võrdlemine oleks proportsionaalne, peab tegu olema suure ohuga avalikule julgeolekule. Võrdlemine peab olema tõeliselt vajalik, seotud kindla juhtumiga ja peab olema mõistlik põhjus arvata, et võrdlemine aitab oluliselt kaasa asjaomase kuriteo ennetamisele, avastamisele või uurimisele, eriti kui on põhjendatud kahtlus, et kahtlustatav, terroriakti

888 *Ibid.*, artikkel 27.

889 *Ibid.*, artikkel 28.

890 *Ibid.*, artikkel 29.

891 *Ibid.*, artikkel 29.

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

893 Uuesti sõnastatud Eurodaci määrus, ELT 2013 L 180, lk 1, artikkel 31.

894 *Ibid.*, artikkel 37.

895 Roots, L. (2015), *The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination*, Baltic Journal of European Studies, Tallinn University of Technology, 5. aastakäik, nr 2, lk 108–129.

või muu raske kuriteo sooritaja või kannatanu kuulub kategooriasse, kelle suhtes kohaldatakse sõrmejälgede kogumist Eurodaci süsteemi. Võrrelda tohib üksnes sõrmejäljeandmeid. Europol peab saama loa liikmesriigilt, kes sõrmejäljeandmed kogus.

Eurodacis säilitatavaid varjupaigataotlejate isikuandmeid hoitakse 10 aastat pärast sõrmejälgede võtmist, v.a kui andmesubjekt saab ELi liikmesriigi kodakondsuse. Sellisel juhul peab andmed kohe kustutama. Välispiiri ebaseaduslikul ületamisel kinni peetud välismaalaste andmeid säilitatakse 18 kuud. Kui andmesubjektile antakse elamisluba, ta lahkub ELi territooriumilt või on saanud liikmesriigi kodakondsuse, peab need andmed kohe kustutama. Varjupaiga saanud isikute sõrmejälgi võib võrrelda kolme aasta jooksul terroriaktide ja muude raskete kuritegude ennetamise, avastamise ja uurimise kontekstis.

Lisaks kõigile ELi liikmesriikidele rakendavad Eurodaci rahvusvaheliste lepingute alusel ka Island, Norra, Liechtenstein ja Šveits.

Eurodaci järelevalve tagamiseks moodustati Eurodaci järelevalve koordineerimisrühm. See koosneb Euroopa Andmekaitseinspektori ja riiklike järelevalveasutuste esindajatest, kes kohtuvad kuni kaks korda aastas. Rühm koosneb 28 ELi liikmesriigi ning Islandi, Liechtensteini, Norra ja Šveitsi esindajatest[896].

Väljavaated

2016. aasta mais tegi komisjon Euroopa ühise varjupaigasüsteemi toimimise parandamise reformi raames ettepaneku Eurodaci uuesti sõnastatud määruse kohta[897]. Kavandatav uuesti sõnastamine on oluline, sest sellega laiendatakse oluliselt Eurodaci algse andmebaasi ulatust. Eurodac loodi algselt selleks, et toetada Euroopa ühise varjupaigasüsteemi rakendamist, andes sõrmejäljetõendeid, mis võimaldavad määrata, mis liikmesriik vastutab ELis esitatud varjupaigataotluse läbivaatamise eest. Kavandatava uuesti sõnastamisega laiendatakse andmebaasi ulatust,

896 Vt Euroopa Andmekaitseinspektori veebileht Eurodaci kohta.

897 Euroopa Komisjon, ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem [määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest)] tõhusaks kohaldamiseks ja ebaseaduslikult riigis viibivate kolmandate riikide kodanike ja kodakondsuseta isikute tuvastamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil (uuesti sõnastatud), COM(2016) 272 final, 4. mai 2016.

et lihtsustada ebaseaduslike rändajate tagasisaatmist[898]. Riiklikud ametiasutused saavad andmebaasi alusel tuvastada kolmandate riikide kodanikud, kes viibivad ELis ebaseaduslikult või on sisenenud ELi ebaseaduslikult, et saada tõendeid, mis aitavad liikmesriikidel neid tagasi saata. Praeguse õiguskorra kohaselt tuleb koguda ja säilitada ainult sõrmejälgi, kuid ettepanekus kehtestatakse lisaks ka isikute näokujutiste kogumine[899], mis on samuti biomeetriliste andmete liik. Ettepanekuga vähendataks ka lastelt biomeetriliste andmete võtmise miinimumvanust – 6 aastani[900] 14 aasta asemel, mis on 2013. aasta määruse kohane miinimumvanus. Ettepaneku laiendatud kohaldamisala tähendab, et see sekkub enamate isikute eraelu puutumatuse ja andmekaitseõigusesse, kelle andmed võivad olla andmebaasi kantud. Sekkumise tasakaalustamiseks püütakse ettepanekus ning Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjoni (LIBE) esitatud muudatusettepanekutes[901] tugevdada andmekaitsenõudeid. Käsiraamatu koostamise ajal ettepaneku arutelu Euroopa Parlamendis ja nõukogus alles kestis.

Eurosur

Euroopa piiride valvamise süsteem (Eurosur)[902] on välja töötatud eesmärgiga tugevdada Schengeni välispiiride kontrolli ebaseadusliku sisserände ja piiriülese kuritegevuse avastamise, tõkestamise ja nende vastu võitlemise kaudu. See pakub teabevahetust ja operatiivkoostööd riiklike koordinatsioonikeskuste ja Frontexi, integreeritud

898 Vt ettepaneku seletuskiri, lk 3.

899 Euroopa Komisjon, ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem [määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest)] tõhusaks kohaldamiseks ja ebaseaduslikult riigis viibivate kolmandate riikide kodanike ja kodakondsuseta isikute tuvastamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil (uuesti sõnastatud), COM(2016) 272 final, 4. mai 2016, artikli 2 lõige 1.

900 *Ibid.*, artikli 2 lõige 2.

901 Euroopa Parlament, raport ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem [määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest)] tõhusaks kohaldamiseks ja ebaseaduslikult riigis viibivate kolmandate riikide kodanike ja kodakondsuseta isikute tuvastamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil (uuesti sõnastatud), PE 597.620v03-00, 9. juuni 2017.

902 Euroopa Parlamendi ja nõukogu 22. oktoobri 2013. aasta määrus (EÜ) nr 1052/2013, millega luuakse Euroopa piiride valvamise süsteem (EUROSUR), ELT 2013 L 295.

piirihalduse kontseptsiooni väljatöötamise ja kohaldamise eest vastutava uue ELi asutuse vahel[903]. Eurosuri üldeesmärgid on järgmised:

- vähendada ELi märkamatult sisenevate ebaseaduslike rändajate arvu;
- vähendada surmajuhtumite arvu ebaseaduslike rändajate seas, vältides inimeste hukkumist merel;
- suurendada kogu ELi sisejulgeolekut, aidates kaasa piiriülese kuritegevuse tõkestamisele[904].

Eurosur alustas tööd 2. detsembril 2013 kõigis välispiiridega liikmesriikides ja muudes liikmesriikides 1. detsembril 2014. Määrust kohaldatakse liikmesriikide maismaa-, mere- ja õhu-välispiiride valvamise suhtes. Eurosur vahetab ja töötleb isikuandmeid väga vähe, sest liikmesriikidel ja Frontexil on õigus vahetada ainult laevade registreerimisnumbreid. Eurosur vahetab operatiivteavet, näiteks patrullide asukoha ja vahejuhtumite toimumiskoha teavet, ning üldreeglina ei tohi vahetatav teave sisaldada isikuandmeid[905]. Erandjuhtudel, kui Eurosuri raames vahetatakse isikuandmeid, sätestatakse määruses, et täielikult kohaldatakse ELi andmekaitse üldist õigusraamistikku[906].

Eurosur tagab seega andmekaitse õiguse, nimelt märkides, et isikuandmete vahetamine peab vastama politsei- ja kriminaalõigusasutuste andmekaitse direktiivi ning isikuandmete kaitse üldmääruse kriteeriumidele ja kaitsemeetmetele[907].

---

903 Euroopa Parlamendi ja nõukogu 14. septembri 2916. aasta määrus (EL) 2016/1624, mis käsitleb Euroopa piiri- ja rannikuvalvet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2016/399 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 863/2007, nõukogu määrus (EÜ) nr 2007/2004 ning nõukogu otsus 2005/267/EÜ, ELT 2016 L 251.

904 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.

905 Euroopa Komisjon, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29. november 2013.

906 Määruse (EL) nr 1052/2013 põhjendus 13 ja artikkel 13.

907 *Ibid.*, põhjendus 13 ja artikkel 13.

Tolliinfosüsteem

Veel üks oluline ELis loodud ühine infosüsteem on tolliinfosüsteem (TIS)[908]. Siseturu loomisel kaotati kõik ELi territooriumil liikuvate kaupade kontrollid ja formaalsused, mis suurendas pettuste riski. Vastuseks sellele riskile tugevdati liikmesriikide tolliametite koostööd. Tolliinfosüsteemi eesmärk on aidata liikmesriike ELi tolli- ja põllumajanduseeskirjade raskete rikkumiste tõkestamisel, uurimisel ja nende eest vastutusele võtmisel. Tolliinfosüsteemi aluseks on kaks eri õigusliku alusega õigusakti. Üks on nõukogu määrus (EÜ) nr 515/97, mis käsitleb riigisiseste haldusasutuste koostööd eesmärgiga võidelda pettuste vastu tolliliidu ja ühise põllumajanduspoliitika raames, ning teine on nõukogu otsus 2009/917/JSK, mille eesmärk on abistada tollieeskirjade raskete rikkumiste ennetamisel, uurimisel ja nende eest vastutusele võtmisel. See tähendab, et tolliinfosüsteem on õiguskaitsest laiema kohaldusalaga.

Tolliinfosüsteemis sisalduv teave koosneb isikuandmetest, mis on seotud kaupade, transpordivahendite, äriühingute, isikute ning kinnipeetud, arestitud või konfiskeeritud esemete ja sularahaga. Töödeldavate andmete liigid on selgelt määratletud ja on muu hulgas asjaomaste isikute nimed, kodakondsus, sugu, sünnikoht ja -kuupäev, andmete süsteemi sisestamise põhjus ja sõiduki registreerimisnumber[909]. Seda teavet tohib kasutada üksnes vaatluste, aruannete, erikontrolli ja strateegilise või tegevusanalüüsi jaoks seoses tollieeskirjade rikkumises kahtlustatavatega.

Tolliinfosüsteemile on juurdepääs riikide tolli-, maksu-, põllumajandus-, rahvatervise- ja politseiasutustel ning Europolil ja Eurojustil.

Isikuandmete töötlemine peab toimuma kooskõlas määruses (EÜ) nr 515/97 ja nõukogu otsuses 2009/917/JSK kehtestatud erieeskirjadega, samuti isikuandmete kaitse üldmääruse, ELi institutsioonide andmekaitse määruse, nüüdisajastatud konventsiooni nr 108 ja politseisoovituse sätetega. Tolliinfosüsteemi määruse (EÜ) nr 45/2001 nõuetele vastavuse järelevalve eest vastutab Euroopa Andmekaitseinspektor. Ta kutsub vähemalt kord aastas kokku koosoleku kõigi riiklike andmekaitse järelevalveasutustega, kellel on pädevus seoses tolliinfosüsteemi järelevalvega.

908 Euroopa Liidu Nõukogu (1995), nõukogu 26. juuli 1995. aasta akt, millega koostatakse infotehnoloogia tolliotstarbelise kasutamise konventsioon, EÜT 1995 C 316, mida on muudetud järgmiste õigusaktidega: Euroopa Liidu Nõukogu (2009), nõukogu 13. märtsi 1997. aasta määrus (EÜ) nr 515/97 liikmesriikide haldusasutuste vastastikusest abist ning haldusasutuste ja komisjoni vahelisest koostööst tolli- ja põllumajandusküsimusi käsitlevate õigusaktide nõutava kohaldamise tagamiseks, nõukogu 30. novembri 2009. aasta otsus 2009/917/JSK infotehnoloogia tollialase kasutamise kohta (tolliinfosüsteemi otsus), ELT 2009 L 323.

909 Vt tolliinfosüsteemi otsuse artiklid 24, 25 ja 28.

ELi infosüsteemide koostalitlusvõime

Rändehaldus, ELi välispiiride integreeritud haldamine ning terrorismi- ja piiriülese kuritegevuse vastane võitlus on olulised ülesanded, mille keerukus globaliseerunud maailmas üha suureneb. Viimastel aastatel on EL püüdnud välja töötada uut terviklikku lähenemisviisi, et kaitsta ja säilitada julgeolekut, kahjustamata seejuures ELi väärtusi ja põhivabadusi. Selles tegevuses on eriti tähtis riiklike õiguskaitseasutuste ning liikmesriikide ja asjaomaste ELi asutuste tõhus teabevahetus[910]. Olemasolevatel ELi piirihalduse ja sisejulgeoleku infosüsteemidel on oma eesmärgid, institutsiooniline ülesehitus, andmesubjektid ja kasutajad. EL on töötanud selle nimel, et kõrvaldada ELi eri infosüsteemide, näiteks SIS II, VISi ja Eurodaci vahelise killustatud andmehalduse funktsioonide puudused, uurides selleks koostalitlusvõime võimalusi[911]. Põhieesmärk on tagada, et pädevatel politsei-, tolli- ja õigusasutustel oleks süstemaatiliselt olemas vajalik teave oma ülesannete täitmiseks, säilitades samal ajal tasakaalu eraelu puutumatuse, andmekaitse ja muude põhiõigustega.

Koostalitlusvõime on „infosüsteemide suutlikkus vahetada andmeid ja võimaldada teabe jagamist"[912]. Selline teabevahetus ei tohi rikkuda isikuandmete kaitse üldmääruses, politsei- ja kriminaalõigusasutuste andmekaitse direktiivis ja ELi põhiõiguste hartas tagatud vajalikke rangeid juurdepääsu- ja kasutustingimusi ega ühtki muud asjakohast eeskirja. Ükski integreeritud andmehalduse lahendus ei tohi mõjutada eesmärgipiirangu, lõimitud või vaikimisi andmekaitse põhimõtet[913].

910 Euroopa Komisjon (2016), komisjoni teatis Euroopa Parlamendile ja nõukogule „Piirivalve ja julgeoleku tugevamad ja arukamad infosüsteemid", COM(2016) 205 final, Brüssel, 6. aprill 2016; komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule ja nõukogule „Julgeoleku suurendamine liikuvas maailmas: parem teabevahetus terrorismivastase võitluse valdkonnas ja tugevamad välispiirid", COM(2016) 602 final, Brüssel, 14. september 2016; Euroopa Komisjon (2016), ettepanek: Euroopa Parlamendi ja nõukogu määrus Schengeni infosüsteemi kasutamise kohta ebaseaduslikult riigis viibivate kolmandate riikide kodanike tagasisaatmiseks. Vt ka komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule ja nõukogule „Kolmas eduaruanne tulemusliku ja tegeliku julgeolekuliidu suunas liikumise kohta", COM(2017) 261 final, Brüssel, 16. mai 2017.

911 Euroopa Liidu Nõukogu (2005), Haagi programm: vabaduse, turvalisuse ja õiguse tugevdamine Euroopa Liidus, ELT 2005 C 53, Euroopa Komisjon (2010), komisjoni teatis Euroopa Parlamendile ja nõukogule „Ülevaade teabehaldusest vabadusel, turvalisusel ja õigusel rajaneval alal", COM(2010) 385 final, Euroopa Komisjon (2016), komisjoni teatis Euroopa Parlamendile ja nõukogule „Piirivalve ja julgeoleku tugevamad ja arukamad infosüsteemid", COM(2016) 205 final, Brüssel, 6. aprill 2016; Euroopa Komisjon (2016), komisjoni 17. juuni 2016. aasta otsus, millega luuakse kõrgetasemeline infosüsteemide ja koostalitlusvõime eksperdirühm, ELT 2016 C 257.

912 Euroopa Komisjon (2016), komisjoni teatis Euroopa Parlamendile ja nõukogule „Piirivalve ja julgeoleku tugevamad ja arukamad infosüsteemid", COM(2016) 205 final, Brüssel, 6. aprill 2016, lk 14.

913 *Ibid.*, lk 4–5.

Lisaks kolme peamise infosüsteemi – SIS II, VIS ja Eurodac – funktsionaalsuse parandamisele on komisjon teinud ettepaneku luua neljas tsentraliseeritud piirihaldussüsteem, mis käsitleb kolmandate riikide kodanikke: riiki sisenemise ja riigist lahkumise süsteem (EES),[914] mis rakendatakse eeldatavasti 2020. aastaks[915]. Ka on komisjon teinud ettepaneku Euroopa reisiinfo ja -lubade süsteemi (ETIAS)[916] loomise kohta; süsteemi hakatakse koguma teavet ELi piires viisavabalt reisivate isikute kohta, et võimaldada teha ebaseadusliku rände ja julgeoleku eelkontrolle.

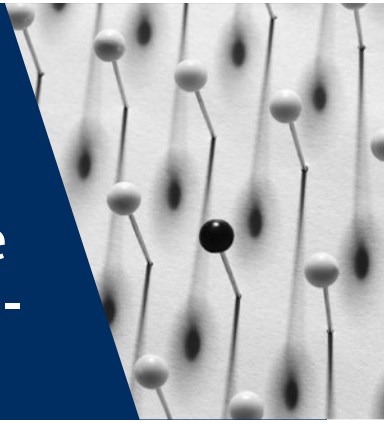
914 Euroopa Komisjon (2016), ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse riiki sisenemise ja riigist lahkumise süsteem Euroopa Liidu liikmesriikide välispiire ületavate kolmandate riikide kodanike riiki sisenemise ja riigist lahkumise andmete ja sisenemiskeelu andmete registreerimiseks ning määratakse kindlaks riiki sisenemise ja riigist lahkumise süsteemile õiguskaitse eesmärgil juurdepääsu andmise tingimused ning millega muudetakse määrust (EÜ) nr 767/2008 ja määrust (EL) nr 1077/2011, COM(2016) 194 final, Brüssel, 6. aprill 2016.

915 Euroopa Komisjon (2016), komisjoni teatis Euroopa Parlamendile ja nõukogule „Piirivalve ja julgeoleku tugevamad ja arukamad infosüsteemid", COM(2016) 205 final, Brüssel, 6. aprill 2016, lk 5.

916 Euroopa Komisjon (2016), ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse ELi reisiinfo ja -lubade süsteem (ETIAS) ning muudetakse määrusi (EL) nr 515/2014, (EL) 2016/399, (EL) 2016/794 ja (EL) 2016/1624, COM(2016) 731 final, 16. november 2016.

9

Andmete eriliigid ja nende asjakohased andmekaitse-eeskirjad



EL	Teemad	EN
Isikuandmete kaitse üldmäärus Eraelu puutumatuse ja elektroonilise side direktiiv	**Elektrooniline side**	Nüüdisajastatud konventsioon nr 108 Sideteenuste soovitus
Isikuandmete kaitse üldmääruse artikkel 88	**Töösuhted**	Nüüdisajastatud konventsioon nr 108 Tööhõivesoovitus EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 2007
Isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktid h ja i	**Meditsiinilised andmed**	Nüüdisajastatud konventsioon nr 108 Meditsiiniandmete kaitse soovitus EIK, *Z. vs. Soome*, nr 22009/93, 1997
Kliiniliste uuringute määrus	**Kliinilised uuringud**	
Isikuandmete kaitse üldmääruse artikli 6 lõige 4 ja artikkel 88	**Statistika**	Nüüdisajastatud konventsioon nr 108 Statistikaandmete kaitse soovitus
Määrus (EÜ) nr 223/2009 Euroopa statistika kohta ELK, C-524/06, *Huber vs. Bundesrepublik Deutschland* [suurkoda], 2008	**Ametlik statistika**	Nüüdisajastatud konventsioon nr 108 Statistikaandmete kaitse soovitus

EL	Teemad	EN
Direktiiv 2014/65/EL 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	Nüüdisajastatud konventsioon nr 108 Soovitus 90 (19) maksete ja muude seonduvate tehingute eesmärgil kasutatavate isikuandmete kaitse kohta EIK, *Michaud vs. Prantsusmaa*, nr 12323/11, 2012

Paljudel juhtudel on Euroopa tasandil vastu võetud eriõigusaktid, et kohaldada nüüdisajastatud konventsiooni nr 108 või isikuandmete kaitse üldmääruse üldpõhimõtteid teatud olukordade suhtes üksikasjalikumalt.

9.1. Elektrooniline side

Põhipunktid

- Erieeskirjad isikuandmete kaitse osas elektroonilise side teenuse osutamisel, eelkõige telefoniteenuse osas, on sätestatud Euroopa Nõukogu 1995. aasta soovituses.
- Isikuandmete töötlemist elektroonilise side teenuste osutamisel ELi tasandil reguleeritakse eraelu puutumatuse ja elektroonilise side direktiiviga.
- Elektroonilise side konfidentsiaalsus on seotud peale side sisu ka metaandmetega, näiteks teabega, kelle vahel side toimus, millal ja kui kaua, ning asukohaandmetega, näiteks kust andmeid edastati.

Sidevõrkudes on potentsiaalne kõrgendatud oht põhjendamatuks sekkumiseks isiku eraellu, sest sidevõrkudes on olemas võimsad tehnilised võimalused, millega pealt kuulata ja jälgida võrkudes toimuvat sidet. Sel põhjusel peeti vajalikuks kehtestada andmekaitse erieeskirjad, mis kaitseksid sideteenuste kasutajaid eririskide eest.

1995. aastal tegi **Euroopa Nõukogu** soovituse isikuandmete kaitse osas elektroonilise side teenuse osutamisel, eelkõige telefoniteenuste korral[917]. Soovituse kohaselt

917 Euroopa Nõukogu ministrite komitee (1995), *Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services*, 7. veebruar 1995.

peab isikuandmete kogumine ja töötlemine elektroonilise side teenuse osutamisel piirduma järgmiste eesmärkidega: kasutaja ühendamine võrguga, konkreetse sideteenuse pakkumine, arveldamine, kontrollimine, optimaalse tehnilise toimimise tagamine ning võrgu- ja teenusearendus.

Erilist tähelepanu pöörati ka sidevõrkude kasutamisele otseturustuse saatmise eesmärgil. Üldiselt ei tohi otseturustuspakkumisi saata ühelegi abonendile, kes on nende saamisest selge sõnaga loobunud. Automatiseeritud kõneseadmeid võib eelsalvestatud reklaamteadete saatmiseks kasutada üksnes siis, kui abonent on selleks andnud selgesõnalise nõusoleku. Valdkonna üksikasjalikud eeskirjad sätestatakse riigisisestes õigusaktides.

ELi õigusraamistikus võeti 2002. aastal, pärast esimest katset 1997. aastal, vastu eraelu puutumatuse ja elektroonilise side direktiiv, mida muudeti 2009. aastal. Eesmärk oli täiendada ja täpsustada eelmise andmekaitsedirektiivi sätteid sidesektori kohta[918].

Eraelu puutumatuse ja elektroonilise side direktiivi kohaldamisala hõlmab üldkasutatavate elektrooniliste võrkude sideteenuseid.

Eraelu puutumatuse ja elektroonilise side direktiivis eristatakse kolme põhiliiki andmeid, mis tekivad side ajal:

- side ajal saadetavate teadete sisu moodustavad andmed; need andmed on rangelt konfidentsiaalsed;
- side alustamiseks ja säilitamiseks vajalikud andmed ehk metaandmed (direktiivis „liiklusandmed") – näiteks sidepartnerite ning side toimumise aja ja kestuse teave;
- metaandmed sisaldavad sideseadme asukohta ehk asukohaandmeid eriandmeid – need andmed on ühtlasi seotud sidevahendi kasutaja asukohaga, eelkõige mobiilsidevahendite korral.

---

918 Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT 2001 L 201, mida on muudetud Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiviga 2009/136/EÜ, 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 2009 L 337.

Teenuseosutaja võib liiklusandmeid kasutada üksnes arveldamiseks ja teenuse tehniliseks pakkumiseks. Andmesubjekti nõusolekul võib neid andmeid siiski avaldada teistele vastutavatele töötlejatele, kes osutavad lisateenuseid, näiteks annavad kasutaja asukohaga seotud teavet lähima metroojaama või apteegi kohta või kohaliku ilmateate.

Lähtudes e-privaatsuse direktiivi artiklist 15, peab muu juurdepääs elektroonilistes võrkudes sisalduvatele andmetele vastamata isikuandmete kaitse õiguse õigustatud sekkumise nõuetele, nagu on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 lõikes 2 ning kinnitatud ELi põhiõiguste harta artiklitega 8 ja 52. Selline juurdepääs võib hõlmata näiteks kuritegude uurimist.

Eraelu puutumatuse ja elektroonilise side direktiivi 2009. aasta muudatused[919] lisasid direktiivile järgmist.

- Otseturunduslike e-kirjade saatmise piiranguid laiendati lühisõnumiteenustele, multimeediateenustele ja muudele sarnastele rakendustele; turunduse eesmärgil ei tohi e-kirju ilma eelneva nõusolekuta saata. Ilma sellise nõusolekuta tohib turunduse eesmärgil e-kirju saata ainult varasematele klientidele, kui nad on oma e-posti aadressi avaldanud ja kui neil ei ole selle saamise kohta vastuväiteid.

- Liikmesriikidele pandi kohustus luua õiguskaitsevahendid soovimatute teadete keelu rikkumiseks[920].

- Arvutikasutaja toiminguid jälgivate küpsiste ja tarkvara rakendamine ei ole ilma arvutikasutaja nõusolekuta enam lubatud. Nõusoleku esitamise ja saamise viisi tuleb piisava kaitse tagamiseks üksikasjalikumalt reguleerida riigisiseste õigusaktidega[921].

Ebaseadusliku juurdepääsu või andmete kaotsimineku või hävimise tõttu tekkinud rikkumisest tuleb viivitamata teavitada pädevat järelevalveasutust. Abonente

919 Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiv 2009/136/EÜ, 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 2009 L 337.

920 Vt muudetud direktiivi artikkel 13.

921 Vt *ibid.*, artikkel 5; vt ka artikli 29 töörühm (2012), *Opinion 04/2012 on cookie consent exemption*, WP 194, Brüssel, 7. juuni 2012.

tuleb teavitada, kui rikkumise tagajärjel on võimalik, et neile on tekkinud selle tõttu kahju[922].

Andmete säilitamise direktiivi[923] kohaselt peavad sideteenuste osutajad säilitama metaandmeid. Euroopa Liidu Kohus siiski tühistas selle direktiivi (üksikasjalikum teave on peatükis 8.3).

Väljavaated

2017. aasta jaanuaris tegi Euroopa Komisjon e-privaatsuse määruse ettepaneku, et asendada vana e-privaatsuse direktiiv. Eesmärk jääks samaks: kaitsta füüsiliste ja juriidiliste isikute põhiõigusi ja -vabadusi elektroonilise side teenuste pakkumisel ja kasutamisel ning eelkõige eraelu ja side puutumatuse õigusi ning kaitsta füüsilisi isikuid isikuandmete töötlemisel. Samal ajal on uue ettepaneku eesmärk tagada elektroonilise side andmete ja elektroonilise side teenuste vaba liikumine liidus[924]. Kui isikuandmete kaitse üldmääruse põhieesmärk käsitleb peamiselt ELi põhiõiguste harta artiklit 8, on kavandatud määruse ettepaneku eesmärk üle võtta ELi teisestesse õigusaktidesse harta artikkel 7.

Määrusega kavandatakse kohandada varasema direktiivi sätteid uute tehnoloogiate ja turuolukorraga ning luua terviklik ja järjepidev raamistik isikuandmete kaitse üldmäärusega. Selles mõttes oleks e-privaatsuse määrus isikuandmete kaitse üldmääruse suhtes *lex specialis*, kohandades seda isikuandmeid sisaldavate elektrooniliste sideandmetega. Uus määrus käsitleb ka elektroonilise side andmete töötlemist, sealhulgas elektroonilise side sisu ja metaandmeid, mis ei pruugi olla isikuandmed. Territoriaalne kohaldamisala piirdub ELiga, ka siis, kui ELis saadud andmeid töödeldakse väljaspool ELi, ja kohaldamisala laiendatakse „*over-the-top*"-sideteenuse osutajatele. Need on teenuseosutajad, kes pakuvad interneti kaudu sisu, teenuseid või rakendusi ilma võrguoperaatori või internetiteenuse osutaja otsese osaluseta. Sellised teenuseosutajad on näiteks Skype (hääl- ja videokõned), WhatsApp

922 Vt ka artikli 29 töörühm (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Brüssel, 5. aprill 2011.

923 Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, ELT 2006 L 105.

924 Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus) (COM(2017) 10 final), artikkel 1.

(sõnumside), Google (otsing), Spotify (muusika) või Netflix (videosisu). Uue määruse suhtes kohaldatakse isikuandmete kaitse üldmääruse jõustamismehhanisme.

Eeldatavasti võetakse e-privaatsuse määrus vastu enne 25. maid 2018, seni kohaldatakse isikuandmete kaitse üldmäärust kõigis 28 liikmesriigis. See sõltub siiski nii Euroopa Parlamendi kui ka nõukogu kokkuleppest[925].

9.2. Andmed töösuhtes

Põhipunktid

- Töösuhete andmekaitse erieeskirjad on esitatud Euroopa Nõukogu soovituses isikuandmete kaitse töösuhetes.
- Isikuandmete kaitse üldmääruses viidatakse konkreetselt töösuhetele ainult delikaatsete isikuandmete töötlemise sätetes.
- Nõusolek, mis peab olema antud vabatahtlikult, on töötajate isikuandmete töötlemise õigusliku alusena küsitav, sest tööandja ja töötajad on majanduslikult ebavõrdses seisundis. Nõusoleku andmise tingimusi tuleb hoolikalt hinnata.

ELis kohaldatakse töösuhete kontekstis isikuandmete töötlemisel ELi üldisi isikuandmete kaitse õigusakte. On siiski olemas määrus[926], mis konkreetselt käsitleb isikuandmete kaitset andmete töötlemisel (muu hulgas) töösuhete kontekstis Euroopa institutsioonides. Isikuandmete kaitse üldmääruses viidatakse otseselt töösuhetele artikli 9 lõikes 2, milles sätestatakse, et isikuandmeid võib töödelda, kui see tuleneb vastutava töötleja või andmesubjekti tööõigusest tulenevatest kohustustest ja eriõigustest.

Isikuandmete kaitse üldmääruse kohaselt peab töötajal olema võimalik selgelt eristada andmeid, mille töötlemise/säilitamisega ta on vabatahtlikult nõus, ning eesmärke, milleks tema andmeid säilitatakse. Enne nõusoleku andmist tuleb töötajaid teavitada ka nende õigustest ja andmete säilitamise ajast. Kui isikuandmetega

925 Lisateave: vt Euroopa Komisjon (2017), Komisjon teeb ettepaneku võtta elektroonilise side valdkonnas vastu kõrgetasemelised eraelu kaitse normid ja ajakohastab ELi institutsioonide andmekaitsenorme, pressiteade, 10. jaanuar 2017.

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

seotud rikkumine võib põhjustada füüsiliste isikute õigustele ja vabadustele suurt ohtu, peab tööandja teatama rikkumisest töötajale. Määruse artikkel 88 lubab liikmesriikidel kehtestada üksikasjalikumad eeskirjad, et tagada töötajate õiguste ja vabaduste kaitse seoses nende isikuandmetega töösuhete kontekstis.

Näide: kohtuasi *Worten*[927] käsitles juhtumit, kus andmed sisaldasid tööaja arvestust, sealhulgas igapäevast töö- ja puhkeaega, mis on isikuandmed. Riigisisese õigusega võidakse tööandjalt nõuda, et ta teeb tööaja arvestuse töötingimuste järelevalve eest vastutavatele riiklikele ametiasutustele kättesaadavaks. See annaks asjakohastele isikuandmetele vahetu juurdepääsu. Juurdepääs isikuandmetele on siiski vajalik, et võimaldada riiklikul ametiasutusel teha järelevalvet töötingimuste osas[928].

Euroopa Nõukogu tegi 1989. aastal töösuhete kontekstis soovituse ja 2015. aastal vaadati see läbi[929]. Soovitus hõlmab isikuandmete töötlemist era- ja avalikus sektoris. Töötlemine peab vastama teatud põhimõtetele ja piirangutele, mis on näiteks läbipaistvuse põhimõte ja töötajate esindajatega konsulteerimine enne jälgimisseadmete paigaldamist töökohas. Soovituses märgitakse ka, et tööandjad peaksid töötajate internetikasutuse jälgimise asemel kasutama ennetusmeetmeid, näiteks filtreid.

Artikli 29 töörühma töödokumendis on kõige sagedamate töösuhetega seotud andmekaitseprobleemide ülevaade[930]. Töörühm analüüsis nõusoleku olulisust töösuhete kontekstis töötlemise õigusliku alusena[931]. Leiti, et nõusolekut võtva tööandja ja nõusolekut andva töötaja majanduslik ebavõrdsus tekitab sageli kahtlusi, kas nõusolek anti vabatahtlikult. Sel põhjusel tuleb nõusoleku kehtivuse hindamisel hoolikalt kaaluda, kas nõusolek saab töösuhte kontekstis olla andmetöötluse õiguslikuks aluseks.

927 ELK, C-342/12, *Worten – Equipamentos para o Lar SA vs. Autoridade para as Condições de Trabalho (ACT)*, 30. mai 2013, punkt 19.

928 *Ibid.*, punkt 43.

929 Euroopa Nõukogu ministrite komitee (2015), *Recommendation Rec(2015)5 to member states on the processing of personal data in the context of employment*, aprill 2015.

930 Artikli 29 töörühm (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brüssel, 8. juuni 2017.

931 Artikli 29 töörühm (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brüssel, 25. november 2005.

Üks tänapäeva töökeskkonna andmekaitseprobleeme on see, mis ulatuses on töötajate elektroonilise side jälgimine töökohas õiguspärane. Sageli väidetakse, et probleemi lihtne lahendus oleks keelata töökohal sidevahendite isiklik kasutamine. See üldine keeld võib siiski olla ebaproportsionaalne ja seda võib olla raske teostada. Selles kontekstis pakuvad erilist huvi Euroopa Inimõiguste Kohtu otsused kohtuasjades *Copland vs. Ühendkuningriik* ja *Bărbulescu vs. Rumeenia*.

Näide: kohtuasi *Copland vs. Ühendkuningriik*[932] käsitles juhtumit, kus kolledžitöötaja telefoni-, e-posti ja internetikasutust jälgiti salaja, et kontrollida, kas ta kasutab kolledži ressursse isiklikul eesmärgil liiga palju. EIK leidis, et helistamine töökohast kuulub eraelu ja sõnumisaladuse mõiste alla. Seepärast kaitstakse sellist helistamist töökohast ja töökohast saadetavaid e-kirju, samuti interneti isikliku kasutamise jälgimisest saadavat teavet Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8. Kaebuse esitaja juhtumi korral leiti, et riigi õigusaktides puudusid sätteid, millega oleks reguleeritud, mis tingimustel tohib tööandja jälgida töötajate telefoni-, e-posti ja internetikasutust. Seega ei olnud sekkumine kooskõlas õigusaktidega. Kohus järeldas, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Näide: kohtuasi *Bărbulescu vs. Rumeenia*[933] käsitles juhtumit, kus kaebuse esitaja vallandati töökohal internetiühenduse kasutamise pärast töö ajal, mis rikkus sise-eeskirju. Tööandja jälgis tema sidet. Riigisiseses menetluses esitati tõendid, mis näitasid täiesti eraviisilisi sõnumeid. EIK leidis, et artikkel 8 on kohaldatav, ja jättis lahtiseks küsimuse, kas tööandja piiravad eeskirjad jätavad taotlejale eraelu puutumatuse õigustatud eelduse, kuid oli seisukohal, et tööandja juhised ei saa vähendada era- ja sotsiaalset elu töökohas nullini.

Sisulisest küljest tuli konventsioonis osalevatele riikidele anda ulatuslik kaalutlusruum, kui nad hindavad vajadust luua õigusraamistik, mis hõlmab tingimusi, mille alusel tööandja võib reguleerida oma töötajate töövälist elektroonilist või muus vormis teabevahetust töökohal. Riigisisesed ametiasutused peavad siiski tagama, et tööandja poolt kirjavahetuse ja muu teabevahetuse jälgimise meetmete kehtestamisega, olenemata meetmete ulatusest ja kestusest, kaasnevad asjakohased ja piisavad kaitsemeetmed kuritarvitamise vastu. Proportsionaalsus ja omavolivastased menetlustagatised on

932 EIK, *Copland vs. Ühendkuningriik*, nr 62617/00, 3. aprill 2007.

933 EIK, *Bărbulescu vs. Rumeenia* [suurkoda], nr 61496/08, 5. september 2017, punkt 121.

hädavajalikud ning Euroopa Inimõiguste Kohus tuvastas mitu nende asjaolude seisukohast olulist tegurit, näiteks mis ulatuses tööandjad töötajaid jälgivad, töötajate eraelu puutumatusse sekkumise ulatus, tagajärjed töötajale ning see, kas tagatud on piisavad kaitsemeetmed. Peale selle peavad riigisisesed ametiasutused tagama, et töötajale, kelle teabevahetust on jälgitud, on juurdepääs õiguskaitsevahendile kohtus, kelle pädevuses on vähemalt sisuliselt määrata, kuidas neid kriteeriume järgiti ja kas vaidlustatud meetmed olid seaduslikud.

Kohtuasjas tuvastas Euroopa Inimõiguste Kohus konventsiooni artikli 8 rikkumise, sest riigisisesed ametiasutused ei pakkunud piisavat kaitset kaebuse esitaja õigusele eraelu ja sõnumisaladuse austamisele ning ei suutnud seega õiglaselt tasakaalustada asjaomaseid huve.

Euroopa Nõukogu soovituse kohaselt peavad töösuhete eesmärgil kogutud isikuandmed olema saadud otse asjaomaselt töötajalt.

Töölevõtmise eesmärgil võib isikuandmeid koguda üksnes ulatuses, mida on vaja kandidaatide sobivuse ja karjääripotentsiaali hindamiseks.

Soovituses käsitletakse konkreetselt ka andmeid, mis sisaldavad hinnanguid töötaja töötulemuste või potentsiaali kohta. Need andmed peavad põhinema õiglastel ja ausatel hinnangutel ning nende sõnastus ei tohi olla solvav. See tuleb tagada ka andmete õiglase töötlemise ja andmete õigsuse põhimõtetest lähtudes.

Tööandja ja töötajate suhetes on andmekaitseõiguse eriaspektina käsitletav ka töötajate esindajate roll. Esindajad võivad saada töötajate isikuandmeid ainult ulatuses, mida on vaja töötajate huvide esindamiseks, või kui neid on vaja kollektiivlepingutes sätestatud kohustuste täitmiseks või järelevalveks.

Töösuhete raames kogutud delikaatseid isikuandmeid võib töödelda ainult erijuhtudel ja riigi õigusaktides sätestatud tagatiste alusel. Tööandjad võivad töötajatelt või töölesoovijatelt küsida terviseseisundi kohta või teha meditsiinilise läbivaatuse üksnes siis, kui see on vajalik, näiteks selleks, et leida, kas nad sobivad töökohale, et täita ennetava meditsiini nõudeid, kaitsta andmesubjekti või muude töötajate ja üksikisikute elulisi huve, võimaldada anda sotsiaaltoetusi või vastata kohtunõuetele. Terviseandmeid ei tohi koguda muudest allikatest kui asjaomaselt töötajalt endalt, v.a kui ta on andnud selleks selgesõnalise ja teadliku nõusoleku või kui see on ette nähtud riigisiseste õigusaktidega.

Soovituse kohaselt tuleb töötajatele teatada, mis eesmärgil nende isikuandmeid töödeldakse, mis liiki isikuandmeid kogutakse, kellele neid korrapäraselt edastatakse ning mis eesmärgil ja õiguslikul alusel selline andmete avalikustamine toimub. Elektroonilisele sidele võib töökohas olla juurdepääs ainult turvalisuse või muudel õiguspärastel põhjustel ja selline juurdepääs on lubatud alles pärast seda, kui töötajaid on teavitatud, et tööandjal võib olla juurdepääs sellisele teabevahetusele.

Töötajatel peab olema õigus tutvuda töösuhte raames kogutud andmetega ja lasta need vajaduse korral parandada või kustutada. Hinnanguid sisaldavate andmete töötlemisel peab töötajatel olema ka õigus hinnanguid vaidlustada. Neid õigusi võib siiski ajutiselt piirata sisejuurdluste eesmärgil. Kui töötajale ei võimaldata töösuhtega seotud isikuandmetega tutvumist või nende parandamist või kustutamist, peab tal riigisisestes õigusaktides sätestatud asjakohaste menetluste abil olema võimalik keeldumine vaidlustada.

9.3. Terviseandmed

Põhipunkt

- Meditsiiniandmed on delikaatsed andmed ja seega kohaldatakse nende suhtes erikaitset.

Andmesubjekti terviseseisundit käsitlevad isikuandmed on isikuandmete kaitse üldmääruse artikli 9 lõike 1 ja nüüdisajastatud konventsiooni nr 108 artikli 6 alusel delikaatsed isikuandmed. See tähendab, et terviseandmete suhtes kohaldatakse rangemaid andmetöötlusnõudeid kui tavaliste andmete suhtes. Isikuandmete kaitse üldmäärusega keelatakse töödelda „terviseandmeid“ (st „kõik andmesubjekti tervislikku seisundit käsitlevad andmeid, mis annavad teavet andmesubjekti endise, praeguse või tulevase füüsilise või vaimse tervise kohta“)[934], samuti geneetilisi andmeid ja biomeetrilisi andmeid, v.a kui nende töötlemine on lubatud artikli 9 lõike 2 kohaselt. Mõlemat liiki andmed on lisatud andmete eriliikide loetellu[935].

934 Isikuandmete kaitse üldmäärus, põhjendus 35.

935 *Ibid.*, artikkel 2.

Näide: kohtuasi *Z. vs. Soome*[936] käsitles juhtumit, kus kaebuse esitaja endine abikaasa, kellel oli HIV-infektsioon, oli sooritanud mitu seksuaalkuritegu. Hiljem mõisteti ta süüdi tapmises, sest oli teadlikult ohustanud ohvreid HIV-infektsiooni riskiga. Soome kohus otsustas hoida kohtuotsust ja kohtutoimikuid konfidentsiaalsena 10 aastat, kuigi kaebuse esitaja taotles pikemat tähtaega. Apellatsioonikohus ei rahuldanud neid taotlusi ja selle otsuses oli kaebuse esitaja ja tema endise abikaasa täisnimi. EIK leidis, et seda sekkumist ei saa pidada demokraatlikus ühiskonnas vajalikuks, sest era- ja perekonnaelu austamise õiguse kasutamise korral on meditsiiniandmete kaitse väga oluline, eelkõige kui tegu on HIV-infektsiooni teabega, mida peetakse paljudes ühiskondades häbistavaks. Seega kohus järeldas, et kui apellatsioonikohtu otsus on konfidentsiaalne ainult 10 aastat pärast otsuse tegemist ning tähtaja möödumisel tekib juurdepääs otsuses sisalduvale teabele, milles kirjeldatakse kaebuse esitaja isikut ja terviseseisundit, rikutakse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

ELi õiguses võib isikuandmete kaitse üldmääruse artikli 9 lõike 2 kohaselt meditsiiniandmeid töödelda, kui seda on vaja ennetava meditsiini, meditsiinilise diagnoosi, meditsiinilise abi või ravi võimaldamise või tervishoiuteenuste juhtimise jaoks. Neid andmeid tohib siiski töödelda üksnes kutsesaladuse hoidmise kohustusega tervishoiutöötaja või muu isik, kellel on samaväärne kohustus.

Euroopa Nõukogu õiguses käsitletakse konventsiooni nr 108 põhimõtete rakendamist meditsiinis toimuva andmetöötluse suhtes üksikasjalikumalt Euroopa Nõukogu 1997. aasta meditsiiniandmete kaitse soovituses[937]. Selles soovitatud eeskirjad on kooskõlas isikuandmete kaitse üldmääruse sätetega, mis käsitlevad meditsiiniandmete töötlemise õiguspäraseid eesmärke, terviseandmete kasutajate kutsesaladuse hoidmise kohustust ning andmesubjektide õigusi seoses läbipaistvuse, andmetega tutvumise ning andmete parandamise ja kustutamisega. Lisaks ei tohi meditsiiniandmeid, mida tervishoiutöötajad töötlevad seaduslikult, edastada õiguskaitseasutustele, v.a kui kehtestatud on piisavad tagatised, et vältida andmete sellist avaldamist, millega rikutakse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni

936 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.

937 Euroopa Nõukogu ministrite komitee (1997), *Recommendation Rec(97)5 to member states on the protection of medical data*, 13. veebruar 1997. Soovitust vaadatakse praegu läbi.

artikliga 8 tagatud õigust eraelu puutumatusele[938]. Riigisisene õigus peab olema sõnastatud piisavalt täpselt ja tagama piisava õiguskaitse omavoli eest[939].

Meditsiiniandmete kaitse soovituses on esitatud ka erisätted loote ja piiratud teovõimega isikute meditsiiniandmete kohta ning geneetiliste andmete töötlemise kohta. Soovituses on selge sõnaga viidatud, et andmeid võib vajadusest pikema aja jooksul säilitada teadusuuringute eesmärkidel, kuigi tavaliselt tuleb andmed selleks anonüümida. Meditsiiniandmete kaitse soovituse artiklis 12 soovitatakse üksikasjalikke eeskirju juhtudeks, kui teadlastel on vaja kasutada isikuandmeid ja anonüümitud andmetest ei piisa.

Et täita teadustöö vajadusi ja ühtlasi kaitsta patsientide huve, võib olla vaja andmed pseudonüümida. Pseudonüümimist andmekaitses käsitletakse üksikasjalikumalt punktis 2.1.1.

Euroopa Nõukogu 2016. aasta geneetiliste uuringute tulemuste andmete kaitse soovitus kehtib ka meditsiinis toimuva andmetöötluse suhtes[940]. See soovitus on väga oluline e-tervishoius, kus meditsiiniteenuseid osutatakse IKT-vahendite abil. Näide: patsiendi isadustesti tulemuste saatmine ühelt tervishoiuteenuse osutajalt teisele. Soovituse eesmärk on kaitsta nende isikute õigusi, kelle isikuandmeid töödeldakse kindlustuse eesmärgil, et teda kindlustada tervise, kehalise puutumatuse, vanuse või surmaga seotud riskide vastu. Kindlustusandjad peavad põhjendama terviseandmete töötlemist ning see peab olema proportsionaalne hinnatava riski olemuse ja tähtsusega. Selliste andmete töötlemine sõltub isiku nõusolekust. Kindlustusandjad peaksid olema võtnud kaitsemeetmed ka terviseandmete säilitamisel.

Kliinilised uuringud mis hõlmavad uute ravimite toime hindamist patsientidele dokumenteeritud uuringukeskkonnas, on oluline andmekaitsemõju. Inimravimite kliinilisi uuringuid reguleeritakse Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta määruses (EL) nr 536/2014, milles käsitletakse inimtervishoius kasutatavate ravimite

938 EIK, *Avilkina jt vs. Venemaa*, nr 1585/09, 6. juuni 2013, punkt 53. Vt ka EIK, *Biriuk vs. Leedu*, nr 23373/03, 25. november 2008.

939 EIK, *L.H. vs. Läti*, nr 52019/07, 29. aprill 2014, punkt 59.

940 Euroopa Nõukogu ministrite komitee (2016), *Recommendation Rec(2016)8 to member states on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests*, 26. oktoober 2016.

kliinilisi uuringuid ja millega tunnistatakse kehtetuks direktiiv 2001/20/EÜ (kliiniliste uuringute määrus)[941]. Kliiniliste uuringute määruse põhielemendid on järgmised:

- ühtlustatud taotlusmenetlus ELi portaali kaudu[942];
- kliiniliste uuringute taotluste hindamise tähtajad[943];
- hindamises osaleb eetikakomitee kooskõlas liikmesriikide õigusega (ja Euroopa õigusaktidega, milles sätestatakse asjaomased ajavahemikud),[944] ning
- kliiniliste uuringute ja nende tulemuste suurem läbipaistvus[945].

Isikuandmete kaitse üldmääruses on sätestatud, et kliiniliste uuringutega teadusuuringutes osalemiseks nõusoleku küsimisel kohaldatakse määrust (EL) nr 536/2014[946].

ELi tasandil on menetluses paljud õiguslikud ja muud algatused, mis käsitlevad isikuandmeid tervishoius[947].

Digitaalsed terviselood

Digitaalne terviselugu on määratletud kui „isiku varasemat ja praegust füüsilist ja vaimset tervist kirjeldav terviklik digitaalne meditsiinikaart või samalaadne dokument, mille andmed on hõlpsasti kättesaadavad ravialastel ja muudel nendega lähedalt seotud eesmärkidel“[948]. Digitaalsed terviselood on patsientide haiguslugude elektroonilised versioonid, mis võivad sisaldada nende kliinilisi andmeid, näiteks varasemate haiguste, terviseprobleemide ja seisundite, ravimite ja ravi

941 Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta määrus (EL) nr 536/2014, milles käsitletakse inimtervishoius kasutatavate ravimite kliinilisi uuringuid ja millega tunnistatakse kehtetuks direktiiv 2001/20/EÜ (kliiniliste uuringute määrus), ELT 2014 L 158.

942 Kliiniliste uuringute määruse artikli 5 lõige 1.

943 *Ibid*., artikli 5 lõiked 2–5.

944 *Ibid*., artikli 2 lõike 2 punkt 11.

945 *Ibid*., artikli 9 lõige 1 ja põhjendus 67.

946 Isikuandmete kaitse üldmääruse põhjendused 156 ja 161.

947 Euroopa Andmekaitseinspektor (2013), Euroopa andmekaitseinspektori arvamus komisjoni teatise „E-tervise 2012.–2020. aasta tegevuskava: innovatiivne tervishoid 21. sajandil“ kohta, Brüssel, 27. märts 2013.

948 Komisjoni 2. juuli 2008. aasta soovitus digitaalsete terviseloosüsteemide piiriülese koostalitlusvõime kohta, punkti 3 alapunkt c.

ning uuringu- ja laboritulemuste vastuseid. Neid elektroonilisi faile, mis võivad olla täielikud terviselood, katkendid või kokkuvõtted, saavad kasutada perearstid, apteekrid ja muud tervishoiutöötajad. Mõiste „e-tervis" on seotud ka digitaalsete terviselugudega.

> Näide: A on sõlminud kindlustusandjaga B kindlustuspoliisi. B kogub A-lt teatud terviseandmeid, näiteks olemasolevate terviseprobleemide või haiguste kohta. B peaks säilitama A terviseandmeid muudest andmetest eraldi. Samuti peab B säilitama A terviseandmeid eraldi muudest isikuandmetest. See tähendab, et A terviseandmetele on juurdepääs üksnes A toimiku menetlejal.

Digitaalsete tervisetoimikute tõttu tekivad siiski teatud andmekaitseprobleemid, näiteks nende kättesaadavus, nõuetekohane säilitamine ja andmesubjekti juurdepääs.

Lisaks digitaalsete terviselugude soovitusele avaldas komisjon 10. aprillil 2014 mobiilse tervishoiu (m-tervis) käsitleva rohelise raamatu, kus leidis, et m-tervis on arenev ja kiiresti kasvav valdkond, mis võib tervishoidu muuta, suurendada selle tõhusust ja arendada kvaliteeti. Mõiste hõlmab meditsiini- ja rahvatervishoiu tavasid, mida toetavad mobiilseadmed, näiteks mobiiltelefonid, patsiendi jälgimisseadmed, personaalarvutid ja muud juhtmeta seadmed, samuti meditsiiniseadmete või anduritega ühendatavad rakendused (nt heaolurakendused)[949]. Dokumendis kirjeldatakse riske isikuandmete kaitse õigusele, mis võib kaasneda m-tervise arenguga, ning sätestatakse, et terviseandmete delikaatsust arvestades peaks areng hõlmama patsiendi andmete konkreetseid ja sobivaid turvameetmeid (nt krüptimine) ja asjakohaseid patsiendi autentimise mehhanisme, et turvariske leevendada. M-tervise lahenduste vastu usalduse tekitamiseks on hädavajalik järgida isikuandmete kaitse eeskirju, muu hulgas andmesubjektile teabe andmise kohustust, andmete turvalisust ja isikuandmete seadusliku töötlemise põhimõtet[950]. Sel eesmärgil on nimetatud valdkonnas välja töötatud tegevusjuhend, mis põhineb paljude sidusrühmade sisendil, sealhulgas andmekaitse, enese- ja kaasreguleerimise, IKT ja tervishoiu valdkonnas kogemusi omavatelt esindajatelt[951]. Käsiraamatu koostamise ajal esitati käitumisjuhendi kavand artikli 29 töörühmale kommenteerimiseks enne ametlikku heakskiitmist.

949 Euroopa Komisjon (2014), Roheline raamat mobiilse tervishoiu ehk m-tervise kohta, COM(2014) 219 final, Brüssel, 10. aprill 2014.

950 *Ibid.*, punkt 8.

951 *Draft Code of Conduct on privacy for mobile health applications*, 7. juuni 2016.

9.4. Andmete töötlemine teadusuuringute ja statistilisel eesmärgil

Põhipunktid

- Teadus- või ajaloouuringute või statistilisel eesmärgil kogutud andmeid ei tohi kasutada muul eesmärgil.
- Teatud eesmärgil seaduslikult kogutud andmeid võib täiendavalt kasutada teadus- või ajaloouuringute või statistilisel eesmärgil, kui on kehtestatud piisavad kaitsemeetmed. Selleks võivad niisuguseid tagatisi pakkuda andmete anonüümimine või pseudonüümimine enne edastamist kolmandatele isikutele.

ELi õiguse kohaselt on lubatud andmete töötlemine statistilisel ja teadus- või ajaloouuringute eesmärgil, kui on sätestatud andmesubjektide õiguste ja vabaduste asjakohased kaitsemeetmed. Need meetmed võivad hõlmata pseudonüümimist[952]. ELi või riigisiseses õiguses võidakse sätestada andmesubjektide õiguste teatud erandid, kui need õigused muudavad uuringu õiguspärase eesmärgi saavutamise tõenäoliselt võimatuks või takistavad seda oluliselt[953]. Erandeid võib kehtestada andmesubjekti õigusele andmetega tutvuda, neid parandada, andmete töötlemist piirata ja vastuväiteid esitada.

Kuigi vastutav töötleja võib andmeid, mille ta seaduslikul alusel teatud eesmärgil kogus, taaskasutada omaenda statistilisel, teadus- või ajaloouuringute eesmärgil, tuleb andmed enne kolmandale isikule statistilisel, teadus- või ajaloouuringute eesmärgil edastamist olenevalt kontekstist anonüümida või pseudonüümida, v.a kui andmesubjekt on andnud nõusoleku või see on sätestatud riigisiseses õiguses. Teisiti kui anonüümsete andmete korral, kohaldatakse pseudonüümitavate andmete suhtes jätkuvalt isikuandmete kaitse üldmäärust[954].

Seega kohaldatakse määruses teadusuuringute suhtes andmekaitse üldeeskirjade kontekstis erikohtlemist, et vältida teadusuuringute arendamise piiranguid ja täita Euroopa teadusruumi saavutamise eesmärki, mis on sätestatud ELi toimimise lepingu artiklis 179. Määruses sätestatakse isikuandmete teaduslikel eesmärkidel töötlemise lai tõlgendus, mille hulka kuuluvad tehnika arendamine ja tutvustamine,

952 Isikuandmete kaitse üldmääruse artikli 89 lõige 1.

953 *Ibid.*, artikli 89 lõige 2.

954 *Ibid.*, põhjendus 26.

alusuuringud, rakendusuuringud ja erasektori rahastatud teadusuuringud. Määruses tunnustatakse andmete teadustöö eesmärgil registritesse kogumise tähtsust ja võimalikke raskust isikuandmete töötlemise edasise eesmärgi täielikul tuvastamisel andmete teadusuuringute eesmärgil kogumise ajal[955]. Sel põhjusel võimaldab määrus neid andmeid töödelda ilma andmesubjektide nõusolekuta, kui on olemas asjakohased kaitsemeetmed.

Oluline näide andmete kasutamisest statistilisel eesmärgil on riikide ja ELi statistikaametite ametlik statistika, mida nad saavad riigisiseste ja ELi ametliku statistika õigusaktide kohaselt, mille järgi on kodanikud ja ettevõtjad üldiselt kohustatud avaldama andmeid asjaomastele statistikaasutustele. Statistikaasutuste töötajatel on kutsesaladuse hoidmise erikohustused, mida tuleb nõuetekohaselt täita, sest see on statistikaasutustele andmeid avaldavate kodanike usalduse seisukohalt väga oluline[956].

Määrus (EÜ) nr 223/2009 Euroopa statistika kohta (Euroopa statistika määrus) sisaldab olulisi andmekaitse-eeskirju ametliku statistika kontekstis ning seepärast võib seda pidada asjakohaseks ka riigisisese ametlikku statistika sätete korral[957]. Määruses kasutatakse põhimõtet, et ametliku statistika koostamine vajab piisavalt selget õiguslikku alust[958].

Näide: kohtuasjas *Huber vs. Bundesrepublik Deutschland*[959] kaebas Saksamaale kolinud Austria ärimees, et välisriigi kodanike isikuandmete kogumise ja säilitamisega Saksa ametiasutuste poolt keskregistris (AZR) ka statistilisel eesmärgil rikuti tema andmekaitsedirektiivist tulenevaid õigusi. Arvestades, et direktiivi 95/46/EÜ eesmärk on tagada kõikides liikmesriikides samaväärne

955 *Ibid.*, põhjendused 33, 157 ja 159.

956 *Ibid.*, artikkel 90.

957 Euroopa Parlamendi ja nõukogu 11. märtsi 2009. aasta määrus (EÜ) nr 223/2009 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 2009 L 87, mida on muudetud Euroopa Parlamendi ja nõukogu 29. aprilli 2015. aasta määrusega (EL) 2015/759, millega muudetakse määrust (EÜ) nr 223/2009 Euroopa statistika kohta, ELT 2015 L 123.

958 Seda põhimõtet käsitletakse üksikasjalikumalt Eurostati Euroopa statistika tegevusjuhises, milles on Euroopa statistika määruse artikli 11 kohased ametliku statistika koostamise eetikajuhised, sealhulgas isikuandmete vastutustundliku kasutamise kohta.

959 ELK, C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008; vt eelkõige punkt 68.

andmekaitse tase, leidis Euroopa Liidu Kohus, et kõrgetasemelise kaitse tagamiseks ELis ei saa artikli 7 punktis e esitatud vajalikkuse mõistel olla liikmesriigiti erinev tähendus. Seega on see mõiste, millel on ELi õiguses oma iseseisev tähendus ja mida tuleb tõlgendada viisil, mis vastab täielikult direktiivi 95/46/EÜ eesmärgile. Euroopa Liidu Kohus märkis, et statistilisel eesmärgil tuleks nõuda ainult anonüümset teavet, ja otsustas, et Saksamaa register ei ole kooskõlas artikli 7 punktis e sätestatud vajalikkuse nõudega.

Euroopa Nõukogu kontekstis võib andmeid edasi töödelda teadus- ja ajaloouuringute või statistilisel eesmärgil, kui see on avalikes huvides, ning selle suhtes tuleb kohaldada asjakohaseid kaitsemeetmeid[960]. Andmesubjektide õigusi võib andmete statistilisel eesmärgil töötlemisel piirata ka tingimusel, et puudub nende õiguste ja vabaduste rikkumise risk[961].

1997. aastal avaldati statistikaandmete kaitse soovitus, mis käsitleb avaliku ja erasektori statistikat[962].

Vastutava töötleja poolt statistilisel eesmärgil kogutud andmeid ei tohi kasutada muul eesmärgil. Muul kui statistilisel eesmärgil kogutud andmed peavad olema kättesaadavad edasiseks statistiliseks kasutamiseks. Statistikaandmete kaitse soovituses sätestatakse ka, et andmeid tohib edastada kolmandatele isikutele, kui see toimub üksnes statistilisel eesmärgil. Sellistel juhtudel peavad pooled kokku leppima ja kirjalikult vormistama, mis ulatuses on andmete kasutamine statistilistel eesmärkidel õiguspärane. Et see ei asenda andmesubjekti nõusolekut – kui seda on vaja –, peavad riigisisestes õigusaktides olema sätestatud asjakohased kaitsemeetmed, mis minimeeriksid isikuandmete väärkasutamise riske; need võivad olla näiteks kohustus andmed enne avalikustamist anonüümida või pseudonüümida.

Kutseliste statistikute suhtes tuleb riigisiseste õigusaktide alusel kohaldada kutsesaladuse hoidmise erikohustusi, nagu tavaliselt tehakse ametliku statistika korral. Need kohustused peavad kehtima ka küsitlejate ja teiste isikuandmete kogujate suhtes, kelle tööülesanne on koguda andmeid andmesubjektidelt või teistelt isikutelt.

960 Nüüdisajastatud konventsiooni nr 108 artikli 5 lõike 4 punkt b.

961 *Ibid.*, artikli 11 lõige 2.

962 Euroopa Nõukogu ministrite komitee (1997), *Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes*, 30. september 1997.

Kui õigusaktid ei luba isikuandmeid kasutavat statistikauuringut, võib selleks, et andmete kasutamine oleks seaduslik, olla vaja saada andmesubjektide nõusolek või vähemalt tuleb anda neile võimalus esitada vastuväiteid. Kui küsitlejad koguvad statistilisel eesmärgil isikuandmeid, tuleb neile selgelt teatada, kas andmete esitamine on riigisiseste õigusaktide alusel kohustuslik või mitte.

Kui statistikauuringut ei saa teha anonüümsete andmetega ning vaja on isikuandmeid, tuleb sel otstarbel kogutud andmed anonüümida kohe, kui võimalik. Miinimumtingimusena ei tohi sellise statistikauuringu tulemustest olla võimalik tuvastada andmesubjekte, v.a kui on selge, et sellega ei kaasne riske.

Kui statistikaanalüüs on valmis, tuleb isikuandmed kustutada või anonüümida. Sellistes olukordades soovitab statistikaandmete kaitse soovitus, et tuvastamist võimaldavaid andmeid tuleb hoida muudest isikuandmetest eraldi. See tähendab näiteks, et kas krüptimisvõtit või tuvastamissünonüümide loetelu tuleb säilitada muudest andmetest eraldi.

9.5. Finantsandmed

Põhipunktid

- Kuigi finantsandmeid ei peeta nüüdisajastatud konventsiooni nr 108 ega isikuandmete kaitse üldmääruse tähenduses delikaatseteks andmeteks, peab nende töötlemisel õigsuse ja andmeturbe tagamiseks rakendama eritagatisi.
- Eriti vajavad sisseehitatud andmekaitset ehk lõimitud ja vaikimisi andmekaitset elektroonilised maksesüsteemid.
- Sellele valdkonnale omased andmekaitseprobleemid võivad tuleneda eelkõige sobivate autentimismehhanismide vajadusest.

Näide: kohtuasjas *Michaud vs. Prantsusmaa*[963] vaidlustas kaebuse esitaja (Prantsusmaal tegutsev advokaat) talle Prantsuse õigusaktide alusel kohaldatava kohustuse teatada kahtlustest seoses klientide võimaliku rahapesuga. EIK täheldas, et advokaatidele määratud kohustusega edastada

963 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.

haldusasutustele teise isiku kohta teavet, mida nad on saanud kutsetegevuses, sekkutakse advokaatide õigusesse nende sõnumisaladuse ja eraelu austamisele Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 tähenduses, sest see õigus hõlmab ka kutse- või äritegevust. Sekkumine oli siiski kooskõlas õigusaktidega ja sellel on õiguspärane eesmärk – ennetada rikkumisi ja kuritegevust. Et advokaadid peavad kahtlustustest teatama üksnes väga piiratud asjaoludel, leidis EIK, et see kohustus on proportsionaalne. Kohus järeldas, et artiklit 8 ei rikutud.

Näide: kohtuasjas *M.N. jt vs. San Marino*[964], sõlmis kaebuse esitaja (Itaalia kodanik) usalduslepingu uurimise all oleva äriühinguga. See tähendas, et äriühingu suhtes kohaldati (elektrooniliste) dokumentide läbiotsimist ja arestimist. Hageja esitas kaebuse San Marino kohtule, väites, et tal puudub seos väidetavate kuritegudega. Kohus lükkas tema kaebuse siiski tagasi, sest ta ei olnud huvitatud isik. Euroopa Inimõiguste Kohus leidis, et võrreldes huvitatud isikuga oli kaebaja kohtuliku kaitse seisukohast oluliselt ebasoodsas olukorras, kuid tema andmete suhtes kohaldati siiski läbiotsimis- ja arestimistoiminguid. Seega otsustas kohus, et rikuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8.

Näide: kohtuasjas *G.S.B. vs. Šveits*[965] saadeti kaebuse esitaja pangakonto andmed Šveitsi ja USA vahelise halduskoostöölepingu alusel USA maksuhaldurile. Euroopa Inimõiguste Kohus leidis, et edastamine ei olnud vastuolus Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8, sest kaebuse esitaja eraelu puutumatuse õiguse rikkumine oli seadusega ette nähtud, selle eesmärk oli õiguspärane ja see oli proportsionaalne asjaomase avaliku huviga.

Andmekaitse üldise õigusraamistiku kohaldamine (nagu on sätestatud konventsioonis nr 108) maksete kontekstis töötati välja **Euroopa Nõukogu** 1990. aasta soovituses R(90)19[966]. Soovituses selgitatakse andmete seadusliku kogumise ja kasutamise ulatust maksete kontekstis, eriti maksekaartide abil. Ka antakse riikide seadusandjatele üksikasjalikud soovitused makseandmete kolmandatele isikutele avalikustamise eeskirjade, andmete säilitamise tähtaegade, läbipaistvuse, andmeturbe,

964 EIK, *M.N. jt vs. San Marino*, nr 28005/12, 7. juuli 2015.

965 EIK, *G.S.B. vs. Šveits*, nr 28601/11, 22. detsember 2015.

966 Euroopa Nõukogu ministrite komitee (1990), *Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations*, 13. september 1990.

andmete piiriülese liikumise ning järelevalve ja õiguskaitsevahendite kohta. Euroopa Nõukogu on koostanud ka arvamuse maksuteabe edastamise kohta[967], milles on soovitused ja küsimused, mida arvestada maksuteabe edastamisel.

Euroopa Inimõiguste Kohus lubab edastada finantsandmeid – konkreetselt isiku pangakonto andmeid – vastavalt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 8, kui see on seadusega ette nähtud, selle eesmärk on õiguspärane ja proportsionaalne asjaomase avaliku huviga[968].

ELi õiguse kohaselt peavad isikuandmete töötlemisega seotud elektroonilised maksesüsteemid vastama isikuandmete kaitse üldmäärusele. Need süsteemid peavad seega tagama lõimitud ja vaikimisi andmekaitse. Lõimitud andmekaitse kohustab vastutavat töötlejat võtma andmekaitsepõhimõtete rakendamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. Vaikimisi andmekaitse tähendab, et vastutav töötleja peab tagama, et vaikimisi saab töödelda üksnes isikuandmeid, mis on vajalikud konkreetse eesmärgi täitmiseks (vt peatükk 4.4). Finantsandmete suhtes leidis Euroopa Liidu Kohus, et edastatud maksuandmed võivad olla isikuandmed[969]. Artikli 29 töörühm avaldas asjakohased suunised liikmesriikidele, sealhulgas kriteeriumid, millega tagada kooskõla andmekaitse-eeskirjadega isikuandmete automaatsel vahetamisel maksustamise eesmärgil automaatvahendite abil[970]. Lisaks on jõustatud mitu õigusakti, mis reguleerivad finantsturge ning krediidiasutuste ja investeerimisühingute tegevust[971]. Muud õiguslikud vahendid aitavad võidelda

967 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2014), *Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes*, 4. juuni 2014.

968 EIK, *G.S.B. vs. Šveits*, nr 28601/11, 22. detsember 2015.

969 ELK, C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 1. oktoober 2015, punkt 29.

970 Artikli 29 töörühm (2015), *Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes*, 14/EN WP 230.

971 Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/65/EL finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL, ELT 2014 L 173; Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta määrus (EL) nr 600/2014 finantsinstrumentide turgude kohta ning millega muudetakse määrust (EL) nr 648/2012, ELT 2014 L 173; Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ, ELT 2013 L 176.

siseringitehingute ja turuga manipuleerimise vastu[972]. Peamised andmekaitset mõjutavad valdkonnad on järgmised:

- finantstehingute andmete säilitamine;
- isikuandmete edastamine kolmandatesse riikidesse;
- telefonivestluste või elektroonilise side salvestamine, sealhulgas pädevate ametiasutuste õigus nõuda telefonikõnede ja andmeliikluse kirjeid;
- isikuandmete avaldamine, sealhulgas karistuste teabe avaldamine;
- pädevate asutuste järelevalve- ja uurimisvolitused, seahulgas kohapealsed kontrollid ja eravaldusesse sisenemine dokumentide kaasavõtmiseks;
- rikkumistest teatamise mehhanismid (s.t vilepuhumise süsteemid);
- liikmesriikide pädevate asutuste ning Euroopa Väärtpaberiturujärelevalve koostöö (ESMA).

Nendes valdkondades käsitletakse ka muid küsimusi, näiteks andmete kogumist andmesubjektide finantsseisundi kohta[973] või piiriüleseid makseid pangaülekannete kaudu, millega paratamatult kaasneb isikuandmete liikumine[974].

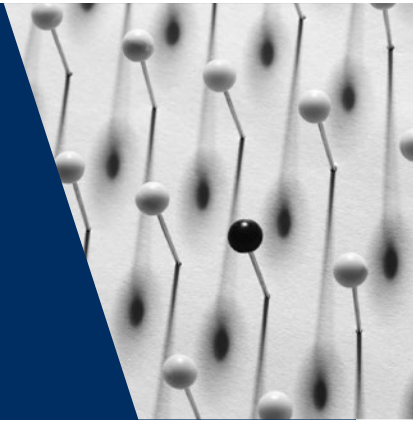
---

972 Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta määrus (EL) nr 596/2014, mis käsitleb turukuritarvitusi (turukuritarvituse määrus) ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2003/6/EÜ ja komisjoni direktiivid 2003/124/EÜ, 2003/125/EÜ ja 2004/72/EÜ, ELT 2014 L 173.

973 Euroopa Parlamendi ja nõukogu 16. septembri 2009. aasta määrus (EÜ) nr 1060/2009 reitinguagentuuride kohta, ELT 2009 L 302, ja mida muudeti viimati Euroopa Parlamendi ja nõukogu 16. aprilli 2014. aasta direktiiviga 2014/51/EL, millega muudetakse direktiive 2003/71/EÜ ja 2009/138/EÜ ning määrusi (EÜ) nr 1060/2009, (EL) nr 1094/2010 ja (EL) nr 1095/2010 seoses Euroopa Järelevalveasutuse (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve) ning Euroopa Järelevalveasutuse (Euroopa Väärtpaberiturujärelevalve) volitustega, ELT 2014 L 153; Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta määrus (EL) nr 462/2013, millega muudetakse määrust (EÜ) nr 1060/2009 reitinguagentuuride kohta, ELT 2013 L 146.

974 Euroopa Parlamendi ja nõukogu 13. novembri 2007. aasta direktiiv 2007/64/EÜ 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 2007 L 319, mida on muudetud Euroopa Parlamendi ja nõukogu 16. septembri 2009. aasta direktiiviga 2009/111/EÜ, millega muudetakse direktiive 2006/48/EÜ, 2006/49/EÜ ja 2007/64/EÜ seoses keskasutustega seotud pankade, teatavate omavahendite kirjete, suure riskikontsentratsiooni, järelevalvesüsteemide ja kriisijuhtimisega, ELT 2009 L 302.

10 Isikuandmete kaitse nüüdisprobleemid



Digiajastut ehk infotehnoloogia ajastut iseloomustab arvutite, interneti ja digitehnoloogiate laialdane kasutamine. Kogutakse ja töödeldakse tohutus koguses andmeid, sealhulgas isikuandmeid. Isikuandmete kogumine ja töötlemine globaliseerunud majanduses tähendab, et piiriüleste andmevoogude arv kasvab. Igapäevaelus võib selline töötlemine anda olulisi ja nähtavaid eeliseid: otsingumootorid lihtsustavad juurdepääsu suurele hulgale teabele ja teadmistele, suhtlusvõrgustike teenused võimaldavad inimestel suhelda üle kogu maailma, avaldada arvamust ja koguda toetust ühiskondlikele, keskkonna- ja poliitilistele eesmärkidele ning ettevõtted ja tarbijad saavad kasu mõjusatest ja tõhusatest turundustehnikatest, mis edendavad majandust. Tehnoloogia ja isikuandmete töötlemine on ka riigiasutuste jaoks hädavajalikud vahendid võitluses kuritegevuse ja terrorismiga. Samamoodi võivad suurandmed – suurte andmehulkade kogumine, säilitamine ja analüüsimine, et tuvastada mustrid ja prognoosida käitumist – olla ühiskonna jaoks olulise väärtusega, suurendades tootlikkust, avaliku sektori tulemuslikkust ja ühiskonnas osalemist[975].

Kuigi digiajastul on palju eeliseid, tekitab see ka eraelu puutumatuse ja andmekaitse probleeme, sest tohutus koguses isikuandmeid kogutakse ja töödeldakse üha keerukamalt ja läbipaistmatumalt. Progress tehnoloogias on toonud kaasa massiivse andmekogumite arengu, mida on lihtne võrrelda ja edasi analüüsida mustrite otsimiseks või algoritmipõhiste otsuste tegemiseks, mis võivad anda enneolematu ülevaate inimeste käitumisest ja eraelust[976].

975 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. jaanuar 2017.

976 Euroopa Parlament (2017), Resolutsioon suurandmete mõju kohta põhiõigustele, sealhulgas eraelu puutumatusele, andmekaitsele, diskrimineerimiskeelule, turvalisusele ja õiguskaitsele (P8_TA-PROV(2017)0076), Strasbourg, 14. märts 2017.

Uued tehnoloogiad on võimsad ja võivad olla väärkasutamisel üliohtlikud. Riigiasutused, kes kasutavad massilist jälgimist, milles võidakse neid tehnoloogiaid kasutada, on näide sellest, kui oluliselt võivad need tehnoloogiad mõjutada üksikisikute õigusi. 2013. aastal tekitasid Edward Snowdeni paljastused luureagentuuride ulatuslike interneti- ja telefonijärelevalve programmide kasutamise kohta mõnes riigis suuri kartusi ohtude pärast, mida jälgimistegevus põhjustab eraelu puutumatusele, demokraatlikule valitsemistavale ja sõnavabadusele. Massiline jälgimine ja tehnoloogiad, mis võimaldavad isikuandmete ülemaailmset säilitamist ja töötlemist ning juurdepääsu suurtele andmekogustele, võivad mõjutada eraelu puutumatuse õiguse olemust[977]. Lisaks võivad need kahjustada poliitikakultuuri ja demokraatiat, loovust ja innovatsiooni[978]. Üksnes hirm, et riik võib pidevalt jälgida ja analüüsida kodanike käitumist ja tegevust, võib hirmutada neid väljendamast oma seisukohti teatud küsimustes ning tekitada ettevaatlikkust[979]. Need probleemid on ajendanud paljusid avaliku sektori asutusi, uurimiskeskusi ja kodanikuühiskonna organisatsioone analüüsima uute tehnoloogiate võimalikku mõju ühiskonnale. 2015. aastal tegi Euroopa andmekaitseinspektor mitu algatust, mille eesmärk oli hinnata suurandmete ja asjade interneti mõju eetikale. Eelkõige moodustas ta andmekaitse eetikanõukogu, mille eesmärk on kannustada „avatud ja teadlikku arutelu digitaalse eetika teemal, mis võimaldab Euroopa Liidul realiseerida tehnoloogiast saadavat kasu ühiskonna ja majanduse hüvanguks ning mis samal ajal kindlustab üksikisikute õigusi ja vabadusi, eelkõige nende õigust privaatsusele ja andmekaitsele“[980].

Isikuandmete töötlemine on võimas vahend ka äriühingutele. Tänapäeval võivad isikuandmed avaldada üksikasjalikku teavet inimese tervise või finantsolukorra kohta, mille alusel teevad äriühingud üksikisikute jaoks olulisi otsuseid, näiteks otsustades nende ravikindlustusmakse summat või krediidivõimelisust. Andmetöötlusmeetodid võivad mõjutada ka demokraatlikke protsesse, kui poliitikud või äriühingud mõjutavad nendega valimisi – näiteks valijate täppismõjutamise kaudu teabevahetuse raames. Teisisõnu, kui algselt mõisteti eraelu puutumatust kui õigust kaitsta üksikisikuid avaliku sektori ametiasutuste põhjendamatu sekkumise eest, siis praegu võib seda

977 Vt ÜRO Peaassamblee (2017), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23. september 2014, punkt 59. Vt ka Euroopa Inimõiguste Kohus (2017), *Factsheet on Mass surveillance*, juuli 2017.

978 Euroopa Andmekaitseinspektor (2015), „Suurandmetega kaasnevad probleemid“, arvamus 7/2015, Brüssel, 19. november 2015.

979 Vt eelkõige ELK, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt ja Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014, punkt 37.

980 Euroopa andmekaitseinspektori 3. detsembri 2015. aasta otsus, millega asutatakse organisatsiooniväline andmekaitse eetilise ulatuse nõuanderühm („eetikanõukogu“), 3. detsember 2015, põhjendus 5.

ohustada ka eraõiguslike osalejate mõjuvõim. See tekitab küsimusi tehnika kasutamise ja prognoosiva analüüsi kohta seoses otsustega, mis mõjutavad üksikisikute igapäevaelu, ning tugevdab vajadust tagada, et isikuandmete mis tahes töötlemine oleks kooskõlas põhiõiguste nõuetega.

Andmekaitse on olemuslikult seotud tehnoloogia, ühiskonna ja poliitika muutumisega, mistõttu ei ole võimalik koostada tulevaste probleemide ammendavat loetelu. Käesolevas peatükis käsitletakse valitud valdkondi, mis on seotud suurandmete, interneti suhtlusvõrgustike ja ELi digitaalse ühtse turuga. See ei ole nende valdkondade ammendav andmekaitsehinnang, vaid selle asemel rõhutatakse uute või muutunud inimtegevuste ja andmekaitse võimalike vastastikmõju paljusust.

10.1. Suurandmed, algoritmid ja tehisintellekt

Põhipunktid

- IKT murrangulised uuendused kujundavad uut eluviisi, kus ühiskondlikud suhted, äri, era- ja avaliku sektori teenused on digitaalses vastastikseoses, mis tekitab üha rohkem andmeid, millest paljud on isikuandmed.
- Valitsused, ettevõtjad ja kodanikud tegutsevad üha andmepõhisemas majanduses, kus andmed ise on muutunud väärtuslikuks varaks.
- Suurandmete mõiste viitab nii andmetele kui ka nende analüüsimisele.
- Suurandmete analüüsimisel töödeldavate isikuandmete suhtes kohaldatakse ELi ja Euroopa Nõukogu õigusakte.
- Andmekaitse-eeskirjade ja -õiguste erandid piirduvad valitud õigustega ja eriolukordadega, kus õiguse jõustamine oleks võimatu või nõuaks vastutavatelt andmetöötlejatelt ebaproportsionaalset jõupingutust.
- Täisautomaatne otsustusprotsess on üldiselt keelatud, v.a erijuhtudel.
- Õiguste jõustamise tagamisel on võtmetähtsusega üksikisikute teadlikkus ja kontroll.

Üha digitaalsemas maailmas jätab iga tegevus digitaalse jälje, mida saab koguda, töödelda ja hinnata või analüüsida. Uute info- ja sidetehnoloogiate abil kogutakse ja säilitatakse üha rohkem andmeid[981]. Alles hiljuti puudusid tehnoloogiad, mis

981 Euroopa Komisjon, komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Eduka andmepõhise majanduse suunas", COM(2014) 442 final, Brüssel, 2. juuli 2014.

suutnuks andmeid massiliselt analüüsida, hinnata või teha nende alusel kasulikke järeldusi. Andmeid oli hindamiseks lihtsalt liiga palju, need olid suundumuste ja mustrite tuvastamiseks liiga keerukad, vähe struktureeritud ja muutlikud.

10.1.1. Suurandmete, algoritmide ja tehisintellekti määratlemine

Suurandmed

Termin „suurandmed" on moesõna, millel võib eri kontekstides olla erinev tähendus. Tavaliselt hõlmab see kasvavat tehnoloogilist suutlikkust koguda andmete suurest mahust, kiirusest ja mitmekesisusest protsessiteadmisi ning eraldada uusi ja prognoosivaid teadmisi[982]. Suurandmete mõiste hõlmab seega nii andmeid kui ka nende analüüsimist.

Andmeallikaid on mitut liiki, näiteks inimesed ja nende isikuandmed, masinad või andurid, kliimateave, satelliitkujutised, digitaalsed pildid ja videod või GPS-signaalid. Suur osa andmeid ja teavet on siiski isikuandmed: kõik, mis saadakse nime, foto, e-posti aadressi, pangaandmete, GPS-jälitusandmete, suhtlusvõrgustike veebikohtades tehtud postituste, meditsiiniteabe või arvuti IP-aadressi põhjal[983].

Suurandmed tähendavad ka suurte andmehulkade ja kättesaadava teabe **töötlemist**, analüüsimist ja hindamist, st suurandmete analüüsimiseks kasuliku teabe saamist. See tähendab, et kogutud andmeid ja teavet võib kasutada algselt kavandatud eesmärgil (nt statistilised suundumused) või üksikasjalikuma teenuse jaoks (nt reklaam). Kui on olemas suurandmete kogumise, töötlemise ja hindamise tehnoloogiad, võib kombineerida ja taashinnata mis tahes liiki teavet: finantstehinguid, krediidivõimelisust, ravi, eratarbimist, kutsetegevus, teekondi, internetikasutust, kiipkaarte ja nutitelefone, video või side seiret. Suurandmete analüüsiga kaasneb andmete uus kvantitatiivne mõõde, mida saab hinnata ja kasutada reaalajas, näiteks tarbijatele kohandatud teenuste pakkumiseks.

982 Euroopa Nõukogu, konventsiooni nr 108 nõuendekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 2; Euroopa Komisjon, komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Eduka andmepõhise majanduse suunas", COM(2014) 442 final, Brüssel, 2. juuli 2014, lk 4; Rahvusvaheline Telekommunikatsiooni Liit (2015), soovitus Y.3600, *Big Data – Cloud computing based requirements and capabilities*.

983 Euroopa Komisjoni teabeleht ELi andmekaitse reformi ja suurandmete kohta; Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 2.

Algoritmid ja tehisintellekt

Tehisintellekt (TI) tähendab intelligentsete tehisagentidena tegutsevate masinate intellekti. Intelligentse tehisagendina võivad teatud seadmed tarkvara abil tajuda keskkonda ja tegutseda algoritmide järgi. Terminit „tehisintellekt" kasutatakse, kui masin kasutab kognitiivseid funktsioone (nt õppimist ja probleemide lahendamist), mida tavaliselt seostatakse elusolenditega[984]. Otsustusprotsessi matkimiseks kasutatakse nüüdisaegsetes tehnoloogiates ja tarkvaras algoritme, millega seadmed teevad automaatotsuseid. Algoritmi saab kõige paremini kirjeldada kui etapilist arvutamise, andmetöötluse, hindamise ja automaatse põhjendamise ja otsustamise menetlust.

Sarnaselt suurandmete analüüsiga eeldavad tehisintellekt ja selle sooritatav automaatotsustusprotsess suure andmekoguse kogumist ja töötlemist. Need andmed võivad pärineda seadmest endast (piduritemperatuur, kütus jne) või keskkonnast. Näiteks on profiilianalüüs protsess, mis võib tugineda eelmääratud mustritel ja teguritel põhinevale automaatotsustusprotsessile.

Näide: profiilianalüüs ja sihtreklaam

Suurandmetel põhinev profiilianalüüs hõlmab selliste mudelite otsimist, mis kajastavad isikutüübi omadusi – näiteks kui veebipõhised kaubandusettevõtted pakuvad tooteid, mis „võivad ka teile meeldida", lähtudes kliendi ostukorvis varem olnud toodetest saadud teabest. Mida rohkem andmeid, seda selgem tervikpilt. Näiteks nutitelefon toimib võimsa küsimustikuna, mida kasutajad täidavad igal kasutuskorral kas teadlikult või alateadlikult.

Tänapäeva psühhograafia – isikuomadusi uuriv teadus – liigitab iseloomutüüpe OCEAN-meetodil. Lühend tähendab iseloomu viit suurt mõõdet: O (*openness*) – avatus (kui avatud on isik uuele); C (*conscientiousness*) – kohusetundlikkus (kui palju sarnaneb isik perfektsionistiga), E (*extraversion*) väljapoole suunatus (kui hea suhtleja on isik), A (*agreeableness*) – leplikkus (kui kokkuleppealdis on isik) ja N (*neuroticism*) neutrootilisus (kui haavatav on isik). See teave kirjeldab isikut, tema vajadusi ja hirme, käitumist jne.

984 Stuart Russel ja Peter Norvig, *Artificial Intelligence: A Modern Approach (2. väljaanne)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, lk 27, 32–58, 968–972; Stuart Russel ja Peter Norvig, *Artificial Intelligence: A Modern Approach* (3. väljaanne), 2009, Upper Saddle River, New Jersey: Prentice Hall, lk 2.

Seejärel täiendatakse seda profiili muu teabega isiku kohta, mis on saadud mis tahes olemasolevatest allikatest, andmebüroodelt, suhtlusvõrgustikest (näiteks mis postitusi ja fotosid on ta märkinud meeldivaks), veebis kuulatud muusika või GPS-andmed ja teekonnad.

Suurandmete analüüsi tehnikate abil loodud profiilide kogumit võrreldakse hiljem sarnaste käitumismustrite tuvastamiseks ja isikutüübiklastrite tõlgendamiseks. Seega on see teave teatud isikutüüpide käitumise ja hoiakute kohta, mitte vastupidi. Suurandmetele juurdepääsu ja nende kasutamisega pööratakse isikuomaduste test ümber ehk käitumise ja hoiaku teabe alusel kirjeldatakse isiksust. Kui on olemas teabekogum suhtlusvõrgustikes meeldimiste, teekondade, kuulatud muusika või vaadatud filmide kohta, võib kujuneda selge pilt inimese isiksusest, mis võimaldab ettevõtetel edastada talle kohandatud reklaami ja/või teavet tema isikuomaduste alusel. Eelkõige on tähtis, et seda teavet saab töödelda reaalajas[985].

10.1.2. Suurandmete kasulikkuse ja riskide tasakaalustamine

Nüüdisaegsed töötlemismeetodid suudavad käsitleda suuri andmemahte, importida kiiresti uusi andmeid, suudavad töödelda teavet reaalajas, st lühikese reageerimisajaga (ka keerukate päringute korral), võimaldavad teha korraga mitut ja samaaegset päringut ning analüüsivad mitmesuguseid teabeliike (fotod, tekstid, arvud). Need tehnoloogilised uuendused võimaldavad andme- ja teabemasse liigendada, töödelda ja hinnata reaalajas[986]. Olemasoleva andmekoguse eksponentsiaalse suurendamise ja analüüsimisega on nüüd võimalik saavutada tulemusi, mis on väiksemas analüüsis võimatud. Suurandmed on aidanud arendada uut ärivaldkonda, kus võib tekkida ettevõtetel ja tarbijatele uusi teenuseid. ELi kodanike isikuandmete väärtus

985 Töötlemismeetodite ja uue tarkvaraga hinnatakse reaalajas teavet, mis inimesele meeldib, mida ta veebis ostes vaatab või lisab veebipoe ostukorvi, ning talle võidakse pakkuda tooteid, mis võiksid teda kogutud teabe põhjal huvitada.

986 Suurandmete töötlemise tarkvara arendamine on alles algusjärgus. Hiljuti on siiski välja töötatud analüüsiprogramme, eelkõige suurte andme- ja teabekoguste reaalajas töötlemiseks seoses üksikisikute tegevusega. Suurandmete struktureeritud analüüsimine ja töötlemine on tekitanud uusi profiilianalüüsi ja suunatud reklaamimise meetodeid. Euroopa Komisjon, komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Eduka andmepõhise majanduse suunas", COM(2014) 442 final, Brüssel, 2. juuli 2014; Euroopa Liidu Komisjon, *EU Commission Fact Sheet on The EU Data Protection Reform and Big Data*; Euroopa Nõukogu, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 2.

võib 2020. aastaks kasvada ligi 1 triljonit eurot aastas[987]. Seepärast võivad suurandmed pakkuda uusi **võimalusi**, mis tulenevad massandmete hindamisest uute ühiskonna-, majandus- või teadusteadmiste saamiseks, mis võivad olla kasulikud nii üksikisikutele kui ka ettevõtetele ja valitsustele[988].

Suurandmete analüüs võib tuua esile eri allikates ja andmekogumites korduvaid mustreid, mis võimaldavad saada kasulikke teadmisi näiteks teaduses ja meditsiinis, muu hulgas seoses tervishoiu, toiduga kindlustatuse, arukate transpordisüsteemide, energiatõhususe või linnaplaneerimisega. Teabe sellise reaalajas analüüsimisega saab täiustada rakendatud süsteeme. Teadusuuringutega on võimalik saada uusi teadmisi suuri andmekoguseid ja statistilist hindamist ühendades, eriti valdkondades, kus seni on hinnatud suuri andmekogumeid käsitsi. Võimalik on välja töötada ravimeetodeid, mis on üksikpatsientidele kohandatud võrdluse alusel kättesaadava teabe kogumiga. Ettevõtted loodavad suurandmete analüüsiga saavutada konkurentsieeliseid ja kokkuhoidu ning luua uusi ärivaldkondi otsese, kliendiga kohandatud teenuste kaudu. Riigiasutused loodavad täiustada kriminaalõigust. Komisjoni digitaalse ühtse turu strateegias tunnistatakse andmepõhiste tehnoloogiate, teenuste ja suurandmete potentsiaali toimida ELi majanduskasvu, innovatsiooni ja digiteerimise katalüsaatorina[989].

Suurandmetega kaasnevad siiski ka **riskid**, mis üldiselt seostuvad töödeldavate andmete mahu, kiiruse ja varieeruvusega. Maht tähendab töödeldavate andmete kogust, varieeruvus andmetüüpide arvu ja mitmekesisust ning kiirus andmetöötluse kiirust. Andmekaitse erikaalutlused tekivad eriti siis, kui suurandmete analüüsil kasutatakse suuri andmekogumeid uute ja prognoosivate teadmiste kogumiseks, et teha üksikisikuid ja/või rühmi puudutavaid otsuseid[990]. Suurandmetega seotud andmekaitse ja eraelu puutumatuse riske on rõhutatud Euroopa Andmekaitseinspektori

987 Euroopa Komisjoni teabeleht ELi andmekaitse reformi ja suurandmete kohta.

988 Andmekaitse ja eraelu puutumatuse eest vastutavate volinike rahvusvaheline konverents (2014), *Resolution on Big Data*; Euroopa Komisjon, komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Eduka andmepõhise majanduse suunas", COM(2014) 442 final, Brüssel, 2. juuli 2014; Euroopa Komisjoni teabeleht ELi andmekaitse reformi ja suurandmete kohta; Euroopa Nõukogu (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 1.

989 Euroopa Parlamendi 14. märtsi 2017. aasta resolutsioon suurandmete mõju kohta põhiõigustele, sealhulgas eraelu puutumatusele, andmekaitsele, diskrimineerimiskeelule, turvalisusele ja õiguskaitsele (2016/2225(INI)).

990 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 2.

ja artikli 29 töörühma arvamustes, Euroopa Parlamendi resolutsioonides ning Euroopa Nõukogu poliitikadokumentides[991].

Riskiks võib olla suurandmete väärkasutamine isikute poolt, kellel on juurdepääs teabemassile üksikisikute või ühiskonnarühmade manipuleerimise, diskrimineerimise või rõhumise kaudu[992]. Kui kogutakse, töödeldakse ja hinnatakse suuri isikuandmete või teabe koguseid üksikisikute käitumise kohta, võivad nende kasutamisega kaasneda olulised põhiõiguste ja -vabadustega seotud rikkumised, mis on raskemad kui eraelu puutumatuse rikkumine. Võimalikku mõju eraelu puutumatusele ja isikuandmetele ei ole võimalik täpselt mõõta. Euroopa Parlament tuvastas, et puudub metoodika, mille alusel hinnata tõenduspõhiselt suurandmete kogumõju, kuid on tõendeid, mis viitavad, et suurandmete analüüsil võib olla oluline horisontaalne mõju nii avalikus kui ka erasektoris[993].

Isikuandmete kaitse üldmääruses on sätted, mis käsitlevad isiku õigust, et tema kohta ei tehtaks automaatotsuseid, sealhulgas automaatset profiilianalüüsi[994]. Eraelu puutumatusega seotud küsimused tekivad, kui õigus vaidlustada eeldab isiklikku kontakti, mis võimaldab andmesubjektidel väljendada oma seisukohta ja vaidlustada otsus[995]. See võib tekitada probleeme isikuandmete kaitse piisava taseme tagamisel, näiteks siis, kui sekkumine isikliku kontakti võtmise kaudu ei ole võimalik või kui algoritmid on liiga keerulised ja kaasatud andmete hulk on liiga suur, et esitada üksikisikutele teatud otsuste põhjendused ja/või eelnevat teavet nende nõusoleku saamiseks. Tehisintellekti kasutamise ja automaatotsuste tegemise näide on hüpoteegiavalduste käsitlemise või värbamisprotsesside hiljutised suundumused. Taotlused lükatakse tagasi või jäetakse kõrvale põhjusel, et taotlejad ei vasta eelmääratletud parameetritele või teguritele.

991 Vt näiteks Euroopa Andmekaitseinspektor (2015), „Suurandmetega kaasnevad probleemid", arvamus 7/2015, 19. november 2015; Euroopa Andmekaitseinspektor (2016), „Tõhusa nõuete täitmise tagamine digitaalühiskonnas ja -majanduses", arvamus 8/2016, 23. september 2016; Euroopa Parlament (2016), *Resolution on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law enforcement*, P8_TA(2017)0076, Strasbourg, 14. märts 2017; Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. jaanuar 2017.

992 Andmekaitse ja eraelu puutumatuse eest vastutavate volinike rahvusvaheline konverents (2014), *Resolution on Big Data*.

993 Euroopa Parlamendi 14. märtsi 2017. aasta resolutsioon suurandmete mõju kohta põhiõigustele, sealhulgas eraelu puutumatusele, andmekaitsele, diskrimineerimiskeelule, turvalisusele ja õiguskaitsele (2016/2225(INI)).

994 Isikuandmete kaitse üldmääruse artikkel 22.

995 *Ibid.*, artikli 22 lõige 3.

10.1.3. Andmekaitseküsimused

Andmekaitse seisukohalt puudutavad peamised küsimused ühelt poolt töödeldavate isikuandmete mahtu ja mitmekesisust ning teisalt töötlemist ja selle tulemusi. Keerukate algoritmide ja tarkvara kasutuselevõtt, mis muudavad suure andmekoguse otsustusprotsessi ressursiks, mõjutab eelkõige üksikisikuid ja rühmi, eriti profiilianalüüsi või märgistamise korral, ning tekitab lõppkokkuvõttes palju andmekaitseprobleeme[996].

Vastutavate ja volitatud töötlejate tuvastamine ning nende vastutus

Suurandmed ja tehisintellekt tõstatavad arvukaid küsimusi vastutavate ja volitatud töötlejate tuvastamise ning nende vastutuse kohta: kes on andmete omanik, kui kogutakse ja töödeldakse nii suurt andmekogust? Kes on vastutav töötleja, kui andmeid töötlevad nutikad masinad ja tarkvara? Mis on töötlemisel iga osaleja täpsed kohustused? Mis eesmärkidel võidakse kasutada suurandmeid?

Vastutuse küsimus tehisintellekti kontekstis muutub veelgi keerukamaks, kui tehisintellekt teeb otsuseid, mis põhinevad tehisintellekti enda välja töötatud andmetöötlusel. Isikuandmete kaitse üldmääruses sätestatakse vastutava töötleja ja volitatud töötleja vastutuse õigusraamistik. Isikuandmete ebaseaduslikul töötlemisel vastutavad nii vastutav kui ka volitatud andmetöötleja[997]. Tehisintellekt ja automaatotsuste tegemine tekitavad küsimusi, kes vastutab andmesubjektide eraelu puutumatuse rikkumiste eest, kui töödeldavate andmete keerukus ja kogus on täpselt teadmata. Kui tehisintellekti ja algoritme loetakse tooteks, tekitab see probleeme isikuandmete kaitse üldmäärusega reguleeritava isikliku vastutuse ja tootevastutuse vahel, mida määrus ei reguleeri[998]. See nõuaks vastutuse eeskirju, et kaotada lõhe robootika ja tehisintellektiga seotud isikliku vastutuse ja tootevastutuse vahel, sealhulgas näiteks automaatotsuste tegemisel[999].

996 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23. jaanuar 2017, lk 2.

997 Isikuandmete kaitse üldmääruse artiklid 77–79 ja artikkel 82.

998 Euroopa Parlament, *European Civil Law Rules in Robotics*, sisepoliitika peadirektoraat (oktoober 2016), lk 14.

999 Roberto Viola kõne robootikat käsitlevate tsiviilõiguse Euroopa normide teemalisel meediaseminaril Euroopa Parlamendis, (SPEECH 16/02/2017); Euroopa Parlamendi teadaanne taotluse kohta, mis käsitleb komisjoni ettepanekut robootika ja tehisintellekti tsiviilvastutuse normide kohta.

Mõju andmekaitsepõhimõtetele

Eespool kirjeldatud suurandmete olemus, analüüs ja kasutamine tekitavad raskusi Euroopa andmekaitseõiguse mõne traditsioonilise aluspõhimõtte kohaldamisel[1000]. Sellised probleemid on peamiselt seotud seaduslikkuse, võimalikult väheste andmete kogumise, eesmärgi piirangu ja läbipaistvuse põhimõttega.

Võimalikult väheste andmete kogumise põhimõte nõuab, et isikuandmed oleksid asjakohased, piisavad ja piirduma sellega, mida on nende töötlemise otstarbe jaoks vaja. Suurandmete ärimudel võib siiski olla võimalikult väheste andmete kogumise vastand, sest see nõuab üha rohkem andmeid, sageli määratlemata eesmärkidel.

Sama kehtib eesmärgi piirangu põhimõtte kohta, mis nõuab andmete töötlemist kindlaksmääratud eesmärkidel ja et andmeid ei tohi kasutada eesmärkidel, mis on kokkusobimatu kogumise algse eesmärgiga, v.a kui selline töötlemine põhineb õiguslikul alusel, näiteks andmesubjekti nõusolekul (vt punkt 4.1.1).

Lisaks on suurandmed probleemsed ka andmete õigsuse põhimõtte seisukohast, sest suurandmerakendused koguvad üldiselt andmeid eri allikatest, ilma et oleks võimalik kontrollida ja/või säilitada kogutud andmete õigsust[1001].

Erieeskirjad ja -õigused

Üldiselt kuuluvad suurandmete analüüsi kaudu töödeldavad isikuandmed andmekaitse õigusaktide kohaldamisalasse. Euroopa Liidu ja Euroopa Nõukogu õiguses on siiski kehtestatud erieeskirjad või erandid keeruka algoritm-andmetöötluse kohta.

Euroopa Nõukogu õiguses annab nüüdisajastatud konventsioon nr 108 andmesubjektile uusi õigusi, et võimaldada talle tõhusamat kontrolli oma isikuandmete üle suurandmete ajastul. Täpselt nii on see nüüdisajastatud konventsiooni artikli 9 lõike 1 punktide a, c ja d korral, milles käsitletakse andmesubjekti õigust, et teda märkimisväärselt mõjutavat otsust ei tehtaks üksnes automaattöötluse põhjal, arvestamata tema seisukohti; õigust saada taotluse korral teavet andmetöötluse põhjenduste kohta, kui sellise töötlemise tulemusi kohaldatakse tema suhtes, samuti õigust esitada vastuväiteid. Nüüdisajastatud konventsiooni nr 108 muud sätted,

1000 Euroopa Nõukogu (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. jaanuar 2017.

1001 Euroopa Andmekaitseinspektor (2016), „Tõhusa nõuete täitmise tagamine digitaalühiskonnas ja -majanduses“, arvamus 8/2016, 23. september 2016, lk 8.

eelkõige läbipaistvuse ja lisakohustuste kohta, on nüüdisajastatud konventsiooniga nr 108 digitaalprobleemide lahendamiseks loodud kaitsemehhanismi täiendavad elemendid.

ELi õiguses tuleb (v.a isikuandmete kaitse üldmääruse artiklis 23 loetletud juhud) tagada isikuandmete mis tahes töötlemisel **läbipaistvus**. See on eriti oluline seoses internetiteenuste ja muu keeruka automaatse andmetöötlusega, näiteks algoritmide kasutamisega otsustamisel. Seejuures peavad andmetöötlussüsteemide funktsioonid olema sellised, et andmesubjektid mõistaksid täielikult, mis toimub nende andmetega. Õiglase ja läbipaistva töötlemise tagamiseks nõutakse isikuandmete kaitse üldmääruses, et vastutav töötleja peab andma andmesubjektile olulist teavet automaatotsuste tegemise loogika, sealhulgas profiilianalüüsi kohta[1002]. Soovituses sõnavabaduse ja eraelu puutumatusega seotud õiguste kaitsmise ja edendamise kohta soovitas Euroopa Nõukogu ministrite komitee võrguneutraalsuse huvides, et internetiteenuse osutajad annaksid kasutajatele selget, täielikku ja avalikult kättesaadavat teavet andmeliikluse juhtimise selliste tavade kohta, mis võivad mõjutada kasutajate juurdepääsu sisule, rakendustele või teenustele ning nende levitamist[1003]. Kõigi liikmesriikide pädevate asutuste koostatud aruanded interneti andmeliikluse juhtimise tavade kohta tuleks koostada avatud ja läbipaistval viisil ning need tuleks teha üldsusele tasuta kättesaadavaks[1004].

Vastutavad andmetöötlejad peavad andmesubjekte **teavitama –** siis kui andmed andmesubjektidelt koguti või kui ei kogutud – mitte ainult konkreetsete kogutavate andmete ja kavandatava töötlemise kohta (vt punkt 6.1.1), vaid ka automaatotsustusprotsessi olemasolust, kui asjakohane, andes neile „sisulist teavet kasutatava loogika“[1005], protsessi eesmärkide ja võimalike tagajärgede kohta. Ka on isikuandmete kaitse üldmääruses selgitatud (ainult juhtudel, kui isikuandmeid ei saadud andmesubjektilt), et vastutaval töötlejal ei ole kohustust anda andmesubjektile sellist teavet, kui „selle teabe esitamine osutub võimatuks või eeldaks ebaproportsionaalseid jõupingutusi“[1006]. Samas, nagu rõhutas artikli 29 töörühm suunistes individuaalsete automaatotsuste tegemise ja profiilianalüüsi kohta määruse 2016/679 kohaldamisel, ei tohiks töötlemise keerukus iseenesest takistada vastutaval töötlejal anda

1002 Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt f.

1003 Euroopa Nõukogu ministrite komitee (2016), *Recommendation CM/Rec(2016)1 of the Committee of Ministers to the member states on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*, 13. jaanuar 2016, punkt 5.1.

1004 *Ibid.*, punkt 5.2.

1005 Isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt f ja artikli 14 lõike 2 punkt g.

1006 *Ibid.*, artikli 14 lõike 5 punkt b.

andmesubjektile konkreetseid selgitusi andmetöötluse eesmärkide ja kasutatavate analüüsivahendite kohta[1007].

Sarnast erandit ei hõlma andmesubjektide õigus oma isikuandmetega **tutvuda**, neid **parandada** ja **kustutada** ega nende õigus andmete töötlemist **piirata**. Vastutava töötleja kohustuse teavitada andmesubjekti tema isikuandmete mis tahes parandamisest või kustutamisest (vt punkt 6.1.4) võib siiski tühistada ka siis, kui selline teavitamine „osutub võimatuks või eeldaks ebaproportsionaalseid jõupingutusi“ [1008].

Isikuandmete kaitse üldmääruse artikli 21 kohaselt on andmesubjektidel ka õigus oma andmete mis tahes töötlemise kohta, sealhulgas suurandmete analüüsimise korral, **esitada vastuväiteid** (vt punkt 6.1.6). Kuigi vastutavad töötlejad võidakse sellest kohustusest vabastada, kui nad suudavad tõestada ülekaalukaid õigustatud huve, ei saa nad sellist vabastust, kui töötlemine toimub otseturunduse eesmärgil.

Vastutavad töötlejad võivad rakendada nende õiguste eripiiranguid ka avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringu või statistilisel eesmärgil[1009].

Profiilianalüüsi ja automaatotsuste tegemise kohta on isikuandmete kaitse üldmääruses sätestatud erieeskirjad: artikli 22 lõikes 1 on sätestatud: „Andmesubjektil on õigus, et tema kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju.“ Nagu on rõhutatud artikli 29 töörühma suunistes, sätestatakse artiklis täielikult automaatsete otsuste tegemise üldine keeld[1010]. Vastutav töötleja võib sellisest keelust vabastada ainult kolmel erijuhul: kui otsus 1) on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks, 2) on lubatud liidu või liikmesriigi õigusega või 3) põhineb andmesubjekti selgesõnalisel nõusolekul[1011].

1007 Artikli 29 töörühm (2017), *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, 17/EN WP 251, 3. oktoober 2017, lk 14.

1008 Isikuandmete kaitse üldmääruse artikkel 19.

1009 *Ibid.*, artikli 89 lõiked 2 ja 3.

1010 Artikli 29 töörühm (2017), *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, 17/EN WP 251, 3. oktoober 2017, lk 9.

1011 Isikuandmete kaitse üldmääruse artikli 22 lõige 2.

Üksikisikupoolne kontroll

Suurandmete analüüsi keerukuse ja läbipaistmatuse tõttu võib olla vaja isikuandmete üksikisikupoolse kontrolli idee ümber mõtestada. See peaks olema kohandatud asjaomase ühiskonna- ja tehnikakontekstiga, arvestades üksikisikute teadmiste piiratust. Suurandmetega seotud andmekaitses tuleks seepärast kasutada andmete kasutamise kontrollimise laiem idee, mille kohaselt üksikisikupoolne kontroll areneb keerulisemaks protsessiks, milles hinnatakse andmete kasutamise riske[1012].

See, kui hea on suurandmete rakendus, oleneb sellest, kui hästi suudab see prognoosida katserühma liikmete (või tarbijate) soove või käitumist. Praeguseid suurandmete analüüsil põhinevaid prognoosimudeleid täiustatakse pidevalt. Viimase aja suundumused on peale andmete kasutamise isiksuste liigitamisel (käitumine ja hoiakud) ka käitumise analüüsimine hääletooni ja sõnumite tippimiskiiruse või kehatemperatuuri järgi. Kogu seda teavet saab kasutada reaalajas ja võrrelda seda suurandmete hindamisest saadud andmetega, et näiteks hinnata krediidivõimelisust kohtumisel panga esindajaga. Hindamist ei tehta laenutaotleja faktilise sobivuse põhjal, vaid käitumisnäitajate alusel, mis on saadud suurandmete analüüsist ja hindamisest, näiteks sellest, kas taotleja räägib valju või meelitava häälega, milline on tema kehakeel või kehatemperatuur.

Profiilianalüüs ja sihtreklaam ei pruugi olla probleem, kui üksikisikud **teadvustavad**, et neile edastatakse isikustatud reklaame. Profiilianalüüs muutub probleemiks, kui seda kasutatakse üksikisikutega manipuleerimiseks, st otsitakse teatuid isikutüüpe või inimrühmi poliitilise kampaania jaoks. Näiteks saab pöörduda otsustusraskustega valijate poole poliitiliste sõnumitega, mis on kohandatud nende isikuomaduste ja hoiakute järgi. Teine probleem võib olla profiilianalüüsi kasutamine selleks, et piirata teatud isikute juurdepääsu kaupadele ja teenustele. Üks kaitsemeede, mis võib pakkuda kaitset suurandmete ja isikuandmete kuritarvitamise vastu, on pseudonüümimine (vt punkt 2.1.1)[1013]. Kui isikuandmed on tõeliselt anonüümitud, st puuduvad andmesubjektini viiva teabe jäljed, ei kuulu need juhtumid isikuandmete kaitse üldmääruse kohaldamisalasse. Andmesubjektide ja üksikisikute nõusolek suurandmete töötlemisel on probleem ka andmekaitseõiguse seisukohast. See hõlmab nii nõusolekut saada isikustatud reklaame ja lasta enda kohta teha profiilianalüüs, mis võib olla õigustatud kliendikogemuse otstarbel, kui ka nõusolekut kasutada isikuandmete

1012 Euroopa Nõukogu, konventsiooni nr 108 nõuandekomitee (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23. jaanuar 2017.

1013 *Ibid.*, lk 2.

suuri kogumeid, et täiustada ja arendada infopõhiseid analüüsivahendeid. Suurandmete töötlemise teadvustamine või mitteteadvustamine tõstatab küsimusi seoses vahenditega, millega andmesubjektid saavad oma õigusi kasutada, sest suurandmete töötlemine võib tugineda nii pseudonüümitud kui ka anonüümitud andmetele, mille suhtes rakendatakse algoritme. Kuigi pseudonüümitud andmed kuuluvad isikuandmete kaitse üldmääruse kohaldamisalasse, ei kohaldata määrust anonüümitud andmete suhtes. Kontroll oma isikuandmete töötlemise üle ja nende töötlemise teadvustamine on suurandmete analüüsimisel hädavajalik: ilma selleta ei ole üksikisikul selget ettekujutust, kes on vastutav või volitatud töötleja, ja see takistab neil oma õigusi tulemuslikult kasutada.

10.2. Web 2.0 ja 3.0: suhtlusvõrgud ja esemevõrk

Põhipunktid

- Suhtlusvõrgustike teenused on veebipõhised suhtlusplatvormid, mis võimaldavad inimestel liituda sarnaste huvidega kasutajate võrgustikega või selliseid võrgustikke moodustada.
- Esemevõrk ehk asjade internet tähendab esemete ühendamist internetiga ja esemete vastastiksidet.
- Kõige sagedamini kasutavad vastutavad töötlejad suhlusvõrgustikes andmete töötlemise õigusliku alusena andmesubjektide nõusolekut.
- Suhtlusvõrgustiku kasutajad on üldiselt kaitstud koduse tegevuse erandiga, kuid selle erandi võib siiski teatud tingimustel tühistada.
- Suhtlusvõrgustike pakkujaid koduse tegevuse erand ei kaitse.
- Andmeturvalisuse tagamiseks selles valdkonnas on väga olulised lõimitud ja vaikimisi andmekaitse.

10.2.1. Web 2.0 ja 3.0 määratlemine

Suhtlusvõrgustike teenused

Algselt loodi internet arvutite vastastikku ühendamise ja sõnumite edastamise võrguna, mille andmevahetusjõudlus oli piiratud. Esialgu said kasutajad veebilehtede

sisu ainult passiivselt vaadata[1014]. Järgmisel, Web 2.0 ajastul muutus internet foorumiks, kus kasutajad suhtlevad, teevad koostööd ja loovad sisendit. Seda ajastut iseloomustab suhtlusvõrgustike teenuste märkimisväärne edu ja laialdane kasutamine, mis on nüüdseks miljonite inimeste igapäevaelu oluline osa.

Suhtlusvõrgustike teenuseid (sotsiaal- ehk suhtlusmeediat) saab üldiselt määratleda kui interneti suhtlusplatvormi, mis võimaldab inimestel ühineda omasarnaste kasutajate võrgustikega või neid moodustada[1015]. Võrgustikuga liitumiseks või selle moodustamiseks palutakse üksikisikutel anda isikuandmeid ja luua oma profiil. Suhtlusvõrgustike teenused võimaldavad kasutajatel luua digitaalset sisu alates fotodest ja videotest kuni ajalehelinkide ja seisukohti väljendavate isiklike postitusteni. Selliste veebipõhiste suhtlusplatvormide kaudu saavad kasutajad kontakteeruda ja suhelda paljude teiste kasutajatega. On oluline, et enamik populaarseid suhtlusvõrgustikke ei nõua registreerimistasu. Liitumistasu asemel saavad suhtlusvõrgustike teenuste osutajad enamiku tulust suunatud reklaamiga. Reklaamijad saavad suurt kasu isikuandmetest, mida avaldatakse iga päev suhtlusvõrgustike veebilehtedel. Kasutajate vanuse, soo, asukoha ja huvide teave võimaldab neil jõuda oma reklaamidega n-ö õigete inimesteni.

Euroopa Nõukogu ministrite komitee võttis vastu soovituse inimõiguste kaitse kohta seoses suhtlusvõrgustike teenustega,[1016] mille ühes osas käsitletakse andmekaitset ja mida 2018. aastal täiendati soovitusega internetiteenuste vahendajate rollide ja vastutuse kohta[1017].

Näide: Nora on väga õnnelik, sest tema elukaaslane tegi talle abieluettepaneku. Ta tahab jagada head uudist sõpradega ja avaldab suhtlusvõrgustikus rõõmu väljendava emotsionaalse postituse, märkides uueks perekonnaseisuks „kihlatud". Järgmistel päevadel näeb ta kontole sisse logides pulmakleitide ja lillepoodide reklaame. Miks?

1014 Euroopa Komisjon (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

1015 Artikli 29 töörühm (2009), *Opinion 5/2009 on online social networking*, WP 163, 12. juuni 2009, lk 4.

1016 Euroopa Nõukogu ministrite komitee (2012), *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services*, 4. aprill 2012.

1017 Euroopa Nõukogu ministrite komitee (2018), *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries*, 7. märts 2018.

Facebookis reklaami loomise ajal valisid pulmakleitide ja lilledega kauplevad ettevõtted teatud parameetrid, mis võimaldavad neil jõuda selliste inimesteni nagu Nora. Kui Nora profiil näitab, et ta on naine, kihlatud, elab Pariisis reklaame avaldavate kleidi- ja lillepoodide lähedal, näeb ta otsekohe nende reklaame.

Esemevõrk

Esemevõrk ehk asjade internet (IoT) on järgmine samm interneti arendamisel ehk ajastu Web 3.0. Esemevõrgus saab ühendada seadmeid ja need saavad suhelda interneti kaudu teiste seadmetega. See võimaldab seadmetel ja inimestel suhelda sidevõrkude kaudu, teatada oma olekust ja/või ümbruskonna seisundist[1018]. Esemevõrk ja ühendatud seadmed on juba reaalsus ja eeldatavasti see suundumus suureneb lähiaastatel oluliselt, sest luuakse ja arendatakse nutiseadmeid, mis toovad kaasa arukate linnade, kodude ja ettevõtete loomise.

Näide: esemevõrk võib olla eriti kasulik tervishoius. Ettevõtted on juba loonud seadmeid, andureid ja rakendusi, mis võimaldavad jälgida patsiendi tervist. Kaasaskantava häirenupu ja teiste kodus paiknevate juhtmeta andurite abil saab jälgida üksi elavate eakate igapäevatoiminguid ja saata hoiatusi, kui nende toimingutes esineb olulisi häireid. Eakad kasutavad laialdaselt ka kukkumise tuvastusandureid, mis võivad kukkumisi täpselt tuvastada ja teatada neist perearstile ja/või sugulastele.

Näide: Barcelona on üks tuntuimaid aruka linna näiteid. Alates 2012. aastast on linn võtnud kasutusele uuenduslikke tehnoloogiaid, mille eesmärk on luua ühistranspordi, jäätmekäitluse, parkimise ja tänavavalgustuse arukas süsteem. Jäätmekäitluse parandamiseks kasutatakse näiteks arukaid prügikaste, mis jälgivad prügi kogust, et optimeerida prügiautode marsruute. Kui prügikast on peaaegu täis, saadab see mobiilsidevõrgu kaudu signaali jäätmekäitlusettevõtte tarkvararakendusse. Nii saab ettevõte kavandada prügiautode parima marsruudi, eelistades tühjendamist vajavaid prügikaste või tühjendades ainult neid.

1018 Euroopa Komisjon (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19. aprill 2016.

10.2.2. Kasulikkuse ja riskide tasakaalustamine

Suhtlusvõrgustike teenuste kiire laienemine ja edu viimasel kümnendil näitab, et neil on **olulisi eeliseid**. Näiteks on suunatud reklaam (nagu kirjeldatud eespool näites) eriti uuenduslik lahendus, kuidas ettevõtted saavad jõuda sihtrühmani ja mis pakub täpsemat turgu. Ka tarbijatele võib olla kasulikum, kui nad saavad asjakohasemaid ja huvitavamaid reklaame. Olulisem on aga, et suhtlusvõrgustike teenused ja sotsiaalmeedia võivad avaldada positiivset mõju ühiskonnale ja muutuste toimumisele. Need annavad kasutajatele võimaluse neile olulistel teemadel vahetada teavet, suhelda, moodustada rühmi ja korraldada üritusi.

Samamoodi eeldatakse, et esemevõrgust on oluliselt kasu majandusele ja see on osa ELi digitaalse ühtse turu arendamise strateegiast. Hinnangute kohaselt suureneb esemevõrgu ühenduste arv ELis 2020. aastal kuue miljardini. Selline suurem ühenduvus toob eeldatavasti suurt majanduskasu uuenduslike teenuste ja rakenduste arendamise, parema tervishoiu, tarbijate vajaduste parema mõistmise ja suurema tõhususe kaudu.

Samas, arvestades tohutut kogust isikuandmeid, mida sotsiaalmeedia kasutajad loovad ja mida teenust osutavad ettevõtjad seejärel töötlevad, tekitab suhtlusvõrgustike teenuste laienemine **üha suureneva probleemi**, kuidas saab kaitsta eraelu puutumatust ja isikuandmeid. Suhtlusvõrgustike teenused võivad ohustada õigust eraelule ja õigust sõnavabadusele. Sellised ohud võivad olla näiteks õiguslike ja menetluslike kaitsemeetmete puudumine ümbritsevate protsesside puhul, mis võib viia kasutajate välistamiseni; laste ja noorte ebapiisav kaitse kahjuliku sisu või käitumise eest; teiste õiguste austamine; eraelu puutumatust kaitsvate vaikeseadete puudumine; läbipaistvuse puudumine seoses eesmärkidega, milleks isikuandmeid kogutakse ja töödeldakse[1019]. Euroopa andmekaitseõigusega on püütud vastata eraelu puutumatuse ja andmekaitse probleemidele, mis on kaasnenud sotsiaalmeediaga. Sellised põhimõtted nagu nõusolek, lõimitud ja vaikimisi eraelukaitse/andmekaitse ning üksikisikute õigused on eriti olulised sotsiaalmeedia ja võrgustikuteenuste kontekstis.

Esemevõrgu kontekstis põhjustab ohtu eraelu puutumatusele ja andmekaitsele ka paljudest omavahel ühendatud seadmetest saadav tohutu kogus isikuandmeid. Kuigi läbipaistvus on Euroopa andmekaitseõiguse oluline põhimõte, ei ole ühendatud seadmete suure arvu tõttu alati selge, kes saab esemevõrgu seadmetest pärit

1019 Euroopa Nõukogu ministrite komitee (2012), *Rec(2012)4 to member states on the protection of human rights with regard to social networking services*, 4. aprill 2012.

andmeid koguda, nendega tutvuda ja neid kasutada[1020]. Euroopa Liidu ja Euroopa Nõukogu õiguse kohaselt tekitab läbipaistvuse põhimõte siiski kohustuse, et vastutavad töötlejad peavad andma andmesubjektidele selges ja lihtsas keeles teavet, kuidas nende andmeid kasutatakse. Isikuandmete töötlemisega seotud riskid, eeskirjad, kaitsemeetmed ja õigused tuleb asjaomastele isikutele selgeks teha. Esemevõrku ühendatud seadmed, arvukad töötlemistoimingud ja kaasatud andmed võivad samuti muuta keerukaks andmete töötlemiseks vajaliku selge ja teavitatud nõusoleku nõude täitmise, kui töötlemine põhineb nõusolekul. Sageli puudub üksikisikutel arusaam sellise töötlemise tehnilisest toimimisest ja seega ka nende nõusoleku tagajärgedest.

Teine suur probleem on turvalisus, sest ühendatud seadmed on turvariskide suhtes eriti haavatavad. Ühendatud seadmete turvalisuse tase on erinev. Et nad töötavad tavapärasest IT-taristust väljaspool, võib neil puududa piisav töötlemis- ja säilitussuutlikkus, et hostida kasutajate isikuandmete kaitsmiseks turvatarkvara või kasutada selliseid tehnikaid nagu krüpteerimine, pseudonüümimine või anonüümimine.

Näide: Saksamaal otsustasid reguleerivad asutused keelustada internetiga ühendatud mänguasja, kui tekkis tõsine mure mänguasja mõju pärast laste eraelu austamisele. Reguleerivad asutused leidsid, et internetiga ühendatud nukk Cayla oli pigem salajase jälgimise seade. Nukk toimis nii, et edastas mängiva lapse suulised küsimused digitaalseadmes olevale rakendusele, mis muundas need tekstiks ja otsis internetist küsimustele vastuse. Seejärel saatis rakendus vastuse nukule, mis ütles selle lapsele. Nuku kaudu võidi salvestada lapse ja lähedal viibivate täiskasvanute suhtlust ning edastada see rakendusele. Kui nuku tootjad ei oleks võtnud piisavaid turvameetmeid, oleks kes tahes saanud nuku abil vestlusi kuulata.

10.2.3. Andmekaitseküsimused

Nõusolek

Euroopas on isikuandmete töötlemine seaduslik ainult siis, kui see on lubatud Euroopa andmekaitseõiguse alusel. Suhtlusvõrgustike teenuste osutajate korral annab üldjuhul andmetöötluseks seadusliku aluse andmesubjektide nõusolek. Nõusolek peab olema vabatahtlik, konkreetne, teavitatud ja ühemõtteline

1020 Euroopa Andmekaitseinspektor (2017), *Understanding the Internet of Things*.

(vt punkt 4.1.1)[1021]. „Vabatahtlikult antud" tähendab sisuliselt, et andmesubjektidel peab olema võimalik teha tegelik ja tõeline valik. Nõusolek on „konkreetne" ja „teavitatud", kui see on arusaadav, viidates selgelt ja täpselt andmetöötluse täielikule ulatusele, eesmärkidele ja tagajärgedele. Sotsiaalmeedia kontekstis saab küsida, kas nõusolek on vabatahtlik, konkreetne ja teavitatud igat liiki töötluse korral, mida teevad suhtlusvõrgustike teenuseid osutav ettevõtja või kolmandad isikud.

Näide: suhtlusvõrgustike teenustega liitumiseks ja neile juurdepääsuks peavad inimesed sageli nõustuma oma isikuandmete mitmesuguse töötlemisega, ilma et nad saaksid vajalikke täpsemaid selgitusi või valikuvõimalusi. Näide: suhtlusvõrgustiku teenusega liitumiseks on vaja anda nõusolek saada käitumispõhist reklaami. Artikli 29 töörühm märgib arvamuses nõusoleku mõiste kohta: „Arvestades teatud suhtlusvõrgustike tähtsust, nõustuvad teatud kasutajad (nt teismelised) käitumispõhise reklaami saamisega, et vältida sotsiaalsest suhtlemisest osalise väljajäämise riski. Kasutajal peaks olema võimalik anda vabatahtlik ja konkreetne nõusolek käitumispõhise reklaami saamiseks, mis ei ole seotud juurdepääsuga suhtlusvõrgustiku teenustele."[1022]

Isikuandmete kaitse üldmääruse kohaselt ei saa alla 16-aastaste laste isikuandmeid põhimõtteliselt nende nõusoleku alusel töödelda[1023]. Kui töötlemiseks on vaja nõusolekut, peab selle andma lapsevanem või eestkostja. Lapsed väärivad erilist kaitset, sest nad võivad olla vähem teadlikud andmetöötluse riskidest ja tagajärgedest. See on sotsiaalmeedia kontekstis väga oluline, sest lapsed on kaitsetumad teatud kahjuliku mõju suhtes, mis võib kaasneda selliste meediakanalite kasutamisega, näiteks küberkuritegevus, küberkiusamine või identiteedivargus.

Turvalisus ja lõimitud ning vaikimisi eraelukaitse/andmekaitse

Isikuandmete töötlemisega kaasnevad olemuslikud turvariskid, sest pidevalt on võimalik, et töödeldavaid isikuandmed võidakse juhuslikult või ebaseaduslikult hävitada, kaotada, muuta, saada neile volitamata juurdepääs või need avalikustada. ELi andmekaitseõiguses nõutakse, et vastutavad ja volitatud töötlejad võtaksid sobivaid tehnilisi ja korralduslikke meetmeid, et hoida andmetöötlustoimingute puhul ära mis

1021 Isikuandmete kaitse üldmääruse artiklid 4 ja 7; nüüdisajastatud konventsiooni nr 108 artikkel 5.

1022 Artikli 29 töörühm (2011), *Opinion 15/2011 on the definition of consent*, WP 187, 13. juuli 2011, lk 18.

1023 Vt isikuandmete kaitse üldmääruse artikkel 8. ELi liikmesriigid võivad seadusega sätestada madalama asjaomase vanuse, kui see ei ole alla 13 eluaasta.

tahes ebaseaduslikke sekkumisi. Seda kohustust peavad täitma ka Euroopa andmekaitse-eeskirjade kohaldamisalasse kuuluvad suhtlusvõrgustike teenuste osutajad.

Lõimitud ja vaikimisi eraelukaitse/andmekaitse põhimõtted eeldavad, et vastutavad töötlejad säilitavad toodete väljatöötamisel turvalisuse ja kohaldavad automaatselt asjakohaseid eraelu- ja andmekaitsesätteid. See tähendab, et kui inimene otsustab liituda suhtlusvõrgustikuga, ei tohi teenuseosutaja automaatselt anda kogu teavet uue teenusekasutaja kohta kõigile oma kasutajatele. Teenusega liitumisel peaksid eraelukaitse ja andmekaitse vaikesätted olema sellised, et teave on kättesaadav ainult isiku valitud kontaktidele. Juurdepääsu laiendamine inimestele, kes ei kuulu kontaktide loetellu, peaks olema võimalik alles pärast seda, kui kasutaja on muutnud eraelukaitse ja andmekaitse vaikesätteid käsitsi. See võib mõjutada ka juhtumeid, kus andmetega seotud rikkumine toimub kehtestatud turvameetmetele vaatamata. Sellistel juhtudel peavad teenuseosutajad asjaomaseid kasutajaid teavitama, kui see põhjustab tõenäoliselt suure ohu andmesubjekti õigustele ja vabadustele[1024].

Lõimitud ja vaikimisi eraelukaitse/andmekaitse on eriti tähtsad suhtlusvõrgustike teenuste korral, sest lisaks peaaegu igat liiki töötlemisega kaasnevale volitamata juurdepääsu riskile põhjustab isikuandmete jagamine täiendavaid turvariske. Sageli on selle põhjuseks, et ei mõisteta, *kellel* võib olla nende teabele juurdepääs ja kuidas need inimesed võivad seda teavet kasutada. Sotsiaalmeedia laialdase kasutamisega on suurenenud identiteedivarguse juhtumite ja selle ohvrite arv.

Näide: identiteedivargus on nähtus, kui isik saab enda valdusse teisele isikule (ohvrile) kuuluva teabe, andmed või dokumendid ning kasutab seejärel seda teavet, et saada ohvri nimel kaupu ja teenuseid. Näide: Paulil on konto sotsiaalmeedia veebisaidil. Paul on õpetaja ja kogukonna aktiivne liige, väga hea suhtleja ja ta ei muretse eriti oma sotsiaalmeedia konto privaatsus- ega andmekaitsesätete pärast. Tema sõbraloetelu on pikk ja mõnda nendest ei tunne ta isiklikult. Ta töötab suures koolis ja on kooli jalgpallimeeskonna treenerina üsna tuntud, seega ta arvab, et tõenäoliselt on nad tema õpilaste vanemad või kooliga seotud sõbrad. Pauli sotsiaalmeedia kontol on näha tema e-posti aadress ja sünnipäev. Sageli postitab Paul fotosid oma koerast Tobyst, koos näiteks sellise tekstiga nagu „Mina ja Toby hommikul jooksmas“. Paul ei ole taibanud, et üks tavalisimaid turvaküsimusi, millega

1024 *Ibid.*, artikkel 34.

kaitstakse e-posti või mobiiltelefoni kontot, on „Mis on su lemmiklooma nimi?“. Pauli sotsiaalmeedia profiilis olevat teavet kasutades on Nickil lihtne Pauli kontodele sisse murda.

Üksikisikute õigused

Suhtlusvõrgustike teenused peavad austama üksikisikute õigusi (vt peatükk 6.1), sealhulgas õigust olla teavitatud isikuandmete töötlemise eesmärgist ja sellest, kuidas isikuandmeid võidakse kasutada otseturunduse eesmärgil. Üksikisikutele tuleb anda õigus tutvuda nende isikuandmetega, mida nad on loonud suhtlusvõrgustiku platvormil, ja taotleda nende kustutamist. Isegi kui inimesed on nõustunud isikuandmete töötlemisega ja laadinud veebi üles teavet, peab neil olema võimalus taotleda õigust olla unustatud, kui nad ei soovi enam saada suhtlusvõrgustiku teenuseid. Andmete ülekandmine võimaldab kasutajatel saada ka suhtlusvõrgustiku teenuste osutajale antud isikuandmetest struktureeritud, üldkasutatavas ja masinloetavas vormingus koopia ning kanda oma andmed ühelt suhtlusvõrgustiku teenuste osutajalt teisele üle[1025].

Vastutavad töötlejad

Sotsiaalmeedia kontekstis tekib sageli keerukas küsimus: kes on vastutav töötleja ehk isik, kellel on kohustus ja vastutus täita andmekaitse-eeskirju. Euroopa andmekaitseõiguse kohaselt loetakse suhtlusvõrgustike teenuste osutajaid vastutavateks töötlejateks. See on ilmselge, arvestades mõiste „vastutav töötleja“ laia määratlust ja asjaolu, et need teenuseosutajad määravad üksikisikute jagatud isikuandmete töötlemise eesmärgi ja vahendid. ELi õiguse kohaselt peavad vastutavad töötlejad, kes pakuvad teenuseid andmesubjektidele ELis, vastama isikuandmete kaitse üldmääruse sätetele isegi siis, kui nad ei ole ELis asutatud.

Kas vastutavateks töötlejateks võib siiski pidada ka suhtlusvõrgustike teenuste kasutajaid? Kui üksikisikud töötlevad isikuandmeid „eranditult isiklike või koduste tegevuste käigus“, andmekaitse-eeskirju ei kohaldata. Euroopa andmekaitseõiguses nimetatakse seda koduse tegevuse erandiks. Mõnel juhul ei pruugi koduse tegevuse erand hõlmata suhtlusvõrgustiku teenuse kasutajat.

1025 Isikuandmete kaitse üldmääruse artikkel 21.

Kasutajad jagavad oma isikuandmeid veebis vabatahtlikult. Samas sisaldab veebis jagatud teave sageli ka teiste isikute isikuandmeid.

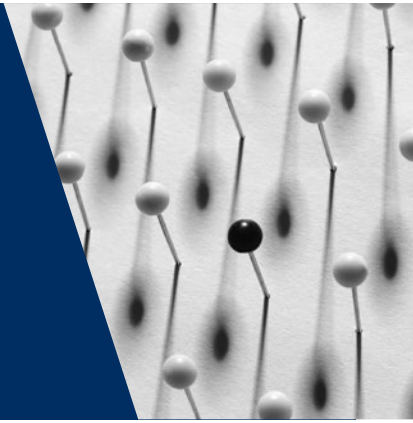
> Näide: Paulil on konto väga populaarsel suhtlusvõrgustiku platvormil. Paul tahab saada näitlejaks ja postitab kontol oma kunstikirge väljendavaid fotosid, videoid ja kirjutisi. Populaarsus on tema tuleviku jaoks tähtis; ta on seega otsustanud, et tema profiil peab olema kättesaadav peale tema sõbraloetelu ka kõigile internetikasutajatele, olenemata sellest, kas nad on tema tuttavad või mitte. Kas Paul võib postitada fotosid ja videoid, millel on tema ja sõber Sarah, ilma viimase nõusolekuta? Algkooliõpetajana töötav Sarah püüab varjata oma eraelu tööandja, õpilaste ja nende vanemate eest. Kujutage ette, kuidas Sarah, kes ei kasuta suhtlusvõrgustikke, saab ühise sõbra Nicki käest teada, et peofoto temast ja Paulist on internetis. Sellisel juhul ei kuulu see, et Paul töötleb andmeid, ELi õiguse kohaldamisalasse, sest see kuulub koduse tegevuse erandi alla.

On siiski oluline, et kasutajad teadvustaksid ja arvestaksid, et teiste isikute kohta teabe üleslaadimine ilma nende nõusolekuta võib rikkuda nende õigust eraelu puutumatusele ja andmekaitseõigusele. Isegi kui koduse tegevuse erand kehtib – näiteks kui kasutajal on profiil, mis on avalik ainult tema valitud sõpradele –, võib teiste isikute kohta teabe avaldamine muuta kasutaja vastutavaks. Kuigi koduse tegevuse erandi korral andmekaitse-eeskirju ei kohaldata, võib vastutus tuleneda muude, näiteks laimamist või isikupuutumatuse rikkumist käsitlevate riiklike eeskirjade kohaldamisest. Koduse tegevuse erandiga on kaitstud ainult sotsiaalvõrgustike teenuste kasutajad – sellist eratöötlust pakkuvad vastutavad ja volitatud töötlejad kuuluvad ELi andmekaitseõiguse kohaldamisalasse[1026].

Eraelu puutumatuse ja elektroonilise side direktiivi reformiga kohaldatakse andmekaitse-, eraelu puutumatuse ja turvalisuse eeskirju, mida praeguses õigusraamistikus kohaldatakse sideteenuste osutajatele, ka masinatevahelise ja elektroonilise side teenuste, sealhulgas interneti kaudu pakutavate teenuste (OTT-teenused) suhtes.

1026 *Ibid.*, põhjendus 18.

Lisateave



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*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C., „Four fundamental rights: finding the balance", *International Data Privacy Law*, 6. aastakäik, nr 3, lk 195–209.

EDRi, *An introduction to data protection*, Brussels.

Frowein, J. ja Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. ja Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, 26. aastakäik (1), lk 73–82.

Grabenwarter, C. ja Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. ja Nouwt, S. (toim.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. ja Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), „EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation".

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. ja Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, 3. aastakäik, nr 4, lk 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, 1. aastakäik, nr 1, lk 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, 63. aastakäik, nr 3, lk 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

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*, Antwerp, 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*, Bruxelles, 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. aastakäik, nr 5, lk 193–220.

White, R. ja Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

2. peatükk

Acquisty, A. ja Gross R. (2009), „Predicting Social Security numbers from public data“, *Proceedings of the National Academy of Science*, 7. juuli 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. ja Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, 3. kd, 2013.

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*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

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*, 57. aastakäik, nr 6, lk 1701–1777.

Samarati, P. ja Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy“, *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 10. aastakäik, nr 5, lk 557–570.

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*.

3.–6. peatükk

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ 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*, Saarbrucken, Éditions universitaires européennes.

Curren, L. ja Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?“, *Computer Law & Security Review*, 26. aastakäik, nr 3, lk 273–283.

Dammann, U. ja Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. ja Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, 22. aastakäik, nr 6, lk 1–5.

De Hert, P. ja Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals“, *Computer Law & Security Review*, 28. aastakäik, nr 2, lk 130–142.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, 20. aastakäik, nr 2, lk 473–506.

FRA (Euroopa Liidu Põhiõiguste Amet) (2010), *Data Protection in the European Union: the role of National Supervisory 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* (konverentsiväljaanne), Viin, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Euroopa Liidu Väljaannete Talitus.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. ja Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, 27. aastakäik, nr 3, lk 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

7. peatükk

Artikli 29 töörühm (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*.

Euroopa Andmekaitseinspektor (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. ja Nouwt, S. (2009), *Reinventing data protection?*, Berlin, 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.

8. peatükk

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. ja Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, 22. aastakäik, nr 6, lk 1–5.

Drewer, D. ja Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, 13. aastakäik, nr 3, lk 381–395.

Europol (2012), *Data Protection at Europol*, Luxembourg, Euroopa Liidu Väljaannete Talitus.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, 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*, 36. aastakäik, 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.

9. 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*, 36. aastakäik, nr 5, lk 722–776.

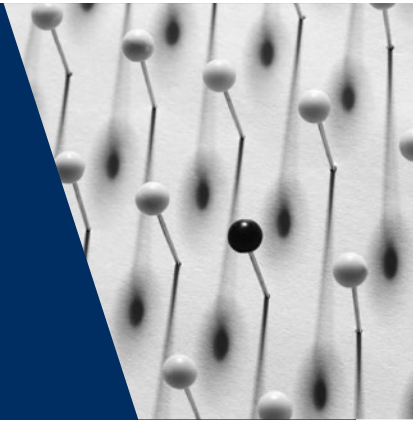
Rosemary, J. ja Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

10. peatükk

El Emam, K. ja Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, 5. aastakäik, nr 1, lk 73–87.

Mayer-Schönberger, V. ja Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, 3. aastakäik, nr 2, lk 67–73.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, 3. aastakäik, nr 2, lk 74–87.



Kohtupraktika

Valitud kohtuasjad Euroopa Inimõiguste Kohtu kohtupraktikast

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
M.K. vs. Prantsusmaa, nr 19522/09, 18. aprill 2013
Odièvre vs. Prantsusmaa [suurkoda], nr 42326/98, 13. veebruar 2003

Andmekaitse ning sõnavabaduse ja teabeõiguse tasakaalustamine
Axel Springer AG vs. Saksamaa [suurkoda], nr 39954/08, 7. veebruar 2012
Bohlen vs. Saksamaa, nr 53495/09, 19. veebruar 2015
Coudec and Hachette Filipacchi Associés vs. Prantsusmaa [suurkoda], nr 40454/07, 10. november 2015
Magyar Helsinki Bizottság vs. Ungari [suurkoda], nr 18030/11, 8. november 2016
Müller jt vs. Šveits, nr 10737/84, 24. mai 1988
Satakunnan Markkinapörssi Oy ja Satamedia Oy vs. Soome [suurkoda], nr 931/13, 27. juuni 2017
Vereinigung bildender Künstler vs. Austria, nr 68354/01, 25. jaanuar 2007
Von Hannover vs. Saksamaa (nr 2) [suurkoda], nr 40660/08 ja nr 60641/08, 7. veebruar 2012

Andmeturve
Haralambie vs. Rumeenia, nr 21737/03, 27. oktoober 2009
K.H. jt vs. Slovakkia, nr 32881/04, 28. aprill 2009

DNA-andmebaasid
S. ja Marper vs. Ühendkuningriik [suurkoda], nr 30562/04 ja nr 30566/04, 4. detsember 2008

GPS-andmed
Uzun vs. Saksamaa, nr 35623/05, 2. september 2010

Terviseandmed
Avilkina jt vs. Venemaa, nr 1585/09, 6. juuni 2013
Biriuk vs. Leedu, nr 23373/03, 25. november 2008
I vs. Soome, nr 20511/03, 17. juuli 2008
L.H. vs. Läti, nr 52019/07, 29. aprill 2014
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
Y vs. Türgi, nr 648/10, 17. veebruar 2015
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

Kutsetegevuse teave
G.S.B. vs. Šveits, nr 28601/11, 22. detsember 2015
M.N. jt vs. San Marino, nr 28005/12, 7. juuli 2015
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
Brito Ferrinho Bexiga Villa-Nova vs. Portugal, nr 69436/10, 1. detsember 2015
Copland vs. Ühendkuningriik, nr 62617/00, 3. aprill 2007
Halford vs. Ühendkuningriik, nr 20605/92, 25. juuni 1997
Iordachi jt vs. Moldova, nr 25198/02, 10. veebruar 2009

Kopp vs. Šveits, nr 23224/94, 25. märts 1998
Liberty jt vs. Ühendkuningriik, nr 58243/00, 1. juuli 2008
Malone vs. Ühendkuningriik, nr 8691/79, 2. august 1984
Mustafa Sezgin Tanrıkulu vs. Türgi, nr 27473/06, 18. juuli 2017
Pruteanu vs. Rumeenia, nr 30181/05, 3. veebruar 2015
Szuluk vs. Ühendkuningriik, nr 36936/05, 2. juuni 2009

Vastutajate 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

Isikuandmed
Amann vs. Šveits [suurkoda], nr 27798/95, 16. veebruar 2000
Bernh Larsen Holding AS jt vs. Norra, nr 24117/08, 14. märts 2013
Uzun vs. Saksamaa, nr 35623/05, 2010

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

Õigus olla unustatud
Satakunnan Markkinapörssi Oy ja Satamedia Oy vs. Soome [suurkoda], nr 931/13, 27. juuni 2017
Segerstedt-Wiberg jt vs. Rootsi, nr 62332/00, 6. juuni 2006

Õigus esitada vastuväiteid
Leander vs. Rootsi, nr 9248/81, 26. märts 1987
M.S. vs. Rootsi, nr 20837/92, 27. august 1997
Mosley vs. Ühendkuningriik, nr 48009/08, 10. mai 2011
Rotaru vs. Rumeenia [suurkoda], nr 28341/95, 4. mai 2000
Sinan Işık vs. Türgi, nr 21924/05, 2. veebruar 2010

Eriliigiliste isikuandmete kategooriad
Brunet vs. Prantsusmaa, nr 21010/10, 18. september 2014
I vs. Soome, nr 20511/03, 17. juuli 2008
Michaud vs. Prantsusmaa, nr 12323/11, 6. detsember 2012
S. ja Marper vs. Ühendkuningriik [suurkoda], nr 30562/04 ja nr 30566/04, 4. detsember 2008

Järelevalve ja nõuete täitmise kontrollimine (eri osaliste, sh järelevalveasutuste 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 nr 60641/08, 7. veebruar 2012

Jälgimismeetodid
Allan vs. Ühendkuningriik, nr 48539/99, 5. november 2002
Association for European Integration and Human Rights ja Ekimdzhiev vs. Bulgaaria, nr 62540/00, 28. juuni 2007
Bărbulescu vs. Rumeenia [suurkoda], nr 61496/08, 5. september 2017
D.L. vs. Bulgaaria, nr 7472/14, 19. mai 2016
Dragojević vs. Horvaatia, nr 68955/11, 15. jaanuar 2015
Karabeyoğlu vs. Türgi, nr 30083/10, 7. juuni 2016
Klass jt vs. Saksamaa, nr 5029/71, 6. september 1978
Roman Zakharov vs. Venemaa [suurkoda], nr 47143/06, 4. detsember 2015
Rotaru vs. Rumeenia [suurkoda], nr 28341/95, 4. mai 2000
Szabó ja Vissy vs. Ungari, nr 37138/14, 12. jaanuar 2016
Taylor-Sabori vs. Ühendkuningriik, nr 47114/99, 22. oktoober 2002
Uzun vs. Saksamaa, nr 35623/05, 2. september 2010
Versini-Campinchi ja Crasnianski vs. Prantsusmaa, nr 49176/11, 16. juuni 2016
Vetter vs. Prantsusmaa, nr 59842/00, 31. mai 2005
Vukota-Bojić vs. Šveits, nr 61838/10, 18. oktoober 2016

Videovalve
Köpke vs. Saksamaa, nr 420/07, 5. oktoober 2010
Peck vs. Ühendkuningriik, nr 44647/98, 28. jaanuar 2003

Häälsalvestis
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 kohtupraktikast

Andmekaitsedirektiiviga seotud kohtupraktika

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*, 4. mai 2017
[Seadusliku töötlemise põhimõte: kolmanda isiku õigustatud huvi]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs. Salvatore Manni*, 9. märts 2017
[Õigus isikuandmete kustutamisele; õigus vaidlustada töötlemist]

Liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen* ja *Secretary of State for the Home Department vs. Tom Watson jt* [suurkoda], 21. detsember 2016.
[Elektroonilise side konfidentsiaalsus; elektroonilise side teenuste osutajad; andmeliiklus- ja asukohaandmete üldise ja valimatu säilitamisega seotud kohustus; puudub kohtu või sõltumatu haldusasutuse eelnev läbivaatamine; Euroopa Liidu põhiõiguste harta; kooskõla ELi õigusega]

C-582/14, *Patrick Breyer vs. Bundesrepublik Deutschland*, 19. oktoober 2016
[Isikuandmete määratlus; IP-aadressid; andmete säilitamine elektrooniliste teabe- ja sideteenuste pakkuja poolt; riigisisesed õigusaktid, mis ei võimalda arvestada vastutava töötleja õigustatud huvi]

C-362/14, *Maximillian Schrems vs. Data Protection Commissioner* [suurkoda], 6. oktoober 2015
[Seadusliku töötlemise põhimõte; põhiõigused; programmi Safe Harbor käsitleva otsuse kehtetuks tunnistamine; sõltumatute järelevalveasutuste volitused]

C-230/14, *Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. oktoober 2015
[Liikmesriigi järelevalveasutuste volitused]

C-201/14, *Smaranda Bara jt vs. Casa Națională de Asigurări de Sănătate jt*, 1. oktoober 2015
[Õigus olla teavitatud isikuandmete töötlemisest]

C-212/13, *František Ryneš vs. Úřad pro ochranu osobních údajů*, 11. detsember 2014
[Mõisted „andmetöötlus" ja „vastutav töötleja"]

C-473/12, *Institut professionnel des agents immobiliers (IPI) vs. Geoffrey Englebert jt*, 7. november 2013
[Õigus olla teavitatud isikuandmete töötlemisest]

T-462/12 R, *Pilkington Group Ltd vs. Euroopa Komisjon*, Üldkohtu presidendi määrus, 11. märts 2013

C-342/12, *Worten – Equipamentos para o Lar SA vs. Autoridade para as Condições de Trabalho (ACT)*, 30. mai 2013
[Mõiste „isikuandmed"; tööaja arvestus; andmete kvaliteedi põhimõtted ja andmete töötlemise õiguspärasuse kriteeriumid; töötingimuste järelevalve riikliku ametiasutuse juurdepääs; tööandja kohustus teha kättesaadavaks tööaja arvestus, et võimaldada sellega viivitamatult tutvuda]

Liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources jt* ja *Kärntner Landesregierung jt* [suurkoda], 8. aprill 2014
[ELi esmaste õigusaktide rikkumine andmete säilitamise direktiiviga; seaduslik töötlemine; eesmärgi ja säilitamise piirang]

C-288/12, *Euroopa Komisjon vs. Ungari* [suurkoda], 8. aprill 2014
[Riigi andmekaitseinspektori ametist kõrvaldamise õiguspärasus]

Liidetud kohtuasjad C-141/12 ja C-372/12, *YS vs. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vs. M ja S*, 17. juuli 2014
[Andmesubjekti andmetega tutvumise õiguse ulatus; üksikisikute kaitse isikuandmete töötlemisel; mõiste „isikuandmed"; elamisloa taotleja andmed ja õiguslik analüüs, mis sisaldub otsust ettevalmistavas haldusdokumendis; Euroopa Liidu põhiõiguste harta]

C-131/12, *Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [suurkoda], 13. mai 2014
[Otsingumootorite haldajate kohustus tagada andmesubjekti taotlusel, et tema isikuandmeid ei näidata otsingutulemustes; andmekaitsedirektiivi kohaldatavus; mõiste „andmetöötlus"; mõiste „vastutavad töötlejad" tähendus; andmekaitse ja sõnavabaduse tasakaalustamine; õigus olla unustatud]

C-614/10, *Euroopa Komisjon vs. Austria Vabariik* [suurkoda], 16. oktoober 2012
[Liikmesriigi järelevalveasutuse sõltumatus]

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-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vs. Netlog NV*, 16. veebruar 2012
[Suhtlusvõrgustike haldajate kohustus takistada võrgustike kasutajatel muusika- ja audiovisuaalteoste ebaseaduslikku kasutamist]

C-70/10, *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011
[Infoühiskond; autoriõigus; internet; võrdõigustarkvara; internetiteenuse osutajad; elektroonilise side filtreerimissüsteemi rakendamine autoriõigusi rikkuva failivahetuse takistamiseks; edastatava teabe üldise jälgimiskohustuse puudumine]

C-543/09, *Deutsche Telekom AG vs. Bundesrepublik Deutschland*, 5. mai 2011
[Uue nõusoleku vajalikkus]

Liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen* [suurkoda], 9. november 2010
[Isikuandmete mõiste; teatud ELi põllumajandusfondide toetusesaajate isikuandmete avaldamisega seotud juriidilise kohustuse proportsionaalsus]

C-553/07, *College van burgemeester en wethouders van Rotterdam vs. M. E. E. Rijkeboer*, 7. mai 2009
[Andmesubjekti õigus tutvuda andmetega]

C-518/07, *Euroopa Komisjon vs. Saksamaa Liitvabariik* [suurkoda], 9. märts 2010
[Liikmesriigi järelevalveasutuse sõltumatus]

C-73/07, *Tietosuojavaltuutettu vs. Satakunnan Markkinapörssi Oy ja Satamedia Oy* [suurkoda], 16. detsember 2008
[Ajakirjandusliku tegevuse mõiste andmekaitsedirektiivi artikli 9 tähenduses]

C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], 16. detsember 2008
[Välismaalastega seotud andmete säilitamine statistikaregistris ja selle õiguspärasus]

C-275/06, *Productores de Música de España (Promusicae) vs. Telefónica de España SAU* [suurkoda], 29. jaanuar 2008
[Mõiste „isikuandmed"; internetiteenuste osutajate kohustus avaldada failivahetusprogrammi KaZaA kasutajate isikud intellektuaalomandi kaitse ühendusele]

C-101/01, *Kriminaalasi, milles süüdistatav on Bodil Lindqvist*, 6. november 2003
[Isikuandmete eriliigid]

Liidetud kohtuasjad C-465/00, C-138/01 ja C-139/01, *Rechnungshof vs. Österreichischer Rundfunk jt* ja *Christa Neukomm ja Jospeh Lauermann vs. Österreichischer Rundfunk*, 20. mai 2003
[Juriidiline kohustus avaldada avaliku sektoriga seotud asutustes töötavate ja teatud kategooriatesse kuuluvate isikute palgaandmeid ning selle õiguspärasus]

C-434/16, *Peter Nowak vs. Data Protection Commissioner*, kohtujuristi ettepanek, Juliane Kokott, 20. juuli 2017
[Mõiste „isikuandmed"; juurdepääs enda eksamitööle; eksamineerija tehtud parandused]

C-291/12, *Michael Schwarz vs. Stadt Bochum*, 17. oktoober 2013
[Eelotsusetaotlus; vabadusel, turvalisusel ja õigusel rajanev ala; biomeetriline pass; sõrmejäljed; õiguslik alus; proportsionaalsus]

Direktiiviga (EL) 2016/681 seotud kohtupraktika

Euroopa Kohtu (suurkoda) arvamus 1/15, 26. juuli 2017
[Õiguslik alus; Kanada ja Euroopa Liidu vahelise broneeringuinfo edastamist ja töötlemist käsitleva lepingu eelnõu; broneeringuinfo; lepingu eelnõu vastavus ELi toimimise lepingu artiklile 16 ning Euroopa Liidu põhiõiguste harta artiklitele 7 ja 8 ja artikli 52 lõikele 1]

ELi institutsioonide andmekaitse määrusega seotud kohtupraktika

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) vs. Euroopa Toiduohutusamet (EFSA), Euroopa Komisjon*, 16. juuli 2015
[Juurdepääs dokumentidele]

C-28/08 P, *Euroopa Komisjon vs. The Bavarian Lager Co. Ltd.* [suurkoda], 29. juuni 2010
[Juurdepääs dokumentidele]

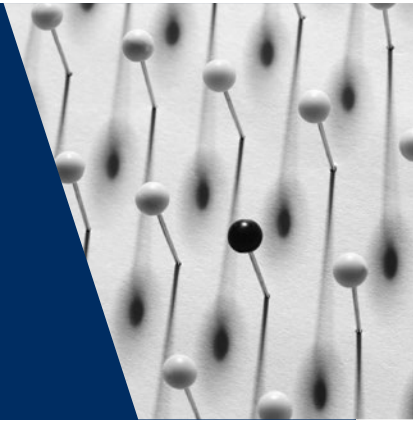
Direktiiviga 2002/58/EÜ seotud kohtupraktika

C-536/15, *Tele2 (Netherlands) BV jt vs. Autoriteit Consument en Markt (AMC)*, 15. märts 2017
[Diskrimineerimiskeelu põhimõte; abonentide isikuandmete avaldamine üldkasutatavate numbriinfo- ja kataloogiteenuse osutamiseks; abonendi nõusolek; eristamine selle alusel, mis liikmesriigis osutatakse üldkasutatavat numbriinfo- ja kataloogiteenust]

Liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen* ja *Secretary of State for the Home Department vs. Tom Watson jt* [suurkoda], 21. detsember 2016
[Elektroonilise side konfidentsiaalsus; elektroonilise side teenuste osutajad; andmeliiklus- ja asukohaandmete üldise ja valimatu säilitamisega seotud kohustus; puudub kohtu või sõltumatu haldusasutuse eelnev läbivaatamine; Euroopa Liidu põhiõiguste harta; kooskõla ELi õigusega]

C-70/10, *Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. november 2011
[Infoühiskond; autoriõigus; internet; võrdõigustarkvara; internetiteenuse osutajad; elektroonilise side filtreerimissüsteemi rakendamine autoriõigusi rikkuva failivahetuse takistamiseks; edastatava teabe üldise jälgimiskohustuse puudumine]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB vs. Perfect Communication Sweden AB*, 19. aprill 2012
[Autoriõigus ja seonduvad õigused; andmete töötlemine interneti teel; ainuõiguse rikkumine; audioraamatud, mis on tehtud kättesaadavaks FTP-serveri kaudu interneti teel IP-aadressilt, mille on andnud internetiteenuste osutaja; internetiteenuste osutajale tehtud ettekirjutus avaldada IP-aadressi kasutaja nimi ja aadress]



Register

Euroopa Liidu Kohtu kohtupraktika

Euroopa Inimõiguste Kohtu kohtupraktika

Riigisiseste kohtute kohtupraktika

Euroopa Liidu Põhiõiguste Ameti kohta on palju teavet internetis. See on FRA veebilehel aadressil fra.europa.eu

Lisainfo Euroopa Inimõiguste Kohtu praktikast on kättesaadav Kohtu veebilehel: 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 (https://hudoc.echr.coe.int).

Kuidas hankida Euroopa Nõukogu väljaandeid?

Euroopa Nõukogu kirjastus avaldab materjale kõigis organisatsiooni töövaldkondades, mis hõlmavad inimõigusi, õigusteadust, tervishoidu, eetikat, sotsiaalala, keskkonda, haridust, kultuuri, sporti, noorsugu ja arhitektuuripärandit. Laias valikus raamatuid ja elektroonilisi publikatsioone saab tellida intenetist (http://book.coe.int).

Virtuaalne lugemistuba võimaldab kasutajatel tasuta tutvuda väljavõtetega värskelt avaldatud teostest või teatud ametlike dokumentide täistekstidega.

Informatsioon Euroopa Nõukogu Lepingute kohta koos lepingutekstidega on kättesaadav lepingubüroo veebilehel http://conventions.coe.int

Ühenduse võtmine ELiga

Isiklikult

Kõikjal Euroopa Liidus on sadu Europe Directi teabekeskusi. Teile lähima keskuse aadressi leiate: https://europa.eu/european-union/contact_et

Telefoni või e-postiga

Europe Direct on teenus, mis vastab Teie küsimustele Euroopa Liidu kohta. Teenusega saate ühendust võtta:

— helistades tasuta numbril: 00 800 6 7 8 9 10 11 (mõni operaator võib nende kõnede eest tasu võtta),
— helistades järgmisel tavanumbril: +32 2299 9696 või
— e-posti teel: https://europa.eu/european-union/contact_et

ELi käsitleva teabe leidmine

Veebis

Euroopa Liitu käsitlev teave on kõigis ELi ametlikes keeltes kättesaadav Euroopa veebisaidil: https://europa.eu/european-union/index_et

ELi väljaanded

Tasuta ja tasulisi ELi väljaandeid saab alla laadida või tellida EU Bookshopi kaudu: https://op.europa.eu/et/publications. Suuremas koguses tasuta väljaannete saamiseks võtke ühendust talitusega Europe Direct või oma kohaliku teabekeskusega (vt https://europa.eu/european-union/contact_et)

ELi õigus ja seonduvad dokumendid

ELi käsitleva õigusteabe, sealhulgas alates 1951. aastast kõigi ELi õigusaktide konsulteerimiseks kõigis ametlikes keeleversioonides vt EUR-Lex: http://eur-lex.europa.eu

ELi avatud andmed

ELi avatud andmete portaal (http://data.europa.eu/euodp/et) võimaldab juurdepääsu ELi andmekogudele. Andmeid saab tasuta alla laadida ja taaskasutada nii ärilisel kui ka mitteärilisel eesmärgil.

doi:10.2811/383697 TK-05-17-225-ET-N

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

EDPS

Infotehnoloogia hoogne areng on teravdanud vajadust tugeva isikuandmete kaitse järele, sest õigus isikuandmete kaitsele on sätestatud nii Euroopa Liidu kui ka Euroopa Nõukogu õigusaktides. Selle olulise õiguse tagamisel tekib uusi ja olulisi probleeme, sest tehnika areng laiendab selliseid valdkondi nagu seire, side pealtkuulamine ja andmete säilitamine. Käsiraamatu eesmärk on tutvustada andmekaitset kui arenevat õigusvaldkonda juristidele, kes ei ole andmekaitse spetsialistid. Käsiraamatus on ülevaade kohaldatavatest Euroopa Liidu ja Euroopa Nõukogu õigusraamistikest. Olulisi kohtuasju selgitatakse Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu kohtulahendite kokkuvõtetega. Lisaks esitatakse hüpoteetilisi stsenaariume, mis illustreerivad selles pidevalt arenevas valdkonnas tekkida võivaid probleeme.

FRA – EUROOPA LIIDU PÕHIÕIGUSTE AMET
Schwarzenbergplatz 11 – 1040 Viin – Austria
Tel +43 158030-0 – Faks +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EUROOPA INIMÕIGUSTE KOHUS
EUROOPA NÕUKOGU
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 – twitter.com/ECHR_CEDH

EUROOPA ANDMEKAITSEINSPEKTOR
Rue Wiertz 60 – 1047 Brüssel – Belgia
Tel +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

Euroopa Liidu Väljaannete Talitus

ISBN978-92-871-9833-4(EuroopaNõukogu)
ISBN 978-92-9474-446-3 (FRA)